CA CloudMinder™

Identity Management Connectors Guide

1.5

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.

CA Technologies Product References

This document references the following CA Technologies products:

- CA CloudMinder™ Identity Management
- CA CloudMinder™ Advanced Authentication
- CA CloudMinder™ Single Sign-On
- CA Directory
- CA IdentityMinder™
- CA AuthMinder™
- CA RiskMinder™
- CA SiteMinder®
- CA SiteMinder® for Secure Proxy Server
- CA Layer 7

Contents

Chapter 1: Endpoints, Connectors, and the Connector Server

This guide describes how to use the following connector servers:

- CA IAM Connector server (CA IAM CS)
- C++ Connecter Server (CCS)

The following products can use these connector servers to connect to endpoints:

- Identity Management
- CA CloudMinder
- CA GovernanceMinder

In this guide, we refer to these products as *clients* of CA IAM CS.

For information about each connector, download the Endpoint Guide for that connector from the Connector Download page.

Audience

This guide is for administrators of CA IAM CS and CCS, who are responsible for the following tasks:

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

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

Path Notation	Default Directory	
	Windows	**UNIX**
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 Identity Management to synchronize information. A connector server uses a connector to manage an endpoint.

An endpoint is any system that communicates with Identity Management 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 Identity Management, 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 Identity Management manages.

For each endpoint type, Identity Management manages user accounts. Other managed objects that Identity Management 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 Identity Management will manage on the endpoint.

Connectors

A *connector* is the software that enables communication between Identity Management 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 Identity Management 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).

Two Types of Connectors

Identity Management has two 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.

Installing a Connector

Connectors that are available at the time of a release are installed with the CA IAM CS.

For more information on installing the CA IAM CS, see How To Set Up On-Premise Provisioning.

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 Identity Management. 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 Identity Management.

You can read the documentation, and then download the new connector from CA Support and use it with your current version of Identity Management. 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 Identity Management.

Connector Servers

Identity Management comes with the following connector servers:

- **CA IAM CS**—In previous releases, this component was called Java Connector Server, or Java CS. From Identity Management 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 Identity Management.

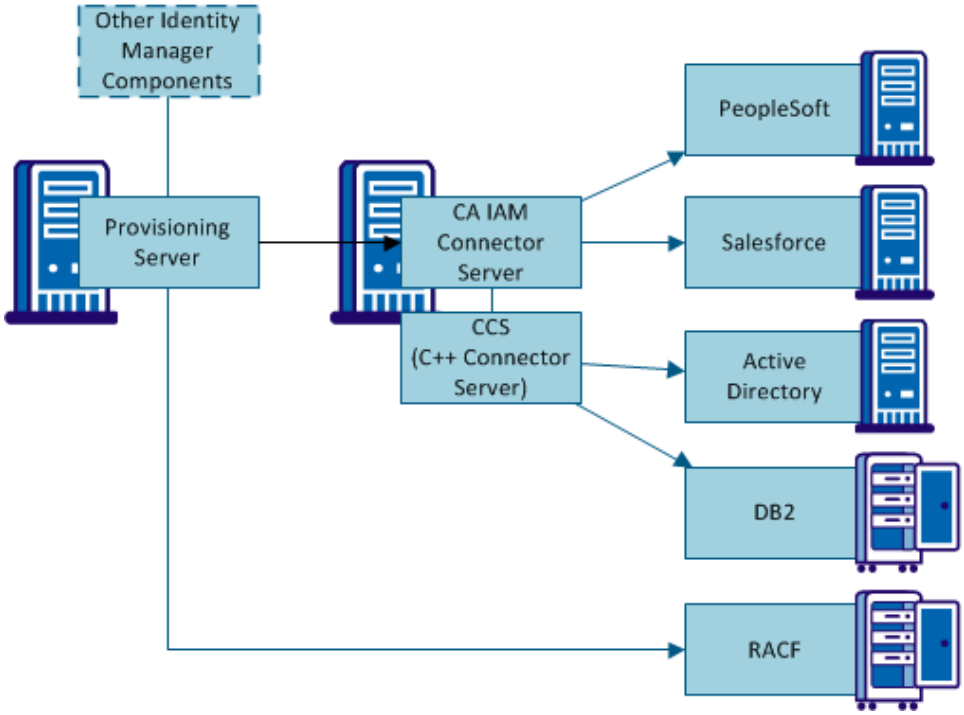
Example Installation: Three Types of Connectors

Identity Management supports three types of connector. 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, see the Connector Support Matrix.

