# CA IdentityMinder™

## Connectors Guide

r12.6.1

technologies

# CA Technologies Product References

This document references the following CA Technologies products:

- CA IdentityMinder ™
- CA SiteMinder®
- CA Directory
- CA User Activity Reporting (CA UAR)
- CA CloudMinder™ Identity Management
- GovernanceMinder (Formerly called CA Role & Compliance Manager)

# Contact CA Technologies

**Contact CA Support**

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

**Providing Feedback About Product Documentation**

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

# Contents

Chapter 1: Endpoints, Connectors, and the Connector Server 13

Audience ..... 13
File Locations ..... 13
Endpoints ..... 14
    Managed Objects on an Endpoint ..... 14
Connectors ..... 15
    What Connectors Can Do ..... 15
    Three Types of Connectors ..... 16
    Ways to Create a New Connector ..... 16
    Where to Find Documentation for Connectors ..... 17
Connector Servers ..... 18
    Example Installation: Three Types of Connectors ..... 19
    CCS on Windows and UNIX ..... 20

Chapter 2: Managing CA IAM CS 21

Log In to CA IAM CS ..... 21
Start and Stop CA IAM CS ..... 22
Logging ..... 22
    View a Log ..... 23
    Create Logs for CA Support ..... 24
    Increase the Number of Log Messages Seen ..... 25
    Configure Logging for CA IAM CS ..... 26
    Configure Logging for a Connector ..... 27
    Interpreting Log Messages ..... 28
Change the Administrator Password for CA IAM CS ..... 29
Connect to CA IAM CS from JXplorer ..... 30
Find the Version of CA IAM CS ..... 30

Chapter 3: Configuring CA IAM CS 31

Configuration Files for CA IAM CS ..... 31
    server_osgi_jcs.xml ..... 32
    server_osgi_ad.xml ..... 33
    server_osgi_common.xml ..... 35
    server_osgi_shared.xml ..... 36
    server_osgi_ccs.xml ..... 36
Customize the Configuration for CA IAM CS ..... 37

Retry Configuration ....38
Disable FIPS for CA IAM CS ....39
Configure CA IAM CS to Work Under Heavy Loads (UNIX Only) ....40
Set the TLS Store Certificate Password ....41
Java Virtual Machine Memory Errors ....42
Edit JVM Memory Options ....43
Adjust the Start Parameters for the CA IAM CS Service (Windows Only) ....44

## Chapter 4: Provisioning with CA IAM CS 45

Set Up CA IdentityMinder Provisioning with Active Directory ....46
Install CA IAM CS ....47
Create a Directory Monitor ....48
Create a Directory Synch Template ....49

## Chapter 5: Managing Connectors 51

Add a Connector ....51
Restart a Connector ....52
Add a Third-Party Library to a Connector ....53
Add a Certificate for a Connector ....54
Customize the Configuration for a Connector ....55
Change Pool Settings ....55

## Chapter 6: Connecting to Endpoints 57

CA Access Control Connector ....58
Recommended Patch Levels ....58
ACC Connector Multi-Threading Support ....59
Runtime Environment Settings ....59
Connector-Specific Features ....65
Password Synchronization ....77
CA ACF2 Connector ....82
How to Configure Your CA ACF2 System ....82
Securing Provisioning Server Communication to the CA LDAP Server ....84
ACF2 Support for FIPS and IPv6 ....84
Acquire an ACF2 System Using the User Console ....84
Acquire a CA ACF2 System Using the Provisioning Manager ....86
ACF2 Provisioning Roles and Account Templates ....88
ACF2 Accounts ....88
Validation Errors Thrown on Create or Modify Account/Account Templates Operations when Unsupported Attributes are Defined on Endpoints r12 or Greater ....89
Access and Resource Rules and Rule Keys ....90

Change Control ....90
Rule Lines ....91
Secondary Authids ....91
TSO Alias Support....94
ACF2 Program Exits ....95
Proxy Configuration ....95
Proxy Administration Support....96
Conventions ....97
LDAP Directory Services (LDS)....97
Attributes That Are Marked "Interesting To Compliance"....102
Extend the Schema to Include Custom Attributes ....103
Cannot Create Account When Password Policies Conflict ....106
CA Arcot Connector....107
Embedded Entitlements Manager Connector....108
EEM Installation ....108
EEM Support for FIPS and IPv6....108
Connector-Specific Features ....109
Acquire an EEM Server Machine....109
EEM Account Templates ....110
EEM Accounts ....110
EEM Access Policies....110
EEM Calendars ....111
EEM Groups....111
EEM Resource Classes....111
CA DLP Connector ....111
CA DLP Connector Management....111
FIPS 140 Configuration....112
Connector Specific Features....114
CA SSO Connector for Advanced Policy Server ....125
Configuring the CA Single Sign-On Server....125
Using Failover....128
Enable Application Password Propagation ....129
PLS Support for FIPS and IPv6 ....130
Connector-Specific Features ....130
Frequently Asked Questions ....132
CA Top Secret Connector ....136
Install and Configure the TSS Connector....136
Top Secret Support for FIPS and IPv6....138
Connector-Specific Features ....138
Best Practices....156
DB2 UDB for z/OS Connector ....164
DBZ Endpoint ....165

DBZ Account Templates .....168
Synchronize an Account from an Account Template .....168
DBZ Accounts .....169
Create DBZ Accounts .....170
DBZ User Property Sheet .....170
Google Apps Connector .....171
Configure Google Apps Provisioning API Access .....171
Configure Password Length .....171
Configure NTLM Authentication .....172
Google Apps—CAPTCHA Challenge .....173
IBM DB2 UDB Connector .....173
DB2 UDB Installation .....174
DB2 Limitation .....174
Connector-Specific Features .....175
Kerberos Connector .....180
Kerberos Connector Limitations .....180
Kerberos Installation and Deployment .....182
Connector-Specific Features .....195
LDA Connector Migration to DYN JNDI .....226
Custom Extensions to the LDA Schema .....226
Vendor Support .....226
How the LDAMigrate Script Migrates the LDA Connector .....227
How to Perform the LDA Connector Migration .....230
Post Migration Step .....235
Connector Xpress Templates .....235
Lotus Domino Connector .....237
Privileges Required to Connect to Lotus Domino .....237
LND Support for FIPS and IPv6 .....238
Set Up the Connector for Lotus Domino .....238
LND Java Implementation Considerations .....244
Connector-Specific Features .....246
Microsoft Active Directory Services Connector .....271
Configure Your Windows Servers Using SSL .....272
ADS Defaults .....276
ADS Support for FIPS and IPv6 .....286
Connector-Specific Features .....287
Microsoft Exchange Connector .....307
How to Manage Mailboxes .....308
Configuring the Exchange Remote Agent .....311
Mixed Exchange 2007 or Exchange 2010 Environments with Exchange 2003 not Supported .....316
Enable Exchange 2007/2010 Mixed Environment Support .....317
Configure Exchange 2007 and Exchange 2010 Timeout Settings .....318

- Configure Exchange 2007/2010 Preferred Domain Controller Settings ........ 318
- Activating CAM and CAFT Encryption ........ 319
- Managing the CAM and CAFT Service for Microsoft Exchange 20xx ........ 321
- E2K Support for FIPS and IPv6 ........ 322
- Managing Exchange Users ........ 322

Microsoft SQL Server Connector ........ 330
- MS SQL Configuration ........ 331
- MS SQL Migration Steps ........ 332
- Acquire an MS SQL Server Using the User Console ........ 332
- MSSQL Endpoint with Trusted Connection Fails ........ 334
- SQL Password Changes ........ 334
- Unlock an Account ........ 334
- Database Users ........ 334
- Database Roles ........ 334
- MS SQL Conventions ........ 335

Microsoft Windows Connector ........ 335
- Configuring ........ 336
- Upgrading the Provisioning Server ........ 336
- Installing the Provisioning Agent for Windows Local Users and Groups with setup.exe ........ 336
- Configure the CAM and CAFT Service for Windows NT ........ 337
- Windows NT Support for FIPS and IPv6 ........ 342
- Connector-Specific Features ........ 342

Oracle Applications Connector ........ 350
- How the Connector Accesses Oracle Applications ........ 350
- Oracle Applications Installation and Configurations ........ 350
- Oracle Applications Support for FIPS and IPv6 ........ 353
- Connector-Specific Features ........ 353

Oracle Connector ........ 357
- Oracle Configuration ........ 358
- Oracle Migration Steps ........ 359
- Oracle Support for FIPS and IPv6 ........ 359
- Connector-Specific Features ........ 359

OS/400 Connector ........ 364
- OS/400 Installation ........ 364
- OS/400 Support for FIPS and IPv6 ........ 373
- Connector-Specific Features ........ 373

PeopleSoft Connector ........ 380
- Requirements for Connecting to Oracle PeopleSoft ........ 380
- Security for the PeopleSoft Connector ........ 381
- Set Up the PeopleSoft Connector ........ 382
- Import and Build the CA-USER Component Interface ........ 383
- Update PeopleSoft Permissions ........ 383

Connector-Specific Features ....................................................................................................385

RACF Connector ....................................................................................................396

How to Configure Your RACF System ....................................................................................................396

Securing Provisioning Server Communication to the CA LDAP Server ....................................................................................................398

RACF Support for FIPS and IPv6 ....................................................................................................398

Connector-Specific Features ....................................................................................................398

RSA ACE (SecurID) Connector....................................................................................................411

RSA Installation ....................................................................................................411

Connector-Specific Features ....................................................................................................414

RSA Authentication Manager SecurID 7 Connector ....................................................................................................423

Set Up the RSA SecurID 7 Connector ....................................................................................................424

Acquire an RSA SecurID 7 Endpoint ....................................................................................................425

Upgrade the RSA SecurID 7 Connector ....................................................................................................426

Upgrade RSA SecurID 7 Connector After CA IdentityMinder Upgrade ....................................................................................................427

Connector Specific Features....................................................................................................427

Salesforce.com Connector ....................................................................................................514

Enable Communication between the Salesforce.com Connector and Salesforce.com ....................................................................................................515

Acquire a Salesforce Endpoint ....................................................................................................515

Connector Features....................................................................................................516

Account Deletion....................................................................................................530

SAP Connector....................................................................................................530

Support for SAP ....................................................................................................531

SAP Support for FIPS and IPv6....................................................................................................531

Set Up the SAP R3 Connector....................................................................................................532

Allow Connector to Read SUSPENDED and LOCKED States ....................................................................................................534

Migrating SAP Endpoints from the C++ SAP Connector ....................................................................................................534

Connector-Specific Features ....................................................................................................535

SAP UME Connector ....................................................................................................547

How the SAP UME Connector Works ....................................................................................................548

Installation ....................................................................................................548

Troubleshooting ....................................................................................................550

Customize Password Restrictions ....................................................................................................553

Siebel Connector ....................................................................................................554

What the Siebel Connector Lets You Do ....................................................................................................555

Siebel Installation....................................................................................................556

Connector-Specific Features ....................................................................................................556

UNIX ETC and NIS Connector....................................................................................................568

Installation Procedures ....................................................................................................568

Install Unix Remote Agent on Red Hat Itanium 64-bit ....................................................................................................578

Manage the CAM Service....................................................................................................578

How to Restrict CAFT Commands ....................................................................................................582

Install the CAM and CAFT Encryption Key....................................................................................................583

UNIX Support for FIPS and IPv6 ....584
Connector-Specific Features ....585
Exit Commands ....591
Managing Passwords....593

## Appendix A: Support for FIPS and IPv6 595

## Appendix B: Endpoint Schema and Structure 597

Endpoint Schema ....597
SchemaAbridged.txt File ....598
SchemaUnabridged.txt File ....598
File Formats....599
Endpoint Structure ....602
Distinguished Names....602
Connector Objects and DNs ....603
Common Objects Tree ....627
Object User-Friendly Names ....634

## Appendix C: Bulk Load Client 647

Introduction ....647
Install the Bulk Load Client....647
Command Line Options....648
Before Using the Bulk Load Client....649
Bulk Load Client Localization....650
Allow Bulk Loader to Load Tasks with Localized Names ....651
Authenticating to the CA IdentityMinder Server ....651
SSL Support ....652
Configuring the Bulk Load Client....652
Properties File Example....653
Use Case for PeopleSoft ....654
Full Dump ....655
Delta Dump ....656
Scheduling a Load ....656
Using the XSLT Template....656
Bulk Load Client Error and Response Handling ....657
Bulk Load Client Log Files....658
Axis Library Logging....658

## Appendix D: Sample Connector 659

Introduction ....659

Terminology ......659
Modes ......659
Non-managed Mode (Asynchronous mode) ......660
Managed Mode (Synchronous mode) ......661
Implementing the Connector ......662
Account Management Screens ......663
Further Enhancements ......663
Configuring a Program Exit for Each UPO Exit ......664
Invoking Program Exits on Managed Mode UPO Exits ......664
Enabling / Disabling UPO Exits ......664
SLA Exits ......664

# Chapter 1: Endpoints, Connectors, and the Connector Server

This section contains the following topics:

Audience (see page 13)
File Locations (see page 13)
Endpoints (see page 14)
Connectors (see page 15)
Connector Servers (see page 18)

## Audience

This guide targets CA IdentityMinder administrators, who are responsible for the following tasks:

- Installing and configuring CA IAM Connector Server (CA IAM CS)
- Connecting endpoint systems to CA IdentityMinder

## File Locations

The default Windows and UNIX directories are listed in the following table. Your actual installation directories depend on your operating system and selections during the installation process.

| **Path Notation** | **Default Directory** | |
|---|---|---|
| | **Windows** | **UNIX** |
| *im-home* | C:\Program Files\CA\Identity Manager | /opt/CA/IdentityManager |
| *imps-home* | C:\Program Files\CA\Identity Manager\Provisioning Server | /opt/CA/IdentityManager/ProvisioningServer |
| *cs-home* | C:\Program Files\CA\Identity Manager\Connector Server | /opt/CA/IdentityManager/ConnectorServer |
| *cs-sdk-home* | C:\Program Files\CA\Identity Manager\Connector Server SDK | /opt/CA/IdentityManager/ConnectorServerSDK |
| *conxp-home* | C:\Program Files\CA\Identity Manager\Connector Xpress | /opt/CA/IdentityManager/ConnectorXpress |

# Endpoints

An *endpoint* is a specific installation of a platform or application, such as Active Directory or Microsoft Exchange, which communicates with CA IdentityMinder to synchronize information. A connector server uses a connector to manage an endpoint.

An endpoint is any system that communicates with CA IdentityMinder to synchronize information, including identities. An endpoint can be any system that uses identities, including the following systems:

- An operating system (such as Windows)
- A security product that protects an operating system (such as CA Top Secret and CA ACF2)
- An authentication server that creates, supplies, and manages user credentials (such as CA Arcot)
- A business application (such as SAP, Oracle Applications, and PeopleSoft)
- A cloud application (such as Salesforce and Google Apps)

For the full list of endpoints that you can connect to CA IdentityMinder, see the Platform Support Matrix. Look for the table named SUPPORTED CONNECTOR ENDPOINT TYPES at the end of the document.

## Managed Objects on an Endpoint

A *managed object* is data on an endpoint that CA IdentityMinder manages.

For each endpoint type, CA IdentityMinder manages user accounts. Other managed objects that CA IdentityMinder is able to manage include groups, roles, certificates and permission lists, depending on the endpoint type.

For dynamic endpoint types, you are able to define which managed objects CA IdentityMinder will manage on the endpoint.

# Connectors

A *connector* is the software that enables communication between CA IdentityMinder and an endpoint system. You can generate a dynamic connector using Connector Xpress, and you can develop a custom static connector in Java.

For each endpoint that you want to manage, you must have a connector. Connectors are responsible for representing each of the managed objects in your endpoint in a consistent manner. Connectors translate add, modify, delete, rename, and search LDAP operations on those objects into corresponding actions against the endpoint system.

A connector acts as a gateway to a native endpoint type system technology. For example, to manage computers running Active Directory Services (ADS) install the ADS connector on a connector server.

Users use Connector Xpress to generate and maintain the XML metadata for JDBC and JNDI dynamic connectors. Developers can also maintain data for other connectors manually, or adjust metadata for released connectors (for instance adding site-specific mappings for custom attributes).

## What Connectors Can Do

Each connector lets CA IdentityMinder perform the following operations on managed objects on the endpoint:

- **Add**
- **Modify**—Changes the value of attributes, including modifying associations between them (for example, changing which accounts belong to a group).
- **Delete**
- **Rename**
- **Search**—Queries the values of the attributes that are stored for an endpoint system or the managed objects that it contains.

For most endpoint types, all of these operations can be performed on accounts. These operations can also be performed on other managed objects if the endpoint permits it.

For information about the limitations for an endpoint, read the section for a particular endpoint in Connecting to Endpoints (see page 57).

## Three Types of Connectors

CA IdentityMinder has three types of connectors:

**Java Connectors**

CA Technologies creates new connectors in Java, and CA IAM Connector Server (CA IAM CS) serves these connectors.

If you create a connector, use Java.

**C++ Connectors**

Previously, CA Technologies created connectors in C++. These connectors still work well, and C++ Connector Server (CCS) serves these connectors. Usually, CCS is installed with and managed by CA IAM CS.

**Note**: You cannot use both CA IAM CS and CCS to manage the same endpoint type.

**Plugin Connectors**

Before CA Technologies developed the CCS, the first connectors were plugins to the Provisioning Server itself. These connectors still work well. They require no connector server. They do require CA LDAP Server on the endpoint. The following plugin connectors are installed with Provisioning Server:

- CA ACF2
- CA Top Secret
- IBM RACF

## Ways to Create a New Connector

You can connect to an endpoint that is not in the list of supported endpoints in the Platform Support Matrix. To do this, create your own connector in one of these ways:

- Use Connector Xpress to create your own connector. For information, see the Connector Xpress Guide.
- Use the CA IAM CS SDK to create your own connector. For information, see the Connector Programming Guide.
- Engage CA Services to create a connector for your organization.
- Ask CA to create a connector. The new connector might be available in a future release of CA IAM CS.

## Where to Find Documentation for Connectors

CA Technologies documents how to set up and use each connector, and also how to fill in the relevant fields in endpoint-specific screens.

**Connectors Guide and online help**

Until recently, each endpoint type was documented with a section in the Connectors Guide and a section in the online help. The Connectors Guide is available in the product bookshelf, and the online help comes with the User Console.

**Endpoint Guide and attribute list**

CA Technologies now documents each new connector with an Endpoint Guide and an attribute list. An *attribute list* is an HTML page that describes every setting that is required for configuring a connector.

The Endpoint Guides and attribute lists are available on the Download page for Endpoint Guides for CA IdentityMinder. To access this page, log in with your CA Support credentials.

The documentation for any new connectors appears on this download page when the connector is released. A connector can be released at any time between releases of CA IdentityMinder.

You can read the documentation, and then download the new connector from CA Support and use it with your current version of CA IdentityMinder. The new connector causes new pages to appear in the User Console. However, the Help links for these new pages will not work until the connector is included in the next release of CA IdentityMinder.

# Connector Servers

CA IdentityMinder comes with the following connector servers:

- **CA IAM CS**—In previous releases, this component was called Java Connector Server, or Java CS. From CA IdentityMinder 12.6, this server is called CA IAM Connector Server, or CA IAM CS.

  CA IAM CS manages the following things:

  - All of the Java connectors
  - Any dynamic connectors that were created with Connector Xpress
  - C++ Connector Server (CCS) and its connectors, if CCS is present

- **CCS**—CCS manages all of the C++ connectors.

  When you install CA IAM CS, you have the option to install CCS in a managed mode. If you do this, CA IAM CS manages CCS and the C++ connectors that it manages.

  If you prefer to install CCS on its own, it manages the C++ connectors as in previous releases of CA IdentityMinder.

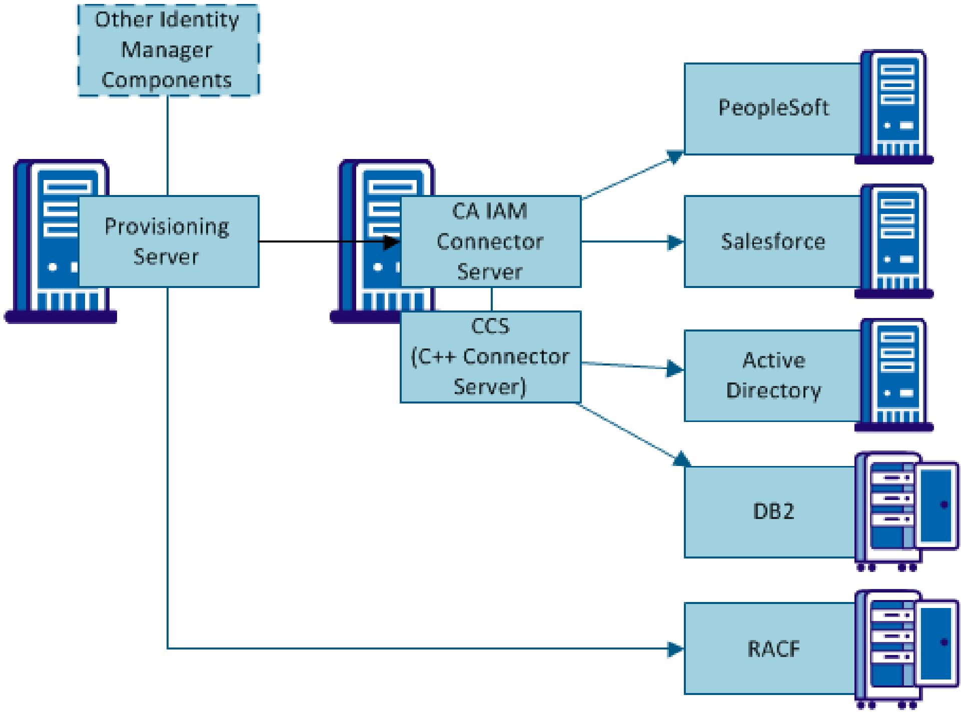
## Example Installation: Three Types of Connectors

CA IdentityMinder supports three types of connector (see page 16). Before you install a connector server, decide which types of connector you intend to use.

The following diagram shows all three types of connector.

In this example, CA IAM CS serves the connectors for PeopleSoft and Salesforce. CCS serves the connectors for Active Directory and DB2, and the RACF connector is actually a plugin on the Provisioning Server.

*Figure 1: The PeopleSoft and Salesforce connectors are Java connectors, the Active Directory and DB2 connectors are C++ connectors, and the RACF connector is a server plugin*



**Note:** To see a list of connectors and their requirements, download the Platform Support Matrix, then find the SUPPORTED CONNECTOR ENDPOINT TYPES table near the end of the document. This table lists the server that is required for each connector.

## CCS on Windows and UNIX

The C++ Connector Server (CCS) works slightly differently on Windows and on UNIX.

If you install CCS on Solaris, it can manage only some endpoints. To see a list of these endpoints, download the Platform Support Matrix, then find the SUPPORTED CONNECTOR SERVERS table. This table includes the list of endpoints supported by CCS on Solaris.

Install the C++ Connector Server on a Windows system and register it with the Provisioning Server installed on Solaris. During installation, specify that this connector server is your default CCS.

You can access the other C++ connectors from the Solaris Provisioning Server by using a Connector Server Framework (CSF). The CSF allows a Provisioning Server on Solaris to communicate with connectors running on Windows.

# Chapter 2: Managing CA IAM CS

This section contains the following topics:

Log In to CA IAM CS (see page 21)
Start and Stop CA IAM CS (see page 22)
Logging (see page 22)
Change the Administrator Password for CA IAM CS (see page 29)
Connect to CA IAM CS from JXplorer (see page 30)
Find the Version of CA IAM CS (see page 30)

## Log In to CA IAM CS

You can use a web browser to log on to CA IAM CS from any computer, using details that you specified during installation.

Use the following URL:

`http://`*`hostname`*`:`*`port`*

**hostname**

Specifies the name of the computer running CA IAM CS, as a fully qualified domain name

**port**

Specifies the HTTP or HTTPS port that was set during installation.

### Example URLs for CA IAM CS

```
http://myserver.mycompany.org:20080
```

```
https://myserver.mycompany.org:20443
```

# Start and Stop CA IAM CS

You can start and stop CA IAM CS using the following methods.

- **UNIX daemon**—The installation process creates a startup script named *im_jcs* and links it to the rc.d system on the local system. The script automatically runs CA IAM CS in run levels 2-5, or shuts it down on 0,1, and 6 corresponding to *system halt*, *single user mode*, and *reboot*.

  Use the following commands to start, restart, and stop the daemon:

  ```
  /etc/init.d/im_jcs start
  ```

  ```
  /etc/init.d/im_jcs restart
  ```

  ```
  /etc/init.d/im_jcs stop
  ```

  Use the following command to display the status of the daemon:

  ```
  /etc/init.d/im_jcs status
  ```

- **Windows service**—Start and stop the CA Identity Manager - Connector Server (Java) service.

- **Windows command line**—Use the following commands to start and stop the service:

  ```
  net start im_jcs
  ```

  ```
  net stop im_jcs
  ```

# Logging

You can see log files for the following components:

- Logging for CA IAM CS
- Logging for each endpoint type

  The endpoint log files contain most of the logging data for the relevant connector.

  However, also look for relevant logging in the jcs_daily.log* systemwide log file. Messages can be logged to the systemwide file for the following reasons:

  - A connector uses third-party libraries.
  - A connector was developed (using Connector Xpress or the SDK) without sufficient attention to logging.
  - Problems occur while creating or activating a connector.

We recommend that you start with jcs_daily* files and work downwards to the connector-specific log files as required.

## View a Log

You can view a log by reading a text file, or through a web browser.

To see the 500 most recent log messages, log in to CA IAM CS (see page 21), and click the Log Entries tab.

To see an entire log, open one of the following files from *cs-home*\jcs\logs:

| Log File Name | Description |
|---|---|
| jcs_daily.log | Today's logging from CA IAM CS |
| jcs_daily.log.*YYYYMMDD* | jcs_daily.log for a particular date |
| servicemix.log | All the content from the jcs_daily.log, plus some additional messages from ServiceMix |
| servicemix.log.*YYYYMMDD* | servicemix.log for a particular date |
| *endpoint-type*/jcs_conn_*connector-name*.log | Logging for a connector |
| *endpoint-type*/jcs_conn_*connector-name*.log.*YYYYMMDD* | Logging for a connector for a particular date |

## Create Logs for CA Support

If you find a problem with a connector or CA IAM CS, contact CA Support. To help the support team analyze the problem, send your log files to them.

By default, your log files do not contain verbose information, because this extra logging slows down CA IdentityMinder. Before you send your logs to the support team, We recommend that you configure the logging to capture detailed information.

**Follow these steps:**

1. Identify how to trigger the problem with your deployment.
2. Log in to CA IAM CS (see page 21).
3. Click the Log File tab. The contents of the logging configuration file appears.
4. To increase the logging, click **Load Verbose**.

   Verbose logging makes CA IAM CS slower. Use this configuration only during debugging.
5. Click Save to upload your changed file to the server.

   The new logging configuration takes effect immediately. You do not need to restart any components.
6. Trigger the problem that you have identified.
7. Zip the entire *cs-home/logs* directory, and include the zipped file with your support request.
8. Log in to CA IAM CS (see page 21).
9. To reduce the logging, click **Load Production**.

   Production-level logging is minimal, and has a low impact on performance.
10. Click Save to upload your changed file to the server.

    CA IAM CS immediately returns to minimal logging.

## Increase the Number of Log Messages Seen

When you log in to CA IAM CS to view log messages, you can see only the 500 most recent messages. These messages are kept in memory, which is why so few can be seen.

You can configure the page to display more or fewer messages.

**Follow these steps:**

1. Open the following file in a text editor:

   `cs_home/etc/org.apache.karaf.log.cfg`

2. Find and edit the following setting:

   ```
   size = 500
   ```

   **Note:** If you set the size too high, CA IAM CS becomes slower.

3. Save the file.

4. Restart CA IAM CS.

## Configure Logging for CA IAM CS

The following configuration file affects the jcs_daily.log and servicemix.log files that are listed in View a Log (see page 23):

*cs-home*/etc/org.ops4j.pax.logging.cfg

This file defines logging for CA IAM CS, including the following:

- The logging levels for each of the components in CA IAM CS.
- Whether log files are appended daily
- The formatting of the lines that are written to the log

You can use these methods to configure logging for CA IAM CS:

### Method 1 (Recommended): Load preformatted versions of the CFG file

Use the following buttons on the Log File tab in CA IAM CS:

**Load Production**

Enable minimal logging for production environments. This configuration has a low impact on performance.

**Load Verbose**

Enables verbose logging, which is useful for analyzing faults.

Verbose logging can make CA IAM CS run slowly. Use this configuration only during debugging.

### Method 2: Edit the CFG file in the Log File tab in CA IAM CS

When you have finished editing, use these buttons to discard or save your changes:

**Reload**

Discard any changes that you have made, and get the latest version of the logging configuration file from the server. Reloading is useful if you have edited the file in the Log File tab.

**Save**

Upload your changed file to the server. The new logging configuration takes effect immediately. You do not need to restart any components.

### Method 3: Edit the CFG file in a text editor

After you save the file, the new logging configuration takes effect immediately. You do not need to restart any components.

## Configure Logging for a Connector

Each endpoint type has a configuration file that defines its logging. You can configure the logging for a particular connector by sending LDAP commands to CA IAM CS.

**Follow these steps:**

1. With an LDAP client, bind to CA IAM CS using the following details:
   - Port: 20410 (LDAP) or 20411 (LDAPS)
   - User: cn=root,dc=etasa
   - Password: Use the password that was specified during installation
2. Find the entry with the following DN:

   ```
   eTDYNDirectoryName=${CONN},eTNamespaceName=${CONN_TYPE},dc=${DO
   MAIN},dc=etasa
   ```

   You can enable and configure logging by changing the attributes of this entry.
3. To enable logging for a connector, modify the following attribute:
   - eTLog=1 (active)
4. To configure the logging level for a connector, include the following attributes:
   - eTLogDestination='F' (file)
   - eTLogFileSeverity=*severity-code*

     Use the following severity codes

| Logging Level | Severity in Provisioning Server | Severity Code in Provisioning Server |
|---|---|---|
| DEBUG | Information | I |
| INFO | Non-Admin Success | S |
| WARN | Warning | W |
| ERROR | Error | E |
| FATAL | Fatal | F |

## Interpreting Log Messages

All log messages include the following information:

**Date and time**

Records the timestamp on the local host when the message was logged. The date and time use ISO8601 format.

**Elapsed time**

The number of milliseconds elapsed since the server started.

**Thread name**

Identifies the thread that logged the message, for example *[Timer-1]*.

**Bundle name, class name, and line number**

Records the bundle that contains the executed code, the class from which the message came, and the line number (if this number is available). This section uses the following format:

```
(bundle-name:class-name:line)
```

For example:

```
(com.ca.jcs.core:com.ca.jcs.osgi.listener.ImplBundleServiceList
ener:123)
```

**Severity level**

Identifies the severity of the message.

**Message**

Gives the actual log message.

# Change the Administrator Password for CA IAM CS

To ensure better security across a deployment you can change the password of the administrative user of CA IAM CS.

CA IAM CS remembers all passwords for all users since it was last restarted. All of these passwords are accepted as valid for bind requests.  Each user can reset only their own cache.

The cache of old passwords is useful for a system where many provisioning servers connect to one connector server. In this situation, the provisioning servers may not update their stored passwords for CA IAM CS at the same time, but they can still access the connector server.

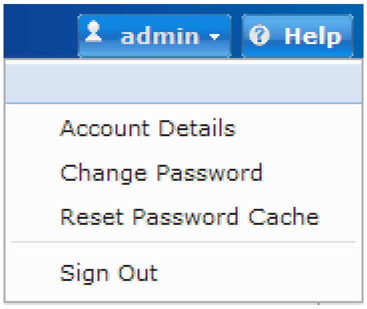
However, these old passwords make your system potentially insecure. To make the connector server forget the old passwords, clear the password cache. To clear a password cache, you must be logged in as that user.

**Follow these steps:**

1. Log in to CA IAM CS as the administrator and change the password.
2. Update the password stored in all provisioning servers and any other clients that connect to CA IAM CS.
3. Log in to CA IAM CS as the administrator.
4. Choose the Reset Password Cache option in your username menu in the top right.

   The following example shows the menu for a user named *admin*:

*Figure 2: The menu under your user name contains the options "Account Details, "Change Password" and "Reset Password Cache"*



# Connect to CA IAM CS from JXplorer

You can use the following parameters to connect to CA IAM CS from an LDAP browser such as JXplorer.

These settings are configured in server_osgi_jcs.xml. Changing the User DN is problematic because of assumptions within ApacheDS. To avoid problems, server_osgi_jcs.xml includes the property *java.naming.security.principal.alias*. This property simulates use of a different user DN, as an alias to "uid=admin,ou=system".

**Host**

Specifies the host server name of CA IAM CS

**Protocol**

LDAP v3

**Port**

Default port number: 20411, when using level: SSL + User + Password (TLS)

20410, when using the less safe level: User + Password

**User DN**

uid=admin,ou=system

**Password**

As configured during installation.

**Note:** For more information on JXplorer, see http://www.jxplorer.org.

# Find the Version of CA IAM CS

To determine the version of your CA IAM CS installation, look in the following file:

`cs_home/version.properties`

# Chapter 3: Configuring CA IAM CS

This section contains the following topics:

Configuration Files for CA IAM CS (see page 31)
Customize the Configuration for CA IAM CS (see page 37)
Java Virtual Machine Memory Errors (see page 42)
Edit JVM Memory Options (see page 43)
Adjust the Start Parameters for the CA IAM CS Service (Windows Only) (see page 44)

## Configuration Files for CA IAM CS

The configuration files for CA IAM CS are in the following location:

```
cs_home/jcs/conf
```

- **server_osgi_jcs.xml**—Configures CA IAM CS and some connector behavior
- **server_osgi_ad.xml**—Configures the LDAP binding
- **server_osgi_ccs.xml**—Configures communication to the CCS (if CA IAM CS manages the CCS)
- **server_osgi_ui.xml**—Configures the user interface for CA IAM CS
- **server_osgi_common.xml**—Configures common items such as security and data persistence
- **server_osgi_shared.xml**—Contains settings for use by different components

**Note:** Any changes that you make to these files are lost when you upgrade CA IAM CS. We recommend that you use the properties files in *cs_home*\conf\override, as described in Customize the Configuration for CA IAM CS (see page 37).

## server_osgi_jcs.xml

The server_osgi_jcs.xml file contains the following configuration settings:

**connectorClientCertStore**

Specifies the client certificate store for CA IAM CS. The value is a path to the file which contains trusted certificates that are used to verify the identity of the endpoint server during SSL handshakes. Used for outbound TLS connections that the connectors make themselves, to the endpoint systems they manage. Import any issuer certificates for the endpoints to which TLS connections into this store.

**connectorClientCertStoreType**

Specifies the certificate store type (JKS or PKCS12).

**connectorClientCertStorePassword**

Specifies the password protecting the connector client store. The same rules apply as for the ldapsCertificatePassword.

**connectorSSLVerifyPeer**

**False (default)**

During SSL handshakes the peer certificate that the endpoint sends is not verified for trust. That is, the connectorClientCertStore value is ignored and not required for outbound SSL connections in this configuration.

**True**

The endpoint host certificate that is presented to CA IAM CS undergoes trust checks against connectorClientCertStore contents.

**connectorSSLTrace**

When TRUE, sends SSL information to a log file.

**httpProxyConfiguration**

Enables or disables the HTTP proxy, and configures the proxy details. Use a proxy if CA IAM CS must communicate with other computers outside the network.

The HTTP proxy can be configured when CA IAM CS is installed. You can change it later by updating this value in the configuration file.

## server_osgi_ad.xml

**java.naming.security.authentication**

Specifies the authentication methods. Only *simple* is currently supported.

**java.naming.security.principal**

Specifies the authentication principal. By default, ApacheDS sets this value to *uid=admin,ou=system* by ApacheDS, but an optional java.naming.security.principal.alias= can be specified to ease integration. When this alias is received for authentication, it is treated exactly as uid=admin,ou=system.

**maxThreads**

Specifies the maximum number of requests that can be processed concurrently for all activated connectors that a single connector server hosts. The default value of 200 matches the Provisioning Server configuration.

If you increase this value, consider also increasing other configuration settings. For example, you can change the heap-space for the Java Virtual Machine or "ulimit –n" setting for open files on Solaris.

**Note:** For more information, see Configure CA IAM CS to Work Under Heavy Loads (UNIX Only) (see page 40).

**ldapPort**

Specifies the port on which CA IAM CS listens for insecure connections. Set the port to one of the recommended ports unless many connector servers run on the same computer. Where a secure port is configured, use the secure port instead.

The insecure port can be useful for debugging purposes. By default, CA IAM CS uses only ldapsPort.

Set the port to one of the following port numbers:

- Production: 20410
- Development: 20412

**ldapsPort**

Specifies the port on which CA IAM CS listens on for secure connections. The ldapsPort, with associated properties enableLdaps, ldapsCertificateFileldapsCertificateFile, and ldapsCertificatePassword, must be a different port from the one chosen for ldapPort. Traffic on this port is secured using the configured certificate and the Transport Layer Security (TLS) protocol.

ldapsPort can also be useful for debugging. Set the logging level in the log4j.properties file to trace LDAP requests as they are delivered to the connector server.

Set the port to one of the following port numbers:

- Production: 20411
- Development: 20413

The ldapsCertificateFile is configured to reference a Java keystore containing the standard IM Provisioning Server certificate. The default ldapsCertificatePassword was set during installation.

**bootstrapSchemas**

Specifies which LDAP schemas the connector server knows. This property incorporates schemas which have been converted to Java objects by the ApacheDS build process.

You can load additional OpenLDAP formatted schema files (see http://www.openldap.org/doc/admin23/schema.html) by placing them in the conf directory (like eta_dyn_openldap.schema) or ideally contributed from the conf/ directory within a specific connector's JCS-connector-*.jar file (refer to SDK connector's conf/etaeta_sdk_openldap.schema _nds_openldap.schema registered through its conf/connector.xml descriptor in the jcs-connector-sdk.jar sample connector).

**ldapsCertificateFile**

Specifies the path to an LDAPS certificate store for CA IAM CS. This store contains all the certificates that CA IAM CS uses to verify its identity during inbound LDAPS (TLS) connections. At least one certificate with an accompanying private key issued to represent CA IAM CS is placed in this store.

To change this value, add it to server_osgi_shared.xml. Values in this file overwrite any in server_osgi_ad.xml.

**ldapsCertificatePassword**

Specifies the password protecting the certificate store specified in ldapsCertificateFile.

The password can either be cleartext or obfuscated. For example:

```
{ALGORITHM}ciphertext
```

where ALGORITHM would be typically set to 'AES' . For example, {AES}LQpBXeIjOMGSsGLU

See The Password Tool.

**interceptorConfigurations**

Specifies any other standard ApacheDS interceptor services. The interceptor services that CA IAM CS does not require have been deactivated.

## server_osgi_common.xml

**cryptoService**

Configure the crypto service for activating encryption convertors on specific fields according to their metadata properties. The most important setting is the isEncrypted boolean metadata setting.

**jcsSslContext**

Contains the path to the Java certificate keystore file in properties “keyStore” and “trustStore”.

**jcs-broker**

Contains the HTTP and HTTPS ports that CA IAM CS uses for sending and receiving messages.

**jmsCredentials**

Contains the user name and password for accessing the broker.

## server_osgi_shared.xml

**fipsEnabled**

Enables or disables FIPS compliance.

**Default:** Enabled.

**camelTimeoutConfiguration**

Contains the timeout periods for messages. When a timeout is reached, CA IAM CS returns an error to the user or to the service that was expecting a response.

**defaultMessageTimeout**

The default message timeout (30 minutes).

**oneLevelSearchMessageTimeout**

The timeout for a one-level LDAP search (1 hour).

**subtreeSearchMessageTimeout**

The timeout for a subtree LDAP search (8 hours).

**managementMessageTimeout**

The timeout for messages coming from the web UI (60 seconds).

**connectionErrorTimeout**

The timeout after a connection error occurs (60 seconds).

**httpInactiveClientTimeout**

The time before an idel HTTP connection is considered inactive (2 minutes).

**httpSocketTimeout**

Default socket timeout for HTTP clients (60 seconds).

**httpRetryCount**

The number of times an HTTP operation can be retried (3).

## server_osgi_ccs.xml

**proxyConnectionConfig**

The connection details to a local or remote CCS.

# Customize the Configuration for CA IAM CS

In previous releases, all configuration for CA IAM CS was stored in server_jcs.xml. From CA IdentityMinder 12.6 onwards, the configuration for CA IAM CS is stored in five configuration files, which are described in Configuration Files for CA IAM CS (see page 31).

When you upgrade CA IAM CS, any changes you made to the XML configuration files are lost. This loss happens whether you are upgrading from Java CS or from CA IAM CS.

However, any changes you made to the following files are preserved:

- *cs_home*\conf\override\server_jcs.properties
- *cs_home*\conf\override\server_ad.properties
- *cs_home*\conf\override\server_shared.properties
- *cs_home*\conf\override\server_ui.properties
- *cs_home*\conf\override\server_common.properties
- *cs_home*\conf\override\server_ccs.properties

The settings in these files override the settings in the XML configuration files.

For this reason, we recommend that you do not change the settings in the XML configuration files. Instead, add any settings that you want to configure to the properties files in the *override* folder.

**Note:** Each XML configuration file has a matching override file. However, the filenames of the override files do not contain *_osgi*. Otherwise they match. For example, *server_ad.properties* is the override file for *server_osgi_ad.xml*.

**Follow these steps:**

1. If the properties file does not exist, copy the matching sample file and change its name.
2. Open the properties file in a text editor.
3. Edit the values for any of the settings already in the file.
4. If you want to customize other settings, add them to the properties file.

   Ensure that you use property names that match the nested structure of the entries in the XML configuration files.
5. Save the edited properties file.
6. Restart CA IAM CS.

## Retry Configuration

You can configure the Exception Map setting to contain groups of exception messages that require special handling (and optionally associated retry delay and retry count settings).

In particular, the JDBC connector defines entries for exceptions signifying these conditions which drive retrying when connections to the endpoint experience problems:

- **Stale**—The connection to the endpoint has become stale and is reestablished immediately.
- **Retriable**—The connection to the endpoint has encountered a transient soft failure, in which case a retry loop is started with the configured count and delay. If the count is exhausted before connectivity is restored, then the current request is considered to have suffered a hard failure which is reported to CA IAM CS.
- **Busy**—The endpoint has reported it is too busy to complete a request in which case a retry loop is started with a separate retry delay and count settings. For example, the MSSQL database reports deadlock exceptions when it is unable to complete processing a transaction within a certain time interval. The delay and recount settings are typically much longer than the Retriable case.

In addition to these triggering exceptions, each ExceptionRetryGroup has associated resilientDelay and resilientMaxRetries settings which specify how many retry attempts are required when a matching exception is encountered, and the delay between each attempt.

## Disable FIPS for CA IAM CS

When you install CA IAM CS, you can enable FIPS. If you upgrade to CA IAM CS from a Java CS that had FIPS enabled, it is still enabled after the upgrade.

In either of these situations, you can disable FIPS without running the installation program again.

The FIPS setting is in the server_osgi_shared.xml. We recommend that you customize this setting in an override file.

**Follow these steps:**

1. Open the following properties file in a text editor:

   ```
   cs_home/conf/override/server_shared.properties
   ```

   If it does not already exist, follow the steps in Customize the Configuration for CA IAM CS (see page 37) to create it.

2. Find the following setting, or add it to the file:

   ```
   JsafeJCE.fipsEnabled=false
   ```

3. Ensure that the setting is not commented out with a # character.
4. Save the edited properties file.
5. Restart CA IAM CS.

## Configure CA IAM CS to Work Under Heavy Loads (UNIX Only)

We recommend that you consider carefully the *ulimit -n* setting for the user for which you install CA IAM CS. The default setting is too low to allow CA IAM CS to function properly under load.

When this problem occurs the Java virtual machine shuts down and the following message appears in the jcs_daily log:

```
exiting because of 120 exceptions in a row: Too many open files
```

CA IAM CS requires a minimum ulimit -n setting of around 80.

**Follow these steps:**

1. Find out the value of maxThreads.

   The default value is stored in the following file:

   *cs_home*`/jcs/conf/server_osgi_ad.xml`

   If a custom value has been specified, it is stored in the following file:

   *cs_home*`/jcs/conf/override/server_ad.properties`

2. Calculate the best ulimit value, using the maxThreads value:

   - ulimit = 50 + 2 x maxThreads

3. Set the ulimit value.

## Set the TLS Store Certificate Password

CA IAM CS uses two certificates: one for each of the following roles:

- **CA IAM CS as a server**—When LDAP and client requests a TLS-secured connection, CA IAM CS acts as an LDAP server. CA IAM CS uses a certificate to secure this communication.
- **CA IAM CS as a client**—When CA IAM CS requests a secure connection with an endpoint, CA IAM CS acts as a client. It uses a different certificate to secure this communication.

When you install CA IAM CS these certificates each have a temporary password. We recommend that you update these passwords.

By default, these certificates are stored in the same keystore. However you can store them in separate keystores if you prefer.

**Follow these steps:**

1. Stop CA IAM CS.
2. Open a command prompt, then change to the following directory:

   ```
   cs_home/jcs/tools/ldaps_password
   ```

3. Use the following command to update the password of the keystore for the **server**:

   ```
   ldaps_password new-password
   ```

   This command updates the encrypted *commonConfiguration.keystorePassword* value in server_shared.properties.

4. Use the following command to update the password of the keystore for the **client**:

   ```
   ldaps_password new-password
   connectorManager.connectorClientCertStorePassword
   ../conf/override/server_jcs.properties
   ```

   This command updates the encrypted *connectorManager.connectorClientCertStorePassword* value in server_jcs.properties.

   **Note:** The password for the keystore is the password that you set during CA IAM CS installation.

5. Restart CA IAM CS.

**Note:** Alternatively, you can manage the keystore using the keytool utility included in the Java Runtime Environment. This lets you install your own certificate instead of the default Provisioning Server certificate that the installer configures.

# Java Virtual Machine Memory Errors

During stress or high load, the Java Virtual Machine can run out of memory. This may affect the functionality of CA IAM CS.

If an out-of-memory error occurs frequently, you can set Java VM debugging options to alert you when it happens.

To do this, use the following debugging setting to specify a command that the Java VM will invoke when the OutOfMemoryError is thrown:

```
-XX:OnOutOfMemoryError= string
```

**Note:** For more information about setting JVM debugging options, see the following pages on www.oracle.com:

- Java HotSpot VM Options
- Using JVM Options to Help Debug

# Edit JVM Memory Options

If the Java process runs out of memory, you can increase the memory available to it.

**On Windows, Follow these steps:**

You need to edit the JVM memory options JvmMs, JvmMx, JvmSs and Classpath. To do this, use the *service update* command or edit the following registry key on Windows:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ComputerAssociates\Identit
y Manager\Procrun 2.0\im_jcs
```

**Note:** You can use Apache procrun arguments to update the service parameters. For more information, see Procrun service application at http://jakarta.apache.org

**On UNIX, Follow these steps:**

Create a file named jvm_options.conf in the data folder with the following Java arguments:

```
-Xms128M -Xmx1024M -d64
```

**-Xms**

Specifies the minimum heap memory allowed for CA IAM CS

**Example:** -Xms128M specifies that the minimum heap memory allowed for CA IAM CS is 128 MB.

**-Xmx**

Specifies the maximum  heap memory allowed for CA IAM CS.

**Example:** -Xmx1024M specifies that the maximum heap memory allowed for CA IAM CS is 1024 MB.

**-d64**

Specifies that the JVM is run in a 64-bit environment.

**Note:** For more information, see the documentation for the Java command tool at www.oracle.com (www.oracle.com).

# Adjust the Start Parameters for the CA IAM CS Service (Windows Only)

To adjust any CA IAM CS service start (including related JVM parameters), go to the following location in the Windows registry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ComputerAssociates\Identit
y Manager\Procrun 2.0\im_jcs
```

# Chapter 4: Provisioning with CA IAM CS

You can use CA IAM CS to provision certain cloud-based endpoints. This is a lightweight alternative to managing user access directly using CA IdentityMinder.

This section contains the following topics:

Set Up CA IdentityMinder Provisioning with Active Directory (see page 46)

# Set Up CA IdentityMinder Provisioning with Active Directory

You can use Active Directory Server (ADS) to synchronize attribute data to supported endpoints. You do this by configuring CA IAM CS to propagate local changes in Active Directory to a cloud-based identity store using a connector.

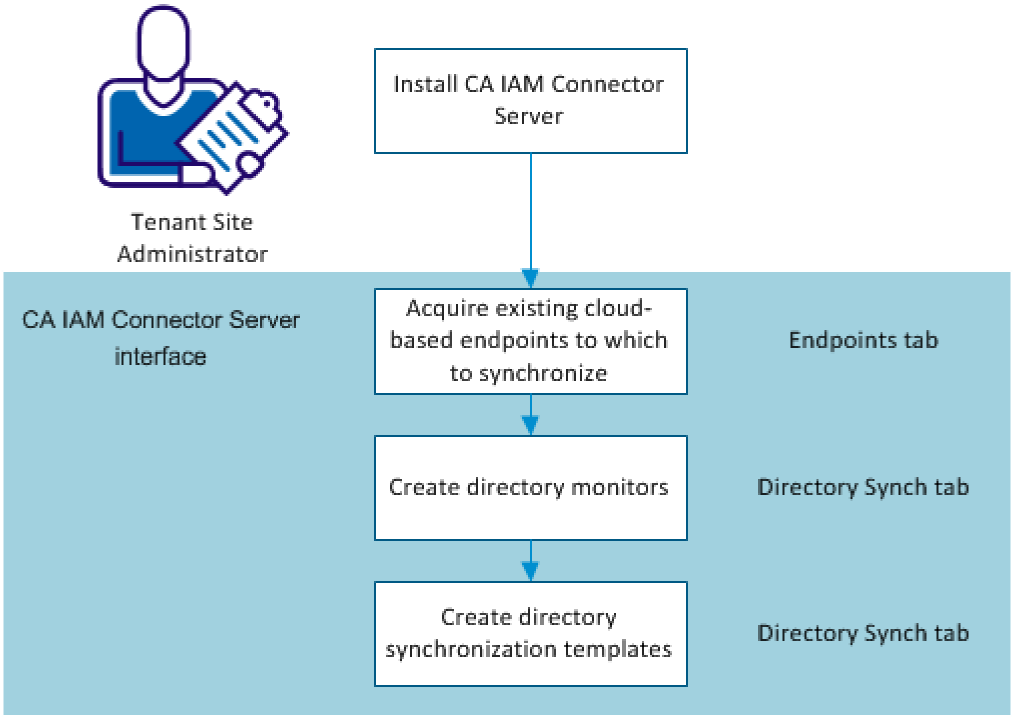
For example, assume that you have a SalesForce installation in the cloud. You could create an ADS group named "SalesForce" and then configure the CA IAM CS to monitor that group. CA IAM CS synchronizes any changes to the SalesForce environment in the cloud.

If you add a user to the ADS Salesforce group, CA IAM CS uses the SalesForce connector to trigger a "Create User" action in the SalesForce environment proper.

To set up directory synchronization, follow this process:

1. Install CA IAM CS in your environment.
2. Acquire the endpoints that you want to synchronize with. Consult the appropriate connector configuration documentation. You must acquire endpoints in order to create templates in step 4.
3. Create one or more directory monitors. Monitors capture changes that you make in your local Active Directory, and report them for the synchronization.
4. Create one or more synchronization templates. Templates control settings for the directory synchronization.

*Figure 3: Flowchart showing the steps to set up directory sychronization*


Tenant Site Administrator
Install CA IAM Connector Server
CA IAM Connector Server interface
Acquire existing cloud-based endpoints to which to synchronize
Endpoints tab
Create directory monitors
Directory Synch tab
Create directory synchronization templates
Directory Synch tab

## Install CA IAM CS

Install CA IAM CS to set up directory synchronization to endpoints such as SalesForce

**Follow these steps:**

1. Download CA IAM CS from support.ca.com, and launch the installer.
2. The C++ connector server is not required for directory synchronization.
3. Clear the "Register this installation with a Provisioning Server" checkbox if it is selected. This setting is not required.
4. You need not enter any information about the Cloud Connector Server screen for the purpose of this configuration.
5. Enter the admin password on the Connector Server Configuration screen, and accept the default LDAP port values.
6. On the Port Configuration screen, accept the default values.
7. Complete the wizard.

## Create a Directory Monitor

Create a directory monitor to find and report changes in your on-premise Active Directory installation. Monitors receive change notifications. Directory synchronization templates then control how the changes are processed.

**Follow these steps:**

1. Select the Directory Sync tab, and click Add in the Monitor area.

   The Add Monitor dialog appears. Both the ADS domain and forest you want to monitor must be Windows 2003 or later.

   > Note: if you are using ldaps, first import the ADS certificate in the Certificates tab. See *Directory Synchronization with Active Directory* for more information.

2. Enter the URL of the Active Directory installation you want to monitor. Type it, or modify the default URL template with the appropriate hostname and port number.
3. Enter User Distinguished Name information to grant access to ADS for synchronization. The user DN you enter must correspond to a valid user object in the Active Directory instance you want to monitor.
4. Enter a password, if necessary for your active directory installation.
5. Click Browse to connect to the ADS and locate a valid Search Base.
6. You can test the LDAP connection if you have entered a password.
7. Click OK.

You can also set connection pool details, such as how many connections can be active at any time.

## Create a Directory Synch Template

Synchronization templates control how local changes are propagated to your endpoints, and how they are formatted. You can create synchronization templates for each of the endpoint types you want to control from your ADS installation. You can also create multiple templates for a single endpoint to subdivide the synchronization data, by business unit, for example.

Add one or more templates to each directory monitor in your environment. Add directory monitors before you can add synchronization templates.

**Follow these steps:**

1. Log in to CA IAM CS, and select the Endpoints tab to see the available endpoints that you can synchronize with.
2. Select the Directory Sync tab, then click the monitor entry where you want to add a synchronization template, and click Add in the Template area.

   The Add Template dialog appears.
3. Select the template type that you want from the drop-down menu, and then select an available endpoint name.
4. Select the User Store tab to set User Store details:
   a. Click Add in the Trigger Groups area.

   b. Enter a filter value if you want to refine the search for available groups. You can also accept the default in the Add Trigger group dialog.

   c. Click Search.

   A list of available Active Directory groups appears.

   d. Select the group or groups you want using the shuttle control, and click OK.
5. Select the Attributes tab to configure how the template maps Active Directory source information to the target endpoint:

   A list of default attributes appears. Attributes that are required for your template type are displayed in bold type.

   a. Set required attribute mappings by selecting available mapping targets from the Maps To pull-down menu. You can also type a literal string.

   b. Set mappings for other available attributes as desired. Select a policy setting (WEAK or STRONG) for each mapping you add.

   For single-value attributes, you need only be sure that the policy is not NONE. For multivalue attributes, Strong replaces any existing attribute value in the endpoint, and weak adds the new attribute value to any existing endpoint values.

   c. If the standard mapping table does not meet your needs, use the advanced editor. Click Advanced to display the editor. The advanced editor allows you to:

- Use JavaScript evaluated attribute values.
- Pick object references for association values.
- Set alternate attribute mappings or default values that apply when the primary mapping cannot be resolved.

6. Click OK.

# Chapter 5: Managing Connectors

This section contains the following topics:

Add a Connector (see page 51)
Restart a Connector (see page 52)
Add a Third-Party Library to a Connector (see page 53)
Add a Certificate for a Connector (see page 54)
Customize the Configuration for a Connector (see page 55)

## Add a Connector

CA IAM CS lets you hot-deploy connectors. This means that you can add, start, stop, and remove connectors while CA IAM CS is running.

**Follow these steps:**

1. Log in to CA IAM CS (see page 21).
2. At the top, click the Connector Servers tab.
3. In the Connector Server Management area, click the Bundles tab.
4. In the Bundles area on the right, click Add.
5. Browse to a connector bundle JAR, then select the connector server on which this connector will be available.

   You can select Start Bundle to have it start automatically after loading, or you can start it yourself later.
6. Click OK.

   The new bundle appears in the Bundles list.
7. Right-click its name in the list, then choose Start from the popup menu.

# Restart a Connector

Restarting a connector is useful when you have changed some configuration and you want the connector to use the new setting.

These instructions apply to connectors that CA IAM CS manages.

**Follow these steps:**

1. Log in to CA IAM CS (see page 21).
2. Click the Connector Servers tab.
3. Click the Bundles tab.
4. Select the correct connector server from the Server Filter list.
5. Right-click on the connector, then select Refresh Imports.

   The selected connector restarts, and any bundles that depend on that connector also restart.

# Add a Third-Party Library to a Connector

The following connectors require libraries that do not ship with CA IAM CS:

- SecurID RSA 7 (see page 411)
- SAP R3 (see page 530)
- Oracle PeopleSoft (see page 380)
- Lotus Domino (see page 237)

If you want to use one of these connectors, you must add the required libraries to the connector bundle.

**Follow these steps:**

1. Download the required libraries.
2. Run the relevant script in this location:

   *cs-home*/bin

   The script prompts for the location of the files that you downloaded.

   The script creates a bundle for the libraries, and saves the bundle in the same folder as the script.
3. Log in to CA IAM CS (see page 21).
4. At the top, click the Connector Servers tab.
5. In the Connector Server Management area, click the Bundles tab.
6. Add the new bundle:
   a. In the Bundles area on the right, click Add.
   b. Browse to the bundle that the script created, then select the connector server on which this connector will be available.
   c. Click OK.

      The new bundle appears in the Bundles list.
7. Find the main connector bundle in the Bundles list, then right-click its name in the list and choose Refresh Imports from the popup menu.

The connector can now use the third-party library bundle.

# Add a Certificate for a Connector

CA IAM CS has its own keystore. You can add trusted certificates (either standalone certificates or keystores) to this keystore, using the Certificates tab.

When you work with CA IAM CS certificates, your changes apply only to the connector server that you are logged in to. The certificates for any peer connector servers remain unchanged.

**Follow these steps:**

1. Log in to CA IAM CS (see page 21).
2. Click the Certificates tab.

   This tab lists all of the certificates in the CA IAM CS keystore. To filter the list of certificates by their names, type in the Certificate Filter box.
3. Click Add, then enter the details of the certificate:
   a. Select Certificate if the target is a standalone certificate file, or Key Store, if it is saved in a keystore.
   b. Browse to the certificate, select it, and click Add.
   c. Enter the alias. If you selected Key Store, this alias identifies the certificate in the keystore.
   d. If you selected Key Store, enter the keystore password.

The certificate or keystore is added to the CA IAM CS keystore, and the certificate is available for use by connectors.

Note the following information:

- To download a certificate, select it then click Download. You can download a certificate for either a private key or trusted certificate. You can then import this file another component, such as another instance of CA IAM CS.
- To delete a certificate from the CA IAM CS keystore, select it then click Remove. You can remove any trusted certificate from the CA IAM CS keystore. However, you cannot remote private key entries, because these keys are required by CA IAM CS.
- You cannot use the Certificates tab to manage private keys. Instead, update the Java keystore file and restart CA IAM CS.

# Customize the Configuration for a Connector

The configuration for each connector is stored in connector.xml in *cs_home*/jcs/conf/. Each connector also has the following files in *cs_home*/jcs/conf/override/*connector*:

- **connector.xml—**Use this file to override settings. By default this file is identical to the main version of connector.xml.
- **SAMPLE.connector.xml—**This is a template file which contains common customizations.

**Follow these steps:**

1. Rename *connector.xml* so that you can revert to it later if you need to.
2. Copy *SAMPLE.connector.xml* and rename the copy to *connector.xml*.
3. Edit the newly renamed file.
4. Restart the connector (see page 52).

## Change Pool Settings

To maximize scalability for a connector by configuring it to match expected usage patterns, you can change pool-related settings.

Connection pooling is configured through the connector.xml file for an individual connector, rather than in the server_jcs.xml global configuration file.

Most connectors use a connection pool configured in connector.xml, for example, through:

- poolConfig for JNDI and most connectors.

  **Note:** For more information, see the Class GenericObjectPool on http://jakarta.apache.org

- dataSourceConfigProps for JDBC

  **Note:** For more information, see http://jakarta.apache.org for a complete list and documentation of available configuration parameters.

**Follow these steps:**

1. Copy *cs-home*/conf/override/jdbc/SAMPLE.connector.xml and rename the copy to connector.xml.
2. Edit the connector.xml file.
3. Restart the connector (see page 52).

# Chapter 6: Connecting to Endpoints

This section contains the following topics:

CA Access Control Connector (see page 58)
CA ACF2 Connector (see page 82)
CA Arcot Connector (see page 107)
Embedded Entitlements Manager Connector (see page 108)
CA DLP Connector (see page 111)
CA SSO Connector for Advanced Policy Server (see page 125)
CA Top Secret Connector (see page 136)
DB2 UDB for z/OS Connector (see page 164)
Google Apps Connector (see page 171)
IBM DB2 UDB Connector (see page 173)
Kerberos Connector (see page 180)
LDA Connector Migration to DYN JNDI (see page 226)
Lotus Domino Connector (see page 237)
Microsoft Active Directory Services Connector (see page 271)
Microsoft Exchange Connector (see page 307)
Microsoft SQL Server Connector (see page 330)
Microsoft Windows Connector (see page 335)
Oracle Applications Connector (see page 350)
Oracle Connector (see page 357)
OS/400 Connector (see page 364)
PeopleSoft Connector (see page 380)
RACF Connector (see page 396)
RSA ACE (SecurID) Connector (see page 411)
RSA Authentication Manager SecurID 7 Connector (see page 423)
Salesforce.com Connector (see page 514)
SAP Connector (see page 530)
SAP UME Connector (see page 547)
Siebel Connector (see page 554)
UNIX ETC and NIS Connector (see page 568)

# CA Access Control Connector

The CA Access Control Connector lets you administer accounts and groups on CA Access Control servers.

The CA Access Control Connector provides a single point for all user administration by letting you do the following:

- Register endpoints, explore them for objects to manage, and correlate their accounts with global users
- Create and manage CA Access Control accounts using account templates specific to CA Access Control
- Change account passwords and account activations in one place
- Synchronize global users with their roles or synchronize global users' accounts with their account templates
- Assign a CA Access Control account template to each of your CA Access Control endpoints
- Use the default Endpoint Type account template to create accounts with the minimum level of security needed to access a CA Access Control endpoint
- Create and manage CA Access Control groups
- Generate and print reports about CA Access Control accounts and groups
- Create and manage objects of the supported CA Access Control resource classes.

This connector is managed using the Connector and C++ Server installation process.

**Note:** For more information and requirements, see *Connector and C++ Connector Server Installation.*

## Recommended Patch Levels

If you are using the Solaris, HP-UX, Linux, or AIX version of CA Access Control UNIX r5.3, you must apply the mandatory patch for the corresponding version of CA Access Control. Consult CA Access Control Customer Support to obtain the latest revisions of these mandatory patches.

If you are using the CA Access Control Connector for UNIX, you must install the latest revision of CA Access Control UNIX r12 on the UNIX system where the C++ Connector Server is to be run.

## ACC Connector Multi-Threading Support

The ACC Connector supports multi-threading and is capable of handling concurrent operations targeting multiple ACC endpoints (AC endpoints) concurrently.

### Managing ACC Sessions

The following parameters have been added to the acc_agent.ini file to support multi-threading:

[SessionManager]

**MaxSessions:**

> Specifies the maximum number of connections initialized by the ACC Connector to simultaneously connect to CA Access Control endpoints.
>
> This value should not be less than the MaxSessionsPerEndpoint parameter. For example, MaxSessions=200 and MaxSessionsPerEndpoint=1, the server can simultaneously connect to 200 ACC endpoints. For MaxSessions=50 and MaxSessionsPerEndpoint=2, the server can simultaneously connect to 25 ACC endpoints.
>
> **Note:** This value should not exceed the number of threads configured in im_css.conf.
>
> **Default:** 200

[Session]

**MaxSessionsPerEndpoint:**

> Specifies the maximum number of connections the server can use for one ACC endpoint.
>
> **Caution:** The ACC endpoint may return a connection reset error if this value is set too high.
>
> **Default:** 1 (This value is optimal for most configurations.)

The acc_agent.ini file is located in the following location:

```
%PS_HOME%\Provisioning Server\Data\ACC\acc_agent.ini
```

## Runtime Environment Settings

The following are the runtime environment settings for the CA Access Control Connector for Windows and the CA Access Control Connector for UNIX.

## Setting the Encryption Key for the CA Access Control Connector

If the CA Access Control Connector has to use an encryption key other than the default one to manage your CA Access Control systems, issue the following commands at the prompt on the Provisioning Server to enter a new encryption key:

```
cd  PS_HOME\Provisioning Server\etc\acc
CHANGE_EAC_KEY
```

**Important!** Restart the Windows service C++ Connector Server after the new encryption key is set.

## Resetting the Encryption Key for the CA Access Control Connector Back to the Default Key

If the CA Access Control Connector has to use the default encryption key to manage your CA Access Control systems, do not change the encryption key. If you need to change your new encryption key back to the default encryption key, issue the following commands at the prompt on the Provisioning Server:

```
cd  PS_HOME\Provisioning Server\etc\acc
RESET_EAC_KEY
```

**Important!** Restart the Windows service C++ Connector Server after the new encryption key is set.

## Changing the Encryption Method for the CA Access Control Connector

If the CA Access Control Connector has to use an encryption method other than the default one to manage your CA Access Control systems, edit the following Windows registry entry on the Provisioning Server and set the value to the path name of the DLL for the new encryption method:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\Identity Manager\Provisioning
Server\NSOptions\ACC\eTrust Access Control SDKrt\Encryption Package
```

For example, you can change the value of the Encryption Package from C:\Program Files\CA\Identity Manager\Provisioning Server\etc\acc\defenc.dll for the default encryption to C:\Program Files\CA\Identity Manager\ Provisioning Server\etc\acc\tripledesenc.dll for triple-DES encryption.

**Note:** The directory *PS_HOME*\Provisioning Server\etc\acc contains the encryption DLLs for the default encryption, DES encryption, triple-DES encryption, and AES encryption.

**Important!** Restart the Windows service C++ Connector Server after the encryption method is changed.

## CA Access Control Connector for UNIX

CA Access Control UNIX r8.0 or greater must be running on the same UNIX system where the CA Access Control Connector is installed. Otherwise, the CA Access Control Connector will not work. For Solaris, if CA Access Control UNIX r8.0 is installed after the CA Access Control Connector is installed, you must add the library pathname for CA Access Control UNIX r8.0 to the environment variable LD_LIBRARY_PATH. For example, if CA Access Control UNIX r8.0 is installed in directory /opt/CA/eTrustAccessControl, add the pathname /opt/CA/eTrustAccessControl/lib to LD_LIBRARY_PATH. You do not have to add the path name if CA Access Control UNIX r8.0 is already installed before the CA Access Control Connector is installed.

The CA Access Control Connector shares the same runtime environment with CA Access Control UNIX r8.0. Therefore, they will have the same encryption settings. In order to change the encryption method or key of the CA Access Control Connector, you have to change the corresponding one of CA Access Control UNIX r8.0. Refer to the documentation for CA Access Control UNIX r8.0 for information about changing the encryption settings. You need to restart the C++ Connector Server process after the encryption settings are changed.

## Configuring CA Access Control UNIX on the C++ Connector Server System

**Note:** This section is only applicable to the CA Access Control Connector for UNIX.

The UNIX user who invokes the C++ Connector Server process for CA IdentityMinder must be properly defined to CA Access Control UNIX. By default, UNIX user *imps* is to run the C++ Connector Server process.

Start CA Access Control command selang on the UNIX system where the C++ Connector Server is installed and issue the following commands in selang:

```
eu imps admin
```

```
auth terminal superagent_workstation_name uid(imps) acc(a)
```

where

***superagent_workstation_name***

Is the machine name of the UNIX system where the superagent is installed.

## Configuring a CA Access Control UNIX or Windows Server

To configure your CA Access Control UNIX or Windows server for CA IdentityMinder, follow these steps:

1. Start the selang command interpreter.
2. Create the system administrator's account on the CA Access Control server if it does not already exist.
3. Authorize CA IdentityMinder to connect to the CA Access Control server.
4. Enable the administrator's account to connect from the Provisioning Server.
5. Install Filtering Rules for the Policy Model Database (PMDB).

**Note:** You can also use the CA IdentityMinder for Access Control utility (SeAM) to perform these authorizations.

## Starting the Selang Command Interpreter

To begin the configuration process, start the selang command interpreter on the CA Access Control server system as follows:

a. Change directory to the home directory of CA Access Control from a UNIX or Window prompt.

b. Change directory to *bin* and then enter the command *selang*

## Creating the System Administrator's Account

Create an administrator's account on the CA Access Control server using the user ID and password that you use when logging on to the Provisioning Server. To do this, issue the following commands in selang:

```
nu administrator_name password (administrator_password) admin auditor
```

***administrator_name***

Is the user ID that you use to log on to the Provisioning Server.

***administrator_password***

Is the administrator's password for the user ID.

**Important!** It is strongly recommended that you do not use a user ID named “Administrator” to define a CA Access Control directory for Windows 2000, because doing so may cause login failures when you try to access the directory.

Ensure that you add the admin and auditor keywords to the command. This gives you administrative privileges.

Next, you must create the administrator's account and password in the native operating system (UNIX). To do this, issue the following commands in selang:

```
env(native)

eu administrator_name password(administrator_password)

env(seos)
```

***administrator_name***

Is the user ID that you use to log on to the Provisioning Server.

***administrator_password***

Is the administrator's password for the user ID.

## Authorizing Access to the CA Access Control Server

To give the Provisioning Server access to the CA Access Control server, issue the following command in selang:

```
nr TERMINAL workstation_name owner(terminal_owner) defacc(R)
```

***workstation_name***

Is the machine name of the Provisioning Server.

***terminal_owner***

Is the owner of the terminal.

For example, if the *workstation_name* is cacc.la.com and the *terminal owner is nobody, enter the following:*

```
nr TERMINAL cacc.la.com owner(nobody) defacc(R)
```

## Enabling the Administrator's Account

Issue the following command in selang so that the administrator's account can access the CA Access Control server:

```
auth TERMINAL workstation_name acc(a) uid(administrator_name)
```

***workstation_name***

Is the machine name of the Provisioning Server or CA IdentityMinder clients.

***administrator_name***

Is the administrator's account that was created in Creating the System Administrator's Account.

For example:

```
auth TERMINAL cacc.la.com acc(a) uid(accadmin)
```

**Note:** To successfully create an Provisioning Account on the CA Access Control Solaris machine, you have to authorize the two machines as follows:

```
auth TERMINAL workstation_name acc(a) uid(administrator_name) Workstation name - Provisioning Server name & Access Control Solaris machine
```

If you are not authorizing the Access Control Solaris machine, an error message "You are not allowed to administer this site from terminal (ACC Control Sol Machine)" is thrown during the Provisioning account creation.

## Installing Filtering Rules for the Policy Model Database (PMDB)

The following step should be performed after you enable the administrator's account.

The following PMDB filtering rules should be specified for each PMDB on the CA Access Control server if you want to administer the PMDB. These rules prevent internal updates to the pre-defined account *__ACCAgt* (use two underscores with this account name) from being propagated to the subscribers of the PMDB.

```
#--------------------------------------------------------------------------------
# ACCESS   ENV.      CLASS     OBJECTS     PROPERTIES   ACTION
#--------------------------------------------------------------------------------
  MODIFY   eTrust    USER        __ACCAgt      *          NOPASS
  CREATE   eTrust    USER        __ACCAgt      *          NOPASS
  DELETE   eTrust    USER        __ACCAgt      *          NOPASS
```

For example, if the PMDB is for CA Access Control for UNIX, add these rules to the filter file specified in the *pmd* section of the *pmd.ini* file for the PMDB.  For CA Access Control for Windows, the filter file is specified in the registry for the PMDB.  For either platform, create the filter file if it does not exist.

The *Utilities Guide* for CA Access Control for UNIX and the *Administrator Guide* for CA Access Control for Windows provide the instructions for setting up filtering rules for PMDB propagation.

## ACC Support for FIPS and IPv6

For this release of CA IdentityMinder, the CA Access Control Connector does not support FIPs or IPv6.

# Connector-Specific Features

This section details your connector's specific management features, such as how to acquire and explore your endpoint. Also included are account, provisioning roles, account template, and group information specifically for your connector.

## Acquire a CA Access Control Server Using the User Console

You must acquire the CA Access Control server before you can administer it with CA IdentityMinder.

**To acquire a CA Access Control server using the User Console**

1. Select Endpoints, Manage Endpoints,Create Endpoint
2. Select Access Control from the drop-down list box on Create a new endpoint of Endpoint Type, and click Ok

   Use the Create Access Control Endpoint page to register a CA Access Control server. During the registration process, CA IdentityMinder identifies the CA Access Control server you want to administer and gathers information about it.
3. After entering the required information, click Submit.

   You are now ready to explore and Correlate the endpoint.
4. Click Endpoints, Explore and Correlate Definitions, Create Explore and Correlate Definition to explore the objects that exist on the endpoint.

   The Exploration process finds all Access Control accounts and groups. You can correlate the accounts with global users at this time or you can correlate them later.
5. Click OK to start a new definition.
6. Complete the Explore and Correlate Tab as follows:
   1. Fill in Explore and Correlate name with any meaningful name.

      Click Select Container/Endpoint/Explore Method to click a Access Control endpoint to explore.
   2. Click the Explore/Correlate Actions to perform:
      - **Explore directory for managed objects**—Finds objects that are stored on the endpoint and not in the provisioning directory.
      - **Correlate accounts to users**—Correlates the objects that were found in the explore function with users in the provisioning directory. If the user is found, the object is correlated with the user. However, you can instead select that you want to assign the account to the existing user (the default user) or create the user.
      - **Update user fields**—If a mapping exists between the object fields and the user fields, the user fields are updated with data from the objects fields.
7. Complete the Recurrence tab if you want to schedule when the task to executes.
   1. Click Schedule.
   2. Complete the fields to determine when this task should execute.

      You may prefer to schedule the task to execute overnight to interfere less with routine access of the system.

**Note**: This operation requires the client browser to be in the same time zone as the server.  For example, if the client time is 10:00 PM on Tuesday when the server time is 7:00 AM, the Explore and Correlate definition will not work.

8. Click Submit.

**To use an explore and correlate definition**

1. In a CA IdentityMinder environment, click Endpoints, Execute Explore and Correlate.
2. Click an explore and correlate definition to execute.
3. Click Submit.

   The user accounts that exist on the endpoint are created or updated in CA IdentityMinder based on the explore and correlate definition you created.

## Acquire the CA Access Control Server Using the Provisioning Manager

You must acquire the CA Access Control server before you can administer it with CA IdentityMinder. When acquiring a CA Access Control server, perform the following steps from the Endpoint Type task view:

1. Register the server as an endpoint in CA IdentityMinder.

   Use the CA Access Control property sheet to register a CA Access Control server. During the registration process, CA IdentityMinder identifies the CA Access Control server you want to administer and gathers information about it.

   **Note:** Ping the node name from the Provisioning Server. If the ping is successful, then you know that CA IdentityMinder will find the CA Access Control node.

2. Explore the objects that exist on the directory.

   After registering the server in CA IdentityMinder, you can explore its contents, using the Explore and Correlate Endpoint dialog. The Exploration process finds all CA Access Control accounts and groups. You can correlate the accounts with global users at this time, or you can correlate them later.

3. Correlate the explored accounts with global users.

   When you correlate accounts, CA IdentityMinder creates or links the accounts on an endpoint with global users. By correlating accounts, you can specify what fields are matched with global user fields. CA IdentityMinder provides a default correlation account template for CA Access Control endpoints. This account template performs the following actions in this order:

   a. CA IdentityMinder attempts to match the account name with each existing global user's unique name. If a match is found, CA IdentityMinder associates the CA Access Control account with the global user. If a match is not found, CA IdentityMinder performs the next step.

   b. CA IdentityMinder attempts to match the full name with each existing global user's full name. If a match is found, CA IdentityMinder associates the CA Access Control account with the global user. If a match is not found, CA IdentityMinder performs the next step.

   c. If the Create Global Users as Needed button is selected, CA IdentityMinder creates a new global user and then associates the CA Access Control account with the global user. If the Create Global Users as Needed button is cleared, CA IdentityMinder performs the next step.

   d. CA IdentityMinder associates the CA Access Control account with the [default user] object.

## ACC Account Templates

The CA Access Control Default Policy, provided with the CA Access Control Connector, gives a user the minimum security level needed to access an endpoint. You can use it as a model to create new account templates.

**Important!** When you associate a new endpoint to an account template, the new endpoint must contain all applications, application groups, and groups that have already been selected for the associated account template. For details, see Associating Account Templates with Endpoints.

## File Class Administration

A property sheet called the CA Access Control File has been added so that you can protect files on a Windows or UNIX operating system.

**General Tab on CA Access Control File Property Sheet**

From this tab you can add file records to the Access Control database to be protected on a CA Access Control Windows or UNIX system.

**Default Access Tab on CA Access Control File Property Sheet**

From this tab you can grant access to an account or group who is not defined to CA Access Control or do not appear in the access control list of the resource. However, an account or group must exist in the CA Access Control database.

**Authorization Tab on CA Access Control File Property Sheet**

From this tab you can set the access control lists or ACLs of a file. You can also set the desired file permissions in the Permissions window on this tab.

**Audit Tab on CA Access Control File, Program, Terminal, Loginappl, Surrogate, and Regkey Property Sheets**

From this tab you can specify various properties for auditing access to a resource.

**Day/Time Restrictions Tab on CA Access Control File, Program, Terminal, Loginappl, Surrogate, and Regkey Property Sheets**

From this tab you can specify the days and hours when access to a resource is allowed.

**ACC Statistics Tab on CA Access Control File, Program, Terminal, Loginappl, Surrogate, and Regkey Property Sheets**

From this tab, you can view the usage statistics for a resource that has been created in the CA Access Control database.

## TERMINAL Class Administration

A property sheet called CA Access Control Terminal has been added so that you can create, modify, delete, or duplicate terminal records in the CA Access Control database.

**General Tab on CA Access Control Terminal Property Sheet**

From this tab you can add terminal records to the Access Control database to be protected on a CA Access Control Windows or UNIX system.

**Default Access Tab on CA Access Control Terminal Property Sheet**

From this tab you can grant access to an account or group who is not defined to CA Access Control or do not appear in the access control list of the resource. However, an account or group must exist in the CA Access Control database.

**Authorization Tab on CA Access Control Terminal Property Sheet**

From this tab you can set the access control lists or ACLs of a terminal.

## PROGRAM Class Administration

A property sheet called CA Access Control Program has been added so that you can protect programs on a Windows or UNIX operating system.

**General Tab on CA Access Control Program Property Sheet**

From this tab you can add program records to the CA Access Control database to be protected on a CA Access Control Windows or UNIX system.

**Trusted Program Tab on CA Access Control Program Property Sheet**

From this tab you can specify the unique security properties of a program, such as the program information to monitor.

**Default Access Tab on CA Access Control Program Property Sheet**

From this tab you can grant access to an account or group who is not defined to CA Access Control or do not appear in the access control list of the resource. However, an account or group must exist in the CA Access Control database.

**Authorization Tab on CA Access Control Program Property Sheet**

From this tab you can set the access control lists or ACLs of a program.

**Note:** You must be running at minimum, CA Access Control r5.3 UNIX or CA Access Control Windows r8.0 in order for the Provisioning Manager to enable the program Condition field.

## LOGINAPPL Class Administration

A property sheet called CA Access Control Loginappl has been added so that you can create, modify, delete, or duplicate loginappl records in the CA Access Control database. Only the UNIX version of CA Access Control supports this resource.

**General Tab on CA Access Control Loginappl Property Sheet**

From this tab you can add loginappl records to the CA Access Control database to be protected on a UNIX system.

**Default Access Tab on CA Access Control Loginappl Property Sheet**

From this tab you can grant access to an account or group who is not defined to CA Access Control or do not appear in the access control list of the resource. However, an account or group must exist in the CA Access Control database.

**Authorization Tab on CA Access Control Loginappl Property Sheet**

From this tab you can set the access control lists or ACLs of a loginappl.

## Surrogate Class Administration

A property sheet called CA Access Control Surrogate has been added so that you can create, modify, delete, or duplicate surrogate records in the CA Access Control database.

**Note:** Surrogate Class is not supported by the Windows NT version of CA Access Control.

**General Tab on CA Access Control Surrogate Property Sheet**

From this tab you can add surrogate records to the CA Access Control database to be protected on an Access Control Windows or UNIX system. The name of a surrogate must be in the form of USER.*name* or GROUP.*name*.

**Default Access Tab on CA Access Control Surrogate Property Sheet**

From this tab you can grant access to an account or group who is not defined to CA Access Control or do not appear in the access control list of the resource. However, an account or group must exist in the CA Access Control database.

**Authorization Tab on CA Access Control Surrogate Property Sheet**

From this tab you can set the access control lists or ACLs of a surrogate.

## REGKEY Class Administration

A property sheet called CA Access Control REGKEY has been added so that you can create, modify, delete, or duplicate regkey records in the CA Access Control database. Only the Windows version of CA Access Control supports this resource class.

**General Tab on CA Access Control Regkey Property Sheet**

From this tab you can add regkey records to the CA Access Control database to be protected on a CA Access Control Window system.

**Default Access Tab on CA Access Control Regkey Property Sheet**

From this tab you can grant access to an account or group who is not defined to CA Access Control or do not appear in the access control list of the resource. However, an account or group must exist in the CA Access Control database.

**Authorization Tab on CA Access Control Regkey Property Sheet**

From this tab you can set the access control lists or ACLs of a regkey.

## ACC Etautil Conventions

Use the following CA Access Control conventions in your etautil commands:

The endpoint type name (eTNamespaceName) is Access Control.

- The endpoint type prefix is ACC. The CA Access Control class names are:
  - eTACCDirectory for an endpoint class
  - eTACCPolicyContainerName for an account template container
  - eTACCPolicy for an account template object

## Associating ACC Account Templates with Endpoints

When associating account templates with endpoints, you must follow the intersection *requirement* for account templates: For any new endpoint that you want to associate with an account template, all groups, categories, and security labels that have previously been selected for the account template *must* exist in the new endpoint. If any of the previously selected groups, categories, or security labels for the account template do not exist in the new endpoint, the attempt to associate the new endpoint to the account template fails, and an error message is displayed.

## Sample Scenario Using Groups

This sample scenario uses groups to illustrate the intersection requirement. At the beginning of this scenario, the following are true:

- Groups 1 through 4 exist in the Endpoint 1.
- Group 1 and Group 4 exist in Endpoint 2.
- Account Template 1 is not associated to any endpoints.

The following table illustrates this setup:

| Endpoint 1 | Endpoint 2 | Account Template 1 |
|---|---|---|
| Group 1 | Group 1 | (none) |
| Group 2 | | |
| Group 3 | | |
| | Group 4 | |

Suppose you perform the following steps:

1. Associate Endpoint 1 with Account Template 1, creating the first endpoint association for Account Template 1.

| Endpoint 1 | Endpoint 2 | Account Template 1 |
|---|---|---|
| Group 1 | Group 1 | + Endpoint 1 (succeeds) |
| Group 2 | | |
| Group 3 | | |
| | Group 4 | |

2. Select Group 1 and Group 2 for Account Template 1. The selection succeeds because these groups exist in Endpoint 1.

| Endpoint 1 | Endpoint 2 | Account Template 1 |
|---|---|---|
| Group 1 | Group 1 | Endpoint 1 |
| Group 2 | | + Group 1 (succeeds) |
| Group 3 | | + Group 2 (succeeds) |
| | Group 4 | |

3. Attempt to associate Endpoint 2 with Account Template 1. The attempt fails because one of the account template's selected groups, Group 2, does not exist in Endpoint 2.

| **Endpoint 1** | **Endpoint 2** | **Account Template 1** |
|---|---|---|
| Group 1 | Group 1 | Endpoint1 |
| Group 2 | | Group 1 |
| Group 3 | | Group 2 |
| | Group 4 | + Endpoint 2 (fails) |

When the attempt fails, the Manager displays an error message similar to the following one:

```
Resources not found
```

Endpoint 2 is not necessarily required to contain the same groups as Endpoint 1. However, Endpoint 2 **must** contain all groups from Endpoint 1 that have already been selected for Account Template 1. In other words, for any new endpoint that you want to associate with an account template, all previously selected groups for the account template must exist in the new endpoint.

## Sample Scenario Using Additional Groups

A new endpoint that you want to associate to an account template  is permitted to contain *additional* groups; that is, groups that have not been selected for the account template. After you associate the new endpoint to the account template, you may optionally select any of these additional groups for the account template. If you do, these groups are **added** to the list of required groups that must exist in all new endpoints that you attempt to associate with the account template in the future.

The following scenario illustrates this principle. At the beginning of this scenario, the following are true:

- Groups 1 through 4 exist in Endpoint 1
- Groups 1 through 3 exist in Endpoint 2
- Account Template 1 has no associated endpoints

The following table illustrates this setup:

| **Endpoint 1** | **Endpoint 2** | **Account Template 1** |
|---|---|---|
| Group 1 | Group 1 | (none) |
| Group 2 | Group 2 | |
| Group 3 | Group 3 | |

| | | |
|---|---|---|
| Group 4 | | |

Suppose you perform the following steps:

1. Associate Endpoint 1 with Account Template 1, creating the first endpoint association for Account Template 1.

| **Endpoint 1** | **Endpoint 2** | **Account Template 1** |
|---|---|---|
| Group 1 | Group 1 | + Endpoint 1 (succeeds) |
| Group 2 | Group 2 | |
| Group 3 | Group 3 | |
| Group 4 | | |

2. Select Group 1 and Group 2 for Account Template 1. The selection succeeds.

| **Endpoint 1** | **Endpoint 2** | **Account Template 1** |
|---|---|---|
| Group 1 | Group 1 | Endpoint 1 |
| Group 2 | Group 2 | + Group 1 (succeeds) |
| Group 3 | Group 3 | + Group 2 (succeeds) |
| Group 4 | | |

   Consequently, any endpoints that you attempt to associate with Account Template 1 in the future must contain Group 1 and Group 2; otherwise, the attempt will fail.

3. Associate Endpoint 2 with Account Template 1, creating the second endpoint association for Account Template 1. The association succeeds, because all groups already selected for Account Template 1 (Group 1 and Group 2) exist in Endpoint 2.

| **Endpoint 1** | **Endpoint 2** | **Account Template 1** |
|---|---|---|
| Group 1 | Group 1 | Endpoint 1 |
| Group 2 | Group 2 | Group 1 |
| Group 3 | Group 3 | Group 2 |
| Group 4 | | + Endpoint 2 (succeeds) |

4. Select Group 3 for Account Template 1. The selection succeeds.

| **Endpoint 1** | **Endpoint 2** | **Account Template 1** |
|---|---|---|
| Group 1 | Group 1 | Endpoint 1 |

| | | |
|---|---|---|
| Group 2 | Group 2 | Group 1 |
| Group 3 | Group 3 | Group 2 |
| Group 4 | | Endpoint 2 |
| | | + Group 3 (succeeds) |

Consequently, any endpoints that you attempt to associate with Account Template 1 in the future must contain groups Group 1 through Group 3; otherwise, the association will fail.

## Availability Requirements for Groups

On the Manager, the groups that you can select for an account template are displayed in the account template's list of available groups. Available groups must meet *both* of the following criteria:

- Are not already selected for the account template
- Exist in all endpoints that are associated with the account template

In the Sample Scenario Illustrating Additional Groups, Group 4 is an available group for Account Template 1 when Endpoint 1 is the only endpoint associated with the account template. However, when Endpoint 2 is associated with Account Template 1, Group 4 is no longer an available group for Account Template 1, because Group 4 does not exist in Endpoint 2.

## Availability Requirements for Categories and Security Labels

The intersection principle described previously for groups also applies to categories and security labels. That is, when you associate a new endpoint to an account template, the new endpoint is not necessarily required to contain all the same categories and security labels as the previous endpoint or endpoints that have already been associated with the account template. However, the new endpoint *must* contain all categories and security labels that have already been selected for the associated account template.

Similarly, a new endpoint that you want to associate to an account template is permitted to contain additional categories or security labels that have not already been selected for the account template. After you associate the new endpoint to the account template, you may optionally select any such categories or security labels for the account template. If you do so, these categories or security labels are *added* to the list of required categories and security labels that must exist in all new endpoints that are associated with the account template in the future.

Finally, the availability requirements discussed previously for groups also apply to categories and security labels. That is, an available category or security label remains available to an account template until an endpoint that does not contain the category or security label is associated with the account template.

### Removing ACC Endpoints from Account Templates

If an associated endpoint is removed from an account template, the list of selected items does not change. This is true even if the last endpoint is removed from an account template, but the list of available items is recomputed. For example, the connector attempts to compute the new list of available groups for the remaining endpoints that are still associated to the account template.

## Password Synchronization

The CA IdentityMinder password synchronization agent supports the interception of Windows password changes.

### Reconfiguring the Password Synchronization Component

These are the steps to reconfigure a CA IdentityMinder password synchronization component:

1. Install the Windows NT Connector after installing the Windows Connector (Windows NT or Active Directory).
2. Install Windows NT Remote Agent for a Windows NT system. Active Directory Services Connector directly manages Active Directory using LDAP.
3. Acquire the Windows directory to create an internal representation of the Windows system in CA IdentityMinder.

   **Note:** Do not explore and correlate the Windows accounts, because they are managed as CA Access Control accounts. Explore and correlate these as CA Access Control accounts.
4. Install the Password Synchronization agent. During the installation process, the Password Synchronization Configuration wizard guides you through the process to set the component as a Windows password interceptor.
5. Install the CA Access Control Connector to manage the CA Access Control accounts.
6. Install CA Access Control on the Windows system if it is not already installed.
7. Acquire the CA Access Control Directory.
8. Explore and correlate CA Access Control accounts to global users in CA IdentityMinder.
9. Revise the Password Synchronization Configuration File to reflect the changes from Windows to the CA Access Control Connector.

## Architecture

The out-of-box configuration does not support intercepting CA Access Control password changes. However, because CA Access Control also manages Windows password changes, you can reconfigure the password synchronization component to propagate CA Access Control password changes.

When a Windows password changes, the password synchronization component intercepts the change and forwards it to Provisioning Server, which then propagates the change to other accounts belonging to the same global user.

You can reconfigure the password synchronization component for synchronizing CA Access Control passwords, using the same Windows password interception.

Thus, users make changes to their passwords using CA Access Control tools. The password changes affect the CA Access Control environment and the native Windows environment. When you make password changes to the Windows environment, the Provisioning password synchronization component intercepts the password changes.

The reconfiguration of the Provisioning password synchronization component sends the password changes to the Provisioning Server, indicating that the password changes are from CA Access Control, instead of a native Windows system.

The Provisioning Server discovers the global user associated with the CA Access Control accounts that originate the password changes, and then propagates password changes to other accounts belonging to the same global users.

## Comparing PMDB to Local Database

CA IdentityMinder manages CA Access Control identities in an identity store that can be either a CA Access Control PMDB or a local database. Since CA IdentityMinder and CA Access Control both manage users and passwords, it is an architecture decision as to which users are managed by CA IdentityMinder and which by CA Access Control. A general guideline is that CA IdentityMinder manages a PMDB and the PMDB handles the propagation of all its subscribers.

## Changing Passwords Using Windows Tools

Besides password changes from CA Access Control tools, users can also change their passwords using Windows native utilities. The CA IdentityMinder password synchronization component intercepts the password change and propagates it to other CA IdentityMinder managed accounts associated with the same global users. However, the CA Access Control managed accounts require a separate mechanism to synchronize passwords initiated from the native Windows environment. CA Access Control also provides a password intercept mechanism for this purpose. We recommend the following guidelines:

- Disable the password quality control of the CA IdentityMinder password synchronization agent.
- Let the CA Access password synchronization component manage the password quality control.

## Mapping Configuration from Windows

The following two configuration files are an example of a conversion from Windows to CA Access Control. The information that you should modify is in italics.

```
;
; This configuration file is used by the CA IdentityMinder Windows Password
; Synchronization Facility.
;
[Server]
host=<Provisioning Server host>
port=20389
use_tls=yes
admin_suffix=dc=<domain suffix>
admin=etaadmin
password=k4tpGDJ8Djg=

;; CA IdentityMinder domain information
;;
;; If the search fails, and the container dn is specified, the account dn is
;; constructed as "<acct_attribute_name>=<native acct name>,<container dn>".
;; The container DN should contain "dc=eta".
;;
[EtaDomain]
domain=<domain name>
etrust_suffix="dc=eta"
domain_suffix=dc=<domain suffix>
Namespace=Windows NT
directory=chete03

directory_dn=eTN16DirectoryName=chete03,eTNamespaceName=Windows
NT,dc=129-731-CHOPIN,dc=eta
container_dn=eTN16AccountContainerName=Accounts,eTN16DirectoryName=chete03,eTName
spaceName=Windows NT,dc=129-731-CHOPIN,dc=eta
acct_attribute_name=eTN16AccountName
acct_object_class=eTN16Account
```

```
;
; This configuration file is used by the CA IdentityMinder Password Synchronization
; Facility for CA Access Control
;

[Server]
host=<Provisioning Server host>
port=20389
use_tls=yes
admin_suffix=dc=<domain suffix>
admin=etaadmin
password=k4tpGDJ8Djg=

;; CA IdentityMinder domain information
;;
;; In order to find the account DN, a search operation will be performed, using
;; the directory dn as the search base, and objectClass and account name as the
;; search filter.
;;
;; If the search fails, and the container dn is specified, the account dn is
;; constructed as "<acct_attribute_name>=<native acct name>,<container dn>".
;; The container DN should contain "dc=eta".
;;
;; Currently, domain, etrust_suffix, Endpoint Type, and directory keys are not used,
;; because all DNs are hardcoded. The future enhancement is to provide "domain",
;; "Endpoint Type" and, "directory name". CA IdentityMinder will find out the DNs based
on
;; the supplied information.