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, see the Connector Support Matrix.

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

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 for CA IAM CS

You can see log files for the following components:

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

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 Logs 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. These messages are also displayed in the Logs tab.
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 is the toolkit with which CA IAM CS was created.
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

When you are trying to identify a fault, we recommend that you start with jcs_daily* files and work downwards to the connector-specific log files.

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 IAM CS. Before you send your logs to the support team, we recommend that you configure the logging to capture detailed information.

The jcs_daily.log and servicemix.log files that are listed in View a Log (see page 23) are configured in a text file. You can modify the file to change the following aspects of logging:

- 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

Follow these steps:

1. Identify how to trigger the problem with your deployment.
2. Replace the default logging configuration file with the verbose configuration:
   a. Find the following file:

      cs_home`/etc/org.ops4j.pax.logging.cfg`

   b. Rename this file to *org.ops4j.pax.logging.cfg.original*.

   c. Find *org.ops4j.pax.logging.cfg.verbose* and rename it to remove *.verbose*. This file will now provide the logging configuration.

   d. Restart CA IAM CS.
3. Trigger the problem that you have identified.
4. Zip the entire *cs_home/logs* directory, and include the zipped file with your support request.
5. To reduce the logging level, reverse step 2:
   a. Rename *org.ops4j.pax.logging.cfg* to *org.ops4j.pax.logging.cfg.verbose.*

   b. Rename *org.ops4j.pax.logging.cfg.original* to *org.ops4j.pax.logging.cfg*.

   c. Restart CA IAM CS.

Configure Logging for CA IAM CS

The jcs_daily.log and servicemix.log files that are listed in View a Log (see page 23) are configured in a text file. You can modify the file to change the following aspects of logging:

- 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

By default, the logging configuration is minimal, so that performance is not reduced.

If you find a problem with a connector or CA IAM CS, contact CA Support. 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. Replace the default logging configuration file with the verbose configuration:
   a. Find the following file:

      `cs_home/etc/org.ops4j.pax.logging.cfg`

   b. Rename this file to *org.ops4j.pax.logging.cfg.original*.

   c. Find *org.ops4j.pax.logging.cfg.verbose* and rename it to remove *.verbose*. This file will now provide the logging configuration.

   d. Restart CA IAM CS.
3. Trigger the problem that you have identified.
4. Zip the entire *cs_home/logs* directory, and include the zipped file with your support request.
5. To reduce the logging level, reverse step 2:
   a. Rename *org.ops4j.pax.logging.cfg* to *org.ops4j.pax.logging.cfg.verbose.*

   b. Rename *org.ops4j.pax.logging.cfg.original* to *org.ops4j.pax.logging.cfg*.

   c. Restart CA IAM CS.

Note: You can also edit *org.ops4j.pax.logging.cfg* in a text editor.

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.

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.

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=${DOMAIN},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

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 filter which messages are shown on the Logs tab, using the options under the Logs heading. These filters apply to the 500 most recent messages. They do not change the way that CA IAM CS records log messages.

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.

Interpreting Log Messages

All log messages include the following information:

Date and time

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

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

Bundle name, class name, and line number

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.ImplBundleServiceListener:123)
```

Severity level

The severity of the message:

- Error
- Warning
- Info
- Debug

Message

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 applications connect to one connector server. In this situation, the applications may not update their stored passwords for CA IAM CS at the same time, but they can still access the connector server.

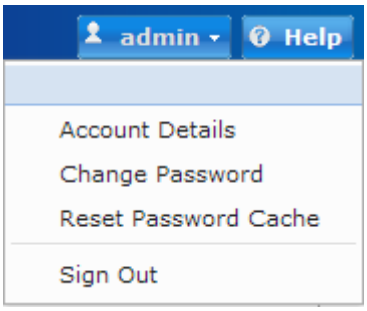
However, these old passwords make your system potentially insecure. To make the connector server forget the old passwords, clear the password cache. To clear a password cache, you must be logged in as that user.

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

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 ideal 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

Previous versions of this connector server were named Java CS or JCS. From Identity Management 12.6 onwards, the connector server is named CA IAM CS At the same time, we changed the way configuration is handled.

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\Identity 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\Identity 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 Identity Management.

This section contains the following topics:

Set Up Identity Management 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.

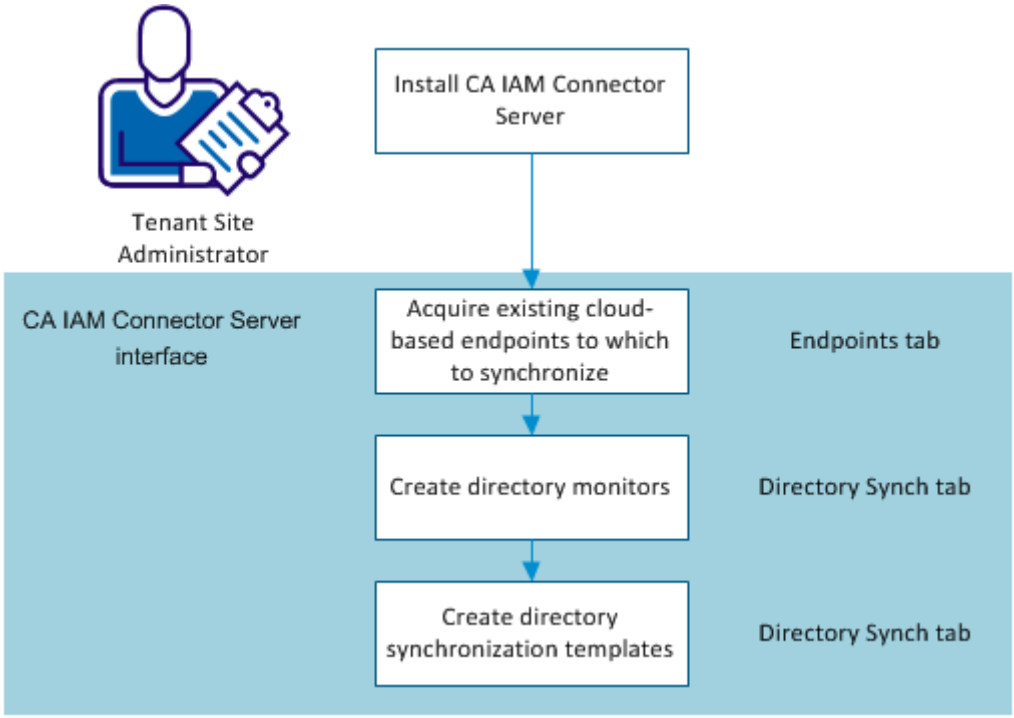
For example, assume that you have a SalesForce installation in the cloud. You could create an ADS group named "SalesForce" and then configure the CA IAM CS to monitor that group. CA IAM CS synchronizes any changes to the SalesForce environment in the cloud.

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



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:

Deploy 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.

You can deploy connectors that came with your product, and connectors that you downloaded from the CA Support site.

Follow these steps:

1. If required, download the connector and save the files locally.
2. Log in to CA IAM CS (see page 21).
3. At the top, click the Connector Servers tab.
4. In the Connector Server Management area, click the Bundles tab.
5. In the Bundles area on the right, click Add.
6. 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.
7. Click OK.

   The new bundle appears in the Bundles list.
8. 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 314)
- SAP R3 (see page 356)
- Oracle PeopleSoft (see page 307)
- Lotus Domino (see page 188)

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:

   Note: You can deploy the OSGI bundle from the connector server GUI or copy the jar files to ca-home/jcs/data/bundles/restore. Then restart the connector server and wait up to ten minutes for it to load.

   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 select 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 template file 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

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.

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 Identity Management 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 Identity Management, 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 Identity Management 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 Identity Management 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 Identity Management 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.