[EtaDomain]
domain=<domain name>
etrust_suffix="dc=eta"
domain_suffix=dc=<domain suffix>
Namespacee=Windows NT
directory=pmdb
;; Directory name of the CA Access Control system
```

```
directory_dn=eTACCDirectoryName=pmdb,eTNamespaceName=Access
Control,dc=129-731-CHOPIN,dc=eta
container_dn=eTACCAccountContainerName=Accounts,eTACCDirectoryName=pmdb,eTNamespa
ceName=Access Control,dc=129-731-CHOPIN,dc=eta
acct_attribute_name=eTACCAccountName
acct_object_class=eTACCAccount

;; Password Profile Configuration
;; profile_enabled = [yes|y|no|n] ---> Unknown values default to "no"
;; profile_dn = "<the DN of the password profile>"
[PasswordProfile]
profile_enabled = no
profile_dn = eTPasswordProfileName=Password
Profile,eTPasswordProfileContainerName=Password
Profile,eTNamespaceName=CommonObjects,dc=129-731-CHOPIN,dc=eta
```

# CA ACF2 Connector

The CA ACF2 Connector lets you administer accounts and resources on CA ACF2 systems and provides a single point for all user administration by letting you do the following:

- Register endpoints, explore them for objects to manage, and correlate their accounts with global users
- Create and manage accounts using account templates specific to CA ACF2
- Change account passwords and account activations in one place
- Synchronize global users with their roles or synchronize global users' accounts with their account templates
- Assign account templates to each of your CA ACF2 endpoints
- Use the default Endpoint Type account template to create accounts with the minimum level of security needed to access an CA ACF2 directory
- Create and delete data set and resource rule lines
- Generate and print reports about CA ACF2 accounts

## How to Configure Your CA ACF2 System

Once the CA ACF2 Connector has been installed with the Provisioning Server, you must configure your CA ACF2 system to communicate with the connector.

**To configure your CA ACF2 system**

1. Install the CA LDAP Server for z/OS on your CA ACF2 system.
2. Review the CA LDAP Server for z/OS configuration options.

## Step 1. Install the CA LDAP Server

The CA LDAP Server for z/OS provides the communication mechanism for this CA IdentityMinder Connector.  This product is a free offering from CA and can be downloaded from support.ca.com.  Once downloaded, refer to the *CA LDAP Server for z/OS Installation Guid*e for information and instructions on how to install it.

**Note:** The following steps are required to migrate from a previous version to r12.6.1:

1. The CA LDAP Server for z/OS must be installed on at least one mainframe system and configured to communicate to every z/OS system being managed by CA IdentityMinder or alternatively, you can install it on every z/OS system managed by CA IdentityMinder.
2. The CA LDAP Server(s) must be configured to have an endpoint entry in Provisioning Manager naming mode for each system. For more information on configuring, see the *CA LDAP Server for z/OS Administrator Guide*.
3. After upgrading, you must update each endpoint and update the information within the Mainframe LDAP Server section. This information matches up with the IP Address, Port, and suffix of the mainframe LDAP Server.

The existing eTrust_ACF.conf file must be removed from the eTrust_Admin.conf file, or alternatively, remove the contents from the file and make blank.

## Step 2. Review the CA LDAP Server for z/OS Configuration Options

Once all CA LDAP Server installation steps have been completed and your CA LDAP Server is started, the Server is ready to support administration for this Connector. Some clients may need or want to setup additional configuration options for the CA LDAP Server in order to provide additional functionality for the this Connector.  Some examples of this additional functionality are the enable_refresh option (instructs the CA LDAP Server to refresh User Profile data whenever it is changed on a Logon ID using the CA LDAP Server), or the enable_secauth option (provides Secondary Authid maintenance on Logon IDs using the CA LDAP Server).

For more information on all available configuration options, see the chapter titled, "CAACF2_DN Backend" in the *CA LDAP Server for z/OS Administrator Guide*.

## Securing Provisioning Server Communication to the CA LDAP Server

All communication between the Provisioning Server and the CA LDAP Server for z/OS can be encrypted using SSL (Secure Socket Layers).

**To establish communication**

- Setup your CA LDAP Server for z/OS to use the Server Mode for SSL connections. For information on how to configure this, see the chapter titled, "CA LDAP Server Using Digital Certificates" in the *CA LDAP Server for z/OS Administrator Guide*.
- Turn on SSL support within the Provisioning Server for your ACF2 endpoint. To do this, bring up the properties of your ACF2 endpoint using the Provisioning Manager. In the section entitled 'Mainframe LDAP Server Information', enable the check box entitled 'Use Server-side SSL' and click Apply. Now, all communication to the configured CA LDAP Server will attempt to use an SSL connection, and will fail and provide an appropriate error message if SSL cannot be established.

## ACF2 Support for FIPS and IPv6

For this release of CA IdentityMinder, the ACF2 Connector and the Password Synchronization Agent for ACF2 support IPv6, but not FIPS.

## Acquire an ACF2 System Using the User Console

You must acquire the ACF2 system before you can administer it with CA IdentityMinder.

**To acquire an ACF2 system using the User Console**

1. Select Endpoints, Manage Endpoints,Create Endpoint
2. Select CA-ACF2 from the drop-down list box on Create a new endpoint of Endpoint Type, and click Ok

   Use the Create CA-ACF2 Endpoint page to register an ACF2 system. During the registration process, CA IdentityMinder identifies the ACF2 system you want to administer and gathers information about it.
3. After entering the required information, click Submit.

   You are now ready to explore and Correlate the endpoint.

4. Click Endpoints, Explore and Correlate Definitions, Create Explore and Correlate Definition to explore the objects that exist on the endpoint.

   The Exploration process finds all ACF2 accounts and groups. You can correlate the accounts with global users at this time or you can correlate them later.

5. Click OK to start a new definition.

6. Complete the Explore and Correlate Tab as follows:

   a. Fill in Explore and Correlate name with any meaningful name.

      Click Select Container/Endpoint/Explore Method to click an ACF2 endpoint to explore.

   b. Click the Explore/Correlate Actions to perform:

      - **Explore directory for managed objects**—Finds objects that are stored on the endpoint and not in the provisioning directory.

      - **Correlate accounts to users**—Correlates the objects that were found in the explore function with users in the provisioning directory. If the user is found, the object is correlated with the user. However, you can instead select that you want to assign the account to the existing user (the default user) or create the user.

      - **Update user fields**—If a mapping exists between the object fields and the user fields, the user fields are updated with data from the objects fields.

7. Complete the Recurrence tab if you want to schedule when the task to executes.

   a. Click Schedule.

   b. Complete the fields to determine when this task should execute.

      You may prefer to schedule the task to execute overnight to interfere less with routine access of the system.

   **Note**: This operation requires the client browser to be in the same time zone as the server.  For example, if the client time is 10:00 PM on Tuesday when the server time is 7:00 AM, the Explore and Correlate definition will not work.

8. Click Submit.

**To use an explore and correlate definition**

1. In a CA IdentityMinder environment, click Endpoints, Execute Explore and Correlate.

2. Click an explore and correlate definition to execute.

3. Click Submit.

   The user accounts that exist on the endpoint are created or updated in CA IdentityMinder based on the explore and correlate definition you created.

## Acquire a CA ACF2 System Using the Provisioning Manager

You must acquire the CA ACF2 system before you can administer it with CA IdentityMinder. When acquiring a CA ACF2 system, perform the following steps from the Endpoint Type task view:

1. Register the server as an endpoint in CA IdentityMinder. This phase is performed by adding a new endpoint under the CA ACF2 Endpoint Type in CA IdentityMinder.

   Use the CA ACF2 Endpoint property sheet to view or customize a CA ACF2 system. During the registration process, CA IdentityMinder identifies the CA ACF2 system you want to administer and gathers information about it.

2. Explore the objects that exist on the endpoint.

   After registering the server in CA IdentityMinder, you can explore its contents. Use the Explore and Correlate Endpoint dialog. The Exploration process finds all CA ACF2 accounts and objects. You can correlate the accounts with global users at this time or you can correlate them later.

3. Correlate the explored accounts with global users.

   When you correlate accounts, CA IdentityMinder creates or links the accounts on an endpoint with global users, as follows:

   a. CA IdentityMinder attempts to match the logon ID with each existing global user name. If a match is found, CA IdentityMinder associates the CA ACF2 account with the global user. If a match is not found, CA IdentityMinder performs the next step.

   b. CA IdentityMinder attempts to match the logon ID name with each existing global user's full name. If a match is found, CA IdentityMinder associates the CA ACF2 account with the global user. If a match is not found, CA IdentityMinder performs the next step.

   c. If the Create Global Users as Needed button is selected, CA IdentityMinder creates a new global user and then associates the CA ACF2 account with the global user. If the Create Global Users as Needed button is cleared, CA IdentityMinder performs the next step.

   d. CA IdentityMinder associates the CA ACF2 account with the [default user] object.

## Register ACF2 Endpoints on a Windows System

If you have a Windows system, you can register CA ACF2 endpoints using the Provisioning Manager.

**From the Endpoint Type task view**

1. Select ACF2 Endpoint from Object Type
2. Click the New button and enter the following information:

   **Endpoint Name**

   Specifies a name to refer to the new CA ACF2 endpoint.

   **Mainframe LDAP IP Address/Machine Name**

   Specifies the IP address of the CA ACF2 managed system where the CA LDAP Server is configured and running.

   **Mainframe LDAP Port**

   Specifies the port number that you specified during the CA LDAP Server for z/OS install. If you are not sure of the Mainframe LDAP Port, see the section Checking Your CA LDAP Server for z/OS Configuration Information.

   **Mainframe LDAP Suffix**

   Click the 'Get Suffixes' button to retrieve a list of valid suffixes configured for this CA LDAP Server operations in im naming mode. (See the chapter titled, "CAACF2_DN Backend" in the *CA LDAP Server for z/OS Administrator Guide* for more information on naming mode.)

   **Admin User**

   Specifies the CA ACF2 LID of an administrator used from within CA IdentityMinder to manage the CA ACF2 system.

   **Password**

   Specifies the password of the CA ACF2 LID above.

   **Confirm Password**

   Specifies the same password as above, for confirmation.

   **Note:** After you click OK, the Provisioning Server attempts to establish a connection with the CA LDAP Server for z/OS at the IP address and port supplied, as well as validating the Admin user and Password values supplied. An appropriate error message is displayed if this connection fails. A Global User is inserted in the Provisioning Server with Domain Administrator authority using the ID and password supplied. This Global User is used to administer this endpoint.

### Register ACF2 Endpoints on a Solaris System

To register CA ACF2 endpoints, use the batch utility etautil to define a CA ACF2 endpoint by specifying a directoryName, Mainframe LDAP IPAddress, Port, and Suffix. For example:

```
etautil -u USERID -p PASSWORD add 'eTNamespaceName=CA-ACF2,dc=DOMAIN,dc=eta'
eTACFDirectory name='DIRECTORYNAME' eTZOSLDAPIPAddress=IPADDRESS
eTZOSLDAPPort=PORT eTZOSLDAPSuffix=SUFFIX
```

where,

**DIRECTORYNAME**

Specifies the name you desire for this endpoint.

**IPADDRESS**

Specifies the IP Address or Machine name of the CA-ACF2 system where your CA LDAP Server for z/OS is running.

**PORT**

Specifies the port number the CA LDAP Server is using.

**SUFFIX**

Specifies a valid suffix configured for this CA LDAP Server operating in im naming mode (For more information on the naming_mode option, see the chapter titled, "CAACF2_DN Backend" in the *CA LDAP Server for z/OS Administrator Guide*.)

### Check Your CA LDAP Server for z/OS Configuration Information

To view all pertinent information regarding your CA LDAP Server and its configuration, issue a STATUS command from the mainframe console where your CA LDAP Server is running.  The STATUS command provides information such as, version information, port number, configured databases, and suffixes. See the chapter titled, "Startup Options" in the *CA LDAP Server for z/OS Administrator Guide* for more information on the STATUS command.

## ACF2 Provisioning Roles and Account Templates

The CA-ACF2 Default Policy, provided with the C-ACF2 connector gives a user the minimum security level needed to access an endpoint. You can use it as a model to create new account templates.

## ACF2 Accounts

When synchronizing CA ACF2 accounts, strong synchronization is always the default.

## Validation Errors Thrown on Create or Modify Account/Account Templates Operations when Unsupported Attributes are Defined on Endpoints r12 or Greater

A set of attributes have been removed from CA ACF2 r12 servers and are no longer supported but are supported in ACF2 r9 and are currently defined in the CA IdentityMinder ACF2 Account and Account Template objects. When using these attributes, the account create or modify operations fail with 'unsupported attribute' errors. If an endpoint is r12 or greater, validation errors are thrown for each of the attributes defined. You must clear the text value or uncheck Boolean values in checkboxes to proceed.

The screen handlers must be aware of the associated endpoint's ACF2 version and hide/show these attributes depending on the version. Below are the obsolete option in r12 and its associated Provisioning attribute:

| Obsolete Option in CA ACF2 r12 | Associated Provisioning Attribute |
|---|---|
| CICSKEY | eTACFCICSSecKey1-3 |
| CICSKEYX | eTACFCICSSecKeyLast5 |
| IDMS | eTACFGeneralIDMSAccess |
| IDMSPROF | eTACFIDMSSignonClist |
| IDMSPRV | eTACFIDMSClistVersion |
| MUSOPT | eTACFIDMSMusassOpts10-2 |
| MUSPGM | eTACFIDMSMusassStartPgm |
| VAX | eTACFGeneralVAXAccess |

## Access and Resource Rules and Rule Keys

CA IdentityMinder lets you maintain existing access and resource rules created in CA ACF2.

CA IdentityMinder protects all resources and data sets by default. Since resources and data sets are evaluated in the same way, CA IdentityMinder provides a consistent approach to security regardless of the physical characteristics of the protected resource or data set.

Access rules and resource rules are defined with different rule types. When you expand the rule types, rule keys appear. Access and resource rules are defined as rule keys.

An individual resource or data set exists in CA IdentityMinder only as a specific member in a rule key. A rule key can represent one resource or data set, or a group of them.

A rule key protects resources and data sets from access by users other than the owner. When a user tries to access a rule key, CA IdentityMinder checks for a rule permission allowing the access. The rule permissions associated with that user determine which resources and data sets that user is authorized to access and the conditions under which access can occur. A user who is not the owner of the resource can access the resource only if the owner or the security administrator authorizes access in a rule permission.

In CA-ACF2, resources and rule keys are only accessed by the following:

- A user who has been granted specific access by the rule permission
- An owner of the rule key
- A user with special override privileges specified in the user's logon ID

## Change Control

This identifies the logon IDs or UIDs that can change the rule set. This is called a *change permission.* The change control is defined on the Rule Key Property page under - Change or Restricted Change.

**Note:** You can only view existing Change Control in the list boxes. You cannot create or delete them.

## Rule Lines

*Rule lines* identify asset type, any qualifiers of the rule key name, or a mask that applies to the rule key. In CA IdentityMinder, rule lines appear under the Rule Lines Tab.

You must identify the logon IDs or UIDs that have access to the resource or data set. This is called a *rule permission*. When a user attempts to access an asset, CA ACF2 checks for a rule permission allowing the access.

UID strings appear under rule lines. These UID strings identify a user or a group of users in a rule permission. The rule permission describes the environment for accessing the resource and determines whether the access is permitted for the user or group of users. Access is restricted by day and time, source, and access path (such as a particular program or library).

**Note:** You can create and delete rule lines; however, you cannot modify them after you have added them.

## Secondary Authids

The ACF2 Connector provides support for administration of DB2 Secondary Authids (ACF2 Cross-Reference or XREF records) on ACF2 Accounts and Policies. DB2 Secondary Authids specify the access rights ACF2 Accounts are permitted when accessing DB2 resources.

### Configuration for ACF2

The GSO OPTS record for the current sysid needs to be changed to specify a value in the ALTSYS field. The value should be the same list of sysids (minus the current sysid) as provided on the enable_secauth parameter in the CA LDAP Server for z/OS configuration file (slapd.conf) on the mainframe.

## Administer Secondary Authids

To administer Secondary Authids, there is a tab on ACF2 Accounts and Account Templates called Secondary Authids. This tab contains a list control containing the Secondary Authids assigned to the Account or Account Template. There are four buttons (three for Account) on this screen that provide the following functionality:

- Add Record(s) is always activated and provides a dialog screen for searching existing Secondary Authid records and assigning them to the Account or Account Template.
- Manual Add is always activated and provides a dialog screen to manually define a Secondary Authid to an Account or Account Template. The dialog contains a Sysid field and Secondary Authid field for an Account, and an additional Children field for an Account Template.
- Delete Record is activated when a record is selected in the list control, and will remove a Secondary Authid record from an Account or Account Template.
- Add/Del Children is only visible on an Account Template, and is activated when a record is selected in the list control. This button displays a dialog box that lets you maintain the list of Child Secondary Authids assigned to a Parent.

For account templates, Secondary Authids are classified as Parent and Child Secondary Authids. A Parent Secondary Authid is an XREF group record. The Secondary Authids that belong to this group are known as its Children, or Child Secondary Authids, which are XREF source records. When a Parent Secondary Authid is specified with a list of Children, any Account created from this Account Template will be assigned to one of the Child Secondary Authids, not the Parent. The Child Secondary Authid assigned to the Account is determined by the following algorithm:

The Child Secondary Authids are traversed in the order they are listed in the Account Template:

1. If the Child Secondary Authid has room for another entry, the Account will be added to that record.
2. If the record is full, then the next Child Secondary Authid is examined and if it has room, it is added to that one. This continues until a record is found that has room or does not exist.
3. If a Child Secondary Authid is encountered that does not exist, then it will be created with the Account added to it, and it will be added to the Parent Secondary Authid as a Child.

If a Parent Secondary Authid is added to an Account Template with no Children specified, then that Parent record is treated as a Source record and the Account will be added to that record.

In this case, no Child Secondary Authids should ever exist.

## Search Screen Notes

When searching for existing Parent records to add to the Account Template, clients should take care that the chosen Parent record does not contain any additional Parent records (XREF Group records). This would occur in a multi-layered Source Group record structure. In this case, the Child Secondary Authids that are XREF Group records on that Parent should be manually removed using the Add/Del Children button, and only Child Secondary Authids (XREF Source records) and un-created records should be listed as Children of that Parent.

## Account Screen Specifications

When listing Secondary Authids on an Account, only the Child Secondary Authid records that the Account actually belongs to will be displayed and not the Parent-Child relationship displayed in an Account Template. If an ACF2 Account is deleted, then that Account will be removed from all Secondary Authids it is currently assigned to.

## Policy Synchronization

Secondary Authids are synchronized when an Account/Global User is synchronized to its Account Templates/Provisioning Roles. For Account Templates that use the Parent-Child relationship method, an Account is considered synchronized to a particular Secondary Authid entry if the Account is assigned to one of the Child records specified for that entry in the Account Template. Likewise, if the Account is in possession of a Secondary Authid entry that does not exist on the Account Template as either a stand-alone Parent record or as a Child record in a Parent-Child entry, then that record is removed from the Account.

## Automated Administration of Secondary Authids

The ACF2 Agent performs the following several automated tasks to maintain the Secondary Authids assigned to an Account or Policy:

- Record Creation - The ACF2 Agent will create a Secondary Authid (Parent or Child) if it does not exist. It will add the specified Account to the new Secondary Authid if it is a Child record or stand-alone Parent record, and it will add a new Child record to a new Parent record if the specified Parent does not exist.
- Record Modification - If a new Child record (specified on the Account Template) needs to be created, then it will be created and added to the Parent record.
- Record Deletion - If an ACF2 Account is removed from a Secondary Authid (either through an Account modification or deletion), and the Account is the last Logonid on the Secondary Authid, then that record will be deleted and removed from any Parent records it belongs to. If the Secondary Authid is also the last record on the Parent record, then the Parent record will be deleted also.

## Errors

If an error occurs on an add or modify Account transaction related to Secondary Authids, the LDAP server will return an error code of PARTIAL_SUCCESS. This tells CA IdentityMinder that an error occurred during processing, but processing continued and the transaction is to be considered a success. The reason for this is that any processing that had already occurred against the Account (creation, modification, and deletion) will have occurred successfully before Secondary Authid maintenance was performed. The Provisioning Manager will report the error, but proceed as a successful transaction. The error can then be reviewed, and appropriate action can be determined and taken against Secondary Authids.

For Account delete transactions, if an error occurs during Secondary Authid maintenance, this error will be returned as an error and the Account will not be deleted. This is because the eTA LDAP Server does not handle partial success situations with Account deletes; therefore the message returned must be a success or failure. Review the error returned and take appropriate action to enable the transaction to proceed properly.

The following error messages can be returned when an error occurs with Secondary Authids:

**LDP0143E Manual maintenance required for XREF SGP record(s): recordlist,…**

An error occurred during maintenance of at least one Secondary Authid record and the user will need to examine this list of records and provide appropriate maintenance based upon the type of transaction that occurred.

**LDP0144E F ACF2,NEWXREF failed and manual maintenance required for XREF SGP record(s): recordlist,…**

This is similar to the message above, but the refresh command failed also. Take appropriate action against the list of Secondary Authids and issue a F ACF2,NEWXREF command when completed.

**LDP0145E F ACF2,NEWXREF failed.**

The F ACF2,NEWXREF command failed and needs to be issued manually.

## TSO Alias Support

The ACF2 Connector also supports the creation of a TSO Alias when a user is created or modified with TSO access being granted. The alias value is always the value of the ACF2 Account being created or modified. To enable this support, see the chapter titled, "CAACF2 DN Backend" in the *CA LDAP Server for z/OS Administrator Guide*, for more information.

## ACF2 Program Exits

The CA ACF2 Connector supports the use of Program Exits which are incorporated as Common Exits. Program Exits provide you with the capability to perform certain actions before or after an account is created, modified or deleted from CA IdentityMinder. These exits are referenced either on the Endpoint property page to execute custom code on a single endpoint, or on the Account Template property page to execute custom code on multiple endpoints. Actions might include native CA DSI (CA Distributed Security Integration) or CA LDAP Server for z/OS commands in order to modify account privileges or access to resources on the CA ACF2 system.

To see a sample program exit, refer to *PS_HOME*\Templates\OS390Exits.

For more detailed information about how to write program exits, see the *Programming Guide for Provisioning*.

## Proxy Configuration

The CA ACF2 Endpoint page contains a section where clients can configure a Proxy administrative ID and password to be used for user password changes from the SAWI. When configured, this ID and password is used to issue the password change request for the Self-Service user to change their password. This is helpful and needed if a Self-Service user cannot supply a password (for example, the password is forgotten) or their password is expired on ACF2 and they cannot be authenticated. When using a proxy administrative ID, standard ACF2 security rules apply (for example, scoping) and password syntax checking specified in the GSO Pswd Record is enforced. However, the ACF2 mindays value for the user is not enforced since the password change is done through an administrator.

**Note:** The check boxes on the Endpoints Setting tab are for legacy purposes only. You can perform proxy configuration and administration support from the Self-Service interface.

## Proxy Administration Support

You can configure a proxy ID for all tasks accomplished within CA IdentityMinder. Previously, a proxy ID could only be configured for use with requests generated from the SAWI interface. This proxy ID is maintained on the main Endpoint page in the Proxy Administration Configuration section. The proxy ID can be used for any type of CA IdentityMinder request against supported objects, and for any CA IdentityMinder Administrator that is logged on.

**Note:** The enhancement is only recommended to use after careful consideration (and preparation) of the following consequences:

1. Any Global User (with the proper privileges provided within CA IdentityMinder) is able to administer ACF2 Logonids and Rules under the configured proxy ID. Any mainframe security product scoping is lost; only the scoping of the proxy ID is enforced.
2. As mentioned above, security settings are now the only point of enforcement against a Global User manipulating mainframe security data.
3. Any reports or auditing methods against administration of your mainframe security data that originate from the mainframe is now compromised; the only ID that shows up for any administration that occurred from CA IdentityMinder is the configured proxy ID.
4. If the proxy ID's password changes on the mainframe, the password must be changed on every Endpoint Page within CA IdentityMinder that it is configured for.

By default, the Connector operates in the same mode as in past releases; the logged-on Global User and their password are used for submitting any requests destined to the mainframe security product. The common directory page entitled Endpoint Settings provides two checkbox controls under the description Administrator Credentials that control the three possible settings:

**Use logged-in Administrator's credentials**

Default setting. Indicates that the logged-in Administrator (Global User) is used as the credentials for ALL requests, even from the SAWI.

**Use proxy for SAWI changes**

Indicates that the logged-in Administrator (Global User) is used as the credentials for all requests EXCEPT for requests from the SAWI interface. The proxy ID credentials (if available) are used for requests coming from the SAWI interface.

**Use proxy for ALL requests**

When no checkbox is checked, this indicates that the proxy ID credentials (if available) are to be used for ALL requests.

When any request occurs from CA IdentityMinder, these settings are checked against the endpoint where the request is targeted. If, based on the endpoint settings and the type of request (SAWI or otherwise), proxy credentials are to be used, the credentials that are defined for that endpoint are retrieved and used for the request. In the case where endpoint credentials are supposed to be used, but no credentials exist (either Proxy ID or password contains no value), the proxy credentials are not used for the request and the request proceeds using the logged-in Administrator (Global User) credentials.

**Note:** The check boxes on this tab are for legacy purposes only. You can perform proxy configuration and administration support from the Self-Service interface.

## Conventions

Use the following CA-ACF2 conventions in your etautil commands:

- The endpoint type name (eTNamespaceName) is CA-ACF2
- The endpoint type prefix is ACF. Therefore, the CA-ACF2 class names are:
  - eTACFDirectory for an endpoint
  - eTACFPolicyContainer for an account template container
  - eTACFPolicy for an account template

## LDAP Directory Services (LDS)

CA-ACF2 provides the ability to synchronize z/OS security information management with LDAP compliant directory managed servers. The LDS component of the CA-ACF2 system sends requests through LDAP commands to the Provisioning service and is directed to the LDS backend that is located on a Windows based PC.

The module that handles LDS processing within CA IdentityMinder is named back_lds.dll (dynamic link library) and is intended to augment the functionality provided within CA IdentityMinder and the CA ACF2 Security product. The CA IdentityMinder LDS backend allows the user of the CA ACF2 for z/OS the ability to interface directly with the CA IdentityMinder database.

When a command is issued on the CA ACF2 system to add a user, a Global User is created in the local CA IdentityMinder database with the specified password. Additionally, if the user is to be associated with a Provisioning Role, the CA IdentityMinder inclusion will be generated to associate this user with the desired provisioning role(s).

When a command is issued to the CA ACF2 system to change the password, or any other mapped field of a user, a change results in the local CA IdentityMinder database and optionally is propagated to all necessary platforms.

When a command is issued to the CA ACF2 system to delete a user, the Global User is deleted from the local CA IdentityMinder database and any associated inclusions are removed. Depending upon the platform and CA IdentityMinder settings, this may also result in the deletion of accounts on other platforms.

## LDS Features

The LDS backend within CA IdentityMinder provides special processing when any of the following LDAP attributes are mapped to respective CA ACF2 fields in the LDS XREF field mapping:

- If LDAP attribute eTS390Role is specified as part of the command, the user is attached or removed from the specified Provisioning Role value. This may result in the addition or removal of accounts on any platform depending upon the Account Templates attached to that Provisioning Role. Typically, this attribute is mapped to a single-valued, user-defined field containing a comma-separated list of Provisioning Roles of which the user is a member.
- If the CA ACF2 password is mapped to the eTS390Password attribute, the password is applied to the Global User and automatically propagated to all accounts associated with that Global User.

  **Note:** This attribute should only be used by clients that do **NOT** explore/correlate their ACF accounts into CA IdentityMinder. Clients that do run explore/correlates should follow the instructions in the Password Synchronization feature bulletin.
- Password Synchronization - Password changes to ACF2 Loginids can be propagated into CA IdentityMinder to change a Global User's password and all accounts associated with the Global User. To accomplish this, an LDS record must be manually created (not from the LDS wizard) using the instructions from the Configuration and Usage section with the following changes:
  - Step 3: Set the USERDNS (user dns) as follows:

    ```
    eTACFLidName=%L,eTACFLidContainerName=Accounts,
    eTACFDirectoryName=www,
    eTNamespaceName=CA-ACF2,dc=XXX,dc=eta
    ```

    where eTACFDirectoryName=www equals the CA ACF2 Endpoint name and dc=XXX is the name of the CA IdentityMinder domain for this LDAP node. The case of the domain name should be as it exists in CA IdentityMinder.
  - Step 4: Set the OBJCLASS (object class) to eTACFLid
  - Step 6: In the XREF section, add the entry: Password/eTSyncPassword
- If the CA ACF2 password is mapped to the eTPassword attribute, this causes the password to only be applied to the Global User with no propagation to other accounts.
- If LDAP attribute eTS390Profile is specified as part of the command, the user is attached or removed from the specified Role value. This may result in the addition or removal of accounts on any platform depending upon the Account Templates attached to that Provisioning Role.

  **Note:** Values specified for both eTS390Profile and eTS390Role must exist within CA IdentityMinder as valid Provisioning Role names.

## Configuration and Usage

In order to configure your CA ACF2 system to drive requests through LDS to your Provisioning service, we recommend that you use the LDS Wizard provided within CA IdentityMinder on the Endpoint property page, to create or modify the LDS record on your ACF2 system. This wizard is only active and usable if the appropriate version of ACF2 is running, which supports LDS.

**Note:** For CA IdentityMinder users, you should only run this wizard from the Provisioning Manager.

If you choose not to use the wizard, then you must perform the following steps on the LDS record to invoke the LDS backend. For detailed information on LDS and setting up the LDS record, see the CA ACF2 Administrator Guide.

1. Sign on to the mainframe CA ACF2 system and create an LDS LDAP control record with the INSERT command. Set the ADMDN (admin dn) as follows:

   ```
   eTGlobalUserName=<user>,eTGlobalUserContainerName=Global Users,
   eTNamespaceName=CommonObjects,dc=XXX,dc=eta
   ```

   where eTGlobalUserName is the name of a CA IdentityMinder global user that has full authority to the domain (DomainAdministrator). dc=XXX is the name of the CA IdentityMinder domain for this LDAP node. The case for the domain name should be as it exists in CA IdentityMinder.

2. Set the ADMPSWD (admin password) to the correct password for the CA IdentityMinder global user.

3. Set the USERDNS (user dns) as follows:

   ```
   eTACFLidName=%L,eTACFLidContainerName=Accounts,
    eTACFDirectoryName-www,
    eTNamespaceName=CA-ACF2,dc=XXX,dc=eta
   ```

   where eTACFDirectoryName=www equals the CA ACF2 directoryname and dc=XXX is the name of the CA IdentityMinder domain for this LDAP node. The case for the domain name should be as it exists in CA IdentityMinder.

4. Set the OBJCLASS (object class) to eTGlobalUser.

5. Set the URL (uniform resource locator) to the machine name or IP address that is running the Provisioning service. Make sure that this URL contains the correct port. 20389 is used in the following example:

   ```
   LDAP://machine.ca.com:20389
   ```

6. Add the appropriate XREF mappings between ACF2 fields and LDAP attributes as required.

7. Refresh LDS by issuing the following commands:

   ```
   F ACF2,REFRESH(LDAP),TYPE(LDS)
   ```

8. Confirm that LDS is started on the ACF2 system.

## Implement LDS Password Syncing

When implementing LDS password syncing from a mainframe endpoint, do the following on the Provisioning server.

This procedure uses the default installation path for both files. Use the path that is appropriate for your CA IdentityMinder installation.

**To implement LDS password syncing**

1. Navigate to the following directory:

   ```
   C:\Program Files\CA\Identity Manager\Provisioning Server\data\
   ```

2. Add the following statement to the etrust_admin.conf file

   ```
   include "C:\\Program Files\\CA\\Identity Manager\\Provisioning
   Server\\data\\etrust_lds.conf "
   ```

3. Save the file and restart the Provisioning services.

## Attributes That Are Marked "Interesting To Compliance"

Most of the attributes that are marked "Interesting to Compliance" are Boolean. When you import into CA GovernanceMinder, only those with the value of TRUE are imported. Any attributes which are set to FALSE will not appear in your data.

The following attributes are marked "Interesting to Compliance", for use by CA GovernanceMinder:

- Account
- Audit
- Autodump
- Batch Job
- Bypass Label Processing
- CICS
- CMD Prop
- Consult
- IMS
- Leader
- Limited bypass label processing
- Non-cancel
- Prefix
- ReadAll
- Restrict
- RSRC Vld
- Rulevld
- Security
- Started Task
- Store Rule
- Submit Authority (JCL)
- TSO
- Tso Trace

These attributes can be found on the MVS Privileges 1, MVS Privileges 2, and MVS TSO 2 tabs.

# Extend the Schema to Include Custom Attributes

When you connect to a CA ACF2 system through CA IAM CS, you can correlate on any of the attributes are exposed by the connector. If you want to correlate on an attribute that the connector does not expose, you can extend the connector's schema to include up to twenty extra attributes.

To set up these extra attributes:

1. Create a mapping file that maps each attribute on the endpoint to an attribute in CA IdentityMinder (see page 103).

   This includes the custom attributes in the Provisioning Server.

2. Add the custom attributes to a new tab in the User Console. (see page 105)

## Create a Mapping File for the Custom Attributes

The mapping file lists the custom attributes.

**Note:** This section refers to the Provisioning Server installation location as *ps_install*. By default, *ps_install* is in the following locations:

- **Windows**—C:\Program Files (x86)\CA\Identity Manager\Provisioning Server
- **Linux and Solaris**—/opt/CA/IdentityManager/ProvisioningServer/

**Follow these steps:**

1. Create a new directory in *ps_install*\data, and name the new directory *ACF*.
2. Create a text file named schema_map.txt and save it in *ps_install*\data\ACF.
3. In the text file, create entries with the format described in Format of the Mapping File for Custom Attributes (see page 104).
4. Restart the Provisioning Server service.

The Provisioning Server now includes the custom attributes.

## Format of the Mapping File for Custom Attributes

The mapping file contains a list of the custom attributes, each with the following format:

```
eTACFCustomAttribute001=attribute1
eTACFCustomAttribute002=attribute2
…
eTACFCustomAttribute020=attribute20
```

In this list, the names on the left are the attributes in CA IdentityMinder and the names on the right are the attributes on the endpoint.

Each custom attribute in CA IdentityMinder is named eTACFCustomAttributeNNN, where NNN is a number from 001 to 020. You can use these names in any order, but we recommend that you start with eTACFCustomAttribute001, to avoid confusion.

There must be no spaces before or after each attribute name.

The attribute names are case-sensitive.

On Solaris, make sure the mapping file is world-readable (its permission should be at least 444).

## Add the Custom Attributes to a Tab in the User Console

You can include the custom attributes in a tab in the User Console.

**Follow these steps:**

1. Log in to the User Console as a user with administrative rights.
2. Click the Roles and Tasks tab, then click Admin Tasks, Manage Admin Tasks.
3. Search for *ACF2*.
4. Click on the name of the screen that you want to change, for example *Modify CA ACF2 Account*.
5. Select Tabs.
6. Find Custom Attributes in the table, and click its Edit button.
7. Select the Browse button beside the Screen field.
8. Select “Modify CA ACF2 Account – Custom Attributes”. Click Copy.
9. Give the new screen a unique name by editing the Name and Tag values.
10. Delete any Custom Attribute fields that should not appear on the final screen.
11. For each custom attribute, change its name to the actual attribute name on the endpoint:
    a. Click the attribute's Edit icon.
    b. Edit the Name to show the attribute's real name on the endpoint. This will appear on the final screen
    c. Edit the Tag to be unique. This is usually the same as the Name, but with no spaces.
12. Click OK.
13. Click Select.
14. Click OK, then click Submit.

The new tab is now available in the User Console.

## Cannot Create Account When Password Policies Conflict

This section applies to all connectors. However, it is most likely to be relevant to the mainframe connectors.

**Symptom:**

In many organizations, some endpoints (such as the mainframe systems) have stricter restrictions on passwords than the corporate password policy.

This conflict causes problems if you create a password that meets the requirements of the CA IdentityMinder password policy but is invalid on an endpoint. In this situation, the following problems can occur:

- When you use a provisioning role to create an endpoint account for an existing global user with such a password, the account is not created.
- When you attempt to create a new user with a temporary password, the user is not created.
- When you change the password of an existing account on the endpoint, the changed password is not saved.

**Solution:**

To avoid this problem, make one or both of the following changes:

- Make the password policy in CA IdentityMinder more restrictive than the password policy on the mainframe endpoint.
- Make the policy for temporary passwords more restrictive than the password policy on the mainframe endpoint.

  This change forces new users to change their password when they log in to User Console.

# CA Arcot Connector

After you have set up a connection to a CA Arcot WebFort endpoint, you can use CA IdentityMinder to do the following tasks:

- Create, view, and modify WebFort users
- Create, view, and modify OTP, ArcotID, and QnA credentials
- View and modify ArcotOTP credentials

**Note:** You cannot use CA IdentityMinder to create ArcotOTP credentials.

After you have set up a connection to CA Arcot RegFort, you can use CA IdentityMinder to do the following tasks:

- Create certificate provisioning tasks for Arcot users directly or using an account template
- Invalidate any pending certificate provisioning tasks of an Arcot user
- View pending and completed certificate provisioning tasks
- List the certificates that have been issued for an Arcot user, and the status of those certificates
- Manage each certificate through its lifecycle. For example:

  a. Create Certificate Provisioning Tasks (CPTs) to generate certificates for a new employee’s smartcard

  b. When the CPT completed or the certificate is downloaded to the smartcard, the Life Cycle Management (LCM) shows that the certificate is ACTIVE.

  c. When the validity of the certificate is finished, the certificate's status changes to EXPIRED.

  d. If the employee resigns, then you can use the LCM action REVOKE, which changes the certificate's status to REVOKED.

**Note**: To see a list of supported objects and attributes, or to download the endpoint guide for CA Arcot, see the Download page for Endpoint Guides for CA IdentityMinder.

# Embedded Entitlements Manager Connector

The Embedded Entitlement Manager (EEM) Connector lets you create management interfaces for EEM servers and provides a single point for all user administration by letting you do the following:

- Administer two types of EEM applications: the built-in "Global" application and the user-defined application
- Add accounts and account containers to any level of the tree
- Delete accounts and account containers from any level of the tree
- Modify and search accounts from any level of the tree
- Add groups to the accounts
- Modify user attributes for accounts in user-defined applications
- Create, search, modify, and delete access policies
- Create, search, modify, and delete calendars
- Add, search, and delete groups
- Search resource classes

**Note**: Only Provisioning manager can be used in order to manage EEM connector.

The EEEM Connector supports multiple, simultaneous connections to different EEM servers and multiple applications on the same server.

**Note:** The EEM Connector refers to the EIAM Connector for this release.

## EEM Installation

This connector is managed using the Connector and C++ Server installation process.

**Note:** For more information and requirements, see *Connector and C++ Connector Server Installation.*

## EEM Support for FIPS and IPv6

The Embedded Entitlements Manager Connector does not support FIPs or IPv6.

## Connector-Specific Features

This section details your connector's specific management features, such as how to acquire and explore your endpoint. Also included are account, provisioning roles, account template, and group information specifically for your connector.

## Acquire an EEM Server Machine

You must acquire the EEM server machine before you can administer it with CA IdentityMinder.

**From the Endpoint Type task view**

1. Register the machine as an endpoint in CA IdentityMinder.

   Use the EEM Endpoint property sheet to register an EEM server machine. During the registration process, CA IdentityMinder identifies the EEM server machine you want to administer and gathers information about it.

   Then choose the application name and specify the name and password for the management account that has been configured on the EEM Backend Server.

2. Explore the accounts that exist on the endpoint.

   After registering the machine in CA IdentityMinder, you can explore its accounts. Use the Explore and Correlate Endpoint dialog. The Exploration process finds all EEM accounts. You can correlate the accounts with global users at this time, or you can wait to correlate them.

3. Correlate the explored accounts with global users.

   When you correlate accounts, CA IdentityMinder creates or links the accounts on an endpoint with global users, as follows:

   a. CA IdentityMinder attempts to match the username with each existing global user name. If a match is found, CA IdentityMinder associates the EEM account with the global user. If a match is not found, CA IdentityMinder performs the next step.

   b. CA IdentityMinder attempts to match the account name with each existing global user's full name. If a match is found, CA IdentityMinder associates the EEM account with the global user. If a match is not found, CA IdentityMinder performs the next step.

   c. If the Create Global Users as Needed button is checked, CA IdentityMinder creates a new global user and associates the EEM account with the global user. If the Create Global Users as Needed button is unchecked, then CA IdentityMinder performs the next step.

   d. CA IdentityMinder associates the EEM account with the [default user] object.

## EEM Account Templates

The EEM Connector account template can be associated with two types of EEM applications, (build-in and user-defined). If the associated directory is the Global application, the "Application Properties tab in the account template is disabled, whereas, the Global Properties tab is disabled for user-defined application directories.

Since the Connector is a hierarchical Endpoint Type, the account container must be specified for the account template in order to create accounts in the right place.

### Global and Application Endpoints are Managed Separately

No accounts can be added to the build-in Global application endpoint when adding accounts to user-defined application endpoints and conversely the opposite applies. You can now view which endpoint the accounts are being associated to on the Account Template Property Sheet.

## EEM Accounts

When creating application users using the EEM Web User Interface (not recommended), all users will be created under the root folder regardless of what folder is specified, although the Web User Interface appears to display the user with the correct path. This indicates that such application users created using the EEM Web User Interface will all appear under the "EEM Accounts" container after exploration in the Provisioning Manager.

If you use CA IdentityMinder or Safex to create users, all users will be created in the correct folders or they will be displayed correctly after an exploration.

## EEM Access Policies

You can create and maintain EEM access policies using the Endpoint Type task view. Use the EEM Access Policies property sheet when defining and managing your access policies.

Any changes made in this object using native tools are kept in sync with the views in the Provisioning Server without requiring a re-exploration.

## EEM Calendars

Calendars define dates and times that users can access system functions. Use the EEM Calendars property sheet to set user access times.

Any changes made in this object using native tools are kept in sync with the views in the Provisioning Server without requiring a re-exploration.

## EEM Groups

You can create and maintain EEM groups using the Endpoint Type task view. Use the EEM Group property sheet when managing your groups.

Any changes made in this object using native tools are kept in sync with the views in the Provisioning Server without requiring a re-exploration.

### Available Groups in Account Template Property Sheet

You can now view and choose from all the available groups, where to add group members to an account template.

## EEM Resource Classes

You can view the resource classes for the EEM server.

# CA DLP Connector

The CA DLP Connector provides a single point for CA DLP account administration. The connector lets you administer account objects on CA DLP endpoints.

You can use the CA DLP Connector to:

- Acquire CA DLP endpoints
- Explore CA DLP endpoints for existing accounts
- Create, update, or delete CA DLP accounts
- Move a CA DLP user to a different location in the CA DLP hierarchy

## CA DLP Connector Management

The CA DLP Connector is managed using the CA IdentityMinder User Console.

## FIPS 140 Configuration

CA IAM CS and CA DLP CMS (Central Management Server) must be in the same FIPS 140 mode before CA IAM CS can use the CA DLP Connector to manage a CA DLP endpoint.

The following table shows the supported configuration modes for CA IAM CS and CA DLP CMS.

| CA IAM CS | CA DLP CMS | Supported | Connection Type |
|---|---|---|---|
| FIPS 140 Mode | FIPS 140 Mode | Yes | TLS |
| Non-FIPS 140 Mode | Non-FIPS 140 Mode | Yes | Unauthenticated SSL |
| FIPS 140 Mode | Non-FIPS 140 Mode | No | N/A |
| Non-FIPS 140 mode | FIPS 140 Mode | No | N/A |

The CA DLP Connector detects whether CA IAM CS is running in FIPS 140 mode, and configures itself to communicate with the CA DLP endpoint using a FIPS 140 encrypted connection.

If CA IAM CS and CA DLP CMS are both running in FIPS mode, you must install certificates that the CA DLP CMS trusts on CA IAM CS. The certificates are stored in a keystore, copied from the CA DLP CMS.

If CA IAM CS and CA DLP CMS are both running in non-FIPS 140 mode, the CA DLP CMS uses unauthenticated SSL and a CA DLP keystore file is not required.

## Enable Communication Between CA IAM CS and CA DLP In FIPS 140 Mode

To enable communication between CA IAM CS and CA DLP CMS in FIPS 140 mode, CA IAM CS must be installed with FIPS 140 mode enabled and the CA DLP CMS must be deployed in Advanced Encryption Mode.

To enable communication in FIPS 140 mode, copy the CA DLP keystore to CA IAM CS configuration directory.

**Note:** For more information on FIPS 140 mode, see FIPS 140-2 Compliance in the *Configuration Guide*. For more information about how to deploy CA DLP in Advanced Encryption Mode, see the *CA DLP Deployment Guide*.

**Follow these steps:**

1. Verify that the CA DLP CMS is in Advanced Encryption Mode. Do the following:

   a. Start the CA DLP Administration console.

   b. Verify that the activity log contains a message similar to one of the following:

   ```
   I0100     JCE Provider CRYPTOJ 4.0 20071129 1450: Standard
   mode.
   I00FE     JCE Provider CRYPTOJ 4.0 20071129 1450: Advanced mode
   startup tests ran successfully
   ```

   If the most recent message starts with id I0100, the CA DLP CMS is deployed in standard mode and is not in FIPS 140 mode. You must configure the CA DLP CMS to use FIPS 140 mode before you can enable FIPS 140 mode for CA IAM CS.

   If the most recent message starts with id I01FE, the CA DLP CMS is deployed in Advanced Encryption mode, and the CA DLP CMS is deployed in FIPS 140 mode.

2. On the computer used to create certificates for use by CA DLP, navigate to the following folder:

   ```
   C:\FIPS\AdvancedEncryption\output
   ```

3. Copy the keystore.dat file to the following folder on the CA IAM CS computer:

   ```
   cs-home\conf
   ```

4. Rename the keystore.dat file to dlp.ssl.keystore.

5. Restart CA IAM CS.

   CA IAM CS is now in FIPS 140 mode and can use the CA DLP connector to manage the CA DLP CMS endpoint.

## Generate a New Keystore

When the keystore.dat file on the CA DLP CMS changes or is compromised, generate a new keystore file so that CA IAM CS and CA DLP CMS can communicate in FIPS 140 mode.

**To generate a new keystore**

1. On the CA DLP CMS, revoke the current CA DLP keystore.
2. On the CA DLP CMS, install the new keystore.
3. On the computer used to create certificates for use by CA DLP, navigate to the following folder:

   C:\FIPS\AdvancedEncryption\output
4. Copy the keystore.dat file to the following folder on the CA IAM CS computer:

   *CS_HOME*\conf
5. Rename the keystore.dat file to dlp.ssl.keystore.
6. Restart CA IAM CS.

   CA IAM CS is now in FIPS 140 mode and you can now use the CA DLP connector to manage the DLP CMS endpoint.

   **Note:** For information about revoking and generating a keystore, see the *CA DLP Deployment Guide*.

# Connector Specific Features

This section details the management features of your connector, including account, group, and least privilege information for your connector.

## How to Rename CA DLP Connector User Attributes

CA DLP Connector account management screens use the labels User Attribute 1 – User Attribute 10 by default on the User Attributes 1 and User Attributes 2 tabs in the CA IdentityMinder User Console.

If you rename user attributes in your CA DLP environment, we recommend that you also rename the corresponding user attributes in the CA DLP Connector account management screens. Using identical attribute names in your CA DLP environment and the CA DLP Connector account management screens makes administration easier.

For example, if you rename User Attribute 1 to City in your CA DLP environment, you can change the name of User Attribute 1 to City in the CA DLP Connector account management screens. You can change the name of the user attribute by editing the metadata of the CA DLP Connector by using Connector Xpress.

To rename a user attribute in the CA DLP Connector account management screens, do the following:

1. Edit the metadata of the CA DLP Connector using Connector Xpress as follows:
   a. Create a Connector Xpress project based on the existing CA DLP Connector metadata.
   b. Rename the CA DLP Connector user attribute so that its name matches the corresponding user attribute in your CA DLP environment.

      **Important!** We recommend that you edit only the Name attribute in the CA DLP Connector metadata. Editing other attributes can make the CA DLP Connector inoperable.
   c. Redeploy the CA DLP Connector metadata to the provisioning server.
2. Generate the CA DLP account management screens, as follows:
   a. Use the Role Definition Generator to generate the CA_DLP.jar file.

      The CA_DLP.jar file contains the role, task, and screen definitions for the CA DLP account management screens in the CA IdentityMinder User Console.
   b. Import the CA_DLP.jar file into the CA IdentityMinder User Console.

### Example: Edit the metadata of the CA DLP Connector using Connector Xpress

The following example shows you how to rename a CA DLP user attribute on the CA DLP account management screen so that it matches the name of the corresponding attribute in your CA DLP environment. You rename the attribute by using Connector Xpress to edit the CA DLP Connector metadata. This example assumes that you have changed the name of the User 1 Attribute in your CA DLP environment to City.

This example shows you how to change the name of User Attribute 1 to City on the User Attribute 1 tab in the CA IdentityMinder User Console.

**To edit the metadata of the CA DLP Connector using Connector Xpress**

1. Start Connector Xpress.
2. If necessary, add and configure the provisioning server that manages the CA DLP Connector.
3. In the Provisioning Servers tree, navigate to your CA DLP endpoint.
4. Right-click the CA DLP endpoint, then click Create a Project.

   Connector Xpress creates a project based on the existing CA DLP Connector metadata.
5. In the Mapping Tree, expand the Classes Node, expand the eTDYNAccount node, then expand the Attributes node.
6. Click the User Attribute 1 node.

   The Attribute Details dialog appears.
7. In the Name field, change the name of the attribute to City.
8. In the Provisioning Servers tree, navigate to your CA DLP endpoint.
9. Right-click the CA DLP endpoint, then Click Deploy Metadata.

   The Deploy Metadata dialog appears.
10. When prompted, increase the version number of the CA DLP Connector and confirm that you want to deploy the new metadata to the provisioning server.

    Connector Xpress deploys the CA DLP Connector metadata to the provisioning server.

    Next, use the Role Definition Generator to generate the CA DLP account management screens.

**Note:** For more information about how to add and configure a provisioning server, create a Connector Xpress project, and generate CA IdentityMinder User Console account management screens, see the *Connector Xpress Guide*.

### Example: Generate CA DLP account management screens using the Role Definition Generator

This example shows you how to use the Role Definition Generator to generate the CA_DLP.jar file and how to import it into the CA IdentityMinder User Console to generate DLP account management screens. This example uses a provisioning server named myProvisioningServer, with administrator login name AdminLogin for a CA DLP endpoint named CA DLP.

This example assumes that you have edited the metadata of the CA DLP Connector using Connector Xpress and renamed User Attribute 1 to City.

**Note:** For more information about how to use the Role Definition Generator, see *How you Generate CA IdentityMinder User Console Account Screens* in the *Connector Xpress Guide*.

**To generate CA DLP account management screens using the Role Definition Generator**

1. On the computer where you installed CA IdentityMinder, stop the CA IdentityMinder Server.
2. Navigate to the following folder:
   `<jboss_home>\server\default\deploy\iam_im.ear\user_console.war\WEB-INF\lib`
3. Back up the current CA_DLP.jar file.

   Making a backup of the CA_DLP.jar file allows you to restore the previous version of the CA DLP Connector metadata and revert to the previous version of the CA DLP account management screens, if necessary.
4. Navigate to one of the following directories according to your operating system:
   - (Windows) *<identity manager_HOME>*\tools\RoleDefinitionGenerator\bin
   - (UNIX) *<identity manager_HOME>/* tools/RoleDefinitionGenerator/bin
5. Open a Command Prompt window or a terminal window according to your operating system, then enter one of the following commands:
   - (Windows) RoleDefGenerator.bat -d *exampledomain* –h *im.example.com* -p *port*–u *adminusername* EndpointType
   - (UNIX) RoleDefGenerator.sh -d *exampledomain* –h *im.exmaple.com* –p *port* –u *adminusername* EndpointType

   For example:

   ```
   RoleDefGenerator.bat -d im -h myProvisioningServer -p myport -u Adminlogin "CA DLP"
   ```

   When prompted, enter the provisioning server password.

   The Role Definition Generator creates the CA_DLP.jar file and puts it in the following folder by default:
   `<identity manager_home>\RoleDefinitionGenerator\bin`

   **Note:** For more information about the Role Definition Command, see the *Connector Xpress Guide.*
6. Copy the CA_DLP.jar that you generated to the following folder:
   `<jboss_home>server\default\deploy\iam_im.ear\user_console.war\WEB-INF\lib`
7. Restart the CA IdentityMinder Server.

   CA IdentityMinder loads the new role, screen, and task definitions for the CA DLP account management screens.
8. Start the CA IdentityMinder Management Console.
9. Click Environments, then click the environment that you want to change.

The Environment Properties page appears.

10. Click Role and Task Settings, then click Import.

    CA IdentityMinder displays the currently installed version of the CA DLP metadata in the Installed Version column. The version of the CA DLP Connector metadata that you deployed to the Provisioning Server in Step 6 appears in the Version column.

11. In the Name column, select the check box next to CA_DLP, then click Finish.

    CA IdentityMinder deploys the role definitions, screens, tasks, and roles for the CA DLP Connector and updates the CA IdentityMinder environment you selected.

12. Click Continue, then click Restart Environment.

13. Start the CA IdentityMinder User Console.

14. Verify that CA IdentityMinder has renamed the User Attribute 1 field to City, as follows:

    a. In the CA IdentityMinder User Console, view the CA DLP account of a user.

    b. Click the User Attributes 1 Tab.

    c. Verify that CA IdentityMinder has renamed the User Attribute 1 field to City.

## How to Create Custom User Categories

CA DLP Connector account management screens display the same user categories used in CA DLP by default. For example, Administrator, Manager, User, Policy Administrator, and Reviewer.

CA DLP supports the addition of new user categories. If you add a user category in your CA DLP environment, we recommend that you also add the new user category to the CA DLP Connector account management screens. Adding user categories to the CA DLP Connector account management screens to match the user categories on your CA DLP endpoint makes administration easier.

For example, if you add a user category named Assistant Manager to your CA DLP environment, you can add a user category attribute named Assistant Manager to the CA DLP Connector account management screens.

You can add the new user category attribute by using Connector Xpress to edit the metadata of the CA DLP Connector.

To create a custom user category on the CA DLP Connector Account tab in the CA IdentityMinder User Console account management screens, do the following:

1. Edit the metadata of the CA DLP Connector using Connector Xpress as follows:
   a. Create a Connector Xpress project based on the existing CA DLP Connector metadata.
   b. In Connector Xpress, add the same User Category attribute that you added to the CA DLP endpoint.
   c. Redeploy the CA DLP Connector metadata to the provisioning server.

      **Important!** We recommend that you edit only the DLPUserCategory attribute in the CA DLP Connector metadata. Editing other attributes can make the CA DLP Connector inoperable.
   d. Redeploy the CA DLP Connector metadata to the provisioning server.
2. Generate the DLP account management screens, as follows:
   a. Use the Role Definition Generator to generate the CA_DLP.jar file.

      The CA_DLP.jar file contains the role, task, and screen definitions for the DLP account management screens in the CA IdentityMinder User Console.
   b. Import the CA_DLP.jar file into the CA IdentityMinder User Console.

### Example: Edit the metadata of the CA DLP Connector using Connector Xpress

The following example shows you how to add a CA DLP user category attribute named Assistant Manager to the CA DLP account management screen. You add the attribute by using Connector Xpress to edit the CA DLP Connector metadata. This example assumes that you have added a user category named Assistant Manager to your CA DLP environment.

This example shows you how to add a user category named Assistant Manager to the Account Management tab in the CA IdentityMinder User Console.

**To edit the metadata of the CA DLP Connector using Connector Xpress**

1. Start Connector Xpress.
2. If necessary, add and configure the provisioning server that manages the CA DLP Connector.
3. In the Provisioning Servers tree, navigate to your CA DLP endpoint.
4. Right-click the CA DLP endpoint, then click Create a Project.

   Connector Xpress creates a project based on the existing CA DLP Connector metadata.
5. In the Mapping Tree, click the Custom Types node.

   The Custom Types dialog appears.
6. Under Enumerated Types, click DLPUserCatergory.
7. In the Values list, click Add, then enter the following:

   **Value**

   Defines the value of the enumerated type used on the endpoint system.

   **Example:** Assistant Manager

   **Display Name**

   (Optional) Defines the name of the enumerated type displayed in the CA IdentityMinder User Console.

   **Example:** Assistant Manager

   **Ordinal**

   (Optional) Defines the order of the enumerated values.

   **Example:** 2
8. In the Provisioning Servers tree, navigate to your CA DLP endpoint.
9. Right-click the CA DLP endpoint, then click Deploy Metadata.

   The Deploy Metadata dialog appears.
10. When prompted, increase the version number of the CA DLP Connector and confirm that you want to deploy the new metadata to the provisioning server.

    Connector Xpress deploys the CA DLP Connector metadata to the provisioning server.

    Next, use the Role Definition Generator to generate the CA DLP account management screens.

**Note:** For more information about how to add and configure a provisioning server, create a Connector Xpress project, and generate CA IdentityMinder User Console account management screens, see the *Connector Xpress Guide*.

### Example: Generate CA DLP account management screens using the Role Definition Generator

This example shows you how to use the Role Definition Generator to generate the CA_DLP.jar file and how to import it into the CA IdentityMinder User Console to generate DLP account management screens. This example uses a provisioning server named myProvisioningServer, with administrator login name AdminLogin for a CA DLP endpoint named CA DLP.

This example assumes that you have edited the metadata of the CA DLP Connector using Connector Xpress and added a new user category named Assistant Manager to the CA DLP account management screens.

**Note:** For more information about how to use the Role Definition Generator, see *How you Generate CA IdentityMinder User Console Account Screens* in the *Connector Xpress Guide*.

**To generate DLP account management screens using the Role Definition Generator**

1. On the computer where you installed CA IdentityMinder, stop the CA IdentityMinder Server.
2. Navigate to the following folder:

   ```
   <jboss_home>\server\default\deploy\iam_im.ear\user_console.war\WEB-INF\lib
   ```
3. Back up the current CA_DLP.jar file.

   Making a backup of the CA_DLP.jar file allows you to restore the previous version of the CA DLP Connector metadata, and revert to the previous version of the DLP account management screens, if necessary.
4. Navigate to one of the following directories according to your operating system:
   - (Windows) *<identity manager_HOME>*\tools\RoleDefinitionGenerator\bin
   - (UNIX) *<identity manager_HOME>/* tools/RoleDefinitionGenerator/bin
5. Open a Command Prompt window or a terminal window according to your operating system, then enter one of the following commands:
   - (Windows) RoleDefGenerator.bat -d *exampledomain* –h *im.example.com* -p *port*–u *adminusername* EndpointType
   - (UNIX) RoleDefGenerator.sh -d *exampledomain* –h *im.exmaple.com* –p *port* –u *adminusername* EndpointType

   For example:

   ```
   RoleDefGenerator.bat -d im -h myProvisioningServer -p myport -u Adminlogin "CA
   DLP"
   ```

When prompted, enter the provisioning server password.

The Role Definition Generator creates the CA_DLP.jar file and puts it in the following folder by default:

```
<identity manager_home>\RoleDefinitionGenerator\bin
```

6. Copy the CA_DLP.jar that you generated to the following folder:
   `<jboss_home>\server\default\deploy\iam_im.ear\user_console.war\WEB-INF\lib`
7. Restart the CA IdentityMinder Server.

   CA IdentityMinder loads the new role, screen, and task definitions for the CA DLP account management screens.
8. Start the CA IdentityMinder Management Console.
9. Click Environments, then click the environment that you want to change.

   The Environment Properties page appears.
10. Click Role and Task Settings, then click Import.

    CA IdentityMinder displays the currently installed version of the DLP metadata in the Installed Version column. The version of the CA DLP Connector metadata that you deployed to the provisioning server in Step 6 appears in the Version column.
11. In the Name column, select the check box next to CA_DLP, then click Finish.

    CA IdentityMinder deploys the role definitions, screens, tasks, and roles for the CA DLP Connector and updates the CA IdentityMinder environment you selected.
12. Click Continue, then click Restart Environment.
13. Start the CA IdentityMinder User Console.
14. Verify that CA IdentityMinder has added the user category Assistant Manager to the CA DLP account management screens, as follows:

    a. In the CA IdentityMinder User Console, view the CA DLP default template

    b. Click the Account tab.

    c. Verify that CA IdentityMinder has added the new user category Assistant Manager.

## Least Privilege Considerations

To manage objects on a CA DLP endpoint using the CA DLP Connector, the administrator account that manages the CA DLP endpoint requires the following minimum permissions and privileges:

- User: Reset user passwords
- User: Edit the user hierarchy

In CA DLP, the administrator user category inherits these privileges by default, however you can configure other user categories to have these privileges.

**Note:** For more information, see the *CA DLP Deployment Guide*.

## Account Management

You can use the CA DLP Connector to view, create, modify, or delete an account.

## Account Suspension and Unlocking

The CA DLP Connector does not support account suspension and unlocking.

## Groups and Hierarchies

CA DLP maintains a user hierarchy. Groups can also contain users. The user hierarchy is built up dynamically as users are provisioned to CA DLP. Groups that contain users and other groups are typically built from the attributes belonging to users provisioned to CA DLP.

The CA DLP Connector does not display the CA DLP group hierarchy. However, you can use the CA DLP Connector to provision a user into a group or groups on the CA DLP endpoint.

The account template associated with a CA DLP endpoint lets you define a rule string that specifies the group hierarchy and the groups you want to provision the user to. The rule string is defined in the Groups field.

When you provision a user with the CA DLP Connector, CA DLP dynamically creates the groups and the group hierarchy based on the rule strings specified in the Group field on the CA IdentityMinder account template.

For example, specifying the following rule string *%COUNTRY%/%UC%/%UB%/%UL%* in the Group field groups users by country, city, building, and location on the CA DLP endpoint.

## Troubleshooting

### Unable to View or Modify CA DLP Accounts with Unicode or UTF-8 Characters in the User Console

**Symptom:**

I created a CA DLP account with Japanese or other non-English characters. When I try to view the account, I get an error message that starts with Not a valid IAM handle, and then contains unintelligible characters.

**Solution:**

The account was created in CA IdentityMinder, but it is not visible in the User Console. However, it is visible in the Provisioning Manager.To display CA DLP accounts created with non-English characters in the User Console, configure the JBoss server.xml file for UTF-8 encoding for URI.

**Note:** For information about configuring server.xml file for UTF-8 encoding for URI, see Change JBoss server.xml in the *User Console Design Guide*.

### Removal of Email Address from a CA DLP Account is Ignored

**Symptom:**

I am modifying a CA DLP account with more than one email address. When I try to remove one of the email address in the CA IdentityMinder User Console, the changes are applied, but the email address is not removed.

**Solution:**

Removal of an email address from a CA DLP account is not supported in the CA IdentityMinder User Console.

**Note:** Attempts to delete an email address from a CA DLP account in the CA IdentityMinder User Console are recorded in the logs, and include the reason for preventing the operation.

To remove an email address from a CA DLP account, use the CA DLP administrative tools.

**Important!** Deleting an email address from a DLP account can impair the event tracking and search capabilities of CA DLP.

# CA SSO Connector for Advanced Policy Server

The CA SSO Connector for Advanced Policy Server (PLS) is a Endpoint Type connector for CA IdentityMinder that lets you administer CA Single Sign-On, version 7.0 or higher. The CA SSO Connector for Advanced Policy Server provides a single point for all user administration by letting you do the following:

- Manage Endpoint, Account, Group, Terminal, Authentication Host, Application, Application Group and Account Template object classes.
- Create, modify, or delete an account or group in a user data store.
- Add accounts to a group, or remove them.
- Authorize an account or group to access selected applications and application groups.
- Administer passwords for the SSO and LDAP authentication methods.
- Administer login information for applications.
- Administer various pre-defined account and group properties, such as expiration date, suspension date, and resumption date.
- Administer date and time restrictions for Account, Account Template, and Terminal objects.
- Specify user attribute values for accounts in a user data store.
- Create, modify, or delete Terminal or Authentication Host objects in SSO endpoints
- Authorize users and groups to access Terminal or Authentication Host objects

**Note:** Terminal and Authentication Host classes are only available to be managed in the PLS Connector when the SSO servers are v8.0 and higher.

This connector is managed using the Connector and C++ Server installation process.

**Note:** For more information and requirements, see *Connector and C++ Connector Server Installation.*

## Configuring the CA Single Sign-On Server

Follow the steps below to configure your CA Single Sign-On server for CA IdentityMinder.

1. Start the selang command interpreter.
2. Create the system administrator's account on the CA Single Sign-On server if it does not already exist.
3. Enable the administrator's account to connect from the Provisioning Server.

## Create the System Administrator Account

Create the CA Single Sign-On administrator account on the CA Single Sign-On server. Add the admin and auditor keywords to the selang command to grant the correct privileges to the administrator. In selang, enter the following command:

```
nu administrator_name password(administrator_password) admin auditor
```

***administrator_name***

The user ID that the administrator uses to log on to the CA Single Sign-On Server.

***administrator_password***

The administrator password for the user ID.

**Note:** We recommend that you do **not** use a user ID named “Administrator” to define a CA Single Sign-On endpoint for Windows 2000.

Enter the following command to add *administrator_name* to the predefined group _ps-adms.

join *administrator_name* group(_ps-adms)

Enter the following commands to ensure the administrator account is created in the native operating system with the same password.

```
env(native)

eu administrator_name password(administrator_password)

env(seos)
```

## Enable the Administrator Account

Enter the following command to enable the CA Access Control and CA Single Sign-On authentication methods for the administrator.

```
eu administrator_name auth_type(method5, method20)
```

Enter the following command to set the CA SSO password for the administrator's account to the same password you specified in Step 1.

```
el administrator_name appl(__SSO__) currpwd(administrator_password)
```

Give the administrator access to the CA Single Sign-On server by issuing the following command.

```
auth terminal server_name uid(administrator_name) acc(access_type)
```

***server_name***

Is the machine name of the CA Single Sign-On Server.

***administrator_name***

Is the administrator's account.

***access_type***

Is the access that the administrator needs. Read and write access is necessary. The keywords for access_type are READ, WRITE.

## Using Failover

When using the PLS Connector to connect to a policy server farm, you can set up a failover system that automatically switches from a failed server to a running server to let you keep working without interruption. For large sites that use a policy server farm, failover can provide reliable and rapid service.

When discovering the SSO endpoint, the policy server that is to be the primary policy server must be provided. After the discovery, the Fail-Over property page in the Endpoint Property Sheet shows the policy server that was specified. You can then add more policy servers to the list. Once the policy servers have been added, they can be edited or even removed as needed.

The PLS Connector always tries to connect the first policy server in the list, so the order of the policy servers in the list is significant. If the connection fails to the first policy server then the PLS Connector tries connecting to the second policy server and so on. Once a connection is successfully made, PLS continues to work with the server. Every 60 seconds, PLS checks whether failed servers are available again.

**Note:** When changing the policy server list in the Fail-Over tab, the primary server, (for example, the first entry in the list) must be responsive for the changes to be accepted and applied.

## Enable Application Password Propagation

Currently, in an SSO endpoint, every SSO user record contains a login application and every login application record contains a username and password. This username and password does not have to be the same as the SSO username. For example:

```
SSOuser1 Username=Doe Password=Doe

        TelnetAppl1 Username=Doe1 Password=Doe1  (Unix Host Srv1)

        TelnetAppl2 Username=Doe2 Password=Doe2 (Unix Host Srv2
```

SSO has password synchronization. If you (or SSO) change the password from TelnetApp1, SSO also changes the password for TelnetApp2.

If you put CA IdentityMinder into this equation, Admin is able to do password synchronization and has an SSO Connector and a UNIX Connector. You now have the following scenario:

```
Global User=Doe

SSO User=Doe

        Inside SSO TelnetApp1 username=Doe, TelnetApp2 username=Doe

Unix User on Srv1=Doe

Unix User on Srv2=Doe
```

If you change the password for the global user Doe and propagate the password to all of the global user accounts, the password will change on the following Endpoint Types: SSO, Unix Srv1 and Unix Srv2. However, the password in the loginapplications (TelnetApp1, TelnetApp2, and so forth) for the SSO user will not be changed and those using SSO cannot use SSO to log into their applications anymore because the password stored in their loginappl record is out of sync.

To solve this problem, a master application, for example, eTrustIAM, can be defined and TelnetApp1 and TelnetApp2 can be set to use eTrustIAM as the master application. The PLS Connector can then update the password of the master application eTrustIAM when it receives the password propagation request caused by the CA IdentityMinder global user password change. As a result, the Policy Server updates the passwords for TelnetApp1 and TelnetApp2. Because the UNIX Connector updates the passwords for the user in both Unix Srv1 and Unix Srv2, and the PLS Connector updates the SSO password if the user uses the SSO authentication method, the passwords in all levels are in sync.

If you are using an older Policy Server version that does not have the eTrustIAM master application defined automatically after installation, do the following to use this feature:

- Using Policy Manager, create a master application "eTrustIAM" in the Policy Server and set _SSO_ as the master application.

- Like the _SSO_ application, the eTrustIAM application should be available for every user, so set the default access rights to EXECUTE. And, since the eTrustIAM application should not be shown in the SSO client, the access rights must also be set to HIDDEN.
- Set eTrustIAM as the master application for all applications where you want password propagation.

If you want to integrate admin applications (Provisioning Manager, IA Manager, and Self Service) with SSO, do the following to start these Admin applications through the SSO client:

1. Using Policy Manager, create SSO applications for each Admin application (Provisioning Manager, IA Manager, and so forth).
2. Set eTrustIAM as the master application for these SSO applications.
3. Create TCL scripts for each Admin application, (These are used to start the applications through SSO.), and put these TCL scripts in the following directory:

   ```
   eTrust Policy Server\Scripts
   ```

## PLS Support for FIPS and IPv6

For this release of CA IdentityMinder, the PLS Connector does not support FIPs or IPv6.

## Connector-Specific Features

This section details your connector's specific management features, such as how to acquire and explore your endpoint. Also included are account, provisioning roles, account template, and group information specifically for your connector.

## Acquire a CA Single Sign-On Server

You must acquire the CA Single Sign-On server before you can administer it with CA IdentityMinder. When acquiring an CA Single Sign-On server, perform the following steps from the Endpoint Type task view:

1. Register the server as an endpoint in CA IdentityMinder.

   Use the PLS Endpoint property sheet to register an CA Single Sign-On server. During the registration process, CA IdentityMinder identifies the CA Single Sign-On server you want to administer and gathers information about it.

   **Note:** Ping the node name from the Provisioning Server. If the ping is successful, then you know that CA IdentityMinder will find the PLS node.

2. Explore the objects that exist in the endpoint.

   After registering the server in CA IdentityMinder, you can explore its contents. Use the Explore and Correlate Endpoint dialog. The Exploration process finds all accounts and groups in the SSO server.. You can correlate the accounts with global users at this time or you can correlate them later.

3. Correlate the explored accounts with global users.

   When you correlate accounts, CA IdentityMinder creates or links the accounts on an endpoint with global users, as follows:

   a. CA IdentityMinder attempts to match the account name with each existing global user name. If a match is found, CA IdentityMinder associates the PLS account with the global user. If a match is not found, CA IdentityMinder performs the next step.

   b. CA IdentityMinder attempts to match the full name with each existing global user's full name. If a match is found, CA IdentityMinder associates the PLS account with the global user. If a match is not found, CA IdentityMinder performs the next step.

   c. If the Create Global Users as Needed button is checked, CA IdentityMinder creates a new global user and then associates the PLS account with the global user. If the Create Global Users as Needed button is unchecked, CA IdentityMinder performs the next step.

   d. CA IdentityMinder associates the PLS account with the [default user] object.

## Roles and Policies

In addition to defining privileges for users, you can also set login information for applications associated with account templates. Once this information is set, users have access to the applications if they provide the correct login information.

The PLS Default Policy, provided with the CA SSO Connector for Advanced Policy Server, gives a user the minimum security level needed to access an endpoint. You can use it as a model to create new account templates.

## PLS Control Applications

You can view certain basic properties of an application on the PLS Application property sheet.  You are not allowed to add, delete, or modify an application.

## PLS Control Application Groups

You can view certain basic properties of an application group on the PLS Application Group property sheet. You are not allowed to add, delete, or modify an application group.

## PLS Terminal

You can assign accounts and groups to access the current terminal objects. Use the PLS Terminal property sheet to set the profile, day/time restrictions, and account and group access to terminals.

## PLS Authorization Hosts

You can assign accounts and groups to access the current authorization host objects. Use the PLS Authhost property sheet to set the profile, and account and group access to authorization hosts.

# Frequently Asked Questions

This section is designed to help solve any problems that may occur and answer any questions you may have when using the CA SSO Option.

This section contains the following topics:

Policy Questions (see page 133)

Authentication Method Question (see page 134)

Buffer Size Question (see page 135)

Exploration Questions (see page 135)

## Policy Questions

**Question:**

I would like to set logon information for an application. How do I do this?

**Answer:**

You can set logon information for an application in a policy only. To set logon information, click the Applications tab in the policy and then double-click the application. The Application Login Information dialog appears. Use this dialog to enter your information.

**Question:**

What do I do if the logon information for an application is incorrect?

**Answer:**

You can correct this information using one of the following methods:

- Synchronize method

  You can use this method if your policy uses strong synchronization. To use this method, remove the application from the policy and then synchronize your accounts with the policy. This method removes the application from all accounts. Once the application is removed, enter the correct logon information for the application, add the application to the policy, and then synchronize your accounts with the policy.

- Force Update method

  You can use this method if your policy uses strong or weak synchronization. To use this method, enter the correct logon information, check the Force Update box, and then click OK. To save the changes, click Apply on the property sheet, and then propagate the changes to the policy.

**Question:**

My policy, when associated to a directory for the Policy data store, cannot be synchronized with an account created by using the policy. The Provisioning Manager always reports that the account's attribute GroupList is out-of-sync with that policy. Is there a solution for this problem?

**Answer:**

You can use *strong synchronization* for the policy and the *administrator* check box is checked on the Privileges tab, PLS Connector automatically joins the account to the predefined group_ps-adms when the account is created in the Policy data store by using the policy. Hence, the Provisioning Manager reports that attribute GroupList is out-of-sync. You may simply add group_ps-adms to the policy to eliminate this problem.

**Question:**

I have added an application to my policy on the Applications tab. The policy has been used to successfully create an account. However, the account's Applications tab does not show that the application in the policy is assigned to the account. If I use the Policy Manager for PLS Connector to verify the application assignment, the account's Applications tab also does not show the application as a linked one. Is this an error?

**Answer:**

An application can be explicitly or implicitly assigned to an account. In general, an application is implicitly assigned to an account if one of the following is true:

- The application's default access is EXECUTE.
- The application belongs to an application group already assigned to the account.
- The application is assigned to the group to which the account belongs.

When a policy is used to create an account, the PLS Connector does not explicitly assign an application to the account if the application has already been implicitly assigned. For performance reasons, this optimization is done to avoid storing redundant data for application authorization in the Policy data store. This optimization is especially important to user data stores with a large number of accounts. The Applications tab only shows the explicitly assigned applications, but the Application Login tab shows the applications explicitly or implicitly assigned to an account.  If you use the SSO Policy Manager, you can also find all assigned applications on the Application List tab.

## Authentication Method Question

**Question:**

I have added a new authentication method to CA Single Sign-On. How can I add the same authentication method to the CA Single Sign-On Option?

**Answer:**

Assume that the new authentication method is Method25 with the symbolic name MyOwnMethodA. Do the following on each of the Provisioning Server and Provisioning Manager systems:

1. Create a directory PS_HOME\Data\SSO.
2. Create a file sso_gui.ini in this directory with the following configuration parameters:

   ```
   # User-defined authentication methods

   [AuthnMap]

   Method25=MyOwnMethodA

   # Put additional methods here, if necessary.
   ```
3. Shut down the Provisioning Manager.
4. Restart the Provisioning Manager. You should be able to find the new method on the Authentication tab.

## Buffer Size Question

**Question:**

How can I change the sizes of the buffers for the CA SSO Connector for Advanced Policy Server to send/receive data to/from PLS Connector?

**Answer:**

The PLS Connector allocates memory buffers to send and receive data to and from the clients that communicate with SSO Servers. The PLS Connector is one of these clients. Each PLS client needs to allocate buffers that are large enough to store the information sent to and from SSO Servers. For example, and in particular, the buffer for the client to receive data from SSO Servers must not be smaller than the buffer for SSO Servers to send data to the client. The configuration file PS_HOME\Data\pls_agent.ini allows you to set the sizes of these buffers for the PLS Connector. Usually, you do not need to change the default settings in pls_agent.ini since the default buffer sizes are large enough to handle the communication between the PLS Connector and SSO Servers in most situations. However, if there are a very large number of accounts within one SSO Server container, you may need to increase the size of the buffers.

## Exploration Question

**Question:**

I received the error “Policy Server Error Buffer is too small” during exploration of a large number of accounts. What caused this to happen?

**Answer:**

When exploring a large number of accounts, the Send Buffer size should be increased in size up to 1 MB. For Policy Server 8.0 you can use a Policy Manager or selang command. For example:

```
chres PSCONFIGPROPERTY (“SendBuffSize@ssod”) gen_prop('VALUE”) gen_value
(“2000000”)
```

For Policy Server 7.0, you must add the SendBuffSize and set the value in the registry or modify the value using the Policy Manager. For example:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\eTrust\Shared\Policy
Server\2.0\ssod
```

# CA Top Secret Connector

The Top Secret Connector lets you administer accounts and resources on CA Top Secret systems. The Top Secret Connector provides a single point for all user administration by letting you do the following:

- Register endpoints, explore them for objects to manage, and correlate their accounts with global users
- Create and manage CA Top Secret accounts using account templates specific to CA Top Secret
- Change account passwords and account activations in one place
- Synchronize global users with their roles or synchronize global users' accounts with their account templates
- Assign an CA Top Secret policy to each of your CA Top Secret endpoints
- Use the default Endpoint Type policy to create accounts with the minimum level of security needed to access an CA Top Secret directory
- Generate and print reports about CA Top Secret accounts

## Install and Configure the TSS Connector

When installing the CA Top Secret Connector, perform the following steps:

1. Install the Provisioning Server with the CA Top Secret Connector
2. Configure your CA Top Secret system.

### How to Configure Your CA Top Secret System

Once the CA Top Secret Connector has been installed with the Provisioning Server, you must configure your CA Top Secret system to communicate with the connector.

**To configure your CA Top Secret system**

1. Install the CA LDAP Server for z/OS on your CA Top Secret system.
2. Review the CA LDAP Server for z/OS configuration options.

## Step 1. Install the CA LDAP Server for z/OS

The CA LDAP Server for z/OS provides the communication mechanism for this CA IdentityMinder Connector.  This product is a free offering from CA and can be downloaded from support.ca.com.  Once downloaded, refer to the *CA LDAP Server for z/OS Installation Guid*e for information and instructions on how to install it.

**Note:** The following steps are required to migrate from a previous version to r12.6.1:

1. The CA LDAP Server for z/OS must be installed on at least one mainframe system and configured to communicate to every z/OS system being managed by CA IdentityMinder or alternatively, you can install it on every z/OS system managed by CA IdentityMinder.
2. The CA LDAP Server(s) must be configured to have an endpoint entry in Provisioning Manager naming mode for each system. For more information on configuring, see the *CA LDAP Server for z/OS Administrator Guide*.
3. After upgrading, you must update each endpoint and update the information within the Mainframe LDAP Server section. This information matches up with the IP Address, Port, and suffix of the mainframe LDAP Server.

The existing eTrust_TSS.conf file must be removed from the eTrust_Admin.conf file, or alternatively, remove the contents from the file and make blank.

## Step 2. Review the CA LDAP Server for z/OS Configuration Options

Once all CA LDAP Server installation steps have been completed and your CA LDAP Server is started, it will be ready to support administration for this Connector. Some clients may need or want to setup additional configuration options for the CA LDAP Server in order to provide additional functionality for the this Connector. An example of this additional functionality is the enable_refresh option (instructs the CA LDAP Server to activate UID or GID fields for an ACID when changed using the CA LDAP Server). For more information on all available configuration options, see the chapter titled, "CATSS_DN Backend" in the *CA LDAP Server for z/OS Administrator Guide*.

## Securing Provisioning Server Communication to the CA LDAP Server

All communication between the Provisioning Server and the CA LDAP Server for z/OS can be encrypted using SSL (Secure Socket Layers).

**To establish communication**

- Setup your CA LDAP Server for z/OS to use the Server Mode for SSL connections. For information on how to configure this, see the chapter titled "CA LDAP Server Using Digital Certificates" in the *CA LDAP Server for z/OS Administrator Guide*.
- Turn on SSL support within the Provisioning Server for your TSS endpoint. To do this, bring up the properties of your TSS endpoint using the Provisioning Manager. In the section entitled 'Mainframe LDAP Server Information', enable the check box entitled 'Use Server-side SSL' and click Apply. Now, all communication to the configured CA LDAP Server will attempt to use an SSL connection, and will fail and provide an appropriate error message if SSL cannot be established.

# Top Secret Support for FIPS and IPv6

For this release of CA IdentityMinder, the TSS Connector and the Password Synchronization Agent for TSS support IPv6 but not FIPS.

# Connector-Specific Features

This section details your connector's specific management features, such as how to acquire and explore your endpoint. Also included are account, provisioning roles, account template, and group information specifically for your connector.

## Acquire a CA Top Secret System Using the User Console

You must acquire the CA Top Secret system before you can administer it with CA IdentityMinder.

**To acquire a TSS system using the User Console**

1. Select Endpoints, Manage Endpoints,Create Endpoint
2. Select CA-Top Secret from the drop-down list box on Create a new endpoint of Endpoint Type, and click Ok

   Use the Create CA-Top Secret Endpoint page to register a CA-Top Secret system. During the registration process, CA IdentityMinder identifies the CA-Top Secret system you want to administer and gathers information about it.
3. After entering the required information, click Submit.

   You are now ready to explore and Correlate the endpoint.

4. Click Endpoints, Explore and Correlate Definitions, Create Explore and Correlate Definition to explore the objects that exist on the endpoint.

   The Exploration process finds all CA-Top Secret accounts and groups. You can correlate the accounts with global users at this time or you can correlate them later.

5. Click OK to start a new definition.

6. Complete the Explore and Correlate Tab as follows:

   a. Fill in Explore and Correlate name with any meaningful name.

      Click Select Container/Endpoint/Explore Method to click a CA-Top Secret endpoint to explore.

   b. Click the Explore/Correlate Actions to perform:

      - **Explore directory for managed objects**—Finds objects that are stored on the endpoint and not in the provisioning directory.

      - **Correlate accounts to users**—Correlates the objects that were found in the explore function with users in the provisioning directory. If the user is found, the object is correlated with the user. However, you can instead select that you want to assign the account to the existing user (the default user) or create the user.

      - **Update user fields**—If a mapping exists between the object fields and the user fields, the user fields are updated with data from the objects fields.

7. Complete the Recurrence tab if you want to schedule when the task to executes.

   a. Click Schedule.

   b. Complete the fields to determine when this task should execute.

      You may prefer to schedule the task to execute overnight to interfere less with routine access of the system.

   **Note**: This operation requires the client browser to be in the same time zone as the server. For example, if the client time is 10:00 PM on Tuesday when the server time is 7:00 AM, the Explore and Correlate definition will not work.

8. Click Submit.

**To use an explore and correlate definition**

1. In a CA IdentityMinder environment, click Endpoints, Execute Explore and Correlate.

2. Click an explore and correlate definition to execute.

3. Click Submit.

   The user accounts that exist on the endpoint are created or updated in CA IdentityMinder based on the explore and correlate definition you created.

## Acquire a CA Top Secret System Using the Provisioning Manager

You must acquire the CA Top Secret system before you can administer it with CA IdentityMinder. When acquiring a CA Top Secret system, perform the following steps from the Endpoint Type task view:

1. Register the server as an endpoint in CA IdentityMinder. This phase is performed by adding a new endpoint under the CA Top Secret Endpoint Type in CA IdentityMinder.

   Use the CA Top Secret Endpoint property sheet to view or customize a CA Top Secret system. During the registration process, CA IdentityMinder identifies the CA Top Secret system you want to administer and gathers information about it.

2. Explore the objects that exist on the endpoint.

   After registering the server in CA IdentityMinder, you can explore its contents. Use the Explore and Correlate Endpoint dialog. The Exploration process finds all CA Top Secret accounts and objects. You can correlate the accounts with global users at this time or you can correlate them later.

3. Correlate the explored accounts with global users.

   When you correlate accounts, CA IdentityMinder creates or links the accounts on an endpoint with global users, as follows:

   a. CA IdentityMinder attempts to match the ACID with each existing global user name. If a match is found, CA IdentityMinder associates the CA CA-Top Secret account with the global user. If a match is not found, CA IdentityMinder performs the next step.

   b. CA IdentityMinder attempts to match the ACID name with each existing global user's full name. If a match is found, CA IdentityMinder associates the CA Top Secret account with the global user. If a match is not found, CA IdentityMinder performs the next step.

   c. If the Create Global Users as Needed button is checked, CA IdentityMinder creates a new global user and then associates the CA Top Secret account with the global user. If the Create Global Users as Needed button is unchecked, CA IdentityMinder performs the next step.

   d. CA IdentityMinder associates the CA Top Secret account with the [default user] object.

**Note:** If you are exploring and correlating a very large database, we recommend that you run the Explore, Correlate, and Update steps individually and use the dxtunedb utility to tune the database after each step. This significantly reduces your explore and correlate time.

To accomplish this, follow these steps:

1. Stop the Provisioning Service and the CA Directory services for etrustadmin.
2. Run the dxtunedb command to tune the CA IdentityMinder database.
3. Restart the Provisioning Service and CA Directory services for etrustadmin.
4. Run each step.

## Register CA Top Secret Endpoints on Windows

If you have a Windows system, you can register CA-Top Secret endpoints using the Provisioning Manager.

From the Endpoint Type task view

1. Select CA Top Secret Endpoints from Object Type.
2. Click the New button. You are required to fill in the following information:

   Endpoint Name

   > Specifies a name to refer to the new CA Top Secret endpoint.

   Mainframe LDAP IP Address/Machine Name

   > Specifies the IP address of the CA-Top Secret managed system where the CA LDAP Server is configured and running.

   Mainframe LDAP Port

   > Specifies the port number that you specified during the CA LDAP Server for z/OS install. If you are not sure of the Mainframe LDAP Port, see the section Checking Your CA LDAP Server for z/OS Configuration Information.

   **Mainframe LDAP Suffix**

   > Click the 'Get Suffixes' button to retrieve a list of valid suffixes configured for this CA LDAP Server operations in im naming mode. (See the chapter titled, "CATSS_DN Backend" in the *CA LDAP Server for z/OS Administrator Guide* for more information on naming mode.)

   Admin User

   > Specifies the CA Top Secret ACID of an administrator to be used from within CA IdentityMinder to manage the Top Secret system.

   Password

   > Specifies the password of the Top Secret ACID above.

   **Confirm Password**

   > Specifies the same password as above, for confirmation.

**Note:** After you click OK, the Provisioning Server attempts to establish a connection with the CA LDAP Server for z/OS at the IP address and port supplied, as well as validating the Admin user and Password values supplied. An appropriate error message is displayed if this connection fails. A Global User is inserted in the Provisioning Server with Domain Administrator authority using the ID and password supplied. This Global User is used to administer this CA Top Secret endpoint.

## Register CA Top Secret Endpoints on Solaris

To register CA-Top Secret endpoints, use the batch utility etautil to define a TSS endpoint by specifying a directoryName, Mainframe LDAP IPAddress, Port, and Suffix. For example:

```
etautil -u USERID -p PASSWORD add 'eTNamespaceName=TSS,dc=DOMAIN,dc=eta'
eTTSSDirectory name='DIRECTORYNAME' eTZOSLDAPIPAddress=IPADDRESS
eTZOSLDAPPort=PORT eTZOSLDAPSuffix=SUFFIX
```

where,

**DIRECTORYNAME**

Specifies the name you desire for this endpoint.

**IPADDRESS**

Specifies the IP Address or Machine name of the TSS system where your CA LDAP Server for z/OS is running.

**PORT**

Specifies the port number the CA LDAP Server is using.

**SUFFIX**

Specifies a valid suffix configured for this CA LDAP Server operating in im naming mode (For more information on the naming_mode option, see the chapter titled, "CATSS_DN Backend" in the *CA LDAP Server for z/OS Administrator Guide*.)

## Check Your CA LDAP Server for z/OS Configuration Information

To view all pertinent information regarding your CA LDAP Server and its configuration, issue a STATUS command from the mainframe console where your CA LDAP Server is running. The STATUS command provides information such as, version information, port number, configured databases, and suffixes. See the chapter titled, "Startup Options" in the *CA LDAP Server for z/OS Administrator Guide* for more information on the STATUS command.

## Limited Turkish and Hebrew Support Provided

Support is provided for a given set of Turkish characters in the name field of CA Top Secret accounts. The environment variable ETATURKISH must be set to 1 on the Provisioning Server for this support to work.

Support is also provided for a given set of Hebrew characters in the name, installation data (instdata), and sysout-appc(waname) fields for CA-Top Secret accounts. The environment variable ETAHEBREW must be set to 1 on the Provisioning Server for this support to work.

## TSS Provisioning Roles and Account Templates

The CA-Top Secret Default Policy, provided with the TSS connector gives a user the minimum security level needed to access an endpoint. You can use it as a model to create new account templates.

## TSS Accounts

*ACIDs* are called accounts in CA IdentityMinder. Use the CA Top Secret Account property sheet when managing your accounts. Only the ACID types of USER, DCA, VCA, ZCA, LSCA and SCA are populated under the accounts container when you explore a CA Top Secret endpoint.

**Note:** The containers described below may or may not get populated depending on the authority of the administrator and the security implementation of the CA Top Secret system.

## Departments

Only the ACID types of DEPARTMENT are populated under the departments container when you explore a CA Top Secret endpoint.

## Divisions

Only the ACID types of DIVISION are populated under the divisions container when you explore a CA Top Secret endpoint..

## Zones

Only the ACID types of ZONE are populated under the zones container when you explore a CA Top Secret endpoint.

## Groups

Only the ACID types of GROUP are populated under the accounts container when you explore a CA Top Secret endpoint.

**Note:** When synchronizing CA Top Secret accounts, strong synchronization is the default.

## Profiles

Profiles let you group a collection of similar resource access authorizations into one ACID. This profile ACID is then added to all users who require those particular access rights. Should the access requirements change, only the profile needs to be changed; the associated ACIDs are automatically updated.

You can create and maintain CA Top Secret profiles using the Endpoint Type task view. Use the CA Top Secret Profile property sheet when managing your profiles.

## Facilities

Facilities identify specific facilities under which the user must access the resource. You can create and maintain CA Top Secret facilities using the Endpoint Type task view. Use the CA Top Secret Facility property sheet when managing your facilities.

## Ownerships

Ownerships identify the resources that are protected by CA Top Secret. You can create and maintain CA Top Secret ownerships using the Endpoint Type task view. Use the CA Top Secret Ownership property sheet when managing your ownerships.

## Permissions

Permissions identify the conditions under which the ACID can access a resource. You can create and maintain CA Top Secret permissions using the Endpoint Type task view. Use the CA Top Secret Permission Name property sheet when managing your permissions.

## Profile Lists

Profile lists identify common resource access authorizations and are usually classified by task. You can create and maintain CA Top Secret profile lists using the Endpoint Type task view. Use the CA Top Secret Profile List property sheet when managing your profile lists.

## TSO Alias Support

The CA Top Secret connector also supports the creation of a TSO Alias when a user is created or modified with TSO access being granted. The alias value is always the value of the TSS Account being created or modified. To enable this support, see the chapter titled, "CATSS_DN Backend" in the *CA LDAP Server for z/OS Administrator Guide* for more information.

## TSS Program Exits

The CA Top Secret connector supports the use of Program Exits which are incorporated as 'Common Exits'. Program Exits provide you with the capability to perform certain actions before or after an account is created, modified or deleted from CA IdentityMinder. These exits can be referenced either on the Endpoint property page to execute custom code on a single endpoint, or on the Account Template property page to execute custom code on multiple endpoints. Actions might include native CA DSI (CA Distributed Security Integration) or CA LDAP Server for z/OS commands in order to modify account privileges or access to resources on the CA Top Secret system.

To see a sample program exit, refer to the OS390 subdirectory under the CA IdentityMinder Templates directory.

For more detailed information about how to write program exits, see the *Programming Guide for Provisioning*.

## Proxy Configuration

The TSS Endpoint page contains a section where clients can configure a Proxy administrative ID and password to be used for user password changes from the SAWI interface. When configured, this ID and password is used to issue the password change request for the SAWI user to change their password. This is helpful and needed if a SAWI user cannot supply a password (for example, the password is forgotten) or their password is expired on Top Secret and they cannot be authenticated. The following is an explanation of the algorithm followed by the TSS Agent when a password change is instantiated through the SAWI using a proxy administrator:

1. Under the authority of the proxy ID, an administrative reset is done to the SAWI users' password to an eight digit random number. This is needed in order to enforce password syntax rules specified by the NEWPW Control Option. The password change must occur under authority of the SAWI user. Since the SAWI user can instantiate a password change without supplying their current password, this administrative reset is necessary to set the password to a known value for the TSS Agent. This password change is immediately expired, so in the event of any kind of failure, this ID cannot access the system.
2. After the administrative reset, the TSS Agent can then issue a password change under the authority of the SAWI user, using the random number password to authenticate. This password change request is now subject to password syntax rules specified by the NEWPW Control Option, and the SAWI user sees an appropriate message if the new password does not comply.

When using a proxy administrative ID, standard TSS security rules apply (for example, scoping) and password syntax checking specified in the NEWPW Control Option is enforced. However, the NEWPW control Option Mindays value for the user is not enforced since the administrative reset password change is done through an administrator and is set to immediately expire. If the administrative password reset was not set to immediately expire, the Mindays Control Option would be enforced on the subsequent password change through the Self-Service user, and would likely fail.

**Note:** The check boxes on the Endpoints Setting tab are for legacy purposes only. You can perform proxy configuration and administrative support from the Self-Service interface.

## Proxy Administration Support

You can configure a proxy ID for all tasks accomplished within CA IdentityMinder. Previously, a proxy ID could only be configured for use with requests generated from the SAWI interface. This proxy ID is maintained on the main Endpoint page in the Proxy Administration Configuration section. The proxy ID can be used for any type of CA IdentityMinder request against supported objects, and for any CA IdentityMinder Administrator that is logged on.

Note: The enhancement is only recommended to use after careful consideration (and preparation) of the following consequences:

1. Any Global User (with the proper privileges provided within CA IdentityMinder) is able to administer Top Secret Acids and their access privileges, (for example, facilities and permissions) under the configured proxy ID. Any mainframe security product scoping is lost; only the scoping of the proxy ID is enforced.
2. As mentioned above, security settings are now the only point of enforcement against a Global User manipulating mainframe security data.
3. Any reports or auditing methods against administration of your mainframe security data that originate from the mainframe is now compromised; the only ID that shows up for any administration that occurred from CA IdentityMinder is the configured proxy ID.
4. If the proxy ID's password changes on the mainframe, the password must be changed on every Endpoint Page within CA IdentityMinder that it is configured for.

By default, the Connector operates in the same mode as in past releases; the logged-on Global User and their password are used for submitting any requests destined to the mainframe security product. The common directory page entitled Endpoint Settings provides two checkbox controls under the description Administrator Credentials that control the three possible settings:

**Use logged-in Administrator's credentials**

Default setting. Indicates that the logged-in Administrator (Global User) is used as the credentials for ALL requests, even from the SAWI.

**Use proxy for SAWI changes**

Indicates that the logged-in Administrator (Global User) is used as the credentials for all requests EXCEPT for requests from the SAWI interface. The proxy ID credentials (if available) are used for requests coming from the SAWI interface.

**Use proxy for ALL requests**

When no checkbox is checked, this indicates that the proxy ID credentials (if available) are to be used for ALL requests.

When any request occurs from CA IdentityMinder, these settings are checked against the endpoint where the request is targeted. If, based on the endpoint settings and the type of request (SAWI or otherwise), proxy credentials are to be used, the credentials that are defined for that endpoint are retrieved and used for the request. In the case where endpoint credentials are supposed to be used, but no credentials exist (either Proxy ID or password contains no value), the proxy credentials are not used for the request and the request proceeds using the logged-in Administrator (Global User) credentials.

**Note:** The check boxes on this tab are for legacy purposes only. You can perform proxy configuration and administration support from the Self-Service interface.

## TSS Conventions

Use the following CA-Top Secret conventions in your etautil commands:

- The endpoint type name is CA-Top Secret
- The endpoint type prefix is TSS. Therefore, the CA-Top Secret class names are:
  - eTTSSDirectory for an endpoint
  - eTTSSPolicyContainerName for an account template container
  - eTTSSPolicy for an account template

## LDAP Directory Services (LDS)

CA Top Secret provides the ability to synchronize z/OS security information management with LDAP compliant directory managed servers. The LDS component of the CA Top Secret system sends requests via LDAP commands through the Provisioning service and is directed to the LDS backend that is located on a Windows-based PC.

The module that handles LDS processing within CA IdentityMinder is named back_lds.dll (dynamic link library) and is intended to augment the functionality provided within CA IdentityMinder and the CA Top Secret Security product. The CA IdentityMinder LDS backend allows the user of the CA Top Secret for z/OS the ability to interface directly with the CA IdentityMinder database.

When a command is issued on the CA Top Secret system, to add a user, a Global User is created in the local CA IdentityMinder database with the specified password. Additionally, if the user is to be  associated with a CA IdentityMinder Role, the CA IdentityMinder inclusion will be generated to associate this user with the desired role or roles.

When a command is issued to the CA Top Secret system to change the password, or any other “mapped” field of a user, a change results in the local CA IdentityMinder database and optionally is propagated to all necessary platforms.

When a command is issued to the CA Top Secret system to delete a user, the Global User is deleted from the local CA IdentityMinder database and any associated inclusions are removed. Depending upon the platform, and CA IdentityMinder settings, this may also result in the deletion of accounts on other platforms.

## Features

The LDS backend within CA IdentityMinder provides special processing when any of the following LDAP attributes are mapped to respective CA Top Secret fields in the NDT XREF record:

- If LDAP attribute eTS390Role is specified as part of the command, the user is attached or removed from the specified Provisioning Role value. This may result in the addition or removal of accounts on any platform depending upon the Account Templates attached to that Provisioning Role. Typically, this attribute is mapped to a single-valued user defined field containing a comma-separated list of Provisioning Roles that the user is a member of.
- If the CA Top Secret password is mapped to the eTS390Password attribute, the password is applied to the CA IdentityMinder Global User and automatically propagated to all accounts associated with that Global User.

  **Note:** This attribute should only be used by clients that do **NOT** explore/correlate their TSS accounts into CA IdentityMinder. Clients that do run explore/correlate should follow the instructions in the Password Synchronization feature bulletin.
- Password Synchronization - Password changes to TSS User Acids (Acid types User, DCA, VCA, ZCA, LSCA, SCA) can be propagated into CA IdentityMinder to change a Global User's password and all accounts associated with the Global User. To accomplish this, an LDS record must be manually created (not from the LDS Wizard) using the instructions from the Configuration and Usage section with the following changes:
  - Step 3. Set the USERDNS (user dns) as follows:

    ```
    eTTSSAcidName=%L,eTTSSAcidContainerName=Accounts,
    eTTSSDirectoryName=www,
    eTNamespaceName=CA-Top Secret,dc=XXX,dc=eta
    ```

    where eTTSSEndpointName=www equals the CA IdentityMinder CA Top Secret Endpoint name and dc=XXX is the name of the CA IdentityMinder domain for this LDAP node in UPPERCASE.
  - Step 4. Set the OBJCLASS (object class) to eTTSSAcid.
  - Step 6. In the XREF section, add the entry: Password,eTSyncPassword.
- If the CA Top Secret password is mapped to the eTPassword attribute, this causes the password to only be applied to the Global User with no propagation to other accounts.
- If LDAP attribute eTS390Profile is specified as part of the command, the user is attached or removed from the specified Provisioning Role value. This may result in the addition or removal of accounts on any platform depending upon the Account Templates attached to that Provisioning Role. Typically, this attribute would be mapped to the Profiles field within TSS, because 'membership' to a TSS Profile can directly translate to Provisioning Role/Account Template concept within CA IdentityMinder.

**Note:** Values specified for both eTS390Profile and eTS390Role must exist within CA IdentityMinder as valid Provisioning Role names.

## Configuration and Usage

In order to configure your CA Top Secret system to drive requests through LDS to your Provisioning service, we recommend that you use the LDS Wizard provided within CA IdentityMinder on the Endpoint property page, to create or modify the NDT record on your CA Top Secret system. This wizard is only active and usable if the appropriate version of CA Top Secret is running, which supports LDS.

**Note:** For CA IdentityMinder users, you should only run this wizard from the Provisioning Manager.

If you choose not to use the wizard, then you must perform the following steps on the LDS record to invoke the LDS backend. For detailed information on LDS and setting up the LDS record, please refer to Chapter 13 of the CA Top Secret 5.3 Administrator Guide under LDAP Directory Services.

1. Sign on to the mainframe CA Top Secret system and create an LDAP node definition with the TSS ADD(NDT) LDAPNODE(XXXXXX) command. Set the ADMDN (admin dn) as follows:

```
eTGlobalUserName=<user>,eTGlobalUserContainerName=Global Users,
eTNamespaceName=CommonObjects,dc=XXX,dc=eta
```

   where eTGlobalUserName is the name of a CA IdentityMinder global user that has full authority to the domain (DomainAdministrator). dc=XXX is the name of the CA IdentityMinder domain for this LDAP node. The case for the domain name should be as it exists in CA IdentityMinder.

2. Set the ADMPSWD (admin password) to the correct password for the CA IdentityMinder global user.

3. Set the USERDNS (user dns) as follows:

```
eTGlobalUserName=%L,eTGlobalUserContainerName=Global Users,
eTNamespaceName=CommonObjects,dc=XXX,dc=lds
```

   where dc=XXX is the name of the CA IdentityMinder domain for this LDAP node. The case for the domain name should be as it exists in CA IdentityMinder.

4. Set the OBJCLASS (object class) to eTGlobalUser.

5. Set the URL (uniform resource locator) to the machine name or IP address that is running the Provisioning service. Make sure that this URL contains the correct port. 20389 is used in the example below:

   ```
   LDAP://machine.ca.com:20389
   ```

6. Add the appropriate XREF mappings between CA Top Secret fields and LDAP attributes as required.

7. Recycle LDS and refresh the NDT by issuing the following commands:

   ```
   TSS MODIFY(LDS(OFF))
   TSS REP(NDT) ACTIVE(YES)
   TSS MODIFY(LDS(ON))
   ```

## Implement LDS Password Syncing

When implementing LDS password syncing from a mainframe endpoint, do the following on the Provisioning server.

This procedure uses the default installation path for both files. Use the path that is appropriate for your CA IdentityMinder installation.

**To implement LDS password syncing**

1. Navigate to the following directory:

   ```
   C:\Program Files\CA\Identity Manager\Provisioning Server\data\
   ```

2. Add the following statement to the etrust_admin.conf file

   ```
   include "C:\\Program Files\\CA\\Identity Manager\\Provisioning
   Server\\data\\etrust_lds.conf "
   ```

3. Save the file and restart the Provisioning services.

## Extend the Schema to Include Custom Attributes

When you connect to a CA Top Secret system through CA IAM CS, you can correlate on any of the attributes are exposed by the connector. If you want to correlate on an attribute that the connector does not expose, you can extend the connector's schema to include up to twenty extra attributes.

To set up these extra attributes:

1. Create a mapping file that maps each attribute on the endpoint to an attribute in CA IdentityMinder (see page 154).

   This includes the custom attributes in the Provisioning Server.

2. Add the custom attributes to a new tab in the User Console (see page 155).

## Create a Mapping File for the Custom Attributes

The mapping file lists the custom attributes.

**Note:** This section refers to the Provisioning Server installation location as *ps_install*. By default, *ps_install* is in the following locations:

- **Windows**—C:\Program Files (x86)\CA\Identity Manager\Provisioning Server
- **Linux and Solaris**—/opt/CA/IdentityManager/ProvisioningServer/

**Follow these steps:**

1. Create a new directory in *ps_install*\data, and name the new directory *TSS*.
2. Create a text file named schema_map.txt and save it in *ps_install*\data\TSS.
3. In the text file, create entries with the format described in Format of the Mapping File for Custom Attributes (see page 154).
4. Restart the Provisioning Server service.

The Provisioning Server now includes the custom attributes.

## Format of the Mapping File for Custom Attributes

The mapping file contains a list of the custom attributes, each with the following format:

```
eTTSSCustomAttribute001=attribute1
eTTSSCustomAttribute002=attribute2
…
eTTSSCustomAttribute020=attribute20
```

In this list, the names on the left are the attributes in CA IdentityMinder and the names on the right are the attributes on the endpoint.

Each custom attribute in CA IdentityMinder is named eTTSSCustomAttributeNNN, where NNN is a number from 001 to 020. You can use these names in any order, but we recommend that you start with eTTSSCustomAttribute001, to avoid confusion.

There must be no spaces before or after each attribute name.

The attribute names are case-sensitive.

On Solaris, make sure the mapping file is world-readable (its permission should be at least 444).

## Add the Custom Attributes to a Tab in the User Console

You can include the custom attributes in a tab in the User Console.

**Follow these steps:**

1. Log in to the User Console as a user with administrative rights.
2. Click the Roles and Tasks tab, then click Admin Tasks, Manage Admin Tasks.
3. Search for *Top Secret*.
4. Click on the name of the screen that you want to change, for example *Modify CA Top Secret Account*.
5. Select Tabs.
6. Find Custom Attributes in the table, and click its Edit button.
7. Select the Browse button beside the Screen field.
8. Select “Modify CA Top Secret Account – Custom Attributes”. Click Copy.
9. Give the new screen a unique name by editing the Name and Tag values.
10. Delete any Custom Attribute fields that should not appear on the final screen.
11. For each custom attribute, change its name to the actual attribute name on the endpoint:
    a. Click the attribute's Edit icon.
    b. Edit the Name to show the attribute's real name on the endpoint. This will appear on the final screen
12. Click OK.
13. Click Select.
14. Click OK, then click Submit.

The new tab is now available in the User Console.

## Error When Updating Expiration Date

**Symptom:**

When I attempt to update the expiration date, the update fails and following message appears:

```
TSS0251E  KEYWORD EXPIRE  DOES NOT SUPPORT SUBFIELDS
```

**Solution:**

To fix this problem, upgrade to CA LDAP Server r14 or later.

## Cannot Create Account When Password Policies Conflict

This section applies to all connectors. However, it is most likely to be relevant to the mainframe connectors.

**Symptom:**

In many organizations, some endpoints (such as the mainframe systems) have stricter restrictions on passwords than the corporate password policy.

This conflict causes problems if you create a password that meets the requirements of the CA IdentityMinder password policy but is invalid on an endpoint. In this situation, the following problems can occur:

- When you use a provisioning role to create an endpoint account for an existing global user with such a password, the account is not created.
- When you attempt to create a new user with a temporary password, the user is not created.
- When you change the password of an existing account on the endpoint, the changed password is not saved.

**Solution:**

To avoid this problem, make one or both of the following changes:

- Make the password policy in CA IdentityMinder more restrictive than the password policy on the mainframe endpoint.
- Make the policy for temporary passwords more restrictive than the password policy on the mainframe endpoint.

  This change forces new users to change their password when they log in to User Console.

# Best Practices

This section describes the recommended practices to use for the implementation of CA Top Secret security administration.

## Using z/OS Security Administration

There is a distinction between a security officer and a security administrator. The security officer for z/OS is a senior CA Top Secret administrator and is typically an infrequent user of CA IdentityMinder. However, the security officer is responsible for the z/OS security policies established and used with CA IdentityMinder.

On the other hand, a designated security administrator manages a subset of the security management function. This subset depends on the management policy of the organization and may include the creation of new user accounts on various systems, the resetting of passwords, and so on. The capabilities of these security administrators (whether through CA IdentityMinder or some other means) is guided by the security officer.

Because policies control the capabilities that a user has on a CA Top Secret security system, it is important that they be set up correctly to enforce the existing policies in your organization. The following sections discuss recommendations for using CA IdentityMinder to create and manage your policies.

However, CA IdentityMinder is not intended to be the primary interface for the experienced CA Top Secret administrator. An experienced CA Top Secret security administrator manages CA Top Secret better by using commands issued under TSO rather than working in the CA IdentityMinder framework. Many functions are managed directly, and certain capabilities are *only* available through direct CA Top Secret commands. For those instances, we recommend that you implement the LDAP Directory Synchronization (LDS) option for CA Top Secret security (available in CA-Top Secret Version 5.3 and above). This ensures that the information that is added into CA Top Secret outside of CA IdentityMinder coincides with CA IdentityMinder.

## Understanding the Explore and Correlate Function

The explore and correlate function gathers ACID, profile, and group information from the CA Top Secret security file. This information is added into CA IdentityMinder at the appropriate level in the endpoint tree. Because the information that is gathered is live data from CA Top Secret, performing the explore and correlate function on a stable, non-changing CA Top Secret data store is recommended. To ensure the information recorded into the Provisioning repository is current and up-to-date, start this process in the evening when there is no activity occurring in the CA Top Secret data store.

With the potential for many thousands of records, the explore and correlate function could run for many hours. As a result, the function for adding CA Top Secret objects runs as a separate task in CA IdentityMinder. This enables you to continue working in CA IdentityMinder while the exploration and correlation of the CA Top Secret security information continues.

The following are three different options for the Explore and Correlate function of a CA Top Secret endpoint:

- No Check - No Action
- Gray check with gray background - explores, correlates, and updates the database section by section
- Black check with white background - explores, correlates, and updates all of the sections of a database as one database in entirety.

The result section and message log reports information consistent with each choice. The difference is most evident with the initial explore and correlate of a CA Top Secret Endpoint.

## How Exploration and Correlation Works

It is important to understand the steps of the explore and correlate function so that you can determine how and when to use it in your organization. There are three steps to performing the explore and correlate function. The first step gathers the information from the CA Top Secret security file. The length of time this step takes is a constant that is based on the number of ACIDs, profiles, and groups on your z/OS system. Because the number of changes that have been made to the CA Top Secret data store outside of CA IdentityMinder cannot be determined, a complete list of objects is always generated.

The second step compares the information in the CA Top Secret security data store to the information in the CA IdentityMinder repository and merges the results. This consists of adding any new account information into the CA IdentityMinder repository and removing accounts that were deleted outside of CA IdentityMinder. The initial exploration takes a long time. However, in each subsequent execution of the exploration, the length of time it takes is directly proportional to the amount of activity and changes made outside of CA IdentityMinder.

The third step correlates the information gathered from the CA Top Secret security file into the Provisioning repository. This step is only performed if the Correlate accounts with global users check box has been selected in the Explore and Correlate Endpoint dialog. We recommend that you also select the Create global users check box at the same time since these two tasks are closely related. The length of time that this step takes, like the previous step, increases with the number of the new objects being added, modified, or deleted.

## When to Perform Exploration and Correlation

Two factors dictate when and how often to run the explore and correlate function. The first factor is based on the amount of activity that takes place in the CA Top Secret security data store outside of CA IdentityMinder. Usually, this can follow a predetermined schedule established in your organization. Periodically, the security officer may request certain CA IdentityMinder administrators to perform this function because they have added a key CA Top Secret profile that may be needed for immediate use, or because they are aware of a high volume of changes that may have occurred.

The second factor is whether your organization has implemented the LDAP Directory Services (LDS) option for CA Top Secret security (available in Version 5.3 and above). If you have implemented this option, the requirement to run the explore and correlate function is dramatically decreased because each modification on the z/OS host is automatically propagated into the CA IdentityMinder repository, if configured on your mainframe. For those organizations that continue to be z/OS-centric, we recommend the implementation and use of the LDS option.

**Note:** If running an explore and correlate on multiple TSS directories, you should have RDT2BYTE activated or deactivated on all directories. Your user defined fields on the system with RDT2BYTE inactive will be incorrect if all are not specified.

## Setting Up Role-based Administration

The basic principle of user administration is allowing the user to access only the resources they need to perform their job. You should also base access rights on a user's responsibility or job role, rather than on the individual user ID. By using these simple rules, you ensure that you are building a structure that does not require constant administrative attention.

CA Top Secret security lets you meet this objective by building profile records that reflect the many job roles and responsibilities in your organization. To start your security implementation, map job roles and responsibilities to CA Top Secret security profiles, and then map those profiles to account templates. You can then implement a provisioning role with the appropriate account template that maps into your CA Top Secret profile. This results in an ACID that has the appropriate CA Top Secret permissions for that job function.

If you spend time building a good profile structure before you start protecting resources, you will have a well-designed security system and simplified administration. Failing to build a strong profile structure results in custom administration based on individual access rights. The load on your security administrators increases as you protect more and more resources. As a result, users have access to the resources that they need to do their job function in addition to other resources that reflect previous job functions and responsibilities. Consequently, the administration tasks continue to increase over time.

## Understanding Account Templates

An account template is used to control the capabilities and attributes of an account on any endpoint. The CA Top Secret policy contains over 150 attributes that you can set. These attributes control everything from what department a user is in, the capabilities the user has when logged on to TSO, and the user's CA Top Secret profiles. Basically, most attributes that you can define for an ACID can be established through an account template.

Account Templates are used to define the attributes to use when creating new accounts and also to ensure that existing accounts conform to established account templates. This is accomplished when you synchronize an account template to the accounts assigned to the account template. Since this concept is vital when implementing security, it is important to fully understand how this functionality works.

## Understanding Synchronization

Synchronization can be either weak or strong. You can set the type of synchronization you want on the account template. For the CA Top Secret Connector, the default action is set to strong synchronization. When you use Provisioning Manager to modify an account template, strong synchronization automatically enforces the attributes on the account template to the account. Any attributes that are enabled at the account level and disabled at the account template level are disabled at the account level after synchronization completes. For more information, see Synchronization in Provisioning Manager in the *Administrator Guide*.

When weak synchronization is performed, the attribute in the account and the attribute in the account template are compared. For example, for Boolean attributes, if an attribute is turned on in the account template and off in the account, it is turned on at the account level. If the attribute is turned off (a value of 0) at the account template level and on (a value of 1) at the account level, the attribute remains on after synchronization occurs. Consequently, the greater value of the attributes, whether in the account template or in the account, takes precedence and is applied.

This same rule applies for string values. For example, if the value for TSOPROC is equal to PROC111 in the account template, and the value that an account has is equal to PROC999, when synchronization occurs, the value on the account remains the same because PROC111 is less than PROC999.

Assigning multiple policies to a role increases the complexity of the merging algorithm, even when using strong synchronization. If multiple policies are assigned to a role, the same logic is used to determine the value applied to the account. For example, if account template1 has a value of CAPROC with strong synchronization selected, account template2 has a value of DAPROC with strong synchronization selected, and the account already has ACPROC, when synchronization completes, the account is updated to DAPROC (the greatest of the three values). This algorithm also applies when a global user is assigned to multiple provisioning roles and each provisioning role has an assigned account template.

## Capability Attributes

An account template can contain two types of attributes: initial or capability. An initial attribute is used only when a CA Top Secret CREATE is done. A capability attribute affects processing when a CA Top Secret CREATE is done and when synchronization is performed. The CA Top Secret security capability attributes appear as boldface characters in the account template property sheet.

In CA IdentityMinder, when a CREATE is done and multiple account templates are assigned to the global user, the product performs a CREATE using the values of the first account template and issues successive MODIFY statements to implement the values of the subsequent account templates. This becomes important with CA Top Secret because, at a minimum, each ACID must be assigned a department. We recommend that you enter a department value in the global user attributes and that each account template use the %UDEPT% rule string to obtain the value from the global user record. This ensures uniformity during the CREATE and also ensures that the ACID does not get moved between departments during subsequent MODIFY statements.

The Department field does not appear in the account template as a required field but may be required for a successful CREATE. You should always verify the use of your account templates under as many conditions as will exist in your CA IdentityMinder implementation.

## Using Account Templates

The effective use of account templates in CA IdentityMinder is critical to establishing a secured environment. We recommend that you use the same values in a CA Top Secret account template that were used in the CA Top Secret profile record (or multiple profile records). This way, the security officer makes a change in one place-the CA Top Secret profile record. The change is effective immediately for every user assigned to use that profile, synchronization does not need to be performed in CA IdentityMinder, and CA Top Secret security is only updated once.