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 Identity Management.

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, Identity Management 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:

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

      Click Select Container/Endpoint/Explore Method to click a Access Control 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 Identity Management 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 Identity Management based on the explore and correlate definition you created.

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.

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 Identity Management password synchronization agent supports the interception of Windows password changes.

Reconfiguring the Password Synchronization Component

These are the steps to reconfigure a Identity Management 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 Identity Management.

   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 Identity Management.
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

Identity Management manages CA Access Control identities in an identity store that can be either a CA Access Control PMDB or a local database. Since Identity Management and CA Access Control both manage users and passwords, it is an architecture decision as to which users are managed by Identity Management and which by CA Access Control. A general guideline is that Identity Management 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 Identity Management password synchronization component intercepts the password change and propagates it to other Identity Management 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 Identity Management 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 Identity Management Windows Password
; Synchronization Facility.
;
[Server]
host=<Provisioning Server host>
port=20389
use_tls=yes
admin_suffix=dc=<domain suffix>
admin=etaadmin
password=k4tpGDJ8Djg=

;; Identity Management 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 Identity Management 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=

;; Identity Management 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". Identity Management 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 v2 Connector

The following sections describe how to use the CA ACF2 v2 connector.

Introduction

This guide describes how to use the following connectors to connect CA IAM CS with CA ACF2 endpoints:

- CA ACF2 v2 Connector with Identity Management and CA CloudMinder (see page 81)

  CA ACF2 v2 is a Java connector that is installed with the CA IAM Connector Server (CA IAM CS). Identity Management and CA CloudMinder can use this connector to gather data and provision users in a CA ACF2 v2 endpoint.

- CA ACF2 ACFESAGE Connector with CA GovernanceMinder

  The CA ACF2 ACFESAGE connector is a dump file Java connector which is installed with the CA IAM CS. The ACFESAGE utility extracts information from the CA ACF2 system to a security file. CA GovernanceMinder can then read endpoint information from that file.

  Note: The CA ACF2 connector is replaced by the CA ACF2 v2 connector. New deployments should use the CA ACF2 v2 connector.

Audience

This guide targets the following people:

- Identity Management administrators responsible for connecting endpoints to Identity Management
- The mainframe security administrator responsible for the endpoint.

Supported Systems

To see a list of supported systems, use the Platform Support Matrix:

- Platform Support Matrix for Identity Management
- Platform Support Matrix for CA GovernanceMinder

To verify which endpoint versions are supported, see the table "Supported Connector Endpoint Types" in the Platform Support Matrix. This table also lists the version of CA LDAP Server that the mainframe requires.

To verify which operating systems CA IAM CS can run on, see the table "Supported Connector Servers" in Platform Support Matrix.

To see a list of attributes that CA IAM CS handles, see the attribute list on the Download page for Endpoint Guides for Identity Management.

What the Connector Can Do

This table lists the tasks that the connector lets applications do:

Task	Identity Management
Create, read, update, and delete an ACID user on the CA Top Secret endpoint	Yes
Assign and unassign a number of *is interesting to compliance* account attributes	No
Map custom attributes	Yes

File Locations

This document refers to the installation location of CA IAM CS as *cs_install*. By default, *cs_install* is in the following locations:

- **Windows:** C:\Program Files (86)\CA\Identity Manager\Connector Server
- **Linux and Solaris:** /opt/CA/IdentityManager/ConnectorServer

The Provisioning Server installation location is referred 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/

For the migration process, the tool uses the default logging configuration path that is specified in *java_home*/lib/logging.properties.

Compare the CA ACF2 and CA ACF2 v2 Connectors

The CA ACF2 connector is hosted by the Provisioning Server as a server plug-in. The new connector (CA ACF2 v2) is hosted by CA IAM CS. The following table compares feature support in the CA ACF2 and CA ACF2 v2 connectors.

Feature	CA ACF2 Connector (Plugin for Provisioning Server)	CA ACF2 v2 Connector (New Java connector with CA IAM CS)
Explore & Correlate Explore and Correlate is used by the connector to discover objects in the endpoint.	Yes	Yes
Provisioning Manager Provisioning Manager is the legacy client of Identity Management. It provides limited access to functionality in the CA ACF2 v2 connector.	Yes	No
Fetch Suffix List The "Get Suffixes" feature is not available in CA ACF2 v2 connector. However, as a workaround, you can enter the attributes and click Submit. An error message displays a list of available suffixes at the endpoint.	Yes	On Error
Use Logged on Administrator Credentials Legacy mainframe connectors can use logged-in user (Global User) credential to access the endpoint. The CA ACF2 v2 connector uses the endpoint administrator's login credentials to access the endpoint.	Yes	No

Feature	CA ACF2 Connector (Plugin for Provisioning Server)	CA ACF2 v2 Connector (New Java connector with CA IAM CS)
SSL All communication between the Client and the CA LDAP Server for z/OS can be encrypted using one way SSL (Secure Socket Layers).	Yes	Yes
Display System Options On the Provisioning Manager Endpoint screen, the System Options feature tab displays endpoint specific information such as version. For supported v2 connectors, this information is available on the endpoint screen of the Identity Management User Console.	Yes	Yes
Account/LID CRUD Account management activities (Create, Read, Update, Delete).	Yes	Yes
Rules Read access and ability to add rule lines.	Provisioning Manager only	No
Associate Account with Secondary Auth IDs	Yes	No
Account Custom Attributes The default connector provides access to commonly used account attributes. However, you may need to manage additional fields as well. With legacy connectors, map the additional attributes to custom attributes in 'schema_map.txt' in the following location: <IMPS_HOME>\data\<Connector Name>\schema_map.txt For new connectors, map custom attributes in Connector Xpress.	Yes	Yes