## Using Profiles with Account Templates

When using CA Top Secret profiles in an account template, there are additional issues to consider. First, because the order of profiles on an ACID are critical to the permissions of that ACID and because LDAP does not provide a guarantee of that order, we recommend entering all profiles on a single account template when the order is imperative. Second, when CA IdentityMinder processes account template changes, the current profiles from the ACID record are removed and the profiles from the account template are added. If you have modified the list of profiles attached to the ACID outside of CA IdentityMinder, these modifications are lost. Finally, the Profile drop-down list is generated based on the exploration of the z/OS host. If changes are made through CA Top Secret or by adding an ACID of TYPE=PROFILE in CA IdentityMinder, you must perform an explore at the profile level to ensure that the information in CA IdentityMinder and CA Top Secret coincides.

There may be instances where profiles do not exist, or it may not be advantageous to establish one for small variations in access authorities, or you may want to set values that are not supported in a profile record. If individual attributes are needed or are going to be used on an account template, we recommend that you establish policies based on the different segments in CA Top Secret. That is, an account template can control TSO information, another may control OMVS, and another may set MISC or PROFILE values. Combined, these policies completely define an ACID's attributes.

The advantage of using this methodology is that it provides a flexible interface to update certain key information in multiple ACIDs with the least amount of overhead. For example, one account template has values that control TSO authorities and is called TSOUser. Another is called TSOProgrammer and has different, expanded TSO authorities. If your provisioning role has the TSOUser account template assigned to it, but you want to provide the users with increased capabilities, you can change the provisioning role to point to the TSOProgrammer account template, and then synchronize the provisioning role. This grants the authorities for TSO based on the TSOProgrammer account template to the users assigned to that provisioning role. If this is a temporary change to last only the length of a project, change the provisioning role back to point to the TSOUser account template when the project is complete and synchronize again. This results in removing those attributes and reapplying the original values. A couple of mouse clicks and you have potentially updated numerous ACIDs with a standard set of attributes and the only attributes affected were those of TSO.

As a general rule, it is always a good practice to run a Check Sync command before doing the actual synchronization. This allows you to validate that the changes you made are the only changes to send to CA Top Secret and you are not affected by a change made to an account template that was not synchronized at an earlier date.

### Using Model ACIDs

User administration also includes decisions about what applications users need access to. Some of these access rights can be defined through the profile definitions, but others have to be defined through the ACID definitions. CA Top Secret allows you to define user definitions to use as a model when you add a new user to a provisioning role in CA IdentityMinder. These are called Model ACIDs. Their use is another effective way to reduce both network and security system overhead. By specifying a Model ACID on an account template in the Using field, you can effectively reduce the magnitude and complexity of the commands issued to CA Top Secret when creating new ACIDs.

### Authorizing Account Template Administration

CA IdentityMinder provides *admin profiles* that give administrators certain types of access and privileges to manage objects in a domain. These profiles ensure that delegated administrators have the authority to change only what they are authorized to change. We recommend that only the administrators involved in account template management be allowed to modify account templates. This can be established for all account templates or for only CA Top Secret account templates depending on your needs. You can also use admin profiles to distribute account template management based on platform.

## DB2 UDB for z/OS Connector

The connector for DB2 UDB for z/OS (DBZ) lets you manage user authorization and privileges of a DB2 UDB on z/OS instance and database on a z/OS mainframe.

Using this connector, you can do the following:

- Create, modify, or delete DBZ Endpoint Types, endpoints, users, and account templates in CA IdentityMinder
- Create, modify, and remove users in the DBZ database on z/OS
- Manage user identifiers, authorizations, and privileges that exist in the DBZ authorization and privileges tables.

However, you cannot use this connector to map stored functions.

This connector does not support FIPs or IPv6.

This connector is managed by CCS.

**Note:** Before you use the connector, set up the license file for JDBC.

## DBZ Endpoint

The DBZ endpoint registers a Windows System ODBC Data Source Name (DSN) for the database and saves the necessary information to establish a connection and execute SQL statements with the database.

### Acquire a DBZ Database Using the User Console

You must acquire the DB2 z/OS database before you can administer it with CA IdentityMinder.

**To acquire an DBZ database using the User Console**

1. Select Endpoints, Manage Endpoints,Create Endpoint
2. Select DB2 ZOS Server from the drop-down list box on Create a new endpoint of Endpoint Type, and click Ok

   Use the Create DB2 ZOS Endpoint page to register a DB2 ZOS database. During the registration process, CA IdentityMinder identifies the DBZ database and gathers information about it.
3. After entering the required information, click Submit.

   You are now ready to explore and Correlate the endpoint.
4. Click Endpoints, Explore and Correlate Definitions, Create Explore and Correlate Definition to explore the objects that exist on the endpoint.

   The Exploration process finds all DBZ accounts and groups. You can correlate the accounts with global users at this time or you can correlate them later.
5. Click OK to start a new definition.
6. Complete the Explore and Correlate Tab as follows:

   a. Fill in Explore and Correlate name with any meaningful name.

      Click Select Container/Endpoint/Explore Method to click a DBZ endpoint to explore.

   b. Click the Explore/Correlate Actions to perform:

      - **Explore directory for managed objects**—Finds objects that are stored on the endpoint and not in the provisioning directory.
      - **Correlate accounts to users**—Correlates the objects that were found in the explore function with users in the provisioning directory. If the user is found, the object is correlated with the user. However, you can instead select that you want to assign the account to the existing user (the default user) or create the user.
      - **Update user fields**—If a mapping exists between the object fields and the user fields, the user fields are updated with data from the objects fields.

7. Complete the Recurrence tab if you want to schedule when the task to executes.

   a. Click Schedule.

   b. Complete the fields to determine when this task should execute.

      You may prefer to schedule the task to execute overnight to interfere less with routine access of the system.

   **Note**: This operation requires the client browser to be in the same time zone as the server. For example, if the client time is 10:00 PM on Tuesday when the server time is 7:00 AM, the Explore and Correlate definition will not work.

8. Click Submit.

**To use an explore and correlate definition**

1. In a CA IdentityMinder environment, click Endpoints, Execute Explore and Correlate.
2. Click an explore and correlate definition to execute.
3. Click Submit.

   The user accounts that exist on the endpoint are created or updated in CA IdentityMinder based on the explore and correlate definition you created.

## Acquire a DBZ Database Using the Provisioning Manager

To acquire a DBZ database, you must do the following:

**From the Endpoint Type task view**

1. Register the database as an endpoint in CA IdentityMinder.

   Use the DBZ Endpoint property sheet to register a DB2 z/OS database. During the registration process, CA IdentityMinder identifies the DBZ database you want to administer and gathers information about it.

2. Explore the objects that exist on the endpoint.

   After registering the database in CA IdentityMinder, you can explore its contents. Use the Explore and Correlate Endpoint dialog. The Exploration process finds all DBZ database authorization names that exist in the database authorization tables. You can correlate the authorization names of the User type (DBZ Users) with global users at this time, or you can wait to correlate them.

3. Correlate the explored DBZ users with global users.

   When you correlate DBZ users, CA IdentityMinder creates or links the DBZ users to an endpoint with global users, as follows:

   a. CA IdentityMinder attempts to match the DBZ user name with each existing global user name. If a match is found, CA IdentityMinder associates the DBZ user name with the global user. If a match is not found, CA IdentityMinder performs the following step.

   b. If the Create Global Users as Needed button is checked, CA IdentityMinder creates a new global user and then associates the DBZ account with the global user. If the Create Global Users as Needed button is unchecked, CA IdentityMinder performs the next step.

   c. CA IdentityMinder associates the DBZ user with the [default user] object.

## Acquire or Remove a New Endpoint

When the DBZ connector receives an 'Add new endpoint' or 'Remove an endpoint' request, the following steps are taken:

**On the machine running the C++ Connector Server**

1. Catalog or un-catalog a database entry for a database within the DBZ instance.
2. Register or un-register an ODBC system data source.

## DBZ Account Templates

The DBZ Default Policy, provided with your connector, gives a user the minimum security level needed to access an endpoint. You can use it as a model to create new account templates.

## Synchronize an Account from an Account Template

There are several rules for account synchronization from an account template in the DBZ Connector.

**During the account synchronization process**

1. When there are multiple account templates associated with a DBZ account, the DBZ Connector merges those account templates to generate an intermediate effective account template. During the merge, if there are conflicting settings with the same authority, database privilege, or object privilege among the different account templates, the DBZ Connector selects the setting with the highest restriction.

   For example, if Account Template One grants DBADM and Account Template Two does not, the effective account template does not grant DBADM. Another example: If Account Template One grants CONTROL and SELECT with GRANT option on view SYSCAT.ATTRIBUTES, but Account Template Two revokes CONTROL from and grants SELECT on view SYSCAT.ATTRIBUTES, the effective account template grants only SELECT on view SYSCAT.ATTRIBUTES and revokes CONTROL from SYSCAT.ATTRIBUTES.

2. If one of the merged account templates is set to use strong synchronization, the DBZ Connector applies the effective account template to the account using strong synchronization. If not, the effective account template uses weak synchronization.
3. For strong synchronization, the DBZ Connector replaces the account's authorities and privilege settings with that of the effective account template.
4. For weak synchronization, if there is a difference between the account settings and the effective account template, the DBZ Connector uses the setting that has the higher restriction.

   For example, if an account is granted DBADM, and the effective account template does not grant DBADM, the account will not be granted DBADM. If an account is not granted DBADM and the effective account template grants DBADM, the account will still not be granted DBADM.

   Another example: If an account is granted CONTROL and SELECT with GRANT option on view SYSCAT.ATTRIBUTES, but the effective account template revokes CONTROL from and grants SELECT on view SYSCAT.ATTRIBUTES, the account is granted only SELECT on view SYSCAT.ATTRIBUTES and CONTROL is revoked from SYSCAT.ATTRIBUTES.

When checking account or account template synchronization, the same process of generating effective account template applies, as do the rules of comparison. If you are going to synchronize account settings with the effective account template, and the account's authority and privilege settings do not change, the DBZ Connector considers the account synchronized with its associated account templates.

## DBZ Accounts

The DBZ Account represents the authentication and privileges of the DBZ users of the DBZ instance and database on a z/OS mainframe.

The DBZ Connector does not manage user accounts and groups of the operating system. The DB2 Users that are managed by the DB2 z/OS Connector are the user identifiers, authorizations, and privileges that exist in the DB2 authorization and privileges tables.

## Create DBZ Accounts

CA IdentityMinder lets you manage accounts from the Endpoint Type task view. Use the DBZ User property sheet when managing your accounts

**To create DBZ Accounts**

1. Click the Endpoint Type task button and select DBZ Endpoint from the drop-down list box.
2. Search for the endpoint on which you want to create an account.
3. Right-click on the endpoint in the list view and choose Content from the pop-up menu.
4. Select Accounts in the Container Tree box and click New.

   The DBZ User Property Sheet appears.
5. Complete the DBZ User Property Sheet and click OK.

   A new DBZ account is now created.

## DBZ User Property Sheet

The DBZ User Property Sheet consists of 16 property pages with the following 14 pages specific to the DBZ Connector that show specific authorization and property information:

- Database
- Subsystem
- Table
- View
- Buffer Pool
- Storage Group
- Collection
- Package
- Plan
- Table Space
- Procedure
- User Defined Function
- Schema
- User Defined Type

# Google Apps Connector

The Google Apps Connector provides a single point for all Google Apps account administration. The connector lets you administer account objects and groups on Google Apps endpoints.

You can use the Google Apps Connector to perform the following actions:

- :Endpoint Management
  - Create and delete an endpoint
  - Acquire Google Apps endpoints
  - Explore Google Apps endpoints for existing accounts and groups
- Group Management
  - View the Google Apps groups a user is a member of
  - Assign or remove a user from a Google Apps group
- Account Management
  - View, create, modify, or delete an account

Note: If you delete a Google Apps account, you cannot create an account with the same name until five days after the original account was deleted.

  - Suspend or resume an account
  - Assign or revoke a Google Apps account to or from a user

## Configure Google Apps Provisioning API Access

To manage a Google Apps endpoint with CA IdentityMinder, log in to the Google Apps Control Panel and enable the provisioning API in your Google Apps settings.

CA IdentityMinder can now manage the Google Apps endpoint.

**Note:** For more information, see the *Google Apps Admin Help*.

## Configure Password Length

To ensure password compatibility between Google Apps and CA IdentityMinder, configure the minimum and maximum length for passwords in Google Apps and in CA IdentityMinder so they match.

**Note:** For more information, see Password Policies in the CA *IdentityMinder Administration Guide*.

## Configure NTLM Authentication

If CA IAM CS is running on a Windows computer and NTLM is the strongest authentication scheme supported by the HTTP proxy, the Google Apps connector attempts to use NTLM authentication with the HTTP proxy.

On a Windows computer, CA IAM CS is installed as a Windows Service and runs as Local System by default. If your HTTP proxy server uses NTLM authentication, configure CA IAM CS to run under a Windows domain account or a Windows local account.

To configure NTLM authentication, do either of the following:

- Run CA IAM CS with a Windows account that can be authenticated with the HTTP proxy server without providing a user name and password for proxy authentication when creating the endpoint.
- Run CA IAM CS with a Windows account that cannot be authenticated with the HTTP proxy server, and provide a HTTP user name and password that can be authenticated with the proxy when creating the endpoint.

**Note:** If you use a Windows domain user for HTTP proxy authentication, prefix the HTTP proxy user name with the Windows domain that the user is in. For example, *DOMAIN**ProxyUserAccountName.*

## Google Apps—CAPTCHA Challenge

**Symptom:**

During authentication, I receive the following error message with a CAPTCHA challenge:

```
Authentication failed, CAPTCHA requires answering. Please use the following website
to unlock JCS computer: https://www.google.com/a/yourdomain/UnlockCaptcha
```

**Solution:**

Do the following:

1. Log on to the computer where CA IAM CS is running.
2. Open a web browser.
3. Follow the link provided in the error message, and replace yourdomain.com with your Google Apps domain. For example:

   `https://www.google.com/a/`*`yourdomain.com`*`/UnlockCaptcha`
4. Answer the CAPTCHA question.

   The Google Apps server issues a new authentication token and trusts your computer.

**Note:** For more information, about CAPTCHA challenge, see http://code.google.com/googleapps/faq.html#handlingcaptcha

# IBM DB2 UDB Connector

Along with the CA IdentityMinder Connector for the underlying operating system, the DB2 UDB Connector lets you administer accounts and groups on DB2 UDB databases and provides a single point for all user administration by letting you:

- Register DB2 UDB endpoints, explore them for objects to manage, and correlate their accounts with global users
- Create and manage DB2 UDB database authorization names (users and groups) using DB2 UDB-specific account templates
- Synchronize global users with their provisioning roles or synchronize global users' accounts with their account templates
- Assign a DB2 UDB account template to each of your DB2 UDB endpoints
- Use the default endpoint type account template to create DB2 UDB users with the minimum security level needed to access a DB2 UDB endpoint
- Create and manage DB2 UDB groups (Windows only)

# DB2 UDB Installation

This connector is managed using the Connector and C++ Server installation process.

**Note:** For more information and requirements, see *Connector and C++ Connector Server Installation.*

## Installation Requirements for Windows

The following connector and agent are necessary to administer the DB2 Universal Database:

- **DB2 UDB Connector** must be installed.
- To administer DB2 UDB authentication, an appropriate CA IdentityMinder Connector for the underlying operating system of DB2 UDB Server installation must be installed on the Provisioning Server. Such options include, but are not limited to the NT Connector, ETC Connector, NIS Connector and the ADS Connector.
- **DB2 UDB** Administration Client must already be installed where the DB2 UDB Connector will be installed.

  **Note:** You must install the 32-bit version of the DB Connect client package.
- **TCP/IP** must be one of the supported communication protocols of the DB2 UDB installation when DB2 UDB server is at a remote location.
- **TCP/IP Communication** must be set up for the DB2 UDB Instance on DB2 UDB Server using Control Center and have either a TCP/IP Service Name or Port Number assigned (default to 50000) when the DB2 UDB server is at a remote location.
- **Database Manager Instance** should be started on the DB2 UDB Server.

**Note:** The DB2 UDB Connector supports any DB2 UDB server installations that the DB2 UDB Administrative Client for Window supports, but tests have been done only with DB2 UDB server installations on Windows 2000 and AIX.

## DB2 UDB Support for FIPS and IPv6

For this release of CA IdentityMinder, the DB2 UDB Connector supports IPv6, but not FIPS.

# DB2 Limitation

You cannot associate a DB2 provisioning role created with English characters to a user created with French or Japanese characters. This is a limitation of DB2.

## Connector-Specific Features

This section details your connector's specific management features, such as how to acquire and explore your endpoint. Also included are account, provisioning roles, account template, and group information specifically for your connector.

### Acquire a DB2 UDB Database Using the User Console

You must acquire the DB2 database before you can administer it with CA IdentityMinder.

**To acquire an DB2 database using the User Console**

1. Select Endpoints, Manage Endpoints,Create Endpoint
2. Select DB2 Server from the drop-down list box on Create a new endpoint of Endpoint Type, and click Ok

   Use the Create DB2 Server Endpoint page to register a DB2 database. During the registration process, CA IdentityMinder identifies the DB2 database you want to administer and gathers information about it.
3. After entering the required information, click Submit.

   You are now ready to explore and Correlate the endpoint.
4. Click Endpoints, Explore and Correlate Definitions, Create Explore and Correlate Definition to explore the objects that exist on the endpoint.

   The Exploration process finds all DB2 accounts and groups. You can correlate the accounts with global users at this time or you can correlate them later.
5. Click OK to start a new definition.
6. Complete the Explore and Correlate Tab as follows:
   a. Fill in Explore and Correlate name with any meaningful name.

      Click Select Container/Endpoint/Explore Method to click a DB2 endpoint to explore.
   b. Click the Explore/Correlate Actions to perform:
      - **Explore directory for managed objects**—Finds objects that are stored on the endpoint and not in the provisioning directory.
      - **Correlate accounts to users**—Correlates the objects that were found in the explore function with users in the provisioning directory. If the user is found, the object is correlated with the user. However, you can instead select that you want to assign the account to the existing user (the default user) or create the user.
      - **Update user fields**—If a mapping exists between the object fields and the user fields, the user fields are updated with data from the objects fields.

7. Complete the Recurrence tab if you want to schedule when the task to executes.

   a. Click Schedule.

   b. Complete the fields to determine when this task should execute.

      You may prefer to schedule the task to execute overnight to interfere less with routine access of the system.

   **Note**: This operation requires the client browser to be in the same time zone as the server. For example, if the client time is 10:00 PM on Tuesday when the server time is 7:00 AM, the Explore and Correlate definition will not work.

8. Click Submit.

**To use an explore and correlate definition**

1. In a CA IdentityMinder environment, click Endpoints, Execute Explore and Correlate.

2. Click an explore and correlate definition to execute.

3. Click Submit.

   The user accounts that exist on the endpoint are created or updated in CA IdentityMinder based on the explore and correlate definition you created.

## Acquire a DB2 UDB Database Using the Provisioning Manager

You must acquire the DB2 UDB database before you can administer it with CA IdentityMinder.

**From the Endpoint type task view**

1. Register the database as an endpoint in CA IdentityMinder.

   Use the DB2 UDB Endpoint property sheet to register a DB2 UDB database. During the registration process, CA IdentityMinder identifies the DB2 UDB database you want to administer and gathers information about it.

2. Explore the objects that exist on the endpoint.

   After registering the database in CA IdentityMinder, you can explore its contents. Use the Explore and Correlate Endpoint dialog. The Exploration process finds all DB2 UDB database authorization names that exist in the database authorization tables. You can correlate the authorization names of the User type (DB2 UDB Users) with global users at this time, or you can wait to correlate them.

3. Correlate the explored DB2 UDB users with global users.

   When you correlate DB2 UDB users, CA IdentityMinder creates or links the DB2 UDB users to an endpoint with global users, as follows:

   a. CA IdentityMinder attempts to match the DB2 UDB user name with each existing global user name. If a match is found, CA IdentityMinder associates the DB2 UDB user name with the global user. If a match is not found, CA IdentityMinder performs the following step.

   b. If the Create Global Users as Needed button is checked, CA IdentityMinder creates a new global user and then associates the DB2 UDB account with the global user. If the Create Global Users as Needed button is unchecked, CA IdentityMinder performs the next step.

   c. CA IdentityMinder associates the DB2 UDB user with the [default user] object.

## DB2 Provisioning Roles and Account Templates

By defining account templates for the underlying operating system to a provisioning role, you can manage the operating system accounts and groups while managing the authorization name of the DB2 UDB database. Therefore, provisioning roles and account templates let you manage all the aspects of the DB2 UDB database security.

The DB2 UDB Default Policy, provided with the DB2 UDB Connector, gives a user the minimum security level needed to access an endpoint. You can use it as a model to create new account templates.

## Create Account Templates

The Default Account Template, provided with each connector, gives a user the minimum security level needed to access an endpoint. You can use it as a model to create new account templates.

**To create an account template**

1. Click the Provisioning Roles task button, select the connector's Account Template in the Object Type drop-down list box and click New.

   The Account Template Property Sheet for the specified connector appears.

2. Complete the Account Template Property Sheet by:

   a. Selecting an endpoint to populate the drop-down and group selection lists.

   b. Selecting group memberships and other account settings.

   c. Clicking OK.

   A new account template is created for your connector.

## DB2 UDB Users

In CA IdentityMinder DB2 UDB Users give users access to the resources on an endpoint. CA IdentityMinder lets you manage all DB2 UDB database authorization names of the type User from the Endpoint type task view. Use the DB2 UDB User property sheet when managing your users.

## DB2 UDB Groups

CA IdentityMinder lets you create and maintain DB2 UDB authorization names of the type Group using the Endpoint type task view. Use the DB2 UDB Group property sheet when managing your groups.

## Add New Endpoint Request

When the DB2 Connector receives an 'Add new endpoint' request, it:

1. Catalogs a new DB2 Local or TCP/IP node for the instance.
2. Catalogs a new DB2 Database entry for the database.
3. Configures an ODBC system data source for the database.

## How to Synchronize an Account from an Account Template

These are the rules for account synchronization from an account template in the DB2 Connector.

1. During the account synchronization process, when there are multiple account templates associated with a DB2 account, the DB2 connector merges those account templates to generate an intermediate effective account template. During the merge, if there are conflicting settings with the same authority, database privilege, or object privilege among the different account templates, the DB2 Connector selects the setting with the highest restriction.

   For example, if Account Template One grants DBADM and Account Template Two does not, the effective account template does not grant DBADM. Another example: If Account Template One grants CONTROL and SELECT with GRANT option on view SYSCAT.ATTRIBUTES, but Account Template Two revokes CONTROL from and grants SELECT on view SYSCAT.ATTRIBUTES, the effective account template grants only SELECT on view SYSCAT.ATTRIBUTES and revokes CONTROL from SYSCAT.ATTRIBUTES.

2. If one of the merged account templates is set to use strong synchronization, the DB2 Connector applies the effective account template to the account using strong synchronization. If not, the effective account template uses weak synchronization.

3. For strong synchronization, the DB2 Connector replaces the account's authorities and privilege settings with that of the effective account template.

4. For weak synchronization, if there is a difference between the account settings and the effective account template, the DB2 Connector uses the setting that has the higher restriction.

   For example, if an account is granted DBADM, and the effective account template does not grant DBADM, the account will not be granted DBADM. If an account is not granted DBADM and the effective account template grants DBADM, the account will still not be granted DBADM.

   Another example: If an account is granted CONTROL and SELECT with GRANT option on view SYSCAT.ATTRIBUTES, but the effective account template revokes CONTROL from and grants SELECT on view SYSCAT.ATTRIBUTES, the account is granted only SELECT on view SYSCAT.ATTRIBUTES and CONTROL is revoked from SYSCAT.ATTRIBUTES.

   When checking account or account template synchronization, the same process of generating effective account template applies, as do the rules of comparison. If you are going to synchronize account settings with the effective account template, and the account's authority and privilege settings do not change, the DB2 Connector considers the account synchronized with its associated account templates.

# Kerberos Connector

You can use the Kerberos Connector to administer Kerberos principals and Kerberos password policies on Solaris servers. The Kerberos Connector provides a single point for all user administration by letting you do the following:

- Register endpoints, explore them for objects to manage, and correlate their accounts with global users.
- Create and manage Kerberos principals using Kerberos-specific account templates.
- Change principal passwords and principals activations in one place.
- Synchronize global users with their provisioning roles or synchronize global users' accounts with their account templates.
- Assign a Kerberos account template to each of your Kerberos endpoints.
- Create accounts with the minimum level of security needed to access a Kerberos endpoint using the default endpoint type account template.
- Create, edit and delete password policies.

This connector is installed using the Connector and Java Connector Server installation process. For more information and requirements, click here.

## Kerberos Connector Limitations

When you use the Kerberos Connector, we recommend that you consider the following limitations:

- The connector is based on the Solaris implementation of Kerberos version 5.
- The Windows CA IAM CS supports the Kerberos connector only when you use SSH.
- The connector can be installed with both the Windows and Solaris Server version of the Provisioning Server and manage the connector using CA IAM CS.
- The connector does not currently support keytab management of kadmin.
- The connector generates an error if you use any characters other than non-control ASCII characters in principal names, password policy names, and passwords, as Kerberos accepts only non-control ASCII characters.

## Unsupported kadmin Options

The Kerberos Connector is integrated with the kadmin interface to let you provision KRB principal and password policies; however you should be aware of the following:

- The connector does not support kadmin.local. Thus, options that are available only through kadmin.local are not supported.
- The keytab management (ktadd, ktremove) and administration privileges (ACL) aspects of kadmin are currently not supported.
- The –c option of kadmin is not supported since kadmin requests new service tickets from the KDC.
- The –kvno and –keepold password related options are not currently supported.

## Naming Limitations

Because the Kerberos Connector relies on kadmin to communicate with the Kerberos server, kadmin limitations are limitations of the connector.

Principal names, passwords, and password policy names can include any printable ASCII character. However, the following kadmin limitations are applicable, as described in the following sections:

- Principal Naming Limitations (see page 182)
- Password Policy Naming Conventions (see page 182)
- Password Limitations (see page 182)

### Principal Naming Limitations

- The double quote character (“) is used by kadmin only as a quoting character. kadmin does not accept this character as part of a principal name. As a result, the connector will reject principal names containing this character.
- The @ character delimits principal names from realm names, and cannot be part of a principal or realm name.

  The connector and kadmin accept an account name in the form name@realm, but if the realm is not the same as the realm specified by the endpoint, kadmin will treat this as a cross-realm principal. As a result, even though an entry for this principal will be included in the Kerberos database, unless you configure cross-realm authentication properly, this principal may not be able to authenticate to any KDC. If an account name with more than one @ character is used, kadmin will display a *Malformed name* error.
- The backslash character (\) is not properly supported. There are cases where, in a sequence of one or more backslash characters, one character may be dropped depending on the character immediately succeeding the backslash. The connector will not prevent the creation of principal names with backslash characters, but we recommend that you use the backslash character with caution.
- The hash (#) character can be used to start a principal name in kadmin. However, due to DN syntax limitations, the hash at the beginning of a principal name will be escaped with a backslash character (\). Within The Provisioning Manager, this escape character will always be present, but in the Kerberos system, the principal name will not have the escape character.

### Password Policy Naming Limitations

- kadmin uses the double quote character (“) only as a quoting character. kadmin does not accept this character as part of a password policy name. Thus this connector will reject password policy names containing this character.
- kadmin will accept a password policy name that starts with a hash (#). However, due to DN syntax limitations, the hash at the beginning of a name will be escaped with a backslash character. Within the Provisioning Manager and the Kerberos system, this escape character will always be present.

### Password Limitations

The double quote character (“) is used by kadmin only as a quoting character. kadmin does not accept this character as part of a password.

## Kerberos Installation and Deployment

This section provides information about installing and deploying the Kerberos Connector, including firewall configuration and keytab and cross-realm paths setup.

## Installation Prerequisites

The Kerberos server (KDC) must be Sun's Kerberos V5 implementation, and installed on Solaris 10. You must install the following packages.

- SUNWkdcr (Kerberos V5 KDC - root)
- SUNWkdcu (Kerberos V5 Master KDC – user)
- SUNWkrbr (Kerberos version 5 support – Root)
- SUNWkrbu (Kerberos version 5 support – Usr)

The CA IAM CS host must have the SUNWkdcu (Kerberos V5 Master KDC – user) packages installed, and you must configure them as a Kerberos client (that is, you must configure krb5.conf).

## Supported Configurations

The Kerberos Connector supports the following configurations:

| CA IAM CS Host | SSH Server | Supported in CA IdentityMinder version |
|---|---|---|
| Solaris 10 and a member of the Kerberos realm | None | SP8 and earlier |
| Solaris 10 and not a member of the Kerberos realm | Solaris 10, and a member of the realm | SP7 and later |
| Windows or Linux and not a member of the Kerberos realm | Solaris 10, and a member of the realm | SP7 and later |

## How to Configure Authentication to Kerberos

If you are creating or migrating an endpoint, configure authentication to Kerberos using one or both of the following methods, depending on your configuration (see page 184):

- Kerberos authentication (see page 187)
- SSH authentication

## Install and Deploy the Connector

The installation package contains the components required to install the Kerberos Connector.

**Note:** If you have any standalone Provisioning Manager installations that require access to Kerberos, reinstall the Provisioning Manager to add the Kerberos Connector.

**Follow these steps:**

1. Run the Provisioning Server install, and add the Kerberos Connector when prompted.

   The server and directory components are updated with the schema for the Kerberos Connector.

2. Install the CA IdentityMinder – Connector Server, and register it to the domain during the installation.

   The connector is deployed and tells the server where to send Kerberos requests. When complete, you can start to acquire Kerberos endpoints.

   **Note:** For more about setting up hosts, keytabs, and configuration files on a computer that hosts CA IAM CS where it is not the same computer as the KRB endpoint, see How to Set Up CA IAM CS Host to be a Member of the Target Realm (see page 188).

3. Depending on your configuration, set up SSH Permissions for the Kerberos Connector.

   **Note:** For more information about when to configure the connector to use SSH, see When to Configure the Kerberos Connector to Use SSH (see page 184).

## When to Configure the Kerberos Connector to Use SSH

From CA IdentityMinder 12.5 SP7 onwards, the Kerberos connector uses SSH to execute the kadmin command remotely. Set up SSH permissions on the SSH server under any of the following scenarios:

- You are upgrading any version of CA IdentityMinder to SP7 or later, you have existing KRB endpoints, and you move CA IAM CS from Solaris to a Windows, Linux, or a Solaris host that is not a member of the realm.

  **Note:** We recommend that you upgrade the CA IdentityMinder Provisioning Directory, Provisioning Server, Provisioning Manager and the CA IdentityMinder User Console. When installing the new CA IAM CS, register CA IAM CS to the Provisioning Server during installation.

- You are creating a Kerberos endpoint

## Pre-requisite Knowledge Required to Set Up SSH Permissions

To configure the Kerberos connector to use SSH, we recommend that you are familiar with the following:

- Basic UNIX file commands
- Basic UNIX concepts such as:
  - Output redirection
  - File permissions
  - Understanding, checking, and setting environment variables such as PATH
  - Navigating directories
  - Hidden directories and files
- User Administration
- Advanced commands for user and group administration such as useradd –create users and passwd – changing user passwords
- Advanced commands for services such as svcs – list services, svcadm – service administration

## Firewall Configuration

There are three main Kerberos components:

- Kerberos client applications (for example, kinit, telnet, pop)
- Server applications (for example, telnetd, popper)
- Kerberos KDC

Different types of traffic go between each pair of components your firewall is between. Depending on the pair of components your firewall is between, you will need to allow different types of traffic through your firewall.

**Note:** The notation xxxx/udp or xxxx/tcp used in the following table refers to an ephemeral port number (that is, >1024). This refers to a return port that the system assigns. The only assumption you can make about the port number is that it will be greater than 1024.

You may need to configure your firewall to allow traffic between a client program and the KDC on the following ports and protocols:

| Client Application | To KDC | Return Traffic |
|---|---|---|
| Ticket requests (for example, kinit) | 88/udp | xxxx/udp |
| Kerberos 5-to-4 ticket conversion | 4444/udp | xxxx/udp |

| Client Application | To KDC | Return Traffic |
|---|---|---|
| Changing password (kpasswd under Unix) | 749/tcp | xxxx/tcp |
| Changing password (under Windows, old interface) | 464/tcp | xxxx/tcp |
| Changing password (under Windows, new interface) | 464/udp | xxxx/udp |
| Running kadmin (also requires initial ticket, 88/udp) | 749/tcp | xxxx/tcp |

You may need to configure your firewall to allow traffic between an application server and the KDC on the following ports/protocols:

| Application Server | To KDC | Return Traffic |
|---|---|---|
| Initial ticket request (for example, kinit) | 88/udp | xxxx/udp |
| Kerberos 5-to-4 ticket conversion | 4444/udp | xxxx/udp |

You may need to configure your firewall to allow traffic between a client program and an application server on the following ports/protocols:

| Application Program Server | To Server | To ClientTraffic |
|---|---|---|
| rlogin/rlogind (w/o encryption) | 543/tcp | xxxx/tcp |
| rlogin/rlogind (w/encryption) | 2105/tcp | xxxx/tcp |
| rsh/rshd | 544/tcp | xxxx/tcp |
| pop/popper | 1109/tcp | xxxx/tcp |
| telnet/telnetd | Same as non-kerberos telnet/telnetd | |
| ftp/ftpd | Same as non-kerberos ftp/ftpd | |

## Keytab and Cross-realm Paths Setup

Depending upon the Administrative principal’s authentication options, and whether the host where CA IAM CS is deployed is in the realm specified for the endpoint, you may need to set up keytabs and cross-realm paths on the CA IAM CS host.

**Note:** For more information, see the *Solaris 10 System Administration Guide: Security Services.*

## Kerberos Authentication Methods

You can set up authentication using several different methods:

- CA IAM CS host principal (see page 190)
- CA IAM CS principal and a custom keytab (see page 191)
- A principal other than CA IAM CS host principal and the default keytab (see page 192)
- A principal other than CA IAM CS host principal and a custom keytab (see page 194)
- Principal and password authentication (see page 195)

## How to Set Up the CA IAM CS Host to be a Member of the Target Realm

The following section shows an example you how you can set up the host for use with CA IAM CS where the host will be a member of the target realm.

**Note:** This scenario is only applicable where CA IAM CS is on a Solaris that is not a member of the realm and you want to make it a member of the realm. If your CA IAM CS is on Windows or Linux, configure the connector to use SSH instead.

1. Copy the file /etc/krb5/krb5.conf from the key distribution center to the CA IAM CS host. Ensure that:
   - The default_realm entry in the libdefaults section points to the target realm.
   - The KDC entry in the appropriate realm relation in the realms section points to the target KDC.
   - The domain_realm section has the correct mapping of the CA IAM CS host to the target realm.
2. Modify the logging and appdefaults sections in the /etc/krb5/krb5.conf file as required.
3. On the KDC, create a host principal for the CA IAM CS host and give it a random key. For example, use the following command in kadmin to create a new host principal:

   ```
   add_principal -randkey host/jcs_host.ca.com
   ```
4. Set up authentication to use one of the following:
   - CA IAM CS host principal (see page 190)
   - CA IAM CS host principal and a custom keytab (see page 191)
   - A principal other than CA IAM CS host principal and the default keytab (see page 192)
   - A principal other than CA IAM CS host principal and a custom keytab (see page 194)
   - Principal and password authentication (see page 195)

**Note:** For information on using the host for other Kerberos-related purposes, such as hosting other Kerberos applications or services, see the relevant sections on kadmin, ktutil and krb5.conf in the *Solaris 10 System Administration Guide: Security Services*.

## How you set Up Keytab Authentication Using the Host Principal

To set up keytab authentication using the host principal, do one of the following:

- If the default keytab file exists, add the entries into a temporary keytab. (see page 190)
- If the default keytab file does not exist, create a new keytab file. (see page 191)

## Set Up Keytab Authentication Using the CA IAM CS Host Principal if Keytab File Does Not Exist

To set up keytab authentication using the host principal if the default keytab file does not exist, you need to create a new keytab file.

**To specify keytab authentication using the CA IAM CS host principal if keytab file does not exist**

1. Enter the following command in kadmin:

   ```
   kadmin: ktadd -k temp_keytab jcs-host-principal
   ```

   Kerberos adds the entries into a temporary keytab.

   **Note:** This creates a new randomized password for the host principal, thus any entries for the host principal in any existing keytab file are no longer valid.

2. In the KDC, modify the kadm5.acl file using a text editor.

   The connector adds the necessary privileges to the host principal.

   **Note:** Use * to specify all privileges.

3. In the Provisioning Manager, on the Endpoint Property sheet, click the Properties tab.

   The Properties tab is displayed.

4. Select the Keytab option.
5. Leave the Keytab and Principal fields blank.
6. Click Apply.

   The Kerberos Connector uses the CA IAM CS host principal for keytab authentication.

## Set Up Keytab Authentication Using the CA IAM CS Host Principal if Keytab File Exists

To set up keytab authentication using the host principal if the keytab file exists, you need to add keytab entries for the CA IAM CS host principal to the default /etc/krb5/krb5.keytab file.

**To specify keytab authentication using the CA IAM CS host principal if keytab file exists**

1. Enter the following commands in ktutil:

   ```
   ktutil: read_kt temp_keytab
   ```

   ```
   ktutil: read_kt /etc/krb5/krb5.keytab
   ```

   Kerberos reads both keytabs.

2. Enter the following command in ktutil:

   ```
   ktutil: write_kt /etc/krb5/krb5.keytab
   ```

   **Note:** Make sure that the entries for the host principal are the same, and are the latest key version number.

   Kerberos writes the entries to the default keytab file and the temporary keytab file is merged into the default keytab.

3. In the KDC, modify the kadm5.acl file using a text editor.

   The connector adds the necessary privileges to the host principal.

   **Note:** Use * to specify all privileges.

4. In the Provisioning Manager, on the Endpoint Property sheet, click the Properties tab.

   The Properties tab is displayed.

5. Select the Keytab option.

6. Leave the Keytab and Principal fields blank.

7. Click Apply.

   The Kerberos Connector uses the CA IAM CS host principal for keytab authentication.

## Set Up Keytab Authentication Using a Custom Keytab and CA IAM CS Host Principal

To set up keytab authentication using a custom keytab file rather than the default keytab file and the CA IAM CS host principal, you can add keytab entries for the CA IAM CS host principal to you custom keytab file.

**To set up keytab authentication using a custom keytab and the CA IAM CS host principal**

1. If the keytab file you want to use does not exist, use the following command to add entries to your custom keytab file.

   ```
   kadmin: ktadd -k keytab jcs-host-principal
   ```

   **Note:** This creates a new randomized password for the host principal, therefore any entries for the host principal in any existing keytab file are no longer valid.

2. If the keytab file exists, do the following:

   a. Enter the following command in kadmin to add entries into a temporary keytab:

      ```
      kadmin: ktadd -k temp_keytab jcs-host-principal
      ```

      **Note:** This creates a new randomized password for the host principal, thus any entries for the host principal in any existing keytab file are no longer valid.

   b. Enter the following command in ktutil to read both keytabs:

      ```
      ktutil: read_kt temp_keytab
      ```

   c. Enter the following command in ktutil to write it to the keytab file you want to use:

      ```
      ktutil: write_kt keytab
      ```

      The temporary keytab file is merged into the keytab file you want to use.

   **Note:** Make sure that the entries for the host principal are the same, and are the latest key version number.

3. In the KDC, modify kadm5.acl using a text editor to add necessary privileges to the host principal.

   **Note:** Use * to specify all privileges.

4. In the Provisioning Manager, on the Endpoint Property sheet, click the Properties tab.

5. Specify the keytab file you want to use, but leave the Principal field blank.

6. Click Apply.

   The Kerberos Connector uses the keytab you specified for authentication.

## Set Up Keytab Authentication Using the Default Keytab and a Principal Other than the CA IAM CS Host Principal

To specify keytab authentication using the default keytab and a principal other than the CA IAM CS host principal, you can add keytab entries for the principal to the keytab file.

**To specify keytab authentication using the default keytab and a principal other than the CA IAM CS host principal**

1. If the principal has a random password and the default keytab file does not exist, enter the following command in kadmin to add entries to the file:

   ```
   kadmin: ktadd principal
   ```

   **Note:** This creates a new randomized password for the target principal, therefore any entries for the target principal in any existing keytab file are no longer valid.

2. If the principal has a random password and the keytab file exists, do the following:

   a. Enter the following command in kadmin to add entries into a temporary keytab:

      ```
      kadmin: ktadd -k temp_keytab principal
      ```

      **Note:** This creates a new randomized password for the target principal, thus any entries for the target principal in any existing keytab file are no longer valid.

   b. Enter the following commands in ktutil to read both keytabs:

      ```
      ktutil: read_kt temp_keytab
      ```

      ```
      ktutil: read_kt /etc/krb5/krb5.keytab
      ```

   c. Enter the following command in ktutil to write the entries to the target keytab file you want to use.

      ```
      ktutil: write_kt /etc/krb5/krb5.keytab
      ```

      The temporary keytab file is merged into the target keytab file you want to use.

   **Note:** Make sure that the entries for the target principal are the same, and are the latest key version number.

3. If the principal has a specific password, do the following:

   a. Enter the following command in ktutil:

      ```
      ktutil: read_kt /etc/krb5/krb5.keytab
      ```

   b. Enter the following command in ktutil:

      ```
      ktutil: addent –password –p principal –k kvno –e enctype
      ```

   c. Repeat Step b for all enctypes.

      ktutil adds the entries to the default keytab file.

   **Note:** Ensure you add all keys for the principal, and that all resulting entries for the principal are the same and latest key version number.

4. Enter the following command in ktutil to verify that the list contains all required keys:

   ```
   ktutil: list
   ```

5. Enter the following command in ktutil to write the entries to the keytab file:

   ```
   ktutil: write_kt /etc/krb5/krb5.keytab
   ```

6. In the KDC, modify kadm5.acl using a text editor to add necessary privileges to the target principal.

   **Note:** Use * to specify all privileges.

7. In the Provisioning Manager, on the Endpoint Property sheet, click the Properties tab.

8. Specify the principal you want to use, but leave the Keytab field blank.

9. Click Apply.

   The Kerberos Connector uses the keytab you specified for authentication.

## Set Up Keytab Authentication Using a Custom Keytab and a Principal Other than the CA IAM CS Host Principal

To specify keytab authentication using a keytab file other than the default keytab and a principal other than the CA IAM CS host principal, you can add entries for the desired principal to the desired keytab file.

**To set up keytab authentication using a custom keytab and a principal other than the CA IAM CS host principal**

1. If the principal has a random password and the keytab file you want to use does not exist, use the following command to add entries:

   ```
   kadmin: ktadd -k keytab principal
   ```

   **Note:** This creates a new randomized password for the target principal, therefore any entries for the target principal in any existing keytab file are no longer valid.

2. If the principal has a random password and the keytab file exists, do the following:

   a. Enter the following command in ktutil to add entries into a temporary keytab:

      ```
      kadmin: ktadd -k temp_keytab principal
      ```

      **Note:** This creates a new randomized password for the desired principal, thus any entries for the desired principal in any existing keytab file are no longer valid.

   b. Enter the following commands in ktutil to read both keytabs:

      ```
      ktutil: read_kt keytab
      ```

      ```
      ktutil: read_kt temp_keytab
      ```

   c. Enter the following command in ktutil to write the entries to the keytab file you want to use.

      ```
      ktutil: write_kt keytab
      ```

      The temporary keytab file is merged into the target keytab file you want to use.

   **Note:** Make sure that the entries for the desired principal are the same, and are the latest key version number.

3. If the principal has a specific password, do the following:

   a. Enter the following command in ktutil:

      ```
      ktutil: read_kt /etc/krb5/krb5.keytab
      ```

   b. Enter the following command in ktutil:

      ```
      ktutil: addent –password –p principal –k kvno –e enctype
      ```

c. Repeat Step b for all enctypes.

ktutil adds the entries to the keytab file you want to use.

**Note:** Ensure you add all keys for the principal, and that all resulting entries for the principal are the same and latest key version number.

4. Enter the following command in ktutil to verify that the list contains all required keys:

```
ktutil: list
```

5. Enter the following command in ktutil to write the entries to the keytab file:

```
ktutil: write_kt /etc/krb5/krb5.keytab
```

6. In the KDC, modify kadm5.acl using a text editor to add necessary privileges to the target principal.

   **Note:** Use * to specify all privileges.

7. In the Provisioning Manager, on the Endpoint Property sheet, click the Properties tab.
8. Specify the principal and keytab you want to use.
9. Click Apply.

   The Kerberos Connector uses the keytab you specified for authentication.

### Set Up Principal and Password Authentication

You can specify authentication using principal and password authentication.

**To set up principal and password authentication**

1. In the KDC, modify kadm5.acl to add necessary privileges to the target principal.

   **Note:** Use * to specify all privileges.

2. In the Provisioning Manager, on the Endpoint Property sheet, click the Properties tab.
3. Specify the principal and keytab you want to use.
4. Click Apply.

   Kerberos uses the principal and password for authentication.

## Connector-Specific Features

This section details your connector's specific management features, such as how to acquire and explore your endpoint. Also included are account, provisioning roles, account template, and group information specifically for your connector.

## Tools for Managing Data in Endpoints

You can manage the accounts on your directories using any of the client interfaces. Each of these interfaces offers unique functionality:

- **Provisioning Manager**—Lets you perform all administrative tasks. It is the most commonly used interface that all administrators can access.
- **Batch Utility**—Lets you perform repetitive and time-consuming tasks offline through a command line interface.

## KRB Etautil Conventions

Use the following Kerberos conventions in your etautil commands:

- The endpoint type name (eTNamespaceName) is KRB
- The endpoint type prefix is KRB. Therefore, the Kerberos class names are:
  - - eTKRBDirectory for an endpoint
  - - eTKRBAccountContainer for an account container
  - - eTKRBAccount for an account
  - - eTKRBPasswordPolicyContainer for a password policy container
  - - eTKRBPasswordPolicy for a password policy
  - - eTKRBPolicyContainer for an account template container
  - - eTKRBPolicy for an account template

## Program Exits (Common or Native)

Program Exits let you write software that executes during certain actions that the Provisioning Manager carries out. Program exits extend the framework of the Provisioning Manager and allow for additional functionality that can change or augment the standard Provisioning Manager behaviors. Of the two types of exits, the Kerberos Connector supports *Native Exits.*

*Native exits* are program exits executed from within the managed endpoint types. Program exits let you reference custom code from within the Provisioning Manager process flow.

Information about the Kerberos exit program is entered on the Kerberos Program Exit property sheet.

**Note**: For more detailed information about how to write program exits, see the *Programming Guide for Provisioning* for Common Exits.

## Acquire a Kerberos Machine Using the User Console

You must acquire the Kerberos machine before you can administer it with CA IdentityMinder.

**To acquire a Kerberos machine using the User Console**

1. Select Endpoints, Manage Endpoints,Create Endpoint
2. Select KRB Namespace from the drop-down list box on Create a new endpoint of Endpoint Type, and click Ok

   Use the Create KRB Endpoint page to register a Kerberos machine. During the registration process, CA IdentityMinder identifies the Kerberos machine you want to administer and gathers information about it.
3. After entering the required information, click Submit.

   You are now ready to explore and Correlate the endpoint.
4. Click Endpoints, Explore and Correlate Definitions, Create Explore and Correlate Definition to explore the objects that exist on the endpoint.

   The Exploration process finds all Kerberos accounts and groups. You can correlate the accounts with global users at this time or you can correlate them later.
5. Click OK to start a new definition.
6. Complete the Explore and Correlate Tab as follows:
   a. Fill in Explore and Correlate name with any meaningful name.

      Click Select Container/Endpoint/Explore Method to click an Kerberos endpoint to explore.

   b. Click the Explore/Correlate Actions to perform:
      - **Explore directory for managed objects**—Finds objects that are stored on the endpoint and not in the provisioning directory.
      - **Correlate accounts to users**—Correlates the objects that were found in the explore function with users in the provisioning directory. If the user is found, the object is correlated with the user. However, you can instead select that you want to assign the account to the existing user (the default user) or create the user.
      - **Update user fields**—If a mapping exists between the object fields and the user fields, the user fields are updated with data from the objects fields.
7. Complete the Recurrence tab if you want to schedule when the task to executes.
   a. Click Schedule.

   b. Complete the fields to determine when this task should execute.

      You may prefer to schedule the task to execute overnight to interfere less with routine access of the system.

**Note**: This operation requires the client browser to be in the same time zone as the server. For example, if the client time is 10:00 PM on Tuesday when the server time is 7:00 AM, the Explore and Correlate definition will not work.

8. Click Submit.

**To use an explore and correlate definition**

1. In a CA IdentityMinder environment, click Endpoints, Execute Explore and Correlate.
2. Click an explore and correlate definition to execute.
3. Click Submit.

   The user accounts that exist on the endpoint are created or updated in CA IdentityMinder based on the explore and correlate definition you created.

## How You Acquire and Manage Kerberos Endpoints Using the Provisioning Manager

You must acquire the Kerberos endpoint before you can administer it with the Provisioning Manager. When acquiring a Kerberos endpoint, perform the following steps from the Endpoint task view:

1. Acquire the machine as an endpoint in the Provisioning Manager.

   **Note:** There are two ways to authenticate to the endpoint: use a keytab or use a principal and a password. To specify the authentication method, complete the fields on the on the Properties Tab on the KRB Endpoint Property Sheet.

2. Explore the objects that exist in the endpoint.

   After registering the machine in the Provisioning Manager, you can explore its contents. The exploration process finds all Kerberos objects. You can correlate the principals with global users at this time, or you can wait to correlate them.

3. Correlate the explored principals to global users. You can choose to:

   - Use existing global users. Do this when there are already global users in the Provisioning Manager and you want to connect the existing global users to the Kerberos principals.
   - Create global users as needed. Do this when there are no global users and you want to populate the Provisioning Manager from the Kerberos principals.

When you correlate principals, the Provisioning Manager creates or links the principals on an endpoint with global users, as follows:

- The Provisioning Manager attempts to match the Kerberos principal name with each existing global user name. If a match is found, the Provisioning Manager associates the Kerberos principal with the global user. If a match is not found, the Provisioning Manager performs the next step.
- The Provisioning Manager attempts to match the Kerberos principal name with each existing global user's full name. If a match is found, the Provisioning Manager associates the Kerberos principal with the global user. If a match is not found, The Provisioning Manager performs the next step.
- The Provisioning Manager associates the Kerberos principal with the [default user] object or a new global user is created depending on your choice.

**More Information:**

Acquire a New Endpoint (see page 200)
Explore and Correlate Principals (see page 202)
View All Principals (see page 203)

## Acquire a New Endpoint

You must acquire and register a Kerberos endpoint before you can administer it with the Provisioning Manager.

**To acquire a new endpoint**

1. In the Provisioning Manager, click the Endpoints button.
2. In the Object Type list, select KRB Policy, then click New.

   The  KRB Account Template dialog appears.

   The KRB Directory dialog appears.
3. Complete the fields on the KRB Directory tab, then click OK.

   The parameters you need to acquire and register a KRB Directory are specified.
4. Complete the fields on the Properties tab, and then click OK.

   The Kerberos Server, Realm and the credentials used for the connection are specified.
5. Complete the fields on the Endpoint Settings tab.

   The various settings that apply to controlling endpoints, such as password propagation and synchronization are specified.
6. Complete the fields on the Program Exits Reference tab.

   Program exits are viewed added edited or removed as specified.
7. Complete the fields on the Custom Settings tab.

   The supported encryption types and salt pairs for this endpoint are specified.
8. Complete the fields on the Attribute Mapping tab.

   The default attribute mapping defined in the schema file for the endpoint type are specified.
9. Complete the fields on the Logging tab.

   The logging settings for the new endpoint are specified.
10. Click Apply.

**More information:**

KRB Directory Tab (see page 216)
Endpoint Custom Settings Tab (see page 217)
KRB Endpoint Property Sheet (see page 215)

## Modify an Endpoint

You can modify the parameters of an already registered KRB endpoint, such as the default account template used and the authentication mode used.

**Note:** If you modify any of the connection-related fields (for example, kerberos server, port, realm, security credentials), the connector will, as when acquiring a new endpoint, run a kadmin command to validate the changed values.

**To modify an endpoint**

1. In the Provisioning Manager, acquire the endpoint you want to modify.
2. Explore and correlate the endpoint you want to modify.
3. In the EndpointName column on the leftmost side of the Provisioning Manager, double-click the endpoint you want to modify.

   The KRB Endpoint Property Sheet dialog appears.
4. Modify the fields on the KRB Endpoint tab as required, and then click OK.

   **Note:** You can only change comments and the default account template. You cannot change the name of the endpoint.
5. Modify the fields on the Properties tab as required, and then click OK.

   You have specified the Kerberos Server, Realm and the credentials used for the connection.
6. Complete the fields on the Endpoint Settings tab.

   The various settings that apply to controlling endpoints, such as password propagation and synchronization are specified.
7. Complete the fields on the Program Exits Reference tab.

   Program exits are viewed added edited or removed as specified..
8. Complete the fields on the Custom Settings tab.

   The supported encryption types and salt pairs for this endpoint are specified.
9. Complete the fields on the Attribute Mapping tab.

   The default attribute mapping defined in the schema file for the endpoint type are specified.
10. Complete the fields on the Logging tab.

    The logging settings for the new endpoint are specified.
11. Click Apply.

**More information:**

KRB Directory Tab (see page 216)
Endpoint Custom Settings Tab (see page 217)

## Change Administrator Passwords

If the admin principal password has been changed or reset or due to expire, you can update the Provisioning Directory with the new password.

**Note:** You cannot update the password for an endpoint that uses keytab.

**To change administrator passwords**

1. In the Provisioning Manager, acquire the endpoint you want to view principals for.
2. Explore and correlate the endpoint you want to view principals for.
3. In the EndpointName column on the leftmost side of the Provisioning Manager, double-click on the endpoint you want to change the administrator password for.

   The KRB Endpoint Property Sheet appears.
4. Click the Properties tab.

   The Properties tab appears.
5. Complete the Password field on the Properties tab.

   The password for the principal is specified.
6. Click Apply.

   The updated password is applied.

## Explore and Correlate Principals

You can correlate the explored principals with global users.

**To explore and correlate principals**

1. In the Provisioning Manager, right-click on an acquired KRB endpoint and then click Explore/Correlate.

   The Explore and Correlate Endpoint dialog appears.
2. Complete the fields on the Explore and Correlate Endpoint dialog.
3. Click Start.

   The Explore & Correlate Principals process starts.

   When the process is finished, the Provisioning Manager displays the number of objects created in the endpoint in the Results section of the Explore and Correlate Endpoint dialog.

## View All Principals

After you acquire an endpoint you can view all principals, or you can specify search criteria to view specific principals.

**To view all principals**

1. In the Provisioning Manager, acquire the endpoint you want to view principals for.
2. Explore and correlate the endpoint you want to view principals for.
3. In the EndpointName column on the leftmost side of the Provisioning Manager, right-click on an endpoint and click Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select KRB Accounts.
5. Complete the fields on the Endpoint Content dialog as required, then click Search.

   The Provisioning Manager displays the KRB accounts in the endpoint in the KRBAccount column.
6. In the main the Provisioning Manager window, double-click the KRB principal you want to view the properties for.

   The KRB Account Property sheet appears and displays the KRB account settings.

**More Information:**

KRB Account Property Sheet (see page 218)

## Add a Principal

After you acquire an endpoint, you can add principals as required.

**To add a principal**

1. In the Provisioning Manager, acquire the endpoint you want to add principals to.
2. Explore and correlate the endpoint you want to add principals to.
3. In the EndpointName column on the leftmost side of the Provisioning Manager, right-click on an endpoint and then click Content.
4. The Endpoint Content dialog appears.
5. In the Container tree, select KRB Accounts.
6. Click New.

   The KRB Account Property sheet appears and displays the KRB account settings.
7. Complete the fields on the Profiles tab.

   The userid and provisioning status information are specified.
8. Complete the fields on the Account Properties tab.

   The account properties of the principal and account template are specified.
9. (Optional) Click enc:salt.

   The Encryption Type and Salt Pairs dialog appears.

   Complete the fields on the Encryption Type and Salt Pairs dialog, and then click OK.

   The encryption types and salt pairs are specified.
10. Click OK.

    Kerberos adds the principal you specified.

**More Information:**

Acquire a New Endpoint (see page 200)
Naming Limitations (see page 181)
Profiles Tab (see page 218)
Account Properties Tab (see page 219)
Encryption Type and Salt Pairs Dialog (see page 224)

## Modify a Principal

You can modify the properties of a principal such as user options and the associated the KRB account templates.

**To modify a principal**

1. In the Provisioning Manager, acquire the endpoint that contains the principal you want to modify.
2. Explore and correlate the endpoint that contains the principal you want to modify.
3. In the EndpointName column on the leftmost side of the Provisioning Manager, right-click on an endpoint and then click Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select KRB Accounts.
5. Complete the fields on the Endpoint Content dialog as required, then click Search.

   The Provisioning Manager displays the KRB accounts in the endpoint in the KRBAccount column.
6. In the main Provisioning Manager window, double-click the KRB principal you want to modify the properties for.

   The KRB Account dialog appears and displays the KRB account settings.
7. Complete the fields on the Profiles tab.

   The userid and provisioning status information are specified.
8. Complete the fields on the Account Properties tab.

   The account properties of the principal and account template are specified.
9. (Optional) Click enc:salt.

   **Note:** The enc:salt button is only available if you select the Choose Random Password check box or if you modify the Password field.

   The Encryption Type and Salt Pairs dialog appears.

   Complete the fields on the Encryption Type and Salt Pairs dialog, and then click OK.

   The encryption types and salt pairs are specified.
10. Complete the fields on the Account Templates tab.

    The account properties of the principal are specified.
11. Click OK.

    Kerberos modifies the principal you specified.

**More Information:**

Acquire a New Endpoint (see page 200)
Explore and Correlate Principals (see page 202)
Profiles Tab (see page 218)
Account Properties Tab (see page 219)
Encryption Type and Salt Pairs Dialog (see page 224)

## Delete a Principal

Once you have explored an endpoint, KRB principals can be deleted as required.

**To delete a principal**

1. In the Provisioning Manager, acquire the endpoint that contains the principal you want to delete.
2. Explore and correlate the endpoint that contains the principal want to delete.
3. In the KRB Account column, right-click the principal you want to delete, then click Delete.
4. When prompted, confirm that you want to delete the principal.

   The Provisioning Manager removes the Kerberos principal from the Kerberos database.

## Duplicating a KRB Account

When you duplicate a KRB account, you must make sure the following attributes are duplicated properly:

- eTKRBPasswordExpireDateTime
- eTKRBUserExpireDateTime
- eTKRBEncSalts
- eTKRBMaxTicketLife
- eTKRBMaxTicketRenewLife

## Kerberos Default Account Template

The Kerberos default account template, provided with the Kerberos Connector, gives a user the minimum security level needed to log in using Kerberos authentication. You can use it as a model to create new account templates. The account template contains the following values:

| Account Template | Value |
|---|---|
| -expiry dates | Never |

| Account Template | Value |
|---|---|
| -ticket lives | Connector specified defaults |
| -flags | Default Kerberos flags |
| -password policy | None |

## View KRB Account Templates

You can view all KRB account templates, or you can specify search criteria to view specific KRB account templates.

To view password policies, you can specify search criteria to view all or specific KRB password policies.

**To view KRB account templates**

1. Click the Roles button.
2. In the Object Type list, select KRB Policy, then click Search.

   The Provisioning Manager displays the KRB account templates in the AccountTemplateName column.

## Add a KRB Account Template

After you acquire an endpoint, you can add KRB account templates as required.

**To add a KRB account template**

1. Click the Roles button.
2. In the Object Type list, select KRB Policy, then click New.

   The  KRB Account Template dialog appears.
3. Click the  Account Template tab.

   The Account Template tab appears.
4. Complete the fields on the Account Template tab.

   The Provisioning Manager specifies general information about the Account Template.
5. Complete the fields on the Profiles tab.

   The Provisioning Manager specifies the attribute values of the principal.
6. Complete the fields on the Account Properties tab.

   The Provisioning Manager specifies the attribute values of the principal.

7. (Optional) Click enc:salt.

   The Encryption Type and Salt Pairs dialog appears.

8. Complete the fields on the Encryption Type and Salt Pairs dialog, and then click OK.

   The Provisioning Manager specifies the encryption types & salt pairs.

9. Complete the fields on the Program Exits Reference dialog.

   The Provisioning Manager specifies the Program Exits.

10. Complete the fields on the Workflow tab.

    The Provisioning Manager assigns approvers to an account template.

11. Complete the fields on the KRB Endpoints tab.

    The Provisioning Manager populates the password policies on the Account Properties tab.

12. Complete the fields on the Roles tab.

    The Provisioning Manager associates the provisioning roles with KRB account templates.

13. Click OK.

    The Provisioning Manager creates a new KRB account template.

**More Information:**

KRB Account Property Sheet (see page 218)
Profiles Tab (see page 218)
KRB Endpoints Tab (see page 223)

## Modify a KRB Account Template

You can modify the properties of a KRB account template such as attributes and the encryption types and salt pairs.

**To modify a KRB account template**

1. Click the Roles button.
2. In the Object Type list, select KRB Policy, then click Search.

   The  KRB Account Template dialog appears.
3. Click Search.

   The Provisioning Manager displays the KRB account templates in the AccountTemplateName column.
4. In the AccountTemplateName column, right click the account template you want to modify.
5. To modify general information about an account template, complete the fields on the Account Template tab.
6. To modify the attribute values of a principal, complete the fields on the Profiles tab.

   The Account Template Property dialog displays.
7. To modify the attributes of a principal, complete the fields on the Account Properties tab.
8. To modify the encryption types & salt pairs, do the following:

   a. Click enc:salt.

      The Encryption Type and Salt Pairs dialog appears.

      **Note:** The enc:salt button is only available if you select the Choose Random Password check box or if you modify the Password field.

   b. Complete the fields on the Encryption Type and Salt Pairs dialog, and then click OK.

      **Note:** The enc:salt and random passwords are account template-only attributes, and so changes will not be propagated to associated accounts.
9. To modify program exits, complete the fields on the Program Exits Reference dialog.
10. To assign approvers to a account template, complete the fields on the Workflow tab.
11. To associate provisioning roles with KRB account templates, complete the fields on the Roles tab.
12. Click OK.
13. When prompted, confirm that you want to apply the changes to the associated accounts.

**More information:**

Profiles Tab (see page 218)
KRB Endpoints Tab (see page 223)

## Delete a KRB Account Template

You can delete KRB account templates as required.

**Note:** You may not be able to delete the account template if there are accounts that have this template assigned.

**To delete a KRB account template**

1. Click the Roles button.
2. In the Object type list, select KRB Policy.
3. Click Search.

   The Provisioning Manager displays the KRB account templates in the AccountTemplateName column.
4. In the Provisioning Manager, right click the KRB account template you want to delete and then click Delete.
5. When prompted, confirm that you want to delete the KRB account template.

## Synchronize Accounts with Account Templates

To synchronize an account with a KRB account template, right-click on the KRB account template and select Synchronize Accounts with Account Template.

## View a KRB Password Policy

After you acquire an endpoint you can view all KRB password policies, or you can specify search criteria to view specific KRB password policies.

**To view a KRB password policy**

1. In the Provisioning Manager, acquire the endpoint you want to view password policies for.
2. Explore and correlate the endpoint you want to view password policies for.
3. In the EndpointName column, right-click the endpoint you want to view password policies for, then click Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select KRB Password Policies.
5. Complete the fields on the Endpoint Content dialog as required, then click Search.
6. In the main the Provisioning Manager window, double-click the KRB password policy you want to view the properties for.

   The Password Policy Properties dialog appears and displays the parameters of the password policy.

**More information:**

Acquire a New Endpoint (see page 200)
Explore and Correlate Principals (see page 202)
Password Account Template Properties Tab (see page 222)

## Add a KRB Password Policy

After you acquire an endpoint, you can add KRB password policy as required.

**To add a KRB password policy**

1. In the Provisioning Manager, acquire the endpoint you want to view password policies for.
2. Explore and correlate the endpoint you want to view password policies for.
3. In the EndpointName column, right-click the endpoint you want to add a password policy for, then click Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select KRB Password Policies.
5. Click New.

   The Password Policy Properties dialog appears.
6. Complete the fields on the Password Policy Properties dialog, and then click OK.

   The connector creates the password policy in the endpoint, and is now available to be assigned to principals.

**More information:**

Acquire a New Endpoint (see page 200)
Explore and Correlate Principals (see page 202)
Password Account Template Properties Tab (see page 222)

## Modify a KRB Password Policy

After you acquire an endpoint, you can modify KRB password policies as required.

When you modify a Kerberos password policy, the accounts that refer to that policy are not affected until the account's password is changed. When the password is changed, the new password must conform to the properties of the modified policy.

**Note:** If the password policy is assigned to principals, you can only modify the account template in a way that is below the current rule enforcement. For example, if the minimum password length is specified as eight characters, you cannot change it to ten characters.

**To modify a KRB password policy**

1. In the Provisioning Manager, acquire the endpoint you want to view password policies for.
2. Explore and correlate the endpoint you want to view password policies for.
3. In the EndpointName column, right-click the endpoint you want to view password policies for, then click Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select KRB Password Policies.
5. Complete the fields on the Endpoint Content dialog as required, then click Search.

   The Provisioning Manager displays the password policies in the main Provisioning Manager window.
6. In the main Provisioning Manager window, double-click the KRB password policy you want to modify the properties for.

   The Password Policy Properties dialog appears.
7. Modify the fields on the Password Properties dialog as required, and then click OK.

   The Provisioning Manager modifies the password policy.

**More information:**

Password Account Template Properties Tab (see page 222)

## Delete a KRB Password Policy

After you acquire an endpoint, you can delete KRB password policies as required.

**Note:** You cannot remove a password policy if a principal is assigned to it.

**To delete a KRB account template**

1. In the Provisioning Manager, acquire the endpoint you want to view password policies for.
2. Explore and correlate the endpoint you want to view password policies for.
3. In the EndpointName column, right-click the endpoint you want to view password policies for, then click Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select KRB Password Policies.
5. Complete the fields on the Endpoint Content dialog as required, then click Search.

   The Provisioning Manager displays the password policies in the main Provisioning Manager window.
6. In the Provisioning Manager, right click the KRB password policy you want to delete, then click Delete.
7. When prompted, confirm that you want to delete the password policy.

   The connector removes the password policy from the endpoint.

**More information:**

Acquire a New Endpoint (see page 200)
Explore and Correlate Principals (see page 202)

## KRB Endpoint Property Sheet

Use this property sheet to register or view the properties of a Kerberos endpoint. The following property pages apply to Kerberos endpoints:

**KRB Endpoint**

Specifies information about the endpoint.

**Endpoint Settings**

Specifies endpoint attributes.

**Properties**

Specifies the Kerberos Sever and Realm and the credentials used for connection.

**Custom Settings**

Specifies the supported encryption type and salt pairs of the endpoint and how the disablement of the principal is implemented.

**Program Exits Reference**

Specifies the priority, name, and type of program exit to be used.

**Attribute Mapping**

Specifies endpoint mapping configuration information.

**Logging**

Specifies logging information.

**Statistics**

Provides read-only information reporting on activity for this object.

The fields in this property sheet are listed below:

**OK/Apply**

Accepts or saves the information in the property sheet or dialog.

**Cancel/Reset**

Exits or resets the values in the property sheet or dialog.

## KRB Directory Tab

Use this tab to register or view the properties of a Kerberos endpoint.

The fields in this tab are listed below:

**Directory Name**

Specifies the name of the Kerberos directory.

**Size/Type**: 1 to 100 characters

This is a required field.

**Comments**

User-supplied description field.

**Size/Type**: 1 to 128 characters

**Default Domain**

Specifies the name of the domain where the default account template exists.

This drop-down list box displays your personal domain list only. This list is a local list and is unique for each account on the client workstation. This list is intended for the domains that you use frequently. Selecting a domain from this list does not require a request to a network server and is therefore very fast.

To display and access every domain in your entire network, click the Domains button. When you do so, you can add one or more domains to your personal domain list.

**Default Account Template**

Specifies the default account template of the endpoint.

The default account template is used to create new accounts on the endpoint. You must define a default account template to activate the drag-and-drop feature on an organization or organizational unit. If the organization or organizational unit is not associated with an account template, the default account template at the tree level is applied.

The drop-down list box contains all the account templates defined for KRB endpoints.

**Domain**

Displays every domain in the entire network and makes them available for you to access. Clicking this button displays the Full Domain List Selector dialog.

If desired, you can add one or more of these domains to your personal domain list, which is stored in the Default Domain drop-down list box.

Clicking the Domain button issues a request to a network server, and may take longer than using the Default Domain drop-down list box.

**More Information:**

KRB Endpoint Property Sheet (see page 215)

## Endpoint Custom Settings Tab

Use this tab to specify the supported encryption type and salt pairs for the endpoint.

The fields in this tab are listed below:

**Supported Encryption Type and Salt Pairs List Box**

When acquiring a directory for the first time, this list is pre-populated with the following six items:

- aes128-cts-hmac-sha1-96:normal
- arcfour-hmac-md5:normal
- arcfour-hmac-md5-exp:normal
- des-cbc-crc:normal
- des-cbc-md5:normal
- des3-cbc-sha1:normal

You can also manually add the type and pairs here and they will be made available at the Principal and Account Template property sheets. Once the pairs have been added, you can select a pair to be removed or edited.

To remove an encryption type and salt pair from this list box, select the encryption type and salt pairs and click the down arrow (Delete).

**Supported Encryption Type and Salt Pairs**

Specifies the supported encryption type and salt pairs to be added for this endpoint. To add an encryption type and salt pair, type the encryption type and salt pair in this field and click the up arrow (Add).

**Disable Principal Will Set "ALLOW TIX" to False**

When checked, specifies that the DISALLOW_ALL_TIX flag is set when the principal is disabled. This results in the suspended principal’s ALLOW TIX check box on the Account Properties Tab to be unchecked.

**Disable Principal Will Expire the Principal**

When checked, specifies that the expiration date is set to a date in the past so that the principal is disabled.

**More Information:**

KRB Endpoint Property Sheet (see page 215)

## KRB Account Property Sheet

Use this property sheet to create, view, or modify the current properties of a KRB account. The following property pages apply to KRB accounts:

**Profiles**

Specifies user information such as userid and status information of the account.

**Account Properties**

Specifies account properties including the password, password account template, and advanced Kerberos options.

**Account Templates**

Maintains account template inclusions.

**Statistics**

Provides read-only information reporting on activity for this object.

The fields in this property sheet are listed below:

**OK/Apply**

Accepts or save the information in the property sheet or dialog.

**Cancel/Reset**

Exits or reset the values in the property sheet or dialog.

## Profiles Tab

Use this tab to view and modify the userid and provisioning status information.

The fields in this tab are listed below:

**Userid**

Specifies the name of the Kerberos principal.

**Rule String:** %AC%

This is a required field.

**Provisioning information: Status**

Specifies whether or not the user profile is suspended:

- 0 - active
- 1 - suspended

**More Information:**

KRB Account Property Sheet (see page 218)
KRB Account Template Property Sheet (see page 221)

## Account Properties Tab

Use this tab to view and modify the account properties of a principal and account template.

The fields in this tab are listed below:

**Password**

Specifies the password of the Kerberos principal.

**Size/Type**: 0 to 64 alpha-numeric characters

**Rule String**: %p%

**Choose Random Password Check Box**

When checked, specifies that the password of the principal is randomly generated. The generated password conforms to the selected password account template.

**enc:salt Button**

Displays the Encryption Type and Salt Pairs dialog where you can view or edit the encryption types and key salt pairs.

**Note:** If there is no password change, the dialog is read-only. If the password is changed or Choose Random Password is selected, the dialog is enabled and can be edited.

**Maximum Ticket Life**

Specifies the maximum ticket life of the Kerberos principal in days, hours minutes and seconds.

**Maximum Renewable Life of a Ticket**

Specifies the maximum renewable life of a ticket for the Kerberos principal in days, hours, minutes and seconds.

**Password Account Template**

Specifies the password account template that is assigned to the principal.

**Size/Type:** up to 128 alpha-numeric characters

**Expiration Date Time: User**

Specifies the expiration date of the principal.

**Expiration Date Time: Password**

Specifies the expiration date of the principal's password.

**ALLOW POST DATED Check Box**

When checked, specifies that the principal is can receive post-dated tickets.

**ALLOW PROXIABLE**

When checked, specifies that the principal can receive proxiable tickets.

**REQUIRES HWAUTH**

When checked, specifies that the principal must pre-authenticate using a hardware device before being allowed to kinit.

**ALLOW TIX**

When checked, specifies that the principal can be issued tickets.

**ALLOW FORWARDABLE**

When checked, specifies that the principal can receive forwardable tickets.

**ALLOW DUP SKEY**

When checked, specifies that the principal can receive a session key for another user.

**ALLOW SVR**

When checked, specifies service tickets can be issued to this principal.

**NEED PWD CHANGE**

When checked, specifies that a flag is set to force a password change.

**ALLOW RENEWABLE**

When checked, specifies that the principal is *not* prohibited from obtaining renewable tickets.

**REQUIRES PREAUTH**

When checked, specifies that the principal must pre-authenticate before being allowed to kinit.

**ALLOW TGS REQ**

When checked, specifies that a Ticket-Granting Service request for a service ticket is permitted for this principal.

**PWD CHANGE SERVICE**

When checked, specifies that a flag is set to mark this principal as a password change service.

**More Information:**

KRB Account Property Sheet (see page 218)
KRB Account Template Property Sheet (see page 221)

## KRB Account Template Property Sheet

Use this property sheet to create, view, or modify the current properties of a KRB account template. The following property pages apply to KRB account templates:

**Account Template**

Specifies general information about an account template.

**Profiles**

Specifies the userid of the principal.

**Account Properties**

Specifies the account properties of the account template including password, password account template, and advanced Kerberos options.

**Program Exits Reference**

Specifies the priority, name, and type of program exit to be used.

**Workflow**

Specifies the name of the technical approver for this account template.

**KRB Endpoints**

Maintains endpoint group inclusions.

**Roles**

Maintains provisioning role inclusions.

**Statistics**

Provides read-only information reporting on activity for this object.

The fields in this property sheet are listed below:

**OK/Apply**

Accepts or saves the information in the property sheet or dialog.

**Cancel/Reset**

Exits or resets the values in the property sheet or dialog.

## Password Account Template Properties Tab

Use this tab to add a new or modify an existing password account template.

The fields in this dialog are listed below:

**Account Template Name**

Specifies the name of a Kerberos password account template.

**Size/Type:** 1 to 128 alphanumeric characters.

This is a required field.

**Description**

Specifies the description of the password account template.

This description only exists in the Provisioning repository.

**Size/Type:** 1 to 128 alphanumeric characters.

**Maximum Password Life**

Specifies the maximum password life in days, hours, minutes, and seconds.

**Minimum Password Life**

Specifies the minimum password life in days, hours, minutes, and seconds.

**Minimum Password Length**

Specifies the minimum password length in number of characters.

**Minimum Number Password Character Class**

Specifies the minimum number of password characters. You can choose one of the following valid values:

- 1 - only letters
- 2 - both letters and numbers
- 3 - letters, numbers, and punctuation

**Number of Old Keys Kept**

Specifies the number of old keys to be kept to disallow reuse.

**Reference Count**

Specifies the number of principals that reference this password account template.

This is a read-only field.

## KRB Endpoints Tab

Use this tab to associate one or more KRB endpoints in order to pre-populate password policies on the Account Property Tab.

The fields on this page are listed below:

**Available**

Specifies the objects that are available for inclusion.

**Included**

Specifies the objects that have been added as inclusions.

**Add**

After selecting an object in the Available list, click the Add (>) button to add it to the Included list.

**Add All**

After selecting an object in the Available list, click the Add All (>>) button to add all the objects to the Included list.

**Remove**

After selecting an object in the Included list, click the Remove (<) button to remove it to the Available list.

**Remove All**

After selecting an object in the Included list, click the Remove All (<<) button to remove all the objects to the Available list.

**Domain**

Specifies the domain for the search.

**Domain**

Displays the Full Domain List Selector dialog to add domains to the Domain field.

**Attribute**

Specifies a simple attribute that is used to search.

**Advanced**

Displays the Advanced Search Attributes dialog. Use this dialog to set more advanced search criteria.

**Tip**: This is useful if you want to narrow down the list of objects in the class. Click the Search button to start the search.

**Value**

Specify a value in the Value field to restrict the search criteria, and click the Search button. By default, the wildcard character (*) is specified, which causes the search to return all entries.

**Note**: If you perform an advanced search for an attribute, this field is disabled.

**Search**

Starts the search.

**More Information:**

KRB Account Template Property Sheet (see page 221)

## Encryption Type and Salt Pairs Dialog

Use this dialog to view and edit the encryption type and salt pairs.

The fields in this dialog are listed below:

**Available List Box**

Specifies the encryption types and salt pairs that are available.

**Add Button**

Adds the selected available pair into the Included List box.

**Note:** If you try to add two pairs of the same type, only one will be added.

**Remove Button**

Removes the selected pair from the Included List Box.

**Included List Box**

Specifies the encryption type and salt pairs that have been included. Once you have clicked OK, the pairs are kept in memory and committed to the KDC together with the password change of the principal.

If there are invalid entries, an error message is displayed. To correct the error, you must go back to the Customization Tab of the endpoint property sheet.

**Note**: The encryption type and salt pairs listed here are sorted per Java's implementation of the natural ordering of strings. When two similar encsalts are passed to Kerberos, only the first one is used. For example, if both des-cbc-crc:normal and des-cbc-md5:normal are listed, only des-cbc-crc:normal is used because "c" has a lower value than "m".

## Known Issues

This section contain the following topics:

Account Creation Fails with Invalid Date Specification (see page 225)

Account Creation Fails with Parameter is Incorrect (see page 225)

## Invalid Date Specification on Account Creation

**Valid on Windows and Solaris**

**Symptom:**

When I enter an account expiry date greater than 2038 in the User or Password Expiration fields on the Account on the Account Properties tab on the KRB Account dialog I receive an invalid date specification message.

**Solution:**

Enter a date before 2038. kadmin only supports dates from 1970 to 2038.

## Account Creation Fails with Parameter is Incorrect

**Valid on Windows and Solaris**

Symptom:

When I enter an account expiry date greater than 2038 in the User or Password Expiration fields on the Account on the Account Properties tab on the KRB Account dialog I receive an invalid date specification message.

**Solution:**

Enter a date before 2038. kadmin only supports dates from 1970 to 2038.

# LDA Connector Migration to DYN JNDI

You can perform a migration of the LDA C++ connector included in CA IdentityMinder r12, to DYN JNDI in the current release of CA IdentityMinder. The migration changes the parser table from LDA to DYN, and changes the connector implementation.

The LDAMigrate script provides support for the migration of the LDA Connector to DYN JNDI  and is part of the CA IAM CS installation.

**Note:** You must upgrade or install the r12.6.1 CA IAM CS and register it with the CA IdentityMinder Provisioning Server before running the migration.

When you upgrade to CA IdentityMinder, the upgrade process retains all existing LDA data. Retaining all existing data lets you run the LDA Connector migration against the environment. However, the LDA connector is not functional after you upgrade. The LDA connector is not functional because the migration does not update the LDA connector and the CA IdentityMinder Provisioning Manager GUI plug-in to the new version of Visual Studio.

**Note:** A new CA IdentityMinder installation does not install any LDA components, such as parser tables, the C++ Connector, or the CA IdentityMinder Provisioning Manager plug-in.

## Custom Extensions to the LDA Schema

The LDA connector included an SDK that allowed you to make custom extensions to the LDA schema. To make custom extensions, you ran a make step that created a customized parser table, and created a custom CCS connector and CA IdentityMinder Provisioning GUI DLLs.

If you have made extensions to the LDA schema, copy the.txt files describing your auxiliary class extensions to the correct directory before you start the LDAMigrate script.

## Vendor Support

For a list of vendors that support the inetOrgPerson schema (with minor variations), see the CA IdentityMinder support matrix on the CA Support Site.

## How the LDAMigrate Script Migrates the LDA Connector

During the migration, the LDAMigrate script does the following:

- Rolls the LDA extension mapping files from the mappings/ directory into an equivalent metadata document against the DYN schema (including visual grouping metadata). The LDAMigrate script then uses this document to create a DYN JNDI namespace named LDAP DYN.
- Copies all LDA directories and LDA account templates to the new DYN JNDI namespace.
- Updates all provisioning roles referencing LDA account templates to reference the equivalent DYN JNDI account templates.
- Creates a DYN JNDI namespace named LDAP DYN which replaces the superseded LDA namespace.
- Creates equivalents to any existing LDA directories under LDAP DYN.
- Creates equivalents of all existing LDA account templates under LDAP DYN.

**Note:** Before running the migration script, you must be able to contact the LDA endpoint because the LDAMigrate script must validate the password. To ensure that the migration runs smoothly:

- Wait until the endpoint becomes available before running the LDAMigrate script (preferred method), or
- Skip the unavailable endpoint by entering 'B' for its password when prompted by LDAMigrate.

### Migration Phases

The migration consists of two phases. During the migration, the LDAMigrate script does the following:

- Constructs DYN metadata (see page 227) for existing (possibly customized through custom extensions) LDA parser tables and schemas.
- Creates equivalent DYN objects (see page 229) that match existing LDA objects.

## DYN Metadata Construction

The LDAMigrate script uses some in-built base DYN JNDI metadata documents as a starting point.

These base metadata documents include the matching LDA attribute name for each DYN attribute in their <doc> sections. The LDAMigrate script captures this mapping information in the .properties files written to the mappings/ directory.

If you specify that you have extensions to the LDA schema during the migration process, the script appends the extensions to the base metadata.

The migration process writes the compiled metadata and some supporting .properties files showing the LDA to DYN attribute to the mappings/ directory.

During this phase of the migration, you can review the output metadata, make any manual adjustments if necessary, and ask the script to read the file you edited again.

## DYN Object Creation

After the migration process calculates metadata for the new endpoint type, the script prompts you for the connection details to a target CA IdentityMinder Provisioning Server. The migration process makes the following changes to the Provisioning Server that you specified:

- Creates a DYN JNDI endpoint type named LDAP DYN and populates the endpoint with the calculated metadata. The LDA namespace remains unchanged.
- Searches under the LDA namespace and clones any directories discovered into equivalent DYN endpoints under the LDAP DYN endpoint type. This process maps LDA attributes on directories to their DYN equivalents. The migration script prompts you for the password for each directory, because the migration process cannot discover the passwords. The migration does not affect the LDA directories.
- Searches and clones all LDA account templates (policies) by mapping their LDA attributes to their DYN equivalents, and puts them in the following container:

  ```
  eTDYNPolicyContainerName=DYN Policies, eTNamespaceName=LDAP DYN,…
  ```

  **Note:** The migration process does not affect the LDA account templates.
- Searches for all role and account template inclusions which name LDA account templates. The script changes all references to point to the equivalent DYN account templates, optionally deleting the existing LDA references. This deletion is the only change that the script makes to the LDA data that existed before the migration.
- Creates a list of the existing LDA inclusions in the LDAMigrate.log file.
- Performs the policy and directory inclusions migration.

  For example, the script creates a clone of an entry in the first container in the second container listed, as shown in the following example:

  ```
  eTSubordinateClass=eTLDADirectory,eTSuperiorClass=eTLDAPolicy,eTInclusionCont
  ainerName=Inclusions,eTNamespaceName=CommonObjects,dc=…
  ```

  ```
  eTSubordinateClass=eTDYNDirectory,eTSuperiorClass=eTDYNPolicy,eTInclusionCont
  ainerName=Inclusions,eTNamespaceName=CommonObjects,dc=…
  ```

## How to Perform the LDA Connector Migration

To perform the LDA Connector migration, do the following:

1. Upgrade your CA IdentityMinder installation to r12.6.1.

   The installation preserves all LDA data.

2. Run the LDA migration script specifying the file names of any custom LDA extension files you have made.

3. Reexplore and recorrelate your new LDAP DYN endpoints and validate their behavior. (see page 232)

4. Synchronize global users with roles.

   **Note:** For more information, see *Synchronize Global Users or Roles* in the *Administration Guide*.

5. Remove LDA data. (see page 233)

6. Reactivate program exits manually.

   **Note:** Although the script migrates program exits, you still need to reactivate program exits manually.

7. (Optional) Remove the LDAMigrate log files.

**Note:** To perform a new mapping, manually remove the output .xml and .properties files from the mappings/ directory, and then rerun the LDA migration.

## Run the LDA Migration Script

To migrate the LDA connector, run the LDAMigrate scripts.

**To run the LDA migration script**

1. If you have made extensions to the LDA schema, copy any relevant LDA extension mapping .txt files to the following directory:

   *cs-home*/resources/jndi/mappings/

2. (Windows) Do the following:

   a. Open a command prompt window.

   b. Navigate to following folder of the connector server:

      *cs-home*/resources/jndi

   c. Enter the following command, including the file names of any custom LDA extension files you have made.

      LDAMigrate

      **Example:** LDAMigrate mappings\myext1.txt mappings\myext2.txt

3. (UNIX) Do the following:

   a. Open a terminal window.

   b. Navigate to the bin folder of the connector server:

      *cs-home*/resources/jndi

   c. Enter the following command, including the file names of any custom LDA extension files you have made:

      LDAMigrate

      **Example:** LDAMigrate mappings/myext1.txt mappings/myext2.txt.

   **Important! (Windows and UNIX)** The order in which you specify these files defines the order in which the screens appear for the extensions in the CA IdentityMinder Provisioning Manager, and the CA IdentityMinder GUIs.

   **Note:** If you do not provide any extension files, the unextended LDA schema is migrated.

4. If you are running the migration for the first-time, the process prompts you for connection details to a provisioning server.

   The script displays default connection details in square [] brackets.

   **Note:** For security reasons, the migration process does not echo password characters.

   After the script makes a successful connection to the provisioning server, the script saves all the connection details, except the password. The migration script runs a query that finds all the existing LDA endpoints that are registered on the provisioning server.

5. When prompted, confirm that you want to review the metadata generated to match your .txt mapping files. Do the following:

   a. Edit the dyn_ldap_metadata.xml file in the following location:

      *cs-home*/resources/jndi/mappings/dyn_ldap_metadata.xml

   b. Make any manual adjustments required.

   c. Confirm that you want the script to read the manually adjusted file again.

6. When prompted, confirm that you want clean LDA inclusions.

   **Note:** If you do not confirm that you want to clean up LDA inclusions, then delete any LDA inclusions manually. Deleting the files helps ensure the roles that reference them are usable, as there is no LDA connector in CA IdentityMinder r12.6.1.

7. When prompted, confirm that you want to delete the obsolete LDA references.

   **Note:** You can safely delete the obsolete references as all role to LDA account template links are logged to LDAMigrate.log. Also, the roles are not functional until the LDA references are deleted (either automatically or manually).

8. When prompted, enter the password for each endpoint.

   When the migration process makes a successful connection to the LDA endpoint, the migration saves the connection details in the provisioning server and the data migration starts.

   The name of the newly created endpoint type is LDAP DYN.

## Reexplore and Recorrelate the New LDAP DYN Endpoints

After the migration is complete, we recommend that you reexplore and recorrelate your new LDAP DYN endpoints and validate their behavior. Adjust the data on the endpoints in the cases where there are:

- Direct inclusions between global users and account templates, but a role was not used to establish these links.
- Incorrect inclusions that the correlation established that you adjust manually.
- Configuration settings such as preferred exploration algorithm, which are persisted externally to the namespace and Directory objects.

We recommend that you correlate using the Use existing global users option. As you are doing a migration, all the required global users should already exist. If correlation attributes were not set correctly then using this option prevents the creation of unexpected global users. Once the corelation is complete, you can validate whether the accounts linked to the [default user] are expected or not. If it is necessary to create a Global User, then start a new correlation with the Create Global User as needed option. Starting a correlation with this option helps ensure that the correlation does not create a large amount of spurious accounts.

## Remove LDA data

To remove all LDA data, validate the LDAP DYN endpoint, then run the cleanendpointtype utility included with the CA IdentityMinder Provisioning Server.

**Valid on Windows and UNIX**

**To remove LDA data**

1. Copy the deprecated endpoint's .dxc or .schema file (for example, etrust_lda.dxc) into the cleanendpointtype directory.

   The cleanendpointtype utility will find these files when you run it based on the file extension.

2. (Windows) Enter *either* of the following commands from the cleanendpointtype sub-directory of either the Provisioning Directory or the Provisioning Server:

   ```
   C:\Program Files\CA\Identity Manager\Provisioning Directory\cleanendpointtype
   -password <password>
   ```

   ```
   C:\Program Files\CA\Identity Manager\Provisioning Server\cleanendpointtype
   -password <passwordfile.txt>
   ```

3. (UNIX) Enter *either* of the following commands from the cleanendpointtype sub-directory of either the Provisioning Directory or the Provisioning Server:

   ```
   /opt/CA/IdentityManager/ProvisioningDirectory/cleanendpointtype -password
   <password>
   ```

   ```
       /opt/CA/IdentityManager/ProvisioningServer/cleanendpointype/cleanendpoint
       type <passwordfile.txt>
   ```

   The cleanendpointtype utility removes all LDA data from the endpoint.

## Cleanendpointtype Utility

The cleanendpointtype utility removes all LDA data from the endpoint.

This command has the following format for both UNIX and Windows:

```
cleanendpointtype {-password <password>} [-hostname <hostname>] [-port CA Portal]
[-username <username>] [-filename  "[set the File Name variable]"] [-readonly]
[-createundo] [-verbose]
```

**-password <password>**

(Required) Specifies the password string or the filename that contains the password required to connect to the Provisioning Directory.

**-hostname <hostname>**

(Required if the Provisioning Directory is installed on a different computer) Specifies the hostname for the Provisioning Directory.

**Default:** local hostname

**-port CA Portal**

(Optional) Defines the port for the Provisioning Directory.

**Default**: 20394

**-username <username>**

(Optional) Defines the username to connect to the Provisioning Directory.

**Default:**
eTDSAContainerName=DSAs,eTNamespaceName=CommonObjects,dc=etadb)

**-filename "[set the File Name variable]"**

(Optional) Specifies the relative or absolute filename(s) for deprecated dxc/schema file(s), comma-delimited. If not specified, the utility uses all .dxc and .schema files in the current directory.

**-readonly**

(Optional) Runs the utility in read-only mode. The utility displays the changes that would occur, and produces LDIF files but does not change the endpoint data.

**-createundo**

(Optional) Creates undo LDIF files that allow you to undo any modifications or deletions made by the utility.

**-verbose**

(Optional) Displays additional operational messages and results.

## Remove the LDAMigrate Log Files

To remove the log files generated by the migration process, delete the log files in the following directory:

*cs-home*/resources/jndi/LDAMigrate.log

## Post Migration Step

If you want to edit the default screen definitions generated by LDAMigrate, you can use Connector Xpress to generate the account screens to view them in CA IdentityMinder.

For more information, see the topic *How you Generate CA IdentityMinder User Console Account Screens* in the *Connector Xpress Guide*.

For more information on the Role Definition Generator command, see the *Connector Xpress Guide*.

## Connector Xpress Templates

Connector Xpress includes templates to help you when you start new JNDI mappings. These templates provide a useful starting point for all JNDI mapping projects, and include specialized JavaScript mark-up that CA IdentityMinder uses to render account management screens.

You can use these templates for creating new JNDI endpoint types rather than new LDA endpoints.

**Note:** For more information about Connector Xpress templates, see the *Connector Xpress Guide*.

| Project Name Setting | Endpoint type | Description | Metadata File Name |
|---|---|---|---|
| JNDI NIS NetGroup | JNDI | For use with LDAP endpoints supporting NIS Netgroup Schema. This template demonstrates advanced association handling. | jndi_assoc_nisnetgroup_metadata |
| JNDI inetOrgPerson (Common) | JNDI | LDAP inetOrgPerson. This template should be used when no vendor-specific template is required. | jndi_inetorgperson_common_metadata |

| Project Name Setting | Endpoint type | Description | Metadata File Name |
|---|---|---|---|
| Lotus Notes Domino | JNDI | Lotus Notes Domino Server. This template allows easy mapping of eTLNDCustomAttribute* and eTLNDCustomCapabilityAttribute* attributes (the latter set are relevant for account template synchronization). | lnd_metadata |
| SDK DYN Compound | Any | Like SDKDYN but demonstrates use of Compound Values. This template uses compound values which allow complex data to be represented as a single string in JSON syntax, for instance '{"attr1": 42, "attr2": [ "a", "b" ], attr3: { "objName" : "jack" } }' represents a top level object with three attributes, the first is an integer (42), the next is an array of strings and the last a nested object. | sdkcompound_metadata |
| SDK DYN | Any | Software Development Kit demo connector. This template is a flat (i.e. non-hierarchical) case-sensitive connector that uses the recommended eTDYN* schema to save provisioning information to local files on the CA IAM CS host computer. Because it is flat, its containers are Virtual Containers not actually stored on the endpoint. | sdkdyn_metadata |
| SDK DYN Script | Any | Like SDKDYN but implemented in Java Script. This template demonstrates how to implement an entire connector (all operation bindings) in JavaScript, as well as configuration information usually found in a connector.xml file, using the connectorXML metadata setting on the top-level namespace. | sdkscript_metadata |
| SDK DYN UPO Script | Any | Like SDK DYN Script but sends emails rather than writing to local files. This connector has similar functionality to the deprecated C++ UPO connector except that it sends emails rather than writing information to local files. | sdkuposcript_metadata |

# Lotus Domino Connector

The Lotus Domino Connector lets you administer accounts and groups on Lotus Domino servers and provides a single point for all user administration by letting you do the following:

- Register multiple endpoints, explore them for objects to manage, and correlate their accounts with global users
- Create and manage Lotus Domino accounts using Lotus Domino-specific account templates
- Create and manage Lotus Domino groups and organizational units
- Activate accounts in one place
- Synchronize global users with their roles or synchronize global users' accounts with their account templates
- Assign Lotus Domino endpoints to your Lotus Domino endpoints
- Use the default Endpoint Type account template to create accounts with the minimum level of security needed to access the Lotus Domino endpoints
- Recertify, rename, and move Lotus Domino accounts in the hierarchy
- Generate and print reports about Lotus Domino accounts and groups

The Lotus Domino Connector uses the inherent object model and administrative processes underlying the Lotus Domino product. The next sections introduce the native Lotus Domino object model, the security application databases, and the administrative processes used by the Lotus Domino Connector to perform user management.

## Privileges Required to Connect to Lotus Domino

The user account that the connector uses to acquire a Lotus Domino endpoint must have the same access level, privileges, and roles as the Lotus Domino domain administrator in the following databases:

- names.nsf
- admin4.nsf
- certlog.nsf

**Important!** Consider logging in to the Lotus Domino Administrator application using the ID file for the user that the connector uses to access the endpoint. Using the same ID file helps ensure that the user has the necessary access level, privileges, and roles to complete user management actions.

## LND Support for FIPS and IPv6

For this release of CA IdentityMinder, the LND Connector does not support FIPS or IPv6.

## Set Up the Connector for Lotus Domino

Before you connect to a Lotus Domino endpoint, complete the following steps:

1. Install or upgrade CA IAM CS.

   The installation registers CA IAM CS with the provisioning server, creates the endpoint, and populates it with its associated metadata.

2. Verify your access to the Lotus Notes Domino databases.
3. Enable the administration process (Adminp) (see page 238).
4. Add encryption keys to the server ID (see page 239).
5. Configure remote access to the Domino Server (see page 240).
6. Sign the agents used by the connector (see page 241).
7. Enable SSL between Lotus Domino and CA IAM CS (see page 242).
8. Add NCSO.jar to the Lotus Domino connector (see page 243).

**Note:** If you currently use the older C++ connector to Lotus DOmino, you can migrate to the newer Java connector. For advice, see LND Java Implementation Considerations (see page 244).

### Enable the Administration Process (Adminp)

This procedure is for the Lotus Domino administrator.

This step helps ensure that you can use all of the Administration Process (Adminp) features. By default, Adminp runs when a Lotus Domino server is started; however, it is not automatically enabled for the domain.

**Follow these steps:**

1. Designate a server in the domain as the administration server for the Lotus Domino endpoint (Public Address Book).
2. Verify that the administration server for the endpoint is running the most recent version of Lotus Domino.

**Note:** After assigning an administration server to the endpoint, use the server copy of the Public Address Book for Adminp tasks. Do not use the local copy of the Address Book.

## Add Encryption Keys to the Server ID

This procedure is for the Lotus Domino administrator.

To allow CA IAM CS to communicate with the Lotus Domino server, add encryption keys to the server ID file. These keys let CA IAM CS encrypt and decrypt the archive and certifier databases (RegXArchive and RegXCertifier).

**Follow these steps:**

1. Create an encryption key, naming it RegXArchive.

   **Note:** To create this key, follow "To create a secret encryption key" in this document: http://publib.boulder.ibm.com/infocenter/domhelp/v8r0/topic/com.ibm.notes85.help.doc/sec_encryp_doc_t.html

2. Repeat the previous step to create another key, naming it *RegXCertifier*.

**Note:** If you have already set up the connection between Lotus Domino and CA IAM CS, you have already created these encryption keys. To import these existing keys instead of creating new ones, use these instructions: http://publib.boulder.ibm.com/infocenter/domhelp/v8r0/topic/com.ibm.notes85.help.doc/sec_encryp_doc_imp_t.html

## Configure Remote Access to the Domino Server

This procedure is for the Lotus Domino administrator.

**Follow these steps:**

1. Verify that the Domino server is accessible through the network, using TCP/IP. You must be able to ping the server using its Internet host name.
2. Enable the HTTP and DIIOP tasks on the Domino server, in one of these ways:
   - Add these tasks to the ServerTasks variable in the server's notes.ini file
   - Load these tasks at the server console
3. Use Domino Administrator to modify the server document to allow and restrict access as desired. The following are some suggested settings:
   a. On the Security tab, in the Server Access section:
      - Access server – All users can access this server
      - Not access server – blank
      - Create new databases – blank (= everyone)
      - Create replica databases – LocalDomainAdmins, LocalDomainServers, and the Domino Administrator account used by the LND Connector if that account is not a member of LocalDomainAdmins

   b. On the Security tab, in the Programmability Restrictions section:
      - Run unrestricted methods and operations – the Domino server name, the Domino Administrator account used by the LND Connector
      - Run restricted LotusScript Java agents – the Domino Administrator account used by the LND Connector

   c. On the Security tab, in the Internet Access section:
      - Internet authentication – Few name variations with higher security

   d. On the Ports tab, under Internet Ports, for DIIOP:
      - Authentication options
      - Name & password - Yes
      - Anonymous - Yes

   e. On the Internet Protocols tab, under HTTP, in the R5 Basics section
      - Allow HTTP clients to browse databases – Yes

## Sign the Agents Used by the Connector

This procedure is for the Lotus Domino administrator.

Before you acquire the endpoint for the first time, sign the agents that the connector uses. Use the keys discussed in Add Encryption Keys to the Server ID.

**Follow these steps:**

1. Copy the regarchv.ntf and regcerts.ntf database templates from this location:

   `cs_home\resources\lnd`

2. Place the copies in the data folder of the Domino Server endpoint:

   - **Windows:** *lotus_home*\Data
   - **UNIX:** /local/notesdata

3. Log in to Domino Designer using the account used by the connector.
4. Update the regarchv.ntf database template:

   a. Open the regarchv.ntf database template.

   b. In the Database View window on the right, expand Shared Code and click Agents.

      A list of agents located in each template is displayed.

   c. For each agent, select the agent then click Sign.

      This signs each of the agents that the connector is deployed within your environment.

5. Repeat step 4 for the regcerts.ntf database template.

   If the regarc.nsf and regcert.nsf databases have not already been created, skip to the last step.

   If these databases have already been created, follow the next steps to refresh the database designs.

6. Switch to the file view in Domino Designer.
7. Select regarc.nsf and click File, Database, Refresh Design.
8. Select regcert.nsf and click File, Database, Refresh Design.

   The designs for these databases have been refreshed.

9. Close Domino Designer.

## Enable SSL between Lotus Domino and CA IAM CS

Communication between the Lotus Domino connector and the endpoint is not encrypted by default. To secure the connection, use SSL encryption. This is optional, but recommended.

**Follow these steps:**

1. The Domino administrator does the following:
    a. Configure the Lotus Domino endpoint to accept SSL connections.
    b. IBM provides the following documentation on SSL Encryption:

       http://publib.boulder.ibm.com/infocenter/domhelp/v8r0/topic/com.ibm.help.domino.admin85.doc/H_ABOUT_SETTING_UP_SSL_ON_A_SERVER.html

       http://www.ibm.com/developerworks/lotus/library/ls-Java_access_2/index.html
       http://www.ibm.com/developerworks/lotus/library/ls-Java_access_2/index.html
    c. After the keyring files are on the server, start or restart the DIIOP task. This generates a file named TrustedCerts.class in the following location:

       `lotus_home/Lotus/Domino/data/domino/Java/`
    d. Send the file to the CA GovernanceMinder integrator (if applicable).
2. The CA IdentityMinder administrator does the following:
    a. Save the *TrustedCerts.class* file in this location:

       `cs_home/extlib/`
    b. Restart the CA IAM CS service (im_jcs).

In the next procedure, you add this class to the connector.

## Add NCSO.jar to the Lotus Domino Connector

The Lotus Domino connector uses the Domino Java API to access the Domino server using CORBA, and it requires the CORBA interface jar (NCSO.jar). Before you use the connector, create a bundle that contains this JAR, and then add the bundle to the connector.

Although the Notes client is not required on the client system, it must contain NCSO.jar in the classpath.

**Follow these steps:**

1. Ask the Lotus Domino administrator to send you a copy of NCSO.jar, which is in the following location:

   *lotus-home*/Data/domino/java

2. Save NCSO.jar locally.
3. Run the *lnd_post_install* script, which is in the following location:

   *cs-home*/bin

   The script asks for the location of the following items:

   - **NSCO.jar**—This file is essential to the connector.
   - **TrustedCerts.class**—(Optional) This file is required only if you want the connector to use SSL when communicating with the endpoint.

   The script then creates a bundle and saves it in the same location as the script.

4. Log in to CA IAM CS (see page 21).
5. At the top, click the Connector Servers tab.
6. In the Connector Server Management area, click the Bundles tab.
7. Add the new bundle:

   a. In the Bundles area on the right, click Add.

   b. Browse to the bundle that the script created, then select the connector server on which this connector will be available.

   c. Click OK.

      The new bundle appears in the Bundles list.

8. Find the main connector bundle in the Bundles list, then right-click its name in the list and choose Refresh Imports from the popup menu.

The Lotus Domino connector can now use NCSO.jar.

## LND Java Implementation Considerations

The Java version of the LND Connector (installed with JCS) provides the same functionality as the previous (eTrust Admin r8.1) C++ version of the LND Connector with the added benefit of DJX support, but there are a few things to consider when switching from the C++ version.

- To add the Java LND connector to an existing system:

  1. Run the Provisioning Server install to reconfigure and add the LND connector.
  2. Run CA IAM CS installer and select Register with the Provisioning Server.

     Doing this routes requests from the Provisioning Server to JCS for the LND endpoint type. See "Install the LND Connector" for more information.

- For this release it is no longer required to have Lotus Notes Client software installed, or a Notes.ini file available on the computer where the Provisioning Manager is running. The same is true for the computer where CA IAM CS hosting the LND connector is run.
- Connector operation, as well as migration requires the Lotus Notes Domino remote Corba interface jar (NCSO.jar) to be copied to

  ```
  <jcs-home>/extlib/
  ```

  from the server installation directory

  (Windows) <lotus-home>\Data\domino\java

  (UNIX) /local/notesdata/domino/java

  and im_jcs restarted.

- If existing Regarc and Regcert databases are used, these encryption Keys must be imported from the Admin ID used previously, to the Server ID, or all documents in the database created using the old encryption keys will show an error.
- ID file paths should be specified local to the endpoint or use a UNC style path.
- Organization names and organizational unit names no longer appear prefixed by "O:" and "OU:".
- There are new choices for mail systems that correspond to the available choices in Domino R6 and R7

  - Lotus Notes
  - POP
  - IMAP
  - Domino Web Access
  - Other Internet
  - Other
  - None

- The mapping information for the custom attributes is now contained in

  `<jcs-home>/conf/override/lnd/lnd_custom_metatdata.xml`

  Two sample files with the prefix of "SAMPLE" are provided including one covering DJX mappings. the override connector.xml file of the Java LND Connector. For existing LND endpoints, the credential information currently stored in the registry is no longer required.

- The following settings must be made to the Domino server's notes.ini file:

  - *$Reg_TempDir* variable representing the temp directory on the Domino server, must be added to the notes.ini file. If you add or change the variable, the Domino server must be restarted.

    **Note:** The directory specified must already exist. The LND Connector will not create the directory. An example of this setting:

    (Windows) $Reg_TempDir=c:\lotus\domino\data\temp

    (Windows) $Reg_TempDir=\\user01w2k3\c$\lotus\domino\data\temp

    (UNIX) $Reg_TempDir=/local/notesdata/temp

    The value is necessary for the temporary placement of ID files during ID password changes. For ID password changes to be successful, the ID must be located on the server at the time of the change. The value is also necessary for the temporary placement of ID files during account and certifier creation if another location is not specified for the ID.

- Two new fields are required when acquiring an LND Endpoint:

  - DIIOP Port

    The LND connector uses the remote access support provided in the Lotus Domino Toolkit for Java/CORBA 2.1 to communicate with the endpoint.

  - Use SSL/TLS

- The connector is now case insensitive. Objects existence is checked ignoring case. If duplicate objects already exist during an explore operation, only one is managed (silently) by the Provisioning Manager.

- If connection to the endpoint is temporarily lost, the default retry settings of six retries 10 seconds apart are enforced. As for all CA IAM CS connectors, these settings can be adjusted using the *exceptionRetryMap* settings in the connector.xml file located in:

  `<jcs-home>/conf/override/lnd/.`

- Search results are streamed so the connector passes search results on to the Provisioning Server immediately rather than buffering all results before passing any on. This keeps the memory usage of the Connector Server to a minimum, regardless of the number of objects in an LND endpoint.

- Custom delete of an account in a secondary directory is not supported by the Administration Process (adminp) JAVA API used by the connector so the connector explicitly deletes only the person document itself. You must manually clean up any references to the person's name in group members/ACL's and so forth, where they exist.

  **Note:** Account operations are not supported on accounts that are in a secondary directory and require the intervention or spawning of requests from the Domino administration process ‘adminp’.

## Connector-Specific Features

This section details your connector's specific management features, such as how to acquire and explore your endpoint. Also included are account, provisioning roles, account template, and group information specifically for your connector.

### Acquire a Lotus Notes/Domino Server Using the User Console

You must acquire the Lotus Notes/Domino server before you can administer it with CA IdentityMinder.

**To acquire a Lotus Notes/Domino server using the User Console**

1. Select Endpoints, Manage Endpoints,Create Endpoint
2. Select Lotus Domino Server from the drop-down list box on Create a new endpoint of Endpoint Type, and click Ok

   Use the Create Lotus Domino Server Endpoint page to register a Lotus Notes/Domino server. During the registration process, CA IdentityMinder identifies the Lotus Notes/Domino server you want to administer and gathers information about it.
3. After entering the required information, click Submit.

   You are now ready to explore and Correlate the endpoint.

4. Click Endpoints, Explore and Correlate Definitions, Create Explore and Correlate Definition to explore the objects that exist on the endpoint.

   The Exploration process finds all Lotus Notes/Domino accounts and groups. You can correlate the accounts with global users at this time or you can correlate them later.

5. Click OK to start a new definition.
6. Complete the Explore and Correlate Tab as follows:
   a. Fill in Explore and Correlate name with any meaningful name.

      Click Select Container/Endpoint/Explore Method to click a Lotus Domino Server endpoint to explore.

   b. Click the Explore/Correlate Actions to perform:
      - **Explore directory for managed objects**—Finds objects that are stored on the endpoint and not in the provisioning directory.
      - **Correlate accounts to users**—Correlates the objects that were found in the explore function with users in the provisioning directory. If the user is found, the object is correlated with the user. However, you can instead select that you want to assign the account to the existing user (the default user) or create the user.
      - **Update user fields**—If a mapping exists between the object fields and the user fields, the user fields are updated with data from the objects fields.
7. Complete the Recurrence tab if you want to schedule when the task to executes.
   a. Click Schedule.
   b. Complete the fields to determine when this task should execute.

      You may prefer to schedule the task to execute overnight to interfere less with routine access of the system.

   **Note**: This operation requires the client browser to be in the same time zone as the server. For example, if the client time is 10:00 PM on Tuesday when the server time is 7:00 AM, the Explore and Correlate definition will not work.

8. Click Submit.

**To use an explore and correlate definition**

1. In a CA IdentityMinder environment, click Endpoints, Execute Explore and Correlate.
2. Click an explore and correlate definition to execute.
3. Click Submit.

   The user accounts that exist on the endpoint are created or updated in CA IdentityMinder based on the explore and correlate definition you created.

## Acquire a Lotus Notes/Domino Server Using the Provisioning Manager

Acquiring an LND endpoint is the first task you must perform before you can manage Lotus Notes/Domino accounts.

**From the Endpoint Type task view**

1. Register the server as an LND endpoint using the Provisioning Manager.

   Use the LND Endpoint property sheet to register a Domino Server. During the registration process, the Provisioning Server identifies the Domino Server you want to administer and gathers information about it.

   **Note:** Regarc and Regcert databases are created when a new endpoint is acquired. For the LND Connector to work, you must copy the database templates, REGARCHV.NTF and REGCERTS.NTF, from the <*jcs-home*>\resources\lnd folder to the data folder of the domino server endpoint, (<*lotus-home*>\Data), prior to acquiring the endpoint for the first time.

2. Explore the objects that exist on the endpoint.

   After registering the server with the Provisioning Manager you can explore its contents. Use the Explore and Correlate Endpoint dialog. The Exploration process finds all LND accounts, organizations, organizational units, and groups that exist on the server. You can correlate the accounts with global users at this time or later

3. Correlate the explored accounts with global users.

When you correlate accounts, the Provisioning Server creates or links the accounts on an endpoint with global users. By correlating accounts, you can specify what fields are matched with global user fields. The Provisioning Server provides a default correlation account template for Lotus Notes/Domino endpoints. This account template performs the following actions in this order:

1. The Provisioning Server attempts to match the Lotus Notes/Domino Account short name with each existing global user's unique name. If a match is found, the Provisioning Server associates the Lotus Notes/Domino account with the global user. If a match is not found, the Provisioning Server performs the next step.
2. The Provisioning Server attempts to match the Lotus Notes/Domino Account name with each existing global user's full name. If a match is found, The Provisioning Server associates the Lotus Notes/Domino account with the global user. If a match is not found, the Provisioning Server performs the next step.
3. If Create Global User is checked, the Provisioning Server creates a new global user; otherwise, it associates the Lotus Notes/Domino account with the [default user] object.

Once the endpoint is acquired, your Lotus Notes/Domino server appears as an endpoint object and your accounts are organized according to their respective certifier container.

The position of user objects within the endpoint is specified by its context. The complete context or path from an object to the country of the endpoint tree identifies and forms the object's hierarchical name, for example, eTLNDAccountName=xx,eTLNDOrganizationUnitName=yy,eTLNDOrganizationName,eTLNDCountryName=zz. All hierarchical names must be unique in the endpoint.

Before accounts can be created under the explored organizations or organizational units, each of the account containers must have their certifier details registered in the regcert.nsf database.

**To register the certifier details**

1. Search for the appropriate certifier (eTLNDOrganization or eTLNDOrganizationalUnit) in Provisioning Manager, and select it.
2. Right click the certifier, and from the popup menu, select custom.
3. Select 'Certifier Detail' and provide the certifier ID location on the Domino server and the certifier ID password and type.

## Managed Objects

CA IdentityMinder organizes the following objects into a hierarchical endpoint tree:

- **Country object** depicts the country that is selected as the organizational root. This object is generally implicit in the Lotus Notes/Domino representation of the organizational hierarchy. Countries appear directly under the root container and their use is optional. Only Organization objects can be their direct children.
- **Organization objects** represent the Lotus Notes/Domino organization level certifiers that are registered with the Domino Administration Server and stored in the Domino Address Book. These can contain organizational unit objects or account objects. They can only appear under a Country object or root level.
- **Organizational Unit objects** represent the Lotus Notes/Domino organizational unit level certifiers that are registered with the Domino Administration Server and stored in the Domino Address Book. These can contain other organizational unit objects or account objects. (Maximum four OU objects).
- **Group objects** represent the groups on the Lotus Notes/Domino server. Group objects are leaf objects, but all appear directly under the single eTLNDGroupContainer container.

  **Note:** LND groups cannot be added to other LND groups that are not in the same Domino directory. A group in the primary Domino directory cannot be added to a group that is in the secondary Domino directory, and vice versa.
- **Account objects** represent the accounts on the Lotus Notes/Domino server. Account objects are leaf objects and can appear under any Organization or Organizational Unit.

For more information about the managed objects or the endpoint schema, see the appendix “Endpoint Schema and Structure.”

## How Managed Objects are Referred to in the Java LND Connector

The LND Connector uses Provisioning Server DNs to refer to all managed objects (except the DN of the administrative account used to connect to the endpoint). This includes syntax used to distinguish LND "Unique OUs" from real Organizational Units. For example, previously a group may have named an account (with a Unique OU) that was a member of the group as, "CN=user,OU=uou,O=Acme". An equivalent reference using the new connector is "eTLNDAccountName=user /uou,eTLNDOrganizationName=Acme".

## Update Notes.ini Settings

The following settings must be made to the Domino server's notes.ini file:

- *LDAP_Disable_QRCache* must be set to 1 to allow immediate updates to LND accounts through CA IdentityMinder. The cache stores user names and attributes that have been previously searched for in order to speed up frequently performed searches.
- *$Reg_TempDir* variable representing the temp directory on the Domino server, must be added to the notes.ini file. The value for this variable must reflect the URL of the directory as it can be accessed from the client system. If you add or change the variable, the Domino server must be restarted.

  **Note:** The directory pointed to by the URL must already exist. The LND Connector does not create the directory. An example of the of this setting:

  (Windows) *$Reg_TempDir=\\user01w2k3\c$\lotus\domino\data\temp*

  (UNIX) *$Reg_TempDir=\local\notesdata/temp*

  The value is necessary for the temporary placement of ID files during ID password changes. For ID password changes to be successful, the ID must be located on the server at the time of the change. The value is also necessary for the temporary placement of ID files during account and certifier creation if another location is not specified for the ID.
- The DIIOPIORHOST parameter accepts fqdn as the format for the hostname. For example, DIIOPIORHOST=<fqdn hostname>

## System Databases

The Provisioning Server uses five system databases to manage users. The first three databases originate from the Lotus Notes/Domino product. The last two databases are created when an LND endpoint is acquired and their templates have been copied to the Domino\data folder from *<jcs-home>*\resources\lnd folder.

| Database | Description |
|---|---|
| ADMIN4.NSF | The Administration Process (Adminp) uses this database to post and respond to requests. You can approve requests that move users to different organization hierarchies, delete objects, delete mail files, and monitor Administration Process errors. |
| CERTLOG.NSF | Lists the names of all registered and certified users in a domain. This database is required if you want to use the Administration Process to simplify user management. |
| NAMES.NSF | Provides a domain-wide directory of the server, including its users, certifiers, foreign domains, and groups. This database includes documents that manage server-to-server communication and server programs. |

| Database | Description |
|---|---|
| REGARC.NSF | Stores archive documents for all managed accounts. Each archive document includes the login name, password, certificate expiration date, and a copy of the user ID file.<br>**Note:** Agents in this template must be signed by the Admin account used by the Provisioning Server to connect to the Domino Server. |
| REGCERT.NSF | Stores certifier documents for all organization and organizational unit certifiers that certify accounts. Each certifier document includes the certifier name, type, password, and ID file.<br>**Note:** Agents in this template must be signed by the Admin account used by the Provisioning Server to connect to the Domino Server. |

**Note:** For details on the access privileges that you need to perform user management in your Lotus Notes/Domino domain, see the section, Configure the Lotus Notes/Domino Connector.”

Each time a request is sent or received, the Provisioning Server opens these databases and makes changes to the information stored in them.

## Locations for Storing IDs

You can choose to store user and certifier IDs on the LND server or on a separate server. The following table lists the supported ID types and how to configure CA IdentityMinder to store them.

| ID Type | ID Location | Steps |
|---|---|---|
| User ID | On LND Server | 1. Select the User ID File Path check box on the UserID tab.<br>2. Specify the absolute path (on the LND server) and filename as follows:<br>■ Windows: C:\Program Files\Lotus\Domino\data\user.id<br>■ Unix: /local/notedata/user.id |

| ID Type | ID Location | Steps |
|---|---|---|
| | On separate system | 1. Select the User ID File Path check box on the UserID tab.<br>2. Enter the full UNC path, including the drive as follows:<br>\\server\c$\share\user.id<br>Do not omit the c$. |
| Certifier ID | On LND Server | 1. Select the Specify a Location for the Certifier ID check box on the Organization Certifiers tab.<br>2. Specify the absolute path (on the LND server) and filename as follows:<br>■ Windows: C:\Program Files\Lotus\Domino\data\certifier.id<br>■ Unix: /local/notedata/certifier.id |
| | On separate system | 1. Select the User ID File Path check box on the UserID tab.<br>2. Enter the full UNC path, including the drive as follows:<br>\\server\c$\share\certifier.id<br>Do not omit the c$. |

## DJX Support

DJX extensions are now supported by LND Connector and are managed through the Custom Attributes tab.

See Custom Attribute Support, for more information on this feature.

## Custom Attribute Support

Several enhancements have been made for custom attribute support. They include:

- The connector supports up to 50 custom attributes eTLNDCustomAttribute01-50 and up to 50 custom capability attributes eTLNDCustomCapabilityAttribute01-50 (policySync="yes").
- Connector Xpress must be used to map custom attributes and custom capability attributes. Mapping custom attributes using XML file <jcs-home>/conf/override/lnd/lnd_custom_metatdata.xml is no longer available.
- Only power users should modify the custom metadata file and should take precautions like saving a backup copy of any existing file before updating. Tests to verify mapping changes should be conducted immediately after modifications are made, as any syntax errors introduced will render any LND connector hosted by the modified CA IAM CS inoperable until a valid custom file is reinstated (or the offending custom mapping file deleted).
- If customized mappings need to be active on multiple CA IAM CS installations, the same metadata needs to be deployed on each of them.
- Attribute values entered on the Custom Attributes tab are subject to validation by the connector. For example, integer fields emit a validation failure when non-digit characters are present.
- The values provided for any custom attribute configured to be date or dateTimes on the Custom Attributes tab, must be entered in the UTC time zone, not local time, unless the computers on which the client is running and the LND endpoint are configured to use the same time zone.

## Use Connector Xpress to Map Custom Attributes and Custom Capability Attributes

To specify custom attributes for LND, use Connector Xpress. To add custom attributes and map them, do the following:

**From Connector Xpress**

1. Select Project, Create New from Template.
2. From the pop-up, select the relevant template, for example, 'Lotus Domino Server.con' or 'Lotus Notes Domino (DJX).con'.
3. Edit the custom attributes in Classes, eTLNDAccount, Attributes.
4. Save the updated ‘Lotus Domino Server.con’ or 'Lotus Notes Domino (DJX).con' file.
5. Right-click the Lotus Domino Server endpoint and select ‘Deploy Metadata’.

## Alternative Languages Support for both Organization and Organizational Unit Certifiers

You can now Add, Delete, Query, and Modify the alternative language list from the Provisioning Manager. When adding an alternate language, both the normal (long) name and short name for the language is accepted. For example, both Japanese and ja are valid names. You must separate multiple languages by commas. The normal (long) name of the language is now displayed from the Provisioning Manager. The short name is stored in the repository the same as the previous C++ Connector.

The following are the alternative languages available for this Connector:

- Arabic [ar]
- Byelorussian [be]
- Bulgarian [bg]
- Catalan [ca]
- Czech [cs]
- Danish [da]
- German [de]
- Greek [el]
- English [en]
- Spanish [es]
- Estonian [et]
- Finnish [fi]
- French [fr]
- Gujarati [gu]
- Hebrew [he]
- Hindi [hi]
- Croatian [hr]
- Hungarian [hu]
- Indonesian [id]
- Icelandic [is]
- Italian [it]
- Japanese [ja]
- Korean [ko]
- Lithuanian [lt]
- Latvian [lv]
- Macedonian [mk]

- Marathi [mr]
- Malay [ms]
- Dutch [nl]
- Norwegian [no]
- Polish [pl]
- Portuguese [pt]
- Romanian [ro]
- Russian [ru]
- Slovak [sk]
- Slovenian [sl]
- Albanian [sq]
- Serbian [sr]
- Swedish [sv]
- Tamil [ta]
- Telugu [te]
- Thai [th]
- Turkish [tr]
- Ukrainian [uk]
- Vietnamese [vi]
- Konkani [x-KOK]
- Chinese (Simplified) [zh-CN]
- Chinese (Traditional) [zh-TW]

## Organizations and Organizational Units Handling Extended

Organizations and Organizational Units can now be deleted. However, it is not possible to delete these objects while they still contain child objects.

**Note:** Organizations cannot be created using the Provisioning Manager, although explored and listed organizations can be deleted.

## Correlate on Shortname

The default correlation attribute used by the Lotus Notes/Domino Connector is the Shortname attribute. When creating new global users, they will, by default, have the LND account shortname as the global user name. Accounts are then correlated to existing global users if the global user name matches the LND account's shortname value.

To use another attribute as the correlation attribute, for example, the full name, follow these steps:

1. From the System task in Provisioning Manager, select Domain Configuration.

   Several folders appear in the right-hand frame.

   Select Explore and Correlate, Correlation attribute from the right-had frame

   The Domain Configuration tab appears.

2. From the Domain Configuration tab, modify the Correlation attribute appropriately.

   For example, to change the correlation attribute to the full name, you would set the Correlation Attribute to “GlobalUserName=Lotus Domino Server:Name”.

## Configure Shortname Verification

The LND connector automatically generates unique short names. By default the LND connector searches existing Address Books for short names. However, if you store short names in non-standard locations and want to verify that short names that are automatically generated do not conflict with existing short names, you can change the default search behavior. You can specify the databases and views you want to search for shortnames by configuring the connector.xml file.

**Follow these steps:**

1. Navigate to the folder *cs_home*/conf/override/lnd/connector.
2. Add the following to the <property name="defaultConnectorConfig"> section of the SAMPLE.connector.xml file:

   ```
   <property name="shortNameSearchViews">
       <map>
       <entry key="names.nsf"><value>$Users</value></entry>
       </map>
   </property
   ```

   This configuration specifies the databases and views to search for short names. This configuration replaces the default connector behavior of searching existing Address Books for short names.

   **Note:** For more information about customizing a connector.xml file, see Configuring a Connector.
3. To search multiple views, add extra <entry> lines. For example:

   ```
   <property name="shortNameSearchViews">
       <map>
       <entry key="db1.nsf"><value>$view1</value></entry>
       <entry key="db2.nsf"><value>$view2</value></entry>
       <entry key="db3.nsf"><value>$view3</value></entry>
       </map>
   </property>
   ```

   **Note:** You can only specify one view per database. For example, you cannot do the following:

   ```
   <property name="shortNameSearchViews">

       <map>
       <entry key="db1.nsf"><value>$view1</value></entry>
        <entry key="db1.nsf"><value>$view2</value></entry>
       <entry key="db1.nsf"><value>$view3</value></entry>
       </map>
       </property>
   ```
4. Rename the SAMPLE.connector.xml file to connector.xml.
5. Copy the file to the following folder on CA IAM CS:

   conf/override/lnd

6. Restart the connector (see page 52).

## Attribute Mapping

In order to improve performance, a minimum number of attributes is retrieved from the Domino server during exploration. By default, most Domino attributes are not mapped to the Global Users. If you need to populate Global User information from the Domino database, this information can be retrieved by defining additional attribute mappings. Follow these steps to set up attribute mapping:

1. Select Use custom settings from the Attribute Mapping tab.
2. Click Set Default and define at least one additional attribute mapping.

   The LND Connector is now forced to retrieve all data from the Domino server.

   **Note:** Exploration times are likely to increase due to extra information retrieval from the Domino endpoint.

## LND Account Templates

The Lotus Notes/Domino Default Policy, provided with the Lotus Notes/Domino Connector, gives a user the minimum security level needed to access an endpoint. You can use this account template as a model to create new account templates.

CA IdentityMinder lets you manage provisioning roles and account templates from the User Console. For example, with Lotus Notes/Domino you can give a person access to the Lotus Notes/Domino server by registering the person using the Lotus Notes Domino Client. When registering a user, the connector creates a Person document in the Public Address Book (PAB), a user ID file, and a server-based mail file that defines the types of mail the user can receive. (The PAB is also called the Domino Endpoint.)

Similarly, an Internet user is defined as someone who is required to provide a password when accessing a Lotus Notes/Domino server or someone who uses client authentication with Secure Sockets Layer (SSL). In addition, this user uses either no mail or Internet mail, in which case a user ID and mail file are not necessary. An Internet user can by added by the connector creating a Person document in the Public Address Book (PAB). The document contains information about the user's name and Internet password.

In CA IdentityMinder, you register both of these users by adding them to a provisioning role that has a Lotus Notes/Domino account template defined and a Lotus Notes/Domino endpoint associated with the account template.

## Archive Database Data Collection

Before password synchronization can take place, all current Notes account ID files with their passwords need to be obtained. The repository for these account IDs and passwords is the existing Archive database. Keeping this repository current allows for ID and password recovery. If you lose your account ID, the Administrator can retrieve the current account ID and password from the Archive database and send them to you.

To obtain the current account IDs and passwords, the archive database on the Domino server needs to be designated as “Mail-in” database and the *Send ID to Archive* DB hidden agent needs to be copied to all user mailfiles by the Administrator. The agent can be copied in one of the following ways:

- Using the Domino Designer client, copy the hidden agent from the Archive DB to each mailfile individually.
- Using the Domino Designer client, copy the hidden agent from the Archive DB to the mail template and let the Designer task automatically update the mailfiles. (recommended) By default, the Designer task runs daily at 1:00 a.m.

This agent gets the user's Notes account ID specified by the “KeyFilename” entry in their notes.ini file on the Domino Client, prompts the user to enter his or her password and then mails these items to the Archive database. The Archive DB must be configured as a Mail-in Database in the Domino endpoint using the Mail-in name “Archive Database”.

Once the agent is present in the user mailfiles, a mail message is sent notifying them that their account ID and password need to be sent to the Archive database. This message contains a button that activates the *Send ID to Archive DB* hidden agent which retrieves the ID file and mails both ID and password to the Archive database.

You must sign the agents with a signature that is valid in your organization in order for the new agents to run successfully. To do this, edit and save each agent in the Domino Designer client.

If a database is designed to receive mail, you must create a Mail-In Database document in the Domino Directory. This document must exist in the Domino Directory of every server that stores a replica of the database. The database cannot receive mail until you create this document.

To create a Mail-In Database Document

1. Make sure you have at least Author access with the Create Documents privilege selected.
2. From the People & Groups tab of the Domino Administrator, choose the Mail-In Databases Resources view, and click Add Mail-In database.
3. On the Basics tab, complete these fields:

   **Mail-in name**: “Archive Database”

   **Domain:** <Your domain name>

**Server:** <Your server>

**File name:** regarc.nsf

4. Save the document.

Another hidden agent called *Update ID File* has been added to the Archive database. This agent gets the current Archive documents for the user whose ID has been received and replaces the ID and password values on the document with those received in the mailed-in document. If a previous Archive document exists for that user, a new document containing the new ID and password is linked to the Archived document.

The RegXArchive encryption key must also be available in the current User.ID of the Administrator as well as the Server.ID of the Registration server to let the mail-triggered background agent in the Archive database run successfully. Alternatively, the agent can be run manually in the foreground by the Administrator if the encryption key cannot be added to the Server.ID.

You must have at least Designer access with Create LotusScript/Java agent to the user mailfiles in order to copy the hidden agent.

Add the following parameter to the NOTES.INI file on the Registration server:

```
Mgr_DisableMailLookup = 1
```

```
This parameter lets the mail-triggered agent in the Archive database to run even if
the server is not the mail server for the Administrator.
```

A third, optional agent, *Remove ID Agent from User Mailfiles* can be added to the Archive database. This agent can be run manually by the administrator to remove the hidden agent from user mailfiles after the ID repository has been created.

## Password Synchronization

The administrative user of CA IdentityMinder can change the password associated with an account's ID file in one of the following ways:

- Directly modifying the account
- Propagate a Global User password change to associated accounts.

Once the password is changed, an email is sent to the account, optionally, including the new server ID file.

To customize the subject and body of the email that is sent, set the following parameters in the NOTES.INI file on the Domino server:

“$Password_Change_Subject=” specifies the message body to be used: If not specified, the parameter defaults to a generic subject.

“$Password_Change_Message=” specifies the message body to be used. If not specified, the parameter defaults to a generic body.

“$Password_Change_Attach_ID=” specifies whether the new ID file is attached to the message. If not specified, the default is “Yes”. Any value other than a case-insensitive match to “Yes” is interpreted as “No.”

"$Password_Send_To=" specifies who receives the message.

## Suspend/Resume

A combobox called Status located on the Profile tab of the Account and Account Template Property sheets provides a form of suspension using Deny Access groups.

When Status is set to Active, the account is not in a Deny Access group on the Domino server. When Status is set to Suspended, the account has been added to a Deny Access group on the Domino server.

**Note:** This functionality is currently limited in the number of accounts that can be concurrently suspended. For Domino 6.x, the limit is 64 KB. For Domino 7.x, the limit is 32 KB.

## LND Accounts

To manage LND Accounts, some manual steps are required.

Each Organization or Organizational Unit must have an entry in RegCert.nsf to permit CA IdentityMinder access.

To create this entry, do the following:

1. Explore the Lotus/Domino endpoint.
2. Expand Organizations or Organizational Units in the List Tab.
3. Select an item and right-click it to select Custom, then Certifier Details.
4. Fill in all mandatory fields (Name, Storage location, and Password of the Certifier ID).

## Account Custom Operation (Rename, Recertify, Move In Hierarchy)

For Account Custom Operation (Rename, Recertify, and Move In Hierarchy), you must add an entry in RegArc.nsf for explored accounts. This is only for Accounts created with native tool and explored with the Provisioning Server.

To create this entry, do the following:

1. Explore the Lotus/Domino endpoint.
2. Expand Accounts in a List Tab.
3. On the History tab of each account for which you want to add an archive entry, click the Add/Update Archive button.
4. Fill in all mandatory fields (Location and Password of the Certifier Id).
5. Click OK.

## Cannot Create Notes Account When Mail Home Server Is not the Registration Server

**Symptom:**

When I create a Notes user, I specify a mail home server that is not the same as the registration server. The user creation fails.

My organization uses the following separate Domino servers:

- A registration server
- A mail server

**Solution:**

When you acquire a Lotus Domino endpoint, you specify the registration server.

When you attempt to create a new user, you specify the mail home server. The connector looks for the mail template file on the mail server. If it is not there, CA IdentityMinder cannot create the new user.

To allow CA IdentityMinder to create new Lotus Domino users, configure the registration server to allow the connector to find the file.

**Follow these steps:**

1. Ensure that the registration server and the mail server are in the same Domino domain.
2. On the registration server, enable the Domain Catalog server task, then include the mail server in the catalog.

## Modify Home Server

The Provisioning Manager allows the Home Server field to be modified on LND accounts. Changing the Home Server only changes the value on the LND account. The mail file is not moved to the new server. You must still ensure that a mail file exists on that server.

## Management of Alternate Names on LND Accounts

The LND connector supports the management of alternate names on your LND accounts. The account ID must be certified by a certifier ID that has at least one alternate name configured for it in order to add alternate name information. To include the management of alternate languages on certifier files, the administrator must perform the following steps prior to using this new functionality:

1. Use the Domino Administrator (see Domino Administrator Help for more information) to configure the certifier ID with alternate names.
2. Update the existing Certifier documents for each certifier in the Certifiers database by using the Domino Administrator client to delete the existing certifier ID file from the Certifier document and then attach the updated certifier ID. You must also supply a password for the password field.

   **Note:** This step is necessary any time the alternate name information is changed in a certifier ID file.
3. Update each Organization or Organizational Unit certifier that contains alternate information within the Provisioning database. The multi-valued attribute eTLNDOrgCertAltLanguageList for Organization and Organizational Unit objects must contain all the languages supported by the certifier.

   You can Add, Delete, Query, and Modify the language list from the Provisioning Manager by using the LND Organization and Organization Unit management dialogs. The language codes are automatically expanded to language names when added. However, you can still use etautil to add or update the list. See Sample etautil Commands (see page 269) for an example.

Only those valid languages added to the Organization or Organizational Unit objects in the Provisioning database are displayed as choices when creating accounts using that Org or OU. For a list of languages and associated codes, see Alternative Languages Support for both Organization and Organizational Unit Certifiers. (see page 255)

## How New Short Names are Created and Verified

Every Lotus Notes/Domino account has a unique short name.

When you create a new LND account in CA IdentityMinder, you can enter the account's short name, or you can allow the connector to create it for you. The connector uses the account's first name, last name, and (if necessary) numbers to generate a unique short name.

It works like this:

1. You create a new LND account in CA IdentityMinder, leaving the Short Name field blank.
2. After you click Submit, the connector uses an algorithm to create a short name.

   The short name includes the first letter of the first name, some or all letters from the last name, and some numbers if necessary.

3. The connector checks the new short name against the existing short names in the available address books.
4. If the short name already exists, the connector modifies the new short name and checks it again.
5. When the new short name is found to be unique, the new account is created.

   **Note:** If the connector cannot create a unique short name, the creation of the new account fails. If this happens, you should enter the new short name yourself, instead of allowing the connector to create it.

### Example: How the connector generates a short name

In this example, you create a new account with the following details:

- First name: Peter
- Last name: Smith

When you create the new LND account, you leave the Short Name field blank.

The connector creates the short name *psmith*, and checks it for uniqueness. In this example, the short name *psmith* already exists.

The connector creates the new short name *psmith1*, and checks it for uniqueness. This short name is not in the available address books, so the new account is created.

## Configure the Location for Verifying Short Names

Normally, the new short name is checked for uniqueness in the available address books. However, you can configure CA IdentityMinder to check the new short name's uniqueness in one or more other databases. To set this up, you need to edit a configuration file.

**Follow these steps:**

1. Find CUSTOM_SHORTNAME_VALIDATION.connector.xml, in *cs-home*/conf/override/lnd.
2. Copy the file into the same directory, and rename it to connector.xml.
3. Open the new XML file, and find the <property name="shortNameSearchViews"> section, which is commented out.
4. Remove the comment marks to activate the shortNameSearchViews section.
5. Edit the <entry> section to point to the database view that contains the short names:

   ```
   <property name="shortNameSearchViews">
       <map>
           <entry key="database-name.nsf"><value>$view-name</value></entry>
       </map>
   </property>
   ```

   where

   ***database-name***

   Specifies the name of a database in which to search for matching short names

   ***view-name***

   Specifies the view in that database. You can specify only one view for each database.

   **Note:** To search multiple database views, add extra <entry> lines.

6. Save the file.
7. Restart the connector (see page 52)

### Example: Point to multiple databases

```
<property name="shortNameSearchViews">
    <map>
       <entry key="db1.nsf"><value>$view1</value></entry>
        <entry key="db2.nsf"><value>$view2</value></entry>
        <entry key="db3.nsf"><value>$view3</value></entry>
    </map>
</property>
```

## Etautil Script Considerations

For this release of the Java LND connector, there are several things to be aware of regarding etautil scripts:

- The connector now uses Provisioning Server DNs to refer to all managed objects (except the administrative user value during an acquire). Any existing scripts will have to be changed to comply.
- AddCert objects only need to appear in LDAP ADD requests achieve their intended goal as effective function calls. No error will be returned if an LDAP DELETE request targeting an AddCert object is received, but such a request is not necessary (the AddCert object is transient and immediately deleted once the ADD request is processed).

  **Note:** An AddCert request targeting an object can be used to update the object where it already exists, It behaves like an LDAP MODIFY request.
- The **etautil_addarchive.bat** script installed into **C:\Program Files\CA\Identity Manager\Provisioning Server\etc\lnd** has been updated to match the new connector behaviour.

## LND Etautil Conventions

Use the following Lotus Notes/Domino conventions in your etautil commands:

- The endpoint type name (eTNamespaceName) is Lotus Domino Server
- The endpoint type prefix is LND. For example, some of the Lotus Notes/Domino object class names are as follows:
  - eTLNDDirectory for an endpoint
  - eTLNDPolicyContainer for an account template container
  - eTLNDPolicy for an account template

## Sample etautil Commands

### Update Language List

The following is an example etautil command to update the Language List for an Organization or Organizational Unit using etautil:

```
etautil -d DOEJO03W2K3 -u etaadmin -p password update
'eTLNDDirectoryName=doeja03w2k3,eTNamespaceName=Lotus Domino
Server,dc=DOEJA03W2K3,dc=eta' eTLNDOrganization eTLNDOrganizationName='
eTLNDOrganizationName=cai' to +eTLNDOrgCertAltLanguageList='ko'
+eTLNDOrgCertAltLanguageList='fr'
```

### Modify Home Server

The following is an example etautil command to modify the Home Server on an LND account using the Provisioning Manager and etautil:

```
etautil -d DOEJA01XP -u <eta administrator> -p <eta password>
'eTLNDOrganizationName=cai,eTLNDDirectoryName=doeja01w2k3,eTNamespaceName=Lotus
Domino Server' eTLNDAccount eTLNDAccountName='mail location03'
eTLNDHomeServer='CN=doeja01w2k3/O=cai'
```

You must ensure that the Mail Server attribute in the user's person document is updated correctly.

**Note:** The mail file must be manually created on the new server.

### Modify Mail Quota and Warning Threshold

The following is an example etautil command to modify the Mail Quota and Warning Threshold values of an LND account using the Provisioning Manager and etautil:

```
etautil -d DOEJA01XP -u <eta administrator> -p <password> update
'eTLNDOrganizationName=cai,eTLNDDirectoryName=doeja01w2k3,eTNamespaceName=Lotus
Domino Server' eTLNDAccount eTLNDAccountName='file test02' eTLNDMailFileQuota=500
eTLNDMailFileThreshold=400
```

### Delete Accounts (With and Without Mail Files)

The following is an example etautil command to delete LND accounts using etautil:

```
etautil -d DOEJA01XP -u <eta administrator> -p <password> update
'eTLNDOrganizationName=cai,eTLNDDirectoryName=doeja01w2k3,eTNamespaceName=Lotus
Domino Server' eTLNDAccount eTLNDAccountName='mail file02' eTLNDAdminp=1
eTLNDAccountOperation=2 eTLNDAccountState=2 eTLNDDelFlag=0
```

The possible values for eTLNDDelFlag, which controls deletion of the mail file are as follows:

- 0 = Don't delete mail file(s)
- 1 = Delete primary mail file
- 2 = Delete primary mail file and all replicas

### Rename Accounts

The following is an example etautil command to rename LND accounts using etautil:

```
etautil -d DOEJA01XP -u <eta administrator> -p <password> update
```

```
eTLNDOrganizationName=cai,eTLNDDirectoryName=doeja01w2k3,eTNamespaceName=Lotus
Domino Server' eTLNDAccount eTLNDAccountName='rename me107' eTLNDAdminp=1
eTLNDAccountOperation=3 eTLNDAccountState=3 eTLNDNewLastName=me107
eTLNDNewInitials='' eTLNDNewFirstName=renaming
```

### Move Accounts in Hierarchy

The following is an example etautil command to move LND accounts using etautil:

```
etautil -d DOEJA01XP -u <eta administrator> -p <password> update
'eTLNDOrganizationalUnitName=ou1,eTLNDOrganizationName=cai,eTLNDDirectoryName=doe
ja01w2k3,eTNamespaceName=Lotus Domino Server' eTLNDAccount eTLNDAccountName='move
me202' eTLNDAdminp=1 eTLNDAccountOperation=5 eTLNDAccountState=5
eTLNDNewOrganization='eTLNDOrganizationName=cai'
```

### Recertify Accounts (by Exact Date and by Number of Months)

The following are example etautil commands to recertify users by using both Provisioning Manager and etautil**.**

*By exact date:*

```
etautil -d DOEJA01XP -u <eta administrator> -p <password> update
'eTLNDOrganizationName=cai,eTLNDDirectoryName=doeja01w2k3,eTNamespaceName=Lotus
Domino Server' eTLNDAccount eTLNDAccountName='exp date01' eTLNDAdminp=1
eTLNDAccountOperation=1 eTLNDAccountState=1 eTLNDExpiration='10/13/2010 12:00:00
PM'
```

*By number of months:*

```
etautil -d DOEJA01XP -u <eta administrator> -p <password> update
'eTLNDOrganizationName=O:cai,eTLNDDirectoryName=doeja01w2k3,eTNamespaceName=Lotus
Domino Server' eTLNDAccount eTLNDAccountName='exp date01' eTLNDAdminp=1
eTLNDAccountOperation=1 eTLNDAccountState=1 eTLNDExpireMonths=24
```

To confirm that the ID was recertified correctly, perform a "Refresh Status" on the account in Provisioning Manager to update the Archive document. Also view the account in Provisioning Manager to ensure the expiration date displays properly.

### Cannot Open Database on Remote System

**Symptom:**

To open a database on a remote system, that system must list the server where the agent is running as a trusted server.

**Solution:**

Run the explore and correlate on the LND endpoint to remove the eTLNDHomeServer attribute from the repository.

## Microsoft Active Directory Services Connector

The Active Directory Services Connector lets you administer accounts, groups, containers, printers, computers, and shared folders on Active Directory Services servers.Using the connector you can do the following:

- Register endpoints, explore them for objects to manage, and correlate their accounts with global users
- Create and manage Active Directory Services accounts using account templates specific to Active Directory Services
- Synchronize global users with their roles or synchronize global users' accounts with their account templates
- Change account passwords and account activations in one place
- Assign an Active Directory Services account template to each of your Active Directory Services endpoints
- Use the default Endpoint Type account template to create accounts with the minimum level of security needed to access an Active Directory Services directory
- Create and manage Active Directory Services groups, containers, printers, shared folders, and computers
- Generate and print reports about Active Directory Services accounts

# Configure Your Windows Servers Using SSL

Perform the following steps if you are using Secure Socket Layer (SSL) communication:

1. Install the High Encryption Pack on the Active Directory Services (ADS) server you want to manage.
2. Install and configure a Certificate Authority (CA).
3. Set up ADS, the Certificate Authority, and CA IdentityMinder on a single system, on a dual computer system, or on multiple computers.
4. Verify the C++ Connector Server service logon ID.

**Note:** SSL communication is not mandatory when using the Active Directory Services Connector. However, if you do not use SSL communication, you are not able to use the password management features of the Active Directory Services Connector.

## Step 1. Install the High Encryption Pack

You should have the High Encryption Pack for Active Directory Services installed. To verify this, from the Internet Explorer menu, select Help, About Internet Explorer. The Cipher Strength should be listed as 128-bit. If it is not, you need to install the High Encryption Pack.

If necessary, download the High Encryption Pack for Active Directory Services from the Microsoft web site (the pack is free of charge).

Install the High Encryption Pack on the Active Directory Services servers that you want to manage with CA IdentityMinder.

## Step 2. Install and Configure a Certificate Authority

There are two types of Certificate Authority you can install, each of which can be either the root or a child. This document addresses the use of one of the types of Root CAs, either an Enterprise Root CA or a Standalone Root CA.

For information on installing one of these CAs:

- For Windows 2000, refer to Microsoft Knowledge Base Article #231881 at the following URL;

  http://support.microsoft.com/kb/231881

- For Windows 2003, refer to the section "Installing and Configuring a Certification Authority" of TechNet library for Windows 2003 at the following URL:

  http://technet.microsoft.com/en-us/library/cc756120(WS.10).aspx

- For Windows 2008, refer to the section "Install a Root Certification Authority" on TechNet library for Windows 2008 at the following URL:

  http://technet.microsoft.com/en-us/library/cc731183(WS.10).aspx

## Step 3. Set Up ADS, Certificate Authority, and CA IdentityMinder

To establish trust of root certification authorities in post-Windows 2000 servers, you must use trusted root certification authority in group Policy to distribute your organization's root certificates. For more information, see the section *Add a trusted root certification authority to a Group* on the TechNet library for Windows 2003:

http://technet.microsoft.com/en-us/library/cc738131%28v=ws.10%29.aspx

For exact steps on how to add a trusted root certification authority to a Group Policy object, see the section *Manage Trusted Root Certificates* on the TechNet library for Windows 2008:

http://technet.microsoft.com/en-us/library/cc754841.aspx

You can set up ADS, the Certificate Authority, and CA IdentityMinder on a single system or distributed across multiple computers.

### Step 3a. Set Up on a Single Computer

When the C++ Connector Server and Active Directory Services are installed on a single machine, it should not be necessary to do anything with certificates, as the machine inherently trusts itself.

### Step 3b. Set Up Multiple Systems

When the C++ Connector Server is installed on an individual system (separate from ADS Certificate Authority,) for the Active Directory Connector to manage Active Directory it is necessary to import the trusted root certificate on the system hosting the C++ Connector Server.

There are various ways of importing the certificate and this can be done by using web enrollment or by using export/import procedure.

The sample steps  in the following topics are provided only as a guide and may differ for different versions of Windows. Refer to the appropriate Microsoft documentation for specific instructions.

## Import the Root Certification Authority Using Web Enrollment

Use the following procedure to import the root certification authority.

**On the machine hosting the C++ Connector Server**

1. Open a web browser and access the URL, http://CA_FQDN/certsrv.
2. Select Retrieve the CA certificate or certificate revocation list. (On some platforms, this option may appear as Download a CA certificate, certificate chain, or CRL.)
3. Select Install this CA certification path. (On some platforms, this option may appear as Install this CA certificate chain.)

## Import the Root Certification Authority Using Manual Export/Import Process

If Certificate Authority is not set up with web access, you can manually export the certificate on the Certificate Authority machine and import it to the C++ Connector server.

For more information, see the section "Importing and Exporting Certificates" on the TechNet library at the following URL:

http://technet.microsoft.com/en-us/library/cc738545%28WS.10%29.aspx

## Step 4. Verify the C++ Connector Server Service Logon ID

In the previous step, you set up a trust relationship. Normally, the account used to start the C++ Connector Server is Local System account. To manage ADS however, this account should be the same account that acquired the Root Certification Authority in Step 3. Use the following procedure to ensure that the service is logged on properly.

**From the Control Panel**

1. Select Administrative Tools, Services.
2. Double-click the C++ Connector Server entry.
3. Verify that the account (a local administrator or a domain administrator) being used to run the service is the same account that was used to install the Root Certification Authority.
4. Verify that the account password is correct.
5. If you have changed either the account or password, restart the C++ Connector Server service.

## Install Without a Microsoft Certificate Authority

If you are not able to install a Microsoft certificate authority, you must acquire the certificates for all of your domain controllers and any you add in the future.

**To acquire the certificates**

- Purchase the certificates using the fully qualified machine names for the domain controllers from trusted certificates vendors and handle the renewal activity based on the terms that are agreed upon.
- Create and maintain your own certificates using tools that are available to you.

  **Note:** Two certificates are usually received for each domain controller, a certificate authority certificate and a certificate for the machine.

Once you have received the certificates, you can use the mmc.exe utility to install them. You must also install the certificate authority certificate on all of your Provisioning Servers and the machines where the C++ Connector Server is installed.

## Connect to a Child-Domain

If you are using SSL, and want to use CA IdentityMinder to manage a child-domain, you must establish permissions within Active Directory so that the child-domain can refer to the Certificate Authority that is defined on the parent domain. This is required if you are using an Enterprise Certificate Authority.

Please refer to the following Microsoft articles for further instructions on this:

- Q281271 - Win2000 Certification Authority Configuration to Publish Certificates in Active Directory of Trusted Domain
- Q271861 - Windows Cannot Find a Certificate Authority that Processes the Request

**Note:** Confirm that your DNS configuration is correct. From both the parent and the child, you should be able to ping the other and receive back the correct IP address. Likewise, you should be able to run an 'nslookup' command on the IP address and receive back the correct fully-resolved name of the other.

If you are using SSL, and experience errors when you attempt to manage a child domain, you can use the standalone ADSLDAPDiag utility to connect to the child domain. ADSLDAPDiag is located in the bin folder of the C++ Connector Server installation. For example:

```
C:\Program Files\CA\CA IdentityMinder\Provisioning Server\bin
```

**Note:** ADSLDAPDiag should be run on the same machine as the C++ Connector Server. If ADSLDAPDiag fails, this indicates that the CA IdentityMinder-errors are due to an SSL problem with the child domain (the syntax of ADSLDAPDiag is: ADSLDAPDiag *fully_qualified_name_of_the_ADS_server*).

**Important!** If your Certificate Authority is installed on a Windows 2003 server, auto-enrollment for the child domain needs to be working properly before a proper trust relationship can be established between the parent and child domains.

# ADS Defaults

Once the Active Directory Services Connector has been installed and configured, you have everything that you need to run and use the connector. The following sections describe the basic ADS Connector settings and their defaults.

## Failover

B default, Failover is not enabled. To enable Failover, set the environment variable ADS_FAILOVER to 1 and restart the C++ Connector Server and the Provisioning Manager.

**Note:** If the Provisioning Manager and the C++ Connector Server run on different machines, you must set the ADS_FAILOVER variable on both machines.

After failover is enabled, you can turn on failover support for individual directories by going to the Endpoint Property Sheet and checking the failover checkbox on the Failover tab.

## Understanding Failover

Prior to Windows 2000, Windows NT supported multiple domain controllers: Primary (PDC) and Backup (BDC). You could query any controller for information, but changes could only be made to the PDC. Active Directory, introduced as part of the Windows 2000 Server, goes a step further. It allows all controllers to be primaries, and a change to any one controller is automatically propagated to the other controllers.

This allows CA IdentityMinder, which is used to manage an installation, to have failover support. For example, ADS is communicating with a single domain controller and it goes down. ADS then automatically connects to an alternate domain controller and retries the failed operation. Thereafter, all communications happen with the alternate controller.

For technical reasons, it is advantageous to establish an order in which the controllers are to be used. This can be done from the Failover page on the Endpoint property sheet. This page automatically displays the alternate controllers (as retrieved from DNS) and allows the user to prioritize them.

In the background, ADS periodically attempts to reconnect to any failed controllers. When ADS detects that a failed controller of a higher priority than the current controller is back online, it automatically reroutes the next request to the restored controller.

## Using Failover

**IMPORTANT!** By default, ADS Failover logic is disabled. If you decide to use Failover, you must be aware of the following Failover behaviors. Otherwise, you will encounter unexpected Failover behaviors. Please review this section carefully.

- If you wish to activate Failover, you must set the environment variable ADS_FAILOVER to 1.

  Note: ADS_FAILOVER should be set on the machine where the C++ Connector Server and ADS connector run, and on the machine where the Provisioning Manager runs.

- The specified server name (the name of the Active Directory server specified on the Endpoint page) should match its fully qualified DNS server name.

- You should consider enabling logging when using Failover. (For more information, see the Endpoint Logging page on the Endpoint property sheet.) With logging enabled, in the event of unexpected behaviors, the logs provide a record of what transpired.

- The Provisioning Server attempts to retrieve the complete list of backup domain controllers from DNS, or you may elect to supply this list manually.

  If DNS is not available or you want to bypass DNS, you may supply a configuration file *PS_HOME*\data\ads\*directory-name*.DNS. (A sample DNS-configuration file is provided in the distribution of the file *PS_HOME*\data\ads\endpoint-*name*.dns.)

  where endpoint-*name* is the name of the endpoint that you specified in the Name field on the ADS Server tab of the ADS Endpoint property sheet.

  In order to view the list of domain controllers, select the Failover tab in the Endpoint property sheet. This page provides the list of domain controllers that ADS uses for failover. If there is only one item in the list (the primary server being managed), or failover was not enabled using the ADS_FAILOVER environment variable, then this page is disabled and failover is not operational.

  Whether CA IdentityMinder can determine the list of backup controllers automatically from DNS is heavily dependent on your environment. If this attempt fails, try one of the following suggestions:

  - Run the Provisioning Server in the same domain as the ADS Server.
  - Set the preferred DNS server field on the Provisioning Server correctly.
  - Run the Provisioning server under a domain-administrator account.

  If all of your domain controllers in your enterprise are not listed on the Failover tab, then failover was unable to retrieve the list from DNS. You must manually provide the .dns config file.

  You can run the ADSListSites *servername* diagnostic utility to determine what information DNS is returning. If a list of sites or servers is returned, then automatic failover is operational. If ADSListSites is not configured for automatic failover, you will have to manually supply the list of domain controllers.

- If you are using SSL, Provisioning Server must be able to connect to all domain controllers listed on the Failover tab of the Endpoint page using SSL. You must configure each of these servers to present a valid acceptable certificate to the Provisioning Server.

  If SSL is used, all the domain controllers associated with a single endpoint must be able to communicate with CA IdentityMinder using SSL. If an SSL connection cannot be established with any one of the domain controllers, then you should not use SSL, or you should omit that domain controller in the .dns configuration file.

- Active Directory guarantees that all changes made on any one domain controller are propagated to all other domain controllers. The time that the propagation occurs is installation-defined.

- You must be aware of the effects of propagation delays.

  For example, if the Provisioning server makes a change to a controller that subsequently goes down, and CA IdentityMinder automatically connects to a backup controller, any changes made earlier may not yet be reflected on the backup because of propagation delays. This can have adverse results.

  That is, if Provisioning Server is communicating with the primary server and encounters a failure, it immediately switches to the secondary server.  If the user subsequently creates accounts on the secondary server, and the primary comes back up, ADS reconnects to the primary.

  If Active Directory has not propagated the new accounts from the secondary to the primary controller, you receive a not-found error when you attempt to view the new accounts from CA IdentityMinder. This occurs because the account does not yet exist on the primary server.

  Even more serious is the case in which you proceed to do an Explore (executed on the primary, now that the connection is restored). When Explore fails to find the newly created accounts, it assumes they have been deleted from the target system. Consequently, CA IdentityMinder then deletes the accounts from the repository.

  **Note:** You may also encounter a situation wherein conflicting changes made on different controllers could cause one of them to be lost.

- There are separate timeouts for the agent and for the Provisioning Manager.

  For example, if the agent timeout value is one minute, and the Provisioning Manager timeout is 90 seconds, when CA IdentityMinder attempts to communicate with a particular controller, it takes a full minute before the agent gives up. If the secondary controller is also down, another minute lapses before the agent declares the backup as down and attempts the tertiary controller. In the meantime, the Provisioning Manager times out and the initial operation fails, although the (tertiary) controller was actually available.

- When you change the order of the controllers on the Failover tab, the changes are only in effect for subsequent connections to the server (for example, a new user logs in, or the original primary controller goes down). However, existing valid connections continue to be used until the background process runs again and attempts a better connection.

- Although you can order the controllers in any desired sequence on the Failover tab, the server always arranges the list so that the primary server (that is, the one used on the Endpoint page) is always first. This prevents an inadvertent connection to an alternate controller during a restart.
- As mentioned previously, a background thread runs periodically to attempt to reestablish existing connections to the more preferred domain-controller. By default, this thread runs every 15 minutes. However, you can change this setting by setting the environment variable ADS_RETRY to the desired number of minutes.

## Failover Retry Interval

The default for Failover Retry Interval is 15 minutes. When failover is enabled and the domain controller(s) are down, the ADS connector periodically checks the downed domain controller(s). To increase or decrease the interval time (in minutes), set the ADS_RETRY environment variable and restart the C++ Connector Server. If the value is set to less than one minute, the value is ignored and a one minute interval is used.

## ADSI Option

**Important!** ADSI is not fully supported in this release and, by default, is disabled. Contact technical support to enable this option.

ADS lets you use a non-SSL connection to the Active Directory Server so you can use ADS in a test environment when enabling SSL is not feasible. The non-SSL connection lets you connect in one of the following two ways:

- Use ADSI for passwords only and non-secure LDAP for everything else.
- Use non-secure LDAP for all communications. This option silently ignores all password change requests.

**Note:** Both options use a normal authentication with LDAP that sends the user's credentials over the network. This practice can be a serious security risk. Neither of these options should be used in a production environment.

ADSI provides a way to manage accounts and passwords with SSL. This option uses ADSI to set passwords while all other operations use a non-secure LDAP connection.

ADSI does not work in all environments, particularly in cross-domain networks. Only use this option when you do not want to use the non-SSL option.

If ADSI does not work, try the following:

- Install the Windows 2000 Support Tools on the Active Directory Services server you want to manage.
- Run the Provisioning Server in the same domain as the Active Directory server.
- Confirm that the Preferred DNS server field is set correctly on the Provisioning Server.
- Start the Provisioning service with an ADS-domain -administrator account.

**WARNING!** Do not use the ADSI or non-secure LDAP options in production environments.

## ADS_MANAGE_GROUPS

For an account template marked as strong sync policy, previously for account sync operation (that is, Synchronize Account with Account Template, or Check Account Sync) the ADS option may fail to find remote Universal Group that the account belongs to. For example, if an account on domain D1 is a member of a Universal Group on domain D2, a sync operation may not notice that the account belongs to that remote Universal Group.

CA IdentityMinder supports a mode where the user can specify whether to search the global catalog to find Remote Universal Groups that the account may be a member of, when performing a sync operation.

In some environments, not all domains of an Active Directory forest are managed by CA IdentityMinder. For example, a hypothetical AD forest has three domains, D1, D2 and D3. You have two CA IdentityMinder-managed domains D1 and D2 (that is, you acquire D1 and D2). You can specify whether the new global catalog search feature manages Universal Groups from all domains (D1, D2, and D3), or just the CA IdentityMinder-managed domains (D1 and D2). If you choose to have the new global catalog search feature only deal with CA IdentityMinder-managed domains, then CA IdentityMinder will not deal with groups on domain D3, even if the account belongs to a group that resides on domain D3. For example, if the account's policy indicates that it should not belong to any group, and your account belongs to a Universal Group on domain D3, a check account sync operation will not show that the account is out-of-sync, if you chose to deal only with CA IdentityMinder-managed domains. If you chose to deal with all domains, then the account will be considered out-of-sync (even when domain D3 is not managed by CA IdentityMinder).

By default the sync feature is off.

To run this global catalog search feature, you have to set the environment variable ADS_MANAGE_GROUPS.

ADS_MANAGE_GROUPS can be set to xy as defined in the following paragraphs.

The first digit x - can be 0 or 1:

- 0 - You get the current behavior (default).
- 1 - Optional behavior to query using the global catalog as well.

The second digit y - can be 0 or 1:

- 0 - Deal with groups in all domains (whether they are managed by CA IdentityMinder or not).
- 1 - Deal with groups in CA IdentityMinder-managed domains only.

**Note:** The x value must be set to 1 in order for the y value to have any affect.

Once this environment variable is set, you must restart the C++ Connector Server for the variable to take effect.

## Force Logging

The default for force logging is 0 for no force log. To enable force logging, even if the endpoint has logging turned off, set the environment variable ADS_FORCELOG to 1 and restart the C++ Connector Server.

## Ignore Group Insufficient Rights Error

The default for ignore group insufficient rights error is set to false, (do not ignore group insufficient rights error).

When you perform a delete operation to delete a user from a remote group and get back a permissions-error (insufficient rights), you can set the environment variable ADS_NOGROUP_PERMS to 1 to ignore this error and consider the operation a success.

## Extend the ADS Schema

The ADS connector lets you manage additional attributes that are used by your Active Directory implementation including, the extended ADS schema you may have implemented on your Active Directory system. If you want to have CA IdentityMinder manage these extended attributes, create a flat file called *PS_HOME\data\ADS\schema.ext.* This file should contain a list of the extended attributes that you want to manage.

**Note:** Not every attribute is manageable through CA IdentityMinder as the Active Directory does try to protect certain sensitive ones.

Each attribute should be listed on a single line by itself and have the same name as the LDAP display name of the attribute on the target ADS system. For example, if the LDAP display name of the attribute on the target system is extendedAttribute, the attribute name in the schema.ext file needs to be extendedAttribute. The LDAP display name can be found under the Name column of the Active Directory Schema\Attributes or the attribute name when you use the JXplorer to connect to the Active Directory and browse a user account.

With this file in place, (you may have to recycle the Provisioning Server), the Provisioning Manager will then display an additional property page called Custom for both account templates and accounts. This page provides a list of all the extended attributes and their values.

**Notes:**

- The ADS schema should already be extended on the target machine in order to see the extended attributes.
- CA IdentityMinder assumes that these extensions are in effect for the entire enterprise.

Once the extended ADS schema has been configured in CA IdentityMinder, the extended ADS attributes can be mapped to global user's attributes/custom fields by using rule strings in ADS account templates. For more information on how to create custom fields for Global User objects and how to use rule strings, see the *Administrator Guide.*

## Modify the schema.ext File

You can modify the schema.ext file (for example, add or remove attributes) and have the changes picked up by existing objects by restarting the C++ Connector Server and establishing a connection to the target system after making your changes. For example, a connection to the target system can be established by opening the Explore/Correlate window or opening properties of an account from the Provisioning Manager.

Any new attributes that are added to the schema.ext file can be found in the list of extended attributes on the Custom tab on the ADS Account or ADS Account Template property sheet. Attributes that are removed from the schema.ext file are handled in one of two ways:

- From the ADS Account property sheet, the attributes will be automatically removed from the list of extended attributes on the Custom tab.
- From the ADS Account Template property sheet, under the Valid column, the attributes will be marked as invalid (N). The attribute can then be removed and deleted from the provisioning repository.

## Correlate ADS Extended Attributes

Extended Active Directory schema attributes that are set for a particular account are stored together with their values in the account's attribute called 'eTADSpayload' (user-friendly name 'payload') in the following format:

```
<extendedAttributeName1>:<reservedValue>:<valueLength>=<value>;<extendedAttribute
Name2>:<valueN>
```

**Note:** <reservedValue> is a value reserved for future use. It is currently always set to 01.

Attribute mapping can be set from the managed ADS endpoint by specifying a mapping function substring with an offset and length. For more detailed information, see the section Explore and Correlate Parameters in the *Administrator Guide*.

```
GUAttrName[=Endpoint Type:AccountAttrName[:Offset,Length]]
```

The following is an example of mapping the extended attributes to a global user's custom attributes:

```
eTADSpayload
extendedAttribute1:01:0006=value1;extendedAttribute2:01:0007=value10;extendedAttr
ibute2:01:0008=value100

eTCustomField01=eTADSpayload:SUB(28,6)
eTCustomField02=eTADSpayload:SUB(62,7)
eTCustomField03=eTADSpayload:SUB(97,8)
```

We can see that the attribute mapping mechanism is using substring (SUB) and specifying the offset and the length of the value.

**Important!** The mapping extended ADS attributes mechanism has limited functionality and is not intended to support the full functionality of built-in ADS attributes. The mechanism assumes that all of the following conditions are true:

- Extended attributes that are defined in the attribute map must be set for all managed accounts.
- The values of the extended attributes that are defined in the attribute map must have a fixed length.

# ADS Support for FIPS and IPv6

The ADS Connector does not support IPv6.

# Connector-Specific Features

This section details your connector's specific management features, such as how to acquire and explore your endpoint. Also included are account, provisioning roles, account template, and group information specifically for your connector.

## Acquire an ADS Server Using the User Console

You must acquire the Active Directory Services server before you can administer it with CA IdentityMinder.

**To acquire an Active Directory Services server using the User Console**

1. Select Endpoints, Manage Endpoints,Create Endpoint
2. Select ActiveDirectory from the drop-down list box on Create a new endpoint of Endpoint Type, and click Ok

   Use the Create Active Directory Endpoint page to register an Active Directory Services server. During the registration process, CA IdentityMinder identifies the Active Directory Services server you want to administer and gathers information about it.
3. After entering the required information, click Submit.

   You are now ready to explore and Correlate the endpoint.
4. Click Endpoints, Explore and Correlate Definitions, Create Explore and Correlate Definition to explore the objects that exist on the endpoint.

   The Exploration process finds all Active Directory Services accounts and groups. You can correlate the accounts with global users at this time or you can correlate them later.
5. Click OK to start a new definition.
6. Complete the Explore and Correlate Tab as follows:
   a. Fill in Explore and Correlate name with any meaningful name.

      Click Select Container/Endpoint/Explore Method to click an Active Directory endpoint to explore.

   b. Click the Explore/Correlate Actions to perform:

      - **Explore directory for managed objects**—Finds objects that are stored on the endpoint and not in the provisioning directory.
      - **Correlate accounts to users**—Correlates the objects that were found in the explore function with users in the provisioning directory. If the user is found, the object is correlated with the user. However, you can instead select that you want to assign the account to the existing user (the default user) or create the user.
      - **Update user fields**—If a mapping exists between the object fields and the user fields, the user fields are updated with data from the objects fields.

7. Complete the Recurrence tab if you want to schedule when the task to executes.

   a. Click Schedule.

   b. Complete the fields to determine when this task should execute.

      You may prefer to schedule the task to execute overnight to interfere less with routine access of the system.

   **Note**: This operation requires the client browser to be in the same time zone as the server. For example, if the client time is 10:00 PM on Tuesday when the server time is 7:00 AM, the Explore and Correlate definition will not work.

8. Click Submit.

**To use an explore and correlate definition**

1. In a CA IdentityMinder environment, click Endpoints, Execute Explore and Correlate.
2. Click an explore and correlate definition to execute.
3. Click Submit.
4. The user accounts that exist on the endpoint are created or updated in CA IdentityMinder based on the explore and correlate definition you created.

## Acquire an ADS Server Using the Provisioning Manager

You must acquire the Active Directory Services server before you can administer it with CA IdentityMinder. When acquiring an Active Directory Services server, perform the following steps from the Endpoint Type task view:

1. Register the server as an endpoint in CA IdentityMinder.

   Use the Active Directory Services Endpoint property sheet to register an Active Directory Services server. During the registration process, CA IdentityMinder identifies the Active Directory Services server you want to administer and gathers information about it.

2. Explore the objects that exist on the endpoint.

   After registering the server in CA IdentityMinder, you can explore its contents. Use the Explore and Correlate Endpoint dialog. The Exploration process finds all Active Directory Services accounts and groups. You can correlate the accounts with global users at this time or you can correlate them later.

3. Correlate the explored accounts with global users.

   When you correlate accounts, CA IdentityMinder creates or links the accounts on an endpoint with global users, as follows:

   a. CA IdentityMinder attempts to match the logon name with each existing global user name. If a match is found, CA IdentityMinder associates the Active Directory Services account with the global user. If a match is not found, CA IdentityMinder performs the next step.

   b. CA IdentityMinder attempts to match the display name with each existing global user's full name. If a match is found, CA IdentityMinder associates the Active Directory Services account with the global user. If a match is not found, CA IdentityMinder performs the next step.

   c. If the Create Global Users as Needed button is selected, CA IdentityMinder creates a new global user and then associates the Active Directory Services account with the global user. If the Create Global Users as Needed button is cleared, CA IdentityMinder performs the next step.

   d. CA IdentityMinder associates the Active Directory Services account with the [default user] object.

## Re-Initialize an ADS Endpoint

**Note:** Certain Active Directory settings rarely change and for performance gain, the ADS connector only reads the data once when the endpoint is initialized and stores the value internally instead of reading the value on each operation. So, if these settings change, the ADS connector needs to be re-initialized to review the new values.

Some events require that the C++ Connector Server to be restarted include the following:

- Group account template changes are made on the ADS system, for example, changing password account template. You must also restart the Provisioning Manager after making these changes.
- Failover seems to be configured, but is not working.
- Either the administrative user (used to acquire an ADS endpoint) or the administrative users' password is updated.

To restart the C++ Connector Server, follow these steps:

1. Select Start, Settings, Control Panel, Administrative Tools, Services.
2. Right-click the C++ Connector Server entry and select Restart.
3. Click Yes when prompted to restart the CA IdentityMinder Provisioning service.

## ADS Default Account Template

The Active Directory Services Default Account Template, provided with the Active Directory Services connector, gives a user the minimum security level needed to access an endpoint. You can use it as a model to create new account templates.

**Note:** You can create ADS account templates that are associated with multiple endpoints. These account templates can only be used to grant privileges to existing accounts.

## Special Characters for ADS

ADS objects cannot contain an equal sign (=) and comma (,) in the same object common name.

## New ADS Accounts

Use the New Object - Account wizard to create new accounts.

## Account Management - Map a Certificate to an Account Object

To map a certificate or certificates to an account object, use the Security Identity Mapping or User Certificates Tabs from an ADS Account Property Sheet.

## Relocate Accounts

Using the Relocate Accounts function in the Provisioning Manager, you can specify that an account belonging to a account template be moved to the container that is specified by the container rule within the account template. You can also request that all accounts belonging to an account template be moved to their respective containers.

In ADS, the container rule selects a container based on global user attribute values that allow one account template to prescribe different containers for different accounts. The Relocate Accounts function re-evaluates the rule using current global user attribute values and moves each account to the prescribed container.

For accounts, a list of assigned account templates for the account is retrieved and if there is only one account template, an LDAP operation for the account is issued using that account template value. If there is more than one account template assigned to an account, a list of account templates to choose from is retrieved. If there are no account templates assigned to the account, an error message is displayed.

For account templates, child Relocate Accounts operations on each account currently assigned to the account template are initiated. These child operations can succeed or fail individually and the completion message for the account template Relocate Accounts operations contains statistics for the following categories:

- Updated - Account moved to new container
- Unchanged - Account already in correct container
- Failure - Problem determining container or moving account

Relocate operations can also be executed with the Batch Utility (etautil).

- For Account Template:

```
etautil -d <eTADomain> -u <eTAUser> p <password> update
eTADSPolicyContainerName=Active Directory
Policies,eTNamespaceName=CommonObjects,dc=<eTADomain> eTADSPPolicy
eTADSPolicyName=<policyeName> to eTRelocateAccounts=1
```

- For Account:

```
etautil -d <eTADomain> -u <eTAUser> p <password> update
'eTADSContainerName=Users,eTADSDirectoryName=<directoryName>,eTNamespaceName=Acti
veDirectory' eTADSAccount eTADSAccountName=<accountName> to eTRelocateAccounts=1
eTSyncPolicyDN='eTADSPolicyName=<policyName>,eTADSPolicyContainerName=Active
Directory Policies,eTNamespaceName=CommonObjects,dc=<eTADomain>'
```

## User Groups

You can create and maintain user groups using the Endpoint Type task view. Use the Active Directory Services User Group property sheet when managing your groups.

## Group Management - Changing Group Scope

The ADS connector lets you change the scope and type of groups in native mode only.

The following sections list the scopes that can be changed along with their rules for changing.

### Domain Local to Universal

Domain Local groups can be converted to Universal groups, provided that the following is true:

- The domain local group is not already a member of another domain local group.
- The domain local group does not contain any other domain local groups.

### Global to Universal

Global groups can be changed to Universal groups.

### Universal to Domain Local

Universal groups can be changed to Domain Local groups only if the change is written to the Global Catalog (GC).

**Note:** If the original Universal group has any members that cannot be a member of a Domain Local group, the request to convert fails.

### Universal to Global

Universal groups can be changed to Global groups.

**Note:** If the original Universal group has any members that cannot be a member of a Global group, the request to convert fails.

## Group Management - Changing Group Type

The ADS connector lets you change the scope and type of groups in native mode only.

The following sections list the group types that can be changed along with their rules for changing.

### Distribution to Security

Distribution type groups can be changed to security type groups.

## Security to Distribution

Security type groups can be changed to distribution type groups, but the original group objects access privileges are lost.

**Note:** A warning indicates that changing a group from security type to distribution type may cause a loss of access control for the members of that group.

## Microsoft Best Practices for Group Memberships

Using Microsoft guidelines are recommended when designing how group memberships should be used in ADS, especially where more than one ADS domain is involved. For more information, refer to Microsoft Windows Server 2003 Techcenter, and in particular, the following topics:

- Group Scope; and
- Global Catalog Replication

## Terminal Services

The Terminal Services Tab on the Active Directory AccountTemplate and Account Property Sheets lets you configure the Terminal Services user profile, startup environment, and remote control settings and set the Terminal Services timeout and re-connection settings.

Search (read) of Terminal Services is now done in parallel to improve performance.

**Note:** To set terminal services, the Windows "Workstation" service must be running on the machine where the C++ Connector Server is installed.

## Connecting to the Nearest Domain Controller

Since an Active Directory domain consists of multiple domain controllers, the question to which domain controller should ADS commands be sent is now extremely important.

The ADS connector lets you choose from the following options, which domain controller to target:

- Always use the primary domain controller
- Direct the commands to the closest domain controller
- Allow the caller to manually specify the intended target domain controller

See the ADS section of the Provisioning Manager online help for more information on setting your preferences for connecting to the nearest domain controller.

## Resource Management

The ADS connector lets you manage various resources, including computers, printers, and shared folders. New property pages have been created to support these resources.

### Computers

The Computer property sheet lets you add and delete computers. A list of associated printers is also displayed. For creation, you can only enter the computer name and pre-Windows 2000 computer name.

A button to launch the Windows MMC Computer Management tool is also available. Since this tool supports numerous functions, the ability to perform any given function depends on the credentials of the user making the request. Clicking this button launches an additional dialog giving you three different options for selecting credential. They are as follows:

1. Use the Global-User Administrator's credentials
2. Use the Window's credentials of the logged in user
3. Use an alternate set of credentials that the user must manually enter

**Note:** Options 1 and 3 are only supported on Windows 2000 (or Windows XP) platforms. When running on an NT platform, these options are disabled.

### Printers

The Printer property sheet lets you add and delete printers. For creation you can only enter the server and printer name. A button to launch the Windows Print Queue is also available for printer and print job management.

**Note:** If you set the attribute on the endpoint using native tools, owner of the printer, shared folder, or group cannot be set.

### Shared Folders

The Shared Folders property sheet lets you add and delete shared folders. For creation you can only enter the server and share name. A button to launch the Windows MMC Computer Management tool is also available for shared folder management.

**Note:** If you set the attribute on the endpoint using native tools, owner of the printer, shared folder, or group cannot be set.

## Paged Searches

Active Directory normally restricts the number of objects that can be returned in a single search operation. To ensure successful management of containers with a large number of objects (that is where the number of objects exceeds the maximum), ADS implements a paged-search operation.

**Note:** A page is defined as the number of objects that can be returned in a single search.

If too many objects are returned in a single page, ADS queries the Active Directory server for one page at a time. It continues to query Active Directory, until it retrieves the entire set of objects. This process is automatically handled by the ADS agent, so you do not need to control the paging operation.

Although this is normally not necessary, you can adjust the page size. To do this, you must set the environment variable ADS_SIZELIMIT. However, you should never set this value larger than the limit on the Active Directory server. If you set the value too large, it may negatively impact performance on the Active Directory server. (To change the value on the server, see the section, Changing the Active Directory Search Limit).

**Note:** The ADS_SIZELIMIT variable should be set on the machine where the C++ Connector Server and ADS connector run.

## Change the Active Directory Search Limit

For servers with an excessive number of accounts or groups in a single endpoint, ADS automatically does a paged search to retrieve all objects, thus it should not be necessary to increase the search limits.

However, if you choose to increase this limit, you should modify the following parameters for Active Directory:

- MaxPageSize, the maximum page size that is supported for LDAP responses. The default is 1000 records.
- MaxResultSetSize, the maximum size of the LDAP result set. The default is 262144 bytes.

By default, these objects are located at:

```
CN=Default Query Policy,CN=Query-Policies,CN=Active Directory Service,CN=Windows
NT,CN=Services,CN=Configuration
```

Increase the values of these parameters to meet your needs. If necessary, consult your ADS system administrator for recommended values.

You can use the Windows 2000 NTDSUTIL.EXE utility to modify these parameters. Start the utility and select the LDAP Policies option from the prompt. For detailed instructions to use this utility, see article Q315071 on the Microsoft web site.

## Move Functions

There are several ways to move accounts and groups in ADS. The following sections describe using LDAPMODRDN command, and Relocate to Sync with Account Template.

## Provisioning Manager

If you want to move an account or group from one Organizational Unit to another, follow these steps:

1. List the account or group
2. Right-click on the account or group to be moved
3. Select the Move menu item.

   A dialog appears and you can select the Organization Unit that you want to move to.

## Relocate to Sync with Account Template

Another Move task you can perform from the Provisioning Manager is the Relocate to Sync with Account Template. If your accounts have been moved around and you want to move them back to the Organizational Unit that is specified in their account template, follow these steps:

1. From the Provisioning Roles Task Frame, list the account template.
2. Right-click the account and select Relocate.

The accounts are moved into the correct Organization Unit as specified in their account template.

## LDAPMODRDN Command

You can also use the following ldapmodrdn command to specify the new Organization Unit for an ADS account or group:

```
ldapmodrdn -h localhost -p 20389 -D
"eTGlobalUserName=etaadmin,eTGlobalUserContainerName=Global
Users,eTNamepsaceName=CommonObjects,dc=<your_eta_domain>,dc=eta" -w
<etaadmin_password> -s
"eTADSOrgUnitName=<original_ou_name>,eTADSDirectoryName=<your_ads_name>,eTNamespa
ceName=ActiveDirectory,dc=<your_eta_domain>,dc=eta"
eTADSAccountName=<account_name>,eTADSOrgUnitName=<target_ou_name>,eTADSDirectoryN
ame=<your_ads_name>,eTNamespaceName=ActiveDirectory,dc=<your_eta_domain>,dc=eta"
"eTADSAccountName=<account_name>"
```

## ETAUTIL Tool

You can use the ETAUTIL tool to sync with the account template. To relocate an account to the Organizational Unit according to the account template by running the following command:

```
etautil -d <domain> -u <user> -p <pass> UPDATE '<ADS Policies Base DN> eTADSPolicy
eTADSPolicyName='<policyName>' to eTRelocateAccounts='1'
```

For example:

```
etautil -d sup154 -u etaadmin -p adminadmin UPDATE 'eTADSPolicyContainerName=Active
Directory Policies,eTNamespaceName=CommonObjects' eTADSPolicy
eTADSPolicyName='ADSAccountPolicy1' to eTRelocateAccounts='1'
```

## Move Using ETAUTIL

Important! Using the ETAUTIL tool to move accounts or groups is not recommended.

ETAUTIL does not actually move the account or group, only simulates the move by first deleting the account and then re-adding the account. The newly added account is not exactly the same as the deleted account since there is some internal data that is different in the new account. For ADS, this can be a problem so ETAUTIL is not recommended to move accounts or groups.

## ADS Etautil Conventions

Use the following Active Directory Services conventions in your etautil commands:

- The endpoint type name (eTNamespaceName) is ActiveDirectory
- The endpoint type prefix is ADS. Therefore, the Active Directory Services class names are:
  - eTADSDirectory for an endpoint
  - eTADSPolicyContainer for an account template container
  - eTADSPolicy for an account template

## Reduce the Time to View Accounts

For some systems, viewing account data can take a long time. This delay can be due to the time taken to retrieve terminal services attributes. You can avoid this delay by setting a timeout value for these attributes.

**To reduce the time to view accounts**

1. Set the following configuration parameter:

   ```
   ADS_WTS_TIMEOUT
   ```

   **-1**

   Indicates that the connector does not attempt to retrieve terminal services attributes. Use this option if you do not want to manage these attributes.

   **0**

   (Default) No timeout. The connector waits until terminal services attributes are retrieved.

   **1..*seconds***

   Specifies the time (in seconds) that the connector waits for terminal services attributes to be returned. For example: 1..2147483647.

   You can set this parameter in the following ways:

   - In data\ads\<endpoint_name>.cfg
   - In data\ads\config.opt
   - As a system environment variable

2. Restart the CCS.

## Incomplete or Truncated Search Results When Searching for or Importing more than 20000 Users in CA IdentityMinder or RCM

**Symptom:**

When I search for more than 20000 users in CA IdentityMinder, or try to import more than 20000 users into CA Role and Compliance Manager, the search results only display a maximum of 20000 users. I am using Active Directory 2008 r2 as a data store.

**Solution:**

Microsoft has imposed hard-coded LDAP query limits of 20000 for MaxPageSize and 5,000 for MaxValRange. As a result, the maximum number of users an LDAP query can return is 20000, and the maximum number of attributes a query can return is 5,000.

**Note:** For more information, see Windows Server 2008 R2 or Windows Server 2008 domain controller returns only 5000 attributes in a LDAP response at: http://support.microsoft.com/kb/2009267

To resolve the problem, do the following:

1. If you have Active Directory 2003, 2008, or 2008 r2, set the Active Directory max page size to a high value depending on the number of users you have.

   **Note:** For more information on setting the max page size, see:

   http://support.microsoft.com/kb/315071 ( http://support.microsoft.com/kb/315071)

2. If you have Active Directory 2008 r2 modify the dSHeuristic attribute in Active Directory.

   **Note:** For more information about modifying the dSHeuristic attribute in Active Directory, see:

   http://blogs.technet.com/b/qzaidi/archive/2010/09/02/override-the-hardcoded-ldap-query-limits-introduced-in-windows-server-2008-and-windows-server-2008-r2.aspx

## Program Exits

Program Exits (Common or Native) let you write software that executes during certain actions that CA IdentityMinder carries out. Program exits extend the framework of CA IdentityMinder and allow for additional functionality that can change or augment the standard CA IdentityMinder behaviors.

With CA IdentityMinder Program Exits, you can write the Common Program Exits and configure them to work with ADS. In addition, ADS has its own separate program exits called The Dynamic Link Library (DLL) Interface and Command Line Interface which are described in the next sections.

## Using Program Exits When Creating ADS Objects

The ADS connector can be modified to execute custom or third-party software each time an ADS object is created. You can use one of the following two methods to accomplish this task:

- Dynamic Link Library (DLL) interface
- Command line interface

## The Dynamic Link Library (DLL) Interface

If you create your own Windows DLL with the name ADSOptsExits.dll (case-insensitive) and replace this DLL in the %PSHOME%\Bin directory, the ADS connector will call entry points into the DLL to execute your custom code each time an ADS object is created.

The following two optional entry points (exits) into ADSOptsExits.dll are called from the ADS connector:

- The PreAdd entry point
- The PostAdd entry point

The PreAdd entry point is called immediately before an ADS object is created and the PostAdd entry point is called immediately after an ADS object is created. By implementing these entry points in your version of ADSOptsExits.dll, your custom code is executed each time an ADS object is created by the ADS Connector. From the custom code it is possible to read the attribute values of the new ADS object.

**Note:** The ADS connector is a Windows DLL that is called from the C++ Connector Server process. After ADSOptsExits.dll is added to %PSHOME%\Bin, the C++ Connector Server process must be restarted.

## Sample .CPP file

The following sample .CPP file demonstrates how to construct this DLL. The sample source code assumes the 32-bit edition of Visual C++. Different compilers may require different calling conventions. If Microsoft Visual Studio is used to create the DLL, the Visual Studio project should be created as a Win32 Dynamic Link Library. Use the following defaults for the project settings.

```
#include <stdio.h>
#include <windows.h>
#include <winldap.h>

BOOL APIENTRY DllMain( HANDLE hModule,
                       DWORD  ul_reason_for_call,
                       LPVOID lpReserved
                                          )
{
    switch (ul_reason_for_call)
        {
                case DLL_PROCESS_ATTACH:
                case DLL_THREAD_ATTACH:
                case DLL_THREAD_DETACH:
                case DLL_PROCESS_DETACH:
                        break;
    }
    return TRUE;
}

#ifdef  __cplusplus
#define ADS_C_PROTO     extern "C"
#else
#define ADS_C_PROTO
#endif

// this exit is called immediately prior to the creation of the ADS object
// logfile is NULL or if ADS logging is enabled
//  a handle to PS_HOME\Logs\ADS\eTrustDirectoryName.log
ADS_C_PROTO __declspec(dllexport) int _cdecl PreAdd(const PWCHAR pszDN, LDAPModW
*ppmods[], FILE *logfile)
{
        // example to print fully distinguished name of ADS object
        wprintf(L"In PreAdd %s\n", pszDN);
    if (logfile != NULL)
        fwprintf(logfile, L”PreAdd %s\n”, pszDN) ;
        return 0;
        // return 0 to let the ADS option create the object.
        // return -1 to stop creation of the object
}

// this exit is called immediately after the creation of the ADS object
ADS_C_PROTO __declspec(dllexport) int _cdecl PostAdd(const PWCHAR pszDN, LDAPModW
*ppmods[], FILE *logfile)
{
        // example to print fully distinguished name of ADS object
        // and list the string based attribute values used to create the object
        wprintf(L"In PostAdd %s\n", pszDN);
        for (int i=0; ppmods[i] != NULL; i++)
        {
                if (!(ppmods[i]->mod_op & LDAP_MOD_BVALUES))
                {
                        // string data
                        wprintf(L"Attribute name: %s\n", ppmods[i]->mod_type);
                        for (int j=0; ppmods[i]->mod_vals.modv_strvals[j] != NULL;
j++)
                                wprintf(L"   Attribute value %d)%s\n", j,
ppmods[i]->mod_vals.modv_strvals[j]);
                }
        }
    return 0;
    // return 0 to indicate success
    // return -1 to indicate an error
}
```

## The Command Line Interface

The command line interface executes Windows commands as ADS accounts are created. Unlike the DLL interface, the command line interface is not invoked during the creation of all ADS objects. This interface is only invoked when ADS objects with object class user are created.

## Passing Account Attributes

Immediately before each ADS account is created, the command line interface will load the optional file %PSHOME%\bin\ADSExitUsrPreAdd.txt. Each line in the file is inspected and anything that has the form *%LDAP_attribute_name%* is replaced with the actual attribute value of that attribute. (Where *LDAP_attribute_name* is the LDAP name of the attribute on the new ADS account object.)

For example, the ADS connector is creating an ADS account with the givenName of YourName and ADSExitUsrPreAdd.txt contains the line:

```
test.bat “%givenName%.txt”
```

The command line interface replaces this line with the following and then invokes the batch file:

```
test.bat “YourName.txt”
```

Test.bat must not expect user input from the Provisioning Manager since it is running as part of the C++ Connector Server. Test.bat should be placed in the %PSHOME%\bin directory.

Similar to the processing of ADSExitUsrPreAdd.txt, the optional file %PSHOME%\bin\ADSExitUsrPostAdd.txt is processed immediately after an ADS account is created.

If a multi-valued attribute is specified by *%LDAP_attribute_name%*, the attribute values are appended together with a semicolon (;) as a delimiter between each value. If the actual data contains semicolons (;), the command line interface cannot distinguish between the data and the delimiter.

The command line interface does not support the following:

- Binary attributes
- Commands native to the Windows command line interpreter (cmd.exe) in the text file. These commands include: if, call or dir.
- These commands should be wrapped in your own .bat or .cmd file or used with the cmd /c command.

**Note:** The command line interface uses the Windows API CreateProcess on each line in the text file.

## Passing Global User Attributes

When ADS accounts are created through an ADS account template, attributes from the global user associated with the account template can be passed to the Windows command line commands in ADSExitUsrPreAdd.txt and ADSExitUsrPostAdd.txt.

For each global user attribute that is to be passed to the ADS command line interface, a custom ADS attribute must be created. (See the section on Creating Custom ADS Attributes, for more information.) Once a custom ADS attribute is created, the attribute appears in the ADS Account Template property sheet on the Custom page. The custom attributes do not appear on account templates that do not have an ADS endpoint assigned on the Endpoint property page of the account template. A new ADS account template will not display the custom attributes until an ADS endpoint is added on the Endpoint property page and the new ADS account template is saved.

The ADS custom attributes can be assigned to any rule string representing attribute values on the global user. During ADS account creation, the value of the ADS custom attribute contains the global user attribute value that is specified in the rule string. This value is accessible in ADSExitUsrPreAdd.txt and ADSExitUsrPostAdd.txt by specifying the ADS custom attribute name surrounded with the percent sign (%) delimiter. The following is an example:

```
myfile.bat %eTADSExitOnlyDiskSize%
```

## Creating Custom ADS Attributes

The file *PS_HOME*\data\ADS\schema.ext is used to create custom ADS attributes.

**Note:** You must first create this file.

Custom ADS attributes are placed one per line in the text file *PS_HOME*\data\ADS\schema.ext. This file is used to specify any custom ADS account attributes that have been added to the ADS schema and any ADS account attributes that do not actually exist in the ADS schema but are used in ADSExitUsrPreAdd.txt and ADSExitUsrPostAdd.txt. For more information on extending the ADS schema, see the topic Extending the ADS Schema in the ADS Defaults section.

To let the ADS connector know that the custom ADS account attribute being added is to be used for exit processing and does not exist in ADS, the attribute name in schema.ext must begin with eTADSExitOnly. This prefix lets the ADS connector know that the custom attribute can be passed to the ADS connector command line interface. Since the attribute does not exist in the ADS schema, the syntax and the single or multi-value indicator must be included in the schema.ext. These two values follow the attribute name and are delimited with a colon (:). An example of a line in schema.ext follows:

```
eTADSExitOnlyDiskSize:2.2.5.12:T
```

The syntax of the attribute is 2.2.5.12. These syntaxes are defined at the following website:

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/adsi/adsi/mapping_active_directory_syntax_to_adsi_syntax.asp

The following characters indicate the value of the attribute:

- **T** indicates that the attribute is single-valued.
- **F** indicates that the attribute is multivalued.

**Note:** Any changes to the schema.ext require a restart of the CA IdentityMinder Provisioning service and the Provisioning Manager.

By default, any attribute listed is assumed to exist for both contacts and accounts. To indicate that a given attribute is to be defined for accounts or contacts only, add an optional prefix (account) or (contact) to the attribute name. Optionally, you can use the prefix (both) to indicate an attribute is valid for both accounts and contacts.

For example, your installation added three new attributes to the schema. BirthDate is valid for accounts only. SSN is valid for accounts and contacts. DoNotCall is valid for contacts only. You can add these entries into your schema.ext file as follows:

- (account)BirthDate
- (both)SSN
- (contact)DoNotCall

## Example Files

In this example we are creating ADS accounts through an account template. We would like to obtain the value of the homepage and office from the global user and pass it to the command line interface, but we do not want to send that information to the ADS server when the account is created.

This example requires the following files to be in the *PS_HOME*\bin directory:

- ADSExitUsrPreAdd.txt

  ```
  precopy.bat "%CN%" "%eTADSExitOnlyHomePage%" "%eTADSExitOnlyOffice%"
  ```

- ADSExitUsrPostAdd.txt

  ```
  postcopy.bat "%givenName%" "%eTADSExitOnlyHomePage%" "%eTADSExitOnlyOffice%"
  ```

- precopy.bat

  ```
  copy ADSExitUsrPreAdd.txt PreADSExit.txt
  echo object name is %1 >> PreADSExit.txt
  echo home page is %2 >> PreADSExit.txt
  echo office is %3 >> PreADSExit.txt
  ```

- postcopy.bat

  ```
  copy ADSExitUsrPostAdd.txt PostADSExit.txt
  echo first name is %1 >> PostADSExit.txt
  echo home page is %2 >> PostADSExit.txt
  echo office is %3 >> PostADSExit.txt
  ```

- schema.ext

  ```
  eTADSExitOnlyHomePage:2.2.5.12:T
  eTADSExitOnlyOffice:2.2.5.12:T
  ```

When the CA IdentityMinder Provisioning service and Provisioning Manager are restarted using the schema.ext file shown, the attributes listed in this file will appear on the Custom property sheet of the ADS account template. The rule string %UHP% must be placed in the value field of the eTADSExitOnlyHomePage attribute and the rule string %UO% must be placed in the value field of the eTADSExitOnlyOffice attribute. When this account template is used to create new ADS accounts, the homepage and office values of the associated global user are passed to the command line interface.

# Microsoft Exchange Connector

The Microsoft Exchange connector lets you administer mailboxes on Active Directory Services (ADS) servers and is intended to manage Exchange 2000, Exchange 2003, Exchange 2007 and Exchange 2010 mailboxes.

The Microsoft Exchange Connector is designed to run with the Active Directory Services Connector. It provides a single point for all user administration by letting you do the following:

- Create and manage Microsoft Exchange mailboxes for any existing ADS account
- Create and manage new Microsoft Exchange mailboxes
- Create and manage contacts with email addresses and create and delete email addresses of the contacts
- Create and manage Microsoft Exchange distribution lists and groups
- Create and delete email addresses of an existing distribution group
- Generate and print reports about Microsoft Exchange mailboxes
- Explore an ADS/Microsoft Exchange computer, distribution groups, and Microsoft Exchange users

This connector is managed using the Connector and agent installation process. For more information and requirements, click here.

This connector can also be managed using the Connector and C++ Server installation process as well.

# How to Manage Mailboxes

Understanding how to manage your mailboxes is helpful in understanding how the Microsoft Exchange 20xx Connector is integrated into CA IdentityMinder. The Microsoft Exchange 20xx Connector is designed to run in conjunction with the ADS Connector. With the technology from both connectors, you can manage ADS users who have mailboxes.

Because the Microsoft Exchange 20xx Connector runs with the ADS Connector, you will manage ADS objects, not Microsoft Exchange objects. For example, if you want to do the following:

- To acquire a Microsoft Exchange 20xx server, you must acquire its ADS server
- Use an account template that creates Microsoft Exchange 20xx mailboxes, you must create an ADS account template and assign Microsoft Exchange attributes to the account template
- Create mailboxes for global users, you must create the mailboxes using the global users' ADS accounts
- Create distribution lists, you must assign an email address to each of the ADS groups
- Perform a synchronization on mailboxes, you must synchronize the ADS accounts

To manage Microsoft Exchange 20xx mailboxes, install the ADS and Microsoft Exchange 20xx connectors on your Provisioning Server.

**Note:** Unlike previous versions of Exchange Server, Exchange 2007 and Exchange 2010 do not allow creation of a user mailbox for suspended accounts. All other types of mailboxes will have their associated user disabled.  Such accounts will not have their suspension state propagated from the Global User.

The ADS connector uses the following remote agents for all Exchange related operations:

- Remote agent that is used to manage Exchange 2000 and 2003
- Remote agent that is used to manage Exchange 2007 and Exchange 2010. These versions of Exchange are only supported on 64-bit operating systems.

For more information about installing and configuring the ADS Connector, see the *Active Directory Services section of this guide.*

## Exchange 20xx Log Files

Log files generated for "Move Mailbox" and "Manage Mailbox Rights" can be found in the following directory:

*PS_HOME*\Logs\ADS

## Exchange 2007 and Exchange 2010 Support

The CA IdentityMinder Exchange 2007 or 2010 Connector supports standard user mailboxes in addition to the following resource types:

- Linked Mailbox for a user account in a trusted forest or domain
- Shared Mailbox
- Equipment Mailbox
- Room Mailbox

To enable these mailboxes, select the Exchange General tab from an ADS Account Template property sheet and use the Mailbox Type button to create the mailboxes. After creation, these mailboxes can be managed directly or by using the Account Template, however, the mailbox type can no longer be changed. By default, the corresponding account to Linked, Shared, Equipment, and Room mailboxes is disabled.

The requirements for managing Microsoft Exchange 2007 and Microsoft Exchange 2010 mailboxes are as follows:

- Install the Exchange 2007 or 2010 remote agent on each managed Exchange 2007 or 2010 Server that hosts the Exchange *Mailbox* role.
- To install shared components from the Exchange 2007 or 2010 remote agent silent install, set the following SharedComponent install location in the command line:

  `SHAREDCOMPONENTS=\"<Path>\"`

  Where *Path* specifies the SharedComponent install location. The following command line is an example where the SharedComponents install path is set to 'E' drive.

  ```
  SHAREDCOMPONENTS=\"E:\\Program Files\\CA\\SC\\\"
  ```

- Install the Exchange 2007 or 2010 Management Console on the Exchange 2007 or 2010 Servers respectively.
- Configure the Exchange Gateway Server in the ADS endpoint properties.
- When installing the Exchange 2007 or Exchange 2010 Remote Agent, perform post installation steps to grant the remote agent enough rights to perform the required operations. Update the CA Messaging Queuing Server to start with an account granted enough rights on the Exchange Server and the ADS Domain for all mailbox operations on the Exchange 2007 or Exchange 2010 Server.

  **Note:** The Exchange 2007 Remote Agent does not return inherited mailbox rights.

  **Note:** Exchange Server 2007 and Exchange Server 2010 do not allow creation of a user mailbox for suspended accounts. All other types of mailbox have their associated user disabled. Such accounts do not have their suspension state propagated from the Global User.

## Linked Mailboxes

When creating a Linked Mailbox using the Account Template, the following information is required:

- Linked Domain Controller
- Linked Master Account name
- Linked Domain Administrator
- Linked Administrator Password

To add an account in another domain or trusted forest to the Send-As or Mailbox Rights permission lists in the Provisioning Manager, hold down the SHIFT key and click ADD while viewing either the "Permissions" page or the "Manage AD permissions" page. This lets the user be added directory, for example, "trustedDomain\account".

**Note:** You cannot add an account in another domain or trusted forest to the Send-As or Mailbox Rights permission lists in the CA IdentityMinder User Console.

## Configuring the Exchange Remote Agent

In an Exchange 2000/2003 environment, the Exchange 2000/2003 remote agent is required to manage mailbox permissions and to perform the operation of moving mailboxes between mailbox stores.

For Exchange 2007 and Exchange 2010 environments, refer to Exchange 2007/ 2010 Support (see page 309) for more information.

The remote agent uses APIs that have to be launched on the Microsoft Exchange computer.

The Exchange Remote Agent should be installed and the CAM and CAFT Service should be configured on Exchange servers that you plan to use as a gateway server to manage the Exchange site.

In the Provisioning Server, for each managed ADS/Exchange endpoint, you must define the Exchange gateway server that should be used. This can be done from the Exchange General tab of the managed endpoint property page.

**For Windows 2003 with Exchange 2000/2003 Machines:**

When installing the Exchange Remote Agent, you need to perform post installation steps to grant the remote agent enough rights to perform the required operations. The CA Message Queuing Server service needs to be updated to be started with an account granted enough rights on both the Exchange Server and the ADS Domain (for move mailbox operations and management of mailbox rights).

If the Remote Agent is installed on a Windows 2000/2003 server, the ‘Local System’ account used by the CA Message Queuing Server service, by default, may have insufficient rights to run commands. Therefore, the account starting this service needs to have the following rights (found under Local Security Policy\Local Policies\User Rights Assignment):

- Act as part of the operating system
- Log on as a batch job
- Log on as a service

## Step 1. Configure the CAM and CAFT Service

You must configure CAFTHOST to recognize the C++ Connector Server and the CA IdentityMinder clients.

1. Issue the following command on the computer where the remote agent is installed:

   ```
   $ CAFTHOST -a Windows_node_name
   ```

   where *Windows_node_name* is the name of the C++ Connector Server host.

   **Note:** If the C++ connector Server is networked using DHCP or you do not use DNS for name resolution, the network name will not be recognized. Under these conditions, use the TCP/IP address for the Windows node name or add a Windows node entry in the local hosts file on your Microsoft Exchange server.

2. Verify this command by issuing:

   ```
   $ CAFTHOST -l
   ```

The previously mentioned steps can also be performed by using the Host to Caft Definition Provisioning Manager that can be selected from the following location:

```
Start/Program Files/CA/CA IdentityMinder/Host to Caft Definition
```

For more information about viewing, starting, or stopping the CAM and CAFT Service, see Managing the CAM and CAFT Service in this section.

## Step 2. Update the CAM and CAFT Service Logon Account

By default, the CAM and CAFT Service is started by the system account when you install the Remote Agent. CA IdentityMinder needs this service to be started by an account that has exchange administrative rights in the domain; therefore, you must change the account that starts this service.

## Windows 2000/2003

To change the account on a Windows computer, do the following:

1. Open the Services console. You can do this by running *services.msc*.
2. Open the CA Message Queuing Server service.
3. Modify this service so that it is run by the service account.
4. Double-click the CA Message Queuing Server service.
5. Click the Log On tab.
6. Select This Account and enter the name and password of an account with administrative rights to the domain.
7. Click OK.
8. Stop the CA Message Queuing Server service with the following command:

   ```
   camclose
   ```

9. Start the service with the following command:

   ```
   cam start
   ```

## Exchange 2007

We recommended that the specified directory Exchange Gateway Server be a domain controller. If the specified Exchange Gateway Server is not a domain controller, you must create a service account for the Remote Agent and delegate it the appropriate rights to manage the Exchange environment. To do this, do one of the following:

- Leave the 'CA Message Queuing Server' so that it is being run by the Local System account if the machine is also a domain controller.
- Use the Exchange Management Console to delegate the service account the required rights.

The following are the Exchange 2007 required rights:

| Required Tasks | Administrator Group |
|---|---|
| Mailbox Move, Mailbox Rights (Full Access Permissions) | Exchange Organization Administrator |
| All other Exchange Tasks (Not required if a member of Exchange Organization Administrator | Exchange Recipient Administrator |

- On each machine with the Exchange 2007 Remote Agent installed, add the service account to the Local Administrators group and also the domain builtin\Administrators group.
- If the Exchange Gateway Server specified is a mailbox server within a CCR on Windows Server 2008, the server must have full access permissions to manage the Cluster running the CCR (not applicable to Windows Server 2003).

When the service account has been granted the appropriate permissions above, use the windows services console (services.msc) and modify the settings for the CA Message Queuing Server so that it is run by the service account. Once complete, restart the service by running, the following command from a command prompt

```
'camclose'
```

To start the service again, run this command:

```
'cam start'
```

## Manage an Exchange 2010 Environment

To manage the Exchange 2010 environment, create a service account for the Remote Agent and delegate the appropriate rights to the Remote Agent.

**Note:** Use Active Directory Users and Computers to delegate a service account the required rights.

The following are the Exchange 2010 recommended roles:

| Required Tasks | Suggested Role Group |
|---|---|
| Mailbox Move, Mailbox Rights (Full Access Permissions) | Exchange Organization Administrators |
| All other Exchange Tasks (Not required if a member of Exchange Organization Administrator) | Exchange Recipient Administrators |

When the service account has been granted the appropriate permissions as described in the table above, use the windows services console (services.msc) and modify the settings for the CA Message Queuing Server so that it is run by the service account.

When complete, restart the service enter the following command from a Windows Command Prompt to restart the service.

'camclose'

To start the service again, enter the following command:

'cam start'

## Mixed Exchange 2007 or Exchange 2010 Environments with Exchange 2003 not Supported

Managing both Exchange 2003 and Exchange 2007 or Exchange 2010 in a mixed Exchange 2003/2007/2010 environment is not supported with this release. If you have updated your Microsoft Active Directory schema by running the Exchange 2007/2010 Setup tool in either your domain or forest, the im_ccs automatically identifies all Exchange servers in the domain as Exchange 2007/2010. If you want to continue managing Exchange 2003 servers only, you must first disable the Exchange 2007/2010 functionality using a registry key on the machine(s) running the im_ccs services.

If you do not apply this change, the Connector Server is unable to correctly manage the Exchange 2003 functionality in a mixed Exchange 2003/2007/2010 environment.

To disable Exchange 2007 or Exchange 2010, perform the following steps:

1. Open the following registry key using regedit:

   ```
   HKLM\SOFTWARE\ComputerAssociates\Identity Manager\Provisioning Server
   ```

2. Add this new string value under the registry key:

   ```
   DisableExchange2007
   ```

3. Set DisableExchange2007 value to 1 or 2. The values are as follows:

   1 disables most Exchange 2007 functionality and treats all Exchange servers as 2000/2003.

   2 allows both Exchange 2003 and Exchange 2007/2010 with reduced functionality

4. Restart im_ccs service.

   **Note:** The ADS log will include a message about the status of the DisableExchange2007 setting.

The Provisioning Manager cannot create an Exchange 2000/2003 mailbox using an Exchange 2007/2010 specified Account Template.

When you have completed the above procedure and set the registry key value to 1, the following are disabled for Exchange 2007 and Exchange 2010.

- Mailbox creation
- Mailbox deletion
- Mailbox movement
- Mailbox Send-As permission management
- Mailbox Full Access permission management

If you have completed the above procedure and set the registry key value to 2, the following applies to managed Exchange 2000/2003 directories:

- Mailbox rights cannot be managed.

- Send-As permissions cannot be managed.
- When creating or modifying an Exchange 2000/2003 account template, clicking the 'Mailbox Types' button enables the Exchange 2007/2010 functionality. Mailboxes are not created on Exchange 2000/2003-based systems and no error message are returned. Do not click on the 'Mailbox Types' button if you want to create or manage Exchange 2000/2003 Mailboxes using that account template.

  If you do not apply this change the im_ccs service is unable to correctly manage the Exchange 2003 functionality.

Notes on setting the registry value to 2:

1. By default, Mailboxes are created as "Legacy Mailboxes". For example, right clicking on an account and selecting 'custom > create mailbox' creates a Legacy Mailbox.
2. If you want to create Exchange 2007/2010 Mailboxes, set the mailbox type on the appropriate account template. If you do not set the mailbox type, mailboxes created by the account template are of type 'Legacy Mailbox'.

## Enable Exchange 2007/2010 Mixed Environment Support

CA IdentityMinder r12.6.1 supports Exchange 2007/2010 in mixed environments.

To enable support for Exchange 2007/2010 mixed environments, select the Exchange 2010 Server with the Mailbox role that is configured as the Exchange Gateway server on the Active Directory Exchange General directory properties page.

**Note:** The Exchange 2007/2010 remote agent must be installed on the Exchange Gateway server and any Exchange 2007 servers you want to create mailboxes on.

## Configure Exchange 2007 and Exchange 2010 Timeout Settings

If your managed Exchange Gateway server is not a domain controller, configure the following:

- Maximum timeout period the Remote Agent continues to try to read new Active Directory accounts
- Maximum timeout period the Connector Server waits to confirm mailbox existence.