Reverse Sync Reverse sync is a process that allows users to take actions on endpoint accounts discovered by the explore and correlate process based on a set of defined policies.	Yes	Yes
Multithreading An execution model that provides higher processing efficiency.	No	Yes
Password Options The Password Options tab in the Provisioning Manager displays endpoint password information. A similar tab is available in the Identity Management User Console endpoint screen when the relevant mainframe v2 connector supports this feature.	Yes	Yes

Feature	CA ACF2 Connector (Plugin for Provisioning Server)	CA ACF2 v2 Connector (New Java connector with CA IAM CS)
Password Synch Agent The Password Synch Agent is installed at the endpoint. When the global user is enabled for the password synchronization agent (in the Provisioning Manager Global user screen, Password tab), a password change at the endpoint, using the native tool, can be propagated back to the Global User and to the other endpoint accounts of the same Global User.	Yes	No
LDS Wizard LDAP directory services.	Provisioning Manager only	No
Import from Identity Management 12.6 to CA GovernanceMinder 12.5 SP8/12.6.1 The connector marks a set of objects and attributes as 'Interesting to compliance' for CA GovernanceMinder. CA GovernanceMinder (CA RCM) connects to Identity Management and extracts Users, Account Templates, Provisioning Roles and Resources.	Yes	No
Export to Identity Management 12.6 from CA GovernanceMinder 12.5 SP8/12.6.1 CA GovernanceMinder can modify associations on the imported data set. These changes can be pushed to the endpoint through Identity Management. This process is called an export.	Yes	No

Chapter 7: Security

Privileges Required to Connect to ACF2

To connect to a CA ACF2 endpoint, the Identity Management administrator must have access to Time Sharing Option (TSO) to generate and issue commands for CA LDAP Server.

Securing Communication between ACF2 and CA IAM CS

Identity Management can send passwords and other security information across the network.

We recommend that you use SSL to secure the connection between ACF2 and CA IAM CS, using the steps in Set up SSL in ACF2. When you do not set up SSL communication, the information is sent without encryption, which is creating a security risk.

We recommend that you use SSL to secure the connection between CA ACF2 and CA IAM CS, using the steps in Install and Configure CA LDAP Server (see page 83) and Import the CA LDAP Server Certificate into the CA IAM CS Keystore (see page 85).

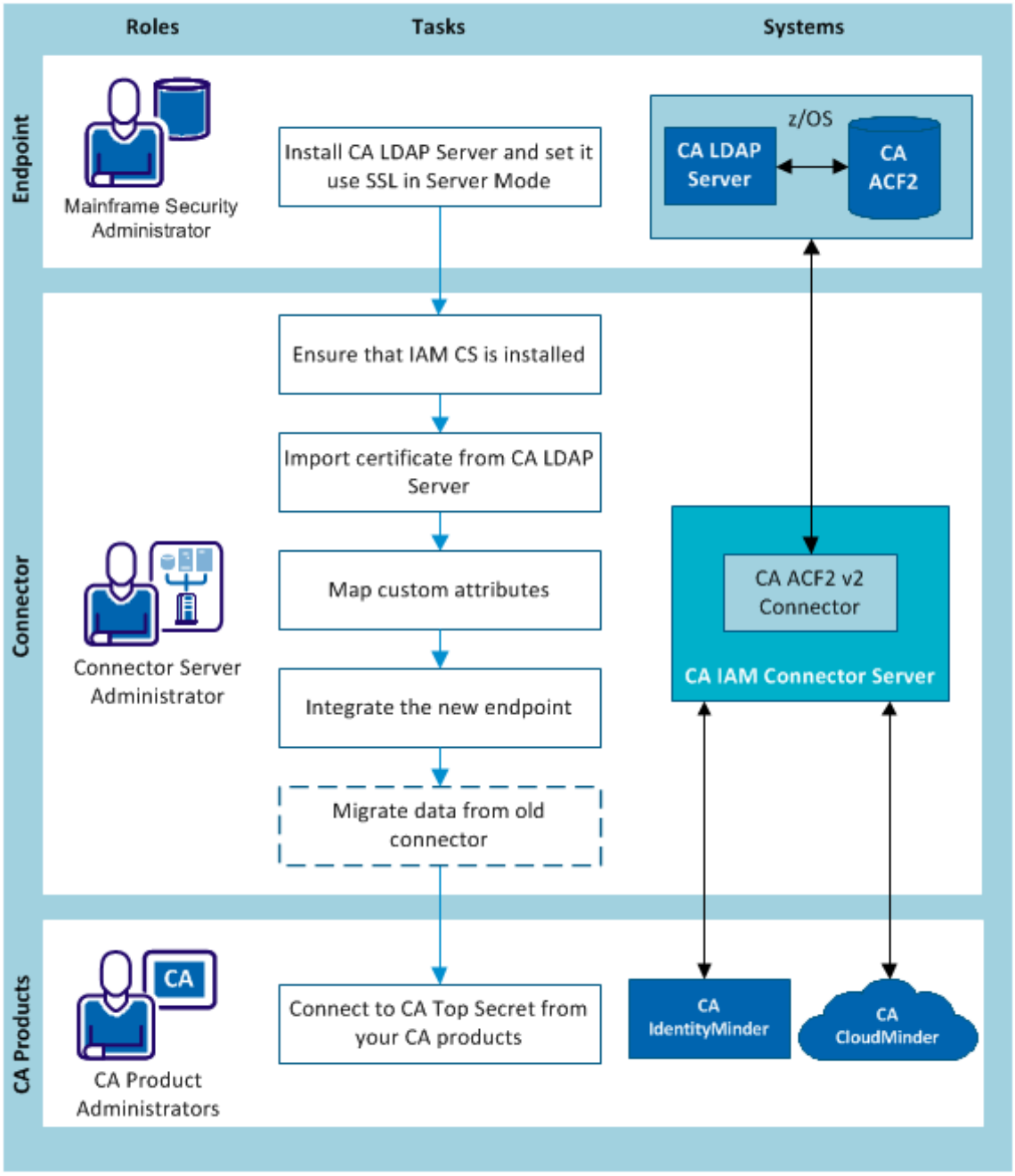
CA ACF2 v2 Connector

CA ACF2 v2 is a Java connector that is installed with the CA IAM CS. This chapter describes how to connect to a CA ACF2 v2 connector. You can use the CA ACF2 v2 connector to allow the following products to connect to a CA ACF2 endpoint:

- Identity Management
- CA CloudMinder

In Identity Management, if you are replacing the CA ACF2 connector with the CA ACF2 v2 connector, use the migration tool to migrate account templates and their associations to objects in the CA ACF2 v2 connector. For more information, see Appendix A: How to Migrate Data from the Plug-in Connector (see page 88) section in this guide.

The following diagram shows the tasks that are required to connect to the endpoint, and who does each task.



1. The mainframe security administrator installs CA LDAP Server on the mainframe, then sets it to use SSL in Server Mode (see page 83).
2. The connector server administrator does the following steps:
   a. (If necessary) Install CA IAM CS. For details, search for *Install CA IAM CS* in the Identity Management bookshelf.
   b. (If necessary) Import the CA LDAP Server certificate into the CA IAM CS keystore (see page 85).