**To configure Exchange 2007 and Exchange 2010 timeout settings**

1. On Remote Agent installations, set the value on the following Windows registry keys
   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\Identity
   Manager\Ex2k7AgentTimeout
   ```
   **DWORD value**

   > Defines the maximum timeout period the Remote Agent continues to try to read new Active Directory accounts during replication. The value required for inter-site replication depends on the replication topology settings.
   >
   > **Default:** 60

2. On computers running the CA IdentityMinder Connector Server (C++) service, set the following Windows system environment variable:

   **ADS_CONFIRM_MAILBOX**

   > Specifies the maximum timeout period the Connector Server waits to confirm mailbox existence. The value required for inter-site replication will depend on replication topology settings.
   >
   > **Default:** 35

## Configure Exchange 2007/2010 Preferred Domain Controller Settings

In some managed Exchange 2007 and 2010 environments, the preferred Domain Controller used by Exchange servers is different from the Domain Controller used by the Active Directory connector. As a result, the Active Directory replication latency can introduce mailbox creation failure. To prevent mailbox creation failure, configure the Exchange Server so that it communicates directly with the Active Directory connector-preferred Domain Controller.

To resolve the issue, set the ADS_E2K_SEND_DC system environment variable on the IM_CCS computer to 1.

**Note:** By default the value of the ADS_E2K_SEND_DC system environment variable value is 0.

## Activating CAM and CAFT Encryption

To install the encryption key, follow these steps:

1. Enter the following command at the command prompt to generate your key file:

   ```
   #PATH=`cat/etc/catngcampath`/bin:$PATH

       #export PATH
       #caftkey -g keyfile password
   ```

   where:

   *keyfile* is the name you assign to the key file.

   *password* is the password you assign to the key file.

   **Note:** The caftkey command and attributes are the same for Win32 platforms.

2. Install your Public Key on both CAFT Agent and CAFT Admin computers using the previously-generated key file by entering the following command at the command prompt:

   ```
   #PATH=`cat/etc/catngcampath`/bin:$PATH
       #export PATH
       #caftkey -policy_setting keyfile password
   ```

   - *keyfile* and *password* must be the same values you specified in Step 1.-*policy_setting* is -i, -m, or blank.
   - The policy_setting governs the communication between this computer (the local computer) and other computers that have the CAM and CAFT Service installed, but may or may not have the CAM and CAFT encryption certificates installed.

**Policy -1 (caftkey -i keyfile password)**

The -i option specifies Policy -1. This policy lets computers running previous versions of the CAM and CAFT Service execute commands on this computer and lets this computer execute commands on those computers. Policy -1 encrypts messages if the other computer has these certificates installed. This policy does not encrypt messages if the other computer does not have these certificates installed.

**Policy 1 (caftkey -m keyfile password)**

The -m option specifies Policy 1. This policy prohibits other computers from executing commands on this computer if they are running previous versions of the CAM and CAFT Service without the encryption certificates. This policy also prohibits this computer from executing commands on those computers.

If both computers have the CAM and CAFT encryption certificates installed, but have different Public Key Files installed when Policy 1 is set, the command requests between the two computers always fail.

**The Blank Option**

The blank option specifies Policy 0. This policy is set if no Public Key File is installed, the CAM and CAFT encryption certificates were not installed properly, or if you do not specify a policy setting when you enter the caftkey command. Policy 0 specifies no encryption.

**Note:** The CAM and CAFT Service must already be installed on the computer in your network. For example, to install the encryption key on Linux computers, run the following commands:

```
#tar xvf LINUX_V1.07_20020319_Build230.tar
#cd ./cam/scripts
#./install
```

3. Recycle the CAM Service on each computer where you install the new Key as follows:

```
prompt> camclose              //stop Cam/Caft service and processes

prompt> cam start             //start CAM service and process
```

**Check the Policy setting:**

To see what mode the computer is operating in, look in the following file:

```
%CAI_MSQ%\ftlogs\dg000
```

## Managing the CAM and CAFT Service for Microsoft Exchange 20xx

**Note:** The CAM and CAFT Service allows encryption using certificates.

The CAM and CAFT Service is a daemon process. You can control this process using the Services dialog on your Control Panel. To view the Services dialog, click the Services icon. The CAM and CAFT Service is called CA Message Queuing Server.

### View the CAM/CAFT Process

To view this process, perform the following steps:

1. Open the Windows Task Manager.
2. Click the Processes tab on the Windows Task Manager.

   The CAM and CAFT daemon processes appear. The following is a sample of these processes:

   ```
   Image name         PID    CPU        CPU Time           Mem Usage
   Caftf.exe         1364     00         0:00:16             1 600 K
   Cam.exe            516     00         0:00:08               704 K
   ```

### Start the CAM/CAFT Service

Although the CAM and CAFT Service starts automatically, there may be times when you have to manually start it.

To start the CAM and CAFT Service, do the following:

1. Double-click the Services icon on the Control Panel.

   The Services dialog appears.

2. Select CA Message Queuing Server from the Service window and click Start.
3. Click Close.

**Note:** After you stop the CAM and CAFT Service, you must restart it so CA IdentityMinder can communicate with the Microsoft Exchange Remote Agent.

### Stop the CAM/CAFT Service

To stop the CAM and CAFT Service,open a Command Prompt window, then enter the following command:

```
camclose
```

**Note:** After stopping the CAM and CAFT Service, you must restart it so that CA IdentityMinder can communicate with the Microsoft Exchange Remote Agent.

# E2K Support for FIPS and IPv6

For this release of CA IdentityMinder, the Exchange 20xx Connector does not support FIPs or IPv6.

# Managing Exchange Users

CA IdentityMinder manages mailboxes on ADS endpoints. Information about these mailboxes is stored in the ADS endpoint associated with the Microsoft Exchange server. For this reason, you must acquire the ADS endpoint, when you want to manage your Microsoft Exchange users.

When you acquire an ADS endpoint, the Endpoint Content dialog displays the following containers:

- **Builtin** contains all security groups that are built into ADS, such as Administrators and Backup Operators
- **Computers** contains computers that belong to the ADS directory
- **Microsoft Exchange System Objects** contains Microsoft Exchange system mailboxes
- **Users** contains all ADS accounts and groups, including those with mailboxes

Other organizational containers may appear in this dialog. These containers reflect the structure that exists within the ADS directory. For example, an ADS directory may contain a Human Resource container for all Human Resource users and groups.

## Authentication Process

Exchange management for the ADS Endpoint is now enabled or disabled when you supply a new Userid/Password during authentication. If the new Userid/Password is incorrect, management is disabled, and conversely for the other.

## E2KSAUtil.Exe Option

An option has been added to the E2KSAUtil.exe file to add additional time for the Recipient Update Service (RUS) to be updated before processing other tasks. The optional environment variable eTrustIM_RUS_Delay_Seconds can be set to compensate for delays in time that Exchange takes to update the RUS information. If used, the environment variable should be set to an integer indicating the number of seconds to pause after triggering the RUS update, before processing continues. The delay allows additional time so that Exchange data is fully updated before continuing. For example,

```
Set eTrustIM_RUS_Delay_Seconds=3
```

If not set, the variable defaults to 1 second. You can also set the variable to 0 to disable. The code automatically pauses up to five times, each for the specified seconds. After each delay, CA IdentityMinder attempts to read the necessary data. If it fails, CA IdentityMinder pauses and tries again until the data is properly updated or five attempts to read the data have failed.

**Note:** Only the number of seconds to pause is configurable. If the data is read properly after the first pause, no additional delay occurs. If the 5th try fails, E2KSAUtil returns control to CA IdentityMinder with an error code.

E2KSAUtil.exe reads the environment variable each time that it is called. Any change to the environment variable value is used the next time E2KSAUtil runs. No reboot is necessary.

## ADS Account Templates

The ADSContactAccountTemplate, provided with the Active Directory Services Connector, provides a user with the minimum-security level needed to access an ADS endpoint. You can use it as a model to create new account templates with Exchange specific options.

When working with ADS Contact account templates, the Exchange General tab defines the Microsoft Exchange attributes that you can set, for example:

- Any delivery restrictions, such as the messages that are accepted by the mailbox and their maximum size
- Any delivery options, such as any forwarding addresses or permissions that the user has when sending messages on other user's behalf
- All storage limits, such as the size limit and the length of time that a user can keep deleted items
- The Exchange 2007 specified Mailbox Type (if applicable)

This tab contains all the attributes that are necessary for you to create a Microsoft Exchange 20xx mailbox.

## Specifying Datastore Names in an ADS Account Template

**Important:** The following is an alternate way to specify the Datastore Name. You can also specify the datastore name using the Home Server and Mailbox Datastore fields on the Provisioning Manager.

**Note:** When you create an ADS account template that uses a rule string for the name of a Microsoft Exchange server, do not specify the datastore location. Datastores are dependent on the server name.

To create a default location for the datastore, follow these steps:

1. Open the default.e2k file located in the following directory:

   ```
   \PS_HOME\data\ads
   ```

   **Note:** This file should be manually created if needed and should contain two columns. The first column contains the Relative Distinguished Name (RDN) of the Microsoft Exchange server. The second column contains the RDN of the datastore that is used as the default.

2. Update this file by entering the RDN of the datastore or a complete DN in the second column. If you enter the RDN, you must specify a unique value. In addition, the second column must be delimited with a double quote.

3. After saving and closing the file, you must restart the C++ Connector Server.

## Microsoft Exchange Distribution Lists and ADS Account Templates Using Strong Synchronization

Microsoft Exchange uses Active Directory Server for its directory. Microsoft Exchange distribution lists are implemented as Active Directory groups. Because the groups are defined in ADS, the members of these groups are subject to ADS account templates. If an ADS account template does not list the Microsoft Exchange distribution list, which is now an Active Directory group, in the Groups (Member Of) tab of the account template and the account template uses strong synchronization, the accounts that are synchronized by this account template will lose their membership in the Microsoft Exchange Distribution list. To prevent this loss of membership, the ADS group representing the Microsoft Exchange distribution list needs to be added to the account template.

For some installations, adding the distribution lists to the ADS account template is not desired. From the Exchange General tab of the Active Directory endpoint property sheet, you can select the Active Directory container used to store the Microsoft Exchange Distribution lists.  During account template synchronization, the synchronization mechanism will not remove the account from a group that exists in the specified container or any container owned by the specified container. This lets you use current ADS strong synchronization account templates with having accounts lose membership in ADS groups used for Microsoft Exchange Distribution lists.

## Exchange Accounts

Accounts give users access to the resources on an endpoint. CA IdentityMinder lets you manage Microsoft Exchange mailboxes from the Endpoint Type task view.

- Use the Active Directory Services Account property sheet when managing mailboxes
- Use the New User property sheet when creating a new ADS account that will have a mailbox
- Use the Custom menu to create or delete mailboxes that are associated with ADS accounts
- Use the Active Directory Services Account property sheet when deleting a mailbox of an Active Directory Services account without deleting the account

There are the following three Account-specific tabs for Exchange on the ADS Account Property Sheet:

**Email Addresses Tab**

Contains email addresses for the corresponding mailbox.

**Exchange General Tab**

Contains Exchange attributes such as Server, Alias name, or the limits for a mailbox.

**Exchange Advanced Tab**

Contains all of the advanced Exchange properties such as custom attributes, protocol settings, ILS settings, mailbox rights, and Exchange 2007-specific mailbox AD rights, when applicable.

## Setting Live Communication Server 2003 Attributes for ADS

You can set Live Communication Server 2003 attributes for ADS accounts and ADS account policies. There is no Provisioning Manager support for setting or viewing these attributes. However, they can be set through the eTA Batch Utility (etautil) or through an LDAP browser (for example, JXplorer).

The following attributes need to be set to enable live communications:

- eTADSmsRTCSIP-IsMaster. For example, TRUE.
- eTADSmsRTCSIP-PrimaryHomeServer. For example:

  ```
  CN=RTC Services,CN=Microsoft,CN=<YourDC>,OU=Domain
  Controllers,DC=<YourDOMAIN>,DC=com
  ```

- eTADSmsRTCSIP-PrimaryUserAddress. For example:

  ```
  sip:<account>@DOMAIN.com.
  ```

- eTADSmsRTCSIP-UserEnabled. For example, TRUE.

The attributes of an account that has Live Communications enabled can be viewed as an example.

**Note:** It is possible to use rule strings for the attributes in the ADS account account template. For example, eTADSmsRTCSIP-PrimaryUserAddress can be set as sip:%AC%@DOMAIN.com.

## How you Manage the Office Communications Server (OSC 2007)

To manage the Office Communications Server 2007, do the following:

1. Extend the Active Directory schema for CA IdentityMinder.
2. Determine the correct ADS common attribute values. (see page 328)

## Extend the Active Directory Schema for CA IdentityMinder

To manage Office Communications Server 2007, extend the Active Directory schema for CA IdentityMinder.

**To extend the Active Directory schema for CA IdentityMinder**

1. Add the following attributes to the *Provisioning_Server_HOME\data\ADS\schema.ext* file:

   **msRTCSIP-ArchivingEnabled**

   Specifies whether archiving is enabled. This attribute is an integer mask. You can leave this attribute blank.

   Valid values are:

   - **0** - Use the global default values defined by msRTCSIP-ArchiveDefault and msRTCSIP-ArchiveFederation.
   - **1** - Archive all communications.
   - **2** - Do not archive.

   **Note:** For more information about the attributes values, see http://technet.microsoft.com/en-us/library/bb663647(office.12).aspx. http://technet.microsoft.com/en-us/library/bb663647(office.12).aspx

   **msRTCSIP-OptionFlags**

   Specifies the different options enabled for the user or contact object. This attribute is a bit-mask value of type *integer*.

   **Default:** This attribute has a value 256 when enabling users natively (enhanced presence).

   As the value for this attribute is a bit-mask, add the required values together. For example, to enable enhanced presence (256) and remote call control (16), enter a value of 272 (256+16) as the value for this attribute.

   **Note:** For more information about this attribute, see the Attribute Descriptions page in the Office Communications Server 2007 Active Directory Guide.

   **msRTCSIP-PrimaryHomeServer**

   Defines the DN of the OCS server where the account is located. For example:

   ```
   CN=LC Services,CN=Microsoft,CN=<Servername>,CN=Pools,CN=RTC
   Service,CN=Microsoft,CN=System,DC=<domain>,DC=<com>
   ```

   **msRTCSIP-PrimaryUserAddress**

   Defines a user address in the form: sip:username@domain.com

   **msRTCSIP-UserEnabled**

   If TRUE, specifies that OCS features are enabled. If you omit or set this value to FALSE, the OCS is disabled.

**proxyAddresses**

Defines the sip proxy address in the form: sip:username@domain.com

**Note:** This attribute is a multivalued field also used by Exchange. We recommend that you add rather than replace any existing values.

2. Restart the CA IdentityMinder – Connector Server (C++) service.
3. Next, determine the correct ADS common attribute values (see page 328).

**Note:** For more information about extending the schema, see the sections *Extend the ADS Schema* and *Modify the schema.ext File* in the *CA IdentityMinder Connectors Guide*. For a full list of OCS attributes including their possible values, see the following Microsoft Technet OCS reference page:

http://technet.microsoft.com/en-us/library/bb663647.aspx.

## Determine Correct ADS Common Attribute Values

Attributes managed by extending the ADS schema do not have error-checking enforced. We recommend that you enable an account for OCS2007 using native tools so that you can determine the correct common ADS values (such as PrimaryHomeServer). Determining the correct common values minimizes the risk of entering incorrect values, particularly for long strings such as DNs.

**To determine ADS correct attribute values**

1. Create or modify a native template user using either Office Communications Server 2007 (R2) snap-in for MMC, or ADUC (Active Directory Users and Computers).
2. View the user using the Provisioning Manager with the extended schema enabled.

   **Note:** If you created a new user, it may be necessary to explore the endpoint or container.
3. Copy or note the values for the extended attributes.
4. Add the attribute values to the appropriate Active Directory User Template or Account.
5. Repeat steps 1 through 4 for any alternate settings required for templates, such as different activation levels.

## Cannot Set Enhanced Presence or Archive Options with User Console

**Symptom:**

I cannot use the CA IdentityMinder User Console to set Enhanced Presence or Archive options for Office Communications Server 2007 R2.

**Solution:**

The User Console does not contain options that let you set up Enhanced Presence.

Office Communications Server (OCS) relies on Enhanced Presence. If Enhanced Presence is not set up, when a user tries to use OCS (for example, by logging in to Office Communicator), they receive a message similar to the following:

```
You will not be able to sign in because your account is not configured to support
enhanced presence features.
Please contact your system administrator.
```

However, you can set up Enhanced Presence and archiving using Provisioning Manager, on the Custom tab.

## Custom Menu on Accounts and Contacts

The following Exchange operations are available from the Custom Menu:

- Create Mailbox (accounts)
- Enable e-mail addresses (contacts)
- Move Mailbox (accounts)
- Delete Mailbox (accounts)
- Disable e-mail addresses (contacts)
- Remove Exchange Attributes

**Note:** The User Console can be used to create a mailbox for an existing ADS account by assigning the account template that enables the mailbox feature to the account. Alternatively, you can create a mailbox for an existing ADS account by right-clicking on an account in the Provisioning Manager and selecting "Create Mailbox" from the Custom menu.

All other custom exchange operations (“Mailbox Move”, “Delete Mailbox” and “Remove Exchange Attributes”) can only be performed by selecting them from the Custom menu the Provisioning Manager.

## Custom Menu on Group

The following Exchange operations are available from the Custom Menu:

- Enable e-mail address
- Disable e-mail address

### Creating E-mail Addresses for Groups

E-mail addresses for groups can be created:

- During the creation of a group using the Content menu
- On an existing group using the Custom Menu

### Distribution Lists

An ADS security group that has an active email address is called a *distribution list*. CA IdentityMinder lets you create and maintain distribution lists using the Endpoint Type task view. Use the Active Directory Services Group property sheet when managing these lists.

### E2K Etautil Conventions

Use the following ADS conventions in your etautil commands:

- The endpoint type name (eTNamespaceName) is ActiveDirectory
- The endpoint type prefix is ADS. Therefore, the Active Directory Services class names are:
  - eTADSDirectory for an endpoint
  - eTADSPolicyContainerName for an account template container
  - eTADSPolicy for an account template
- The Description line for all Microsoft Exchange attributes contain the phrase (Exchange2000 only)

# Microsoft SQL Server Connector

The MS SQL Server Connector provides a single point for all user administration by letting you perform the following:

- Manage logins on MS SQL server platforms
- Register endpoints, explore them for objects to manage, and correlate their logins with global users
- Create and manage MS SQL server logins using MS SQL server-specific account templates
- Change login passwords and activations in one place
- Synchronize users with their provisioning roles or synchronize users' logins with their account templates
- Assign a MS SQL server account template to each of your MS SQL server endpoints

- Use the SQL Default Policy to create logins with the minimum level of security needed to access an MS SQL server endpoint
- Generate and print reports about MS SQL server logins and hosts

This connector supports IPv6, but not FIPS.

**Note:** Before you use the connector, you can set up Windows authentication. This is optional.

## MS SQL Configuration

The MS SQL connector must be managed with the CA IAM CS installation process. For more information on this installation process, click here.

To administer MS SQL server machines with CA IdentityMinder, the MS SQL server connector must be installed on each Provisioning server.

The following sections detail the configurations that are needed in order for the MS SQL connector to work correctly.

### Configure the JDBC URL

Communication between the Provisioning server and the MS SQL server relies on a JDBC connection. A URL specifies connection details to each server, as illustrated in the following examples:

**Basic URL**

```
jdbc:sqlserver://serverHost
```

**Integrated Security URL**

```
jdbc:sqlserver://serverHost;integratedSecurity=true
```

**Named instance on port 1433 URL**

```
jdbc:sqlserver://serverHost:1433;instanceName=instance1
```

**Connecting with IPv6**

```
jdbc:sqlserver://;serverName=<IPv6 address here>

jdbc:sqlserver://;serverName=<IPv6 address>;port=CA Portal;databaseName=<DB>
```

**Note:** For more details see Building the Connection URL on MSDN.

## Configure the Windows Service

If you want to use Windows NT authentication, you must ensure that the system account running the im_jcs service also exists as an account on the server running MS SQL and has administrative rights. The im_jcs service by default runs as the LocalSystem account. You will need to change this to an account on the same domain or system as the MS SQL servers you wish to manage using the ‘Services’ dialog in the ‘Control Panel’.

**Note:** Windows NT trusted authentication is only supported on Windows platforms.

## MS SQL Migration Steps

To migrate from the C++ MS SQL connector to the Java MS SQL connector, you must do the following:

- Install the MS SQL Java connector using the CA IAM CS installation
- You can remove your DSN if it is not being used for another other purpose
- Add the URL as defined in Configure the JDBC URL (see page 331) to each existing MS SQL endpoint.  To do this, right click on each endpoint and select “Custom… -> Change Admin Password” and supply the URL in the JDBC URL field.

Once this has been done, all types of operations can be executed against the existing MS SQL endpoints seamlessly.

## Acquire an MS SQL Server Using the User Console

You must acquire the MS SQL server before you can administer it with CA IdentityMinder.

**To acquire an MS SQL server using the User Console**

1. Select Endpoints, Manage Endpoints,Create Endpoint
2. Select MS SQL Server from the drop-down list box on Create a new endpoint of Endpoint Type, and click Ok

   Use the Create MS SQL Endpoint page to register an MS SQL server. During the registration process, CA IdentityMinder identifies the MS SQL server you want to administer and gathers information about it.
3. After entering the required information, click Submit.

   You are now ready to explore and Correlate the endpoint.

4. Click Endpoints, Explore and Correlate Definitions, Create Explore and Correlate Definition to explore the objects that exist on the endpoint.

   The Exploration process finds all MS SQL accounts and groups. You can correlate the accounts with global users at this time or you can correlate them later.

5. Click OK to start a new definition.

6. Complete the Explore and Correlate Tab as follows:

   a. Fill in Explore and Correlate name with any meaningful name.

      Click Select Container/Endpoint/Explore Method to click an MS SQL endpoint to explore.

   b. Click the Explore/Correlate Actions to perform:

      - **Explore directory for managed objects**—Finds objects that are stored on the endpoint and not in the provisioning directory.

      - **Correlate accounts to users**—Correlates the objects that were found in the explore function with users in the provisioning directory. If the user is found, the object is correlated with the user. However, you can instead select that you want to assign the account to the existing user (the default user) or create the user.

      - **Update user fields**—If a mapping exists between the object fields and the user fields, the user fields are updated with data from the objects fields.

7. Complete the Recurrence tab if you want to schedule when the task to executes.

   a. Click Schedule.

   b. Complete the fields to determine when this task should execute.

      You may prefer to schedule the task to execute overnight to interfere less with routine access of the system.

   **Note**: This operation requires the client browser to be in the same time zone as the server. For example, if the client time is 10:00 PM on Tuesday when the server time is 7:00 AM, the Explore and Correlate definition will not work.

8. Click Submit.

**To use an explore and correlate definition**

1. In a CA IdentityMinder environment, click Endpoints, Execute Explore and Correlate.

2. Click an explore and correlate definition to execute.

3. Click Submit.

   The user accounts that exist on the endpoint are created or updated in CA IdentityMinder based on the explore and correlate definition you created.

## MSSQL Endpoint with Trusted Connection Fails

The sqljdbc_auth.dll is not available out of the box with CA IdentityMinder. You must download the file from the Microsoft website.

**Note:** For more details see Building the Connection URL on MSDN.

## SQL Password Changes

When trying to make SQL account password changes using the User Console, you must set the "Enforce synchronized account passwords" configuration parameter to No. You can access this parameter from the System, Domain Configuration, Password section of the Provisioning Manager.

## Unlock an Account

You can use the CA IdentityMinder User Console to unlock an account on a Microsoft SQL Server endpoint.

An account is locked after too many attempts to log in with an incorrect password.

**Follow these steps:**

1. Log in to the User Console as an administrator.
2. Click Users, Modify User's Endpoint Accounts, then search for the user.
3. Click the Account tab, then find the Status section.

   If the Account is Locked box is checked, this account is locked.
4. Uncheck the box to unlock the account, then click Submit.

The MS SQL Connector uses Logins in place of accounts. Use the MS SQL Server Login property page to manage MS SQL Logins.

## Database Users

The database users have administrative power in the system.

## Database Roles

You can list the database roles, and include (or exclude) users from the database roles.

## MS SQL Conventions

Use the following MS SQL Server conventions in your etautil commands:

- The endpoint type name (eTNamespaceName) is MS SQL Server
- The endpoint type prefix is SQL. Therefore, the MS SQL Server class names are the following:
  - eTSQLDirectory for an endpoint
  - eTSQLPolicyContainer for an account template container
  - eTSQLPolicy for an account template

# Microsoft Windows Connector

The Windows NT option provides a single point for all user administration by letting you do the following:

- Register endpoints, explore them for objects to manage, and correlate their accounts with global users
- Create and manage Windows NT accounts using Windows NT-specific policies
- Change account passwords and account activations in one place
- Synchronize global users with their roles or synchronize global users' accounts with their policies
- Assign a Windows NT account template to each of your Windows NT endpoints
- Manage Windows NT Trust relationship between your Windows domains
- Use the default Endpoint Type account template to create accounts with the minimum level of security needed to access a Windows NT endpoint
- Create and manage Windows NT user groups
- Create and manage Windows NT shared folders
- Generate and print reports about Windows NT accounts, groups, and hosts

This connector is managed using the Connector and agent installation process. For more information and requirements, click here.

This connector can also be managed using the Connector and C++ Server installation process as well.

## Configuring

If you plan to acquire that Provisioning Server system as an endpoint, you must install the Provisioning Agent for Windows Local Users and Groups.

**Note:** After installing the Provisioning Agent for Windows Local Users and Groups, add the local machine to the Caft host list.

## Upgrading the Provisioning Server

After upgrading the Provisioning Server to r12.6.1, you must install the Provisioning Agent for Windows Local Users and Groups if you want to acquire and manage the Provisioning Server host as an endpoint. After installing the Agent, you may need to re-authorize the Provisioning Server with cafthost by issuing the following command from the SharedComponents\CAM\bin directory:

cafthost -a hostname/IP address

## Installing the Provisioning Agent for Windows Local Users and Groups with setup.exe

In this example, we install the Provisioning Agent for Windows Local Users and Groups by using the setup.exe command. Perform the following steps:

1. Copy the contents of the folder ~\RemoteAgent\Windows200x from the CD to your local machine. For example, C:\temp\RN16.
2. Open a Command Prompt and navigate to the directory where you copied the folder.
3. Issue the following command:

   ```
   setup.exe
   ```

   The graphical installer will launch and the Remote Agent can be installed by following the prompts.
4. (Optional) To perform a silent install, add the qn argument and the licence=Accept line found at the bottom of the EULA. (Read the EULA in graphical mode first):

   ```
   setup.exe /w /S /v"/qn LICENSE=Accept /norestart"
   ```

## Configure the CAM and CAFT Service for Windows NT

The CAM/CAFT service is used to communicate between the C++ Connector Server and the Windows NT targets.

### Install the CAM and CAFT Service for Windows NT

You must install the Provisioning Agent for Windows Local Users and Groups and configure the CAM and CAFT Service on any Windows NT machine that you want to administer.

**Important!** For installing both the Provisioning Agent for Windows Local Users and Groups **and** the CA IdentityMinder Microsoft Exchange Agent on the same machine, use the CAM and CAFT configuration steps for the Microsoft Exchange Agent in the Groupware Connectors section. Be sure to update the CAM and CAFT service logon account, as described in that section.

## How to Configure the CAM and CAFT Service for Windows NT

There are two ways to configure the CAM and CAFT service.

**To configure the CAM and CAFT Service using the command prompt**

1. Log on to your Windows NT machine as the domain administrator or log on to your Windows NT Workgroup machines as the local administrator.
2. Issue the following command from a command window:

   ```
   CAFTHOST -a NT_node_name
   ```

   **NT_node_name**

   Name of the C++ Connector Server if used.

   **Note:** If the Provisioning Server is networked using DHCP or you do not use DNS for name resolution, the network name will not be recognized. Under these conditions, use the TCP/IP address for the Windows NT node name or add a Windows NT node entry in the local hosts file on your Windows NT machine.
3. Verify the previous command by issuing the following command:

   ```
   CAFTHOST -l
   ```

   **Note:** Firewalls may need to be configured to allow communications using the CAM/CAFT service.

**To configure the CAM and CAFT Service using the Host to Caft Definition dialog**

1. Log on to your Windows NT machine as the domain administrator or log on to your Windows NT Workgroup machines as the local administrator.
2. Run Host to Caft Definition located in the default CA IdentityMinder Start program group.

   Start > Programs > CA > Identity Manager > Host to Caft Definition
3. In the Enter a server name field, enter the name of the C++ Connector Server if used. Click Add.

   **Note:** The same conditions regarding DHCP and DNS listed in the previous section also applies here.
4. Verify that the server name added is listed in the Permitted managing servers list. Click OK.

Note: Firewalls may also need to be configured to allow communications using the CAM/CAFT service.

## Activate the CAM and CAFT Encryption for Windows NT

If your CA IdentityMinder installation is using the CAM/CAFT encryption, ask your CA IdentityMinder administrator for a copy of the Public Key keyfile and password in use.

If this is an initial installation of Provisioning Server, Provisioning Manager or CA IdentityMinder Agent, and you want to activate CAM/CAFT encryption for the communication between the Provisioning Server and other CA IdentityMinder servers or system endpoints, you must generate a Public Key file by entering the following command at the command prompt:

```
>caftkey -g keyfile password
```

**keyfile**

Defines the name that you assign to the key file.

**password**

Defines the password that you assign to the key file.

**To activate the CAM and CAFT encryption**

1. Install your Public Key on both CAFT Agent and CAFT CA IdentityMinder boxes using the previously-generated key file (see above) by entering the following command at the command prompt:

   ```
   >caftkey -policy_setting keyfile password
   ```

   - keyfile and password must have the values that you specified while generating the Public Key file.
   - policy_setting must be -i, -m, or blank.

   The policy_setting governs the communication between this computer (the local computer) and other computers that have the CAM and CAFT service installed, but may or may not have the CAM and CAFT encryption certificates installed.

   - Policy -1 (caftkey -i keyfile password)

   The -i option specifies Policy -1. This policy lets computers running previous versions of the CAM and CAFT service execute commands on this computer and lets this computer execute commands on those computers. Policy -1 encrypts messages if the other computer has these certificates installed. This policy does not encrypt messages if the other computer does not have these certificates installed.

   - Policy 1 (caftkey -m keyfile password)

   The -m option specifies Policy 1. This policy prohibits other computers from executing commands on this computer if they are running previous versions of the CAM and CAFT service without the encryption certificates. This policy also prohibits this computer from executing commands on those computers.

   If both computers have the CAM and CAFT encryption certificates installed, but have different Public Key Files installed when Policy 1 is set, the command requests between the two computers always fails.

- Blank Option

  The blank option specifies Policy 0. This policy is set if no Public Key File is installed, the CAM and CAFT encryption certificates were not installed properly, or if you do not specify a policy setting when you enter the caftkey command. Policy 0 specifies no encryption.

2. Recycle the CAM Service on each box where you install the new Key as follows:

   ```
   prompt> cam close             //stop Cam/Caft service and processes

   prompt> cam start            //start CAM service and process
   ```

3. After recycling the CAM service, recycle the CAFT service by issuing the following statement:

   ```
   prompt> caft
   ```

4. Check the log produced by the CAFT service, and confirm the policy setting  by issuing the following statement:

   ```
   prompt> type "%CAI_MSQ%\ftlogs\dg000"
   ```

   The output will be similar to the following example:

   ```
   D:\> type "%CAI_MSQ%\ftlogs\dg000"

       Thu Feb 16 09:05 Starting CAFT version 1.12 (Build 28)

       Thu Feb 16 09:05 Encryption Policy -1

       Thu Feb 16 09:05 ------- CAFT initialize complete -------
   ```

## Check the Policy Setting

To see what mode the machine is operating in, look in the following file:

```
%CAI_MSQ%/ftlogs/dg000
```

The log is as it was lastly generated by the CAFT command. After you change the configuration, you must initiate a new CAFT command so that the log will reflect the latest configuration. You can do this by issuing the following command:

```
Prompt> caft
```

## Manage the CAM and CAFT Service for Windows NT

**Note:** The CAM and CAFT Service allows encryption through certificates.

The CAM and CAFT Service is a daemon process. You can control this process using the Services panel on your Control Panel. To view the Services panel, click the Services icon. The CAM and CAFT Service is called CA Message Queuing.

## View the CAM and CAFT Service for Windows NT

Perform the following procedure to view the CAM and CAFT service.

**To view the CAM and CAFT service**

1. Open the Windows Task Manager.
2. Click the Processes tab on the Windows Task Manager.

   The CAM and CAFT daemon processes appear. The following is a sample of these processes:

   ```
   Image Name     User Name       CPU     CPU Time      Mem Usage
   Caftf.exe            Administartor     00         0:00:16          1,600 K
   Cam.exe            SYSTEM           00         0:00:08          704 K
   ```

## Start the CAM and CAFT Service for Windows NT

Although the CAM and CAFT Service starts automatically, there may be times when you have to manually start it.

**To start the CAM and CAFT Service**

1. Double-click the Services icon on the Control Panel.

   The Services dialog appears.
2. Select CA Message Queuing Server from the Service window, and click the Start button.
3. Click Close.

## Stop the CAM and CAFT Service for Windows NT

Perform the following procedure to stop the CAM and CAFT service.

**To stop the CAM and CAFT Service**

1. Double-click the Services icon on the Control Panel.

   The Services dialog appears.
2. Select CA Message Queuing Server from the Service window, and click the Stop button.
3. Click Close.

**Note:** After you stop the CAM and CAFT Service, the service must be restarted so CA IdentityMinder can communicate with the Windows NT Remote Agent.

## Windows NT Support for FIPS and IPv6

For this release of CA IdentityMinder, the Windows NT Connector supports both FIPs and IPv6.

## Connector-Specific Features

This section details your connector's specific management features, such as how to acquire and explore your endpoint. Also included are account, provisioning roles, account template, and group information specifically for your connector.

### Acquire a Windows NT Machine Using the User Console

You must acquire the Windows NT machine before you can administer it with CA IdentityMinder.

**To acquire a Windows NT machine using the User Console**

1. Select Endpoints, Manage Endpoints,Create Endpoint
2. Select Windows NT from the drop-down list box on Create a new endpoint of Endpoint Type, and click Ok

   Use the Create Windows NT Endpoint page to register a Windows NT machine. During the registration process, CA IdentityMinder identifies the Windows NT machine you want to administer and gathers information about it.
3. After entering the required information, click Submit.

   You are now ready to explore and Correlate the endpoint.

4. Click Endpoints, Explore and Correlate Definitions, Create Explore and Correlate Definition to explore the objects that exist on the endpoint.

   The Exploration process finds all Windows NT accounts and groups. You can correlate the accounts with global users at this time or you can correlate them later.

5. Click OK to start a new definition.

6. Complete the Explore and Correlate Tab as follows:

   a. Fill in Explore and Correlate name with any meaningful name.

      Click Select Container/Endpoint/Explore Method to click an Windows NT endpoint to explore.

   b. Click the Explore/Correlate Actions to perform:

      - **Explore directory for managed objects**—Finds objects that are stored on the endpoint and not in the provisioning directory.

      - **Correlate accounts to users**—Correlates the objects that were found in the explore function with users in the provisioning directory. If the user is found, the object is correlated with the user. However, you can instead select that you want to assign the account to the existing user (the default user) or create the user.

      - **Update user fields**—If a mapping exists between the object fields and the user fields, the user fields are updated with data from the objects fields.

7. Complete the Recurrence tab if you want to schedule when the task to executes.

   a. Click Schedule.

   b. Complete the fields to determine when this task should execute.

      You may prefer to schedule the task to execute overnight to interfere less with routine access of the system.

   **Note**: This operation requires the client browser to be in the same time zone as the server.  For example, if the client time is 10:00 PM on Tuesday when the server time is 7:00 AM, the Explore and Correlate definition will not work.

8. Click Submit.

**To use an explore and correlate definition**

1. In a CA IdentityMinder environment, click Endpoints, Execute Explore and Correlate.

2. Click an explore and correlate definition to execute.

3. Click Submit.

   The user accounts that exist on the endpoint are created or updated in CA IdentityMinder based on the explore and correlate definition you created.

## Acquire the Windows NT Machine Using the Provisioning Manager

You must acquire the Windows NT machine before you can administer it with CA IdentityMinder. Perform the following procedure to acquire a Windows NT machine.

**From the Endpoint Type task view**

1. Register the machine as an endpoint in CA IdentityMinder.

   Use the Windows NT Endpoint property sheet to register a Windows NT machine. During the registration process, CA IdentityMinder identifies the Windows NT machine you want to administer and gathers information about it.

2. Explore the objects that exist on the endpoint.

   After registering the machine in CA IdentityMinder, you must explore its contents by means of the Explore and Correlate Endpoint dialog. The Exploration process finds all the Windows NT objects.

3. Correlate the explored accounts with global users.

   When you correlate accounts, CA IdentityMinder creates or links the accounts on an endpoint with global users, as follows:

   a. CA IdentityMinder attempts to match the username with each existing global user name. If a match is found, CA IdentityMinder associates the Windows NT account with the global user. If a match is not found, CA IdentityMinder performs the next step.

   b. CA IdentityMinder attempts to match the full name with each existing global user's full name. If a match is found, CA IdentityMinder associates the Windows account with the global user. If a match is not found, CA IdentityMinder performs the next step.

   c. If the Create Global Users as Needed button is checked, CA IdentityMinder creates a new global user and associates the Windows account with the global user. If the Create Global Users as Needed button is unchecked, then CA IdentityMinder associates the Windows account with the [default user] object.

   **Note:** You can correlate the accounts with global users at this time, or you can do it later.

## Significant Fields in the Endpoint Tab of the Endpoint Property Sheet

The Endpoint Tab of the Endpoint Property Sheet includes the following significant fields:

**Explore timeout:**

Specifies, in seconds, the maximum duration time a request takes for the explore operation (one level and sub-tree searches). Default is 7200 seconds (2 hours).

**Operations timeout:**

Specifies, in seconds, the maximum time any CAM/CAFT request can take, except the explore option (based searches). The minimum value that can be entered in this field is 30 seconds. The default is 300 seconds (5 minutes).

**Changing password**

Removes expired flag field. When this field is checked and a password is changed by an administrator, the expired password flag is removed (W2K and Win2003 behavior). If the field is not checked, the expired flag remains (NT behavior), and you must change your password on the first logon.

## Terminal Server Attributes Management for Accounts

On the Windows NT Node Property Tab (Windows NT Endpoint Property Sheet), the Terminal Server field is used to identify the Terminal Services family machines. If there are no Terminal Server machines, the field is blank.

For each account in the Terminal Services systems, you can see and manage the attribute from the Environment and Sessions Tab and Terminal Services Profile Tab (Windows NT Account Template or Windows NT Account Property Sheets).

The values associated with the fields on these tabs are the same as those that are provided in the NT native tools, as listed below:

**Starting program**

When checked, the program in the Program file name field from the directory in the Start in field is launched.

**Client devices**

When checked, each box causes the action it describes to be performed at account login.

**Sessions**

Lets you specify actions to be taken in case of long time idle sessions or disconnected sessions.

**Terminal Services Profile**

Lets you specify the user profile, home directory and login to the terminal server.

**Important!** Do not use the @ symbol in an NT account name if you are managing NT systems (NT4, 2000, 2003, XP) with the terminal services option.

## Synchronize BDC Systems

**Note:** This feature is only available using the Provisioning Manager.

If a Backup Domain Controller (BDC) has been promoted to a PDC (Primary Domain Controller) using NT native tools, you can synchronize BDC promotions.

**To synchronize BDC systems**

1. Right-click the endpoint and select Custom, Synchronize BDC Promotion.

   The NT4 Synchronize with BDC promotion dialog appears.

2. If the selected machine is a BDC, that has been promoted to PDC using NT native tools, fill in the dialog and click Start.

   When the operation has run, the BDC is flagged as being the action PDC.

   **Note:** Once the Start button has been clicked, the action cannot be stopped.

## Rename Accounts

**Note:** This feature is only available using the Provisioning Manager.

You have the ability to rename accounts.

**To rename an account**

1. Right-click the required account, and select Rename from the menu.

   The Windows NT account renaming dialog appears.

2. Enter a new name into the New name field and click OK.

   At the end of the action, the old name is deleted and the new name is added.

   **Note:** If the name is empty or longer than 20 characters, an error message is displayed.

## Windows NT Groups

**Note:** This feature is only available using the Provisioning Manager.

You can create and maintain Windows NT groups using the Endpoint Type task view. Use the Windows NT Group property sheet to manage your groups.

## Trust Relationships

**Note:** This feature is only available using the Provisioning Manager.

You create and maintain Windows NT trust relationships using the Endpoint Type task view. Use the Windows NT Endpoint property sheet to manage your trust relationships. The endpoint containing the trust relationships must be a PDC.

In managed NT4 PDC properties, you can create or delete inclusions between objects by clicking the Group Settings or Account Settings buttons in the Trust Relationship page.

Search filters for the local groups and for the global objects, where you can specify the attribute and corresponding value, enable you to restrict lists to see only a portion of the available objects.

## Shared Folders

**Note:** This feature is only available using the Provisioning Manager.

You can create and maintain shared folders on Windows NT machines from the Endpoint Type task view. Use the Windows NT Shared Folder property sheet to manage your shared folders.

## Size Limit Exceeded

When result size limits are exceeded, every panel only returns as many items as possible. The following are particularly affected:

- Endpoint screens where inclusions are made for trust relationships
- Local Group tab for global group inclusions

For more information, see the following:

- The *Administrator Guide*
- The Working with Endpoints, Windows NT topic in the *Procedures* help

## Exit Commands

The following native program exits are supported for the NT connector:

- Pre-Exit: The Windows NT agent executes a user command *before* it performs its own operation.
- Post-Exit: The Windows NT agent executes a user command after it performs its own operation.

Resources to write program exits comes with the Provisioning SDK. For more information, see the *Programming Guide for Provisioning*.

## Configuration File

Currently, CA IdentityMinder implements the pre-exits and post-exits in the NT Domain. Therefore, to trigger the user add-on commands, you must define them in the ExitSetup.ini file that is installed by CA IdentityMinder. By default, this file does not activate any specific command.

The ExitSetup file is located in the following directory:

```
Agent Home Dir\Config\ExitSetup.ini
```

For example:

```
C:\Program Files\CA\Identity Manager\Provisioning Agent for Windows Local Users and Groups\data\ExitSetup.ini
```

The following table describes the typical contents of the configuration file:

| Headers and Variables | Value | Description |
|---|---|---|
| [Pre-exit] | | Pre-exit section header |
| Command= | Provided by the user | User command specified with an absolute path |

| Headers and Variables | Value | Description |
|---|---|---|
| Stop on error= | Yes/No | Yes-indicates that the agent command is not launched if the pre-exit fails<br>No-indicates that the agent command is launched even if the pre-exit fails. This is the default value. |
| [Post-exit] | | Post-exit section header |
| Command= | Provided by the user | User command specified with an absolute path |

## Requirements for the User Commands

The requirements, that are needed to implement the pre-exit and post-exit commands, are as follows:

- For CA IdentityMinder, the execution of a command is successful when its return code (RC) is equal to 0; any other value indicates that the execution failed. This is important because the values that are retrieved by CA IdentityMinder are processed according to this value.
- The argument values, which are sent to CA IdentityMinder agents, are also sent to the user program.
- The pre-exit and post-exit user commands are logged in the CA IdentityMinder log files.
- The pre-exit and post-exit commands are executed each time the agent is executed.

# Oracle Applications Connector

The Oracle Applications Connector lets you administer users of Oracle E-Business Suite applications and provides a single point for all user administration by letting you do the following:

- Register endpoints, explore them for objects to manage, and correlate their accounts with global users
- Create and manage Oracle Applications users by using Oracle-specific account templates
- Manually manage an Oracle Applications user responsibility list or automatically manage a group of users based on provisioning roles and account templates
- Change account passwords and account activations in one place
- Synchronize global users with their provisioning roles or synchronize global users' accounts with their account templates
- Assign an Oracle Applications account template to each of your Oracle Applications directories
- Generate and print reports about Oracle Applications users

## How the Connector Accesses Oracle Applications

The connector communicates with Oracle Applications using ODBC.

When you create an Oracle Applications endpoint, you select the mode of communication:

- **AOL Only mode**—Uses only the database stored procedures (the Application Object Library) to perform updates.
- **Normal mode**—Performs some direct updates to database fields. In previous releases, this mode provided more functionality than AOL Only mode, however this is no longer the case.

## Oracle Applications Installation and Configurations

This connector is managed using the Connector and C++ Server installation process.

**Note:** For more information and requirements, see *Connector and C++ Connector Server Installation.*

The following sections provide installation and configuration information for this connector.

## Oracle Applications Prerequisite

To set up Oracle applications endpoint, as a system administrator, you require an administrator access to the Oracle applications object library, which includes the following access rights:

- Access to "FND_USER_PKG"
- Read permission to the "FND_USER" table.

  **Note**: If it is not running in AOL mode, you also require Update permissions.
- Read and Update permissions to the user responsibilities.

To manage Oracle Applications as an endpoint, set the NLS_LANG as a system environment variable, with a value of *.UTF8*

**Note:** There must be a period (.) before UTF8 on the computer where the Connector Server is installed.

## Oracle Applications Limitations

The known limitations and issues with the Oracle Applications Connector are as follows:

- The Oracle Applications Connector can assign or remove Oracle Applications users from the responsibilities. However you cannot create, update, or delete the responsibilities. The Oracle Applications System Administrator must perform these operations using native Oracle Applications administrative tools (JInitiator).
- An Array Index Out of Bounds Exception error is displayed when you log into Oracle Applications with no responsibilities assigned. The same error occurs when you create the user using Oracle Applications without associating any responsibilities.

## How to Configure the Oracle Applications Connector

Before installing the Oracle Application Connector, install the Oracle Client on the same machine that the Oracle Application Connector will be installed on.

After installing your Oracle Administrative Client from the Oracle Client CD, do the following to configure it:

1. Create a service for your Oracle client.
2. Configure ODBC on your Oracle client.

   **Note:**You must install the 32-bit version of the Oracle Client package.

## Creating a Service for Your Oracle Client

Create a service for your Oracle client using the Oracle Net Configuration Assistant for Oracle Client Release 9i or 10g.

**From the Oracle Configuration and Migration Tools program group**

1. Start Oracle Net Configuration Assistant.

   The Oracle Net Configuration Assistant wizard appears.

2. Select Local Net Service Name Configuration.
3. Select Add New Service.
4. Enter the Service Name.
5. Select TCP/IP (Internet Protocol).
6. Enter the host name for the computer where the database is located.
7. Change the port number to match your Oracle server port number.
   - For Windows systems, the default port number on Oracle systems is 1521.
   - For UNIX systems, the default port number on Oracle systems is 1526.
8. Select Yes to perform a connection test.
9. Enter a name for the net service name.
10. Click Finish to save the information.

    You can view configured services by scanning the list of names on the Service Naming node of the Oracle Net Manager.

## Configure ODBC on Your Oracle Client

To configure ODBC on your Oracle client, use this procedure.

**From the Control Panel**

1. Select ODBC Manager/Data Sources, DSN tab, Add.

   The Create New Data Source wizard appears.

2. Select the Oracle ODBC Driver, and click Finish.

   The Oracle ODBC Driver Setup dialog appears.

3. Enter the data source name for the Oracle server in the Data Source Name text box.
4. Enter the service name that you created in Creating A Service For Your Oracle client
5. Enter the Oracle administrator's ID in the UserID text box.
6. Click OK.

After configuring the Oracle client, you are ready to install the Oracle Applications Connector.

### Required Oracle Administrator Account Privileges

The Oracle Applications Connector requires the user names and passwords of two users when you set up an endpoint:

**Database User**

This account is used when connecting to the database. The database user must have the appropriate privileges to manage the Oracle Applications tables.

**Applications User**

This account is used when managing Oracle applications. You can use any user that has already been created in Oracle Applications and that has the System Administrator standard responsibility.

## Oracle Applications Support for FIPS and IPv6

For this release of CA IdentityMinder, the Oracle Applications Connector does not support FIPs or IPv6.

## Connector-Specific Features

This section details your connector's specific management features, such as how to acquire and explore your endpoint. Also included are account, provisioning roles, account template, and group information specifically for your connector.

### Acquire an Oracle Applications System Using the User Console

You must acquire the Oracle Applications system before you can administer it with CA IdentityMinder.

**To acquire an Oracle Applications system using the User Console**

1. Select Endpoints, Manage Endpoints,Create Endpoint
2. Select Oracle Applications from the drop-down list box on Create a new endpoint of Endpoint Type, and click Ok

   Use the Create Oracle Applications Endpoint page to register an Oracle Applications system. During the registration process, CA IdentityMinder identifies the Oracle Applications system you want to administer and gathers information about it.
3. After entering the required information, click Submit.

   You are now ready to explore and Correlate the endpoint.

4. Click Endpoints, Explore and Correlate Definitions, Create Explore and Correlate Definition to explore the objects that exist on the endpoint.

   The Exploration process finds all Oracle Applications accounts and groups. You can correlate the accounts with global users at this time or you can correlate them later.

5. Click OK to start a new definition.

6. Complete the Explore and Correlate Tab as follows:

   a. Fill in Explore and Correlate name with any meaningful name.

      Click Select Container/Endpoint/Explore Method to click an Oracle Applications endpoint to explore.

   b. Click the Explore/Correlate Actions to perform:

      - **Explore directory for managed objects**—Finds objects that are stored on the endpoint and not in the provisioning directory.
      - **Correlate accounts to users**—Correlates the objects that were found in the explore function with users in the provisioning directory. If the user is found, the object is correlated with the user. However, you can instead select that you want to assign the account to the existing user (the default user) or create the user.
      - **Update user fields**—If a mapping exists between the object fields and the user fields, the user fields are updated with data from the objects fields.

7. Complete the Recurrence tab if you want to schedule when the task to executes.

   a. Click Schedule.

   b. Complete the fields to determine when this task should execute.

      You may prefer to schedule the task to execute overnight to interfere less with routine access of the system.

   **Note**: This operation requires the client browser to be in the same time zone as the server. For example, if the client time is 10:00 PM on Tuesday when the server time is 7:00 AM, the Explore and Correlate definition will not work.

8. Click Submit.

**To use an explore and correlate definition**

1. In a CA IdentityMinder environment, click Endpoints, Execute Explore and Correlate.

2. Click an explore and correlate definition to execute.

3. Click Submit.

   The user accounts that exist on the endpoint are created or updated in CA IdentityMinder based on the explore and correlate definition you created.

## Acquire an Oracle Application System Using the Provisioning Manager

You must acquire the Oracle Applications system before you can administer it with CA IdentityMinder.

**From the Endpoint type task view**

1. Register the Oracle Applications system as an endpoint in Provisioning Manager.

   Use the Oracle Applications Endpoint property sheet to register an Oracle Applications system. During the registration process, CA IdentityMinder identifies the Oracle Applications system that you want to administer and gathers information about it.

   **Note:** Use the native Oracle tools to verify that the Oracle Applications system can be accessed using the given system login ID and password.

2. Explore the objects that exist on the endpoint.

   After registering the server in CA IdentityMinder, you can explore its contents using the Explore and Correlate Endpoint dialog. The Exploration process finds all Oracle Applications users. You can correlate the accounts with global users at this time or you can correlate them later. The topic “Explore and Correlate Endpoint Dialog” in Provisioning Manager help provides a complete explanation of this dialog.

3. Correlate the explored accounts with global users.

   When you correlate accounts, the CA IdentityMinder creates or links the accounts on an endpoint with global users as follows:

   a. CA IdentityMinder attempts to match the Oracle Applications user name with each existing global user name. If a match is found, CA IdentityMinder associates the Oracle Applications user with the global user. If a match is not found, CA IdentityMinder performs the next step.

   b. If the Create Global Users as Needed button is checked, CA IdentityMinder creates a new global user and associates the Oracle Applications user with the global user. If the Create Global Users as Needed button is unchecked, CA IdentityMinder performs the next step.

   c. CA IdentityMinder associates the Oracle Applications user with the [default user] object.

**Note:** Use the User Console to add or remove the Oracle roles to any of the Oracle Account Templates. When you add or remove the Oracle roles to Oracle Account Template and execute the Synchronize Accounts with Account Templates task using the Provisioning Manager, the eTORACompoundRoles attribute does not hold any value causing problems such as automatic detachment of Oracle roles.

## Update Endpoint Responsibilities Tab in User Console

After creating an FND Endpoint in the User Console, you must update the Attribute Oracle Applications User and Security Context details on the Endpoint Responsibilities Tab to successfully create the provisioning account.

To update this information, follow this procedure:

**From the User Console**

1. Select the Endpoints, Manage Endpoints, Modify Endpoints.

   The Modify Endpoint: Select Endpoint screen appears.

2. Select Oracle Applications from the drop-down list, enter the endpoint name in the search box, and click Search.

   The endpoint appears in the search table results.

3. Select the endpoint and click Select.

   The Endpoint property page appears.

4. Select the Endpoint Responsibilities Tab and enter the Attribute Oracle Applications User and Security Context details and click Submit.

   The Modify Endpoint task has been submitted.

## Changing the Oracle Account Password

Before changing the password of an Oracle account in the User Console, you must reset the user password first.

## Oracle Applications User Provisioning Roles and Account Templates

The Oracle Applications Default Account Template, provided with the Oracle Applications Connector, does not give a user the minimum security level needed to access an endpoint. One or more responsibilities need to be assigned for the account to be active. The list of responsibilities depends on which Oracle Applications are installed. However, you can use it to as a model to create new account templates.

**Note:** The Oracle Applications Default Account Template automatically sets the user name and password to the global user account ID so that the user can access Oracle Applications.

**Note:** An endpoint must first be included (associated) with an account template before responsibilities can be added to it.

## Create Account Templates

The Default Account Template, provided with each connector, gives a user the minimum security level needed to access an endpoint. You can use it as a model to create new account templates.

**To create an account template**

1. Click the Provisioning Roles task button, select the connector's Account Template in the Object Type drop-down list box and click New.

   The Account Template Property Sheet for the specified connector appears.

2. Complete the Account Template Property Sheet by:

   a. Selecting an endpoint to populate the drop-down and group selection lists.

   b. Selecting group memberships and other account settings.

   c. Clicking OK.

   A new account template is created for your connector.

## Manage Oracle Applications User Accounts

To manage FND accounts in the Provisioning Manager, use this procedure:

**From the Endpoint Type task view**

1. Select an endpoint and click Search.

   A list of endpoints for the selected endpoint type is presented.

2. Right-click an endpoint, and select Content from the context menu.

   The Endpoint Content appears.

3. Select the Users container from the container tree and enter the search criteria in Search For Content, and then click Search.

4. Click Done.

   A list of the user accounts in that endpoint appears.

# Oracle Connector

The Oracle Connector lets you administer accounts and groups on Oracle systems and provides a single point for all user administration by letting you do the following:

- Register endpoints, explore them for objects to manage, and correlate their accounts with global users
- Create and manage Oracle accounts using Oracle-specific account templates
- Change account passwords and account activations in one place

- Synchronize global users with their provisioning roles or synchronize global users' accounts with their account templates
- Assign an Oracle account template to each of your Oracle endpoints
- Use the default Oracle Policy to create accounts with the minimum security level needed to access an Oracle endpoint
- Create and manage Oracle profiles and roles
- Generate and print reports about Oracle accounts
- Assign Oracle packages and procedures to Oracle accounts

## Oracle Configuration

The Oracle connector is managed by CA IAM CS.

Communication between the Provisioning Server and the Oracle server relies on a JDBC connection. A URL specifies connection details to each server, as illustrated in the following example:

`jdbc:oracle:thin:@`*`hostname:port:servicename`*

**hostname**

The hostname or IP address of the Oracle Server

**port**

The port number of the Oracle service. **Default:** 1521.

**servicename**

Oracle Service Name to connect to.

### Example URL

The following URL connects to an Oracle instance named ORACLE running on the default port on the server named oracle_server_host:

```
jdbc:oracle:thin:@oracle_server_host:1521:ORACLE
```

For more information, search for JDBC on the Oracle site.

## Oracle Migration Steps

To migrate from the C++ Oracle connector to the Java Oracle connector, you must do the following:

- Install the Oracle Java connector using the CA IAM CS installation
- Add the URL as defined in Oracle Configuration to each existing Oracle endpoint. To do this, edit the endpoint and supply the URL in the JDBC URL field.
- You can remove your DSN if it is not being used for another other purpose

Once this has been done, all types of operations can be executed against the existing Oracle endpoints seamlessly.

## Oracle Support for FIPS and IPv6

For this release of CA IdentityMinder, the Oracle Connector does not support FIPs or IPv6.

## Connector-Specific Features

This section details your connector's specific management features, such as how to acquire and explore your endpoint. Also included are account, provisioning roles, account template, and group information specifically for your connector.

### Oracle Limitations

The Oracle connector cannot be used to perform the following operation. The Oracle database administrator must perform this operation using native Oracle administrative tools.

- Manage system privileges or object privileges that apply to Oracle accounts or Oracle roles

### Suspend Operation Locks User Accounts

After suspending an Oracle account from either the User Console, the user account status shows both Suspended and Locked.

The Oracle Connector considers both Suspend and Lock as one operation. The Oracle account can not be suspended and unlocked nor can it be active and locked.

### Resume Operation Resumes and Unlocks Suspended User Accounts

When performing a Resume operation on a Suspended account, the Oracle Connector both resumes and unlocks the account.

## Required Oracle Administrator Account Privileges

The Oracle administrator account that you use with CA IdentityMinder is the account name that you enter in the System Logon field of the Endpoint tab of the Oracle Endpoint property sheet. This account requires the following minimum privileges to take full advantage of the Oracle Connector:

- The following system privileges:

  Alter Profile
  Alter Any Role
  Alter User
  Create Profile
  Create Role
  Create Session
  Create User
  Drop Profile
  Drop User
  Drop Any Role
  Grant Any Privilege
  Grant Any Role

- The SELECT object privilege on the following views in the SYS schema:

  DBA_OBJECTS
  DBA_PROFILES
  DBA_ROLES
  DBA_ROLE_PRIVS
  DBA_TABLESPACES
  DBA_TAB_PRIVS
  DBA_TS_QUOTAS
  DBA_USERS

To grant privileges to Oracle accounts for packages and procedures, ensure that the account name specified in the Logon field of the Oracle Endpoint property sheet is either:

- The owner of these packages and procedures
- Has execute privileges with "Admin Option" for these packages and procedures

## Acquire an Oracle System Using the User Console

You must acquire the Oracle system before you can administer it with CA IdentityMinder.

**To acquire an Oracle system using the User Console**

1. Select Endpoints, Manage Endpoints,Create Endpoint
2. Select Oracle from the drop-down list box on Create a new endpoint of Endpoint Type, and click Ok

   Use the Create Oracle Endpoint page to register an Oracle system. During the registration process, CA IdentityMinder identifies the Oracle system you want to administer and gathers information about it.
3. After entering the required information, click Submit.

   You are now ready to explore and Correlate the endpoint.
4. Click Endpoints, Explore and Correlate Definitions, Create Explore and Correlate Definition to explore the objects that exist on the endpoint.

   The Exploration process finds all Oracle accounts and groups. You can correlate the accounts with global users at this time or you can correlate them later.
5. Click OK to start a new definition.
6. Complete the Explore and Correlate Tab as follows:
   a. Fill in Explore and Correlate name with any meaningful name.

      Click Select Container/Endpoint/Explore Method to click an Oracle endpoint to explore.

   b. Click the Explore/Correlate Actions to perform:
      - **Explore directory for managed objects**—Finds objects that are stored on the endpoint and not in the provisioning directory.
      - **Correlate accounts to users**—Correlates the objects that were found in the explore function with users in the provisioning directory. If the user is found, the object is correlated with the user. However, you can instead select that you want to assign the account to the existing user (the default user) or create the user.
      - **Update user fields**—If a mapping exists between the object fields and the user fields, the user fields are updated with data from the objects fields.
7. Complete the Recurrence tab if you want to schedule when the task to executes.
   a. Click Schedule.

   b. Complete the fields to determine when this task should execute.

      You may prefer to schedule the task to execute overnight to interfere less with routine access of the system.

**Note**: This operation requires the client browser to be in the same time zone as the server. For example, if the client time is 10:00 PM on Tuesday when the server time is 7:00 AM, the Explore and Correlate definition will not work.

8. Click Submit.

**To use an explore and correlate definition**

1. In a CA IdentityMinder environment, click Endpoints, Execute Explore and Correlate.
2. Click an explore and correlate definition to execute.
3. Click Submit.

   The user accounts that exist on the endpoint are created or updated in CA IdentityMinder based on the explore and correlate definition you created.

## Acquire an Oracle System Using the Provisioning Manager

You must acquire the Oracle system before you can administer it with CA IdentityMinder. To acquire an Oracle system, you must do the following:

**From the Endpoint Type task view**

1. Register the Oracle server as an endpoint using the Provisioning Manager.

   Use the Oracle Endpoint property sheet to register an Oracle system. During the registration process, the Provisioning Server identifies the Oracle system you want to administer and gathers information about it.

   **Note:** Use the native Oracle tools to verify that the Oracle system can be accessed using the given system login ID and password.

2. Explore the objects that exist on the endpoint.

   After registering the server with the Provisioning Manager, you can explore its contents. Use the Explore and Correlate Endpoint dialog. The Exploration process finds all Oracle accounts, profiles, and roles. You can correlate the accounts with global users at this time or you can correlate them later.

3. Correlate the explored accounts with global users.

   When you correlate accounts, the Provisioning Server creates or links the accounts on a endpoint with global users, as follows:

a. The Provisioning Server attempts to match the Oracle name with each existing global user name. If a match is found, the Provisioning Server associates the Oracle account with the global user. If a match is not found, the Provisioning Server performs the next step.

b. If the Create Global Users as Needed button is checked, the Provisioning Server creates a new global user and then associates the Oracle account with the global user. If the Create Global Users as Needed button is unchecked, the Provisioning Server performs the next step.

c. The Provisioning Server associates the Oracle account with the [default user] object.

**Note:** Use the User Console to add or remove the Oracle roles to any of the Oracle Account Templates. When you add or remove the Oracle roles to Oracle Account Template and execute the Synchronize Accounts with Account Templates task using the Provisioning Manager, the eTORACompoundRoles attribute does not hold any value causing problems such as automatic detachment of Oracle roles.

## Oracle Account Templates

The Oracle Default Policy automatically sets the user name and password to the global user account ID and the authentication type to LOCAL.

## Oracle Accounts

Use the Oracle Account property sheet when managing your accounts.

## Oracle Packages

The Oracle Packages container holds all stored Oracle packages on your system.

## Oracle Procedures

The Oracle Procedures container holds all stored Oracle procedures on your system.

## Oracle Roles

The Provisioning Manager lets you create and maintain Oracle roles using the Endpoint Type task view. Use the Oracle Role property sheet when managing your Oracle roles.

## Oracle Profiles

An Oracle profile lets you specify the values of Oracle account attributes such as connect time, CPU time, and password rules.

## Oracle Etautil Conventions

Use the following Oracle conventions in your etautil commands:

- The endpoint type name (eTNamespaceName) is Oracle Server
- The endpoint type prefix is ORA. Therefore, the Oracle class names are:
  - eTORADirectory for an endpoint
  - eTORAPolicyContainerName for an account template container
  - eTORAPolicy for an account template

# OS/400 Connector

The OS/400 Connector lets you administer accounts and groups on OS/400 machines and provides a single point for all user administration by letting you do the following:

- Register endpoints, explore them for objects to manage, and correlate their accounts with global users
- Create and manage OS/400 accounts using OS/400-specific account templates
- Change account passwords and account activations in one place
- Synchronize global users with their provisioning roles or synchronize global users' accounts with their account templates
- Assign an OS/400 account template to each of your OS/400 endpoints
- Use the default endpoint type account template to create accounts with the minimum level of security needed to access an OS/400 endpoint
- Create and manage OS/400 groups
- Generate and print reports about OS/400 accounts and groups

## OS/400 Installation

The OS/400 Connector is installed with CA IAM CS.

## OS/400 Migration Steps

To migrate from the C++ OS/400 connector to the Java OS/400 connector, you must do the following:

- Install the OS/400 Java connector using CA IAM CS
- Using Connector Xpress, switch the OS400 Endpoint Type Connector Server from the C++ Connector Server to CA IAM CS

Once this has been done, all types of operations can be executed against the existing OS400 endpoints seamlessly.

## How to Configure your Machines

You must configure your OS/400 system to use the OS/400 connector. To do this, install and configure programs on your OS/400 system.

## Install and Configure Programs on OS/400

The JTOPEN toolkit used by the OS/400 connector requires the following programs to be installed and configured on your OS/400 system:

- TC1 Licensed Program (TCP/IP Connectivity Utilities for OS/400)
- Host Server Option of OS/400

These programs are necessary so the OS/400 connector can connect to your OS/400 system and access its data and services.

## How to Secure Your Information (Optional)

You can send information through secured or unsecured channels.

For security purposes, we recommend that you secure the communications between all your machines. To do this, you must configure the following:

- Provisioning Server
- CA IAM CS
- OS/400 system

## Connect Using SSL

Communication between the Provisioning Server/CA IAM CS and the  OS/400 machine is secured by SSL. Using SSL is optional in both links and can be switched on when acquiring the OS/400 machine. Certificates are used to authenticate the server and encrypt communications and the username and password are used to authenticate the client request on the OS/400 machine.

To use SSL, the CA IAM CS machine must have the endpoint certificate installed in the Java certificate store in the JRE in which CA IAM CS machine is running.

## Configure Your OS/400 System

Secure the channel between CA IAM CS and your OS/400 system by performing these steps:

1. Prepare the system
2. Select the certificate location
3. Import the certificate authority
4. Request a server certificate from the CA
5. Request a server certificate for your system
6. Import the server certificate
7. Assign the Server Certificate to your OS/400 applications

## Prepare the System

To prepare your OS/400 system, perform the following procedure:

**On your OS/400 system**

1. Verify that one of the following client encryption licensed programs is installed:

   **5722-CE2**

      IBM iSeries Client Encryption (56-bit) Version 5, Release 1. This program is used in countries other than the United States or Canada.

   **5722-CE3**

      IBM iSeries Client Encryption (128-bit) Version 5, Release 1. This program is used in the United States and Canada only.

**5769-CE2**

IBM iSeries Client Encryption (56-bit) Version 4, Release 5. This program is used in countries other than the United States or Canada.

**5769-CE3**

IBM iSeries Client Encryption (128-bit) Version 4, Release 5. This program is used in the United States and Canada only.

**Note**: These programs are an installation option on your OS/400 system.

2. Verify that one of the following server encryption licensed programs is installed:

   **5722-AC2**

   IBM iSeries Server Encryption (56-bit) Version 5, Release 1. This program is used in countries other than the United States or Canada.

   **5769-AC2**

   IBM iSeries Server Encryption (56-bit) Version 4, Release 5. This program is used in countries other than the United States or Canada.

   **5769-AC3**

   IBM iSeries Server Encryption (128-bit) Version 4, Release 5. This program is used in the United States and Canada only.

   **Note**: These programs are an installation option on your OS/400 system.

3. Verify that the following licensed programs are installed:

   **5761-SS1**

   Product Option 34 - Digital Certificate Manager

   **5761-DG1**

   IBM HTTP Server

4. Create a file share from your OS/400 system to your Provisioning Server/CA IAM CS.

## Select the Certificate Location

Select the location where you will import the certificate on your OS/400 system.

**To select the location**

1. Start the HTTP Administration Server using the Operations Navigator or run the following command at your OS/400 command prompt:

   ```
   STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)
   ```

2. Connect to the HTTP Administration Server by pointing your browser at the following location and logging on with your system credentials:
   `http://server:2001`

   ***server***

   Specifies the name of the system running OS/400.

   **Note**: Your logon ID must have the All Object Access and System Configuration permissions.

3. Select the Digital Certificate Manager link.

   The Digital Certificate Manager window appears. The left frame contains navigational buttons and the right frame contains command buttons.

   **Note**: The steps that reference the Digital Certificate Manager are based on Version 5, Release 1. If you are using another version, these steps may vary slightly.

4. Click the Select a Certificate Store button in the left frame.
5. Select the *SYSTEM store radio button and then click Continue.
6. Enter the password for the *SYSTEM certificate store and then click Continue.

## Import the Certificate Authority

Once you have selected the certificate location, import the certificate from your Certificate Authority (CA).

**From the left frame**

1. Expand the Manage Certificates link.
2. Select the Import Certificate link.

   The Import Certificate window appears.

3. Select the Certificate Authority (CA) radio button and then click Continue.
4. Enter the directory location that contains the certificate for the Integrated File System (IFS) on your OS/400 system and then click OK.

   For example, enter: \home\etadmin\*certificate_file_name.*

5. Enter a unique name in the Label field for the certificate, for example etaCACert, and then click Continue.
6. Click the OK button.

The Digital Certificate Manager reads the certificate file and imports it into the system.

## Request a Server Certificate from the CA

After importing the Certificate Authority, you must now request a server certificate.

**From the CA**

1. Select the Create Certificate option.

   The Create Certificate window appears.

2. Select the Server or client certificate radio button and then click Continue.

3. Select the Internet Certificate Authority radio button, for example VeriSign, and then click Continue.

4. Enter at least the following information and then click Continue:

   **Key size**

   1024 bits

   **Certificate Label**

   The name of your certificate

   **Common Name**

   The name of your server

   **Organization Name**

   The name of your organization

   **State or province**

   The name of your state or province

   **Country**

   The name of your country

5. Copy the generated lines (including the BEGIN and END lines) into a file and then save that file on your OS/400 system.

## Request a Server Certificate for Your System

To request a server certificate for your OS/400 system, follow this procedure:

**From a Certificate Authority (CA)**

1. Install and configure Microsoft Certificate Services on your Windows 2000 server.

2. Point your browser to http://*computer-name*/certsrv.

   where *computer-name* is the name of the computer for which you are generating the certificate. The Microsoft Certificate Services Wizard appears.

3. Select Request a certificate, and click Next.

4. Select Advanced request, and click Next.

5. Select Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file, and click Next.
6. Open the certreq.txt file with Notepad and cut its contents.
7. Paste the contents of certreq.txt in the Saved Request box, and click Submit.
8. Select Base 64 Encoded, and click the Download CA Certificate.
9. Save the certificate to your hard drive.

   **Note:** Remember the location where you save the certificate.

## Import the Server Certificate

Once you generate a server certificate, you can import it into the system.

**From the CA**

1. Expand the Manage Certificates link in the left frame.
2. Select the Import Certificate link.

   The Import Certificate window appears.
3. Select the Server or client radio button and then click Continue.
4. Enter the directory path that contains the certificate for the IFS on your OS/400 system and click Continue.

   For example, enter: \home\etadmin\usildaaj.cer.
5. Click OK.

## Assign the Server Certificate to Your OS/400 Applications

After importing the certificate, you must assign the server certificate to the following applications:

- OS/400 TCP Central Server
- OS/400 TCP Remote Command Server
- OS/400 TCP Signon Server

**From the CA**

1. Expand Manage Applications in the left frame.
2. Select Update certificate assignment.
3. Select Server and then click Continue.

   The Update Certificate Assignment window appears.

4. Perform the following steps for each of the applications:

   a. Select the radio button for the application and then click the Update Certificate Assignment button.

   b. Select the server certificate and then click the Assign New Certificate button.

5. Stop the applications by issuing the following command with each argument:

   ```
   ENDHOSTSVR *CENTRAL
   ENDHOSTSVR *RMTCMD

   ENDHOSTSVR *SIGNON
   ```

6. Start the applications by issuing the following command with each argument:

   ```
   STRHOSTSVR *CENTRAL RQDPCL(*TCP)
   STRHOSTSVR *RMTCMD RQDPCL(*TCP)
   STRHOSTSVR *SIGNON RQDPCL(*TCP)
   ```

## Configure CA IAM CS

If you are using a certificate from one of the following CAs, you do not need to perform this step:

- IBM World Registry
- Integrion Financial Network
- RSA Data Security, Inc.
- Thawte Consulting
- VeriSign, Inc.

If you want to use a certificate from a different CA, import the certificate into CA IAM CS. If you use the same certificate for each OS/400 system, you will perform these steps only once.

**Follow these steps: NEW STEPS**

1. Log in to CA IAM CS (see page 21).
2. At the top, click the Certificates tab.

   This tab lists all of the certificates in the CA IAM CS keystore. To filter the list of certificates by their names, type in the Certificate Filter box.
3. To add a certificate, click Add, then enter the details of the certificate.

   Add a certificate:

   - **Certificate**—Enter the path to the certificate file
   - **Alias**—Enter an alias for storing the certificate

   Add a keystore:

   - **Certificate**—Enter the path to the keystore file
   - **Alias**—Enter alias for storing the certificate. This alias also identifies the certificate in that keystore.
   - **Keystore Password**—Enter the password of the keystore

**Follow these steps: OLD STEPS**

1. Stop the CA IAM CS service.
2. Copy the CA certificate from your certificate authority to the directory where the connector client certificate keystore is located. Refer to the server_jcs.properties for the setting of connectorManager.connectorClientCertStore to determine the location of the connector client certificate keystore. The default value is set to ../conf/ssl.keystore.
3. Open a DOS screen and change the DOS prompt to the directory where  the connector client certificate keystore is located. For example,

   ```
   cd C:\Program Files\CA\Identity Manager\Connector Server\conf\
   ```

4. Issue the following command to import the CA certificate into the CA certificate store for Java:

   ```
   ..\..\bin\keytool -import -alias "eTrust Admin CA Certificate" -file
   certificate_name.cer -keystore ssl.keystore
   ```

   a. Enter the default password **secret** (if it has not been changed) at the "Enter a keystore password" prompt.

      **Note:** You can use bin\ ldaps_password.bat utility to change the keystore's password.

   b. Enter **yes** at the "Trust this certificate" prompt.

5. Restart CA IAM CS service.

### Password Synchronization Agent

The Password Synchronization agent lets password changes, made on the OS/400 endpoint system, be propagated to your other accounts managed by CA IdentityMinder. For more information, see the CA IdentityMinder *Administrator's Guide*.

## OS/400 Support for FIPS and IPv6

For this release of CA IdentityMinder, the OS/400 Connector does not support FIPs or IPv6.

The OS/400 Password Synchronization Agent also does not support FIPS or IPv6.

## Connector-Specific Features

This section details your connector's specific management features, such as how to acquire and explore your endpoint. Also included are account, provisioning roles, account template, and group information specifically for your connector.

## Acquire an OS/400 Maching Using the User Console

You must acquire the OS/400 machine before you can administer it with CA IdentityMinder.

**To acquire an OS/400 machine using the User Console**

1. Select Endpoints, Manage Endpoints,Create Endpoint
2. Select OS400 from the drop-down list box on Create a new endpoint of Endpoint Type, and click Ok

   Use the Create OS400 Endpoint page to register an OS/400 machine. During the registration process, CA IdentityMinder identifies the OS/400 machine you want to administer and gathers information about it.
3. After entering the required information, click Submit.

   You are now ready to explore and Correlate the endpoint.
4. Click Endpoints, Explore and Correlate Definitions, Create Explore and Correlate Definition to explore the objects that exist on the endpoint.

   The Exploration process finds all OS/400 accounts and groups. You can correlate the accounts with global users at this time or you can correlate them later.
5. Click OK to start a new definition.
6. Complete the Explore and Correlate Tab as follows:
   a. Fill in Explore and Correlate name with any meaningful name.

      Click Select Container/Endpoint/Explore Method to click an OS/400 endpoint to explore.

   b. Click the Explore/Correlate Actions to perform:
      - **Explore directory for managed objects**—Finds objects that are stored on the endpoint and not in the provisioning directory.
      - **Correlate accounts to users**—Correlates the objects that were found in the explore function with users in the provisioning directory. If the user is found, the object is correlated with the user. However, you can instead select that you want to assign the account to the existing user (the default user) or create the user.
      - **Update user fields**—If a mapping exists between the object fields and the user fields, the user fields are updated with data from the objects fields.
7. Complete the Recurrence tab if you want to schedule when the task to executes.
   a. Click Schedule.

   b. Complete the fields to determine when this task should execute.

      You may prefer to schedule the task to execute overnight to interfere less with routine access of the system.

**Note**: This operation requires the client browser to be in the same time zone as the server. For example, if the client time is 10:00 PM on Tuesday when the server time is 7:00 AM, the Explore and Correlate definition will not work.

8. Click Submit.

**To use an explore and correlate definition**

1. In a CA IdentityMinder environment, click Endpoints, Execute Explore and Correlate.
2. Click an explore and correlate definition to execute.
3. Click Submit.

   The user accounts that exist on the endpoint are created or updated in CA IdentityMinder based on the explore and correlate definition you created.

## Acquire an OS/400 Machine Using the Provisioning Manager

You must acquire the OS/400 machine before you can administer it with CA IdentityMinder.

**From the OS/400 Endpoint Property Sheet**

1. Register the machine as an endpoint in CA IdentityMinder.

   Provide the OS/400 server machine name, the user ID and password when acquiring an OS/400 system.

   **Note:** Before acquiring the endpoint, make sure that it is registered to use the Java connector. To do this:

   1. In Connector Xpress, right-click the OS400 endpoint
   2. Select Set Managing CS
   3. Select Java Connector

   During the registration process, CA IdentityMinder identifies the OS/400 machine you want to administer and gathers information about it.

2. Explore the objects that exist on the endpoint.

   After registering the machine in CA IdentityMinder, you can explore its contents. Use the Explore and Correlate Endpoint dialog. The Exploration process finds all OS/400 objects. You can correlate the accounts with global users at this time, or you can wait to correlate them.

3. Correlate the explored accounts to global users by choosing either of the following Connectors:

   - Use existing global users
   - Choose this option when there are already global users in CA IdentityMinder and you want to connect the existing global users to the OS/400 accounts
   - Create global users as needed

     Choose this option when there are no global users and you want to populate CA IdentityMinder from the OS/400 accounts.

   When you correlate accounts, CA IdentityMinder creates or links the accounts on an endpoint with global users, as follows:

   a. CA IdentityMinder attempts to match the user profile name with each existing global user name. If a match is found, CA IdentityMinder associates the OS/400 account with the global user. If a match is not found, CA IdentityMinder performs the next step.
   b. CA IdentityMinder attempts to match the user profile name with each existing global user's full name. If a match is found, CA IdentityMinder associates the OS/400 account with the global user. If a match is not found, CA IdentityMinder performs the following step.
   c. CA IdentityMinder associates the OS/400 account with the [default user] object or a new global user is created depending on your choice.

**Note**: More information on enabling Secure Socket Layer (SSL) communications between the Provisioning Server and the OS/400 system exists in the Provisioning Manager Help.

## Streaming Search Results

During the explore operation, the connector returns accounts to the Provisioning server as soon as possible instead of waiting until all accounts have been reviewed. This reduces memory usage resulting in a more efficient explore process.

## User ID Limitation

When creating User profiles in an Os/400 system, avoid using User ID numbers larger than 2147483647. A User ID larger than this cannot be mapped to global user UID.

## Non-Latin Characters are not Supported

When creating an OS/400 endpoint, non-latin character encodings are not supported.

## OS/400 Provisioning Roles and Account Templates

The OS/400 Default Policy, provided with the OS/400 Connector, gives a user the minimum security level needed to access an endpoint. You can use it as a model to create new account templates.

## Policy Default Values

The new account templates are created with default values for most attributes. The new account templates are valid as soon as they are created and the attributes can be customized as necessary.

## OS/400 Cascading Delete

In previous versions, if an OS400 account owned objects, the account could not be deleted from CA IdentityMinder. In this version, a flag called “cascadingDelete” in the OS400 connector.xml in CA IAM CS can be used to change this behavior. When the flag is set to true, the account and all objects owned by the account will be deleted. The default value is set to true.

If you want to override the default value, you must:

1. From a command prompt issue the following command:

   ```
   cd cs-home\conf\override\as400\
   copy SAMPLE.connector.xml connector.xml
   ```

2. Edit connector.xml to set "cascadingDelete" property value to either "true" or "false" as desired.

3. Restart the im_jcs so that the change takes effect.

   **Note:** See Customize the Configuration for a Connector (see page 55) for more information on override connector.xml files.

## OS/400 Security Requirements

The OS/400 Connector issues remote commands to the endpoint system to manage accounts. The managing user profile must have permission to issue remote commands for creating, reading, modifying, and deleting accounts. Areas of security to consider include, special authorities of the managing account (*SECADM is mandatory), exit programs implementing security, and authorization to user profiles.

## OS/400 Groups

You can create and maintain OS/400 groups using the Endpoint type task view. Use the OS/400 Group property sheet when managing your groups.

When a new group is defined, you should perform another exploration on the endpoint so CA IdentityMinder has an updated group list.

## Deleting Account Members from Groups

Account members cannot be deleted from a group if that group is designated as the primary group. You must remove the group from the account member . For example, ProvisioningGroup has two account members, Prov1 and Prov2, and ProvisioningGroup is the primary group of Prov1. Prov2 has a primary group FinancialGroup and a supplement group called ProvisioningGroup. If you try to delete Prov1 and Prov2 from ProvisioningGroup, only Prov2 is removed successfully. Prov1 remains as an account member of ProvisioningGroup.

## OS/400 Directory Entry Names

When an account or group is created, a directory entry is created to store personal information about the user. Previously, the directory entry name was assumed to be the same as the user profile name. The attributes can now be set independently. If the Directory Entry Name is not specified, then a directory entry is not created for that user and many attributes cannot be set. Directory entry names must be unique across accounts and groups.

## Changing Connection Settings

The connection settings associated with each endpoint cannot be changed using the Endpoint property sheet. To change incorrect connection settings, follow these steps:

1. Right-click the endpoint name.

   The context sensitive menu appears.

2. Select Custom..., Change Admin Password.

   The Change Password Dialog appears.

3. Fill in the dialog and select OK.

   The dialog closes.

After the connection settings are changed, they are verified by attempting a connection to the OS/400 machine. The new settings are only saved if the connection is successful.

## Conventions

Use the following OS/400 conventions in your etautil commands:

- The endpoint type name (eTNamespaceName) is OS400
- The endpoint type prefix is AS4. Therefore, the OS/400 class names are:
  - eTAS4Directory for an endpoint
  - eTAS4PolicyContainerName for an account template container
  - eTAS4Policy for an account template

## OS/400 Native Program Exits

The Java OS/400 Connector supports Native Program Exits in the same way as the eTrust Admin 8.1 SP2 OS/400 Connector did with the following limitations:

- Only one parameter of the Command Call format can be specified in Program Exits.
- The Program Exits can target only account objects, not groups.

**Note:** CA IAM CS provides a Scripting Style Processor interface for connectors. You can write code in the JavaScript scripting language to add extra logic to, or change the behavior of the OS/400 connector's operations. This approach is much more powerful than the C++ OS/400 Connector's Native Program Exits approach because you can access the full operation's details and write whatever you want to achieve for both account and group objects.

An example of this approach follows:

To change the description for each new account to the value of 'To demo scripting program exit concept works', use the conf/as4script_opbindings.xml file within the OS/400 Connector's archive file: <jcs-home>/lib/jcs-connector-as400.jar. Uncomment the "staticMethodScriptStyleMetaDataFile" in <jcs-home>/conf/override/as400/connector.xml and restart the im_jcs to turn on  this behaviour.

See the *Connector Programming Guide* for more information on scripting-style programming.

# PeopleSoft Connector

The PeopleSoft connector works with Oracle PeopleSoft HRMS.

The PeopleSoft connector manages the PeopleSoft User Profiles, Roles, and Permission Lists on a PeopleSoft application server. You can use the connector as a single point of administration to do the following:

- Explore PeopleSoft user profiles, roles, and permission lists
- Correlate the user profiles to CA IdentityMinder global users
- Modify PeopleSoft user passwords
- Lock and unlock PeopleSoft user profiles
- Add and delete PeopleSoft user profiles
- Modify PeopleSoft user profiles
- Add and delete PeopleSoft roles
- Modify PeopleSoft roles
- Add and delete PeopleSoft permission lists
- Modify PeopleSoft permission lists

## Requirements for Connecting to Oracle PeopleSoft

The following are required to run the PeopleSoft Connector:

- PeopleSoft HRMS 8.9
- PeopleTools 8.48,8.49, 8.50 and 8.51 if the appropriate PeopleSoft API version (psjoa.jar) is used.
- PeopleSoft Internet Architecture, Tuxedo, and Jolt configured on the PeopleSoft application server

## Security for the PeopleSoft Connector

The PPS connector communicates with the PeopleSoft application using the configured Tuxedo port (9000 by default). We recommend that you enable Tuxedo-level encryption on the application server, because passwords are included in the communications.

The encryption level is controlled by the Encryption property in the JOLT Listener section of the psappsrv.cfg file for the PeopleSoft application server domain. The following are the possible values:

- 0 (default) for no encryption
- 64 for 64-bit encryption
- 128 for 128-bit encryption

If you use a Jolt port that is a few port numbers above the configured Jolt port, the connector will appear to hang and after a configurable amount of time, an error message will be sent to its client. To avoid this, you must restart im_jcs.

**Note:** The timeout is configurable in the PeopleSoft Endpoint tab. The default value is 30 seconds.

## Set Up the PeopleSoft Connector

The Oracle PeopleSoft connector uses the PeopleSoft API to access the PeopleSoft, and it requires psjoa.jar. Before you use the connector, create a bundle that contains this JAR, and then add the bundle to the connector.

There is a different version of psjoa.jar for each version of PeopleTools, and the versions are not backward-compatible. Make sure that you use the correct version.

For this reason, use a different CA IAM CS installation for each PeopleTools version that you plan to manage. For example, a set of PeopleSoft installation with PeopleTools 8.48 can be managed by one CA IAM CS installation and a set of PeopleSoft installations with PeopleTools 8.49 is managed by another CA IAM CS installation. You can route each endpoint to the correct CA IAM CS installation using Connector Xpress.

Before you use the connector, create a bundle that contains psjoa.jar, and then add the bundle to the connector.

**Follow these steps:**

1. Install or upgrade CA IAM CS.

   The installation registers CA IAM CS with the provisioning server, creates the PeopleSoft endpoint, and populates it with its associated metadata.

2. Ask the PeopleSoft administrator to send you a copy of psjoa.jar, which is in the following location:

   *peoplesoft-home*/web/psjoa/

3. Save psjoa.jar locally.

4. Run the *pps_post_install* script in the following location:

   *cs-home*/bin

   The script asks for the location of the third-party library. It then creates a bundle and moves it to the right location.

5. Log in to CA IAM CS (see page 21).

6. At the top, click the Connector Servers tab.

7. In the Connector Server Management area, click the Bundles tab.

8. Add the new bundle:

   a. In the Bundles area on the right, click Add.

   b. Browse to the bundle that the script created, then select the connector server on which this connector will be available.

   c. Click OK.

      The new bundle appears in the Bundles list.

9. Find the main connector bundle in the Bundles list, then right-click its name in the list and choose Refresh Imports from the popup menu.

The Peoplesoft connector is now ready to be used.

## Import and Build the CA-USER Component Interface

Due to a limitation of only 300 records being returned in a search in the PeopleSoft Component Interface API, a new Component Interface has been created that allows all records to be returned at once during a search operation. The CA-USER Component Interface must be imported by the administrator to the PeopleSoft application server using the following procedure.

**Follow these steps:**

1. Extract the CA_USER folder from CA IAM CS resource directory to a location on or accessible to the PeopleSoft application server.
2. Open the Application Designer, log into the appropriate database, and select Tools>Copy Project>From File, browse to the CA_USER folder and select the CA_USER Project.

   **Notes:**

   - When extracting, make sure that the folder name does not change and that it contains only the CA_USER.ini and CA_USER.xml files.
   - Make sure that the versions are compatible. For example, import an 8.48 project file into an 8.48 PeopleSoft installation and not an 8.49 one.
   - If this is not the first time you are importing this project, select to Use Project Definition from File to overwrite the existing project.
3. Select All Definition Types and click Copy
4. Build the project by selecting Build > Project…

   **Note:** If the PeopleSoft installation has multiple databases, steps 1 to 3 must be repeated for each database.

## Update PeopleSoft Permissions

Permissions must be set correctly for the user profile used to acquire and manage the PPS endpoint. The minimum permissions needed for the user who acquires the PPS endpoint is to be assigned the Security Administrator role or its equivalent. By default, this role contains the Security Administrator Permission List (PTPT1100)

The permissions can be set in one of two ways:

- Running the SQL script
- Manually adding and setting access permissions for each of the required interfaces.

## Running the SQL Script

**Note:** The SQL script supplied with the Connector has been tested on PeopleSoft with a SQL Server database. For databases other than SQL Server, it may be necessary to use the second method.

The script assumes a database name of PTSYS. If PeopleSoft is using a database with a name other then PTSYS, you must edit the script and replace all instances of PTSYS with the name being used. If the PeopleSoft installation has multiple databases, the script should be run on all databases.

To run the SQL script:

1. Copy the following file to a location on or accessible to the PeopleSoft Application Server:

   *CS_HOME*`\resource\pps\setperms.sql`

2. Open the Microsoft SQL Server Query Analyzer and select File > Open...
3. Browse to the directory where setperms.sql file is located, and select this file.
4. Select Query > Execute to run the script.

   The Connector has been configured and is ready to use.

## Manually Add and Set Permissions

To manually add and set permissions, follow this procedure.

From the PeopleSoft Web GUI

1. Select PeopleTools, Security, Permissions & Roles, Permission Lists
2. Search for and select the PTPT1100 Permission List
3. Go to the Component Interfaces page and select (or add) the CA_ALIASATTR Component Interface.
4. Select Edit and set all methods to "Full Access".
5. Click OK.

   Repeat steps 4 and 5 for all component interfaces that start with CA_, and also for DELETE_ROLE and DELETE_USER_PROFILE

6. Click Save.

   The Connector has been configured and is ready to use.

# Connector-Specific Features

This section details your connector's specific management features, such as how to acquire and explore your endpoint. Also included are account, provisioning roles, account template, and group information specifically for your connector.

## Acquire a PeopleSoft Machine Using the User Console

You must acquire the PeopleSoft machine before you can administer it with CA IdentityMinder.

**To acquire a PeopleSoft machine using the User Console**

1. Select Endpoints, Manage Endpoints,Create Endpoint
2. Select PeopleSoft from the drop-down list box on Create a new endpoint of Endpoint Type, and click Ok

   Use the Create PeopleSoft Endpoint page to register a PeopleSoft machine. During the registration process, CA IdentityMinder identifies the PeopleSoft machine you want to administer and gathers information about it.
3. After entering the required information, click Submit.

   You are now ready to explore and Correlate the endpoint.
4. Click Endpoints, Explore and Correlate Definitions, Create Explore and Correlate Definition to explore the objects that exist on the endpoint.

   The Exploration process finds all PeopleSoft accounts and groups. You can correlate the accounts with global users at this time or you can correlate them later.
5. Click OK to start a new definition.
6. Complete the Explore and Correlate Tab as follows:

   a. Fill in Explore and Correlate name with any meaningful name.

      Click Select Container/Endpoint/Explore Method to click a PeopleSoft endpoint to explore.

   b. Click the Explore/Correlate Actions to perform:

      - **Explore directory for managed objects**—Finds objects that are stored on the endpoint and not in the provisioning directory.
      - **Correlate accounts to users**—Correlates the objects that were found in the explore function with users in the provisioning directory. If the user is found, the object is correlated with the user. However, you can instead select that you want to assign the account to the existing user (the default user) or create the user.
      - **Update user fields**—If a mapping exists between the object fields and the user fields, the user fields are updated with data from the objects fields.

7. Complete the Recurrence tab if you want to schedule when the task to executes.

   a. Click Schedule.

   b. Complete the fields to determine when this task should execute.

      You may prefer to schedule the task to execute overnight to interfere less with routine access of the system.

   **Note**: This operation requires the client browser to be in the same time zone as the server. For example, if the client time is 10:00 PM on Tuesday when the server time is 7:00 AM, the Explore and Correlate definition will not work.

8. Click Submit.

**To use an explore and correlate definition**

1. In a CA IdentityMinder environment, click Endpoints, Execute Explore and Correlate.
2. Click an explore and correlate definition to execute.
3. Click Submit.

   The user accounts that exist on the endpoint are created or updated in CA IdentityMinder based on the explore and correlate definition you created.

## Acquire the PeopleSoft Machine Using the Provisioning Manager

You must acquire the PeopleSoft machine before you can administer it with CA IdentityMinder. When acquiring a PeopleSoft machine, perform the following steps.

**From the Endpoint type task view:**

1. Register the PeopleSoft machine as an endpoint in Provisioning Manager.

   Use the PeopleSoft Endpoint property sheet to register a PeopleSoft endpoint. From the PeopleSoft Endpoint tab, you must specify the Directory Name, Host Name of the application server, Jolt port number, PeopleSoft Username and password.

   Two additional attributes are provided on this tab. The Connection Timeout field specifies the amount of time that the connector must receive a response from PeopleSoft, due to a connection request, before considering that the request has failed. The Number of Retries field specifies the number of times a User Profile transaction will be repeated if the transaction failed due to PeopleSoft database deadlock errors.

   During the registration process, CA IdentityMinder identifies the PeopleSoft machine you want to administer and gathers information about it.

2. Explore the objects that exist on the endpoint.

   After registering the machine in CA IdentityMinder, you can explore its contents. Use the Explore and Correlate Endpoint dialog to explore PeopleSoft user profiles, roles, and permission lists. The Exploration process finds all PeopleSoft user profiles, roles, or permission lists. You can correlate the user profiles with global users at this time, or you can wait to correlate them.

3. Correlate the explored user profiles with global users.

   When you correlate user profiles, CA IdentityMinder creates or links the user profiles on an endpoint with global users, as follows:

   a. CA IdentityMinder attempts to match the username with each existing global user name. If a match is found, CA IdentityMinder associates the PeopleSoft user profile with the global user. If a match is not found, CA IdentityMinder performs the next step.

   b. If the Create Global Users as Needed button is checked, CA IdentityMinder creates a new global user and associates the PeopleSoft user profile with the global user. If the Create Global Users as Needed button is unchecked, then CA IdentityMinder performs the next step.

   c. CA IdentityMinder associates the PeopleSoft user profile with the [default user] object.

## PeopleSoft Accounts

PeopleSoft user profiles are the same as accounts for the PeopleSoft connector.

Accounts give users access to the resources on a directory. You can manage accounts from the Namespace task view. Use the PPS User property sheet when managing your accounts.

## PeopleSoft User Profiles Management

The PPS Connector can acquire the PeopleSoft endpoint and its existing User Profile objects. To manage,create, and delete user profiles, use the PeopleSoft User property sheet. There are six tabs available on the property sheet:

- Profile
- General Properties
- Emails
- ID
- Roles
- Workflow

## PeopleSoft User Profile Tab

The Profile tab displays the user name of the managed PeopleSoft user profile.

## PeopleSoft User General Properties Tab

The General Properties tab specifies general user attributes, login information, and permission lists.

From this tab you can lock and unlock user profiles on the account and modify existing passwords. Click here (see page 388) for the procedure on locking and unlocking user profiles and here (see page 389) for the procedure for modifying passwords.

This tab also contains several attributes that can be modified by clicking on the ellipsis (...) button. After clicking this button, a new dialog (Select Dialog) is opened where you can select from a list of PeopleSoft objects, an entry for that attribute.

## Lock/Unlock User Profiles

User profiles may be locked and unlocked by setting the associated global user's suspension state and synchronizing the change with the account.

## Modifying Passwords

Passwords can be changed directly on the account or by synchronizing with a change on the associated global user.

To modify the password, user this procedure:

**From the General Properties tab of the PeopleSoft User property sheet**

1. Change the password of the user
2. Confirm the new password.
3. Synchronize the change with the associated accounts and ensure the password change is successful.

## Emails Tab

The Emails tab lets you select the primary email address and type for a user profile.

The fields in this tab are listed below:

**Email Addresses List Box**

Lists the email addresses, types, and if the address is the primary address.

**Type**

Specifies the email address type. From the drop-down menu, you can select one of the following:

- Blackberry
- Business
- Home
- Other
- Work

**Primary Check Box**

Check this box, if the specified email address is to be the primary address.

**Address**

Specifies the valid email address.

**Add Button**

Click this button after specifying the email address and type, to add to the Email Addresses list box.

**Modify Button**

After selecting an email address from the Email Addresses list box, click this button to modify.

**Remove Button**

After selecting an email address from the Email Addresses list box, click this button to remove.

Click here (see page 390) for the rules regarding email addresses for this connector.

## Rules for Email Addresses

Both the connector and the Provisioning Manager will enforce the following rules regarding email addresses:

- There should always be a Primary email address.
- There can only be one Primary email address.
- There should be only one Email Address per Type.

## PeopleSoft User ID Tab

The ID tab lets you add (see page 391), modify (see page 391), and delete (see page 391) PeopleSoft ID types and attributes. The left-hand side of the tab displays all set ID types and attribute values. The right-hand side of the tab is the selection and entry area.

## Add an ID Type and Value

To add a new ID Type to the set ID Types and Values list, follow this procedure.

**From the right-hand side of the ID tab**

1. Select the ID Type selected button (...).

   The Select ID Type dialog opens.

2. Select and ID Type and click OK.

   Once an ID Type is selected, the Attributes table is populated with available attributes for the specified ID Type.

   Click Add.

3. Select an attribute and click attribute selected button (….).to choose a new attribute value, or click Clear button to remove existing value

   If attribute selection button is selected, the Select Attributes dialog opens.

4. Select a value for the attribute and click OK.
5. Click Apply/OK to add the ID Type and Value.

## Modify and ID Type and Value

To modify a set ID Type and Value, follow this procedure.

**From the left-hand side of the ID tab**

1. Select the ID Type and Value to modify.

   The right-hand side of the tab is populated with the set values.

2. Select an Attribute from the Attributes list box and click attribute selected button (...).

   The Select Attributes dialog opens.

3. Select a value for the attribute and click OK.
4. Click Apply/OK to save the changes.

## Delete an ID Type and Value

To delete and ID Type and Value, select the ID Type on the left-hand side of the ID tab and click Delete.

## PeopleSoft User Roles Tab

The Roles tab specifies role details such as, role name and route control.

## PeopleSoft User Workflow Tab

The Workflow tab displays PeopleSoft Workflow attributes such as, Alternate User ID, routing preferences, and supervising User ID.

## PeopleSoft Permission Lists Management

The PPS connector lets you create, manage, and delete PeopleSoft permission lists. To create and manage permission lists, use the PeopleSoft Permission Lists property sheet. There are 17 tabs available on the property to manage permission lists:

- General
- Mobile Pages
- People Tools
- Process Group Permissions
- Process Profile Permissions
- Sign-On Times
- Component Interface
- Web Libraries
- Personalizations
- Query Access Group Permissions
- Query Profile
- Mass Change
- Menu Pages
- Web Services
- Object Permissions
- Tools Permissions
- Miscellaneous Permissions

## Permission Lists General Tab

The General tab lets you set general or miscellaneous attributes and PeopleSoft system defaults.

## Permission Lists Mobile Pages Tab

The Mobile Pages tab lets you set which PeopleSoft Pages a user can access.

## Permission Lists Menu Pages Tab

The Pages tab lets you set which PeopleSoft menus a user can access.

## Permission Lists People Tools Tab

The PeopleTools tab lets you specify access to stand-alone PeopleTools applications. These applications refer to Microsoft Windows programs not developed using PeopleSoft Application Designer.

## Permission Lists Object Permissions Tab

The Object Permissions tab lets you manage access permissions for PeopleSoft objects. Properties in this tab depend on the the Application Designer Access property.

## Permission Lists Tools Permissions Tab

The Tools Permissions tab lets you manage access permissions for PeopleSoft tools. Properties in this tab depend on the Application Designer Access property.

## Permission Lists Miscellaneous Permissions Tab

The Miscellaneous Permissions tab lets you manage access permissions for PeopleSoft objects. Properties in this tab depend on the Application Designer Access property.

## Permission Lists Process Tabs

The Process tabs let you specify batch and online processes that you can invoke through PeopleSoft Process Scheduler.

There are two Process tabs:

- Process Group Permissions
- Process Profile Permissions

## Permission Lists Sign-on Times Tab

The Sign-on Times tab lets you set day and time access restrictions.

## Permission Lists Component Interfaces Tab

The Component Interfaces tab lets you set access to Component Interfaces.

## Permission Lists Web Libraries Tab

The Web Libraries tab lets you set the access to Web Libraries.

## Permission Lists Personalizations Tab

The Personalizations tab lets you set user preferences.

## Permission Lists Query Tabs

The Query tabs let you define the records that a user can have access to in PeopleSoft Query, and defines the query operations that a user can perform.

There are two Query tabs:

- Query Access Group Permissions Tab
- Query Profile Tab

## Permission Lists Mass Change Tab

The Mass Change tab lets you set mass change operator security controls and template permissions.

## Permission Lists Web Services Tab

The Web Services tab lets you set the access to Web Services.

## PeopleSoft Roles Management

The PPS Connector lets you create, manage, and delete PeopleSoft Roles. Using the PeopleSoft Role property sheet, you can assign permissions to roles and assign roles to users. There are seven tabs available for this property sheet to manage PeopleSoft roles:

- General
- Permission Lists
- Members
- Dynamic Members
- Workflow
- Roles Grant

## PeopleSoft Role General Tab

The General tab specifies general information, such as role name and description, about the role.

## PeopleSoft Role Permission Lists Tab

The Permission Lists tab lets you assign and remove permissions to a role.

## PeopleSoft Role Members Tab

The Members tab show the users who have been statically assigned this role.

## PeopleSoft Role Dynamic Members Tab

The Dynamic Members tab lets you set rules to invoke to assign roles to members.

## Peoplesoft Role Workflow Tab

The Workflow tab lets you set routing options.

## PeopleSoft Role Role Grantors  Tab

The Role Grantors tab lets you assign limited security administration to specified users.

## PeopleSoft Role Role Grantees Tab

The Role Grantees tab lets you assign limited security administration to specified users.

## PeopleSoft Account Templates

The PPSDefaultPolicy, provided with the PeopleSoft connector, gives a user the minimum security level needed to access an endpoint. You can use it as a model to create new account templates.

The PeopleSoft Account Template property sheet contains the Profile and Properties tabs where you can view the User Name, Description, Symbolic ID, and Locked attributes for each account template.

## PeopleSoft Conventions

Use the following PeopleSoft conventions in your etautil commands:

- The namespace name (eTNamespaceName) is PeopleSoft.
- The namespace prefix is PPS. Therefore, the PeopleSoft class names are the following:
  - eTPPSDirectory for a PeopleSoft directory
  - eTPPSUserContainer for a PeopleSoft user profile container
  - eTPPSUser for a PeopleSoft user profile
  - eTPPSPolicyContainer for a PeopleSoft policy container
  - eTPPSPolicy for a PeopleSoft policy

# RACF Connector

The Resource Access Control Facility (RACF) Connector lets you administer accounts, groups, and resources on RACF systems and provides a single point for all user administration by letting you do the following:

- Register endpoints, explore them for objects to manage, and correlate their accounts with global users
- Create and manage RACF accounts using RACF-specific account templates
- Change account passwords and account activations in one place
- Synchronize global users with their provisioning roles or synchronize global users' accounts with their account templates
- Assign RACF account templates to each of your RACF endpoints
- Use the default endpoint type account template to create accounts with the minimum level of security needed to access a RACF endpoint
- Create and manage RACF groups and permissions
- Generate and print reports about RACF accounts

## How to Configure Your RACF System

Once the RACF connector has been installed with the Provisioning Server, you must configure your system to communicate with the connector.

**To configure your RACF system**

1. Install the CA LDAP Server for z/OS on your RACF system.
2. Review the CA LDAP Server for z/OS configuration options.

## Step 1. Install the CA LDAP Server for z/OS

The CA LDAP Server for z/OS provides the communication mechanism for this CA IdentityMinder Connector.  This product is a free offering from CA and can be downloaded from support.ca.com.  Once downloaded, refer to the *CA LDAP Server for z/OS Installation Guid*e for information and instructions on how to install it.

**Note:** The following steps are required to migrate from a previous version to r12.6.1:

1. The CA LDAP Server for z/OS must be installed on at least one mainframe system and configured to communicate to every z/OS system being managed by CA IdentityMinder or alternatively, you can install it on every z/OS system managed by CA IdentityMinder.
2. The CA LDAP Server(s) must be configured to have an endpoint entry in Provisioning Manager naming mode for each system. For more information on configuring, see the *CA LDAP Server for z/OS Administrator Guide*.
3. After upgrading, you must update each endpoint and update the information within the Mainframe LDAP Server section. This information matches up with the IP Address, Port, and suffix of the mainframe LDAP Server.

The existing eTrust_RAC.conf file must be removed from the eTrust_Admin.conf file, or alternatively, remove the contents from the file and make blank.

## Step 2. Review the CA LDAP Server

Once all CA LDAP Server installation steps have been completed and your CA LDAP Server is started, it will be ready to support administration for the CA IdentityMinder RACF Connector.  However, you may need or want to setup additional configuration options for the CA LDAP Server in order to provide additional functionality for the RACF Connector. For more information on all available configuration options, see the chapter titled "RACF_ETA Backend" of the *CA LDAP Server for z/OS Administrator Guide*.

# Securing Provisioning Server Communication to the CA LDAP Server

All communication between the Provisioning Server and the CA LDAP Server for z/OS can be encrypted using SSL (Secure Socket Layers).

**To establish communication**

- Setup your CA LDAP Server for z/OS to use the Server Mode for SSL connections. For information on how to configure this, see the chapter titled, "CA LDAP Server Using Digital Certificates", in the *CA LDAP Server for z/OS Administrator Guide*.
- Turn on SSL support within the Provisioning Server for your RACF endpoint. To do this, bring up the properties of your RACF endpoint using the Provisioning Manager. In the section entitled 'Mainframe LDAP Server Information', enable the check box entitled 'Use Server-side SSL' and click Apply. Now, all communication to the configured CA LDAP Server will attempt to use an SSL connection, and will fail and provide an appropriate error message if SSL cannot be established.

# RACF Support for FIPS and IPv6

For this release of CA IdentityMinder, the RACF Connector supports IPv6 but not FIPS.

# Connector-Specific Features

This section details your connector's specific management features, such as how to acquire and explore your endpoint. Also included are account, provisioning roles, account template, and group information specifically for your connector.

## Acquire a RACF System Using the User Console

You must acquire a RACF system before you can administer it with CA IdentityMinder.

**To acquire an RACF system using the User Console**

1. Select Endpoints, Manage Endpoints,Create Endpoint
2. Select RACF from the drop-down list box on Create a new endpoint of Endpoint Type, and click Ok

   Use the Create RACF Endpoint page to register a RACF system. During the registration process, CA IdentityMinder identifies the RACF system you want to administer and gathers information about it.
3. After entering the required information, click Submit.

   You are now ready to explore and Correlate the endpoint.

4. Click Endpoints, Explore and Correlate Definitions, Create Explore and Correlate Definition to explore the objects that exist on the endpoint.

   The Exploration process finds all RACF accounts and groups. You can correlate the accounts with global users at this time or you can correlate them later.

5. Click OK to start a new definition.

6. Complete the Explore and Correlate Tab as follows:

   a. Fill in Explore and Correlate name with any meaningful name.

      Click Select Container/Endpoint/Explore Method to click a RACF endpoint to explore.

   b. Click the Explore/Correlate Actions to perform:

      - **Explore directory for managed objects**—Finds objects that are stored on the endpoint and not in the provisioning directory.
      - **Correlate accounts to users**—Correlates the objects that were found in the explore function with users in the provisioning directory. If the user is found, the object is correlated with the user. However, you can instead select that you want to assign the account to the existing user (the default user) or create the user.
      - **Update user fields**—If a mapping exists between the object fields and the user fields, the user fields are updated with data from the objects fields.

7. Complete the Recurrence tab if you want to schedule when the task to executes.

   a. Click Schedule.

   b. Complete the fields to determine when this task should execute.

      You may prefer to schedule the task to execute overnight to interfere less with routine access of the system.

   **Note**: This operation requires the client browser to be in the same time zone as the server. For example, if the client time is 10:00 PM on Tuesday when the server time is 7:00 AM, the Explore and Correlate definition will not work.

8. Click Submit.

**To use an explore and correlate definition**

1. In a CA IdentityMinder environment, click Endpoints, Execute Explore and Correlate.

2. Click an explore and correlate definition to execute.

3. Click Submit.

   The user accounts that exist on the endpoint are created or updated in CA IdentityMinder based on the explore and correlate definition you created.

## Acquire a RACF System Using the Provisioning Manager

Acquiring an endpoint is the first task you must perform before you can administer a RACF system. When acquiring an endpoint, perform this procedure.

**From the Endpoint type task view**

1. Register the server as an endpoint in CA IdentityMinder. This phase is performed by adding a new endpoint under the RACF Endpoint type in CA IdentityMinder.

   Use the RACF Endpoint property sheet to view or customize a RACF system. During the registration process, CA IdentityMinder identifies the RACF system you want to administer and gathers information about it.

2. Explore the objects that exist on the endpoint.

   After registering the server in CA IdentityMinder, you can explore its contents. Use the Explore and Correlate Endpoint dialog. The Exploration process finds all RACF accounts, groups, and permissions. You can correlate the accounts with global users at this time or you can correlate them later.

3. Correlate the explored accounts with global users.

   When you correlate accounts, CA IdentityMinder creates or links the accounts on an endpoint with global users, as follows:

   a. CA IdentityMinder attempts to match the user ID with each existing global user name. If a match is found, CA IdentityMinder associates the RACF account with the global user. If a match is not found, CA IdentityMinder performs the next step.

   b. CA IdentityMinder attempts to match the user ID with each existing global user's full name. If a match is found, CA IdentityMinder associates the RACF account with the global user. If a match is not found, CA IdentityMinder performs the next step.

   c. If the Create Global Users as Needed button is checked, CA IdentityMinder creates a new global user and then associates the RACF account with the global user. If the Create Global Users as Needed button is unchecked, CA IdentityMinder performs the next step.

   d. CA IdentityMinder associates the RACF account with the [default user] object.

## Register RACF Endpoints on Windows Machines

To register RACF endpoints on a Windows system, perform this procedure.

**From the Endpoint task view**

1. Select RACF Endpoint from Object Type
2. Click the New button. You will be required to fill in the following information:
   - **Endpoint Name** specifies a name to refer to the new RACF endpoint.
   - **Mainframe LDAP IP Address/Machine Name** specifies the IP address or machine name of the RACF managed system where the CA LDAP Server is configured and running.
   - **Mainframe LDAP Port** specifies the port number that you specified during the CA LDAP Server for z/OS install. If you are not sure of the Mainframe LDAP Port, see the section "Checking your CA LDAP Server for z/OS Configuration Information".
   - **Mainframe LDAP Suffix** specifies the suffix to use for this endpoint. This combo box is automatically populated with all valid and available suffixes when you click the "Get Suffixes" button. Suffixes can be retrieved once valid values have been provided for the Mainframe IP Address/Machine Name and Mainframe LDAP Port fields.

     **Note:** If, after clicking "Get Suffixes", there are no suffixes showing, you are either pointing to the wrong CA LDAP Server or the CA LDAP Server is not configured for use by CA IdentityMinder.
   - **Admin User** specifies the RACF Userid of an administrator to be used from within CA IdentityMinder to manage the RACF system.
   - **Password** specifies the password of the RACF Userid above.
   - **Confirm Password** specifies the same password as above for confirmation.

**Note:** After you click OK, the Provisioning Server attempts to establish a connection with the CA LDAP Server for z/OS at the IP address and port supplied, as well as, validating the Admin user and Password values supplied. An appropriate error message is displayed if this connection fails.A Global User is inserted in the Provisioning Server with Domain Administrator authority using the ID and password supplied. This Global User should now be used to administer this RACF endpoint.

## Register RACF Endpoints on Solaris Machines

To register IBM RACF endpoints on a Solaris machine, use the batch utility, etautil, to define a RACF endpoint by specifying a directoryName, Mainframe LDAP IPAddress, Port, and Suffix. For example,