   c. (If necessary) Map custom attributes (see page 159).
   d. Integrate the managed endpoints in Identity Management.
   e. For CA CloudMinder, configure the cloud-based CA IAM CS for setting up CA IAM CS on the cloud.
   f. If necessary, the Identity Management administrator migrates data from a CA ACF2 endpoint that used the old plug-in connector. This is described in How to Migrate Data (see page 88).
3. The CA product administrators connect to the endpoint in Identity Management or CA CloudMinder.

Install and Configure CA LDAP Server

This procedure is for the mainframe security administrator.

To allow CA IAM CS to communicate with the endpoint, install CA LDAP Server on the mainframe. To keep your data secure, configure CA LDAP Server to use SSL.

For information about CA LDAP Server, use the following links:

- CA LDAP Server r14 bookshelf
- CA LDAP Server r15 bookshelf

Follow these steps:

1. Install CA LDAP Server.

   Instructions for CA LDAP r15 are in the CA LDAP Installation Guide.

   Instructions for CA LDAP r14, are in the Installation chapter in the CA LDAP Product Guide.

2. Configure CA LDAP Server to use SSL in Server mode.

   Instructions are in "Client SSL Setup From the Command Line" in the CA LDAP Product Guide for CA LDAP r15 bookshelf.

   These instructions also apply to CA LDAP r14.

Ensure that CA IAM CS Is Installed

Check that CA IAM CS is installed and running.

CA IAM CS is installed with the following products, unless you deselected the CA IAM CS option:

- **Identity Management r12.6.2 and later**—For details, search for *Install CA IAM CS* in the Identity Management bookshelf.
- **CA GovernanceMinder r12.6 and later**—For details, search for *Connectivity Use Cases* in the CA GovernanceMinder bookshelf.
- **CA CloudMinder 1.1 and later**—Check that CA IAM CS is installed both in the CA CloudMinder cloud and on-premise:
  - CA IAM CS is installed in the CA CloudMinder cloud by the hosting administrator. For details, search for *Provisioning Server and CA IAM Connector Server* in the CA CloudMinder for Service Providers bookshelf.
  - CA CloudMinder also requires an on-premise installation of CA IAM CS for each tenant. For details, search for *How to Set Up On-Premise Provisioning* in the CA CloudMinder for Tenant Administrator bookshelf.

Import the CA LDAP Server Certificate into the CA IAM CS Keystore

This procedure is for the Identity Management and CA CloudMinder administrator. If CA IAM CS already has the CA LDAP Server certificate, ignore this procedure.

After the mainframe security administrator has confirmed that CA LDAP Server is configured to use SSL, you can import the CA LDAP Server certificate into the CA IAM CS keystore.

Follow these steps:

1. Identify the certificate which you want to import into the CA IAM CS keystore as a trusted certificate:
   - The CA LDAP Server certificate.
   - The root certificate of the certificate authority that has issued the CA LDAP Server certificate, and the application server certificate
2. Import the chosen certificates:
   a. Log in to CA IAM CS (see page 21).
   b. At the top, click the Certificates tab.

      The Certificates 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.
   c. To add a certificate, click Add, then enter the details of the certificate:
      - **Certificate**—Enter the path to the certificate file
      - **Alias**—Enter an alias for storing the certificate

Map Custom Attributes for Identity Management

This procedure is for the CA CloudMinder or Identity Management administrator.