```
etautil -u USERID -p PASSWORD add 'eTNamespaceName=RACF,dc=DOMAIN,dc=eta'
eTRACDirectory name='DIRECTORYNAME' eTZOSLDAPIPAddress=IPADDRESS
eTZOSLDAPPort=PORT eTZOSLDAPSuffix=SUFFIX
```

where,

**DIRECTORYNAME**

Specifies the name you desire for this endpoint.

**IPADDRESS**

Specifies the IP Address or Machine name of the RACF system where your CA LDAP Server for z/OS is running.

**PORT**

Specifies the port number the CA LDAP Server is using,

**SUFFIX**

Specifies a valid suffix configured for this CA LDAP Server operating in im naming mode. (See, "Chapter 3: Configuration Options", in the *CA LDAP Server for z/OS Administrator's Guide* for information on the naming_mode option.)

## Checking Your CA LDAP Server for z/OS Configuration Information

To view all pertinent information regarding your CA LDAP Server and its configuration, issue a STATUS command from the mainframe console where your CA LDAP Server is running.  The STATUS command provides information, such as version information, port number, configured databases, and suffixes.  For more information on the STATUS command, see "Chapter 2: Startup Options" section, "Console Interface" in the *CA LDAP Server for z/OS Administrator Guide*.

## RACF Provisioning Roles and Account Templates

The RACF Default Policy, provided with the RACF Connector, gives a user the minimum security level needed to access an endpoint. You can use it as a model to create new account templates.

## Endpoint Groups Cannot be Removed from an Account Template

If a RACF endpoint has been deleted from CA IdentityMinder, the associated endpoint groups can not be removed from the account templates.

## RACF Accounts

When synchronizing RACF accounts, strong synchronization is always the default.

## RACF Groups

Groups allow users to share common access to the resources on an endpoint.

Like the UNIX file, unix/etc/group, a RACF user can belong to many groups on the RACF system but is defined to one primary group called the Default Group. In CA IdentityMinder, all groups, including the Default Group, appear as provisioning roles in the browser. In CA IdentityMinder, all groups, including the Default Group, appear as provisioning roles in the browser.

By default, RACF systems use a root group called SYS1. This root is defined as the user's default group if no other group is specified. The user's account appears under the role (default group), but the user also appears under each group that the user is defined to.

You can create and maintain RACF groups using the Endpoint type task view. Use the RACF Group property sheet when managing your groups.

## Set the Ownership of Associations between Users and Groups

The association between a user and a group has an owner.

When you use RACF to create this association, the group owns the association.

When you use CA IdentityMinder to create the association, you can set the association owner to be the group or the administrative user.

In previous releases, the association owner was always set to be the administrative user.

**Follow these steps:**

1. Create a RACF endpoint.
2. To make the group own associations between users and the group, select the Set Connect Group Ownership checkbox.
3. To make the administrative user own the associations, leave the checkbox unselected.

## TSO Alias Support

The RACF connector also supports the creation of a TSO Alias when a user is created or modified with TSO access being granted. The alias value is always the value of the RACF Account being created or modified. To enable this support, see the chapter titled, "RACF_ETA Backend" in the *CA LDAP Server for z/OS Administrator Guide* for more information.

## Permissions

Permissions are *resources* in RACF. You can view permissions from any RACF account or endpoint. You can create and maintain RACF permissions using the Endpoint type task view. Use the RACF Permission property sheet when managing your permissions.

**Note:** The following permission classes are **not** supported by the RACF connector: DIGTCERT, DIGTRING, and DIGTNMAP.

## RACF Program Exits

The RACF connector supports the use of Program Exits which are incorporated as 'Common Exits'. Program Exits provide you with the capability to perform certain actions before or after an account is created, modified or deleted from CA IdentityMinder. These exits can be referenced either on the Endpoint property page to execute custom code on a single endpoint, or on the Account Template property page to execute custom code on multiple endpoints. Actions might include native CA DSI Server for z/OS (CA Distributed Security Integration) or CA LDAP Server for z/OS commands in order to modify account privileges or access to resources on the RACF system.

To see a sample program exit, refer to the OS390 subdirectory under the CA IdentityMinder Templates directory.

For more detailed information about how to write program exits, see the Programming Guide for Provisioning.

**Note:** If you are upgrading from a previous release and use exits, those exits should be reviewed. There is the potential that by using CA LDAP Server for z/OS-specific configuration options, you can remove existing exits. Even if the exits cannot be removed completely, the number of operations they need to perform, might be reduced. A detailed review of the exits will let you determine if they can or should be recoded to use the CA LDAP Server instead of the CA DSI Server. While this is not required, if possible, exits should be migrated to use the CA LDAP Server.

## RACF Conventions

Use the following RACF conventions in your etautil commands:

- The endpoint type name (eTNamespaceName) is RAC endpoint type
- The endpoint type prefix is RAC. Therefore, the RACF class names are:
  - eTRACDirectory for an endpoint
  - eTRACPolicyContainerName for an account template container
  - eTRACPolicy for an account template

## Proxy Configuration

The RACF Endpoint page contains a section where clients can configure a Proxy administrative ID and password to be used for user password changes from the SAWI. When configured, this ID and password is used to issue the password change request for the SAWI user to change their password. This is helpful and needed if a SAWI user cannot supply a password (for example, the password is forgotten) or their password is expired and RACF and they cannot be authenticated. When using a proxy administrative ID, standard RACF security rules apply (for example, scoping) and password syntax checking specified in the RACF System Options Password field is enforced.

**Note:** The check boxes on the Endpoints Setting tab are for legacy purposes only. You can perform proxy configuration and administration support from the Self-Service interface.

## Proxy Administration Support

You can configure a proxy ID for all tasks accomplished within CA IdentityMinder. Previously, a proxy ID could only be configured for use with requests generated from the SAWI interface. This proxy ID is maintained on the main Endpoint page in the Proxy Administration Configuration section. The proxy ID can be used for any type of CA IdentityMinder request against supported objects, and for any CA IdentityMinder Administrator that is logged on.

**Note:** The enhancement is only recommended to use after careful consideration (and preparation) of the following consequences:

1. Any Global User (with the proper privileges provided within CA IdentityMinder) is able to administer RACF Userids, Groups, and Permissions under the configured proxy ID. Any mainframe security product scoping is lost; only the scoping of the proxy ID is enforced.
2. As mentioned above, security settings are now the only point of enforcement against a Global User manipulating mainframe security data.
3. Any reports or auditing methods against administration of your mainframe security data that originate from the mainframe is now compromised; the only ID that shows up for any administration that occurred from CA IdentityMinder is the configured proxy ID.

4. If the proxy ID's password changes on the mainframe, the password must be changed on every Endpoint Page within the Provisioning Manager that it is configured for.

By default, the Connector operates in the same mode as in past releases; the logged-on Global User and their password are used for submitting any requests destined to the mainframe security product. The common endpoint page entitled Endpoint Settings provides two checkbox controls under the description Administrator Credentials that control the three possible settings:

**Use logged-in Administrator's credentials**

Default setting. Indicates that the logged-in Administrator (Global User) is used as the credentials for ALL requests, even from the SAWI.

**Use proxy for SAWI changes**

Indicates that the logged-in Administrator (Global User) is used as the credentials for all requests EXCEPT for requests from the SAWI interface. The proxy ID credentials (if available) are used for requests coming from the SAWI interface.

**Use proxy for ALL requests**

When no checkbox is checked, this indicates that the proxy ID credentials (if available) are to be used for ALL requests.

When any request occurs from CA IdentityMinder, these settings are checked against the endpoint where the request is targeted. If, based on the endpoint settings and the type of request (SAWI or otherwise), proxy credentials are to be used, the credentials that are defined for that endpoint are retrieved and used for the request. In the case where endpoint credentials are supposed to be used, but no credentials exist (either Proxy ID or password contains no value), the proxy credentials are not used for the request and the request proceeds using the logged-in Administrator (Global User) credentials.

**Note:** Proxy IDs must be what are referred to as 'logon-able' user IDs.  That means they must be 7 bytes in length or less.  8 byte user IDs are no longer valid.

**Note:** The check boxes on this tab are for legacy purposes only. You can perform proxy configuration and administration support from the Self-Service interface.

## Logging

To view logging information regarding credential lookups, enable logging for the endpoint on the Logging endpoint page and enable the eTrust log Connector, specifying all logging levels. This provides all endpoint credential lookup information (successes and failures) into the standard eTrust log.

## Extend the Schema to Include Custom Attributes

When you connect to a RACF system through CA IAM CS, you can correlate on any of the attributes are exposed by the connector. If you want to correlate on an attribute that the connector does not expose, you can extend the connector's schema to include up to twenty extra attributes.

To set up these extra attributes:

1. Create a mapping file that maps each attribute on the endpoint to an attribute in CA IdentityMinder (see page 407).

   This includes the custom attributes in the Provisioning Server.

2. Add the custom attributes to a new tab in the User Console (see page 409).

## Create a Mapping File for the Custom Attributes

The mapping file lists the custom attributes.

**Note:** This section refers to the Provisioning Server installation location as *ps_install*. By default, *ps_install* is in the following locations:

- **Windows**—C:\Program Files (x86)\CA\Identity Manager\Provisioning Server
- **Linux and Solaris**—/opt/CA/IdentityManager/ProvisioningServer/

**Follow these steps:**

1. Create a new directory in *ps_install*\data, and name the new directory *RAC*.
2. Create a text file named schema_map.txt and save it in *ps_install*\data\RAC.
3. In the text file, create entries with the format described in Format of the Mapping File for Custom Attributes (see page 408).
4. Restart the Provisioning Server service.

The Provisioning Server now includes the custom attributes.

## Format of the Mapping File for Custom Attributes

The mapping file contains a list of the custom attributes, each with the following format:

```
eTRACCustomAttribute001=attribute1
eTRACCustomAttribute002=attribute2
…
eTRACCustomAttribute020=attribute20
```

In this list, the names on the left are the attributes in CA IdentityMinder and the names on the right are the attributes on the endpoint.

Each custom attribute in CA IdentityMinder is named eTRACCustomAttributeNNN, where NNN is a number from 001 to 020. You can use these names in any order, but we recommend that you start with eTRACCustomAttribute001, to avoid confusion.

There must be no spaces before or after each attribute name.

The attribute names are case-sensitive.

On Solaris, make sure the mapping file is world-readable (its permission should be at least 444).

## Add the Custom Attributes to a Tab in the User Console

You can include the custom attributes in a tab in the User Console.

**Follow these steps:**

1. Log in to the User Console as a user with administrative rights.
2. Click the Roles and Tasks tab, then click Admin Tasks, Manage Admin Tasks.
3. Search for *RACF*.
4. Click on the name of the screen that you want to change, for example *Modify RACF Account*.
5. Select Tabs.
6. Find Custom Attributes in the table, and click its Edit button.
7. Select the Browse button beside the Screen field.
8. Select “Modify RACF Account – Custom Attributes”. Click Copy.
9. Give the new screen a unique name by editing the Name and Tag values.
10. Delete any Custom Attribute fields that should not appear on the final screen.
11. For each custom attribute, change its name to the actual attribute name on the endpoint:
    a. Click the attribute's Edit icon.
    b. Edit the Name to show the attribute's real name on the endpoint. This will appear on the final screen
    c. Edit the Tag to be unique. This is usually the same as the Name, but with no spaces.
12. Click OK.
13. Click Select.
14. Click OK, then click Submit.

The new tab is now available in the User Console.

## Cannot Create Account When Password Policies Conflict

This section applies to all connectors. However, it is most likely to be relevant to the mainframe connectors.

**Symptom:**

In many organizations, some endpoints (such as the mainframe systems) have stricter restrictions on passwords than the corporate password policy.

This conflict causes problems if you create a password that meets the requirements of the CA IdentityMinder password policy but is invalid on an endpoint. In this situation, the following problems can occur:

- When you use a provisioning role to create an endpoint account for an existing global user with such a password, the account is not created.
- When you attempt to create a new user with a temporary password, the user is not created.
- When you change the password of an existing account on the endpoint, the changed password is not saved.

**Solution:**

To avoid this problem, make one or both of the following changes:

- Make the password policy in CA IdentityMinder more restrictive than the password policy on the mainframe endpoint.
- Make the policy for temporary passwords more restrictive than the password policy on the mainframe endpoint.

  This change forces new users to change their password when they log in to User Console.

# RSA ACE (SecurID) Connector

The RSA ACE (SecurID) Connector lets you administer the users, groups of users, and tokens of RSA ACE/Server machines and provides a single point for all user administration by letting you do the following:

- Retrieve the existing users from the RSA ACE/Server database
- Display, create, modify, or delete a user
- Assign or un-assign a token to a user
- Create remote users
- Add or remove users on an Agent Host
- Add or remove a user to a group
- Retrieve existing groups from the ACE/Server repository
- Create and delete groups
- Enable or disable a group on an Agent Host
- Retrieve a token's details
- Active operations on a token

## RSA Installation

This connector is managed using the Connector and agent installation process. For more information and requirements, click here.

This connector can also be managed using the Connector and C++ Server installation process as well.

The following sections detail the post installation and configuring requirements for this connector.

## RSA Post Installation Requirements

The following must be done after the connector installation:

- The user named SYSTEM must be added to the Primary RSA ACE/Server and registered as an Administrator.
- CAM CAFT service must be configured on the Primary RSA/ACE Server. For more information, see the following section.
- The RSA Authentication Manager 5.x and higher Administration Toolkit must be installed on the Primary RSA ACE/Server. For token management, the 6.1 Administration Toolkit is required.
- If you plan to install the RSA remote agent on Solaris 8 or 9, you may be required to tune certain kernel parameters if the values are set lower than required. If this is necessary you are notified by an error message during the install. For further details, refer to the readme_install.txt file, found in:

  ```
  /<install path>/RemoteAgent/RSA/solaris/ecs-installation"
  ```

## RSA Limitations

For this release, the following limitations should be considered when using the RSA Connector:

- If the PIN change option is selected for an eTPassword change event propagation, only numeric values for the password change event will be accepted regardless of the PIN options settings specified in the System Parameters of the RSA ACE/Server Administration Tool. This limitation is due to handling of the PIN change by RSA Administration Toolkit function Sd_SetPin(). This restriction is also imposed by the type of the devices (like RSA SecurID PINPAD Token) that are not allowed the use of alphanumeric PINs.
- Management for multiple tokens is not supported. The Agent component processes modify requests for token objects one at a time.
- The assignment of the tokens to the accounts created for global users cannot be done using the RSA Account Template. A token cannot be associated with more than one user at the same time. To do this, you must create the accounts first and then assign tokens using the RSA Connector GUI or RSA native administration tools.

## Install the RSA Remote Agent

To install the RSA Remote Agent, follow this procedure.

**To install the RSA Remote Agent**

1. Locate the Provisioning Component installation media.
2. Run the RSA installer from the following locations:

- For Windows

  ```
  RemoteAgent/RSA/setup.exe
  ```

- For Solaris

  ```
  RemoteAgent/RSA/setup
  ```

Answer the questions to provide information about your system.

## How to Configure the CAM and CAFT Service

Install the RSA Remote Agent and configure the CAM and CAFT Service on any RSA ACE/Server machine that you want to administer.

To configure the CAM and CAFT Service, perform the following procedure.

**From the RSA ACE/Server machine**

1. Log on as the domain or local administrator
2. Issue the following command from a command window:

   ```
   cafthost -a RSA_node_name
   ```

   **RSA_node_name**

   Specifies the name of the Connector Server.

   Note: If the Connector Server is networked using DHCP or you do not use DNS for name resolution, the network name will not be recognized. Under these conditions, use the TCP/IP address for the RSA ACE node name or add an RSA ACE node entry in the local hosts file on your RSA ACE/Server machine.
3. Verify this command by issuing the following command:

   ```
   cafthost -l
   ```

## RSA Support for FIPS and IPv6

For this release of CA IdentityMinder, the RSA Connector does not support FIPs or IPv6.

# Connector-Specific Features

This section details your connector's specific management features, such as how to acquire and explore your endpoint. Also included are account, provisioning roles, account template, and group information specifically for your connector.

## Acquire an RSA ACE Server Using the User Console

You must acquire the RSA ACE server before you can administer it with CA IdentityMinder.

**To acquire an RSA ACE server using the User Console**

1. Select Endpoints, Manage Endpoints,Create Endpoint
2. Select RSA from the drop-down list box on Create a new endpoint of Endpoint Type, and click Ok

   Use the Create RSA Endpoint page to register an RSA ACE server. During the registration process, CA IdentityMinder identifies the RSA ACE server you want to administer and gathers information about it.
3. After entering the required information, click Submit.

   You are now ready to explore and Correlate the endpoint.
4. Click Endpoints, Explore and Correlate Definitions, Create Explore and Correlate Definition to explore the objects that exist on the endpoint.

   The Exploration process finds all RSA accounts and groups. You can correlate the accounts with global users at this time or you can correlate them later.
5. Click OK to start a new definition.
6. Complete the Explore and Correlate Tab as follows:
   a. Fill in Explore and Correlate name with any meaningful name.

      Click Select Container/Endpoint/Explore Method to click an RSA endpoint to explore.

   b. Click the Explore/Correlate Actions to perform:
      - **Explore directory for managed objects**—Finds objects that are stored on the endpoint and not in the provisioning directory.
      - **Correlate accounts to users**—Correlates the objects that were found in the explore function with users in the provisioning directory. If the user is found, the object is correlated with the user. However, you can instead select that you want to assign the account to the existing user (the default user) or create the user.
      - **Update user fields**—If a mapping exists between the object fields and the user fields, the user fields are updated with data from the objects fields.

7. Complete the Recurrence tab if you want to schedule when the task to executes.

   a. Click Schedule.

   b. Complete the fields to determine when this task should execute.

      You may prefer to schedule the task to execute overnight to interfere less with routine access of the system.

   **Note**: This operation requires the client browser to be in the same time zone as the server. For example, if the client time is 10:00 PM on Tuesday when the server time is 7:00 AM, the Explore and Correlate definition will not work.

8. Click Submit.

**To use an explore and correlate definition**

1. In a CA IdentityMinder environment, click Endpoints, Execute Explore and Correlate.

2. Click an explore and correlate definition to execute.

3. Click Submit.

   The user accounts that exist on the endpoint are created or updated in CA IdentityMinder based on the explore and correlate definition you created.

## Acquire an RSA ACE Server Using the Provisioning Manager

You must acquire the RSA ACE/Server machine before you can administer it with CA IdentityMinder. When acquiring an RSA ACE/Server machine, perform the following steps.

**From the Endpoint type task view**

1. Register the machine as an endpoint in CA IdentityMinder.

   Use the RSA ACE (SecurID) Endpoint property sheet to register an RSA ACE/Server machine. During the registration process, CA IdentityMinder identifies the RSA ACE/Server machine you want to administer and gathers information about it.

2. Explore the objects that exist in the endpoint.

   After registering the machine in CA IdentityMinder, you can explore its contents. Use the Explore and Correlate Endpoint dialog. The Exploration process finds all RSA ACE (SecurID) objects. You can correlate the accounts with global users at this time or you can correlate them later.

3. Correlate the explored accounts to global users

   When you correlate accounts, CA IdentityMinder creates or links the accounts on an endpoint with global users, as follows:

   a. CA IdentityMinder attempts to match the username with each existing global user name. If a match is found, CA IdentityMinder associates the RSA ACE (SecurID) account with the global user. If a match is not found, CA IdentityMinder performs the next step.

   b. CA IdentityMinder attempts to match the account name with each existing global user's full name. If a match is found, CA IdentityMinder associates the RSA ACE (SecurID) account with the global user. If a match is not found, CA IdentityMinder performs the following step.

   c. If the Create Global Users as Needed button is checked, CA IdentityMinder creates a new global user and associates the RSA ACE (SecurID) account with the global user. If the Create Global Users as Needed button is unchecked, then CA IdentityMinder performs the next step.

   d. CA IdentityMinder associates the RSA ACE (SecurID) account with the [default user] object.

## RSA Endpoint Property Sheet

The RSA Endpoint Property sheet lets you register or view the properties of an RSA ACE server. From the RSA Endpoint Tab you can specify the endpoint name, host name, account template information, and the password change propagate mode.

## Password Change Propagate Mode

The password change propagate mode on the Endpoint Tab of the Endpoint Property Sheet, specifies the way that the Password and PIN changes are handled during a change event. The following scenarios are possible:

1. If neither the Password Change nor PIN Change check boxes are checked, the password change will not occur.
2. If the Password Change check box is selected, but the PIN Change check box is not selected, only the user password will be changed to the value provided in the eTPassword attribute. No modifications will be applied to the assigned tokens.
3. If the Password Change check box is not selected, but the PIN Change check box is selected, only the value of the PIN for the assigned tokens will be changed to the value provided in the eTPassword attribute.
4. If both the Password Change check box and PIN Change check box are selected, both the user password and assigned tokens PINs will be changed to the value provided in the eTPassword attribute.

   **Note:** For 4, if the user does not have any tokens assigned to them, the request to modify the eTPassword attribute is treated as a request to assign the password to the user using the value provided in the eTPassword attribute.

   **Note:** For 3 and 4, if the user has more than one token assigned, the PIN reset applies to ALL of the tokens that are in possession of the user. The PIN associated with each assigned token is changed to the value provided in the eTPassword attribute.

## RSA Account Templates

The RSA DefaultPolicy, provided with the RSA ACE (SecurID) connector, gives a user the minimum security level needed to access an endpoint. You can use it as a model to create new account templates.

**Note:** You can create RSA account templates that are associated with multiple endpoints. These account templates can only be used to grant privileges to existing accounts.

## RSA Groups

You can create and maintain RSA ACE (SecurID) groups using the Endpoint type task view. Use the RSA Group property sheet when managing your groups.

## Token Management

The Token management features of the RSA Connector let users view and manage RSA Tokens and simulate suspending RSA accounts through a global user or Token properties.

## RSA Tokens Property Sheet

The RSA Tokens property sheet lets you view a token's details and initiate operations on the token. The following property pages apply to RSA tokens:

- Token Profile
- Token Operations

## Tokens Profile Tab

The Tokens Profile tab is a read-only page that displays the following details of a token:

- Serial Number
- Token Type
- Assigned...to..
- Enabled
- Lost
- New PIN Mode
- Expired
- Replacement Status

## Token Operations Tab

The Token Operations tab is used to initiate operations on a token.

**Note:** Operations are initiated on a single token at a time.

Using this tab, you can initiate the following operations:

**Enable Token**

Enables the token.

**Disable Token**

Disables the token

**Set New PIN Mode**

When the Set New PIN operation is selected, you can check the Clear PIN check box to clear the token immediately. A new PIN is assigned the next time you log in with your token code only.

If the Clear PIN check box is not checked, the PIN is cleared the next time you log in with your current PIN and token code.

**Set Emergency Mode Off**

Sets the emergency mode to off.

**Set Emergency Mode On**

When the set emergency mode operation is selected, you can specify the temporary password to be used, how long the emergency access mode is to last, and that the token is not automatically declared lost during the emergency access mode.

**Set Replacement Mode**

When the replacement mode operation is selected, you can search for a replacement token from all the available tokens or narrow the search by specifying specific attributes to search.

### *Enable a Token*

Perform this procedure to run the enable token operation.

**From the Token Operations Tab**

1. Select Enable Token from the Operation field drop-down list.
2. Click Apply/OK to enable the token.

   The enable token operation is performed.

### *Disable a Token*

Perform this procedure to run the disable token operation.

**From the Token Operations Tab**

1. Select Disable Token from the Operation field drop-down list.
2. Click Apply/OK to disable the token.

   The disable token operation is performed.

### *Set Emergency Mode Off*

Perform this procedure to run the set emergency mode off operation.

**From the Token Operations Tab**

1. Select Set Emergency Mode Off from the Operation field drop-down list.
2. Click Apply/OK to turn emergency mode off.

   The set Emergency Mode Off operation is performed.

### *Set New PIN Mode*

Perform the following procedure to run the set new PIN mode operation.

**From the Token Operation Tab**

1. Select Set New PIN Mode from the Operations field drop-down list.

   The Set New PIN Mode controls are activated.
2. Check the Clear PIN check box if the PIN for the token is to be cleared immediately.

   A new PIN must be assigned the next time you log in with your token code. Your current PIN will not work.

   If the Clear PIN check box is not checked, the PIN is cleared when you log in again with you current PIN and token code.
3. Click Apply/OK to put the token into new PIN mode.

   The Set New PIN Mode operation is performed.

### *Set Emergency Mode On*

Perform the following procedure to run the set emergency mode on operation.

**From the Token Operation Tab**

1. Select Emergency Mode On from the Operations field drop-down list.

   The Set Emergency Mode On controls are activated.

2. Enter the temporary password in the Temporary Password field to be used during the emergency operation.

3. Enter the length in the Life time field, in hours, that the emergency mode will be in effect.

4. Check the Auto not lost check box if the token should not be declared lost during emergency mode. If the check box is not selected, the token will be declared lost during the emergency operation.

   **Note:** Auto not lost is only available for RSA 6.1 or higher.

5. Click Apply/OK to turn Emergency Mode on.

   The Set Emergency Mode On operation is performed.

*Set Replacement Mode*

Perform the following procedure to run the set replacement mode operation.

**From the Token Operation Tab**

1. Select Set Replacement Mode from the Operations field drop-down list.

   The Set Replacement Mode Operations controls are activated.

2. Check the Keep Current Pin check box if the replacement token should be given the same PIN as the token being replaced. Leave this check box unchecked if the replacement token should start in new PIN mode.

3. Search for the available tokens by clicking the Search button to list all of the available tokens or specify the seed size, token type, and serial number to narrow the token search.

   The available tokens appear in the Available Tokens List Box.

4. Select a token from the Available Tokens list box and click the Add (>) button to add the token to the replacement serial number field.

5. Click Apply/OK to perform the selected replacement.

   The Set Replacement Mode operation is performed.

## Suspending and Resuming RSA Accounts

The RSA Connector can simulate account suspension by removing all tokens from an account. This approach restricts a user's ability to access the system. Resumption of an account is implemented by re-assigning tokens to an account. Two following two attributes are included in the connectors account class:

- eTSuspensionState
- eTPreSuspensionState

If these two attributes are defined, the following requests on an RSA account are affected:

- Account Search
- Account Modify
- Account Suspend
- Account Resume

*Account Search*

If the eTSuspensionState attribute is explicitly mentioned in a search request the agent plug-in retrieves a list of tokens assigned to an account, generates a corresponding XML document and returns it as an eTSuspensionState value.

*Account Modify*

If the eTSuspensionState attribute is included in a modifications list, an account is considered to be already suspended. If a list of modifications in a request contains any updates of the eTRSATokenNumber multi-value attribute, that request is rejected with an LDAP_OPERATIONS_ERROR code and proper message being sent.

*Account Suspend*

If the eTSuspended attribute is set to "1", the agent plug-in removes all eTRSATokenNumber values from an account. The account is then suspended.

*Account Resume*

To resume an account, a modify operation with eTSuspended set to 0 must be run. If the eTSuspensionState attribute is present in the modifications list, the attribute must be used to restore the eTRSATokenNumber values of an account.

# RSA Authentication Manager SecurID 7 Connector

The RSA SecurID 7 Connector provides a single point for all user administration and lets you administer the following objects on RSA SecurID endpoints:

- Accounts (Local and trusted) (see page 443)
- Administrative roles (see page 456)
- RADIUS profiles (see page 476)
- Tokens (see page 492)
- Security domains (see page 489)
- Trusted groups (see page 473)
- User groups (see page 463)

In addition, you can view read-only information about the following objects on RSA SecurID endpoints:

- Authentication agents (see page 506)
- Authentication grade policies (see page 507)
- Identity sources (see page 507)
- Lockout policies (see page 508)
- Off-line authentication policies (see page 508)
- Password policies (see page 508)
- Self-service troubleshooting policies (see page 510)
- Token policies (see page 509)
- Trusted realms (see page 511)

**Note:** The RSA SecurID 7 connector only supports RSA SecurID 7.1 endpoints.

## Set Up the RSA SecurID 7 Connector

For the RSA SecurID 7 Connector to work, it requires files that are installed with the RSA Authentication Manager server.

Before you use the connector, create a bundle that contains these files, and then add the bundle to the connector.

**Follow these steps:**

1. Install or upgrade CA IAM CS.

   The installation registers CA IAM CS with the provisioning server, creates the Salesforce.com endpoint, and populates it with its associated metadata.

2. Ask the SecurID administrator to send you a copy of the following files from the RSA Authentication Manager server, in *RSA_AM_HOME*/appserver/:

   - license.bea
   - .../modules/com.bea.core.process_5.3.0.0.jar
   - .../weblogic/server/lib/EccpressoAsn1.jar
   - .../weblogic/server/lib/EccpressoCore.jar
   - .../weblogic/server/lib/EccpressoJcae.jar
   - ...weblogic/server/lib/wlcipher.jar
   - .../weblogic/server/lib/wlfullclient.jar

   **Note:** You will need to generate the wlfullclient.jar file. For more information, see the *RSA Authentication Manager 7.1 Developer's Guide*.

3. Ask the SecurID administrator to log in to https://knowledge.rsasecurity.com, and download and extract the contents of the RSA Authentication Manager 7.1 SDK file named  am-7.1-sp3-sdk.zip. The connector needs the following files:

   - am-client.jar
   - ims-client.jar
   - commons-beanutils-1.7.0.jar
   - iScreen-1-1-0rsa-2.jar
   - iScreen-ognl-1-1-0rsa-2.jar
   - ognl-2.6.7.jar
   - systemfields-o.jar
   - hibernate-annotations-3.2.1.jar

4. Export the Server Root Certificate from the RSA Authentication Manager server and copy it to the CA IAM CS computer.

**Note:** For more information about exporting the Root Certificate, see the *RSA Authentication Manager 7.1 Developer's Guide*. The post-installation utility that you run later in this process automatically imports the Server Root Certificate.

5. Save the files on the CA IAM CS computer.
6. Run the *rsa7_post_install* script in the following location:

   *cs-home*/bin

   The script asks for the location of the SecurID files. It then creates a bundle and saves it in the same file as the script.
7. Log in to CA IAM CS (see page 21).
8. At the top, click the Connector Servers tab.
9. In the Connector Server Management area, click the Bundles tab.
10. Add the new bundle:

    a. In the Bundles area on the right, click Add.

    b. Browse to the bundle that the script created, then select the connector server on which this connector will be available.

    c. Click OK.

       The new bundle appears in the Bundles list.
11. Find the main connector bundle in the Bundles list, then right-click its name in the list and choose Refresh Imports from the popup menu.

The RSA SecurID 7 connector can now use the extra files.

## Acquire an RSA SecurID 7 Endpoint

To acquire and manage the RSA SecurID endpoint, you must get the command client user name and password from the RSA Authentication Manager.

**Note:** For more information about getting the command client user name and password, see the *RSA Authentication Manager 7.1 Developer's Guide,* available in the RSA Authentication Manager 7.1 SDK.

The command client credentials let you acquire and manage an RSA SecurID endpoint.

## Upgrade the RSA SecurID 7 Connector

The RSA SecurID 7 connector supports RSA Authentication Manager 7.1 SP3 or higher.

If you have a previous version of the RSA SecurID 7 connector, upgrade your RSA Authentication Manager 7.1 installation to SP3 and run the RSA SecurID 7 Connector post-installation utility.

The utility replaces the current SDK files installed on CA IAM CS computer with RSA 7.1 Authentication Manager SP3 SDK files. To download the required RSA SP3 SDK files, RSA login credentials are required.

**Follow these steps:**

1. Upgrade your RSA Authentication Manager 7.1 endpoint to RSA Authentication Manager 7.1 SP3.

   **Note:** For more information about upgrading your RSA Authentication Manager 7.1 endpoint, see https://knowledge.rsasecurity.com/scolcms/set.aspx?id=8624.

2. Go to the RSA SecurCare Online website:

   https://knowledge.rsasecurity.com

   Download and extract the following file:

   am-7.1-sp3-sdk.zip

3. Navigate to *cs_home*\Resources\rsa7 and enter the following command:

   ```
   RSA7_post_install.bat -rsasdk
   ```

   **Note:** The utility is installed as part of the CA IAM CS installation.

4. When prompted, enter the location of the RSA SP3 SDK files you copied in step 2.

5. Restart the CA IAM CS computer.

   You have upgraded your RSA SecurID 7 connector SDK files and they are now compatible with RSA Authentication Manager 7.1 SP3.

## Upgrade RSA SecurID 7 Connector After CA IdentityMinder Upgrade

If you are upgrading CA IdentityMinder from a previous version, run the RSA SecurID 7 Connector post-installation utility. The utility replaces the current SDK files installed on CA IAM CS computer with RSA 7.1 Authentication Manager SP3 SDK files. To download the required RSA SP3 SDK files, RSA login credentials are required.

**Follow these steps:**

1. Upgrade your RSA Authentication Manager 7.1 endpoint to RSA Authentication Manager 7.1 SP3.

   **Note:** For more information about upgrading your RSA Authentication Manager 7.1 endpoint, see https://knowledge.rsasecurity.com/scolcms/set.aspx?id=8624.

2. Go to the RSA SecurCare Online website:

   https://knowledge.rsasecurity.com

   Download and extract *am-7.1-sp3-sdk.zip*.

3. Navigate to *cs_home*\Resources\rsa7 and enter the following command:

   ```
   RSA7_post_install.bat
   ```

   **Note:** The utility is installed as part of the CA IAM CS installation.

4. When prompted, enter the location of the RSA SP3 SDK files you copied in step 2.

5. When prompted, enter the location of the Weblogic files, and the RSA server certificate.

6. Restart the CA IAM CS computer.

   You have upgraded your RSA SecurID 7 connector SDK files and they are now compatible with RSA Authentication Manager 7.1 SP3.

## Connector Specific Features

This section details your connector's specific management features, such as how to acquire and explore your endpoint. Also included are account, account template, and group information specifically for your connector.

**Note:** For a general overview of the Provisioning Manager and its main features, see Managing the Connectors. For more detailed information about the Provisioning Manager, see the *Provisioning Guide*.

## RSA 6.x Connector Data Migration

You can use the RSA SecurID 7.1 migration utility, RSA7Migrate, to migrate existing RSA 6.1 account templates to the new RSA 7.1 connector data. The migration utility creates new RSA 7.1 account templates; RSA 6 templates are preserved during the migration process.

The migration utility does not migrate RSA 6.1 endpoint data because such migration requires retrieval of all accounts from an RSA 6.1 endpoint. Instead, reexplore the RSA 7.1 endpoint that contains the RSA 6.1 migrated data. Or, to be precise, perform subtree exploration only on an RSA 7.1 security domain where you migrated the RSA 6.1 data.

RSA only supports data migration from RSA Authentication Manager 6.1. As a result, the RSA7Migrate utility only supports the migration of RSA 6.1 endpoint data. The utility cannot differentiate between acquired RSA 5.x, 6.0 and 6.1 endpoints.

**Important!** Verify that all relevant RSA data has been successfully migrated before running the RSA7Migrate utility,

## RSA7Migrate Command

**Valid on Windows and Solaris**

Use the RSA7Migrate command to migrate existing RSA 6.1 account templates to the new RSA 7.1 connector data, or migrates tokens from RSA 6.1 endpoints to RSA 7.1 endpoints.

This command has the following format:

(Windows and UNIX) RSA7Migrate [-tokens]

**-tokens**

(Optional) Migrates tokens from RSA 6.1 endpoints to RSA 7.1 endpoints and populates the CA IdentityMinder Provisioning Directory with RSA 7.1 tokens.

## RSA7Migrate Processing Modes

When you run the RSA7Migrate utility to migrate account templates, you are prompted to run the utility in one of the following modes:

- Mode 0 – Do nothing, that is report only

  We recommend that you first run the utility in this mode, to identify any errors.

- Mode 1 – Create a template only if there are no errors

  If no errors are found after running the utility in mode 0, run the utility in mode 1.

- Mode 2 – Create a template even if errors found, but do not associate it with a namespace.

- Mode 3 – Create a template and associate it with a namespace even if errors found.

  Use this mode to identify and solve problems after you run the migration utility.

- Mode 4 (interactive mode) – Modify a template to make it compatible with a namespace. In interactive mode, you are prompted to specify an existing trusted realm.

  Use this mode to resolve problems with templates. For example, if the utility does not find RSA objects automatically, use this mode to specify the names and locations of the missing RSA7.1 endpoint objects.

## Migration Utility Prerequisites

Before you run the RSA7Migrate utility, do the following:

- Perform a migration of the RSA 6.1 endpoint data to RSA 7.1 endpoint data
- Acquire and explore RSA 7 namespaces that contains the migrated RSA data

You are required to supply the following information during the migration process:

- CA IdentityMinder Provisioning Server connection details:
    - Host name
    - Port
    - TLS status
    - TLS port (if TLS status is enable)
    - User name
    - Password
  - RSA 6 namespace name
  - RSA 7 namespace name, that corresponds to the above RSA 6 namespace
  - Security domain where the migrated RSA 6.1 data is located. This domain is always specified during the data migration process on the RSA side.
  - Suffix you want to add to the RSA 6 template name to create the RSA 7 template name.

## What the Migration Utility Does

The migration utility does the following:

- Searches for all RSA 6 account templates which are associated with the specified RSA 6 namespace. You are asked to specify a search pattern. If the search operation does not return anything, the migration utility prompts you to specify a new search pattern.
- For each account template returned by search operation, the migration utility does the following:
  - Returns all template attributes
  - Verifies that the RSA7 template with the name you specified exists
    - If the name exists, the utility prompts you for a different name
    - If you use an existing RSA7 template, the utility skips template generation and proceeds to verification and association with the specified RSA7 namespace.
- Generates a new RSA 7 template

  If a template is a local template (that is, the realm name is not specified in the RSA 6 template) the utility represents each group listed in the RSA 6 template as a local group in the RSA 7 template. For example, the group Rsa6_group is represented as the following in the RSA 7 template:
  eTDYNGroupName= rsa6_group,eTDYNContainerName=Security_Domain,...

  For example, the group Rsa6_group@site is represented as the following in the RSA 7 template:
  eTDYNGroupName= rsa6_group,eTDYNContainerName=site,
  eTDYNContainerName=Security_Domain,...

  Each agent host listed in RSA 6 template is represented in the RSA 7 template as a local group. For example, the agent host Agent_host.ca.com is represented in the RSA 7 template as:
  eTDYNGroupName= Agent_host,eTDYNContainerName=Security_Domain,...

  If a template is a remote template, that is, the realm name is present in the RSA 6 template, trusted group DNs are generated instead of local ones as previously shown, and the account name is represented as *account % realm.*
- Verifies that specified security domain exists in the RSA 7 namespace.

  If a domain cannot be found in interactive mode, the utility prompts you to provide a proper name.
- Verifies that the specified realm exists in the RSA 7 namespace, if a template is a remote template.

  In interactive mode, you are prompted to choose an existing trusted realm.
- Verifies that all RSA 7 groups (that is, groups corresponding to RSA 6 groups, and groups corresponding to RSA 6 agent hosts) exist in the RSA 7 namespace.

If a group cannot be found in interactive mode, you are prompted to specify a proper group name. Use the following format for DNs composite names:

Realm/SD_Level_1/SD_Level_2/…

- Creates an RSA7 template and associates it with the RSA 7 namespace.

## Account Template Migration Limitations

Account template migration limits are mostly related to RSA6 templates associated with more than one namespace. Observe the following limitations during account template migration.

All namespaces associated with the same template must:

- Have the same security domain DN
- Contain the same Group DN(s) for all the groups associated with a template
- Have the same Identity Source DN for accounts to be stored
- Expose the same realm in case of remote templates

If any of the objects described previously have different names (or DNs) in different namespaces, such namespaces must have a separate set of templates. If necessary, run the migration utility several times to create the templates correctly.

## Migrate RSA 6.1 Account Templates to RSA 7.1 Connector Data

To migrate RSA 6.1 account templates to the RSA 7.1 connector data, run the RSA7Migrate utility.

**To migrate RSA 6.1 account templates to the RSA 7.1 connector data**

1. Verify that the Provisioning Server is running.

   **Note**: The Provisioning server must be running when you migrate templates.

2. Open a command prompt window and navigate to the \bin directory where you installed the Connector Server.

3. Enter the following command:
   ```
   RSA7Migrate
   ```
   The RSA7Migrate utility starts and prompts you for the Provisioning Server connection details.

4. Enter the information requested.

   The RSA7Migrate utility creates an RSA7 template and associates it with the RSA 7.1 namespace.

## What the Token Migration Utility Does

The token migration utility does the following:

- Prompts you for the:
  - CA IdentityMinder Provisioning Directory connection details
  - RSA 6 namespace name where the templates you want to migrate are located
  - RSA 7 namespace name, corresponding to the above RSA 6 namespace
  - Security domain where the migrated RSA 6.1 data is located. This domain is always specified during data migration process on the RSA side.
- Connects to the CA IdentityMinder Provisioning Directory
- Prompts you to provide a search pattern for token serial numbers
- Reads all tokens which satisfy the search pattern, from the RSA 6 explored data in the CA IdentityMinder Provisioning Directory
- Writes the RSA 7 token object into the provided security domain in the RSA 7 explored data for each token.

## Token Migration Prerequisites

Before you run the RSA7Migrate token migration utility, do the following:

- Migrate the RSA 6.1 endpoint data to RSA 7.1
- Acquire and explore the RSA 7.1 namespaces that contains the migrated RSA 6.1 data.

You are required to supply the following information during the migration process:

- CA IdentityMinder Provisioning Directory connection details:
  - Host name
  - Port
  - TLS status
  - TLS port (if TLS status is enabled)
  - Password
- RSA 6 name
- RSA 7.1 endpoint name, corresponding to the above RSA 6 namespace
- RSA 7. 1 security domain where the migrated RSA 6.1 data is located. This domain is always specified during data migration process on the RSA side.

## Migrate Tokens

To migrate tokens to populate the CA IdentityMinder Provisioning Directory with RSA 7.1 tokens, run the RSA7Migrate utility with the -token command-line parameter.

**To migrate tokens**

1. Stop the CA IdentityMinder Provisioning Server.
2. Open a command prompt window and navigate to one of the following directories where you installed the Connector Server.
   - (Windows) C:\Program Files\CA\Identity Manager\Connector Server\resources\rsa7\
   - (Solaris) /opt/CA/IdentityManager/ConnectorServer/resources/rsa7/
3. Enter the following command:
   ```
   RSA7Migrate -tokens
   ```
   The RSA7Migrate utility starts and prompts you for the Provisioning Server connection details.
4. Enter the information requested.

   The migration utility writes the RSA 7 token object into the provided security domain in the RSA 7 explored data for each token.
5. Start the CA IdentityMinder Provisioning Server.

## Local and Remote User Support

The RSA SecurID 7.1 Connector supports both remote users and local users, through the one account object class. Remote users are users that exist in other realms but to whom you want to grant certain rights within the current realm. Local users and remote users (also known as trusted users) can have the same login names within one security domain.

The different account types are distinguished by appending a suffix to the associated RSA user ID and using the percent sign as delimiter. For example, " % ".

**Note:** There is a space before and after the delimiter.

Remote users have special LDAP names with the following format:

*Remote_username< delimiter >Realm_name*

An example of a remote user name is *UserName01% CA*

Using a delimiter to distinguish local and remote users has implications on global user correlation and the use of account templates. During correlation, the delimiter becomes part of the global user name. However global users with the delimiter as part of their name cannot be used to create endpoint users using account templates as the delimiter is treated as a special character.

To allow for some alternatives for correlation, you can use the following hidden attributes:

- LoginID

  The Login Id attribute is always set to the login name of the user regardless of whether the user is a remote or local user. That is, it does not contain the delimiter and realm suffix for remote users.

  Correlating against this attribute means that all global users created can be used with account templates but any users with the same login name as the same user are also correlated.  For example, the local user *janesmith* is correlated to the same global user as *janesmith % sales* and *janesmith % dev1.*

- LocalUserLoginID

  This attribute is set to the login name of the user only for local users, but is not set for remote users.

  Correlating against this attribute creates global users for all local RSA users while correlating all remote RSA users to the default user.

**More information:**

Create a Trusted User (see page 448)

## Windows Password Integration

If Windows password integration enabled in RSA, the RSA server caches the Windows password of each user in the security domain. When a user logs in, they are only required to enter their RSA passcode.

When you select the Clear cached copy of Windows credentials check box on the General 1 Tab (User Account Dialog) or General 1 Tab (Account Template Dialog), the connector removes the user's Windows credentials from the cache. The next time the user logs in, the user is prompted for their Windows password in addition to their RSA passcode.

The check box does not show the status of the cache, or whether the check box has been set on a prior transaction.

## Date and Time Considerations

All dates and times that the RSA SecurID 7.1 Connector receives should be in UTC. All dates and time values that specify time zone information other that +00:00, -00:00 or Z, are invalid and any date or time values received without time zone information are treated as UTC.

In Account screens, values are in Provisioning Manager local time. The Provisioning Manager converts these values to UTC then passes  them to endpoint. The endpoint then converts the values to the time zone it is in. For example, if the Provisioning Manager is in Perth (UTC + 8) and the endpoint is in Melbourne (UTC + 10), to set an endpoint-based time of Sept 1, 2009 10 am, set the value in the Provisioning Manager to September 1, 2009 8 am. (Provisioning Manager local time).

In Account template screens, although you can enter any value, the valid values are:

- %XD%

  Specifies the date and time of account creation. The Provisioning Manager sets this value to the date and time of account creation converted to UTC, in the format yyyy-mm-ddTHH:MM:SSZ. The endpoint converts the value to the time zone it is in.

- Specific date

  Use the same format as the rule string %XD%, with or without the Z. This string is passed as is (no conversion) to the Provisioning Server, and eventually to the endpoint. The endpoint then converts this value to its local time. Therefore, enter the value to whatever endpoint time you want the endpoint time it to be, converted to UTC, that is, use the equivalent UTC. As in the previous example of the endpoint in Melbourne and the Provisioning Manager in Perth, if you want to set the value to be September 1, 2009 10am Melbourne time, enter 2009-09-01T00:00:00.

- Daylight savings time

  As in the previous example of the endpoint in Melbourne and the Provisioning Manager in Perth, if you want to set the value to Dec 25, 2009 10am Melbourne time, the set the value in the Provisioning Manager to 2009-12-24T23:00:00.

- %UCUnn%

  This value works the same way as with the specific date case. That is, enter the UTC equivalent value.

## Group Access Times

The RSA7.1 endpoint stores group access times as UTC but displays them using the RSA7 Server local time. To make it easier for group administrators to set the access times relevant to other time zones, the RSA Security Console provides the ability to select a time zone and displays the group access times relevant to the select time zone. However, the selected time zone is not stored. Each time the page is displayed the time zone control defaults to the RSA server local time.

Due to limitations in the RSA API, the RSA SecurID 7.1 Connector cannot return the RSA server local time. To resolve this limitation, a time zone attribute has been added to the RSA7.1 endpoint dialog, General 1 tab. You can use this attribute to specify the time zone to use for group access times. This attribute defaults to UTC. All times displayed or entered for group access are assumed to be for this time zone.

This solution is also applicable to time zones specified for trusted user groups.

## Multi-value Assignment Dialogs

The multi-value assignment dialogs let you search for a specific object in a selected system domain, then assign those values to a specific object. For example, you can search all administrative roles in a specific system domain, then assign the administrative roles to a user account.

The multi-assignment dialog contains the following fields:

**Available List Search**

Displays the containers in the namespace you can search.

**Class**

Specifies the object class you want to search.

Classes that use the attribute displayed in the Attribute list are displayed in the list.

**Attribute**

Specifies the attribute you want to search for.

**Value**

Specifies the value you want to restrict the search to.

**Default**: Wildcard character (*). The wildcard causes the search to return all entries.

**Note:** If you perform an advanced search for an attribute, this field is not available.

**Search one level only**

Restricts the search to only the level selected in the Available List Search.

**Advanced**

Displays the Advanced Search Attributes dialog. Use this dialog to set more advanced search criteria.

**Note:** Specifying advanced search criteria is useful if you want to narrow the list of objects in the class.

## Assign Multi-values to an Object

To assign multiple values to an RSA object, search for the object you want to assign then select the values you want assign to the RSA object.

**To assign multivalues to an object**

1. On the multivalue assignment dialog (see page 439), select a class from the class list.

   Selecting a class list specifies the object class you want to search. Classes that use the attribute displayed in the Attribute list appear in the list.

2. In the Attribute list, select an attribute.

   Selecting an attribute specifies the attribute you want to search for.

3. Type a value in the Value field.

   The value that you want to restrict the search is specified.

   **Note:** The default is the wildcard character (*). The wildcard causes the search to return all entries.

   **Note:** If you perform an advanced search for an attribute, this field is not available.

4. Select the Search one level only check box.

   Selecting the check box restricts the search to only the level selected in the Available List Search tree.

5. Click Advanced.

   The Advanced Search Attributes dialog appears.

6. If necessary, specify more advanced search criteria.

   **Note:** Specifying advanced search criteria is useful if you want to narrow the list of objects in the class.

7. Click Search.

   The objects you can assign appear in the Available list.

8. Select the objects you want to assign, then move the objects to the Assigned list, then click OK.

   You have assigned the objects to the RSA object you are working with.

## How You Acquire and Manage RSA 7.1 Endpoints

Before you can administer an RSA 7.1 endpoint with the Provisioning Manager, acquire the endpoint. When acquiring an RSA 7.1 endpoint, perform the following steps from the Endpoint task view:

1. Acquire the RSA server as an endpoint in the Provisioning Manager.
2. Explore the objects that exist in the endpoint.

   After registering the computer in the Provisioning Manager, you can explore its contents. The exploration process finds all RSA objects. You can correlate the accounts with global users at this time, or you can wait to correlate them.
3. Correlate the explored accounts to global users. You can:

   - Use existing global users. Use existing global users when there are already global users in the Provisioning Manager and you want to connect the existing global users to the RSA accounts
   - Create global users as needed. Create global users when there are no global users and you want to populate the Provisioning Manager from the RSA accounts.

     When you correlate accounts, the Provisioning Manager creates or links the accounts on an endpoint with global users, as follows:
   - The Provisioning Manager attempts to match the RSA account name with each existing global user name. If a match is found, the Provisioning Manager associates the RSA account with the global user. If a match is not found, the Provisioning Manager performs the next step.
   - The Provisioning Manager attempts to match the RSA account with each existing global user's full name. If a match is found, the Provisioning Manager associates the RSA account with the global user. If a match is not found, the Provisioning Manager performs the next step.
   - The Provisioning Manager associates the RSA account with the [default user] object or a new global user is created depending on your choice.

## Acquire an RSA SecurID 7 Endpoint

Acquire and register an RSA SecurID 7 endpoint before you can administer it with the Provisioning Manager.

**To acquire an RSA SecurID 7 endpoint**

1. In the Provisioning Manager, click the Endpoints button.
2. In the Object Type list, select RSA SecurID 7 [DYN Endpoint], then click New.

   The RSA SecurID namespace dialog appears.
3. On the endpoint tab, specify the Username and Password of a privileged RSA local user, and the command credentials for the RSA endpoint.

   **Note**: Command client credentials are generated on an RSA server and work only with that RSA installation. You require different command credentials for each RSA installation. However, although different realms defined on one RSA server correspond to different CA IdentityMinder endpoints, you can use the same command credentials to acquire them.
4. Complete the remaining fields on the Endpoint tab, then click OK.
5. Complete the fields on the Endpoint Settings tab.

   The various settings that apply to controlling endpoints, such as password propagation and synchronization are specified.
6. Complete the fields on the General 1 tab.

   You have defined the time zone associated with group access times.
7. Complete the fields on the Program Exits Reference tab.

   Program exits are viewed added edited or removed as specified.
8. Complete the fields on the Attribute Mapping tab.

   The default attribute mapping defined in the schema file for the endpoint type are specified.
9. Complete the fields on the Logging tab.

   The logging settings for the new endpoint are specified.
10. Click OK.

    You have specified the administrative and connection details of an RSA SecurID endpoint.

## Account Management

The RSA 7.1 SecurID connector supports the following account management operations:

- Creating, modifying, renaming, moving and deleting accounts
- Creating, modifying and deleting account templates
- Creating, renaming, moving, modifying, and deleting trusted users
- Adding and removing local and trusted users to and from groups

## Add Accounts

To create an account for a user on the RSA endpoint, create a user and specify the details of their account.

**To add accounts**

1. In the Provisioning Manager, click the Endpoints button and select SecurID 7 [DYN Endpoint] in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to add accounts, then select Content.

   The Endpoint Content dialog appears.
4. Select the System Domain container in the Container tree.
5. Select User Account in the Object Type list and click New.

   The User Account dialog appears General 1 tab appears.
6. On the General 1 tab, specify the basic details of the user account you want to add.
7. On the General 2 tab, specify the authentication details of the user account.
8. On the General 3 tab, specify that you want to assign the next available token and clear the incorrect passcode counter.
9. On the Identity Source tab, select the Identity Source where you want to add the user.
10. On the RADIUS profile tab, assign a RADIUS profile to the user.
11. On the Administrative Roles tab, assign an administrative role to the user.
12. On the SecurID Tokens tab, assign a token to the user.
13. On the Member of tab, add the user to a group.
14. Click Ok.

    The user account is created on the RSA endpoint.

## Update Accounts

To modify the details of a user account update the user account on the RSA endpoint.

**To update accounts**

1. In the Provisioning Manager, click the Endpoints button and select SecurID 7 [DYN Endpoint] in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to update accounts and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select the Security Domain you want to search.
5. Select User Account in the Object Type list and click then click Search.

   The accounts for the system domain you selected appear in the list view.
6. Right-click an account in the list view and then click Properties.
7. Modify the properties on the User Account dialog and then click Apply.

   The details of the user account are modified.

## Delete Accounts

If you want to remove an account from an endpoint you can delete the account.

**To delete accounts**

1. Click the Endpoints task button and select SecurID 7 [DYN Endpoint] in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to remove the account and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select the Security Domain you want to search.
5. Select User Account in the Object Type list and click then click Search.

   The accounts for the system domain you selected appear in the list view.
6. Right-click an account in the list view and then click Delete.
7. When prompted, confirm that you want to delete the account.

   The account is deleted.

## Create an Account Template

You can create account templates that specify a set of attributes and for all users assigned the account template.

**To create account templates**

1. Click the Roles task button and select the RSA SecurID 7 [DYN Account Template] type in the Object Type drop-down list.
2. Click New.

   The RSA SecurID 7 Account Template dialog appears.
3. On the Endpoints tab, specify an endpoint for this account template.
4. On the General 1 tab, specify the users details and account credentials for accounts provisioned with this template.

   **Important!** If you are creating an account template for trusted users, delete the rule string  %P%  from the Password field. If you do not delete the rule string, the account template creation for the global user will fail.
5. On the General 2 tab, specify the authentication settings for users that are provisioned with this account template.

   **Important!** If you are creating an account template for trusted users, delete the rule string %XD% from the Start date field, and delete the rule string %UL% from the Last name field. If you do not delete the rule strings, the account template creation for the global user will fail.
6. On the Identity source tab, specify the identity source that accounts based on the template are assigned.
7. On the RADIUS Profile tab, specify the RADIUS profile that accounts based on this template are assigned.

   On the Administrative Roles tab, specify the administrative roles that accounts based on the template are assigned.
8. On the Member of (Trusted Groups) tab, specify the trusted groups that accounts based on the template are members of.
9. On the Member of tab, specify the groups that accounts based on the template are members of.
10. Click OK.

    The account template for the RSA endpoint is created.

## Edit an Account Template

You can modify the account templates that specify a set of attributes and privileges for all users assigned the account template.

**To edit an account template**

1. Click the Roles task button and select and select the RSA SecurID 7 [DYN Account Template] type in the Object Type drop-down list.
2. Click Search.

   The account templates for the system domain you selected appear in the list view.
3. Right-click an account template in the list view and then click Properties.

   The RSA SecurID 7 Account Template dialog appears.
4. Complete the fields on the General 1 tab to specify the users details and account credentials for accounts provisioned with this template.
5. Complete the General 2 tab to specify authentication settings for users that are provisioned with this account template.
6. Complete the fields on the Identity source tab to specify the identity source that accounts based on the template are assigned.
7. Complete the fields on the RADIUS Profile tab to specify the RADIUS profile that accounts based on this template are assigned.
8. Complete the Administrative Roles tab to specify the administrative roles that accounts based on the template are assigned.
9. Complete the Member of (Trusted Groups) tab to specify the trusted groups that accounts based on the template are members of.
10. Complete the Member of tab to specify the groups that accounts based on the template are members of.
11. Click OK.

    The account template for the RSA endpoint is updated.

## Delete an Account Template

You can delete account templates for the RSA 7.1 SecurID endpoint.

**To delete account templates**

1. Click the Roles task button and select the RSA SecurID 7 [DYN Account Template] type in the Object Type drop-down list.
2. Click Search.

   The account templates for the system domain you selected appear in the list view.
3. Right-click an account template you want to delete and then click Delete.
4. When prompted, confirm that you want to delete the account template.

   The account template is deleted.

## Create a Trusted User

To create a user that can authenticate through realms other than their own you can create a trusted user. When you create a user account, you append the name of the trusted realm you want the user to authenticate through to the users login id, which identifies the user as a trusted user.

**To create a trusted user**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to create a trusted user and then select Content.

   The Endpoint Content dialog appears.
4. Select the System Domain container in the Container tree.
5. Select User Account in the Object Type list and click New.

   The User Account dialog appears General 1 tab appears.
6. On the General 1 tab, define a login id for the user, then select the trusted realm you want the trusted user to authenticate through from the drop-down list next to the Login Id field.
7. Complete the Notes field if required.
8. If required complete the Default Shell field in the General 2 tab on the User Account dialog, then click OK.
9. Complete the required fields on the other tabs on the User Account dialog, then click OK.
10. On the RADIUS profile tab, assign a RADIUS profile to the user.
11. On the Member of (Trusted Group) tab, add the user to a trusted group.

    The trusted user is created, and is assigned a login id in the following format:

    *Remote_username< delimiter >Realm_name*

    For example, *UserName01 % CA.*

**More information:**

Local and Remote User Support (see page 435)

## Move a Local or Trusted User into a Different Security Domain

If you want to manage a local or trusted user under a different security domain, you can move the user or local user to another security domains within the realm.

**To move a local user or trusted user into a different security domain**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurId 7 [DYN Endpoint] type in the Object Type drop-down list .
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to move a local or trusted user, and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select the Security Domain you want to search.
5. Select User Account in the Object Type box and click then click Search.

   The accounts for the system domain you selected appear in the list view.
6. Right-click an account in the list view and then click Move.

   The Move in Hierarchy dialog appears.
7. Select the Security Domain you want to move the account into.
8. Click OK.

   The account is moved into the security domain you selected.

## Update a Trusted User

If the account details of a user change, you can update the details of a trusted user.

**To update a trusted user**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to update a trusted user, and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select the Security Domain you want to search.
5. Select User Account in the Object Type list and click then click Search.

   The accounts for the system domain you selected appear in the list view.
6. Right-click an account in the list view and then click Properties.
7. Modify the properties on the User Account dialog and then click Apply.

   The details of the user are modified.

## Rename a Trusted User

If the login id or the trusted realm the user belongs to change, you can change the details of users login id.

**To rename a trusted user**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search to search for the endpoint on which you want to update the account.
3. Right-click the endpoint on which you want to rename a trusted user and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select the Security Domain you want to search.
5. Select User Account in the Object Type list and click then click Search.

   The accounts for the system domain you selected appear in the list view.
6. Right-click a trusted account in the list view and then click Rename.

   The Rename dialog appears.
7. Type the new name of the trusted user in the New name field in the following format:

   *Remote_username <delimiter> Realm_name*

   For example, *UserName01 % CA.*

**More information:**

Local and Remote User Support (see page 435)

## Delete a Trusted User

To remove a trusted user from an endpoint you can delete the trusted user account.

**To delete trusted users**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to delete a trusted user and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select the Security Domain you want to search.
5. Select User Account in the Object Type list and click then click Search.

   The accounts for the system domain you selected appear in the list view.
6. Right-click a trusted user in the list view and then click Delete.
7. When prompted, confirm that you want to delete the trusted user.

   The trusted user is deleted.

## How you Add Trusted Users to Trusted Groups

To add trusted users to trusted groups you can do either of the following:

- Edit an individual trusted user and specify which trusted groups the user is a member of (see page 453)
- Edit a trusted group and specify the trusted members of the group (see page 454)

## Add Trusted Users to Trusted Groups

To manage trusted users as group, you can specify which trusted groups a user is member of.

**To specify which trusted groups the user is a member of**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to specify which trusted groups a user is a member of, and then select Content.

   The Endpoint Content dialog appears.
4. Select the System Domain container in the Container tree.
5. Select User in the Object Type list and click Search.

   The list of users appears in the list view.
6. Right click the user you want to add to a trusted group, then click Properties.

   The User dialog General 1 tab appears.
7. Click the Member of (Trusted Groups) tab.
8. Search for the trusted groups you want to add the user to. (see page 440)

   The trusted groups you can assign to the trusted user appear in the Available list.
9. In the Available list, select the trusted group or group you want to add the user to,and then move the trusted group or groups to the Assigned list, then click OK.

   The trusted users you selected are added to the trusted group.

## Assign a Trusted User to a Trusted Group

To manage trusted users as a group, you can specify the trusted members of a trusted group.

**To specify the trusted members of a trusted group**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to add trusted users to trusted groups and then select Content.

   The Endpoint Content dialog appears.
4. Select the System Domain container in the Container tree.
5. Select Trusted Group in the Object Type list and click Search.

   The list of trusted groups appears in the list view.
6. Right click the trusted group you want to add users to, then click Properties.

   The Trusted Group dialog General 1 tab appears.
7. Click the Trusted User Members tab.
8. Search for the trusted users you want to add to the trusted group. (see page 440)

   The trusted users you can assign to the trusted group appear in the Available list.
9. In the available list, select the trusted user or users you want to add to the trusted group, then move the trusted user or users to the Assigned list, then click OK.

   **Note:** Both local and trusted users appear in the Available list. Verify that you select the correct user type before you move it to the Assigned list. For more information, see Local and Remote User Support (see page 435).

## How you Remove Trusted Users from Trusted Groups

To remove trusted users from groups, you can do either of the following:

- Edit an individual trusted user and remove the trusted group the trusted user is a member of (see page 455)
- Edit a trusted group and remove the trusted user from the trusted group (see page 456)

## Remove the Trusted Groups the User is a Member of

If you no longer want to manage a user as part of a trusted group, you can remove the trusted group or trusted groups a trusted user is a member of.

**To remove the trusted group a trusted user is a member of**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to remove a trusted group a user is a member of and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select the Security Domain you want to search.
5. Select User Account in the Object Type list and click then click Search.

   The accounts for the system domain you selected appear in the list view.
6. Right-click a trusted user account in the list view and then click Properties.

   The User Account dialog appears.
7. Click the Member of (Trusted Groups) tab.

   The trusted groups that the trusted user belongs to appear in the Assigned list.
8. In the Assigned list, select the trusted group or trusted groups you want to remove the trusted user from, then move the trusted group to the Available list, then click OK.

   The trusted groups the trusted user is a member of are removed.

## Remove the Trusted Members of a Trusted Group

If you no longer want to manage a trusted user as part of a trusted group, you can remove the trusted user from a trusted group.

**To remove the trusted members from a trusted group**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint from which you want to remove trusted members of a group and then select Content.

   The Endpoint Content dialog appears.
4. Select the System Domain container in the Container tree.
5. Select Trusted Group in the Object Type list and click Search.

   The list of trusted groups appears in the list view.
6. Right-click the trusted group you want to remove members from, then click Properties.

   The Trusted Group dialog General 1 tab appears.
7. Click the Trusted User Members tab.

   The trusted users that are members of the group appear in the Assigned list.
8. In the Assigned list, select the trusted user or trusted users you want to remove from the trusted group, then move them to the Available list, then click OK.

   The trusted users you specified are removed from the trusted group.

## Administrative Roles

Administrative roles are read-only. You can only view the security domain scope in which the administrator has permission to manage objects and the identity source an administrator has permission to manage users from.

However, you can assign and unassign a user account to an administrative role.

**More information:**

How to Remove an Administrative Role (see page 459)
How to Assign an Administrative Role (see page 457)

## View Administrative Roles

You can view the administrative roles in your organization.

**To view administrative roles**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to view administrative roles, and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select the Administrative Roles container in the Container tree, then click Search.

   The Administrative Roles for the endpoint you specified appear in the list view.
5. Right-click the Administrative role you want to view details for.

   The Administrative Roles dialog appears and displays the identity sources an administrator has permissions to manage users from, and the security domain the administrator has permissions to manage users from.

## How to Assign an Administrative Role

To assign an administrative role use either of the following methods:

- Edit an individual user and specify the administrative roles you want the user to have (see page 458)
- Edit an administrative role and specify the users that have the administrative role (see page 459)

## Specify the Administrative Roles You Want the User to Have

To let a user perform specified actions in a specific security domain, you can assign an administrative role to a user. You can assign multiple administrative roles to a user.

**To specify the administrative roles you want a user to have**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to assign an administrative role to a user account and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select the Security Domain you want to search.
5. Select User Account in the Object Type list and click then click Search.

   The accounts for the system domain you selected appear in the list view.
6. Right click the user account you want to assign and administrative role, then click Properties.

   The User Account dialog appears.
7. Click the Administrative Roles tab.

   The administrative roles that the user is assigned appear in the Assigned list, and the containers in the namespace you can search appear in the Available List Search tree.
8. Search for the administrative roles you want to assign to the user. (see page 440)

   The administrative roles you can assign to the user account appear in the Available list.
9. In the Available list, select the Administrative role or administrative roles you want to assign to the user, then move it to the Assigned list, then click OK.

   The administrative role you selected is assigned to the user.

## Specify the Users That Have the Administrative Role

To let a user perform specified actions in a specific security domain, you can assign a user to an administrator role. You can assign multiple users to an administrative role at the same time.

**To specify the users that have the administrative role**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to specify the users that have the administrative role and then select Content.

   The Endpoint Content dialog appears.
4. Select Administrative Roles in the Object Type list and click then click Search.

   The administrative roles appear in the list view.
5. Right click the administrative role you want to add users to, then click Properties.

   The Administrative Roles dialog appears.
6. Click the Administrator roles tab.

   The users that are assigned the administrative roles appear in the Assigned list, and the containers in the namespace you can search appear in the Available List Search tree.
7. Search for the administrative roles you want to assign to the user. (see page 440)

   The administrative roles assigned to the user account appear in the Available list.
8. In the Available list, select the user or users you want to assign to the administrative role then move it to the Assigned list, then click OK.

   Both local and trusted users appear in the Available list. Verify that you select the correct user type before you move it to the Assigned list. For more information, see Local and Remote User Support (see page 435).

   The user you specified is added to the administrative role.

## How to Remove an Administrative Role

To remove an administrative role use either of the following methods:

- Edit an individual user and remove the administrative roles you do not want the user to have (see page 460)
- Edit an administrative role and remove the users you do not want to have the administrative role (see page 461)

## Unassign an Administrative Role from a User Account

If you no longer want to manage the actions a user can perform in a specific security domain using an administrative role you can remove an administrative role from a user. You can remove multiple administrative roles from a user at the same time.

**To remove the administrative roles you do not want users to have**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you do not want administrative roles a user to have and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select the Security Domain you want to search.
5. Select User Account in the Object Type list and click then click Search.

   The accounts for the system domain you selected appear in the list view.
6. Right click the user account you want to assign and administrative role, then click Properties.

   The User Account dialog appears.
7. Click the Administrative Roles tab.

   The administrative roles that the user is assigned appear in the Assigned list, and the containers in the namespace you can search appear in the Available List Search tree.
8. Search for the administrative roles you want to unassign from a user. (see page 440)

   The administrative roles assigned to the user account appear in the Assigned list.
9. In the Assigned list, select the administrative role or administrative roles you want to remove from the user, then move it to the Available list, then click OK.

   The administrative role is removed from the user.

## Unassign a User Account Assigned to an Administrative Role

If you no longer want to manage the actions a user can perform in a specific security domain using an administrative role you can remove a user from an administrator role. You can remove multiple users from an administrative role at the same time.

**To remove users from an administrative role**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to remove users from an administrative role and then select Content.

   The Endpoint Content dialog appears.
4. Select Administrative Roles in the Object Type list and click then click Search.

   The administrative roles appear in the list view.
5. Right click the administrative role you want to remove users from, then click Properties.

   The Administrative Roles dialog appears.
6. Click the Administrator roles tab.

   The users that are assigned the administrative role appear in the Assigned list, and the containers in the namespace you can search appear in the Available List Search tree.
7. Search for the administrative roles you want to unassign from the user. (see page 440)

   The administrative roles assigned to the user account appear in the Assigned list.
8. In the Assigned list, select the user or users you want to unassign from the administrative role then move it to the Available list, then click OK.

   The user is removed from the administrative role.

## Manage Groups

The RSA 7.1 SecurID connector supports the following user group management operations:

- Creating groups
- Editing groups
- Adding and removing users to or from groups
- Make groups members of other groups
- Creating trusted groups
- Associating groups with authentication agents
- Removing group members from groups
- Associating trusted groups with authentication agents

**More Information:**

Create a User Group (see page 463)
How to Add Users to Groups (see page 465)
How you Remove Users from Groups (see page 467)
Edit a Group (see page 464)
Create a Trusted Group (see page 473)
Edit a Trusted Group (see page 474)
Associate a Trusted Group with Authentication Agent (see page 476)

## Create a User Group

You can organize users into groups based on your specific business needs, for example, locations, business departments or job title. You can also create user groups that contain other user groups, for example, a user group named Melbourne that contains a group named Technical Writers. The members of groups that contain other groups are named group members.

**To create a user group**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint you want to create a trusted user on and then select Content.

   The Endpoint Content dialog appears.
4. Select the System Domain container in the Container tree.
5. Select Group in the Object Type list and click New.

   The Group dialog General 1 tab appears.
6. On the General 1 tab, specify the basic details of the group you want to create.
7. On the Access Times (UTC/GMT) tab, specify the times when the members of a user group can authenticate.
8. On the Identity Source tab, specify the identity source you want to add the user group to.
9. On the Group Members tab, add a user group to the group.
10. On the Authentication tab, specify the user groups access to specific authentication agents.
11. On the User Members tab, search for the user you want to add to the group, then add it to the group.
12. Click Ok.

    The user group you specified is created.

## Edit a Group

To modify the details of a group, such as the times when members of a user group can authenticate, the groups the group belongs to, the groups access to specific authentication agents, and the members of a group, edit the group.

**Note:** The identity source where the group is assigned is read-only. You can only specify an identity source for a group when you create the group.

**To edit a group**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to edit a group, and then select Content.

   The Endpoint Content dialog appears.
4. Select the System Domain container in the Container tree.
5. Select Group in the Object Type list and click Search.

   The list of groups appears in the list view.
6. Right click the group you want to change, then click Properties.

   The Group dialog General 1 tab appears.
7. On the General 1 tab, modify the basic details of the group you want to create.
8. On the Access Times (UTC/GMT) tab, specify the times when the members of a group can authenticate.
9. On the Group Members tab, modify the group the group belongs to.
10. On the Authentication tab, modify the groups access to specific authentication agents.
11. On the User Members tab, search for the user you want to add to the group, then add it to the group.
12. Click Ok.

    The details of the user are modified.

## Move a Trusted Group into a Different Security Domain

If you want to manage a trusted group under a different security domain, you can move the trusted group to another security domains within the realm.

**To move a trusted group into a different security domain**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurId 7 [DYN Endpoint] type in the Object Type drop-down list .
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to move a trusted group and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select the Security Domain you want to search.
5. Select Trusted Group in the Object Type box and click then click Search.

   The trusted groups for the system domain you selected appear in the list view.
6. Right-click a trusted group in the list view and then click Move.

   The Move in Hierarchy dialog appears.
7. Select the Security Domain you want to move the trusted group into.
8. Click OK.

   The trusted group is moved into the security domain you selected.

## How to Add Users to Groups

To add users to groups you can do either of the following:

- Edit an individual user and specify which groups the user is a member of (see page 466)
- Edit a group and specify the members of the group (see page 467)

## Specify the Groups a User is a Member of

To manage users as group, you can add users to groups.

**To specify the groups a user is a member of**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to add user groups and then select Content.

   The Endpoint Content dialog appears.
4. Select the System Domain container in the Container tree.
5. Select Group in the Object Type list and click Search.

   The list of groups appears in the list view.
6. Right click the group you want to change, then click Properties.

   The Group dialog General 1 tab appears.
7. Click the User Members tab.
8. Search for the users you want to add to the group. (see page 440)

   The users you can assign to the group appear in the Available list.
9. In the Available list, select the user or users you want to add to the group, then move the user or users to the Assigned list, then click OK.

   **Note:** Both local and trusted users appear in the Available list. Verify that you select the correct user type before you move it to the Assigned list. For more information, see Local and Remote User Support (see page 435).

   The users you selected are added to the group.

## Specify the Members of a Group

To manage users as group, you can assign a user to a group.

**To assign a user to a group**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint where you want to add users to a group and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select the Security Domain you want to search.
5. Select User Account in the Object Type list and click then click Search.

   The accounts for the system domain you selected appear in the list view.
6. Right-click an account in the list view and then click Properties.

   The User Account dialog appears.
7. Click the Member of tab.
8. Search for the groups you want to add the user to. (see page 440)

   The groups you can assign the user account to appear in the Available list.
9. In the Available list, select the group or groups you want the user to belong to, then move the group to the Assigned list, then click OK.

   The user is made a member of the groups you selected.

## How you Remove Users from Groups

To remove users from groups, you can do either of the following:

- Edit an individual user and remove the group the user is a member of  (see page 469)
- Edit a group and remove the user from the group (see page 468)

## Remove the Group the User is a Member of

If you you no longer want to manage a user as part of a group, you can remove the group or groups a user is a member of.

**To remove the group a user is a member of**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to remove a group a user is a member of,  and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select the Security Domain you want to search.
5. Select User Account in the Object Type list and click then click Search.

   The accounts for the system domain you selected appear in the list view.
6. Right-click an account in the list view and then click Properties.

   The User Account dialog appears.
7. Click the Member of tab.

   The groups that the user belongs to appear in the Assigned list.
8. In the Assigned list, select the group or groups you want to remove the user from, then move the group to the Available list, then click OK.

   The groups the user is a member of are removed.

## Remove the User from a Group

If you you no longer want to manage a user as part of a group, you can remove the user from a groups they are a member of.

**To remove a user from a group**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to remove users from a group, and then select Content.

   The Endpoint Content dialog appears.
4. Select the System Domain container in the Container tree.
5. Select Group in the Object Type list and click Search.

   The list of groups appears in the list view.
6. Right click the group you want to remove members from, then click Properties.

   The Group dialog General 1 tab appears.
7. Click the User Members tab.

   The users that are members of the group appear in the Assigned list.
8. In the Assigned list, select the user or users you want to remove from the group, then move the user or users it to the Available list, then click OK.

   The user you selected is removed from the group.

## Make Groups Members of Other Groups

To manage collections of groups, you can make groups members of other groups. For example, you can make the groups Melbourne and Sydney Technical Writers part of the Technical Writers Australia group.

**To make groups members of other groups**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to make groups members of other groups and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select the security domain where the group you want to add to another group is located.
5. In the Object Type list, select Group, then click Search.

   The Group dialog appears.
6. Select Group in the Object Type list and click Search.

   The list of groups appears in the list view.
7. Right click the group you want to changes, then click Properties.

   The Group dialog General 1 tab appears.
8. Click the Group Members tab.
9. Search for the group you want to add to the group. (see page 440)

   The groups you can add to the group appear in the Available list.
10. Select the group or groups you want to add to the group, then move the group or groups to the Assigned list, then click OK.

    The groups you selected are added to the group.

## Remove Group Members from Groups

If you no longer want to manage a group that is part of another group, you can remove group members from groups. For example, you could remove the Melbourne Sales group from the Australian Sales group.

**To remove groups members from groups**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to remove groups members from groups and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select the security domain where the group you want to add to another group is located.
5. In the Object Type list, select Group, then click Search.

   The Group dialog appears.
6. Select Group in the Object Type list and click Search.

   The list of groups appears in the list view.
7. Right click the group you want to changes, then click Properties.

   The Group dialog General 1 tab appears.
8. Click the Group Members tab.

   The groups that the group is a member of appear in the Assigned list.
9. In the Assigned list, select the group or groups you want to remove from the group, then move the group or groups to the Available list, then click OK.

   The groups you selected are removed from the group.

## Associate a Group with Authentication Agent

You can specify the authentication agents you want to give the group permission to access.

**To associate a group with an authentication agent**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to associate a group with an authentication agent and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select the security domain where the group you want to add to another group is located.
5. In the Object Type list, select Group, then click Search.

   The Group dialog appears.
6. Select Group in the Object Type list and click Search.

   The list of groups appears in the list view.
7. Right click the group you want to change, then click Properties.

   The Group dialog General 1 tab appears.
8. Click the Authentication Agent tab.
9. Search for the authentication agent you want to give the group permission to access. (see page 440)

   The authentication agents you can assign to the group appear in the Available list.
10. In the Available list, select the authentication agent or agents you want to assign to the group, then move the agent or agents to the Assigned list, then click OK.

    You have associated the authentication agent with the group.

## Create a Trusted Group

To manage trusted users as a trusted group, you can create a trusted group and specify its members.

**To create a trusted group**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to create a trusted group and then select Content.

   The Endpoint Content dialog appears.
4. Select the System Domain container in the Container tree.
5. Select Trusted Group in the Object Type list and click New.

   The Trusted Group dialog General 1 tab appears.
6. On the General 1 tab, specify the basic details of the trusted group you want to create.
7. On the Access Times (UTC/GMT) tab, specify the times when the members of a trusted user group can authenticate.
8. On the Authentication tab, search for the authentication agents you want the trusted group to authenticate with.
9. On the Trusted User Members tab, search for the user you want to add to the trusted group, then add it to the trusted group.
10. Click Ok.

    The trusted group is created.

## Edit a Trusted Group

If the details of trusted group change, for example, the authentication agents the group can use to authenticate, the times when members of a trusted user group can authenticate, the members of the trusted group, you can edit the details of the trusted group.

**To edit a trusted group**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to edit a trusted group and then select Content.

   The Endpoint Content dialog appears.
4. Select the System Domain container in the Container tree.
5. Select Trusted Group in the Object Type list and click Search.

   The list of trusted groups appears in the list view.
6. Right click the trusted group you want to change, then click Properties.

   The Trusted Group dialog General 1 tab appears.
7. On the General 1 tab, modify the basic details of the trusted group you want to create.
8. On the Access Times (UTC/GMT) tab, modify the times when the members of a trusted user group can authenticate.
9. On the Authentication tab, modify the authentication agents you want the trusted group to authenticate with.
10. On the Trusted User Members tab, modify the users you want to add to the trusted group, then add it to the trusted group.
11. Click Ok.

    The details of the trusted group are modified.

## Move a Group into a Different Security Domain

If you want to manage a group under a different security domain, you can move the group to another security domains within the realm.

**To move a group into a different security domain**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurId 7 [DYN Endpoint] type in the Object Type drop-down list .
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to move a group and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select the Security Domain you want to search.
5. Select Group in the Object Type box and click then click Search.

   The groups for the system domain you selected appear in the list view.
6. Right-click a group in the list view and then click Move.

   The Move in Hierarchy dialog appears.
7. Select the Security Domain you want to move the group into.
8. Click OK.

   The group is moved into the security domain you selected.

## Associate a Trusted Group with Authentication Agent

To specify the authentication agents you want to give a trusted group permission to access, you can associate a trusted group with an authentication agent.

**To associate a trusted group with an authentication agent**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to associate a trusted group with an authentication agent, and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select the security domain where the trusted group you want to associate with an authentication agent is located.
5. In the Object Type list, select Trusted Group, then click Search.

   The Trusted Group dialog appears.
6. Select Trusted Group in the Object Type list and click Search.

   The list of trusted groups appears in the list view.
7. Right click the trusted group you want to change, then click Properties.

   The Trusted Group dialog General 1 tab appears.
8. Click the Authentication Agents tab.
9. Search for the authentication agent you want to give the trusted group permission to access. (see page 440)

   The authentication agents you can assign to the trusted group appear in the Available list.
10. In the Available list, select the authentication agent or agents you want to assign to the trusted group, then move the agent or agents to the Assigned list, then click OK.

    The authentication agent is associated with the trusted group.

## RADIUS Profiles Management

The RSA 7.1 SecurID connector supports the following RADIUS Profile management operations:

- Creating, editing, modifying and deleting a RADIUS profile
- Assigning and unassigning RADIUS Profiles to users
- Assigning and unassigning RADIUS Profiles to trusted users

**More information:**

How to Assign a User to a RADIUS Profile (see page 477)
How to Unassign RADIUS Profiles from Users (see page 479)
How to Assign a Trusted User to a RADIUS Profile (see page 481)
How to Unassign a Trusted User from a RADIUS Profile (see page 483)
Remove Trusted Users from an Existing RADIUS Profile (see page 485)
Associate a RADIUS Profile with an Authentication Agent (see page 486)
Create a RADIUS Profile (see page 487)
Edit a RADIUS Profile (see page 488)
Delete a RADIUS Profile (see page 489)

## How to Assign a User to a RADIUS Profile

You can assign a RADIUS profile to a user in either of the following ways:

- Assign a RADIUS profile to a user (see page 478)
- Add users to an existing RADIUS profile (see page 479)

## Assign a RADIUS Profile to a User

To specify the session requirements for a user that requests remote network access, you can assign a RADIUS profile to the user.

**To assign a RADIUS profile to a user**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to assign a RADIUS profile to a user and then select Content.

   The Endpoint Content dialog appears.
4. Select RADIUS profiles in the Container tree and then click Search.

   The RADIUS profiles for the system domain you selected appear in the list view.
5. Right-click a RADIUS Profile in the list view and then click Properties.

   The RADIUS Profile dialog appears.
6. Click the Users tab.

   Search for the users you want to assign a RADIUS profile to. (see page 440)

   The users you can assign to the RADIUS profile appear in the Available list, and the users assigned to the profile appear in the Assigned list.
7. In the Available list, select the user or users you want to assign to the RADIUS Profile, then move them to the Assigned list, then click OK.

   The RADIUS profile is assigned to the user.

## Add Users to an Existing RADIUS Profile

To specify the session requirements for a user that requests remote network access, you can add users to an existing RADIUS profile.

**To add users to an existing RADIUS profile**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to add users to an existing RADIUS profile and then select Content.

   The Endpoint Content dialog appears.
4. Select a security domain in the Container tree and then in the Object Type list, select User Account.
5. Click Search.

   The users in the system domain you selected appear in the list view.
6. Right-click a user in the list view and then click Properties.

   The User Account dialog appears.
7. Click the RADIUS Profiles tab.
8. Search for the RADIUS profiles you want add the user too. (see page 440)
9. The RADIUS profiles you can assign to the user appear in the Available list, and the RADIUS profiles assigned to the user appear in the Assigned list.
10. In the Available list, select the RADIUS profile or profiles you want to assign to the user, then move them to the Assigned list, then click OK.

    The user is added to the RADIUS profile.

## How to Unassign RADIUS Profiles from Users

You can unassign a RADIUS profile from a user in either of the following ways:

- Unassign a RADIUS profile from a user (see page 480)
- Remove users from an existing RADIUS profile (see page 481)

## Unassign a User from a RADIUS Profile

If you no longer want to manage the session requirements for a user that requests remote network access using a RADIUS profile, you can unassign a user from a RADIUS profile.

**To unassign a RADIUS profile from a user**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to unassign a RADIUS profile from a user and then select Content.

   The Endpoint Content dialog appears.
4. Select a security domain in the Container tree and then in the Object Type list, select User Account.
5. Click Search.

   The users in the system domain you selected appear in the list view.
6. Right-click a user in the list view and then click Properties.

   The User Account dialog appears.
7. Click the RADIUS Profiles tab.

   The users assigned to the RADIUS profiles appear in the Assigned list.
8. In the Assigned list, select the user or users you want to unassign from the RADIUS profile, then move them to the Available list, then click OK.

   The RADIUS profile is unassigned from the user.

## Remove Users from an Existing RADIUS Profile

If you no longer want to manage the session requirements for a user that requests remote network access using a RADIUS profile, you can can remove users from an existing RADIUS profile.

**To remove users from an existing RADIUS profile**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to remove users from an existing RADIUS profile and then select Content.

   The Endpoint Content dialog appears.
4. Select RADIUS profiles in the Container tree and then click Search.

   The RADIUS profiles for the system domain you selected appear in the list view.
5. Right-click a RADIUS Profile in the list view and then click Properties.

   The RADIUS Profile dialog appears.
6. Click the Users tab.

   The users assigned to the RADIUS profile appear in the Assigned list.
7. In the Assigned list, select the user or users you want to unassign from the RADIUS Profile, then move them to the Available list, then click OK.

   The RADIUS profile is removed from the user.

## How to Assign a Trusted User to a RADIUS Profile

You can assign a RADIUS profile to a trusted user in either of the following ways:

- Assign a RADIUS profile to a trusted user (see page 482)
- Assign trusted users to an existing RADIUS profile (see page 483)

## Assign a RADIUS Profile to a Trusted User

To specify the session requirements for a trusted user that requests remote network access, you can assign a RADIUS profile to the trusted user.

**To assign a RADIUS profile to a trusted user**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to remove users from an existing RADIUS profile and then select Content.

   The Endpoint Content dialog appears.
4. Select RADIUS profiles in the Container tree and then click Search.

   The RADIUS profiles for the system domain you selected appear in the list view.
5. Right-click a RADIUS Profile in the list view and then click Properties.

   The RADIUS Profile dialog appears.
6. Click the Trusted Users tab.
7. Search for the trusted users you want to assign the RADIUS profile to. (see page 440)

   The trusted users you can assign to the RADIUS profile appear in the Available list, and the trusted users assigned to the profile appear in the Assigned list.
8. In the Available list, select the trusted user or trusted users you want to assign to the RADIUS Profile, then move them to the Assigned list, then click OK.

   The RADIUS profile is assigned to the trusted user.

## Assign Trusted Users to an Existing RADIUS Profile

To specify the session requirements for a trusted user that requests remote network access, you can add trusted users to an existing RADIUS profile.

**To add trusted users to an existing RADIUS profile**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to add trusted users to an existing RADIUS profile and then select Content.

   The Endpoint Content dialog appears.
4. Select a security domain in the Container tree and then in the Object Type list, select User Account.
5. Click Search.

   The users in the system domain you selected appear in the list view.
6. Right-click a trusted user in the list view and then click Properties.

   The Trusted User Account dialog appears.
7. Click the RADIUS Profiles tab.
8. Search for the RADIUS profiles you want add the trusted user too. (see page 440)

   The RADIUS profiles you can assign to the trusted user appear in the Available list, and the RADIUS profiles assigned to the trusted user appear in the Assigned list.
9. In the Available list, select the RADIUS profile or profiles you want to assign to the trusted user, then move them to the Assigned list, then click OK.

   The trusted users are added to the RADIUS profile.

## How to Unassign a Trusted User from a RADIUS Profile

You can unassign a RADIUS profile from a trusted user in either of the following ways:

- Unassign a RADIUS profile from a trusted user (see page 484)
- Remove a trusted user from an existing RADIUS profile (see page 485)

## Unassign a Trusted User from a RADIUS Profile

If you no longer want to manage the session requirements for a trusted user that requests remote network access using a RADIUS profile, you can unassign a RADIUS profile from a trusted user.

**To unassign a RADIUS profile from a trusted user**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to unassign a RADIUS profile from a trusted user in the list view and then select Content.

   The Endpoint Content dialog appears.
4. Select a security domain in the Container tree and then in the Object Type list, select Trusted User Account.
5. Click Search.

   The trusted users in the system domain you selected appear in the list view.
6. Right-click a trusted user in the list view and then click Properties.

   The trusted User Account dialog appears.
7. Click the RADIUS Profiles tab.

   The trusted users assigned to the RADIUS profiles appear in the Assigned list.
8. In the Assigned list, select the trusted user or trusted users you want to unassign from the trusted user, then move them to the Available list, then click OK.

   You have unassigned the RADIUS profile from the trusted user.

## Remove Trusted Users from an Existing RADIUS Profile

If you no longer want to manage the session requirements for a trusted user that requests remote network access using a RADIUS profile, you can remove a trusted user from an existing RADIUS profile.

**To remove trusted users from an existing RADIUS profile**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to remove trusted users from an existing RADIUS profile and then select Content.

   The Endpoint Content dialog appears.
4. Select RADIUS profiles in the Container tree and then click Search.

   The RADIUS profiles for the system domain you selected appear in the list view.
5. Right-click a RADIUS Profile in the list view and then click Properties.

   The RADIUS Profile dialog appears.
6. Click the Trusted Users tab.

   The users assigned to the RADIUS profile appear in the Assigned list.
7. Select the trusted user or trusted users you want to unassign from the RADIUS Profile, then move them to the Available list, then click OK.

   The RADIUS profile is removed from the trusted user.

## Associate a RADIUS Profile with an Authentication Agent

To specify the session requirements for a users requesting remote network access using a specific authentication agent, you can associate a RADIUS profile with an Authentication Agent. The RADIUS profile is applied to all users that request remote network access using the specific authentication agent.

**To associate a RADIUS profile with an authentication agent**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to associate a RADIUS profile with an authentication agent and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select RADIUS Profiles, then click Search.

   The list of RADIUS Profiles appears in the list view.
5. Right click the RADIUS profile group you want to associate with an authentication agent, then click Properties.

   The RADIUS Profile dialog appears.
6. Click the Authentication Agents tab.
7. Search for the authentication agent you want to associate with a RADIUS profile. (see page 440)

   The authentication agents you can assign to the RADIUS Profile appear in the Available list.
8. In the Available list, select the authentication agent or agents you want to associate with the RADIUS profile, then move the agent or agents to the Assigned list, then click OK.

   The authentication agent is associated with the RADIUS profile.

## Create a RADIUS Profile

To specify the session requirements for users that request remote network access, you can create a RADIUS profile.

**To create a RADIUS profile**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to assign a RADIUS profile to a user and then select Content.

   The Endpoint Content dialog appears.
4. Select the RADIUS Profiles container in the Container tree, then click New.

   The RSA SecureID 7 RADIUS Profile dialog appears General 1 tab appears.
5. Complete the fields on the General 1 tab.

   You have defined the details of a RADIUS profile.
6. Click the Users tab.
7. Search for the users you want to assign the RADIUS profile to. (see page 440)

   The users you can assign to the RADIUS profile appear in the Available list.
8. In the Available list, select the user or users you want assign to the RADIUS profile, and then move the users to the Assigned list, then click OK.

   You have assigned the select users to RADIUS profiles.
9. Click the Authentication Agents tab.
10. Search for the authentication agents users you want to assign to the RADIUS profile to. (see page 440)

    The authentication agents you can assign to the RADIUS profile appear in the Available list.
11. In the Available list, select the authentication agent or agents you want assign to the RADIUS profile, and then move the authentication agents to the Assigned list.

    You have assigned the select authentication agents to RADIUS profiles.
12. Click OK.

    You have created the RADIUS profile.

## Edit a RADIUS Profile

To modify the session requirements for users that request remote network access, you can modify a RADIUS profile.

**To edit a RADIUS profile**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to assign a RADIUS profile to a user and then select Content.

   The Endpoint Content dialog appears.
4. Select the RADIUS Profiles container in the Container tree, then click Search.

   The RADIUS Profiles for the system domain you selected appear in the list view.
5. Right-click an RADIUS profile in the list view and then click Properties.

   The RSA SecureID 7 RADIUS Profile dialog General 1 tab appears.
6. Edit the fields on the General 1 tab.

   You have defined the details of a RADIUS profile.
7. Click the Users tab.

   The users that are assigned to the RADIUS profile appear in the Assigned list.
8. In the Assigned list, select the user or users you want to unassign from the RADIUS Profile, then move them to the Available list, then click OK.

   You have assigned the select users to RADIUS profiles.
9. Click the Authentication Agents tab.

   The Authentication Agents tab appears.

   The authentication agents that are assigned to the RADIUS profile appear in the Assigned list.
10. In the Assigned list, select the agent or agents you want to unassign from the RADIUS Profile, then move them to the Available list,

    You have edited the select authentication agents assigned to the RADIUS profile.
11. Click OK.

    You have edited the RADIUS profile.

## Delete a RADIUS Profile

If you you no longer want to manage the session requirements of users by using a RADIUS profile, you can delete the RADIUS profile.

**To delete a RADIUS profile**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to assign a RADIUS profile to a user and then select Content.

   The Endpoint Content dialog appears.
4. Select the RADIUS Profiles container in the Container tree, then click Search.

   The RADIUS Profiles for the system domain you selected appear in the list view.
5. Right-click a RADIUS profile in the list view then click Delete.
6. When prompted, confirm that you want to delete the RADIUS profile.

   You have deleted the RADIUS profile.

## Security Domain Management

The RSA 7.1 SecurID connector supports creating, modifying, or deleting security domains.

**More information:**

Create a Security Domain (see page 490)
Update a Security Domain (see page 491)
Delete a Security Domain (see page 492)

## Create a Security Domain

To represent your companies business structure in a hierarchical tree, you can create security domains in a specified realm.

**To create a security domain**

1. Click the Endpoints task button and select the RSA SecurID 7 [DYN Endpoint] in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to create a security domain and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, click the realm where you want to create the security domain.
5. Select Security Domain in the Object Type list and click New.

   The Security Domain dialog General 1 tab appears.
6. On the General 1 tab, specify the name of the security domain you want to create.
7. On the Password Policy tab, assign a password policy to the security domain.
8. On the Self service troubleshooting policy tab, assign a Self service troubleshooting policy to the security domain.
9. On the Default authentication grade policy tab, assign an authentication grade policy to the security domain.
10. On the SecurID Token Policy tab, assign a SecurID token policy to the security domain.
11. On the Off-line authentication policy tab, assign an off-line authentication policy to the security domain.
12. Click Ok.

    The security domain is created in the realm you specified.

## Update a Security Domain

To update the details of your companies business structure and policies, you can update the details of a security domain.

**To update a security domain**

1. Click the Endpoints task button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to enable or disable PINS and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, click the realm where you want to create the security domain.
5. Select Security Domain in the Object Type list and click Search.

   The Security Domains for the endpoint you specified appear in the list view.

   In the list view, right-click the security domain you want to update, then click Properties.

   The Security Domain dialog appears.
6. Update the fields on the tabs on the Security Domain dialog as required, then click OK.

   You have updated the details of the selected security domain.

## Delete a Security Domain

If your companies business structure or policies change, you can delete the appropriate security domain. A security domain must be empty of all objects before it can be deleted, for example, users, groups, and administrative roles.

**To delete a security domain**

1. Click the Endpoints task button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to delete a security domain and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, click the realm where you want to delete the security domain.
5. Select Security Domain in the Object Type list and click Search.

   The Security Domains for the endpoint you specified appear in the list view.
6. In the list view, right-click the security domain you want to delete, then click Delete.
7. When prompted, confirm that you want to delete the security domain.

   The security domain is deleted.

## Token Management

The RSA 7.1 SecurID connector supports the following Token management operations:

- Assigning and unassigning tokens
- Update and deleting tokens
- Enabling and disabling tokens
- Replacing tokens
- Enabling and clearing PINS
- Requesting PIN changes

**More Information:**

Assign a Token to a User (see page 494)
Unassign Tokens (see page 495)
Update Tokens (see page 496)
Delete Tokens (see page 497)
Disable Tokens (see page 499)
Enable Tokens (see page 498)
How to Replace Tokens (see page 499)
Replace Tokens (see page 500)
Replace a Users Token with a Token you Specify (see page 501)
Replace a Selected Token with a Token you Specify (see page 502)
Enable or Disable PINs (see page 503)
Clear PINs (see page 504)
Request PIN Change (see page 505)

## Assign a Token to a User

If you want a user to authenticate using a token, assign a token to the user.

**To assign a token to a user**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to a token to a user and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select the Security Domain you want to search.
5. Select User Account in the Object Type list and click then click Search.

   The accounts for the system domain you selected appear in the list view.
6. Right-click an account in the list view and then click Properties.

   The User Account dialog appears.
7. Click the SecurID Tokens tab.

   The tokens that the user is assigned appear in the Assigned list, and the containers in the namespace you can search appear in the Available List Search tree.
8. Search for the tokens you want to assign to the user. (see page 440)

   The tokens you can assign to the user account appear in the Available list.
9. In the Available list, select the token you want to assign to the user, then move it to the Assigned list, then click OK.

   The selected token is assigned to the user.

## Unassign Tokens

If you no longer want a user to authenticate using a token, you can unassign the token from the user.

**To unassign tokens**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to unassign tokens and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select the Security Domain you want to search.
5. Select User Account in the Object Type list and click then click Search.

   The accounts for the system domain you selected appear in the list view.
6. Right-click an account in the list view and then click Properties.

   The User Account dialog appears.
7. Click The SecurID Tokens tab.

   The tokens roles that the user is assigned appear in the Assigned list, and the containers in the namespace you can search appear in the Available List Search tree.
8. Search for the tokens you want to unassign from the user. (see page 440)

   The tokens assigned to the user account appear in the Assigned list.
9. In the Assigned list, select the token you want to unassign from the user, then move it to the Available list, then click OK.

   The selected token is unassigned from the user.

## Update Tokens

You can update information about token codes, such as whether the token requires the user to enter their SecurID PIN, or whether the user is required to change the SecurID PIN the next time they authenticate with the token. You can also do the following:

- Enable or disable the token
- Clear the SecurID PIN
- Specify the token you want to replace this token with
- Replace a selected token with the current token
- Create, edit, or delete one-time tokencodes

**To update tokens**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to update tokens and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select the Security Domain you want to search.
5. Select Token in the Object Type list and click then click Search.

   The tokens for the system domain you selected appear in the list view.
6. Right-click a token in the list view and then click Properties.

   The Token dialog appears.
7. Update the information you require, then click OK.

   The selected token is updated.

## Delete Tokens

To delete a token, you can remove it from the internal database.

**To delete a token**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to delete a token and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select the Security Domain you want to search.
5. Select Token in the Object Type list and click then click Search.

   The tokens for the system domain you selected appear in the list view.
6. Right-click a token in the list view and then click Delete.
7. When prompted, confirm that you want to delete the token code.

   The token is removed from the system and can no longer be assigned. If the token is assigned to user, the user cannot use the token to authenticate.

## Enable Tokens

To let a user authenticate with a token they are assigned, enable the token.

**To enable tokens**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to enable a token and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select the Security Domain you want to search.
5. Select Token in the Object Type list and click then click Search.

   The tokens for the system domain you selected appear in the list view.
6. Right-click a token in the list view and then click Properties.

   The Token dialog appears.
7. Click the General 1 tab.
8. Select the Enabled Status check box, then click Apply.

   The user that is assigned the token can now use the token to authenticate.

## Disable Tokens

If you no longer want a user to authenticate using the token they are assigned, disable the token.

**To disable tokens**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to disable tokens and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select the Security Domain you want to search.
5. Select Token in the Object Type list and click then click Search.

   The tokens for the system domain you selected appear in the list view.
6. Right-click a token in the list view and then click Properties.

   The Token dialog appears.
7. Click the General 1 tab.
8. Clear the Enabled Status check box, then click Apply.

   The user that is assigned the token can no longer use the token to authenticate.

## How to Replace Tokens

You can put a token in one of the following replacement modes:

- Has a replacement token
- Is a replacement token

You can put a token in replacement mode in either of the following ways:

- Replace a users token with a token assigned by the RSA Server (see page 500)
- Replace a users token with a token you specify (see page 501)
- Replace a selected token with a token you specify (see page 502)

**Note:** You can put a token in only one token replacement mode at a time.

## Replace Tokens

To replace a users token that has been lost or has expired, you can replace the users token with a token assigned by the RSA Server.

**To replace tokens**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to replace tokens and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select the Security Domain you want to search.
5. Select Token in the Object Type list and click then click Search.

   The tokens for the system domain you selected appear in the list view.
6. Right-click a token in the list view and then click Properties.

   The Token dialog appears.
7. Click the General 1 tab.
8. Select the Replace with next available token check box, then click OK.

   The RSA Server assigns the next available token to the user. The token is put in *Has a replacement token mode*. The Replacement mode field on the General 1 tab displays Has a replacement token.

## Replace a Users Token with a Token you Specify

To replace a users token that has been lost or has expired, you can replace a users token with a with a token you specify.

**To replace a users token with a token you specify**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to replace a users token with a token you specify and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select the Security Domain you want to search.
5. Select Token in the Object Type list and click then click Search.

   The tokens for the system domain you selected appear in the list view.
6. Right-click a token in the list view and then click Properties.

   The Token dialog appears.
7. Click the Replacement by Token tab.

   The tokens that the user is assigned appear in the Assigned list, and the containers in the namespace you can search appear in the Available List Search tree.
8. Search for the tokens you want to replace with a specific token. (see page 440)

   The tokens you can assign to the user account appear in the Available list.
9. In the Available list, select the token you want to replace, then move it to the Assigned list, then click OK.

   The users token is replaced. The token is put in *Has a replacement token mode*. The Replacement mode field on the General 1 tab displays Has a replacement token.

## Replace a Selected Token with a Token you Specify

You can replace a selected token with a token you specify. Users that were assigned the token you selected are assigned the new token you specified.

**To replace a selected token with a token you specify**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to replace a selected token with a token you specify and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select the Security Domain you want to search.
5. Select Token in the Object Type list and click then click Search.

   The tokens for the system domain you selected appear in the list view.
6. Right-click a token in the list view and then click Properties.

   The Token dialog appears.
7. Click the Will Replace Token tab.

   The tokens that the user is assigned appear in the Assigned list, and the containers in the namespace you can search appear in the Available List Search tree.
8. Search for the tokens you want to replace (see page 440).

   The tokens that you can replace with the current token appear in the Available list.
9. in the Available list, select the token you want to replace the current token with, then move it to the Assigned list, then click OK.

   The current token is replaced with the token you selected.

   The token is put in *Is a replacement token mode*. The connector updates the Replacement mode field on the General 1 tab and displays Is a replacement token.

## Enable or Disable PINs

To specify whether a user must enter a PIN and their token code when they authenticate, you can enable or disable PINS.

**To enable or disable PINS**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to enable or disable a PIN and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select the Security Domain you want to search.
5. Select Token in the Object Type list and click then click Search.

   The tokens for the system domain you selected appear in the list view.
6. Right-click a token in the list view and then click Properties.

   The Token dialog appears.
7. Click the General 2 tab.
8. Select or clear the PIN is set check box.

   Users that are assigned the token code you modified may have to enter a PIN and their token code when they authenticate, depending on whether you enabled or disabled the PIN.

## Clear PINs

To specify that a user has to enter a tokencode and  has to create a PIN when they next authenticate, you can clear the users current PIN.

**To clear a PIN**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.
3. The RSA 7.1 endpoints appear in the list view.

   Right-click the endpoint on which you want to clear a PIN view and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select the Security Domain you want to search.
5. Select Token in the Object Type list and click then click Search.

   The tokens for the system domain you selected appear in the list view.
6. Right-click a token in the list view and then click Properties.

   The Token dialog appears.
7. Click the General 2 tab.
8. Select the Clear PIN check box.

   The SecurID PIN assigned to a users logon is cleared. The user is required to enter a tokencode and is prompted to create a PIN when they next authenticate.

## Request PIN Change

To specify that the user must change their PIN at the next logon, you can request a PIN change.

**To request a PIN change**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to request a PIN change and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select the Security Domain you want to search.
5. Select Token in the Object Type list and click then click Search.

   The tokens for the system domain you selected appear in the list view.
6. Right-click a token in the list view and then click Properties.

   The Token dialog appears.
7. Click the General 2 tab.
8. Select the PIN change at next logon check box, then click OK.

   The PIN assigned to a users logon is cleared. The user is required to enter a tokencode and is prompted to create a PIN when they next authenticate.

## RSA Read-only Objects

The following endpoint objects are read-only on the RSA 7.1 SecurID endpoint:

- Authentication agents (see page 506)
- Authentication grade policies (see page 507)
- Identity sources (see page 507)
- Lockout policies (see page 508)
- Off-line authentication policies (see page 508)
- Password policies (see page 508)
- Self-service troubleshooting policies (see page 510)
- Token policies (see page 509)
- Trusted realms (see page 511)

## View Authentication Agents

You can view the details of a selected authentication agent.

**To view authentication agents**

1. Click the Endpoints task button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to view authentication agents and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select the SystemDomain container.
5. Expand the System Domain container then select the system domain where you want to view authentication agents.
6. Click Search.

   The authentication agents for the endpoint you specified appear in the list view.
7. Right-click the authentication agents you want to view details for, then click Properties.

   The Authentication Agent dialog General 1 tab appears and displays the details of the selected authentication agent.

## View Authentication Grade Policies

You can view the authentication grade policies in a specified security domain.

**To view authentication grade policies**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to view authentication grade policies and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select the RSA Policies container in the Container tree.
5. In the Object list, select Authentication Grade, then click Search.

   The authentication grade policies for the endpoint you specified appear in the list view.
6. Right-click the authentication grade policy you want to view details for, then click Properties.

   The Authentication Grade dialog General 1 tab appears and displays the details of the selected authentication grade policy.

## View Identity Sources

You can view the details of a selected identity source.

**To view identity sources**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to view identity sources and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select the Identity Source container in the Container tree.
5. Click Search.

   The identity sources for the endpoint you specified appear in the list view.
6. Right-click the identity source you want to view details for, then click Properties.

   The Identity Source dialog General 1 tab appears and displays the details of the selected identity source.

## View Lockout Policies

You can view the lockout policies in a specified security domain.

**To view lockout policies**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to view lockout policies and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select the RSA Policies container in the Container tree.
5. In the Object list select Lockout Policy, then click Search.

   The lockout policies for the endpoint you specified appear in the list view.
6. Right-click the lockout policy you want to view details for, then click Properties.

   The Lockout Policy dialog General 1 tab appears and displays the details of the selected lockout policy.

## View Off-Line Authentication Policies

You can view the off-line authentication policies in a specified security domain.

**To view off-line authentication policies**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search

   The RSA 7.1 endpoints appear in the list view
3. Right-click the endpoint on which you want to view off-line authentication policies and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select the RSA Policies container in the Container tree.
5. In the Object list, select Off-line Authentication Policy, then click Search.

   The SecurID token policies for the endpoint you specified appear in the list view.
6. Right-click the off-line authentication policy you want to view details for, then click Properties.

   The Off-line authentication Policy dialog General 1 tab appears and displays the details of the selected off-line authentication policy.

## View Password Policies

You can view the password policies in a specified security domain.

**To view password policies**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to view password policies and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select the RSA Policies container in the Container tree.
5. In the Object list select Password Policy, then click Search.

   The Password Policies for the endpoint you specified appear in the list view.
6. Right-click the password policy you want to view details for, then click Properties.

   The Password Policies dialog General 1 tab appears and displays the details of the selected password policy.

## View SecurId Token Policies

You can view the SecurID token policies in a specified security domain.

**To view SecurID token policies**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to view SecurID policies and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select the RSA Policies container in the Container tree.
5. In the Object list, select SecurID Token Policy, then click Search.

   The SecurID token policies for the endpoint you specified appear in the list view.
6. Right-click the SecurID token policies policy you want to view details for, then click Properties.

   The SecurID Token Policies dialog General 1 tab appears and displays the details of the selected SecurID token policy.

## View Self-service Troubleshooting Password Policies

You can view the self-service troubleshooting password policies in a specified security domain.

**To view self-service troubleshooting password policies**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to view self-service troubleshooting password policies and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select the RSA Policies container in the Container tree.
5. In the Object list, select Self-service Password policies, then click Search.

   The self-service troubleshooting policies for the endpoint you specified appear in the list view.
6. Right-click the self-service password policy you want to view details for, then click Properties.

   The Self-service Troubleshooting Policy dialog General 1 tab appears and displays the details of the selected self-service troubleshooting policy.

## View RSA Trusted Realms

You can view the details of the trusted realms your realm is permitted to receive authentication requests from.

**To view trusted realms**

1. In the Provisioning Manager, click the Endpoints button and select the RSA SecurID 7 [DYN Endpoint] type in the Object Type drop-down list.
2. Click Search.

   The RSA 7.1 endpoints appear in the list view.
3. Right-click the endpoint on which you want to view trusted realms and then select Content.

   The Endpoint Content dialog appears.
4. In the Container tree, select the Trusted Realms container in the Container tree.
5. Click Search.

   The trusted realms for the endpoint you specified appear in the list view.
6. Right-click the trusted realm you want to view details for, then click Properties.

   The Trusted Realms dialog General 1 tab appears and displays the details of the selected trusted realm.

## Known Issues

This section contains the following known issues for the RSA SecurID 7 Connector.

- Non-English Character Support for RADIUS Profiles (see page 512)
- Attempting to Create a Security Domain Above the Top Level Security Domain Fails (see page 513)
- Attempting to Create a Security Domain Above the Top Level Security Domain Fails (see page 513)

**More information:**

Non-English Character Support  for RADIUS Profiles (see page 512)
RADIUS Profiles with Japanese Characters (see page 512)
Properties of RADIUS Profile Created with Japanese Characters (see page 512)
RADIUS Profiles with French Characters (see page 512)
Trusted Groups with More than 25 French or Japanese Characters (see page 512)
Attempting to Create a Security Domain Above the Top Level Security Domain Fails (see page 513)
Connector Data Migration Fails in Interactive Mode (see page 513)

## Non-English Character Support for RADIUS Profiles

The RSA 7 connector does not support non-English characters for RADIUS Profiles. The following are known issues with non-English character support:

- Deleting RADIUS profiles with Japanese characters (see page 512)
- Displaying properties of RADIUS profiles created with Japanese characters (see page 512)
- Creating RADIUS profiles with French characters (see page 512)
- Creating a Trusted Group with more than 25 French or Japanese characters (see page 512)

## RADIUS Profiles with Japanese Characters

If you try to delete a RADIUS profile on an RSA7 server using CA IdentityMinder Provisioning Manager in a Japanese environment, the delete operation appears to remove the profile in the Provisioning Server. However, when you look at the RSA Server, the RSA Profile is not deleted from the endpoint.

## Properties of RADIUS Profile Created with Japanese Characters

When you create a RADIUS profile in CA IdentityMinder Provisioning Manager using Japanese characters, the profile creation is successful. However you cannot display the property window of the profile after it has been created.

However, the profile is created correctly on the endpoint, and you can view and edit it using the RSA console.

## RADIUS Profiles with French Characters

If you create one RADIUS profile with French characters using CA IdentityMinder Provisioning Manager on an endpoint that does not contain RADIUS profiles with French characters (such as 'àçèéù) two profiles are created on the Endpoint

One profile is correct, however the second profile created contains invalid characters.

In addition, you cannot display properties of RADIUS profiles created with French characters.

## Trusted Groups with More than 25 French or Japanese Characters

The character limit for trusted group name is 50. However, due to the byte limit, you can only enter 25 French or Japanese characters. You can enter a maximum of 16 Kanji characters for a trusted group using CA IdentityMinder Provisioning Manager. The number of Japanese or French characters that you can enter in a particular field can be less than the number of English language characters that you can enter in the same field in the Provisioning Manager.

## Attempting to Create a Security Domain Above the Top Level Security Domain Fails

When you select the top-level of the endpoint in the container tree on the Endpoint Content dialog, the New button on the Endpoint Content dialog is displayed as available. However when you attempt to create a security domain, the creation fails because you cannot create a security domain above the top-level security domain. The New button on the Endpoint Content dialog is incorrectly displayed as available.

## Connector Data Migration Fails in Interactive Mode

If you run the RSA7Migrate utility in Mode 2 (create a template even if errors found, but do not associate it with a namespace) reconcile the templates and their missing objects before you use the templates. If you run the RSA7Migrate utility before you reconcile the templates and their missing objects, the migration utility fails.

## Assigning a Provisioning Role to a Global User to Create an RSA Trusted User Account Fails

**Valid on Windows and Solaris**

Symptom:

When I assign a Provisioning Role to a global user to create an RSA trusted use in CA IdentityMinder, the account creation fails.

**Solution:**

The account creation fails because the account template contains the default rule strings %P%, %UL% and %XD% that are not required for an RSA trusted user.

When you first create the template and delete the rule strings that are not required, the rule strings reappear when you assign the template.

When you create a template for an RSA trusted user, do the following.

1. Create the template using the default rule strings and click Submit.
2. Modify the account template, and delete the %P%, %XD% rule strings from the Password and Start Date fields on the Account tab.
3. Delete the rule string %UL% from the Start Date field on the User tab.
4. Submit the template.
5. Assign the provisioning role to the global user again.

# Salesforce.com Connector

The Salesforce.com connector provides a single point for all user administration and lets you administer the account objects on Salesforce.com endpoints:

Other Salesforce.com objects, such as public groups, roles, and profiles are read-only.

You can use the Salesforce.com connector to:

- Acquire Salesforce.com endpoints
- Explore Salesforce.com endpoints for existing users, public groups, roles and profiles
- Create, update, suspend, resume, or rename a Salesforce.com user

  **Note:** You cannot use the Salesforce.com connector to delete a Salesforce.com user. By, default CA IdentityMinder is configured to suspend the account on the Salesforce.com endpoint and place the account in a delete pending state when any operation that attempts to delete a Salesforce.com account directly or indirectly occurs.

  **Note:** For more information, about suspending and resuming a user, see the *CA IdentityMinder User Console online hel*p.
- Associate or disassociate a Salesforce.com user with, or from, public groups

  **Note:** Salesforce.com users, rather than administrators, manage private groups. Therefore you cannot use the Salesforce.com connector to provision private groups.
- Associate or disassociate a Salesforce.com user with a Salesforce.com role
- Associate a Salesforce.com user with a Salesforce.com profile
- Suspend or resume the account of a Salesforce.com user

## Enable Communication between the Salesforce.com Connector and Salesforce.com

To enable communications between the Salesforce.com connector and Salesforce.com cloud, download and install the SSL client certificate from Salesforce.com. The certificate is required because communications between the Salesforce.com connector and Salesforce.com cloud are performed using an SSL connection. The SSL client certificate validates requests generated by Salesforce.com.

**Follow these steps:**

1. Install or upgrade CA IAM CS.

   The installation registers CA IAM CS with the provisioning server, creates the Salesforce.com endpoint, and populates it with its associated metadata.

2. Generate the SSL client certificate, using the following steps:

   a. Log in Salesforce.com as an administrator.

   b. Select the Setup menu.

   c. Select App Setup, Develop, API, Generate Client Certificate.

3. Copy the SSL client certificate to your computer.

4. Log in to CA IAM CS.

5. Click the Certificates tab, then click Add.

6. When prompted, enter the location of the SSL client certificate that you have copied to the target computer, and the CA IAM CS keystore password.

   **Note:** The password for the keystore is the password that you set when you installed CA IAM CS. For more information, see the *Installation Guide*.

## Acquire a Salesforce Endpoint

To acquire a Salesforce endpoint, use a URL that contains the version number of the Salesforce API that you are using.

For a production environment, use the following URL:

```
https://www.salesforce.com/services/Soap/u/17.0
```

For a test environment, use the following URL:

```
https://test.salesforce.com/services/Soap/u/17.0
```

# Connector Features

This section details the management features of your connector, including account, account template, and group information for your connector.

## Managed Attributes

The Salesforce.com connector exposes attributes that:

- Are mandatory
- Represent membership of a Salesforce.com group
- Represent an association between a Salesforce.com user and a Salesforce.com role
- Represent an association between a Salesforce.com user and a Salesforce.com profile
- Can be mapped to CA IdentityMinder global user attributes for any Salesforce.com user

## Endpoint Attributes

The Salesforce.com connector supports the following endpoint attributes:

**Endpoint Name**

(Mandatory) Defines the name of the Salesforce.com endpoint.

**Description**

Defines a business description of the Salesforce.com endpoint. Use this field to record any information that helps you identify the endpoint.

**Username**

(Mandatory) Defines the name of the account that the client application uses to connect to the Salesforce.com endpoint.

**Password**

(Mandatory, write only) Defines the administrator password that the client application uses to connect to the Salesforce.com endpoint.

**Encrypted:** Yes

**Security Token**

(Write only) Defines the security token the user must use when using an API or desktop client to log in to a Salesforce.com endpoint.

**Encrypted:** Yes

**Do not use HTTP proxy**

Specifies that the connector ignores HTTP settings when communicating with an endpoint that has already been acquired. This may be required, for instance, when CA IAM CS is temporarily moved to a different network without the HTTP proxy server.

**Note**: The HTTP proxy settings were set during the installation of CA IAM CS. If you need to change the HTTP proxy settings, run the CA IAM CS installation again.

**HTTP Proxy Server**

Defines the HTTP proxy server you want to use to connect to the Salesforce.com endpoint.

**HTTP Proxy Server Port**

Defines the proxy server port you want to use to connect to the Salesforce.com endpoint.

**Proxy User Domain**

Defines the domain name where the proxy user is defined.

**Proxy User Name**

Defines the user name you want to use to log in to the proxy server.

**Proxy User Password**

(Write only) Defines the password of the proxy server you use to connect to the Salesforce.com endpoint.

**Encrypted:** Yes

**URL**

Defines the API web service login URL.

Only a valid Salesforce server URL can be used to acquire a Salesforce endpoint. Valid URLs take the following forms:

- https://*.salesforce.com/services/SOAP/u/
- https://*.salesforce.com/services/SOAP/c/
- https://*.visual.force.com/services/SOAP/u/
- https://*.visual.force.com/services/SOAP/c/

## Account Attributes

The Salesforce.com connector supports the following account attributes:

**Alias**

(Mandatory) Defines the alias used to identify the user, when the user name does not fit user on list pages, reports, and other pages.

**Limit:** 8 characters

**Allow Forecasting**

(Mandatory) Specifies that the user is allowed to use customizable forecasting.

**Default value:** false

**City**

Defines the city of the user.

**Limit:** 40 characters

**Community Nickname**

(Mandatory) Defines the name of the user in a community.

**Company**

Defines the name of the company where the user works.

**Data type:** String

**Limit:** 80 characters

**Country**

Defines the country where the user works.

**Limit:** 40 characters

**Created Date**

(Read only) Displays the date and time that the user account was created.

**CRM Content User**

Specifies that the user can use Salesforce.com CRM content.

**Default value:** false

**Customer (Account) name**

Specifies the name of an existing customer new portal account. When you click Browse, you can search through the existing customers, then select the one that needs a new portal account.

**Create new customer**

Identifies whether to create a new customer record.

If there is no customer record in Salesforce, select this box and enter the name in the New Customer Name field.

**New customer name**

Specifies the name of the new customer account.

**Create new contact**

Identifies whether you want CA IdentityMinder to create a new contact object.

**Delegated Approver**

Specifies the delegated  approver for approval requests.

**Department**

Defines the name of the department to which the user belongs.

**Limit:** 80 characters

**Division**

Defines the division to which the user belongs.

**Limit:** 80 characters

**Email Address**

(Mandatory) Defines the email address of the user.

**Limit:** 80 characters

**Note:** When you change an email address, Salesforce.com sends sends a confirmation message to the new address, asking the account owner to validate the change. This is Salesforce.com default behavior when modifying an email address. After the account owner confirms the change, CA IdentityMinder will display the new email address. Until it is validated, the old address appears.

**Email Encoding**

(Mandatory) Specifies the character set and encoding for outbound email sent by users from Salesforce.com.

**Employee Number**

Defines the employee identification number of the user.

**Limit:** 20 characters

**Extension**

Defines the telephone extension of the user.

**Limit:** 40 characters

**Fax Number**

Defines the fax number of the user.

**Limit:** 40 characters

**First name**

Defines the first name of the user.

**Limit:** 40 characters

**Job Title**

Defines the job title of the user.

**Language**

(Mandatory) Specifies the language in which to display text and online help.

**Limit:** 40 characters

**Last Login Date**

(Read only) Defines the date and time the user last logged in.

**Last Name**

(Mandatory) Defines the last name of the user.

**Limit:** 80 characters

**Locale**

(Mandatory) Specifies the country or geographic region where the user is located.

**Limit:** 40 characters

**Login ID**

Defines the login ID of the user.

**Manager**

Specifies the manager of the user.

**Marketing User**

Specifies that the user can create, edit, and delete campaigns, and configure advanced campaign setup.

**Default value:** false

**Mobile Number**

Defines the cellular or mobile telephone number of the user.

**Limit:** 40 characters

**Mobile User**

Specifies that the user is granted a Salesforce.com mobile license.

**Default value:** false

**Offline User**

Specifies that the user is allowed to use Connect Offline.

**Default value:** false

**Password**

(Write only) Defines the password of the user.

**Encrypted:** Yes

**Access restrictions:** Write only

**Phone Number**

Defines the telephone number of the user.

**Limit:** 40 characters

**Postal Code**

Defines the postal code of the user.

**Limit:** 20 characters

**Profile**

Specifies the Salesforce.com profile of the user.

**Receive Salesforce Administrator Newsletter**

Specifies that the user receives the Salesforce.com administrator newsletter.

**Default value:** false

**Receive Salesforce Newsletter**

Specifies that the user receives the Salesforce.com newsletter.

**Default value:** false

**Role**

Specifies the role of the user in an organization.

**State or Locality**

Defines the state or locality of the user.

**Street Address**

Defines the street address of the user.

**Suspended**

Specifies that user account is suspended.

**Time Zone**

(Mandatory) Specifies the main time zone in which the user works.

**User Name**

Defines the username of the user.

## Account Template Attributes

The Salesforce.com connector supports the following account template attributes:

**Alias**

(Mandatory) Defines the alias used to identify the user, when the user name does not fit user on list pages, reports, and other pages.

**Limit:** 8 characters

**Allow Forecasting**

(Mandatory) Specifies that the user is allowed to use customizable forecasting.

**Default value:** false

**City**

Defines the city of the user.

**Limit:** 40 characters

**Default value:** %UC%

**Community Nickname**

(Mandatory) Defines the name of the user in a community.

**Company**

Defines the name of the company where the user works.

**Data type:** String

**Limit:** 80 characters

**Default value:** %UCOMP%

**Country**

Defines the country where the user works.

**Limit:** 40 characters

**Default value:** %UCOUNTRY%

**Created Date**

(Read only) Displays the date and time that the user account was created.

**CRM Content User**

Specifies that the user can use Salesforce.com CRM content.

**Default value:** false

**Customer (Account) name**

Specifies the name of an existing customer new portal account. When you click Browse, you can search through the existing customers, then select the one that needs a new portal account.

**Create new customer**

Identifies whether to create a new customer record.

If there is no customer record in Salesforce, select this box and enter the name in the New Customer Name field.

**New customer name**

Specifies the name of the new customer account.

**Create new contact**

Identifies whether you want CA IdentityMinder to create a new contact object.

**Delegated Approver**

Specifies the delegated  approver for approval requests.

**Department**

Defines the name of the department to which the user belongs.

**Limit:** 80 characters

**Default value:** %UDEPT%

**Division**

Defines the division to which the user belongs.

**Limit:** 80 characters

**Default value:** %UO%

**Email Address**

(Mandatory) Defines the email address of the user.

**Limit:** 80 characters

**Default value:** %UE%

**Email Encoding**

(Mandatory) Specifies the character set and encoding for outbound email sent by users from Salesforce.com.

**Employee Number**

Defines the employee identification number of the user.

**Limit:** 20 characters

**Extension**

Defines the telephone extension of the user.

**Limit:** 40 characters

**Fax Number**

Defines the fax number of the user.

**Limit:** 40 characters

**Default value:** %UFAX%

**First name**

Defines the first name of the user.

**Limit:** 40 characters

**Default value:** %UF%

**Job Title**

Defines the job title of the user.

**Default value:** %UT%

**Language**

(Mandatory) Specifies the language in which to display text and online help.

**Limit:** 40 characters

**Last Login Date**

(Read only) Defines the date and time the user last logged in.

**Last Name**

(Mandatory) Defines the last name of the user.

**Limit:** 80 characters

**Default value:** %UL%

**Locale**

(Mandatory) Specifies the country or geographic region where the user is located.

**Limit:** 40 characters

**Login ID**

Defines the login ID of the user.

**Default value:** %UE%

**Manager**

Specifies the manager of the user.

**Marketing User**

Specifies that the user can create, edit, and delete campaigns, and configure advanced campaign setup.

**Default value:** false

**Mobile Number**

Defines the cellular or mobile telephone number of the user.

**Limit:** 40 characters

**Default value:** %UMP%

**Mobile User**

Specifies that the user is granted a Salesforce.com mobile license.

**Default value:** false

**Offline User**

Specifies that the user is allowed to use Connect Offline.

**Default value:** false

**Password**

Defines the password of the user.

**Encrypted:** Yes

**Default value:** %P%

**Phone Number**

Defines the telephone number of the user.

**Limit:** 40 characters

**Default value:** %UP%

**Postal Code**

Defines the postal code of the user.

**Limit:** 20 characters

**Default value:** %UPC%

**Profile**

Specifies the Salesforce.com profile of the user.

**Receive Salesforce Administrator Newsletter**

Specifies that the user receives the Salesforce.com administrator newsletter.

**Default value:** false

**Receive Salesforce Newsletter**

Specifies that the user receives the Salesforce.com newsletter.

**Default value:** false

**Role**

Specifies the role of the user in an organization.

**State or Locality**

Defines the state or locality of the user.

**Default value:** %US%

**Street Address**

Defines the street address of the user.

**Default value:** %USA%

**Suspended**

Specifies that user account is suspended.

**Time Zone**

(Mandatory) Specifies the main time zone in which the user works.

**User Name**

Defines the username of the user.

## Custom Attributes

The Salesforce.com connector supports the creation of custom attributes. You can customize the metadata of the Salesforce.com connector to create additional attributes for a Salesforce.com user object, including custom Salesforce.com fields.

You can only create custom attributes that have a string data type, for example, text fields, integer fields, date and time fields, and such.

## How to Display Salesforce.com Custom Attributes in the CA IdentityMinder User Console

If you create custom attributes in your Salesforce.com organization, you can display the custom attributes in your client Identity Lifecycle Management application. To display the custom attributes, customize the metadata of the Salesforce.com connector using Connector Xpress.

To display the custom attributes in the CA IdentityMinder User Console do the following:

1. Get the API name of the custom attribute in your Salesforce.com organization that you want to display in the CA IdentityMinder User Console.

   **Note:** For more information, see your Salesforce.com organization.

2. Add custom attributes to the Salesforce.com connector metadata using Connector Xpress.
3. Modify the properties of the attribute as required, for example, Maximum Length, Allowed Operations, and such.
4. Create the presentation metadata that defines how the attribute id displayed in the CA IdentityMinder User Console.
5. Generate the CA IdentityMinder User Console Salesforce.com Account Management screens.

### Example: Display Salesforce.com Custom Attributes

The following example shows you how to display a custom attribute that you create in your Salesforce.com organization in your client ILM application. This example uses CA IdentityMinder as the client ILM application. This example shows you how to customize the metadata of the Salesforce.com connector by using Connector Xpress, and how to display the custom attribute in CA IdentityMinder User Console Salesforce.com account management screens.

This example:

- Assumes that you have created a custom attribute named *MyCustomAttribute* in your Salesforce.com Organization, and defined it as a text field with a length of 25 characters.
- Shows you how to display a custom Salesforce.com text attribute named *MyCustomAttribute* on the Organization section of the User tab of the Salesforce.com Account dialog in the CA IdentityMinder User Console.
- Shows you how to change the length of the field.

**To create custom attributes**

1. Get the API name of your custom Salesforce.com attribute *MyCustomAttributeName.*

   This is the attribute that you want to display on the User tab of the Salesforce.com Account dialog in the CA IdentityMinder User Console.

   **Example:** *MyCustomAttribute__c.*

2. Add and configure a Provisioning Server, in Connector Xpress.
3. Create a project based on the existing Salesforce.com connector metadata.
4. Click Attributes, in the Mapping tree, under User Class.

   The Attributes Summary dialog appears.

5. Under Mapped Attributes, add the custom attribute *MyCustomAttribute*.

   You have added the custom attribute *MyCustomAttribute* to the Salesforce.com user class.

6. In the Mapping tree, click *MyCustomAttribute*.

   The Attributes Details dialog appears.

7. On the Attributes Details dialog, do the following:

   a. Complete the Connector Map To field with the API name of your custom attribute *MyCustomAttribute*. For example, *MyCustomAttribute__c*

      **Connector Map To**

         Specifies which name to map an object class (including the connector itself) or attribute to in connector-speak. For a dynamic connector, this attribute specifies the name of the native system item to map the attribute to.

b. Select String from the Data Type list.

**Data Type**

Specifies the data type of the provisioning attribute that you have mapped to the native attribute.

c. In the Maximum length field, change the length to 50.

**Maximum Length**

Specifies the maximum byte length of values for this attribute value. This value is used for input validation.

8. In the mapping tree, click Attributes.

   The Attributes Summary dialog appears.

9. On the Attributes Summary dialog, do the following:

   a. Under Account Screens, click User.

      The page sections on the User tab appear.

   b. On the Organization page section, select *MyCustomAttribute* from the drop-down list.

      You have created the presentation metadata that defines how the custom attribute *MyCustomAttribute* is displayed in the CA IdentityMinder User Console.

10. Deploy the Salesforce.com connector to the Provisioning Server.

11. Use the Role Definition Generator to generate the CA IdentityMinder User Console Salesforce.com account management screens.

    CA IdentityMinder displays the custom attribute in the Organization section of the User tab of the Salesforce.com Account dialog in the CA IdentityMinder User Console.

**Note:** For more information about how to add and configure a provisioning server, create a project, and generate CA IdentityMinder User Console account screens, see the *Connector Xpress Guide*.

## Account Deletion

You cannot use the Salesforce.com connector to delete a Salesforce.com user, as Salesforce.com does not support account deletion.

CA IdentityMinder simulates account deletion when any operation that attempts to delete a Salesforce.com account directly or indirectly occurs, for example, removing the role that created that account.

When the option *Accounts will be deleted from the provisioning directory and suspended on the managed endpoint* is selected on the Endpoint Settings tab in the User Console, the account is deactivated and placed in a group called CA ILM SFDC Connector Suspended on the Salesforce.com endpoint.

During an add operation, the Salesforce.com connector verifies that the account exists on the Salesforce.com endpoint and checks to see if the account is in the CA ILM SFDC Connector Suspended group.

If the account is in the CA ILM SFDC Connector Suspended group, CA IdentityMinder removes the Suspended membership and modifies the account, instead of adding a new account.

During an explore and correlate, CA IdentityMinder ignores all accounts in the CA ILM SFDC Connector Suspended group.

The Salesforce.com connector creates the CA ILM SFDC Connector Suspended group as required.

**Note:** For more information, about suspending and resuming a user account, see the *CA IdentityMinder User Console online hel*p.

# SAP Connector

The SAP Connector provides a single point for all user administration by letting you perform any of the following actions:

- Retrieve existing users from the SAP repository
- Display, create, modify, or delete a user
- Retrieve the existing authorization profiles from the SAP repository
- Display authorization profiles
- Assign or unassign an authorization profile to a user
- Retrieve the existing SAP roles from the SAP repository
- Display SAP roles
- Assign or unassign a SAP role to a user

- Register endpoints, explore them for objects to manage, and correlate their accounts with global users
- Create and manage SAP accounts using SAP-specific account templates
- Change account passwords and account activations in one place
- Assign a SAP account template to each of your SAP endpoints
- Use the default endpoint type account template to create accounts with the minimum level of security needed to access a SAP endpoint
- Generate and print reports about SAP accounts, SAP profiles, and SAP roles
- Manage SAP CUA environments

## Support for SAP

You can connect CA IdentityMinder to SAP 4.6C systems.

On the SAP 4.6C system, update the SAP_BASIS component to Support Package 50 or above.

In addition, when you use CA IdentityMinder to manage an SAP 4.6C system, the following limitations apply:

- CA IdentityMinder cannot manage the user license type
- The length of the values for SAP parameters ("Parameters" tab) is reduced from 40 characters to 18 characters.

**More information:**

Passwords on SAP 4.6C (see page 546)

## SAP Support for FIPS and IPv6

For this release of CA IdentityMinder, the SAP Connector does not support FIPs or IPv6.

## Set Up the SAP R3 Connector

The SAP R3 connector requires SAP Java Connector (SAP JCo). Before you use the SAP R3 connector, create a bundle that contains the JCo files, and then add the bundle to the connector.

**Follow these steps:**

1. Install or upgrade CA IAM CS.

   The installation registers CA IAM CS with the provisioning server, creates the Salesforce.com endpoint, and populates it with its associated metadata.

2. Ask the SAP administrator to follow these steps:

   a. Log in to http://service.sap.com/connectors using SAP Service Marketplace credentials.

   b. Click SAP Java Connector to display the JCo overview, then click Tools and Services from the menu on the left.

   c. Select Download SAP JCo Release 2.1 from the menu, then select the appropriate 64-bit download from the list.

   d. Extract the following files:

      - **Windows:** librfc32.dll, sapjco.jar, sapjcorfc.dll
      - **UNIX:** sapjco.jar, librfccm.so, libsapjcorfc.so

   e. Send the files to you.

3. Save these files locally.

4. Run the *sap_post_install* script in the following location:

   *cs-home*/bin

   The script asks for the location of the JCo files. It then creates a bundle and saves it in the same location as the script.

5. Log in to CA IAM CS (see page 21).

6. At the top, click the Connector Servers tab.

7. In the Connector Server Management area, click the Bundles tab.

8. Add the new bundle:

   a. In the Bundles area on the right, click Add.

   b. Browse to the bundle that the script created, then select the connector server on which this connector will be available.

   c. Click OK.

      The new bundle appears in the Bundles list.

9. Find the main connector bundle in the Bundles list, then right-click its name in the list and choose Refresh Imports from the popup menu.

You can now use the SAP R3 connector to connect to an endpoint.

## Load the Bundle for SAP r3 Prerequisites

CA IAM CS comes with a script that helps you load the bundle.

**Follow these steps:**

1. Log in to CA IAM CS (see page 21).
2. Click Connector Server, Bundles, and then click Add.
3. Browse to the following file:

   `*cs-home*/jcs/resources/sap/sapConnectorLibsOsgi.jar`

   **Note:** Do not check the Start Bundle box.
4. Click OK.

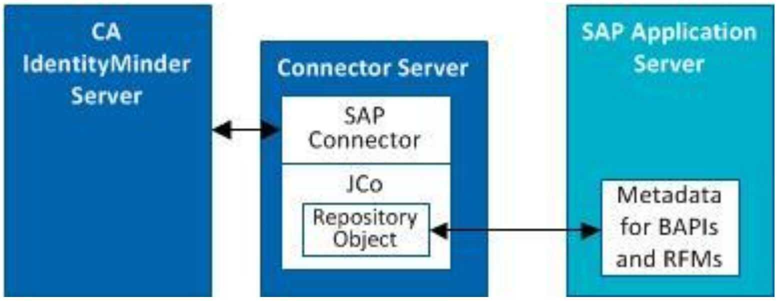
   CA IAM CS loads the bundle and lists it as a fragment.
5. Right-click the SAP R3 connector bundle (not the fragment!) and select Refresh Imports.

   The connector detects the new bundle, and includes it.

You can now use the SAP R3 connector to connect to an endpoint.

## How the SAP Connector Uses JCo

The SAP connector uses the SAP JCo library to communicate with SAP systems.



The SAP connector needs to retrieve metadata for the BAPIs and RFMs on the SAP Application Server. The connector uses the repository object in JCo.

The JCo repository object maintains its connection to the SAP system. The repository object caches the metadata that it receives from the SAP Application Server. For this reason, there is always one connection open to the SAP system once an endpoint is acquired.

When you use the SAP connector to manage an account, CA IAM CS opens a second connection to the SAP Application Server. To maintain high performance, CA IAM CS manages this connection using its own pooling mechanism.

## Allow Connector to Read SUSPENDED and LOCKED States

By default, CA IAM CS cannot correctly read the state of a SAP account. If an account is locked or suspended, it will appear to be active when you view it with the User Console.

To allow the connector to correctly read locked and suspended states, install SAP BASIS support package 50 (SAPKB46C50) on the SAP R/3 46C endpoint.

For information about this support package, see SAP Note 826050 "BAPI_USER_GET_DETAIL: Function enhancement".

## Migrating SAP Endpoints from the C++ SAP Connector

The Java version of the SAP Connector (installed with CA IAM CS) provides all of the functionality of the previous (eTrust Admin r8.1) C++ version of the SAP Connector with the added benefit of full CUA management, but there are a few things to consider when switching from the C++ version.

- When a SAP CUA master endpoint has already been acquired and explored, the endpoint will be managed as a CUA engine after the switch from the C++ connector to the Java connector. Since all existing SAP roles and account templates are still valid after the migration, existing admin account templates targeting the master directory are still usable. Existing managed objects are valid as well. *You must re-explore the endpoint to include the managed objects that exist on child systems.*

- When SAP CUA member endpoints have already been acquired and explored, they should be removed. Account templates pointing to these member endpoints should be pointing to the CUA master endpoint.

  **Note:** Management of local account attributes (for example, default printer) according to the SCUA parameter is still possible by keeping the CUA member endpoint and managing these attributes through this endpoint.

- To add the SAP connector to an existing system:

  1. Run the Provisioning Server install to reconfigure and add the SAP connector.
  2. Run CA IAM CS installer and select Register with the Provisioning Server.

  Doing this will route requests from the Provisioning Server to CA IAM CS for the SAP endpoint type.

- **Important!** Before migrating from C++ to CA IAM CS, the following must be filled out and selected on the Endpoint Tab of the SAP Endpoint property sheet:

  - The check box for 'Use LogonID' must not be selected.
  - The application server name and number must be entered.

## Connector-Specific Features

This section details your connector's specific management features, such as how to acquire and explore your endpoint. Also included are account, provisioning roles, account template, and group information specifically for your connector.

### Acquire a SAP System Using the User Console

You must acquire the SAP system before you can administer it with CA IdentityMinder.

**To acquire a SAP system using the User Console**

1. Select Endpoints, Manage Endpoints,Create Endpoint
2. Select SAP R3 from the drop-down list box on Create a new endpoint of Endpoint Type, and click Ok

   Use the Create SAP R3 Endpoint page to register a SAP system. During the registration process, CA IdentityMinder identifies the SAP system you want to administer and gathers information about it.

3. After entering the required information, click Submit.

   You are now ready to explore and Correlate the endpoint.

4. Click Endpoints, Explore and Correlate Definitions, Create Explore and Correlate Definition to explore the objects that exist on the endpoint.

   The Exploration process finds all SAP accounts and groups. You can correlate the accounts with global users at this time or you can correlate them later.

5. Click OK to start a new definition.

6. Complete the Explore and Correlate Tab as follows:

   a. Fill in Explore and Correlate name with any meaningful name.

      Click Select Container/Endpoint/Explore Method to click a SAP endpoint to explore.

   b. Click the Explore/Correlate Actions to perform:

      - **Explore directory for managed objects**—Finds objects that are stored on the endpoint and not in the provisioning directory.
      - **Correlate accounts to users**—Correlates the objects that were found in the explore function with users in the provisioning directory. If the user is found, the object is correlated with the user. However, you can instead select that you want to assign the account to the existing user (the default user) or create the user.
      - **Update user fields**—If a mapping exists between the object fields and the user fields, the user fields are updated with data from the objects fields.

7. Complete the Recurrence tab if you want to schedule when the task to executes.

   a. Click Schedule.

   b. Complete the fields to determine when this task should execute.

      You may prefer to schedule the task to execute overnight to interfere less with routine access of the system.

   **Note**: This operation requires the client browser to be in the same time zone as the server. For example, if the client time is 10:00 PM on Tuesday when the server time is 7:00 AM, the Explore and Correlate definition will not work.

8. Click Submit.

**To use an explore and correlate definition**

1. In a CA IdentityMinder environment, click Endpoints, Execute Explore and Correlate.

2. Click an explore and correlate definition to execute.

3. Click Submit.

   The user accounts that exist on the endpoint are created or updated in CA IdentityMinder based on the explore and correlate definition you created.

## Acquire a SAP Endpoint Using the Provisioning Manager

SAP must be installed on the machine that you want to administer through the CA IdentityMinder SAP connector.

**From the Endpoint type task view**

1. Register the SAP system as a SAP/R3 endpoint.

   Use the SAP Endpoint property sheet to register a SAP system. During the registration process, the Provisioning Manager identifies the SAP system you want to administer and gathers information about it.

   **Note:** You must provide a SAP user/password with administrator rights when registering a SAP system.

   **More information:**

   Create a New User and SAP Role with Minimum Rights to Administer SAP (see page 538)

2. Explore the objects that exist on the endpoint.

   After registering the system in CA IdentityMinder, you can explore its contents. Use the Explore and Correlate Endpoint dialog. The Exploration process finds all SAP Accounts, SAP Roles (except Generated Roles), and SAP Profiles (except Generated Profiles). You can correlate the accounts with global users at this time or later.

3. Correlate the explored accounts with global users.

   When you correlate accounts, CA IdentityMinder creates or links the accounts on an endpoint with global users, as follows:

   a. CA IdentityMinder attempts to match the eTSAPAccountName with each existing global user name. If a match is found, CA IdentityMinder associates the SAP account with the global user. If a match is not found, CA IdentityMinder performs the next step.

   b. CA IdentityMinder attempts to match the eTSAPLastName with each existing global user's full name. If a match is found, CA IdentityMinder associates the SAP account with the global user. If a match is not found, CA IdentityMinder performs the next step.

   c. CA IdentityMinder associates the SAP account with the *default user* object.

## Changed Passwords are Expired

The SAP Endpoint Property Sheet contains a parameter called Changed passwords are expired. When this field is checked, the user is prompted to change their password when they next log on. If the password has been propagated from a global user password change, the user is also prompted to change their password. This is the SAP recommended behavior for password changes and has been checked by default on all newly created endpoints. Click here (see page 543) for further details on account password management in a CUA environment, or here (see page 541) for account password management with stand-alone SAP systems

## SAP Provisioning Roles and Account Templates

The SAPDefaultPolicy, provided with the SAP Connector, gives a user the minimum security level needed to access an endpoint. You can use it as a model to create new account templates.

### Modify SAP Account Template Properties

To modify or view a SAP account template's properties, perform the following steps:

1. Click the Roles task button.
2. Select SAP Endpoint Account Template in the Object Type drop-down list box.
3. Search for the account template that you want.
4. Right-click on the account template in the list view and choose Properties from the pop-up menu.
5. Modify or view the properties in the SAP Account Template property sheet.
6. Click Apply.

### Create a New User and SAP Role with Minimum Rights for Administration

To set the minimum authorization that a user should have to administrate a SAP system from CA IdentityMinder, you must create a new SAP role.

**Note:** If you are administering a CUA environment, see the notes on CUA below.

**To create a new user with a SAP role with minimum rights to administer SAP**

1. Create a new communications user with no authorizations.
2. Create a new authorization role by using transaction *PFCG*.
3. On the descriptions tab, enter a meaningful description.

4. On the menu tab, copy the "Tools>Administration>**User Maintenance**" menu by selecting *'copy menus>from the SAP menu'*.
5. Select the *'Change Authorization Data*' button on the Authorizations tab:
   - Do not assign the role an organizational level
   - Manually add the authorizations **S_RFC** and **S_TABU_DIS**.
   - Assign the full authorization for all trees by setting the authorization fields to '*****'. **All authorizations must be active (green light) before proceeding**.
   - If necessary, drill down and manually set the 'Human Resources>Personnel Planning>Personnel Planning>**Plan Version**' to full authorization, '*****'.
   - Generate the profile.
6. On the user tab, add the user ID of the previously created communications user and then perform a 'user comparison' to immediately assign the authorizations to the account.

**Notes for SAP CUA**

- You should perform the above steps on the CUA master system only.
- The communications user must be added to the CUA master system (Maintain User Properties>System Tab) **before** completing a user comparison during role creation.

## Grace Interval on Logon Tab of SAP Account Template Property Sheet

When an account is created, you can choose a date from the Valid From and Valid To fields that indicate when the logon credentials are valid or you can specify the number of days from the Valid from date until the credentials become valid, by selecting the Grace Interval field and entering the number of days.

Valid From and Valid To are two SAP account template attributes that can be propagated to the associated accounts. Grace Interval is only valid at the time of account creation. For example, modification applies only for the SAP account template and not the accounts associated to it.

## SAP Accounts

Use the SAP Account property sheet when managing your accounts.

**Note:** The extended attributes include the following:

- Name at birth
- Middle name initial
- Second academic title
- Name prefix
- Second prefix

- Name supplement
- Nickname
- Name format
- Internal mail
- Code
- Second family name
- Second given name

**Note:** Each attribute that may be specified through a rule string in an account template could possibly be truncated. A warning message will display the name of all the attributes that were truncated.

## SAP Profiles

SAP Profiles grant access to the user for SAP transaction menus and other SAP objects.

**Note:** A SAP Profile differs from the Admin Profile, which is attached to the Global User and grants access to CA IdentityMinder objects.

## User License Contractual Type

The License Data tab enables you to manage the account license contractual type, selecting a value for the Contractual User Type.

## Explore Non-Dialog Accounts Without Correlation

Non-dialog accounts are accounts that are used to run the batch process, remotely connecting from a foreign application. To prevent non-dialog accounts from being correlated to a global user, perform the following steps:

1. In the SAP Endpoint tab, check the "Only manage dialog accounts" checkbox prior to exploration and correlation.
2. Uncheck the "Only manage dialog accounts" checkbox, and explore the endpoint accounts without correlate.

## Account Password Management

When connecting to a stand-alone SAP system, if not using a pre-expired password, the following occurs:

- **On Account creation:**

  The password is pre-expired. You must change the password upon first logon.

- **On Account Modify**

  The password is changed.

  **Note:** With SAP Kernel 6.40, it is not possible to change the password on a locked account unless the endpoint is set to use pre-expired passwords. The account must be unlocked before the password change can be applied.

When using a pre-expired password, the following occurs:

- **On Account Creation and Modify**

  The password is pre-expired. You must change the password upon first logon and first logon after the change.

## SAP Conventions

Use the following SAP conventions in your etautil commands:

- The endpoint type name (eTNamespaceName) is SAP R3.
- The endpoint type prefix is SAP. Therefore, the SAP class names are the following:
  - eTSAPAccountContainer for a SAP user container
  - eTSAPAccount for a SAP user name
  - eTSAPProfileContainer for a SAP profile container
  - eTSAPProfile for a SAP profile name
  - eTSAPRoleContainer for SAP role container
  - eTSAPRole for a SAP role name
  - eTSAPPolicyContainer for a SAP account template container
  - eTSAPPolicy for a SAP account template

## Managing SAP Central User Administration (CUA) Environments

The SAP connector lets you manage CUA environments. The following sections apply to CUA and how they are managed by this connector.

## SAP (CUA) Management

CUA is a tool that can be used to manage SAP account on multiple SAP systems centrally on a single Master System. The Java-based SAP connector processes CUA master systems as a CUA engine.

**Note:** While using the new Java-based connector, it is not possible to manage a CUA Master system as a standalone.

The SAP Connector (Java) can manage all SAP systems that are part of a CUA. A new read-only field on the SAP Endpoint property page "CUA Status" displays the status of a SAP endpoint against CUA. When the SAP system is a CUA master, the field shows "CUA master system managed as a CUA engine".

**Note:** CUA management is only effective when the field distribution parameters using transaction SCUM are set to 'GLOBAL'.

### As a CUA Engine Processing Mode

For example, a directory called CUAMAST (CUA master) can grant an account the following roles:

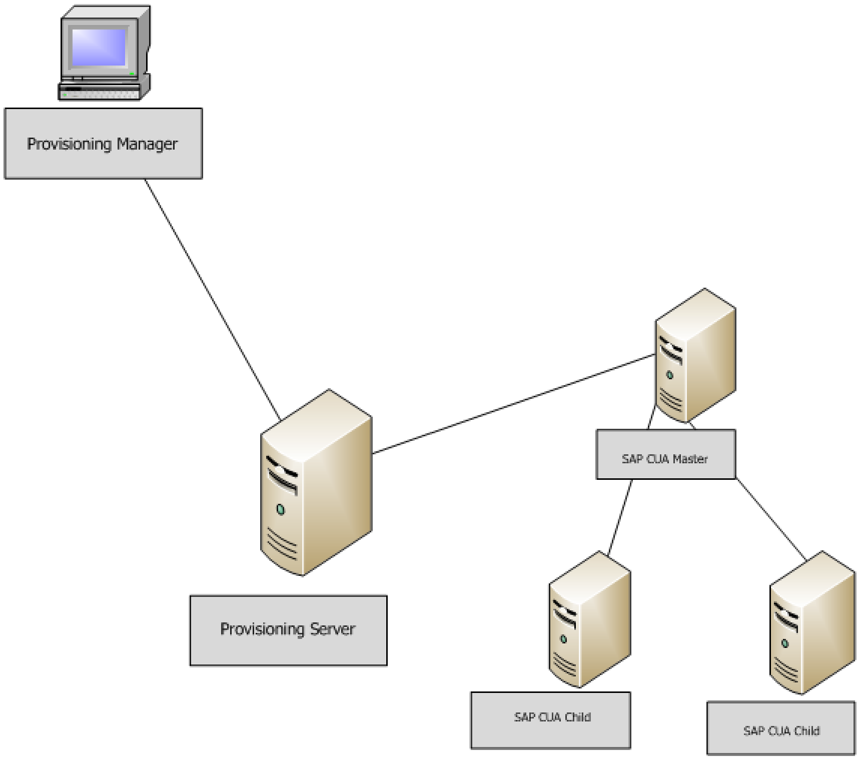
- role1
- CUACHI1/role3
- CUACHI2/role4

The following then occurs:

- An account is created on the CUA master directory by CA IdentityMinder.
- The SAP CUA mechanism grants this account role1 privilege on the directory.
- The SAP CUA mechanism propagates the account to both CUACHI1 and CUACHI2 directories.
- The SAP CUA mechanism grants the account on CUACHI1 the role role3.
- The SAP CUA mechanism grants the account on CUACHI2 the role role4.

The following diagram shows the Java-based connector's As a CUA engine processing mode:

*Equation 1: Provisioning Server connects to SAP CUA Master, which connects to any SAP CUA Child system*



## Account Password Management in CUA Environment

The following sections show how account password management is handled in a CUA environment.

## Connecting to a CUA Master

When connecting to a CUA master system, if not using a pre-expired password, the following occurs:

- **On Account Creation for both CUA Master and CUA Child**

  The password is pre-expired. You must change the password upon first logon.

- **On Account Modify**

  CUA Master - The password is changed.

  CUA Child - The password change is not distributed to child systems. Password management must be done locally.

**Note:** With SAP Kernel 6.40, an attempt to change the password of an account that does not reside on the Master system will return PASSWORD NOT ALLOWED.

When connecting to a CUA master system using a pre-expired password, the following occurs:

On Account Creation for both CUA Master and CUA Child

> The password is pre-expired. You must change the password upon first logon.

On Account Modify

> CUA Master - The password is pre-expired. You must change the password upon first logon after the change.
>
> CUA Child - The password change is not distributed to child systems. Password management must be done locally.

## Connecting to a CUA Child

We recommend using the connector to manage locally managed attributes of the account. To be able to change passwords when connecting to a child system, the distribution model of the initial password should be set to "proposal" using the SAP transaction SCUM.

## Password Management in a CUA Environment

As password changes applied to the CUA Master System are not distributed to other CUA members, you will need to acquire separate SAP endpoints to the Child Systems to be able to manage account passwords on Child Systems. After creating a new account on the CUA Master System, you must re-explore and correlate the users container on the endpoint set up to manage such child systems. The passwords can then be managed by a modification to the Global User associated with these accounts, or directory to the accounts in these managed endpoints. This is a limitation imposed by SAP.

## Remove an Account from the CUA Master System

Removing an account from the CUA Master System with the Java connector removes the account on the Master System as well as all the Child systems.

## CUA Distribution Settings

For further details on the distribution parameters for fields within transaction SCUM, refer to the SAP Central User Administration documentation available at http://service.sap.com. It is important to be aware of the distribution settings within your CUA environment as some settings may end with unexpected results. In particular:

- When the distribution model for an attribute has been set to "Global", these attributes must be managed by the Provisioning Manager using the endpoint connecting to the CUA Master system.
- When the distribution model for an attribute has been set to "Local", the attribute can only be managed from the endpoint(s) connecting directly to each individual member system, regardless of its status within the CUA.
- When changing an attribute that conflicts with the distribution model, the modification attempted by the Connector Server may be ignored. In some cases, an error is returned. You should be aware of the distribution settings and manage accordingly.
- In these cases, the Provisioning Manager may not give a visual indication that the attribute change is permitted under the current distribution settings.
- Passwords cannot be managed as "Global", regardless of the distribution settings. Any changes applied to the password on a CUA Master system are not distributed to the child systems by design. Click here (see page 543) for information on password management using the Provisioning Manager.
- With the exception of the password management, we recommend that where possible, the distribution settings be set to "Global".

## Passwords on SAP 4.6C

Before you enter the password to acquire the endpoint, you need to know the SAP basis version you want to acquire and enter your password accordingly.

- For SAP 4.6C, the password must contain uppercase letters only.
- For SAP basis version 640, the password can use uppercase and lowercase letters.
- For SAP basis version 700 and above, passwords are case-sensitive.

The connector.xml file contains the following flag:

**convertPasswordToUpperCase**

If the SAP basis version is equal to or higher than 700, CA IdentityMinder ignores this flag.

**Note:** This flag only applies to passwords entered when adding new accounts or changing existing accounts.

**true**

(Default) CA IdentityMinder converts the password to all upper case when the SAP basis version is lower that 700. When the SAP basis version is equal to or higher than 700, we will just pass the password through.

**false**

CA IdentityMinder does not convert the password, if the SAP basis version is lower than 700.

**More information:**

Support for SAP (see page 531)

# SAP UME Connector

The SAP UME Connector provides a single point for SAP UME account administration. The connector lets you administer account objects on SAP UME endpoints.

The SAP UME connector lets CA IdentityMinder connect to SAP User Management Engine (SAP UME). SAP UME is the user administration tool for SAP NetWeaver.

When the SAP UME connector is set up, you can use the CA IdentityMinder User Console to do the following:

- Acquire SAP UME endpoints
- Explore SAP UME endpoints for existing users, groups, and roles

You can then use the CA IdentityMinder User Console to do the following provisioning tasks:

- Create, update, and delete SAP UME users

  **Note:** You cannot rename a user using the CA IdentityMinder User Console.

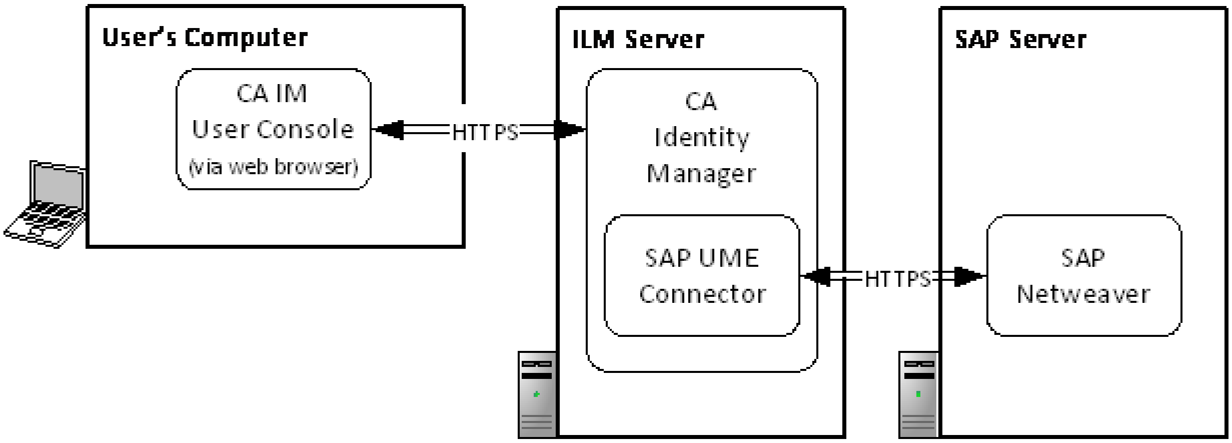
- Change a user's password
- Lock and unlock accounts
- Assign and unassign roles to users
- Assign and unassign groups to users

For known issues related to the SAP UME connector, see the CA *IdentityMinder Release Notes* distributed with the CA IdentityMinder bookshelf.

## How the SAP UME Connector Works

The following diagram shows how the connector links the endpoint (an SAP Netweaver server) with CA IdentityMinder:

*Equation 2: The SAP UME Connector uses HTTPS to connect to SAP Netweaver on the SAP server.*



## Installation

The SAP UME connector is installed with the CA IdentityMinder User Console. You do not need to install any extra components.

We strongly recommend that you set up HTTPS between the connector and SAP NetWeaver.

### Platform Support

The SAP UME connector has the same system requirements as CA IdentityMinder.

The connector supports the following versions and later:

- SAP Netweaver 2004 SP 14
- SAP Netweaver 7.0 SPS 05

## Enable SSL between SAP NetWeaver and CA IAM CS

To improve the security of the link between CA IAM CS and SAP NetWeaver AS Java, we strongly recommend that you set up an HTTPS connection.

**Follow these steps:**

1. The SAP administrator does the following:

   a. Locate the certificate for the AS Java, or its CA certificate.

   b. Send the file to the administrator for CA IdentityMinder .

   The administrator for CA IdentityMinder does the remaining steps.

2. Log in to CA IAM CS (see page 21).

3. At the top, click the Certificates tab.

   This tab lists all of the certificates in the CA IAM CS keystore. To filter the list of certificates by their names, type in the Certificate Filter box.

4. To add a certificate, click Add, then enter the details of the certificate.

   Add a certificate:

   - **Certificate**—Enter the path to the certificate file
   - **Alias**—Enter an alias for storing the certificate

   Add a keystore:

   - **Certificate**—Enter the path to the keystore file
   - **Alias**—Enter alias for storing the certificate. This alias also identifies the certificate in that keystore.
   - **Keystore Password**—Enter the password of the keystore

     **Note:** The keystore is in *jcs-install*/conf/ssl.keystore.

5. Verify that the Use HTTPS check box is selected for each SAP UME endpoint that you create. This check box is selected by default.

## Privileges Required to Connect to SAP UME

To connect to an SAP UME endpoint using the SAP UME connector, the administrator account that manages the endpoint must have a UME role with one of the following UME actions:

- UME.Spml_Write_Action
- UME.Manage_All

  **Note:** This action includes UME.Spml_Write_Action.

# Troubleshooting

## Locked and Suspended Passwords

CA IdentityMinder distinguishes between locked and suspended accounts in the following way:

- **Locked—**An account is locked after repeated attempts to log in with an incorrect password.
- **Suspended**—An administrator can suspend an account for any reason.

SAP UME provides only one attribute for both of these situation cases: *islocked*, which has the value *true* for either situation.

This means that CA IdentityMinder cannot distinguish between these two cases. When either situation happens, the User Console shows that the account is suspended.

If you click the Resume button, CA IdentityMinder unlocks the password or removes the suspension from the account.

## Error When Creating a New Account: "Unable to read response: Can't overwrite cause"

**Symptom:**

When I attempt to create an account on an SAP UME endpoint, a message similar to the following appears on the User Console:

```
SAP-UME: java.security.PrivilegedActionException:
com.sun.xml.internal.messaging.saaj.SOAPExceptionImpl: Unable to read response:
Can't overwrite cause : Unable to read response: Can't overwrite cause
```

**Solution:**

This message appears if the SAP UME endpoint requires that new accounts have a password, and you tried to use the User Console to create an account without a password.

The message should have stated this, but instead an incorrect message appears.

Create the account again, and verify that you included a password.

## Default Java Heap Size Might Be Insufficient

By default, the JVM Java heap size is set to 256 MB. This size is insufficient to explore a directory with 250,000 accounts.

The JVM heap size should be 512 MB.

## Some Attributes Are Unavailable on Some SAP UME systems

Some attributes are available on these newer SAP AS Java systems only:

- SAP NetWeaver 7.0 SP17
- SAP NetWeaver 7.01 SP2 and later

The affected attributes are:

- Street Address
- City
- PO Box
- Zip
- State
- Country
- Orgunit
- Accessibilitylevel
- passwordchangerequired

For earlier SAP AS Java systems, these attributes are ignored.

**Note:** For more information, see "SAP note 1238330 - Missing attribute in SPML schema".

## Unable to View or Modify SAP UME Accounts with Unicode or UTF-8 Characters in CA IdentityMinder User Console

**Symptom:**

I created an SAP UME account with Japanese characters in CA IdentityMinder. When I try to view or modify the account in the User Console, I get an error message that starts with Not a valid IAM handle, and then contains unintelligible characters.

**Solution:**

The account is created successfully in CA IdentityMinder, but you cannot display the account in the User Console. However, you can view the account successfully in the Provisioning Manager.

To display SAP UME accounts created with non-English characters in the CA IdentityMinder User Console, configure the JBoss server.xml file for UTF-8 encoding for URI.

**Note:** For more information about configuring the JBoss server for UTF-8 encoding for URI, see Change Tomcat server.xml in the *User Console Design Guide*.

## Cannot Assign R3/ABAP Groups or Roles to Accounts

Roles in the R3/ABAP data store appear in CA IdentityMinder as groups with the data source R3_ROLE_DS.

When you are assigning groups to accounts, avoid those with this data source, because these groups cannot be assigned to an account.

This is due to a limitation in SAP UME. If you try to assign one of these roles or groups to an account, CA IdentityMinder will attempt to assign it, but it will fail.

## Customize Password Restrictions

The SAP UME Connector does not allow passwords that begin with exclamation points (!) or question marks (?), or allow passwords that contain PASS or SAP*.

The default password restrictions are based on SAP ABAP password rules.

If you are using a different store, for example, Active Directory, you can customize the password and character restrictions. You can configure the illegalPasswords and passwordCannotStartWith properties in the connector.xml file for the SAP UME Connector.

**To customize password and character restrictions**

1. Edit the following parameters in the *cs_home*\conf\override\sap-ume\SAMPLE.connector.xml file.

   **illegalPasswords**

   Specifies passwords that the SAP UME Connector blocks.

   **passwordCannotStartWith**

   Specifies the characters that you cannot use at the start of a password.

   To remove a restriction, delete the <value> parameter of the property.

2. Save the SAMPLEconnector.xml file as connector.xml and then restart CA IAM CS.

### Example connector.xml file

The following is the section of the connector.xml file that specifies the illegal passwords and characters that you cannot use at the start of a password.

```
<!-- This is the list of illegal passwords that would not be allowed
on the SAP UME systems. They are treated as case-sensitive.
This list is only used to check if the generated temporary password
is legal. The legality of the final password is still checked by the
UME system, not the connector. -->
<property name="illegalPasswords">
       <list>
              <value>PASS</value>
              <value>SAP*</value>
       </list>
</property>

<!-- This is the list of characters / strings that cannot be at the
start of a password.  They are treated as case-sensitive.This list is
only used to check if the generated temporary password is legal. The
legality of the final password is still checked by the UME system, not
the connector. -->
<property name="passwordCannotStartWith">
       <list>
```

```
                <value>!</value>
                <value>?</value>
                </list>
</property>
```

# Siebel Connector

The Siebel connector is not enabled by default. It is a Java connector, and it requires some prerequisites.

## What the Siebel Connector Lets You Do

The Siebel Connector lets you manage user accounts on Siebel machines and provides a single point for all user administration by letting you do the following:

- Retrieve the existing user accounts (users, employees) positions, and responsibilities, organizations, internal divisions and views from a Siebel server. Entities from lists of values (LOV) are also retrieved; this happens only when LOV values are used in custom user account mapping.
- Display properties of each of these components
- Create and modify user accounts (users, employees).
- Associate user accounts with responsibilities
- Associate user accounts with positions
- Associate user accounts with organizations
- Remove associations between user accounts and responsibilities
- Remove associations between user accounts and organizations
- Remove associations between user accounts and positions
- Delete a user account. Since deletion of a user in Siebel is not recommended, CA IdentityMinder lets you choose from the following behaviors:
  - Do nothing. Deletion is ignored. A user account disappears from CA IdentityMinder but remains intact in Siebel.
  - Simulate suspension. CA IdentityMinder changes the Siebel user's password and removes all user responsibilities (if possible, with used custom mapping and Siebel configuration).
  - Delete. CA IdentityMinder deletes a user in Siebel. This is not recommended. A user ID (login name) of a deleted account can no longer be used in Siebel.
- Simulate user account suspension/resumption by removing/restoring user’s responsibilities.
- Create, modify, and delete positions.
- Create, modify, and delete responsibilities.
- Associate responsibilities with views
- Associate responsibilities with organizations
- Remove associations between responsibilities and views
- Remove associations between responsibilities and organizations
- Create, modify, and delete internal divisions.
- Map up to 20 fields of a Siebel user to CA IdentityMinder capability attributes
- Map up to 10 fields of exposed Siebel objects other than users, to CA IdentityMinder attributes

# Siebel Installation

This connector is managed using the Connector and C++ Server installation process.

**Note:** For more information and requirements, see *Connector and C++ Connector Server Installation.*

The following section contains additional requirements needed for the connector.

## Siebel Requirements

The following are required for the Siebel connector:

- The Siebel mobile web client or the Siebel dedicated web client has to be manually installed on a machine, before or after CA IdentityMinder installation, where the C++ Connector Server is running. The Siebel web client version must be the same as a version of a managed Siebel server. See the Siebel documentation for more information.
- The Siebel Application Object Manager has to be running on a Siebel Server. See the Siebel documentation about Siebel Object Manager installation and configuration.

## Siebel Support for FIPS and IPv6

For this release of CA IdentityMinder, the Siebel Connector does not support FIPs or IPv6.

# Connector-Specific Features

This section details your connector's specific management features, such as how to acquire and explore your endpoint. Also included are account, provisioning roles, account template, and group information specifically for your connector.

## Acquire a Siebel Server Using the User Console

You must acquire the Siebel server before you can administer it with CA IdentityMinder.

**To acquire a Siebel server using the User Console**

1. Select Endpoints, Manage Endpoints,Create Endpoint
2. Select Siebel from the drop-down list box on Create a new endpoint of Endpoint Type, and click Ok

   Use the Create Siebel Endpoint page to register a Siebel server. During the registration process, CA IdentityMinder identifies the Siebel server you want to administer and gathers information about it.
3. After entering the required information, click Submit.

   You are now ready to explore and Correlate the endpoint.
4. Click Endpoints, Explore and Correlate Definitions, Create Explore and Correlate Definition to explore the objects that exist on the endpoint.

   The Exploration process finds all Siebel accounts and groups. You can correlate the accounts with global users at this time or you can correlate them later.
5. Click OK to start a new definition.
6. Complete the Explore and Correlate Tab as follows:
   a. Fill in Explore and Correlate name with any meaningful name.

      Click Select Container/Endpoint/Explore Method to click a Siebel endpoint to explore.

   b. Click the Explore/Correlate Actions to perform:
      - **Explore directory for managed objects**—Finds objects that are stored on the endpoint and not in the provisioning directory.
      - **Correlate accounts to users**—Correlates the objects that were found in the explore function with users in the provisioning directory. If the user is found, the object is correlated with the user. However, you can instead select that you want to assign the account to the existing user (the default user) or create the user.
      - **Update user fields**—If a mapping exists between the object fields and the user fields, the user fields are updated with data from the objects fields.
7. Complete the Recurrence tab if you want to schedule when the task to executes.
   a. Click Schedule.

   b. Complete the fields to determine when this task should execute.

      You may prefer to schedule the task to execute overnight to interfere less with routine access of the system.

**Note**: This operation requires the client browser to be in the same time zone as the server.  For example, if the client time is 10:00 PM on Tuesday when the server time is 7:00 AM, the Explore and Correlate definition will not work.

8. Click Submit.

**To use an explore and correlate definition**

1. In a CA IdentityMinder environment, click Endpoints, Execute Explore and Correlate.
2. Click an explore and correlate definition to execute.
3. Click Submit.

   The user accounts that exist on the endpoint are created or updated in CA IdentityMinder based on the explore and correlate definition you created.

## Acquire a Siebel Server Using the Provisioning Manager

You must acquire the Siebel server before you can administer it with CA IdentityMinder. When acquiring a Siebel server, use this procedure.

**From the Endpoint type task view**

1. Register the server as an endpoint in CA IdentityMinder.

   Use the Siebel Server Endpoint property sheet to register a Siebel Server. Necessary mapping information should be provided to associate Siebel fields and CA IdentityMinder attributes. This includes information about Siebel business objects, Siebel business components, and necessary Siebel fields for user accounts and required multi-value groups (positions, responsibilities, organizations, and views).

   During the registration process, CA IdentityMinder identifies the Siebel Server you want to administer and gathers information about it.

2. Explore the objects that exist on the endpoint.

   After registering the machine in CA IdentityMinder, you can explore its contents. Use the Explore and Correlate Endpoint dialog. The Exploration process finds all Siebel Server objects. You can correlate the user accounts with global users at this time, or you can wait to correlate them.

3. Correlate the explored user accounts with global users.

   When you correlate user accounts, CA IdentityMinder creates or links the user accounts on an endpoint with global users, as follows:

   a. CA IdentityMinder attempts to match the username with each existing global user name. If a match is found, CA IdentityMinder associates the Siebel Server user with the global user. If a match is not found, CA IdentityMinder performs the next step.

   b. If the Create Global Users as Needed button is checked, CA IdentityMinder creates a new global user and associates the Siebel user account with the global user. If the Create Global Users as Needed button is unchecked, then CA IdentityMinder performs the next step.

   c. CA IdentityMinder associates the Siebel user account with the [default user] object.

## Custom Attribute Handling in the User Console

The following are the limitations for custom attribute handling in the User Console:

- With the Siebel Connector you can have different mapping information for each acquired endpoint. For example, eTSBLUserCustomField1 can be mapped to different Siebel fields on different endpoints. In the User Console, only the same labels for all Siebel endpoints can be displayed. If you have different mapping information for each endpoint, the User Console displays custom attributes on four screens:

  - eTSBLUserCustomField1...eTSBLUserCustomField10
  - eTSBLUserCustomField11...eTSBLUserCustomField20
  - eTSBLUserCustomCapabilityField1...eTSBLUserCustomCapabilityField10
  - eTSBLUserCustomCapabilityField11...eTSBLUserCustomCapabilityField20

  You can use the first ten attributes for endpoints with one mapping type and the second ten attributes for endpoints with another mapping type.

- You can change Siebel mappings in the User Console by editing the labels manually.

  For more information, on editing screens. see the *User Console Design Guide*.

  **Note:** The account template and account profile screens are read-only screens. Before following the procedure for editing profile screens, make a copy of the account template or account profile screens and save.

- In the Provisioning Manager, a combo box control is displayed for custom attributes that have been configured to use only pre-defined values. In the User Console the attributes can be displayed, but you must type in the values.

## Create Position Tab in the User Console

Use this tab to create a special position along with a user and associate that position with the new user, possibly as Primary. A position must be associated with a division so the corresponding division field should be filled in.

The fields in this tab are listed below:

**Name**

Specifies the name of the position.

**Make Position Primary**

When checked, specifies the the position is the primary position.

**Custom Field #1-10**

Specifies the custom fields for the Siebel position.

**Parent Position**

Specifies the position's parent name. Click the Browse button to select a new parent position.

**Division**

Specifies the position's associated division name. Click the Browse button to select a new division

## User Account Suspension Handling

Siebel systems do not support user account suspension directly. Oracle recommends removing all employee's responsibilities in order to simulate suspension. An employee without any responsibility assigned is able to log into Siebel, but is not able to see Siebel data or perform any action.

## User Account Suspension Simulation

The Siebel connector supports the suspension simulation approach.

Once an account has been suspended, you must re-assign the original set of responsibilities back to the account using the Provisioning Server to resume. A new field called Enable user suspension simulation has been added to the Siebel Server tab of the Siebel endpoint and when checked, user suspension simulation is enabled.

## Directly Using the eTSuspended Attributes

In addition to the suspension simulation approach, the Siebel connector lets you map the eTSuspended attribute to any Siebel user's field. After the mapping, Siebel (or some custom code incorporated into Siebel) takes care of suspension/resumption processing.

**Note:** Suspension simulation and direct use of the eTSuspended attribute may interfere with each other, so it is not recommended to enable both direct use and simulation at the same time.

## Create User Position Feature

A new Enable create user position feature has been added to the Siebel Server tab of the Siebel Endpoint property sheet that lets you create a position for accounts. This feature can also be set using account templates. When checked, the feature is enabled and positions are created for each account and account template. When unchecked, the feature is disabled. By default, the feature is disabled.

## Error Message when Removing All Positions from an Employee

**Symptom:**

When I try to remove all positions from an employee record, I see an error message stating that an employee must have at least one position.

However, all positions are removed.

**Solution:**

When you try to remove all positions, the product works correctly and no error message should appear. This problem is due to an error in the Siebel API.

## Siebel Endpoint Property Sheet

The Siebel Endpoint Property Sheet consists of ten property pages with seven being specific to the Siebel Connector. The following property pages are Siebel specific:

**Siebel Server**

Use the Siebel Server Endpoint property page to register a Siebel Server.

**Note:** Siebel employee or user records that are used as proxy accounts in the SBL endpoint object just have a blank "New Responsibility" field.

**Mapping Table: User**

Use the Mapping Table: User property page to configure custom mappings for user single-value fields.  To edit the custom attributes in the custom attributes list box, click the Edit Button to bring up the Attribute Mapping Dialog. You can then add a new entry in a mapping table or edit an existing entry.

**Note:** When more than one item corresponding to the same CA IdentityMinder attribute appears in a mapping table, it is not considered an error. The last item found in the mapping table will be taken. This can happen when a client other than Provisioning Manager is used.

**Note:** Only one user account type is supported per endpoint.

**Mapping Table: MVG**

Use the Mapping Table: MVG property page to view and set mapping information for fields in user accounts and responsibilities associated with multi-value groups. This property page contains three similar groups of controls for the user’s positions, responsibilities, and organizations, and two groups of controls for responsibility’s views and organizations.

**Mapping Table: Position**

Use the Mapping Table: Position property page to configure custom mappings for Position's single-value fields.

**Mapping Table: Organization**

Use the Mapping Table: Organization property page to configure custom mappings for Organization's single-value fields.

**Mapping Table: Responsibility**

Use the Mapping Table: Responsibility property page to configure custom mappings for Responsibility's single-value fields.

**Mapping Table: Division**

Use the Mapping Table: Division property page to configure custom mappings for Internal Division's single-value fields.

**Mapping Table: View**

Use the Mapping Table: View property page to configure custom mappings for View's single-value fields

### Mapping Table: LOV

Use the Mapping Table: LOV property page to configure mappings for list of values' single-value fields.

## Siebel User Property Sheet

The Siebel User Property Sheet consists of six property pages with four being specific to the Siebel Connector. The following property pages are Siebel specific:

**Profile**

Use the Profile property page when managing your users and configuring custom mappings for user single-value fields. To edit the custom attributes in the custom attributes list box, click the Edit Button to bring up the Edit custom attribute Dialog. Depending on the type of control specified in the mapping table for the attribute being edited, you will see either combo box  to select a value of the user attribute or an edit box to type in the value you want for the user attribute.

**Positions**

Use this property page to manage employee positions. You can view a list of all available and occupied positions. You can select a position in the All Positions list box and move it to the Occupied Positions list box to un-assign a position. You can also move a select position from the Occupied Positions list box into the All Positions list box to un-assign an employee position. To assign an employee's primary position, you can copy a selected position from the Occupied Positions list to the Primary Positions text box by clicking the v (Down) button.

**Note:** Only the user account of "employee" type can be associated with positions. Employee must hold at least one position.

**Responsibilities**

Use this property page to manage user account's responsibilities. You can view a list of all available and assigned responsibilities. You can select a responsibility in the All Responsibilities list box and move it to the Assigned Responsibilities list box to un-assign a responsibility. You can also move a selected responsibility from the Assigned Responsibilities list box into the All Responsibilities list box to un-assign an employee responsibility. To assign an employee's primary responsibility, you can copy a selected responsibility from the Assigned Responsibilities list to the Primary Responsibility text box by clicking the v (Down) button.

**Member of (Organizations)**

Use this property page to manage employee's organizations. You can view a list of all available and assigned organizations. You can select an organization in the All Organizations list box and move it to the Member of list box to assign an organization. You can also move a selected organization from the Member of list box into the All Organizations list box to un-assign an employee organization. To assign an employee's primary organization, you can copy a selected organization from the Member of list to the Primary Organization text box by clicking the v (Down) button.

**Note:** Associating a user account with an organization is not required as this is done implicitly by Siebel. Primary organization cannot be removed from a user.

## Siebel Responsibility Property Sheet

This Siebel Responsibility Property Sheet consists of four property pages with three being specific to Siebel.

**Responsibility**

Use this property page to view the Siebel responsibility name and the custom attributes associated with the Siebel responsibility.

**Member of (Organizations)**

Use this property page to manage a responsibility's organizations. You can view a list of all available and assigned organizations. You can select an organization in the All Organizations list box and move it to the Member of list box to assign an organization. You can also move a selected organization from the Member of list box into the All Organizations list box to un-assign a responsibility’s organization. To assign a responsibility's primary organization, you can copy a selected organization from the Member of list to the Primary Organization text box by clicking the v (Down) button.

**Views**

Use this property page to manage responsibility's views. You can view a list of all available and assigned views. You can select a view in the All Views list box and move it to the Assigned list box to assign an view. You can also move a selected view from the Assigned list box into the All Views list box to un-assign a responsibility’s view.
There’s no primary view attribute for a responsibility object.

## Siebel Position Property Sheet

The Siebel Position Property Sheet consists of four property pages with three being specific to Siebel.

**Position**

Use this property page to view the Siebel position name and the custom attributes associated with the Siebel position.

**Parent Position**

Use this property page to manage a position's parent position. You can view a list of all available positions. You can select a position in the All Positions list box and move it to the Parent Position list box to assign a parent position. You can also move a position from the Parent Position list box into the All Positions list box to un-assign a position’s parent position.

**Division**

Use this property page to manage a position's division. You can view a list of all available divisions. You can select a division in the All Divisions list box and move it to the Associated Division list box to assign a division

## Siebel Organization Property Sheet

The Siebel Organization Property Sheet consists of two property pages with one, the Organization property page, being specific to Siebel.

**Organization**

Use this property page to view the Siebel organization name and the custom attributes associated with the Siebel organization.

## Siebel View Property Sheet

The Siebel View Property Sheet consists of two property pages with one, the View property page, being specific to Siebel.

**View**

Use this property page to view the Siebel view name and the custom attributes associated with the Siebel view.

## Siebel Internal Division Property Sheet

The Siebel Internal Division Property Sheet consists of three property pages with two being specific to Siebel.

**Internal Division**

Use this property page to view the Siebel division name and the custom attributes associated with the Siebel division.

**Parent Division**

Use this property page to manage a division's parent division. You can view a list of all available divisions. You can select a division in the All Divisions list box and move it to the Parent Division list box to assign a parent division. You can also move a division from the Parent Division list box into the All Divisions list box to un-assign a division’s parent division.

## Siebel LOV Property Sheet

The Siebel LOV Property Sheet consists of two property pages with one, the Properties property page, being specific to Siebel.

**Properties**

Use this property page to view the LOV code, type of value, and the display value.

# UNIX ETC and NIS Connector

The UNIX Connector provides a single point for all user administration by letting you do the following:

- Register endpoints, explore them for objects to manage, and correlate their accounts with global users
- Create and manage UNIX accounts using UNIX-specific account templates
- Change account passwords and account activations in one place
- Synchronize global users with their roles or synchronize global users' accounts with their account templates
- Assign a UNIX policy to each of your UNIX endpoints
- Use the default Endpoint Type policy to create accounts with the minimum level of security needed to access a UNIX directory
- Create and manage UNIX groups
- Generate and print reports about UNIX accounts and groups

**Note:** This connector manages UNIX NIS master servers only. Do not use this connector to mange NIS slave servers or clients.

## Installation Procedures

After installing the UNIX Connector, you must install and configure the UNIX agents and the CAM Service.

**Note:** Each package can be installed using the script installation (.sh) method.

**Important!** For HP-UX, you must install the latest Gold Quality Pack.

The UNIX agents and the CAM service can be installed by one of the following installation methods:

- Interactive installation
- Silent installation

## Install the UNIX Remote Agent

To install the UNIX Remote Agent, run the installation script from the following location:

```
RemoteAgent/UNIX/[Platform]/IdentityManager.[Platform].sh
```

where

***[Platform]***

Specifies one of AIX, HP-UX, Solaris, SolarisIntel, Linux, LinuxS390, or Tru64.

## Select the Installation Script

The installation packages for the various platforms can be found on the CD-ROM in their own subdirectory. Each package provides an lsm installation method (using a .@pif file) and a script installation method (using a .sh script), in case lsm is not available. For example, when no other CA products are installed on the system.

| Platforms | CD-ROM Folder |
|---|---|
| AIX | /cdrom/RemoteAgent/UNIX/AIX |
| HP-UX | /cdrom/RemoteAgent/UNIX/HPUX |
| Solaris Sparc | /cdrom/RemoteAgent/UNIX/Solaris |
| Solaris Intel | /cdrom/RemoteAgent/UNIX/SolarisIntel |
| Linux ix86 | /cdrom/RemoteAgent/UNIX/Linux |
| Linux s390 | /cdrom/RemoteAgent/UNIX/LinuxS390 |
| Tru64 | /cdrom/RemoteAgent/UNIX/TRU64 |

If you want to copy the Installation files from another machine to the UNIX computer, select the relevant folder for the platform and copy all its contents.

## Installation Options

The installation options are described in the following table:

| Installation Option | Description |
|---|---|
| % sh IdentityManager.[Platform].sh -r [Response File] [-F] | Installs the product.<br>A response file can be added to customize unattended installation.<br>The switch '-F' performs a forced installation and prevents the backup of the previous version of the product. |

| Installation Option | Description |
|---|---|
| lsm -e *product name* [-s] | Removes the installed product.<br>Switch '-s' runs the uninstallation in unattended mode.<br>Example: lsm -e test-product |
| lsm -l [-S] | Lists all installed products or shared components (-S). |
| lsm -A product name -d product file [-o] | Creates a backup from the installed product.<br>Switch '-o' overwrites an existing product file. |
| lsm -c product name | Checks the installed products consistency. |
| lsm -q *product name* [-l] | Shows the content of the product file.<br>Switch '-l' shows a long list including all product files. |
| lsm -Q *product file* [-l] | Shows the content of the product file. Switch '-l' shows a long list including all product files. |
| lsm -a product file -r response file | Runs the installation dialogs and creates a response file with the entered values.<br>The product is not installed. |
| lsm -v | Prints the version of the Installer being used. |

## Interactive Installation

Interactive installation includes the following steps:

1. Mounting the CD-ROM.
2. Selecting the required installation script.
3. Starting the setup wizard

## Start the Installation Wizard

Perform the following procedure to start the installation wizard.

**To start the installation wizard**

1. Switch to the directory where the installation files are located.

   Example for AIX:

   ```
   # cd /cdrom/UNIX/AIX
   ```

2. Depending on the installation method that you want to use, enter either of the following commands to start the setup wizard:

   ```
   sh IdentityManager. platform_name.sh
   ```

   ```
   lsm -i IdentityManager. platform_name.@pif
   ```

   Examples for AIX:

   ```
   # sh IdentityManager.AIX.sh
   ```

   ```
   # lsm -i IdentityManager.AIX.@pif
   ```

lsm provides a variety of installation options that can be viewed by typing lsm -? in the command line.

**More Information**

Installation Options (see page 569)

## Silent Installation

In some cases, for example, Unicenter Software Delivery, it is important to have a software product that installs automatically without any user interaction. The sh command can be executed with the option -r *response file*, and additional options, to install the UNIX Remote Agent without any questions being asked. You must provide the full path to a response file after the -r option..

The following example shows a typical response file:

```
PATHeTrustAdmin=/opt/CA/IdentityManager/ProvisioningUnixAgent
IM_INSTALL=1
OWNERroot=root
GROUPsys=sys
```

The following example shows how a response file is created using a shell script:

```
% sh IdentityManager.[Platform].sh -r [Response File]
```

The following example shows how to install a response file using a shell script:

```
% sh IdentityManager.[Platform].sh -f [Response File]
```

To uninstall, run the following shell script:

```
[Installation Path]/scripts/uninstall.sh
```

For example:

```
/opt/CA/IdentityManager/ProvisioingUnixAgent/scripts/uninstall.sh
```

**More Information**

Installation Options (see page 569)

## Silent Installation Notes

The following is a list of important notes:

- The current installation default path is /opt/CA/IdentityManager  (the previous path was /opt/CA/eta).
- If the same CAM version and build level is already installed on the target machine, CAM will not be re-installed.
- If a previous CAM version and build level is already installed on the target machine, CAM will be upgraded using the installation path of the current installation, which is stored in the following file:

  ```
  /etc/catngcampath
  ```

  If a previous CA IdentityMinder Remote Agent is already installed on the target machine, the Remote Agent will be upgraded using the installation path of the current installation, which is stored in the following file:

  ```
  /etc/catngdmopath.tng
  ```

- If, on the target machine, the DISPLAY variable is set and a JAVA VM is installed, the installation will run in graphical mode.
- In VT100 mode, the terminal must provide a resolution of 80 (columns) x 24 (rows) or higher.
- On a UNIX machine with double-byte characters, CAM must be started with a shell having the “locale” set to C/Posix:

  ```
  `cat /etc/catngcampath`/bin/camclose
  LANG=C
  export LANG
  `cat /etc/catngcampath`/scripts/rc
  ```

- If you install the UNIX agent using Telnet, make sure that the environmental variable TERM is set to VT100.

## Grant Access to the Provisioning Server Host

To grant access to the Provisioning Server host on this machine, run the following command:

```
`cat /etc/catngcampath`/bin/cafthost -a hostname
```

where *hostname* is the name or the IP address of the machine hosting the Provisioning Server.

Example for any platform:

```
# `cat /etc/catngcampath`/bin/cafthost -a etradmsrv01
```

## Install the UNIX Remote Agent

Perform the following procedure to install the UNIX remote agent.

**To install the UNIX remote agent**

1. Locate the Provisioning Component installation media.
2. Run the Agent installer under \Remote Agent

   Follow the onscreen instructions to complete the installation.
3. The Welcome dialog that shows the UNIX Remote Agent version appears. View the dialogue.
4. Click Next. The Select Installation directory dialog appears. Enter a valid installation directory.

   The product is installed under the specified installation directory.

   ```
   /opt/CA/IdentityManager/ProvisioningUnixAgent
   ```

   This is the name of the actual directory where you want to install the UNIX Remote Agent. All files are placed in this directory or its subdirectories. You can change the name of the installation directory or it will be created if it does not already exist.

   **Note:** If you run this procedure on a computer on which an older version of the UNIX Remote Agent is installed, the old installation path is read from the /etc/catngdmopath.tng marker file and set as the Installation directory.

   During an update installation, the product installation directory cannot be modified.
5. Click Next to continue.

   The Summary dialog appears. Check the following installation parameters:

   ```
   PATHCA IdentityMinder=/opt/CA/IdentityManager/ProvisioningUnixAgent
   IM_INSTALL=1
   OWNERroot=root
   GROUPsys=sys
   ```
6. Click Install product to run the installation.

7. View the installation log.

   The following lines are logged by the installation:

```
Installing Dependency - CA Installer [1/2]...
Installing Dependency - CA Installer [2/2]...
Preparing next Installer phase
Executing post interview phase
Checking package dependencies
Checking disk space

Installation product "ca-dsm-sd-installer", version "4.3.x.x"
================================================================
++  Call script "scripts/preinstall_installer.sh"
++  Script executed successfully
++  Installation component "preinstall"
++  Component "preinstall" installed successfully
++  Installation component "base"
++  Component "base" installed successfully
++  Installation component "base_root"
++  Component "base_root" installed successfully
++  Installation component "base_shared"
++  Component "base_shared" installed successfully
++  Installation component "conf"
++  Component "conf" installed successfully
++  Installation component "man, ENU"
++  Component "man, ENU" installed successfully
++  Call script "scripts/postinstall_installer.sh"
++  Script executed successfully
Job executed successfully

Installing Dependency - CAM...
Installing Dependency - ETPKI...
Preparing next Installer phase
Executing post interview phase
```

```
Checking package dependencies
Checking disk space

Backup product "ca-cs-utils", version "11.0.x.x"
===================================================
++  Backup component "preinit_csutils"
++  Component "preinit_csutils" saved successfully
++  Backup component "csutils"
++  Component "csutils" saved successfully
++  Backup component "csutils_platform_files"
++  Component "csutils_platform_files" saved successfully
++  Backup component "csutils_libv2"
++  Component "csutils_libv2" saved successfully
Job executed successfully

Reinstallation product "ca-cs-utils", version "11.0.x.x"
===========================================================
++  Call script "/bin/sh csutils/scripts/prein_csutils.sh"
++  Script executed successfully
++  Reinstallation component "preinit_csutils"
++  Component "preinit_csutils" installed successfully
++  Reinstallation component "csutils"
++  Component "csutils" installed successfully
++  Reinstallation component "csutils_platform_files"
++  Component "csutils_platform_files" installed successfully
++  Reinstallation component "csutils_libv2"
++  Component "csutils_libv2" installed successfully
++  Call script "/bin/sh csutils/scripts/install.csutils"
++  Script executed successfully
Job executed successfully

Installation product "ca-cs-etpki", version "3.2.x.x"
=====================================================
++  Call script "/bin/sh pifscripts/prein.etpki"
++  Script executed successfully
++  Installation component "preinit_etpki"
++  Component "preinit_etpki" installed successfully
++  Installation component "cs-etpki-base"
++  Component "cs-etpki-base" installed successfully
++  Installation component "cs-etpki-lib"
++  Component "cs-etpki-lib" installed successfully
++  Call script "/bin/sh pifscripts/postin.etpki"
++  Script executed successfully
Job executed successfully


Installing CA IdentityMinder
Preparing next Installer phase
Executing post interview phase
Checking package dependencies
Checking disk space
Installation product "IdentityManager", version "12.0.x.x"
=================================================================
++  Installation component "im"
++  Call script "scripts/imscript.sh preinstall"
++  Script executed successfully
+++ Call component script "scripts/imscript.sh postinstall"
+++ Script executed successfully
++  Component "im" installed successfully
++  Installation component "preinstall, ENU"
++  Component "preinstall, ENU" installed successfully
Job executed successfully
```

Note: All prerequisite components are installed after the UNIX Agent installer has been executed. This applies to both upgrade and new installations despite the “Cancel” option being selected during the installation process

## Install Unix Remote Agent on Red Hat Itanium 64-bit

The Unix Remote Agent is a 32-bit package. If you install it on Red Hat/Itanium 64-bit, then you must install the IA-32 Execution Layer and some compatibility libraries before you install the agent.

If you are using RPM v4.2.3 or later, then there is an additional step to perform to work around a known bug in RPM. RPM v4.2.3 or later has a backward-compatibility problem with older RPM packages. The problem causes RPM to resolve the following compatibility library folder incorrectly:

- /emul/ia32-linux as /emul/ia32-Linux (note the capital 'L')

You can work around this problem either of in the two ways listed in Step 3, depending on your environment.

**Note:** For more information, see the Red Hat Knowledge Base and the Red Hat bug report.

**To install UNIX Remote Agent on Red Hat Itanium 64-bit**

1. Install the IA-32 Execution Layer.
2. Install the following compatibility libraries from the 32-bit Compatibility Layer Disc that matches your Red Hat installation.
   - glibc
   - bash
   - libtermcap
3. Work around the bug in RPM in one of the following ways, depending on your environment:
   - Create a symlink. For example:

     ```
     ln -s /emul/ia32-linux /emul/ia32-Linux
     ```
   - Add the following in /etc/rpm/macros:

     ```
     %_autorelocate_path /emul/ia32-linux
     ```

## Manage the CAM Service

The CAM Service is a daemon process that you can view, stop, or start on your UNIX server. Typically, the superuser or the system's root user starts the CAM Service.

## View the CAM Service

You can perform the following procedure to find out who started the service.

**To view the CAM service**

1. Log on to your UNIX machine as root by using the Telnet or SSH client.
2. Issue the following UNIX command:

   ```
   ps -ef | grep cam
   ```

   A display similar to the following one appears:

   ```
   root 13822        1 11 11:30:12 ?   0:00 cam

   root 13843 13753  3 11:56:31 pts/5  0:00 grep cam
   ```

**Note:** If the system's root user does not start the services, they will appear started, but you will be unable to use them. CA IdentityMinder issues the following message: “Permission denied: user must be root”.

## Stop the CAM Service

You can stop the CAM service by performing the following procedure.

**To stop the CAM Service**

1. Log on to your UNIX machine as root by using the Telnet or SSH client.
2. Change to the cam scripts directory:

   ```
   cd `cat /etc/catngcampath`/scripts
   ```

3. Issue the following UNIX command:

   ```
   . ./envset
   ```

   **Note:** This command must have a space between the two dots.
4. Change to the cam bin directory:

   ```
   cd ../bin
   ```

5. Issue the following UNIX command:

   ```
   ./camclose
   ```

   **Note:** This command stops the CAM Service. After stopping this service, you must restart it so CA IdentityMinder can communicate with your UNIX server.

## Restart the CAM Service

You can restart the CAM service by performing the following procedure.

**To restart the CAM Service**

1. Log on to your UNIX machine as root by using the Telnet or SSH client.
2. Change to the cam scripts directory:

   ```
   cd `cat /etc/catngcampath`/scripts
   ```

3. Issue the following UNIX command:

   ```
   . ./envset
   ```

   **Note:** This command must have a space between the two dots.

4. Issue the following command to restart the CAM Service:

   ```
   ./rc
   ```

## How to Restart Automatically the CAM Service

If you want to automatically start the CAM Service after rebooting a machine, you can use the init or rc utilities.

To start the CAM Service automatically after rebooting a UNIX server, verify the following:

- Unicenter runtime environment is known to the CAM Service
- Unicenter BIN directory appears in the PATH variable

For example, a typical Start shell script appears as follows:

```
#!/bin/sh
# @(#)install 3.24 10:15:49 98/05/29
# Date Created: Tue Jul 20 11:57:34 WET DST 2004
.
.
.
.
 # Start CA Message Queuing Server
su $AGENT_OWNER -c /export/home/cam/cam/scripts/rc
If you add the commands above, the Start shell script appears as follows:
 #!/bin/sh
# @(#)install 3.24 10:15:49 04/05/29
# Date Created: Tue Jul 20 11:57:34 WET DST 2004
.
.
.
.
PATH=$PATH:$CAIGLBL0000/bin
export PATH
# Start CA Message Queuing Server
su $AGENT_OWNER -c /export/home/cam/cam/scripts/rc
```

## Using the Init Utility

To start the CAM Service using the init utility, add the following line to the end of the /etc/inittab file:

```
cam::once:`cat /etc/catngcampath`/scripts/rc
```

By adding this line, the shell script created when you installed the CAM Service is executed. After it executes, verify that you can view the daemon process.

## Using the RC Utility

To start the CAM Service using the rc utility, perform the following steps:

1. Copy the start shell script to the init.d directory.
2. Create a shell script under the rc2.d sequencer directory by following the rc syntax.

**Notes:**

- The rc utility is not applicable on IBM-AIX platforms.
- The location of the directories shown previously may be different on each UNIX platform; the directories are normally located under either the /bin or the /etc directory. For more information, see the documentation for your specific UNIX system.

## How to Restrict CAFT Commands

By default, CAFT allows any command to be executed from an authorized host. As the UNIX Connector only needs to run the uxsautil command, the CAFT caftexec script can be customized to filter commands and to allow only the uxsautil binary.

An example of such a script and its configuration file are provided in the

`cat /etc/catngdmopath.tng`/scripts folder, and can be copied to the `cat /etc/catngcampath` folder:

```
# cd `cat /etc/catngcampath`

# mv caftexec caftexec.back

# cp -p `cat /etc/catngdmopath.tng`/scripts/caftexec* .
```

## Install the CAM and CAFT Encryption Key

Encryption is supported for Win32, AIX, HP-UX, Solaris, and Linux x86 applications. The default and only available encryption algorithm is Triple-DES (168 bits key) with CBC mode.

**To install the encryption key**

1. Enter the following command at the command prompt to generate your key file:

   ```
   #PATH=`cat /etc/catngcampath`/bin:$PATH

       #export PATH
   #caftkey -g keyfile password
   ```

   ***keyfile***

   Name that you assign to the key file.

   ***password***

   Password that you assign to the key file.

   **Note:** The caftkey command and attributes are the same for Win32 platforms.

2. Install your Public Key on both CAFT Agent and CAFT Admin boxes using the previously-generated key file by entering the following command at the command prompt:

   ```
   #PATH=`cat /etc/catngcampath`/bin:$PATH
       #export PATH
   #caftkey -policy_setting keyfile password
   ```

   ***keyfile* and *password***

   The values that you specified in Step 1.

   **-Policy_setting**

   -i, -m, or blank.

   **More information:**

   policy_setting Options (see page 584)

3. Recycle the CAM Service on each box where you installed the new Key by stopping the CAM service, and starting it again:

   ```
   prompt> camclose              //stop Cam/Caft service and processes
   prompt> cam start             //start CAM service and process
   ```

### policy_setting Options

Policy_setting governs the communication between this computer (the local computer) and other computers that have the CAM and CAFT service installed, but may or may not have the CAM and CAFT encryption certificates installed.

The options are as follows:

**caftkey -i keyfile password**

The -i option specifies Policy -1. This policy lets computers running previous versions of the CAM and CAFT service execute commands on this computer and lets this computer execute commands on those computers.

Policy -1 encrypts messages if the other computer has these certificates installed. This policy does not encrypt messages if the other computer does not have these certificates installed.

**caftkey -m keyfile password**

The -m option specifies Policy 1. This policy prohibits other computers from executing commands on this computer if they are running previous versions of the CAM and CAFT service without the encryption certificates. This policy also prohibits this computer from executing commands on those computers.

If both computers have the CAM and CAFT encryption certificates installed, but have different Public Key Files installed when Policy 1 is set, the command requests between the two computers fails.

**caftkey keyfile password**

The blank option specifies Policy 0. This policy is set if no Public Key File is installed, the CAM and CAFT encryption certificates were not installed properly, or if you do not specify a policy setting when you enter the caftkey command. Policy 0 specifies no encryption.

**Note:** The CAM and CAFT service must already be installed on the computer in your network.

### Check the Policy Setting

To see the operational mode of the machine, check the following file:

```
%CAI_MSQ%/ftlogs/dg000
```

## UNIX Support for FIPS and IPv6

For this release of CA IdentityMinder, the UNIX Connector supports IPv6. FIPS is supported only on Solaris Sparc, Linux x86, HPUX, and AIX.

UNIX PAM supports IPv6 only.

# Connector-Specific Features

This section details your connector's specific management features, such as how to acquire and explore your endpoint. Also included are account, provisioning roles, account template, and group information specifically for your connector.

## Acquire a UNIX-ETC Server Using the User Console

You must acquire the UNIX-ETC Server before you can administer it with CA IdentityMinder.

**To acquire a UNIX-ETC server using the User Console**

1. Select Endpoints, Manage Endpoints,Create Endpoint
2. Select UNIX-etc from the drop-down list box on Create a new endpoint of Endpoint Type, and click Ok

   Use the Create UNIX-etc plus Domains Endpoint page to register a UNIX-etc system. During the registration process, CA IdentityMinder identifies the UNIX-etc system you want to administer and gathers information about it.
3. After entering the required information, click Submit.

   You are now ready to explore and Correlate the endpoint.
4. Click Endpoints, Explore and Correlate Definitions, Create Explore and Correlate Definition to explore the objects that exist on the endpoint.

   The Exploration process finds all UNIX-etc accounts and groups. You can correlate the accounts with global users at this time or you can correlate them later.
5. Click OK to start a new definition.
6. Complete the Explore and Correlate Tab as follows:

   a. Fill in Explore and Correlate name with any meaningful name.

      Click Select Container/Endpoint/Explore Method to click a UNIX-etc endpoint to explore.

   b. Click the Explore/Correlate Actions to perform:

      - **Explore directory for managed objects**—Finds objects that are stored on the endpoint and not in the provisioning directory.
      - **Correlate accounts to users**—Correlates the objects that were found in the explore function with users in the provisioning directory. If the user is found, the object is correlated with the user. However, you can instead select that you want to assign the account to the existing user (the default user) or create the user.
      - **Update user fields**—If a mapping exists between the object fields and the user fields, the user fields are updated with data from the objects fields.

7. Complete the Recurrence tab if you want to schedule when the task to executes.

   a. Click Schedule.

   b. Complete the fields to determine when this task should execute.

      You may prefer to schedule the task to execute overnight to interfere less with routine access of the system.

   **Note**: This operation requires the client browser to be in the same time zone as the server. For example, if the client time is 10:00 PM on Tuesday when the server time is 7:00 AM, the Explore and Correlate definition will not work.

8. Click Submit.

**To use an explore and correlate definition**

1. In a CA IdentityMinder environment, click Endpoints, Execute Explore and Correlate.

2. Click an explore and correlate definition to execute.

3. Click Submit.

   The user accounts that exist on the endpoint are created or updated in CA IdentityMinder based on the explore and correlate definition you created.

## Acquire a UNIX-NIS Server Using the User Console

You must acquire the UNIX-NIS Server before you can administer it with CA IdentityMinder.

**To acquire a UNIX-NIS server using the User Console**

1. Select Endpoints, Manage Endpoints,Create Endpoint

2. Select UNIX-NIS-NIS plus Domains from the drop-down list box on Create a new endpoint of Endpoint Type, and click Ok

   Use the Create UNIX-NIS_NIS plus Domains Endpoint page to register a UNIX-NIS system. During the registration process, CA IdentityMinder identifies the UNIX-NIS system you want to administer and gathers information about it.

3. After entering the required information, click Submit.

   You are now ready to explore and Correlate the endpoint.

4. Click Endpoints, Explore and Correlate Definitions, Create Explore and Correlate Definition to explore the objects that exist on the endpoint.

   The Exploration process finds all UNIX-NIS accounts and groups. You can correlate the accounts with global users at this time or you can correlate them later.

5. Click OK to start a new definition.

6. Complete the Explore and Correlate Tab as follows:

   a. Fill in Explore and Correlate name with any meaningful name.

      Click Select Container/Endpoint/Explore Method to click a UNIX-NIS endpoint to explore.

   b. Click the Explore/Correlate Actions to perform:

      - **Explore directory for managed objects**—Finds objects that are stored on the endpoint and not in the provisioning directory.

      - **Correlate accounts to users**—Correlates the objects that were found in the explore function with users in the provisioning directory. If the user is found, the object is correlated with the user. However, you can instead select that you want to assign the account to the existing user (the default user) or create the user.

      - **Update user fields**—If a mapping exists between the object fields and the user fields, the user fields are updated with data from the objects fields.

7. Complete the Recurrence tab if you want to schedule when the task to executes.

   a. Click Schedule.

   b. Complete the fields to determine when this task should execute.

      You may prefer to schedule the task to execute overnight to interfere less with routine access of the system.

   **Note**: This operation requires the client browser to be in the same time zone as the server. For example, if the client time is 10:00 PM on Tuesday when the server time is 7:00 AM, the Explore and Correlate definition will not work.

8. Click Submit.

**To use an explore and correlate definition**

1. In a CA IdentityMinder environment, click Endpoints, Execute Explore and Correlate.

2. Click an explore and correlate definition to execute.

3. Click Submit.

   The user accounts that exist on the endpoint are created or updated in CA IdentityMinder based on the explore and correlate definition you created.

## Acquire a UNIX Server Using the Provisioning Manager

You must acquire the UNIX server before you can administer it with CA IdentityMinder. In order to acquire a UNIX server, perform the following steps from the Endpoint Type task view:

1. Register the machine as a stand-alone server or as an NIS or NIS+ server.

   - To register a UNIX endpoint as a stand-alone server, select UNIX ETC Endpoint.
   - To register a UNIX endpoint as an NIS or NIS+ server, select NISEndpoint from the Object Type, and then click New.

   Use the UNIX Endpoint property sheet to register a UNIX machine. During the registration process, CA IdentityMinder identifies the UNIX machine you want to administer and gathers information about it.

2. Explore the objects that exist on the endpoint.

   After registering the server in CA IdentityMinder, you can explore its contents. Use the Explore and Correlate Endpoint dialog. The Exploration process finds all UNIX accounts and groups. You can correlate the accounts with global users at this time or later.

3. Correlate the explored accounts with global users.

   When you correlate accounts, CA IdentityMinder creates or links the accounts on an endpoint with global users, as follows:

   a. CACA IdentityMinder attempts to match the UNIX account name with each existing global user name. If a match is found, CA IdentityMinder associates the UNIX account with the global user. If a match is not found, CA IdentityMinder performs the next step.

   b. CA IdentityMinder attempts to match the UNIX account description field with each existing global user's full name. If a match is found, CA IdentityMinder associates the UNIX account with the global user. If a match is not found, CA IdentityMinder performs the next step.

   c. CA IdentityMinder associates the UNIX account with the *default user* global user object.

## Explore and Correlate on Linux Suse

If you receive an error when trying to explore and correlate on a Linux 390 ETC endpoint, you must manually add the account to /etc/shadow. On Linux Suse, an account exists in /etc/password only.

## Disable Passwd and Shadow Synchronization

If shadow passwords are enabled on the UNIX system, sometimes etc/passwd and /etc/shadow files contain a different number of users. This problem causes failures when the connector attempts to create a user account in UNIX. The connector checks the synchronization between etc/passwd and /etc/shadow files during endpoint acquisition and during exploration. If the UNIX system contains more than 5,000 users, this check can be time-consuming.

To omit the synchronization check, select the following option on endpoint object during acquisition: "Disable etc/passwd and etc/shadow files synchronization check." This option requires that the remote UNIX endpoint is running CA IdentityMinder r12.5 SP9 (or higher) UNIX Remote Agent.

## Default Primary Group on Endpoint Property Sheet

A field called Default Primary Group is available to let you select a default Primary Group at the Endpoint level.

## Default Primary Group on Accounts and Account Templates in the User Console

The default primary group of an NIS/ETC endpoint is populated to an account being created.

If an account is created from an account template, there are two scenarios in the Provisioning Manager.

1. Endpoint has a default primary group, the account is created successfully no matter whether the “primary group” field is blank or [default] in the account template.
2. Endpoint has no default primary group, the account creation fails if “primary group” attribute is [default] unless the attribute is configured with another group name in the account template.

In the User Console, the primary group in an account template is either blank or a real group name. This is the same as the above with the same behaviors on Provisioning Server.

## Selecting the Character Set on the Endpoint Property Sheet

When checked, UTF-8 Character Set encoding will be used for values passed on between the Provisioning Server and the UNIX Remote Agent instead of the one used by the Provisioning Server. A combo list box is enabled in the so that you can select the character set used on the end-point system.

## Long Multi-Byte Character Strings Return Error Message

Using very long multi-byte character strings in the Full Name field can return a deceptive error message.

To avoid getting this error message, do not use extremely long multi-byte character strings in this field.

## UNIX Groups

The Provisioning Manager lets you create and maintain UNIX groups using the Endpoint Type task view. Use the ETC or NIS Group property sheet to manage your groups.

## NIS Netgroups

Netgroups are logical groups of hosts, accounts or both. Use the UNIX NIS Netgroup property sheet when managing netgroups and user netgroup activity.

For more information, see the Working with Endpoints, Connector Procedures in the *Provisioning* help

## Mandatory Properties for etautil Add Command

If you use the etautil add command to register UNIX endpoints, you must specify one of the following properties:

- For stand-alone UNIX servers, specify the eTETCHost eTETCUnicenterSec, and eTETCUnicenterUser properties. For example:

  ```
  etautil ... add
    'eTNamespaceName=UNIX - etc' eTETCDirectory eTETCDirectoryName=exdevsrv
     eTETCHost=exdevsrv  eTETCUnicenterSec=0  eTETCUnicenterUser=0
  ```

- For UNIX servers running NIS or NIS+, specify the eTNISHost , eTNISDomainName, eTNISUnicenterSec, and eTNISUnicenterUser properties.  For example:

  ```
  etautil ... -u etaadmin -p etaadmin add
    'eTNamespaceName=UNIX - NIS-NIS plus Domains'
  eTNISDirectory eTNISDirectoryname='nisdomain.com[exdevsrv]'
      eTNISHost=exdevsrv
      eTNISDomainName=nisdomain.com eTNISUnicenterSec=0 eTNISUnicenterUser=0
  ```

## UNIX Etautil Conventions

Use the following UNIX conventions in your etautil commands:

- The Endpoint Type name (eTNamespaceName) is UNIX - etc for stand-alone servers and UNIX - NIS-NIS plus Domains for NIS and NIS+ servers
- The Endpoint Type prefix is ETC. Therefore, the UNIX class names are:
  - eTETCDirectory for an endpoint on a stand-alone server
  - eTETCPolicyContainer for an account template container on a stand-alone server
  - eTETCPolicy for an account template on a stand-alone server
  - eTNISDirectory for an endpoint on an NIS or NIS+ server
  - eTNISPolicyContainer for an account template container on an NIS or NIS+ server
  - eTNISPolicy for an account template object class on an NIS or NIS+ server

For more information about the etautil command, see the *Reference* help.

**More Information**

Distinguished Names (see page 602)

## Exit Commands

CA IdentityMinder supports the following exit types:

- **Pre Exit** means that the agent executes a user command before it performs its own operation.
- **Post Exit** means that the agent executes a user command after it performs its own operation.

## Configuration File

CA IdentityMinder implements the pre-exits and post-exits on the UNIX agents. To trigger user add-on commands, you must define them in the ExitSetup.ini file that is installed by CA IdentityMinder. By default, this file does not activate any specific command.

The ExitSetup.ini file is located in the following directory:

```
/opt/CA/IdentityManager/ProvisioningUnixAgent/etc/
```

**Note:** The exact location is specified in the /etc/catngdmopath.tng file.

The following table describes the typical contents of the configuration file:

| Headers and Variables | Value | Description |
|---|---|---|
| [Pre-exit] | | Pre-exit section header |
| Command= | Provided by the user | User command specified with the absolute path |
| Stop on error= | Yes/No | Yes-specifies that the CA IdentityMinder agent command is not launched if the pre-exit fails<br>No-specifies that the CA IdentityMinder agent command is launched even if the pre-exit fails. This is the default value. |
| [Post-exit] | | Post-exit section header |
| Command= | Provided by the user | User command specified with the absolute path |

## Conditions for the execution of the EXIT Commands

The conditions for the execution of the exit commands are as follows:

- For CA IdentityMinder, the execution of a command is successful if its return code (RC) is equal to 0; any other code indicates that the execution failed. This is important because the values that are caught by CA IdentityMinder are processed according to the value of the return code.
- The argument values, which are sent to CA IdentityMinder agents, are also sent to the user program.
- The pre-exit and post-exit user commands are logged in the CA IdentityMinder log files. You can also write messages in the log files, using the PrintMessage function, which is defined in the source template and delivered with the product.
- The pre-exit and post-exit commands are executed each time the CA IdentityMinder agent is executed.

# Managing Passwords

CA IdentityMinder can intercept an account password change on a UNIX or Linux system, and propagate it to all other accounts associated with its Global User. CA IdentityMinder Pluggable Authentication Module (PAM) lets CA IdentityMinder authenticate passwords against external security systems so that global users can use their existing system passwords to log on to CA IdentityMinder.

For more information, see the *Administration Guide*.

# Appendix A: Support for FIPS and IPv6

The following table lists the connectors that support FIPS and IPv6:

| Connector | FIPs Support | IPv6 Support |
|---|---|---|
| CA Access Control | No | No |
| CA ACF2 and Password Synchronization Agent for ACF2 | No | Yes |
| CA Arcot RiskFort | No | No |
| CA Arcot WebFort | No | No |
| CA Data Loss Prevention (CA DLP) | Yes | No |
| CA Single Sign-On | No | No |
| CA Top Secret and Password Synchronization Agent for Top Secret | No | Yes |
| Google Apps | No | No |
| IBM DB2 UDB | No | Yes |
| IBM DB2 z/OS | No | No |
| IBM i5/OS (OS/400) | No | No |
| IBM i5/OS (OS/400) Password Synchronization Agent | No | No |
| IBM Lotus Notes Domino Server | No | No |
| IBM RACF - Security | No | Yes |
| Kerberos | No | No |
| Microsoft Active Directory | No | No |
| Microsoft Exchange | No | No |
| Microsoft SQL Server | No | Yes |
| Microsoft Windows (XP, Vista, 7) | Yes | Yes |
| Oracle Server | No | No |
| Oracle E-Business Suite | No | No |
| PeopleSoft HRMS | No | No |
| RSA SecurID | No | No |

| Connector | FIPs Support | IPv6 Support |
|---|---|---|
| SalesForce | No | No |
| SAP R/3 | No | No |
| SAP UME | No | No |
| Siebel CRM | No | No |
| UNIX | Yes<br>**Note:** Supported on Solaris Sparc, Linux x86, HPUX AIX only | Yes |

# Appendix B: Endpoint Schema and Structure

This section contains the following topics:

Endpoint Schema (see page 597)
Endpoint Structure (see page 602)

This appendix provides an overview of the endpoint schema and structure of the Standard Connectors. The endpoint schema and structure is required when you:

- Use a general purpose LDAP utility to construct batch processes interfacing with the Provisioning Server
- Build, interpret, or modify LDAP Interface File Format (LDIF) files to work with CA IdentityMinder data and combine it with data from other LDAP-enabled applications.

For more information about endpoint schemas and structures, see the Administrator Guide and the Programming Guide for Provisioning.

## Endpoint Schema

An endpoint *schema* consists of the object classes, attributes in object classes, and attribute types. All of this information is necessary when constructing syntactically correct LDAP operations, such as LIST, SEARCH, ADD, MODIFY, and DELETE.

The endpoint schema for your directories is described in the following sections. The schema files discussed in these sections are located under the *PS_HOME*\Data\Endpoint TypeDefinition directory.

For more information about schemas, see the *Programming Guide for Provisioning*.

## SchemaAbridged.txt File

The *xxx*SchemaAbridged.txt file provides a list of each object class and attribute in the schema. For each attribute, only the most commonly used keywords are supplied. Use this file if you are constructing LDAP-compatible files for any of the batch processes.

***xxx***

Specifies the three or four letter acronym for a connector. Click here to see the connector names and acronym's.

## SchemaUnabridged.txt File

The *xxx*SchemaUnabridged.txt file provides a complete list of each object class and attribute in the schema and includes all the information provided in the *xxx*SchemaAbridged.txt file, as well as additional information required when parsing, formatting, and presenting the data received from the your Connector. Use this file if you need more detailed information for the object classes and attributes in the your Connector.

***xxx***

Specifies the three or four letter acronym for a connector. Click here to see the connector names and acronym's.

### Connector Acronyms

The following list contains the acronyms for the CA IdentityMinder connectors used in this appendix:

| Acronym | Connector |
|---|---|
| ACC | CA Access Control |
| ACF | CA ACF2 |
| ADS | Active Directory Services |
| AS4 | OS/400 |
| DBZ | DB2 UDB for z/OS |
| DB2 | DB2 UDB |
| ETC | UNIX ETC |
| E2K | Windows Exchange Server |
| FND | Oracle Applications |
| KRB | Kerberos |

| Acronym | Connector |
|---|---|
| LND | Lotus Notes/Domino |
| NIS | UNIX NIS |
| N16 | Windows NT |
| ORA | Oracle |
| PLS | SSO for Advanced Policy Server |
| PPS | PeopleSoft |
| RAC | RACF |
| RSA | RSA ACE (SecurID) |
| SAP | SAP |
| SBL | Siebel |
| SQL | MS SQL |
| TSS | CA Top Secret |

## File Formats

The format of these files is defined using two distinct definitions: object class definitions and attribute definition

## Object Class Definitions

The lines that define the object classes are in the following form:

```
CLASS user_friendly_name
    LDAP ObjectClass Name : ldap_name
    ExternalName: external_name
    NamingAttributes: naming_attribute
```

*user_friendly_name*

Specifies the user-friendly object class name.

*ldap_name*

Specifies the LDAP name used for defining the schema.

*external_name*

Specifies the relative distinguished name (RDN) value for containers.

*naming_attribute*

Specifies the RDN attribute.

## Attribute Definitions

Directly beneath the object class definition are several attribute lines. These lines define the attribute types in the object class. Depending on which file you are viewing, the list can vary.

```
ATTRIBUTE (LDAP Name) ldap_object_class_name::ldap_attribute_name
        User-friendly Name : user_friendly_name
        Description: Global description
        ProhibitedCharacters: prohibchars
        MinLength: minlength
        MaxLength: maxlength
        EditType: edittype
        IsSpaceAllowedIn: spaces
        IsAsciiOnly: ascii
        IsMultiValued: multi-valued
        Case: case
```

***ldap_object_class_name***

Specifies the LDAP name used for the object class.

***ldap_attribute_name***

Specifies the LDAP name of the attribute.

***user_friendly_name***

Specifies the user-friendly name.

***description***

Specifies the description of the attribute.

***prohibchars***

Specifies a list of characters prohibited in the attribute.

***minlength***

Specifies the minimum length of the attribute value.

***maxlength***

Specifies the maximum length of the attribute value.

***edittype***

Determines the type of data in LDAP and its characteristics.

***spaces***

Defines a Boolean value that identifies whether spaces are allowed.

***ascii***

Defines a Boolean value that determines whether the attribute supports ASCII values.

***multi-valued***

Defines a Boolean value that determines whether the attribute is multi-valued.

***case***

Specifies a string that identifies whether the attribute can contain uppercase or lowercase characters. This string can be insensitive, insensitive-upper, insensitive-lower, sensitive, sensitive-upper, or sensitive-lower.

# Endpoint Structure

Equally important to the endpoint schema is the hierarchical relationship that exists between the objects in the endpoint. This relationship is expressed through an endpoint structure called the Data Information Tree (DIT). Knowing the hierarchy is essential to constructing syntactically correct endpoint operations.

## Distinguished Names

Distinguished names (DNs) identify the objects in a Endpoint Type. They contain a sequence of individual entries that specifies the location of an object in the DIT. That is, the DN is similar to a file system path name.

In CA IdentityMinder, the format of the DN consists of two parts: a base DN and a domain name suffix. The base DN specifies the DN of an object without any domain information. You must specify only the base DN when writing batch processes.

For example, a base DN of an Active Directory Services object is:

```
eTADSAccountName=my_account,eTADSContainerName=Active Dir. Folder,
eTADSDirectoryName=directory_name,
eTNamespaceName=ActiveDirectory,domain_name_suffix
```

The domain name suffix specifies the suffix value of the domain. This parameter is the combination of the domain name RDN, its parent domain RDNs, and the CA IdentityMinder suffix (dc=eta). You must specify the domain name suffix and the base DN when writing LDIF files. For example, if your domain name is chicago, its parent domain name is illinois, and the root domain name is usa, then the domain name suffix for your domain is:

```
dc=chicago,dc=illinois,dc=usa,dc=eta
```

Then, when accessing a logon ID using an Active Directory Services account, the DN would look like this:

```
eTADSAccountName=my_account,eTADSContainerName=Active Dir. Folder,
eTADSDirectoryName=directory_name,
eTNamespaceName=ActiveDirectory,dc=chicago,dc=illinois,dc=usa,dc=eta
```

## Connector Objects and DNs

The following sections list the Connector objects and their DNs in hierarchical order:

### DBZ Server Objects

The following table lists the DBZ Server objects and their DNs in hierarchical order:

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTNamespace | eTNamespaceName=DB2 ZOS Server,<br>domain_name_suffix |
| eTDBZDirectory | eTDBZDirectoryName=directory_name,<br>eTNamespaceName=DB2 ZOS Server,<br>domain_name_suffix |

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTDBZNamespace | eTNamespaceName=DB2 ZOS endpoint type name, eTDBZDirectoryName=directory_name, eTNamespaceName=DB2 ZOS Server, domain_name_suffix |
| eTDBZAccountContainer | eTDBZAccountContainerName=Accounts, eTDBZDirectoryName=directory_name, eTNamespaceName=DB2 ZOS Server, domain_name_suffix |
| eTDBZAccount | eTDBZAccountName=DB2 ZOS Account, eTDBZAccountContainerName=Accounts, eTDBZDirectoryName=directory_name, eTNamespaceName=DB2 ZOS Server, domain_name_suffix |

## DB2 UDB Objects

The following table lists the DB2 UDB objects and their DNs in hierarchical order:

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTNamespace | eTNamespaceName=DB2 *Server,domain_name_suffix* |
| eTDB2Directory | eTDB2DirectoryName=*directory_name,* eTNamespaceName=DB2 *Server,domain_name_suffix* |
| eTDB2AccountContainer | eTDB2AccountContainerName=Accounts, eTDB2DirectoryName=*directory_name,* eTNamespaceName=DB2 *Server,domain_name_suffix* |
| eTDB2Account | eTDB2AccountName=DB2 User, eTDB2AccountContainerName=Accounts, eTDB2DirectoryName=*directory_name,* eTNamespaceName=DB2 *Server,domain_name_suffix* |

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTDB2GroupContainer | eTDB2GroupContainerName=Groups,<br>eTDB2DirectoryName=*directory_name,*<br>eTNamespaceName=DB2 *Server,domain_name_suffix* |
| eTDB2Group | eTDB2GroupName=DB2Group,<br>eTDB2GroupContainerName=Groups,<br>eTDB2DirectoryName=*directory_name,*<br>eTNamespaceName=DB2 *Server,domain_name_suffix* |

## MS SQL Server Objects

The following table lists the MS SQL Server objects and their DNs in hierarchical order:

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTSQLDirectory | eTSQLDirectoryName=*directory_name,*<br>eTNamespaceName=MS SQL Server, *domain_name_suffix*<br>datalocation= BOTH (*)<br>edittype=string<br>minlen=1<br>maxlen=100<br>description=Directory Name |
| eTSQLLoginContainer | eTSQLLoginContainerName = MS SQL Logins,<br>eTSQLDirectoryName=*directory_name,*<br>eTNamespaceName=MS SQL Server, *domain_name_suffix*<br>datalocation= BOTH (*)<br>edittype=string<br>maxlen=255<br>description= MS SQL Server Login Container Name |
| eTSQLLogin | eTSQLLoginName=*MS SQL Login Name*<br>eTSQLLoginContainerName=MS SQL Logins,<br>eTSQLDirectoryName=*directory_name,*<br>eTNamespaceName=MS SQL Server, *domain_name_suffix*<br>datalocation= BOTH (*)<br>edittype=string<br>maxlen=128<br>description= MS SQL Server Login Name |
| eTSQLDatabase | eTSQLDatabaseName =*database_name,*<br>eTSQLDirectoryName=*directory_name,*<br>eTNamespaceName=MS SQL Server, *domain_name_suffix*<br>datalocation= BOTH (*)<br>edittype=string<br>maxlen=123<br>description= MS SQL Server Database Name |

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTSQLUser | eTSQLUserName = *MS_SQL_User_Name,*<br>eTSQLDatabaseName=*database_name,*<br>eTSQLDirectoryName=*directory_name,*<br>eTNamespaceName=MS SQL Server, *domain_name_suffix*<br>datalocation= BOTH (*)<br>edittype=string<br>maxlen=128<br>description= MS SQL Server User Name |
| eTSQLRole | eTSQLRoleName = *MS SQL_Role_Name,*<br>eTSQLDatabaseName=*database_name,*<br>eTSQLDirectoryName=*directory_name,*<br>eTNamespaceName=MS SQL Server, *domain_name_suffix*<br>datalocation= BOTH (*)<br>edittype=string<br>maxlen=128<br>description= MS SQL Server Role Name |

(*) datalocation= BOTH means that the object is stored in the Namespace server and in the Provisioning Directory.

## Oracle Objects

The following table lists the Oracle objects and their DNs in hierarchical order:

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTNamespace | eTNamespaceName=Oracle Server, *domain_name_suffix* |
| eTORADirectory | eTORADirectoryName=*directory_name,* eTNamespaceName=Oracle Server, *domain_name_suffix* |
| eTORAAccountContainer | eTORAAccountContainerName=Accounts, eTORADirectoryName=*directory_name,* eTNamespaceName=Oracle Server, *domain_name_suffix* |
| eTORAAccount | eTORAAccountName=*account_name*, eTORAAccountContainerName=Oracle Accounts, eTORADirectoryName=*directory_name,* eTNamespaceName=Oracle Server, *domain_name_suffix* |

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTORARoleContainer | eTORARoleContainerName=Roles, eTORADirectoryName=*directory_name,* eTNamespaceName=Oracle Server, *domain_name_suffix* |
| eTORARole | eTORARole=*role_name*, eTORARoleContainerName=Roles, eTORADirectoryName=*directory_name,* eTNamespaceName=Oracle Server, *domain_name_suffix* |
| eTORAProfileContainer | eTORAProfileContainerName=Profiles, eTORADirectoryName=*directory_name,* eTNamespaceName=Oracle Server, *domain_name_suffix* |
| eTORAProfile | eTORAProfile=*profile_name*, eTORAProfileContainerName=Profiles, eTORADirectoryName=*directory_name,* eTNamespaceName=Oracle Server, *domain_name_suffix* |
| eTORAProcContainer | eTORAProcContainerName=Procedures, eTORADirectoryName=*directory_name,* eTNamespaceName=Oracle Server, *domain_name_suffix* |
| eTORAProc | eTORAProc=*procedure_name*, eTORAProcContainerName=Procedures, eTORADirectoryName=*directory_name,* eTNamespaceName=Oracle Server, *domain_name_suffix* |
| eTORAPkgContainer | eTORAPkgContainerName=Packages, eTORADirectoryName=*directory_name,* eTNamespaceName=Oracle Server, *domain_name_suffix* |
| eTORAPkg | eTORAPkg=*package_name*, eTORAPkgContainerName=Packages, eTORADirectoryName=*directory_name,* eTNamespaceName=Oracle Server, *domain_name_suffix* |

## Oracle Applications Objects

The following table lists the Oracle Applications objects and their DNs in hierarchical order:

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTNamespace | eTNamespaceName=Oracle Applications, *domain_name_suffix* |
| eTFNDDirectory | eTFNDDirectoryName=*directory_name,* eTNamespaceName=Oracle Applications, *domain_name_suffix* |
| eTFNDAccountContainer | eTFNDAccountContainerName=Users, eTFNDDirectoryName=*directory_name,* eTNamespaceName=Oracle Applications, *domain_name_suffix* |
| eTFNDAccount | eTFNDUserName=*user_name*, eTFNDAccountContainerName=Users, eTFNDDirectoryName=*directory_name,* eTNamespaceName=Oracle Applications, *domain_name_suffix* |

## Windows NT Objects

The following table lists the Windows NT objects and their DNs in hierarchical order:

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTNamespace | eTNamespaceName=Windows NT,*domain_name_suffix* |
| eTN16Directory | eTN16DirectoryName=*directory_name,* eTNamespaceName=Windows *NT,domain_name_suffix* |
| eTN16AccountContainer | eTN16AccountContainerName=Accounts, eTN16DirectoryName=*directory_name,* eTNamespaceName=Windows *NT,domain_name_suffix* |
| eTN16Account | eTN16AccountName=Windows NT Account, eTN16AccountContainerName=Accounts, eTN16DirectoryName=*directory_name,* eTNamespaceName=Windows *NT,domain_name_suffix* |
| eTN16GroupContainer | eTN16GroupContainerName=N16GroupContainer, eTN16DirectoryName=*directory_name,* eTNamespaceName=Windows *NT,domain_name_suffix* |

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTN16Groups | eTN16GroupName=N16Group, eTN16GroupContainerName=N16GroupContainer, eTN16DirectoryName=*directory_name,* eTNamespaceName=Windows *NT,domain_name_suffix* |
| eTN16SharedFolder Container | eTN16SharedFolderContainerName=Shared Folders, eTN16DirectoryName=*directory_name,* eTNamespaceName=Windows *NT,domain_name_suffix* |
| eTN16SharedFolder | eTN16SharedFolderName=N16SharedFolder, eTN16SharedFolderContainerName=Shared Folders, eTN16DirectoryName=*directory_name,* eTNamespaceName=Windows *NT,domain_name_suffix* |
| eTn16FolderManager | eTN16FolderManagerName=SF_MNGT_name, eTN16DirectoryName=*directory_name*, eTNamespaceName=Windows *NT,domain_name_suffix* |
| eTN16GroupManager | eTN16GroupManagerName=GRP_MNGT_Name, eTN16DirectoryName=*directory_name*, eTNamespaceName=Windows *NT,domain_name_suffix* |

## CA-ACF2 Objects

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTNamespace | eTNamespaceName=CA-ACF2,*domain_name_suffix* |
| eTACFDirectory | eTACFDirectoryName=*directory_name,* eTNamespaceName=CA-ACF2,*domain_name_suffix* |
| eTACFLidContainer | eTACFLidContainerName=Accounts, eTACFDirectoryName=*directory_name,* eTNamespaceName=CA-ACF2,*domain_name_suffix* |
| eTACFLid | eTACFLidName=*your_lid*,eTACFLidContainerName=Accounts, eTACFDirectoryName=*directory_name,* eTNamespaceName=CA-ACF2,*domain_name_suffix* |
| eTACFRuleContainer | eTACFRuleContainerName=Rules, eTACFDirectoryName=*directory_name,* eTNamespaceName=CA-ACF2, *domain_name_suffix* |
| eTACFACF2RuleType | ETACFACF2RuleTypeName=*ACF2_rule_types*, eTACFRuleContainerName=Rules, eTACFDirectoryName=*directory_name,* eTNamespaceName=CA-ACF2,*domain_name_suffix* |

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTACFACF2RuleKey | eTACFACF2RuleKeyName=*$_key_value*,<br>eTACFACF2RuleTypeName=*ACF2_rule_types*,<br>eTACFRuleContainerName=Rules,<br>eTACFDirectoryName=*directory_name,*<br>eTNamespaceName=CA-ACF2,*domain_name_suffix* |
| eTACFACF2RuleLine | eTACFACF2RuleLineName=*highlevel_qualifier_mask,*<br>eTACFACF2AssetTypeName=*assets_under_$_key*,<br>eTACFACF2RuleKeyName=*$_key_value*,<br>eTACFRuleTypeName=*ACF2_rule_types*,<br>eTACFRuleContainerName=Rules,<br>eTACFDirectoryName=*directory_name,*<br>eTNamespaceName=CA-ACF2,*domain_name_suffix* |

## CA-Top Secret Objects

The following table lists the CA-Top Secret objects and their DNs in hierarchical order:

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTNamespace | eTNamespaceName=CA-Top Secret,*domain_name_suffix* |
| eTTSSDirectory | eTTSSDirectoryName=*directory_name,*<br>eTNamespaceName=CA-Top Secret,*domain_name_suffix* |
| eTTSSAcid | eTTSSAcidName=*acid_name,*<br>eTTSSAcidContainerName=Accounts,<br>eTTSSDirectoryName=*directory_name,*<br>eTNamespaceName=CA-Top Secret,*domain_name_suffix* |
| eTTSSFacilityContainer | eTTSSFacilityContainerName =Facilities,<br>eTTSSAcidName=*acid_name,*<br>eTTSSAcidContainerName=Accounts,<br>eTTSSDirectoryName=*directory_name,*<br>eTNamespaceName=CA-Top Secret,*domain_name_suffix* |
| eTTSSPermissionContainer | eTTSSPermissionContainerName =Permissions,<br>*eTTSSAcidName=acid_name,*<br>eTTSSAcidContainerName=Accounts,<br>eTTSSDirectoryName=*directory_name,*<br>eTNamespaceName=CA-Top Secret,*domain_name_suffix* |
| eTTSSOwnershipContainer | eTTSSOwnershipContainerName =Ownerships,<br>*eTTSSAcidName=acid_name,*<br>eTTSSAcidContainerName=Accounts,<br>eTTSSDirectoryName=*directory_name,*<br>eTNamespaceName=CA-Top Secret,*domain_name_suffix* |

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTTSSProfListContainer | eTTSSProfListContainerName =ProfList, eTTSSAcidName=*acid_name,* eTTSSAcidContainerName=Accounts, eTTSSDirectoryName=*directory_name,* eTNamespaceName=CA-Top Secret,*domain_name_suffix* |
| eTTSSAdminFacContainer | eTTSSAdminFacContainerName = AdminFacility, *eTTSSAcidName=acid_name,* eTTSSAcidContainerName=Accounts, eTTSSDirectoryName=*directory_name,* eTNamespaceName=CA-Top Secret,*domain_name_suffix* |
| eTTSSAdminResContainer | eTTSSAdminResContainerName = AdminResource, *eTTSSAcidName=acid_name,* eTTSSAcidContainerName=Accounts, eTTSSDirectoryName=*directory_name,* eTNamespaceName=CA-Top Secret,*domain_name_suffix* |
| eTTSSAdminScpContainer | eTTSSAdminScpContainerName = AdminScope, *eTTSSAcidName=acid_name,* eTTSSAcidContainerName=Accounts, eTTSSDirectoryName=*directory_name,* eTNamespaceName=CA-Top Secret,*domain_name_suffix* |
| eTTSSAdminFacility | eTTSSAdminFacilityName =*admin_facility_name*, eTTSSAdminFacContainerName = AdminFacility, *eTTSSAcidName=acid_name,* eTTSSAcidContainerName=Accounts, eTTSSDirectoryName=*directory_name,* eTNamespaceName=CA-Top Secret,*domain_name_suffix* |
| eTTSSAdminResource | eTTSSAdminResourceName = *admin_resource_name*, eTTSSAdminResContainerName = AdminResource, *eTTSSAcidName=acid_name,* eTTSSAcidContainerName=Accounts, eTTSSDirectoryName=*directory_name,* eTNamespaceName=CA-Top Secret,*domain_name_suffix* |
| eTTSSAdminScope | eTTSSAdminScopeName = *admin_scope_name*, eTTSSAdminScpContainerName = AdminScope, *eTTSSAcidName=acid_name,* eTTSSAcidContainerName=Accounts, eTTSSDirectoryName=*directory_name,* eTNamespaceName=CA-Top Secret,*domain_name_suffix* |
| eTTSSAcidContainer | eTTSSAcidContainerName=Accounts, eTTSSendpointName=*directory_name,* eTNamespaceName=CA-Top Secret,*domain_name_suffix* |

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTTSSDeptContainer | eTTSSDeptContainerName= Departments,<br>eTTSSDirectoryName=*directory_name,*<br>eTNamespaceName=CA-Top Secret,*domain_name_suffix* |
| eTTSSDept | eTTSSDeptName =*dept_name,*<br>eTTSSDeptContainerName= Departments,<br>eTTSSDirectoryName=*directory_name,*<br>eTNamespaceName=CA-Top Secret,*domain_name_suffix* |
| eTTSSDivContainer | eTTSSDivContainerName= Divisions,<br>eTTSSDirectoryName=*endpoint_name,*<br>eTNamespaceName=CA-Top Secret,*domain_name_suffix* |
| eTTSSDiv | eTTSSDivName=*div_name,*<br>eTTSSDivContainerName= Divisions,<br>eTTSSDirectoryName=*directory_name,*<br>eTNamespaceName=CA-Top Secret,*domain_name_suffix* |
| eTTSSZoneContainer | eTTSSZoneContainerName= Zones,<br>eTTSSDirectoryName=*directory_name,*<br>eTNamespaceName=CA-Top Secret,*domain_name_suffix* |
| eTTSSAcidZone | eTTSSZoneName=*zone_name,*<br>eTTSSZoneContainerName= Zones,<br>eTTSSDirectoryName=*directory_name,*<br>eTNamespaceName=CA-Top Secret,*domain_name_suffix* |
| eTTSSGroupContainer | eTTSSGroupContainerName= Groups,<br>eTTSSDirectoryName=*directory_name,*<br>eTNamespaceName=CA-Top Secret,*domain_name_suffix* |
| eTTSSGroup | eTTSSGroupName =*group_name,*<br>eTTSSGroupContainerName= Groups,<br>eTTSSDirectoryName=*directory_name,*<br>eTNamespaceName=CA-Top Secret,*domain_name_suffix* |
| eTTSSFacility | eTTSSFacilityName=*facility_name*,<br>eTTSSFacilityContainerName=Facilities,<br>eTTSSAcidName=*acid_name,*<br>eTTSSAcidContainerName=Accounts,<br>eTTSSDirectoryName=*directory_name,*<br>eTNamespaceName=CA-Top Secret,*domain_name_suffix* |
| eTTSSOwnedName | eTTSSOwnedNameName=*detail_name,*<br>eTTSSOwnershipName=*owned_name*,<br>eTTSSOwnershipContainerName=Ownerships,<br>eTTSSAcidName=*acid_name,*<br>eTTSSAcidContainerName=Accounts,<br>eTTSSDirectoryName=*directory_name,*<br>eTNamespaceName=CA-Top Secret,*domain_name_suffix* |

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTTSSOwned | eTTSSOwnershipName=*owned_name*, eTTSSOwnershipContainerName=Ownerships, eTTSSAcidName=*acid_name,* eTTSSAcidContainerName=Accounts, eTTSSDirectoryName=*directory_name,* eTNamespaceName=CA-Top Secret,*domain_name_suffix* |
| eTTSSResName | eTTSSResNameName=*permission_detail_name,* eTTSSResClassName=*permission_name*, eTTSSPermissionContainerName=Permissions, eTTSSAcidName=*acid_name,* eTTSSAcidContainerName=Accounts, eTTSSDirectoryName=*directory_name,* eTNamespaceName=CA-Top Secret,*domain_name_suffix* |
| eTTSSResClass | eTTSSResClassName=*permission_name*, eTTSSPermissionContainerName=Permissions, eTTSSAcidName=*acid_name,* eTTSSAcidContainerName=Accounts, eTTSSDirectoryName=*directory_name,* eTNamespaceName=CA-Top Secret,*domain_name_suffix* |
| eTTSSProfList | eTTSSProfListName=*profile_name,* eTTSSProfListContainerName =ProfList*,* eTTSSAcidName=*acid_name,* eTTSSAcidContainerName=Accounts, eTTSSDirectoryName=*directory_name,* eTNamespaceName=CA-Top Secret,*domain_name_suffix* |
| eTTSSProfile | eTTSSProfileName=*profile_name,* eTTSSProfileContainerName=Profiles, eTTSSDirectoryName=*directory_name,* eTNamespaceName=CA-Top Secret,*domain_name_suffix* |
| eTTSSProfileContainer | eTTSSProfileContainerName=Profiles, eTTSSDirectoryName=*directory_name,* eTNamespaceName=CA-Top Secret,*domain_name_suffix* |

## RACF Objects

The following table lists the RACF objects and their DNs in hierarchical order:

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTNamespace | eTNamespaceName=RAC Namespace,*domain_name_suffix* |

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTRACDirectory | eTRACDirectoryName=*directory_name,* eTNamespaceName=RAC Namespace,*domain_name_suffix* |
| eTRACAccount | eTRACAccount=*user_id,*eTRACAccountContainerName=Accounts, eTRACDirectoryName=*directory_name,* eTNamespaceName=RAC Namespace,*domain_name_suffix* |
| eTRACAccountContainer | eTRACAccountContainerName=Accounts, eTRACDirectoryName=*directory_name,* eTNamespaceName=RAC Namespace,*domain_name_suffix* |
| eTRACUserResProfile | eTRACPermissionEntry=*entry_name,* eTRACPermissionClass=*class_name*, eTRACUserPermissionContainerName=Permissions, eTRACDirectoryName=*directory_name,* eTNamespaceName=RAC Namespace,*domain_name_suffix* |
| eTRACUserPermissionResClass | eTRACPermissionClass=*class_name*, eTRACUserPermissionContainerName=Permissions, eTRACDirectoryName=*directory_name,* eTNamespaceName=RAC Namespace,*domain_name_suffix* |
| eTRACUserPermissionContainer | eTRACUserPermissionContainerName=Permissions, eTRACDirectoryName=*directory_name,* eTNamespaceName=RAC Namespace,*domain_name_suffix* |
| eTRACGroupUser | eTRACGroupUserid=*user_id,* eTRACgroupid=*group_id*, eTRACGroupContainer=Groups, eTRACDirectoryName=*directory_name,* eTNamespaceName=RAC Namespace,*domain_name_suffix* |
| eTRACGroup | eTRACgroupid=*group_id*, eTRACGroupContainer=Groups, eTRACDirectoryName=*directory_name,* eTNamespaceName=RAC Namespace,*domain_name_suffix* |
| eTRACGroupContainer | eTRACGroupContainer=Groups, eTRACDirectoryName=*directory_name,* eTNamespaceName=RAC Namespace,*domain_name_suffix* |

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTRACResUser | eTRACPermissionUser=*user_id,*<br>eTRACPermissionEntry=RACF Permission Entry,<br>eTRACPermissionClass=*class_name*,<br>eTRACPermissionContainerName=Permissions,<br>eTRACDirectoryName=*directory_name,*<br>eTNamespaceName=RAC Namespace,*domain_name_suffix* |
| eTRACResProfile | eTRACPermissionEntry=RACF Permission Entry,<br>eTRACPermissionClass=*class_name*,<br>eTRACPermissionContainerName=Permissions, |
| eTRACPermissionResClass | eTRACPermissionClass=*class_name*,<br>eTRACPermissionContainerName=Permissions,<br>eTRACDirectoryName=*directory_name,*<br>eTNamespaceName=RAC Namespace,*domain_name_suffix* |
| eTRACPermissionContainer | eTRACPermissionContainerName=Permissions,<br>eTRACDirectoryName=*directory_name,*<br>eTNamespaceName=RAC Namespace,*domain_name_suffix* |

## OS/400 Objects

The following table lists the OS/400 objects and their DNs in hierarchical order:

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTNamespace | eTNamespaceName=OS400 Namespace,*domain_name_suffix* |
| eTAS4Directory | eTAS4DirectoryName=*directory_name,*<br>eTNamespaceName=OS400 Namespace,*domain_name_suffix* |
| eTAS4AccountContainer | eTAS4AccountContainerName=Accounts,<br>eTAS4DirectoryName=*directory_name,*<br>eTNamespaceName=OS400 Namespace,*domain_name_suffix* |
| eTAS4Account | eTAS4UserProfileName=*OS/400_account*,<br>eTAS4AccountContainerName=Accounts,<br>eTAS4DirectoryName=*directory_name,*<br>eTNamespaceName=OS400 Namespace,*domain_name_suffix* |
| eTAS4GroupContainer | eTAS4GroupContainerName=Groups,<br>eTAS4DirectoryName=*directory_name,*<br>eTNamespaceName=OS400 Namespace,*domain_name_suffix* |

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTAS4Group | eTAS4GroupName=*OS/400_group*, eTAS4GroupContainerName=Groups, eTAS4DirectoryName=*directory_name,* eTNamespaceName=OS400 Namespace,*domain_name_suffix* |

## UNIX ETC Objects

The following table lists the UNIX ETC objects and their DNs in hierarchical order:

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTNamespace | eTNamespaceName=UNIX - *etc,domain_name_suffix* |
| eTETCDirectory | eTETCDirectoryName=*directory_name,* eTNamespaceName=UNIX - *etc,domain_name_suffix* |
| eTETCAccountContainer | eTETCAccountContainerName=*container_name*, eTETCDirectoryName=*directory_name,* eTNamespaceName=UNIX - *etc,domain_name_suffix* |
| eTETCAccount | eTETCAccountName=*account_name*, eTETCAccountContainerName=*container_name*, eTETCDirectoryName=*directory_name,* eTNamespaceName=UNIX - *etc,domain_name_suffix* |
| eTETCGroupContainer | eTETCGroupContainerName=*group_container_name*, eTETCDirectoryName=*directory_name,* eTNamespaceName=UNIX - *etc,domain_name_suffix* |
| eTETCGroup | eTETCGroupName=*group_name*, eTETCGroupContainerName=*group_container_name*, eTETCDirectoryName=*directory_name,* eTNamespaceName=UNIX - *etc,domain_name_suffix* |

## UNIX NIS Objects

The following table lists the UNIX NIS objects and their DNs in hierarchical order:

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTNamespace | eTNamespaceName=UNIX - NIS-NIS plus *Domains,domain_name_suffix* |
| eTNISDirectory | eTNISDirectoryName=*directory_name,* eTNamespaceName=UNIX - NIS-NIS plus *Domains,domain_name_suffix* |

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTNISAccountContainer | eTNISAccountContainerName=*container_name*, eTNISDirectoryName=*directory_name,* eTNamespaceName=UNIX - NIS-NIS plus *Domains,domain_name_suffix* |
| eTNISAccount | eTNISAccountName=*account_name*, eTNISAccountContainerName=*container_name*, eTNISDirectoryName=*directory_name,* eTNamespaceName=UNIX - NIS-NIS plus *Domains,domain_name_suffix* |
| eTNISGroupContainer | eTNISGroupContainerName=*group_container_name*, eTNISDirectoryName=*directory_name,* eTNamespaceName=UNIX - NIS-NIS plus *Domains,domain_name_suffix* |
| eTNISGroup | eTNISGroupName=*group_name*, eTNISGroupContainerName=*group_container_name*, eTNISDirectoryName=*directory_name,* eTNamespaceName=UNIX - NIS-NIS plus *Domainsdomain_name_suffix* |
| eTNISNetGroupContainer | eTNISNetGroupContainerName=*netgroup_container_name* eTNISDirectoryName=*directory_name,* eTNamespaceName=UNIX - NIS-NIS plus Domains,*domain_name_suffix* |
| eTNISNetGroup | eTNISNetGroupName=*netgroup_name,* eTNISNetGroupContainerName=*netgroup_container_name,* eTNISDirectoryName=*directory_name,* eTNamespaceName=UNIX - NIS-NIS plus Domains,*domain_name_suffix* |

## Active Directory Services Objects

The following table lists the Active Directory Services objects and their DNs in hierarchical order:

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTNamespace | eTNamespaceName=ActiveDirectory,*domain_name_suffix* |
| eTADSDirectory | eTADSDirectoryName=*directory_name,* eTNamespaceName=ActiveDirectory,*domain_name_suffix* |
| eTADSContainer | eTADSContainerName=Active Dir. Folder, eTADSDirectoryName=*directory_name,* eTNamespaceName=ActiveDirectory,*domain_name_suffix* |

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTADSAccount | eTADSAccountName=*account_name,* eTADSContainerName=Active Dir. Folder, eTADSDirectoryName=*directory_name,* eTNamespaceName=ActiveDirectory,*domain_name_suffix* |
| eTADSOrgUnit | eTADSOrgUnitName=Active Dir. Org. Unit, eTADSDirectoryName=*directory_name,* eTNamespaceName=ActiveDirectory,*domain_name_suffix* |
| eTADSGroup | eTADSGroupName=Active Dir. Group, eTADSOrgUnitName=Active Dir. Org. Unit, eTADSDirectoryName=directory_*name,* eTNamespaceName=ActiveDirectory,*domain_name_suffix* |

## Lotus Notes\Domino Objects

The following table lists the Lotus Notes\Domino objects and their DNs in hierarchical order:

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTNamespace | eTNamespaceName=Lotus Domino *Server,domain_name_suffix* |
| eTLNDDirectory | eTLNDDirectoryName=*directory_name,* eTNamespaceName=Lotus Domino *Server,domain_name_suffix* |
| eTLNDCountry | eTLNDCountryName=Lotus Domino Country, eTLNDDirectoryName=*directory_name,* eTNamespaceName=Lotus Domino *Server,domain_name_suffix* |
| eTLNDFlatCertifier | eTLNDFlatCertifier=Lotus Domino Flat Certifier, eTLNDDirectoryName=*directory_name,* eTNamespaceName=Lotus Domino *Server,domain_name_suffix* |
| eTLNDAccount | eTLNDAccountName=*account_name*, eTLNDOrganizationalUnit=Lotus Domino Organizational Unit, eTLNDOrganization=Lotus Domino Organization, eTLNDDirectoryName=*directory_name,* eTNamespaceName=Lotus Domino *Server,domain_name_suffix* |

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTLNDOrganizationalUnit | eTLNDOrganizationalUnit=Lotus Domino Organizational Unit,<br>eTLNDOrganization=Lotus Domino Organization,<br>eTLNDDirectoryName=*directory_name,*<br>eTNamespaceName=Lotus Domino *Server,domain_name_suffix* |
| eTLNDOrganization | eTLNDOrganization=Lotus Domino Organization,<br>eTLNDDirectoryName=*directory_name,*<br>eTNamespaceName=Lotus Domino *Server,domain_name_suffix* |
| eTLNDGroupContainer | eTLNDGroupContainerName=LND Groups,<br>eTLNDDirectoryName=*directory_name,*<br>eTNamespaceName=Lotus Domino *Server,domain_name_suffix* |
| eTLNDGroup | eTLNDGroupName=*group_name*,<br>eTLNDGroupContainerName=LND Groups,<br>eTLNDDirectoryName=*directory_name,*<br>eTNamespaceName=Lotus Domino *Server,domain_name_suffix* |

## CA Access Control Objects

The following table lists the CA Access Control objects and their DNs in hierarchical order:

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTNamespace | eTNamespaceName=Access Control,domain_name_suffix |
| eTACCDirectory | eTACCDirectoryName=*directory_name,*<br>eTNamespaceName=Access *Control,domain_name_suffix* |
| eTACCAccountContainer | eTACCAccountContainerName=Accounts,<br>eTACCDirectoryName=*directory_name,*<br>eTNamespaceName=Access *Control,domain_name_suffix* |
| eTACCAccount | eTACCAccountName=*account_name*,<br>eTACCAccountContainerName=Accounts,<br>eTACCDirectoryName=*directory_name,*<br>eTNamespaceName=Access *Control,domain_name_suffix* |
| eTACCGroupContainer | eTACCGroupContainerName=Groups,<br>eTACCDirectoryName=*directory_name,*<br>eTNamespaceName=Access *Control,domain_name_suffix* |

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTACCGroup | eTACCGroupName=*group_name*, eTACCGroupContainerName=Groups, eTACCDirectoryName=*directory_name,* eTNamespaceName=Access *Control,domain_name_suffix* |

## PLS Objects

The following table lists the PLS objects and their DNs in hierarchical order:

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTNamespace Type | eTNamespaceName=CA SSO WAC, *domain_name_suffix* |
| eTPLSDirectory | eTPLSDirectoryName=directory_name, eTNamespaceName=CA SSO WAC, domain_name_suffix |
| eTPLSUserStore | eTPLSUserStoreName=user store name, eTPLSDirectoryName=directory_name, eTNamespaceName=CA SSO WAC, domain_name_suffix |
| eTPLSAccount | eTPLSAccountName=account_name, [eTPLSContainerName=container_name, ...](zero or more containers) eTPLSUserStoreName=user store name, eTPLSDirectoryName=directory_name, eTNamespaceName=CA SSO WAC, domain_name_suffix |
| eTPLSGroup | eTPLSGroupName=group_name, [eTPLSContainerName=container_name, ...](zero or more containers) eTPLSUserStoreName=user store name, eTPLSDirectoryName=directory_name, eTNamespaceName=CA SSO WAC, domain_name_suffix |
| eTPLSContainer | [eTPLSContainerName=container_name, ...](zero or more containers) eTPLSUserStoreName=user store name, eTPLSDirectoryName=directory_name, eTNamespaceName=CA SSO WAC, domain_name_suffix |

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTPLSApplicationContainer | eTPLSApplicationContainerName=Applications, eTPLSDirectoryName=directory_name, eTNamespaceName=CA SSO WAC, domain_name_suffix |
| eTPLSApplication | eTPLSApplicationName=Application_name, eTPLSApplicationContainerName=Applications, eTPLSDirectoryName=directory_name, eTNamespaceName=CA SSO WAC, domain_name_suffix |
| eTPLSApplicationGroupContainer | eTPLSApplicationGroupContainerName=Application Groups, eTPLSDirectoryName=directory_name, eTNamespaceName=CA SSO WAC, domain_name_suffix |
| eTPLSApplicationGroup | eTPLSApplicationGroupName=application_group_name, eTPLSApplicationGroupContainerName=Application Groups, eTPLSDirectoryName=directory_name, eTNamespaceName=CA SSO WAC, domain_name_suffix |
| eTPLSTerminalContainer | eTPLSTerminalContainerName=Terminals eTPLSDirectoryName=directory_name, eTNamespaceName=CA SSO WAC, domain_name_suffix |
| eTPLSTerminal | eTPLSTerminalName=Terminal_name eTPLSTerminalContainerName=Terminals, eTPLSDirectoryName=directory_name, eTNamespaceName=CA SSO WAC, domain_name_suffix |
| eTPLSAuthhostContainer | eTPLSAuthhostContainerName=Authentication Hosts, eTPLSDirectoryName=directory_name, eTNamespaceName=CA SSO WAC, domain_name_suffix |
| eTPLSAuthhost | eTPLSAuthhostName=Authhost_name, eTPLSAuthhostContainerName=Authentication Hosts, eTPLSDirectoryName=directory_name, eTNamespaceName=CA SSO WAC, domain_name_suffix |

## KRB Objects

The following table lists the KRB objects and their DNs in hierarchical order:

| **LDAP Object Name** | **DN of Object Instance** |
|---|---|
| eTNamespace | eTNamespace=KRB Namespace,*domain_name_suffix* |
| eTKRBDirectory | eTKRBDirectoryName=*directory_name,* eTNamespace=*KRB Namespace,domain_name_suffix* |
| eTKRBAccountContainer | eTKRBAccountContainerName=Accounts, eTKRBDirectoryName=*directory_name*, eTNamespace=KRB Namespace,*domain_name_suffix* |
| eTKRBAccount | eTKRBAccountName=*account_name*, eTKRBAccountContainerName=Accounts, eTKRBDirectoryName=*directory_name,* eTNamespace=*KRB Namespace,domain_name_suffix* |
| eTKRBAccount | eTKRBAccountName=KRBUser, eTKRBAccountContainerName=KRB Accounts, eTKRBDirectoryName=directory_name, eTNamespaceName= KRB Namespace,domain_name_suffix |
| eTKRBPasswordPolicyContainer | eTKRBPasswordPolicyContainerName=KRB Password Policies, eTKRBDirectoryName=directory_name, eTNamespaceName=KRB Namespace,domain_name_suffix |
| eTKRBPasswordPolicy | eTKRBPasswordPolicyName=KRBPolicy,eTKRBPasswordPolicyContainerName=KRB Password Policies, eTKRBDirectoryName=directory_name, eTNamespaceName=KRB Namespace,domain_name_suffix |

## SAP Objects

The following table lists the SAP objects and their DNs in hierarchical order:

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTNamespace | eTNamespace=SAP *Namespace,domain_name_suffix* |
| eTSAPDirectory | eTSAPDirectoryName=*directory_name,*<br>eTNamespace=SAP *Namespace,domain_name_suffix* |
| eTSAPAccountContainer | eTSAPAccountContainerName=Accounts,<br>eTSAPDirectoryName=*directory_name*,<br>eTNamespace=SAP *Namespace,domain_name_suffix* |
| eTSAPAccount | eTSAPAccountName=*account_name*,<br>eTSAPAccountContainerName=Accounts,<br>eTSAPDirectoryName=*directory_name,*<br>eTNamespace=SAP *Namespace,domain_name_suffix* |
| eTSAPProfileContainer | eTSAPProfileContainer=Profiles,<br>eTSAPDirectoryName=*directory_name,*<br>eTNamespace=SAP Namespace,*domain_name_suffix* |
| eTSAPProfile | eTSAPProfile=*profile_name*,<br>eTSAPProfileContainer=Profiles,<br>eTSAPDirectoryName=*directory_name,*<br>eTNamespace=SAP *Namespace,domain_name_suffix* |
| eTSAPRoleContainer | eTSAPRoleContainer=SAP Roles<br>eTSAPDirectoryName=*directory_name*<br>eTNamespace=SAP Namespace,*domain_name_suffix* |
| eTSAPRole | eTSAPRole=*role_name*<br>eTSAPRoleContainer=SAP Roles<br>eTSAPDirectoryName=*directory_name,*<br>eTNamespace=SAP *Namespace,domain_name_suffix* |

## Siebel Objects

The following table lists the Siebel objects and their DNs in hierarchical order:

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTNamespace | eTNamespaceName=Siebel,*domain_name_suffix* |
| eTSBLDirectory | eTSBLDirectoryName=Siebel_*directory_name,*<br>eTNamespaceName=Siebel,*domain_name_suffix* |
| eTSBLUserContainer | eTSBLUserContainerName=Users,<br>eTSBLDirectoryName=Siebel_*directory_name,*<br>eTNamespaceName=Siebel,*domain_name_suffix* |
| eTSBLUser | eTSBLUserID=Siebel_user_ID,<br>eTSBLUserContainerName=Users,<br>eTSBLDirectoryName=Siebel_*directory_name,*<br>eTNamespaceName=Siebel,*domain_name_suffix* |
| eTSBLPositionContainer | eTSBLPositionContainerName=Positions,<br>eTSBLDirectoryName=Siebel_*directory_name,*<br>eTNamespaceName=Siebel,*domain_name_suffix* |
| eTSBLPosition | eTSBLPositionName=Siebel_position_name,<br>eTSBLPositionContainerName=Positions,<br>eTSBLDirectoryName=Siebel_*directory_name,*<br>eTNamespaceName=Siebel,*domain_name_suffix* |
| eTSBLDivision Container | eTSBLDivisionContainerName=Divisions,<br>eTSBLDirectoryName=Siebel_directory_name,<br>eTNamespaceName=Siebel,domain_name_suffix |
| eTSBLDivision | eTSBLResponsibilitiyName=Siebel_division_name,<br>eTSBLDivisionContainerName=Divisions,<br>eTSBLDirectoryName=Siebeldirectory_name,<br>eTNamespaceName=Siebel,domain_name_suffix |

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTSBLView Container | eTSBLResponibilityContainerName=Views, eTSBLDirectoryName=Siebel_directory_name, eTNamespaceName=Siebel,domain_name_suffix |
| eTSBLView | eTSBLResponsibilitiyName=Siebel_View_name, eTSBLViewContainerName=Views, eTSBLDirectoryName=Siebeldirectory_name, eTNamespaceName=Siebel,domain_name_suffix |
| eTSBLResponsibility Container | eTSBLResponibilityContainerName=Responsibilities, eTSBLDirectoryName=Siebel_*directory_name,* eTNamespaceName=Siebel,*domain_name_suffix* |
| eTSBLResponsibility | eTSBLResponsibilitiyName=Siebel_responsibility_name, eTSBLResponsibilityContainerName=Responsibilities, eTSBLDirectoryName=Siebel*directory_name,* eTNamespaceName=Siebel,*domain_name_suffix* |
| eTSBLLOVContainer | eTSBLLOVContainerName=LOV, eTSBLDirectoryName=Siebel_directory_name, eTNamespaceName=Siebel,*domain_name_suffix* |
| eTSBLLOVValue | eTSBLLOVValueName=Siebel_ListOfValuest_name, eTSBLUserListContainerName=LOV,<br>eTSBLDirectoryName=Siebel_directory_name, eTNamespaceName=Siebel,*domain_name_suffix* |

## RSA Objects

The following table lists the RSA objects and their DNs in hierarchical order:

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTNamespace | eTNamespace=RSA Server*,domain_name_suffix* |
| eTRSADirectory | eTRSADirectoryName=*directory_name,* eTNamespace=*RSA Server,domain_name_suffix* |

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTRSAAccountContainer | eTRSAAccountContainerName=RSA Accounts, eTRSADirectoryName=*directory_name*, eTNamespace=RSA Server*,domain_name_suffix* |
| eTRSAAccount | eTRSAAccountName=*account_name*, eTRSAAccountContainerName=RSA Accounts, eTRSADirectoryName=*directory_name,* eTNamespace=*RSA Server,domain_name_suffix* |
| eTRSAGrpContainer | eTRSAGrpContainerName=RSA *Groups,* eTRSADirectoryName=*directory_name,* eTNamespaceName=*RSA Server,domain_name_suffix* |
| eTRSAGrp | eTRSAGrpName=Group_Name, eTRSAGrpContainerName=Groups, eTRSADirectoryName=*directory_name,* eTNamespace=RSA Server,*domain_name_suffix* |
| eTRSATokenContainer | eTRSATokenContainerName=RSA *Tokens*, eTRSADirectoryName=*directory_name,* eTNamespace=*RSA Server,domain_name_suffix* |
| eTRSAToken | eTRSATokenSerialNumber=token_serial_number,eTRSATokenContainerName=RSA Tokens, eTRSADirectoryName=*directory_name* eTNamespace=RSA Server,*domain_name_suffix* |
| eTRSAAgentHostContainer | eTRSAAGentHostContainerName=RSA Agent Hosts, eTRSADirectoryName=*directory_name,* eTNamespace=RSA Server,*domain_name_suffix* |
| eTRSAAgentHost | eTRSAAgentHostName=*AgentHost_name*, eTRSAAgentHostContainerName=RSA Agent Hosts, eTRSADirectoryName=*directory_name*, eTNamespaceName=RSA SERVER,*domain_name_suffix* |
| eTRSASiteContainer | eTRSASiteContainerName=RSA Sites, eTRSADirectoryName=*directory_name*, eTNamespaceName=RSA SERVER,*domain_name_suffix* |
| eTRSASite | eTRSASiteName=*Site_name*, eTRSASiteContainerName=RSA Sites, eTRSADirectoryName=*directory_name*, eTNamespaceName=RSA SERVER,*domain_name_suffix* |

## Common Objects Tree

The Connector account templates belong to the common objects tree. The following sections lists the connector account template objects and their DNs in hierarchical order:

### DBZ Server Common Object Tree

DBZ Server account templates belong to the common objects tree. The following table lists the DBZ Server account template objects and their DNs in hierarchical order:

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTDBZPolicyContainer | eTDBZPolicyContainerName=DB2 ZOS Account Templates, eTNamespaceName=DB2 ZOS Server, domain_name_suffix |
| eTDBZPolicy | eTDBZPolicyName=DB2 ZOS Account Template, eTDBZPolicyContainerName=DB2 ZOS Account Templates, eTNamespaceName=DB2 ZOS Server, domain_name_suffix |

### DB2 UDB Common Objects Tree

DB2 UDB account templates belong to the common objects tree. The following table lists the DB2 UDB account template objects and their DNs in hierarchical order:

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTDB2Policy | eTDB2PolicyName=policy_name, eTDB2PolicyContainerName=DB2 Policies, eTNamespaceName=CommonObjects, domain_name_suffix |
| eTDB2PolicyContainer | eTDB2PolicyContainerName=DB2 Policies, eTNamespaceName=CommonObjects, domain_name_suffix |

## MS SQL Server Common Object Tree

MS SQL Server account templates belong to the common objects tree. The following table lists the MS SQL Server account template objects and their DNs in hierarchical order:

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTSQLPolicyContainer | eTSQLPolicyContainerName= MS SQL Policies, eTNamespaceName=CommonObjects, *domain_name_suffix*<br>datalocation=DB (*)<br>edittype=string<br>maxlen=255<br>description= MS SQL Server Policy Container Name |
| eTSQLPolicy | eTSQLPolicyName= *MS SQL Policy name,* eTSQLPolicyContainerName=MS SQL Policies, eTNamespaceName=CommonObjects, *domain_name_suffix*<br>datalocation=DB (*)<br>edittype=string<br>maxlen=50<br>description= MS SQL Server Policy Name |

(*) datalocation =DB means that the object is stored in the Provisioning Directory.

## Oracle Common Objects Tree

Oracle account templates belong to the common objects tree. The following table lists the Oracle account template objects and their DNs in hierarchical order:

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTORAPolicy | eTORAPolicyName=*policy_name*, eTORAPolicyContainerName=Oracle Policies, eTNamespaceName=CommonObjects,*domain_name_suffix* |
| eTORAPolicyContainer | eTORAPolicyContainerName=Oracle Policies, eTNamespaceName=CommonObjects,*domain_name_suffix* |

## Oracle Applications Common Objects Tree

Oracle Applications account templates belong to the common objects tree. The following table lists the Oracle Applications account template objects and their DNs in hierarchical order:

| LDAP Object Name | DN of Object Instance |
|---|---|
| ETFNDPolicy | eTFNDPolicyName=*policy_name*, eTVMSPolicyContainerName=Oracle Applications Policies, eTNamespaceName=CommonObjects,*domain_name_suffix* |
| eTFNDPolicyContainer | eTFNDPolicyContainerName=Oracle Applications Policies, eTNamespaceName=CommonObjects,*domain_name_suffix* |

## Windows NT Common Objects Tree

Windows NT account templates belong to the common objects tree. The following table lists the Windows NT account template objects and their DNs in hierarchical order:

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTN16Policy | eTN16PolicyName=*policy_name*, eTN16PolicyContainerName=Windows NT Policies, eTNamespaceName=CommonObjects,*domain_name_suffix* |
| eTN16PolicyContainer | eTN16PolicyContainerName=Windows NT Policies, eTNamespaceName=CommonObjects,*domain_name_suffix* |

## ACF2 Common Objects Tree

CA-ACF2 account templates belong to the common objects tree. The following table lists the CA-ACF2 account template objects and their DNs in hierarchical order:

| LDAP Object Name | DN of Object Instance |
|---|---|
| ETACFPolicy | eTACFPolicyName=*policy_name*, eTACFPolicyContainerName=CA-ACF2 Policies, eTNamespaceName=CommonObjects,*domain_name_suffix* |
| eTACFPolicyContainer | eTACFPolicyContainerName=CA-ACF2 Policies, eTNamespaceName=CommonObjects,*domain_name_suffix* |

## Top Secret Common Objects Tree

CA-Top Secret account templates belong to the common objects tree. The following table lists the CA-Top Secret account template objects and their DNs in hierarchical order:

| LDAP Object Name | DN of Object Instance |
|---|---|
| ETTSSPolicy | eTTSSPolicyName=*policy_name*, eTTSSPolicyContainerName=CA-Top Secret Policies, eTNamespaceName=CommonObjects,*domain_name_suffix* |
| eTTSSPolicyContainer | eTTSSPolicyContainerName=CA-Top Secret Policies, eTNamespaceName=CommonObjects,*domain_name_suffix* |

## RACF Common Objects Tree

RACF account templates belong to the common objects tree. The following table lists the RACF account template objects and their DNs in hierarchical order:

| LDAP Object Name | DN of Object Instance |
|---|---|
| ETRACPolicy | eTRACPolicyName=*policy_name*, eTRACPolicyContainerName=RACF Policies, eTNamespaceName=CommonObjects,*domain_name_suffix* |
| eTRACPolicyContainer | eTRACPolicyContainerName=RACF Policies, eTNamespaceName=CommonObjects,*domain_name_suffix* |

## OS/400 Common Objects Tree

OS/400 account templates belong to the common objects tree. The following table lists the OS/400 account template objects and their DNs in hierarchical order:

| LDAP Object Name | DN of Object Instance |
|---|---|
| ETAS4Policy | eTAS4PolicyName=*policy_name*, eTAS4PolicyContainerName=OS/400 Policies, eTNamespaceName=CommonObjects,*domain_name_suffix* |
| eTAS4PolicyContainer | eTAS4PolicyContainerName=OS/400 Policies, eTNamespaceName=CommonObjects,*domain_name_suffix* |

## UNIX ETC Common Objects Tree

UNIX ETC account templates belong to the common objects tree. The following table lists the UNIX ETC account template objects and their DNs in hierarchical order:

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTETCPolicy | eTETCPolicyName=*policy_name*,<br>eTETCPolicyContainerName=UNIX - etc Policies,<br>eTNamespaceName=CommonObjects,*domain_name_suffix* |
| eTETCPolicyContainer | eTETCPolicyContainerName=UNIX - etc Policies,<br>eTNamespaceName=CommonObjects,*domain_name_suffix* |

## UNIX NIS Common Objects Tree

UNIX NIS account templates belong to the common objects tree. The following table lists the UNIX account template objects and their DNs in hierarchical order:

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTNISPolicy | eTNISPolicyName=*policy_name*,<br>eTNISPolicyContainerName=UNIX - NIS-NIS plus Domains Policies,<br>eTNamespaceName=CommonObjects,*domain_name_suffix* |
| eTNISPolicyContainer | eTNISPolicyContainerName=UNIX - NIS-NIS plus Domains Policies,<br>eTNamespaceName=CommonObjects,*domain_name_suffix* |

## ADS Common Objects Tree

Active Directory Services account templates belong to the common objects tree. The following table lists the Active Directory Services account template objects and their DNs in hierarchical order:

| LDAP Object Name | DN of Object Instance |
|---|---|
| ETADSPolicy | eTADSPolicyName=*policy_name*,<br>eTADSPolicyContainerName=Active Directory Policies,<br>eTNamespaceName=CommonObjects,*domain_name_suffix* |
| ETADSPolicyContainer | eTADSPolicyContainerName=Active Directory Policies,<br>eTNamespaceName=CommonObjects,*domain_name_suffix* |

## LND Common Objects Tree

Lotus Notes/Domino account templates belong to the common objects tree. The following table lists the Lotus Notes/Domino account template objects and their DNs in hierarchical order:

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTLNDPolicy | eTLNDPolicyName=*policy_name*, eTLNDPolicyContainerName=LND Policies, eTNamespaceName=CommonObjects,*domain_name_suffix* |
| eTLNDPolicyContainer | eTLNDPolicyContainerName=LND Policies, eTNamespaceName=CommonObjects,*domain_name_suffix* |

## Access Control Common Objects Tree

CA Access Control account templates belong to the common objects tree. The following table lists the CA Access Control account template objects and their DNs in hierarchical order:

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTACCPolicy | eTACCPolicyName=*policy_name*, eTACCPolicyContainerName=Access Control Policies, eTNamespaceName=CommonObjects,*domain_name_suffix* |
| eTACCPolicyContainer | eTACCPolicyContainerName=Access Control Policies, eTNamespaceName=CommonObjects,*domain_name_suffix* |

## SSO for Advanced Policy Server Common Objects Tree

PLS account templates belong to the common objects tree. The following table lists the PLS account template objects and their DNs in hierarchical order:

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTPLSPolicy | eTPLSPolicyName=policy_name, eTPLSPolicyContainerName=CA SSO WAC Policies, eTNamespaceName=CommonObjects,domain_name_suffix |
| eTPLSPolicyContainer | eTPLSPolicyContainerName=CA SSO WAC Policies, eTNamespaceName=CommonObjects,domain_name_suffix |

## Kerberos Common Objects Tree

KRB account templates belong to the common objects tree. The following table lists the KRB account template objects and their DNs in hierarchical order:

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTKRBPolicy | eTKRBPolicyName=*policy_name*, eKRBPolicyContainerName=KRB polices eTNamespaceName=CommonObjects, *domain_name_suffix* |
| eTKRBPolicyContainer | eTKRBPolicyContainerName=KRB Policies, eTNamespaceName=CommonObjects, *domain_name_suffix* |

## SAP Common Objects Tree

SAP account templates belong to the common objects tree. The following table lists the SAP account template objects and their DNs in hierarchical order:

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTSAPPolicy | eTSAPPolicyName=*policy_name*, eTSAPPolicyContainerName=SAP Policies, eTNamespaceName=CommonObjects,*domain_name_suffix* |
| eTSAPPolicyContainer | eTSAPPolicyContainerName=SAP Policies, eTNamespaceName=CommonObjects,*domain_name_suffix* |

## Siebel Common Objects Tree

Siebel account templates belong to the common objects tree. The following table lists the Siebel account template objects and their DNs in hierarchical order:

| LDAP Object Name | DN of Object Instance |
|---|---|
| eTSBLPolicy | eTSBLPolicyName=*policy_name*, eTSBLPolicyContainerName=Siebel Policies, eTNamespaceName=CommonObjects,*domain_name_suffix* |
| eTSBLPolicyContainer | eTSBLPolicyContainerName=Siebel Policies, eTNamespaceName=CommonObjects,*domain_name_suffix* |

### RSA Common Objects Tree

RSA account templates belong to the common objects tree. The following table lists the RSA account template objects and their DNs in hierarchical order:

| LDAP Object Name | DN of Object Instance |
|---|---|
| ETRSAPolicy | eTRSAPolicyName=*policy_name*,<br>eTRSAPolicyContainerName=RSA Policies,<br>eTNamespaceName=CommonObjects,*domain_name_suffix* |
| eTRSAPolicyContainer | eTRSAPolicyContainerName=RSA Policies,<br>eTNamespaceName=CommonObjects,*domain_name_suffix* |

## Object User-Friendly Names

The following sections list the LDAP object names for the connectors and their user-friendly names:

### DBZ Object User Friendly Names

The following table lists the DBZ object names and their user-friendly names:

| LDAP Object Name | User-Friendly Name | Description |
|---|---|---|
| eTDBZAccount | DB2 ZOS Account | DB2 ZOS User |
| eTDBZAccountContainer | DB2 ZOS Account Container | DB2 ZOS User container |
| eTDBZDirectory | DB2 ZOS Directory | Directory name |
| eTDBZPolicy | DB2 ZOS Policy | Policy |
| eTDBZPolicyContainer | DB2 ZOS PolicyContainer | Policy container |
| eTNamespace | Namespace | Namespace name |

### DB2 UDB Object User-Friendly Names

The following table lists the LDAP object names and their user-friendly names alphabetically:

| LDAP Object Name | User-Friendly Name | Description |
|---|---|---|
| eTDB2Account | DB2Account | DB2 UDB User |

| LDAP Object Name | User-Friendly Name | Description |
|---|---|---|
| eTDB2AccountContainer | DB2AccountContainer | DB2 UDB User container |
| eTDB2Directory | DB2Directory | Directory name |
| eTDB2Group | DB2Group | DB2 UDB Group |
| eTDB2GroupContainer | DB2GroupContainer | DB2 UDB Group container |
| eTDB2Policy | DB2Policy | Policy |
| eTDB2PolicyContainer | DB2PolicyContainer | Policy container |
| eTNamespace | Namespace | Policy |

## MS SQL Object User-Friendly Names

The following table lists the LDAP object names and their user-friendly names:

| LDAP Object Name | User-Friendly Name | Description |
|---|---|---|
| eTSQLDirectory | SQLDirectory | Directory |
| eTSQLLogin | SQLLogin | MS SQL Login |
| eTSQLLoginContainer | SQLLoginContainer | MS SQL Login Container |
| eTSQLUser | SQLUser | MS SQL User |
| eTSQLRole | SQLRole | MS SQL Role |
| eTSQLDatabase | SQLDatabase | MS SQL Database |
| eTSQLPolicy | SQLPolicy | MS SQL Policy |
| eTSQLPolicyContainer | SQLPolicyContainer | MS SQL Policy Container |

## Oracle Object User-Friendly Names

The following table lists the LDAP object names and their user-friendly names:

| LDAP Object Name | User-Friendly Name | Description |
|---|---|---|
| eTORAAccount | ORAAccount | Account |
| eTORAAccountContainer | ORAAccountContainer | Account container |
| eTORADirectory | ORADirectory | Directory name |
| eTORAPkgContainer | ORAPkgContainer | Package container |
| eTORAPkg | ORAPkg | Package |

| LDAP Object Name | User-Friendly Name | Description |
|---|---|---|
| eTORAProcContainer | ORAProcContainer | Procedure container |
| eTORAProc | ORAProc | Procedure |
| eTORAProfile | ORAProfile | Oracle profile |
| eTORAProfileContainer | ORAProfileContainer | Profile container |
| eTORARole | ORARole | Oracle role |
| eTORARoleContainer | ORARoleContainer | Role container |
| eTORAPolicy | ORAPolicy | Policy |
| eTORAPolicyContainer | ORAPolicyContainer | Policy container |
| eTNamespace | Namespace | Namespace name |

## Oracle Applications Object User-Friendly Names

The following table lists the LDAP object names and their user-friendly names:

| LDAP Object Name | User-Friendly Name | Description |
|---|---|---|
| eTFNDAccount | FNDAccount | Account |
| eTFNDAccountContainer | FNDAccountContainer | Account container |
| eTFNDDirectory | FNDDirectory | Directory name |
| eTFNDPolicy | FNDPolicy | Policy |
| eTFNDPolicyContainer | FNDPolicyContainer | Policy container |
| eTNamespace | Namespace | Namespace name |

## Windows NT Object User-Friendly Names

The following table lists the LDAP object names and their user-friendly names:

| LDAP Object Name | User-Friendly Name | Description |
|---|---|---|
| eTN16Account | N16Account | Account |
| eTN16AccountContainer | N16AccountContainer | Account container |
| eTN16Directory | N16Directory | Directory name |

| LDAP Object Name | User-Friendly Name | Description |
|---|---|---|
| eTN16FolderManager | N16FolderManager | Windows NT directory storage browser |
| eTN16Group | N16Group | Group |
| eTN16GroupContainer | N16GroupContainer | Group container |
| eTN16GroupManager | N16GroupManager | Retrieves user list included in a group |
| eTN16Policy | N16Policy | Policy |
| eTN16PolicyContainer | N16PolicyContainer | Policy container |
| eTN16SharedFolder | N16SharedFolder | Shared folder |
| eTN16SharedFolderContainer | N16SharedFolderContainer | Shared folder container |
| eTNamespace | Namespace | Namespace name |

## ACF2 Object User-Friendly Names

The following table lists the LDAP object names and their user-friendly names:

| LDAP Object Name | User-Friendly Name | Description |
|---|---|---|
| eTACFACF2RuleKey | ACFRuleKey | Rule key |
| eTACFACF2RuleLine | ACFRuleLine | Rule line |
| eTACFACF2RuleType | ACFRuleType | Rule type |
| ETACFDirectory | ACFDirectory | Directory name |
| ETACFLid | ACFAccount | Logon ID |
| ETACFLidContainer | ACFLidContainer | Accounts container |
| ETACFRuleContainer | ACFRuleContainer | Rules container |
| ETNamespace | Namespace | Namespace name |

## Top Secret Object User-Friendly Names

The following table lists the LDAP object names and their user-friendly names:

| LDAP Object Name | User-Friendly Name | Description |
|---|---|---|
| eTNamespace | Namespace | Namespace name |
| eTTSSAcid | TSSAcid | Acid |
| eTTSSAcidContainer | TSSAcidContainer | Acid container |
| eTTSSFacilityContainer | TSSFacilityContainer | Facility Container |
| eTTSSPermissionContainer | TSSPermissionContainer | Permission Container |
| eTTSSOwnershipContainer | TSSOwnershipContainer | Ownership Container |
| eTTSSProfListContainer | TSSProfListContainer | Profile List Container |
| eTTSSAdminFacContainer | TSSAdminFacContainer | Admin Facility Container |
| eTTSSAdminResContainer | TSSAdminResContainer | Admin Resource Container |
| eTTSSAdminScpContainer | TSSAdminScpContainer | Admin Scope Container |
| eTTSSAdminFacility | TSSAdminFacility | Admin Facility |
| eTTSSAdminResource | TSSAdminResource | Admin Resource |
| eTTSSAdminScope | TSSAdminScope | Admin Scope |
| eTTSSDeptContainer | DeptContainer | Department Container |
| eTTSSDept | TSSDept | Department |
| eTTSSDivContainer | DivContainer | Division Container |
| eTTSSDiv | TSSDiv | Division |
| eTTSSZoneContainer | ZoneContainer | Zone Container |
| eTTSSAcidZone | TSSZone | Zone |
| eTTSSGroupContainer | GroupContainer | Group Container |
| eTTSSGroup | TSSGroup | Group |
| eTTSSFacility | TSSFacility | Facility |
| eTTSSDirectory | TSSDirectory | Directory |
| eTTSSOwned | TSSOwned | Owned object |
| eTTSSPolicy | TSSPolicy | Policy |
| eTTSSPolicyContainer | TSSPolicyContainer | Policy container |

| LDAP Object Name | User-Friendly Name | Description |
|---|---|---|
| eTTSSProfile | TSSProfile | Profile |
| eTTSSProfList | TSSProfList | Profile List |
| eTTSSProfileContainer | TSSProfileContainer | Profile container |
| eTTSSResClass | TSSResClass | Resource class |
| eTTSSResName | TSSResName | Resource name |

## RACF Object User-Friendly Names

The following table lists the LDAP object names and their user-friendly names:

| LDAP Object Name | User-Friendly Name | Description |
|---|---|---|
| eTNamespace | Namespace | Namespace name |
| eTRACAccount | RACAccount | Account |
| eTRACAccountContainer | RACAccountContainer | Account container |
| eTRACDirectory | RACDirectory | Directory |
| eTRACGroup | RACGroup | Group |
| eTRACGroupContainer | eTRACGroupContainer | Group container |
| eTRACGroupUser | RACGroupUser | Groupuser |
| eTRACPermissionContainer | RACPermissionContainer | Permission container |
| eTRACPermissionResClass | RACPermissionResClass | Permission resource class |
| eTRACResProfile | RACResProfile | Resource profile |
| eTRACResUser | RACResUser | Resource user |
| eTRACUserPermissionContainer | RACUserPermissionContainer | User permission container |
| eTRACUserPermissionResClass | RACUserPermissionResClass | User permission resource class |
| eTRACUserResProfile | RACUserResProfile | User Resource profile |
| eTRACPolicy | RACPolicy | Policy |
| eTRACPolicyContainer | RACPolicyContainer | Policy container |

## OS/400 Object User-Friendly Names

The following table lists the LDAP object names and their user-friendly names:

| LDAP Object Name | User-Friendly Name | Description |
|---|---|---|
| eTAS4Account | AS4Account | Account |
| eTAS4AccountContainer | AS4AccountContainer | Account container |
| eTAS4Directory | AS4Directory | Directory name |
| eTAS4Group | AS4Group | Group |
| eTAS4GroupContainer | AS4GroupContainer | Group container |
| eTAS4Policy | AS4Policy | Policy |
| eTAS4PolicyContainer | AS4PolicyContainer | Policy container |
| eTNamespace | Namespace | Namespace name |

## UNIX ETC Object User-Friendly Names

The following table lists the LDAP object names and their user-friendly names:

| LDAP Object Name | User-Friendly Name | Description |
|---|---|---|
| eTETCAccount | ETCAccount | Account |
| eTETCAccountContainer | ETCAccountContainer | Account container |
| eTETCGroup | ETCGroup | Group |
| eTETCGroupContainer | ETCGroupContainer | Group container |
| eTETCPolicy | ETCPolicy | Policy |
| eTETCPolicyContainer | ETCPolicyContainer | Policy container |
| eTNamespace | Namespace | Namespace name |

## UNIX NIS Object User-Friendly Names

The following table lists the LDAP object names and their user-friendly names alphabetically:

| LDAP Object Name | User-Friendly Name | Description |
|---|---|---|
| eTNISAccount | NISAccount | Account |
| eTNISAccountContainer | NISAccountContainer | Account container |

| LDAP Object Name | User-Friendly Name | Description |
|---|---|---|
| eTNISGroup | NISGroup | Group |
| eTNISGroupContainer | NISGroupContainer | Group container |
| eTNISNetGroup | NISNetGroup | NetGroup |
| eTNISNetGroupContainer | NISNetGroupContainer | NetGroup Container |
| eTNISPolicy | NISPolicy | Policy |
| eTNISPolicyContainer | NISPolicyContainer | Policy container |
| eTNamespace | Namespace | Namespace name |

## ADS Object User-Friendly Names

The following table lists the LDAP object names and their user-friendly names:

| LDAP Object Name | User-Friendly Name | Description |
|---|---|---|
| ETADSAccount | ADSAccount | Account |
| ETADSContainer | ADSContainer | Account container |
| ETADSDirectory | ADSDirectory | Directory name |
| ETADSGroup | ADSGroup | Group |
| ETADSOrgUnit | ADSOrgUnit | Organizational unit, a container for groups |
| ETADSPolicy | ADSPolicy | Policy |
| ETADSPolicyContainer | ADSPolicyContainer | Policy container |
| ETNamespace | Namespace | Namespace name |

## Lotus Notes/Domino Object User-Friendly Names

The following table lists the LDAP object names and their user-friendly names:

| LDAP Object Name | User-Friendly Name | Description |
|---|---|---|
| eTLNDAccount | LNDAccount | Account |
| eTLNDCountry | LNDCountry | Country name |
| eTLNDDirectory | LNDDirectory | Directory name |
| eTLNDFlatCertifier | LNDFlatCertifier | Flat certifier |

| LDAP Object Name | User-Friendly Name | Description |
|---|---|---|
| eTLNDGroup | LNDGroup | Group |
| eTLNDGroupContainer | LNDGroupContainer | Group container |
| eTLNDOrganizationalUnit | LNDOrganizationalUnit | Organizational unit name |
| eTLNDOrganization | LNDOrganization | Organization |
| eTLNDPolicy | LNDPolicy | Policy |
| eTLNDPolicyContainer | LNDPolicyContainer | Policy container |
| eTNamespace | Namespace | Namespace name |

## Access Control Object User-Friendly Names

The following table lists the LDAP object names and their user-friendly names:

| LDAP Object Name | User-Friendly Name | Description |
|---|---|---|
| eTACCAccount | ACCAccount | Account |
| eTACCAccountContainer | ACCAccountContainer | Account  container |
| eTACCDirectory | ACCDirectory | Directory name |
| eTACCGroup | ACCGroup | Group |
| eTACCGroupContainer | ACCGroupContainer | Group container |
| eTACCPolicy | ACCPolicy | Policy |
| eTACCPolicyContainer | ACCPolicyContainer | Policy container |
| eTNamespace | Namespace | Namespace name |

## PLS Object User-Friendly Names

The following table lists the LDAP object names and their user-friendly names:

| LDAP Object Name | User-Friendly Name | Description |
|---|---|---|
| eTPLSAccount | PLSAccount | Account |
| eTPLSContainer | PLSContainer | Container |
| eTPLSUserStore | PLSUserStore | User store name |
| eTPLSDirectory | PLSDirectory | Directory name |

| LDAP Object Name | User-Friendly Name | Description |
|---|---|---|
| eTPLSGroup | PLSGroup | Group |
| eTPLSPolicy | PLSPolicy | Policy |
| eTPLSPolicyContainer | PLSPolicyContainer | Policy container |
| eTPLSApplicationContainer | PLSApplicationContainer | Application container |
| eTPLSApplication | PLSApplication | Application |
| eTPLSApplicationGroupContainer | PLSApplicationGroupContainer | Application group container |
| eTPLSApplicationGroup | PLSApplicatonGroup | Application group |
| eTPLSTerminalContainer | PLSTerminalContainer | Terminal Container |
| eTPLSTerminal | PLSTerminal | Terminal |
| eTPLSAuthhostContainer | PLSAuthhostContainer | Authhost Container |
| eTPLSAuthhost | PLSAuthhost | Authhost |
| eTNamespace | Namespace | Namespace name |

**Note:** Information about the CA Single Sign-On for Advanced Policy Server policy and policy container can be found in the common objects schema. For details, see the *Programming Guide for Provisioning*.

## KRB Object User-Friendly Names

The following table lists the LDAP object names and their user-friendly names:

| LDAP Object Name | User-Friendly Name | Description |
|---|---|---|
| eTKRBAccount | KRBAccount | KRB User |
| eTKRBAccountContainer | KRBAccountContainer | KRB User container |
| eTKRBPasswordPolicyContainer | KRBPasswordPolicyContainer | KRB Password Policy Container |
| eTKRBPasswordPolicy | KRBPasswordPolicy | KRB Password Policy |
| eTKRBDirectory | KRBDirectory | Directory Name |
| eTKRBPolicy | KRBPolicy | Policy |
| eTKRBPolicyContainer | KRBPolicyContainer | Policy Container |
| eNamespace | Namespace | Namespace name |

## SAP Object User-Friendly Names

The following table lists the LDAP object names and their user-friendly names:

| LDAP Object Name | User-Friendly Name | Description |
|---|---|---|
| eTSAPAccountContainer | SAPAccountContainer | Account container |
| eTSAPAccount | SAPAccount | SAP account |
| eTSAPProfileContainer | SAPProfileContainer | SAP profile container |
| eTSAPProfile | SAPProfile | SAP profile |
| eTSAPRoleContainer | SAPRoleContainer | SAP role container |
| eTSAPRole | SAPRole | SAP role |
| eTSAPPolicyContainer | SAPPolicyContainer | SAP policy container |
| eTSAPPolicy | SAPPolicy | SAP policy |

## Siebel Object User-Friendly Names

The following table lists the LDAP object names and their user-friendly names:

| LDAP Object Name | User-Friendly Name | Description |
|---|---|---|
| eTNamespace | Namespace | Namespace name |
| eTSBLDirectory | SBLDirectory | Siebel directory |
| eTSBLUserContainer | SBLUserContainer | User account container |
| eTSBLUser | SBLUser | User account |
| eTSBLPositionContainer | SBLPositionContainer | Position container |
| eTSBLPosition | SBLPosition | Position |
| eTSBLDivisionContainer | SBLDivisionContainer | Division container |
| eTSBLDivision | SBLDivision | Division |
| eTSBLViewContainer | SBLViewContainer | View container |
| eTSBLView | SBLView | View |
| eTSBLResponsibilityContainer | SBLResponsibilityContainer | Responsibility container |
| eTSBLResponsibility | SBLResponsibility | Responsibility |

| LDAP Object Name | User-Friendly Name | Description |
|---|---|---|
| eTSBLLOVContainer | SBLLOVContainer | List of Values container |
| eTSBLPolicyContainer | SBLPolicyContainer | Policy |

## RSA Object User-Friendly Names

The following table lists the LDAP object names and their user-friendly names:

| LDAP Object Name | User-Friendly Name | Description |
|---|---|---|
| eTNamespace | Namespace | Namespace name |
| eTRSAAccount | RSAAccount | Account |
| eTRSAAccountContainer | RSAAccountContainer | Account container |
| eTRSAAgentHost | RSAAgentHost | Agent Host |
| eTRSAAgentHostContainer | RSAAgentHostContainer | Agent Host container |
| eTRSAGrp | RSAGrp | Group |
| eTRSAGrpContainer | RSAGrpContainer | Group container |
| eTRSAPolicy | RSAPolicy | Policy |
| eTRSAPolicyContainer | RSAPolicyContainer | Policy container |
| eTRSASite | RSASite | Site |
| eTRSASiteContainer | RSASiteContainer | Site container |
| eTRSAToken | RSAToken | Token |
| eTRSATokenContainer | RSATokenContainer | Token container |

# Appendix C: Bulk Load Client

This section contains the following topics:

Introduction (see page 647)
Install the Bulk Load Client (see page 647)
Before Using the Bulk Load Client (see page 649)
Bulk Load Client Localization (see page 650)
Authenticating to the CA IdentityMinder Server (see page 651)
Configuring the Bulk Load Client (see page 652)
Use Case for PeopleSoft (see page 654)
Bulk Load Client Error and Response Handling (see page 657)

## Introduction

The Bulk Load Client is a command line utility that you use to remotely access the CA IdentityMinder Bulk Loader task through TEWS. The command is used for any operation that the Bulk Loader task is capable of performing. For more details, see Bulk Loader in the *Administration Guide*.

## Install the Bulk Load Client

To install the Bulk Load Client utility, run the setup.exe program found in the im-pc package in the following location:

```
Clients\BulkLoader
```

During installation you may be prompted to enter the CA IdentityMinder URL and the credentials of a user with permissions to execute the Bulk Loader task.

## Command Line Options

The following options are used to run the Bulk Load Client:

**-b, --batchSize <number>**

Specifies the maximum number of user data records to be sent to the server in each request. This option is used to avoid overloading the server.We recommend you to use a batchSize of 100.

**-c, --configFile <file>**

Specifies a properties file that contains the configuration options for invoking the Bulk Loader task. The default is "imbulkloadclient.properties".

**-e, --endpointInfoFile**

Specifies a properties file that contains the key or value pairs for "user", "password", and "serverUrl". This option is used together with the (-s, --storeEndpointInfo) option.

**-f, --format (CSV | XML)**

Specifies the format of the input file (-i, --inputFile) that contains the data records to be sent to the server. The default is XML. When the input file format is XML, use the -t, --transformFile <file> option to specify the XSLT template for carrying out the transformation. If the input file format is CSV, the file is submitted to the Bulk Loader task directly without transformation.

**-h, --help**

Displays the command syntax.

**-i, --inputFile <file>**

Determines the user data records to be sent to the server. It can be in XML or CSV format.

**-o, --outputFile <file>**

Writes the result to this file when the input file is transformed.

**-p, --password <pass>**

Specifies the password used for server authentication.

**-s, --serverUrl <url>**

Specifies the URL of the TEWS interface.

**-S, --storeEndpointInfo**

Stores the specified server URL and the Admin user name and password in the configuration file (-c, --configFile). The password is obfuscated before it is stored. The information that is going to be stored can be provided through the endpointInfoFile option.

**-u, --user <username>**

Specifies the user name for CA IdentityMinder authentication.

**Note:** The user must be authorized to use the CA IdentityMinder Bulk Loader task.

**-v, --verbose**

Specifies the output as much of the message as available.

**-V, --version**

Displays the version information of the program.

**-T, --transformOnly**

Specifies to carry out the XSLT transformation of the input XML file into CSV format without submitting to the server. If a valid file name is also specified by -o, --outputFile <file>, the CSV result will be written to that file.

**-t, --transformFile <file>**

Specifies the file that contains the XSLT template for XSLT transformation of the input file, if the file format is in XML.

# Before Using the Bulk Load Client

To allow TEWS access to the CA IdentityMinder Environment being called by the Bulk Load Client, enable the following Environment Advanced Settings:

- Web Services
- WSDL Generation
- admin_id (enable impersonation)

These settings can be set through the CA IdentityMinder Management Console under Home > Environments > your_environment > Advanced Settings > Web Services.

The Environment needs to be restarted to pick up the changes.

The CA IdentityMinder Bulk Loader task itself must also be Web Service enabled. This can be set through the CA IdentityMinder by modifying the Bulk Loader task and enabling Web Services on the Profile tab.

# Bulk Load Client Localization

Bulk Load Client uses the default locale of the Java Virtual Machine when starting up, and the default locale corresponds to system locale of the host platform. All user messages are externalized to the Java ResourceBundles to allow localization. The default resource file (Java Properties file) that contains the English resource imbulkloadclient_msg.properties file is built into the imbulkloadclient.jar file and is used by default.

To use a resource file that contains a different language resource, create the resource file by translating the default resource file and putting the new resource file under

```
$INSTALLATION_DIR\conf\com\ca\iam\imbulkloadclient
```

The file name of the new resource file should have the language and country code appended. For example, for Canadian French, the file name should be

```
imbulkloadclient_msg_fr_CA.properties
```

where

**fr**

Specifies the lowercase two-letter ISO-639 language code

**CA**

Specifies the uppercase two-letter ISO-3166 country code

**Note:** A Java resource file is a Java properties file. The encoding of a properties file is ISO-8859-1, also known as Latin-1. All non-Latin-1 characters must be entered by using Unicode escape characters. For example, \uHHHH, where HHHH is a hexadecimal index of the character in the Unicode character set. You can use the JDK tool native2ascii.exe to convert files which contain other character encodings into files containing Latin-1 and/or Unicode-encoded characters (using Unicode escape characters).

## Allow Bulk Loader to Load Tasks with Localized Names

If CA IdentityMinder Server has been localized, the Bulk Load Client does not perform a load out-of-the-box. This is because the Bulk Loader task name is a localized bundle location map.

For example:

```
${bundle=resourceBundles.FDC-RoleDefinitions_Tokenized:key=propert
y.CreateIdentityPolicySet.Profile.name}
```

By default, the Bulk Loader task uses actions mapped to task names. When the task names have been translated into a different language, the Bulk Load client cannot find the mapped task names to perform the load.

To avoid this problem, you can map the Create, Modify, and Delete actions to the task tag. If the task name search fails, the Feeder searches for the task tag.

There is no need to map the task tag if the task names have not been localized.

**Follow these steps:**

1. In a text editor, open the Bulk Load Client imbulkloadclient.properties file. This file is present in the following location:

   ```
   Bulk Loader\conf\imbulkloadclient.properties
   ```

2. Find the **actionToTaskMapping** property.

   The default setting for this property is:

   ```
   actionToTaskMapping=create.CreateUser;modify.Modify
   User;delete.Delete User
   ```

3. Change the property to map to the new localized task tag.

4. Save the properties file.

   The changes effect immediately.

# Authenticating to the CA IdentityMinder Server

Bulk Load Client uses a user name and a password to authenticate to the CA IdentityMinder Server.

When the CA IdentityMinder Server is protected by CA SiteMinder™, CA SiteMinder™ basic authentication is supported by setting “isProtectedBySiteMinder = true” in \BulkLoader\conf\imbulkloadclient.properties.

## SSL Support

If you want to use SSL to protect the data submitted to CA IdentityMinder, configure the CA IdentityMinder Server to accept HTTPS requests, then setup the Bulk Load Client:

**Follow these steps:**

1. Import the CA IdentityMinder certificate file to the Bulk Load Client keystore from the host where the Bulk Load Client is installed. Use the Java keytool utility to create a keystore and import the server certificate as a trusted certificate.

   ```
   keytool -import -alias imserver -file <your_server_cert_file> -keystore
   %HOMEDRIVE%%HOMEPATH%\.imbulkloaderkeystore
   ```

2. Edit the imbulkloadclient.bat file or the imbulkloadclient.sh file to set TRUSTSTORE_PASSWORD to the value you entered in the previous step.

# Configuring the Bulk Load Client

The following properties of the Bulk Load Client can be configured in the imbulkloadclient.properties file:

- CA IdentityMinder parser class to be used for the Bulk Loader task. At the moment, only "com.ca.identitymanager.feeder.parser.CSVParser" is supported.
- The unique identifier attribute name (column name) in the CSV file.
- The action attribute name (column name) in the CSV file.
- The primary object for the Bulk Loader task that is always *USER.*
- The action to admin task mapping (in the form of "create.Create User;modify.Modify User;delete.Delete User;")
- Whether or not the web service is protected by SiteMinder.

You can also specify the commands in the command line in the properties file also. Add a key and value pair to the properties file with the key being the command line options long form name.

**Note:** The options provided on the command line take precedence over the values specified in the properties file.

## Properties File Example

The following is an example of the Properties file used to configure the Bulk Loader Task and the Bulk Load Client:

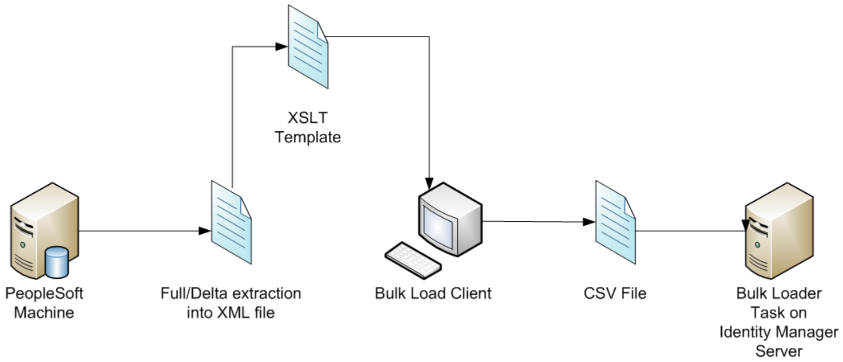
```
#
# These are the connection details of the CA IdentityMinder Server
#

# administrator id and password to be used to carry out the task
user=admin1
password=FPWg3MtYrUnididAMY06LZT/3LPuMtu6O7A+DRzX1JI\=

# server URL
serverUrl=http://imhostname:8080/iam/im/TEWS6/myime?wsdl

#
# these are the configuration items for the CA IdentityMinder ObjectsFeeder task
#

# CA IdentityMinder parser to be used for the ObjectsFeeder task
feederParserClass= com.ca.identitymanager.feeder.parser.CSVParser

# The unique identifier attribute name (column name in the CSV file)
uniqueIdentifierAttrName=uid

# The action attribute name (column name in the CSV file)
actionAttrName=action

# The primary object for the ObjectsFeeder task. (This will always be USER")
primaryObject=USER

# The action to admin task mapping
actionToTaskMapping = create.Create User;modify.Modify User;delete.Delete User

# Is the web service protected by SiteMinder
isProtectedBySiteMinder=false
```

# Use Case for PeopleSoft

The relevant user account information is first extracted manually from the authoritative data source: for example PeopleSoft. The Bulk Load Client can work with XML or CSV input file formats. If the information is XML, the file is transformed to CSV format by the Bulk Load Client using XSL transformation. The resultant CSV file is then sent by the Bulk Load Client to the CA IdentityMinder Bulk Loader task. Based on the mapped admin tasks, users are created, modified, or deleted.

The following is an example of the Bulk Load Client cycle:

*Equation 3: The information is extracted into an XML file, transformed with an XSLT template, converted with the Bulk Load Client to CSV, then imported into IM Server*



**From the PeopleSoft machine:**

1. Extract either a full or delta dump of user records in the form of an XML file.
2. Create an XSLT template to convert the XML file into the standard CSV form that can be used by the CA IdentityMinder Bulk Loader task.
3. Convert the XML file using XSLT template with the CA IdentityMinder Bulk Load Client.

   Bulk Load Client internally transforms the XML file into CSV format required by the CA IdentityMinder Bulk Loader task. You can either write the CSV file to a disk file or use the CSV file to invoke the Bulk Loader task.

   **Note:** The resultant CSV file can be loaded in smaller chunks.
4. Bulk Load Client uses the CSV file to invoke the Bulk Loader task using the TEWS interface.

   If the CSV file has been broken up into smaller chunks, Bulk Load Client invokes the Bulk Loader task for each of the chunks. Subsequent chunks are sent to the Bulk Loader task once the SOAP response from the previous request is received and the response indicates that the previous request is submitted successfully.
5. The SOAP response is logged to a file or written to the standard output.

The following use cases are supported for the Bulk Load Client:

- Full Dump
- Delta Dump
- Scheduling of the full or delta load

## Full Dump

A full dump is a complete dump of all users. The full dump data extraction must present the current state of each record at the time of the extraction.

With PeopleSoft HRMS, the full table synchronization message *PERSON_BASIC_FULLSYNC* is used to publish the full table. This message publishes all the user data records to a local XML file. The XML file can then be used to feed into Bulk Load Client. The *PERSON_BASIC_FULLSYNC* message is customized to suit your specific needs so that it maps all the records to a view only extracts currently affecting the data. A sample message file (peoplesoft2.xml) comes with the installation and is located under the "samples" directory. This file contains sample messages for *PERSON_BASIC_FULLSYNC*.

Refer to the *PeopleSoft Integration Broker PeopleBook* for detailed information on how to set up PeopleSoft Integration Broker and a full table data publish.

## Delta Dump

A delta dump is made of all user changes since the last time a delta or full dump was made. This dump presents the current state of each record modified since the previous delta or full dump identifies the record as deleted, if the user or the account no longer exists.

With PeopleSoft HRMS, there is a pre-defined message (PERSON_BASIC_SYNC) that publishes every change made to the user data records. Use the PeopleSoft Integration Broker to publish these changes to a local XML file. This XML file can then be loaded by Bulk Load Client. A sample message file (for example peoplesoft1.xml) comes with the installation and is located under the "samples" directory. This file contains a sample message for PERSON_BASIC_SYNC.

**Note:** PERSON_BASIC_SYNC publishes every change made to the user data record to its own file, so there could be many files to load.

A message definition is created that publishes all the changes made since the last full or delta dump into one single file. For additional assistance with how to create the custom message, refer to Oracle Support.

## Scheduling a Load

Scheduling the load is done using native OS capabilities and not as part of Bulk Load Client.

## Using the XSLT Template

If the data extracted from the PeopleSoft machine is in an XML file, an XSLT template file called peoplesoft.xslt has been supplied to carry out the transformation into the CSV format. For information on how the CSV file should be formatted, see "Feeder File Format" in the *CA IdentityMinder Administration Guide*.

This template file works with PeopleSoft Rowset-based message format and is customizable. For instructions on how to customize this file, check the comments in the template.

**Note:** The template file is located under the *samples* directory.

# Bulk Load Client Error and Response Handling

Bulk Load Client reports to the user on the status of the SOAP request that is sent to the Bulk Loader task. The report will be to a standard out and/or log file. Only network connection, SOAP or TEWS errors are reported. A successful response to the request does not necessarily mean that the CA IdentityMinder task has been processed without error. The task ID of each successfully submitted task will be output to allow cross-referencing with the User Console's View Submitted Tasks (VST) tab and CA IdentityMinder log files.

The Bulk Loader task can be monitored as any other task using VST. Each nested CA IdentityMinder task can be checked on this tab.

The XSLT transformation error is handled the same way as the errors mentioned above, for example, the error message is output to standard out and the log file. When an error is encountered, it will log the error and exit without submitting the task.

## Bulk Load Client Log Files

The following are the examples of logging destinations and a logging configuration file for the Bulk Load Client:

- Logging to standard out (console window) is set to java.util.logging.Level.INFO when the command line option –verbose is absent. The logging level is set to java.util.logging.Level.CONFIG when the option –verbose is set.
- Logging to standard out is always available no matter whether logging to a log file is configured or not.
- You can provide a logging configuration file to configure extra logging destination. The configuration file is set by starting the application with:

  ```
  java -Djava.util.logging.config.file=configFile MainClass
  ```

- A logging configuration file will be provided to log the message to the file imbulkloadclient.log in the logs subdirectory in the application installation folder.

The following is an example of the logging configuration file:

```
# log to a file
handlers= java.util.logging.FileHandler

# global logging level. The valid settings are SEVERE, WARNING, INFO,
# CONFIG, FINE, FINER and FINEST
.level= INFO

# file handler configuration
java.util.logging.FileHandler.pattern = ../logs/imbulkloadclient.log
java.util.logging.FileHandler.append = true
java.util.logging.FileHandler.limit = 50000
java.util.logging.FileHandler.count = 1
java.util.logging.FileHandler.formatter = java.util.logging.SimpleFormatter
```

## Axis Library Logging

The Axis library that we use as the stub classes to submit task to the CA IdentityMinder Server has its own logging. A log4J configuration file “log4j.properties” is provided in the /conf directory and writes to the log file “axis.log” in or logs directory.

# Appendix D: Sample Connector

This section contains the following topics:

Introduction (see page 659)
Terminology (see page 659)
Modes (see page 659)
Implementing the Connector (see page 662)
Account Management Screens (see page 663)
Further Enhancements (see page 663)

## Introduction

A sample scripting connector (sdkuposcript) is being included in this release to show functionality similar to the previous Universal Provisioning (UPO) Connector. Sdkuposcript is is the Sdkscript connector extended to implement UPO style exits. The following sections detail the steps to extend Sdkscript. As with Sdkscript, Sdkuposcript is implemented in JavaScript.

## Terminology

UPO exits provide the entry points within a user provisioning request where custom code can be referenced.

Program exits are the user-developed custom code referenced by UPO exits. This connector provides two sample exits: a SendMail exit and a Logging exit. The SendMail exit sends an email message containing details of the user provisioning request to an email address configurable at the connector level. The Logging exit stores the user provisioning request details to a file.

## Modes

Sdkuposcript operates in the following two modes:

- Non-managed mode
- Managed mode.

The mode is configured at the connector level on a per-endpoint basis.

## Non-managed Mode (Asynchronous mode)

In non-managed mode, program exits are used to alert the system administrator of a non-managed system regarding user provisioning requests. Two program exits are provided: a SendMail exit and a Logging exit. Both of these exits are enabled at the endpoint level for simplicity, for example, either all UPO exits invoke the SendMail exit or none at all. See Further Enhancements (see page 663) for enabling program exits at the UPO exit level.

This connector defines 10 UPO exits in non-managed mode:

**ADD_ACCOUNT**

Invoked when a new account is created.

**DELETE_ACCOUNT**

Invoked when an account is deleted.

**MODIFY_ACCOUNT**

Invoked when an account is modified, except for password, account status or request status changes. Password and status modifications invoke different UPO exits.

**RENAME_ACCOUNT**

Invoked when an account is renamed.

**CHANGE_ACCOUNT_PASSWORD**

Invoked when the password of an account is changed.

**ENABLE_ACCOUNT**

Invoked when the eTSuspended attribute of an account is set to enabled.

**DISABLE_ACCOUNT**

Invoked when the eTSuspended attribute of an account is set to disabled.

**INVOCATION_ERROR**

Invoked when a UPO exit fails or returns an error. This exit then throws an exception which results in a failed user provisioning request. Note that this is invoked when there is an error in the exit invocation, not due to an error on the endpoint.

**REQUEST_PENDING**

Invoked when a UPO exit was invoked successfully. A file is created containing the account name to indicate that a request for that account is pending. In this state, no other requests are acceptable and any such request should result in an exception.

**Note:** This implementation works well if there is only one CA IAM CS in the provisioning system. If there is more than one CA IAM CS, this implementation does work. Refer to SLA Exits for an alternative solution.

**REQUEST_COMPLETED**

Invoked when the request status is marked as completed. The request file, created on a previous REQUEST_PENDING, is deleted, indicating that further user provisioning requests for the account are now acceptable.

In non-managed mode, the UPO exits do not do anything other than invoke the SendMail or Logging exits if so configured.

**Note:** You are still required to explore the endpoint to create the necessary placeholders such as account and group containers. But exploring in this mode, or performing lookup on specific accounts, does not return or create new accounts.

## Managed Mode (Synchronous mode)

In managed mode, this connector also uses UPO exits, but the UPO exits perform the actual provisioning operations on the endpoint. The operations being performed are the same as what the sdkscript connector performs.

For simplicity, the managed mode UPO exits do not invoke any of the program exits, but there is no reason why this cannot be coded into the connector, if so required.

This connector provides seven UPO exits:

**ADD_ACCOUNT**

Invoked when a new account is created.

**DELETE_ACCOUNT**

Invoked when an account is deleted.

**MODIFY_ACCOUNT**

Invoked when an account is modified.

**RENAME_ACCOUNT**

Invoked when an account is renamed.

**READ_ACCOUNT**

Invoked when a SEARCH for a UPO account is requested.

**LIST_ACCOUNTS**

Invoked when a SEARCH for enumerating accounts is requested. A list of accounts is returned.

**INVOCATION_ERROR**

Invoked when a user provisioning operation has failed. An exception is thrown which results in a provisioning request error.

# Implementing the Connector

Perform the following steps to transform the sdkscript connector into the sdkuposcript connector:

In the sdkdyn metadata

1. Add the following connector level attribute definitions.

   a. managedEndpoint (eTDYN-bool-01) – Used to configure the operational mode of an endpoint.

   b. useSendMailExit (eTDYN-bool-02) – Used to indicate that the SendMail program exit is invoked by the UPO exits.

   c. useLogExit (eTDYN-bool-03) – Used to indicate that the Logging program exit is invoked by the UPO exits.

   d. mailserver (eTDYN-str-03) – Specifies the host name of the mail server that the SendMail exit connects to.

   e. mailrecipient (eTDYN-str-04) – Specifies the email address that the SendMail sends the mail to.

   f. mailsender (eTDYN-str-05) – Specifies the email address that the SendMail exit uses as the sender.

2. Add the following account level attribute definition in the sdkdyn metadata.

   a. requestStatus (eTDYN-int-01) – This indicates the status of the request. This attribute definition is used mainly to receive the completed status of the request.

3. Define the program exits.

   Two program exits are provided as samples. The SendMail exit gets the mail related connector level attributes and sends the message passed to it by the UPO exit. The mail subject is also passed to it by the invoking UPO exit. The code can be changed to include CC recipients if required.

   The Logging exit writes the details of the request to a file, in a sub-directory of that specified by eTDYNConnectionURL.

4. Define the UPO exits.

   One function is defined for each UPO exit. Where there are similarly named exits, a suffix is added indicating the operational mode where that exit is used, so there are functions such as ADD_ACCOUNT_NONMANAGED, ADD_ACCOUNT_MANAGED, ENABLE_ACCOUNT, and so forth.

   The non-managed mode exit functions package the request details in XML, which are made as similar as possible to the data block generated by the UPO connector. This xml block is then passed to the SendMail or Logging program exits, if so configured.

The managed mode exit functions perform the provisioning operations as in the sdkscript connector.

5. Re-structure the code of the functions specified in the opbindings.

   Whereas with sdkscript, the provisioning operations are performed right in the body of the opbindings functions, the sdkuposcript functions first check the operational mode of the endpoint, then invoke the appropriate UPO exit.

## Account Management Screens

Account screens can be generated for inclusion in the User Console help. The CA IdentityMinder r12.6.1 Web User Interface Account Screen Generation document should be consulted if account screens are desired.

Even though this connector uses the DYN namespace, this connector is thought of as a static endpoint type because metadata has already been provided. However, for future connectors that might want to use some of the additional attributes related to UPO implementation, Connector Xpress r12.5 r12.6.1 must be used to create new metadata having these additional attributes and properties.

Two more presentation metadata properties must be added to the additional attributes. These are description and inputHint. In addition, two logical groupings can be added: one group containing the useSendMailExit and useLoggingExit attributes, and the other group containing the mailserver, mailrecipient and mailsender attributes. The other additional attributes may be included in the group containing the other attributes for the object.

The additional attributes are simple types that can already be handled by the current JIAM and CA IdentityMinder server framework, so there is no need to create additional JIAM or CA IdentityMinder handlers. Once the metadata has been completed, you can then proceed with the Role Definition Generator to create the necessary files needed for deployment.

## Further Enhancements

This connector shows one way to implement UPO style exits on a scripting connector. It has been designed to show the salient points in transforming the sdkscript connector into one that uses exits. To avoid clutter that may hide these salient points, some of the UPO features have been left out. This section discusses how those features can be added.

## Configuring a Program Exit for Each UPO Exit

The program exits are enabled at the endpoint level. That is, either all UPO exits invoke the program exits, or none of them do. This connector can be enhanced to enable the program exits to be configured for each UPO exit.

You can implement these in one of the following ways:

- Add one boolean attribute for each program exit – UPO exit pair. There will be additional attributes such as useAddAccountSendMailExit, useAddAccountLoggingExit, useDeleteAccountSendMailExit, useDeleteAccountLoggingExit, and so forth. The code checks the appropriate boolean attribute for each provisioning request to determine whether or not to invoke the program exit.
- Add a multi-valued string attribute for each UPO exit, where such attribute contains the name of the program exit to invoke.

## Invoking Program Exits on Managed Mode UPO Exits

The code can be modified to enable invoking program exits from managed mode UPO exits. For this connector, the code was not modified because the managed mode exits are already performing the provisioning operations. If desired, this can be changed.

## Enabling / Disabling UPO Exits

Similar to invoking program exits as mentioned previously, more boolean attributes can be added to indicate whether or not a specific UPO exit is invoked at all, regardless of any other configuration the UPO exit has.

One use of this is to disable the RENAME_ACCOUNT exit if such functionality is not available at the endpoint.

## SLA Exits

UPO utilizes an SLA (Service Level Agreement) Monitor to poll for requests in the pending state. This connector can be enhanced to provide polling for the existence of request files, although there may be issues if this CA IAM CS is part of an environment containing more than one CA IAM CS, and the location of the request files is localized within each CA IAM CS. A recommended solution is to make use of third party products or systems to store requests data and provide the monitoring of those requests. In this case, the REQUEST_PENDING and REQUEST_COMPLETED exits make connections to those third party systems to update the requests data.