When you connect to an endpoint, the objects on the endpoint are mapped to objects in CA CloudMinder or Identity Management. This happens automatically. If you want to make custom mappings, use Connector Xpress.

For instructions about setting up custom mapping with Connector Xpress, search for *Managing Accounts and Groups* in the CA CloudMinder bookshelf or in the Identity Management bookshelf.

To see a list of the objects on the endpoint, download the attribute list from this page: Download page for Endpoint Guides.

Any LDAP attribute on the mainframe that has a string representation can be exposed as a custom attribute in the connector. To map custom attributes, use Connector Xpress. For information, search for *Managing Accounts and Groups* in the Identity Management bookshelf or CA CloudMinder bookshelf.

Integrate the Managed Endpoint in Identity Management

For the details about the following steps, search for the following topics based on the CA product:

- For CA CloudMinder and Identity Management 12.6 releases, search for *Integrating the Endpoint* in the CA CloudMinder bookshelf or search for *Integrating Managed Endpoints* in the Identity Management bookshelf.
- For CA Identity Manager 12.5 releases, search for *Managed Endpoint Accounts* in the CA Identity Manager bookshelf.

Follow these steps:

1. Navigate to the connectors download page, then open the attribute list for this endpoint type.

   This HTML page lists every endpoint attribute that the connector works with. Use this information in the following steps.

2. Set up the connector:

   a. Import the role definition file.

   b. (CA CloudMinder only) Create a role to manage the endpoint.

   c. Create correlation rules. Skip this step if you plan to migrate data.

   d. (CA CloudMinder only) Configure email notification for the endpoint.

3. Add the endpoint to the environment. In the Endpoint tab, complete the following mandatory fields:

   Endpoint Name

   Specifies the name of the new CA Top Secret endpoint. The endpoint name is the name that appears in the Provisioning Manager. Commas and semi-colons are not allowed.

   Mainframe LDAP IP Address/Machine Name

   Specifies the mainframe LDAP IP Address or machine name of the CA Top Secret.

   Mainframe LDAP Port

   Specifies the Listen Port for the Security Integrator running on the CA Top Secret.

   Use Server-Side SSL

   When checked, specifies that the server's SSL is used.

   Note: Ensure that you have imported the SSL certificate to Provisioning Server (see page 85).

Mainframe LDAP DN Suffix

Specifies valid suffixes that are configured for the current 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.)

Proxy Admin ID

Allows you to specify an ID that is used to issue the password modifications that are requested through the workflow. This provides users with the ability to change or reset their passwords if their password has expired and they cannot be authenticated to the system.

Proxy Admin Password

The password to the Proxy Admin ID on the CA Top Secret endpoint.

When you complete the fields on the Endpoint tab, use the information in the Endpoint section of the attribute list. You can find the details on the Download page.

4. Create an explore and correlate definition. Do not include the correlation if you plan to migrate data.

   Important! If you plan to migrate data from the plug-in connector, explore but **do not correlate**. Correlation of the new endpoint can introduce new associations that conflict with the correlation rules of the old endpoint.

5. Explore and correlate the endpoint.

   Note: If your explore-and-correlate definition does not include correlation, this step explores only.

How to Migrate Data

This section applies to Identity Management only.

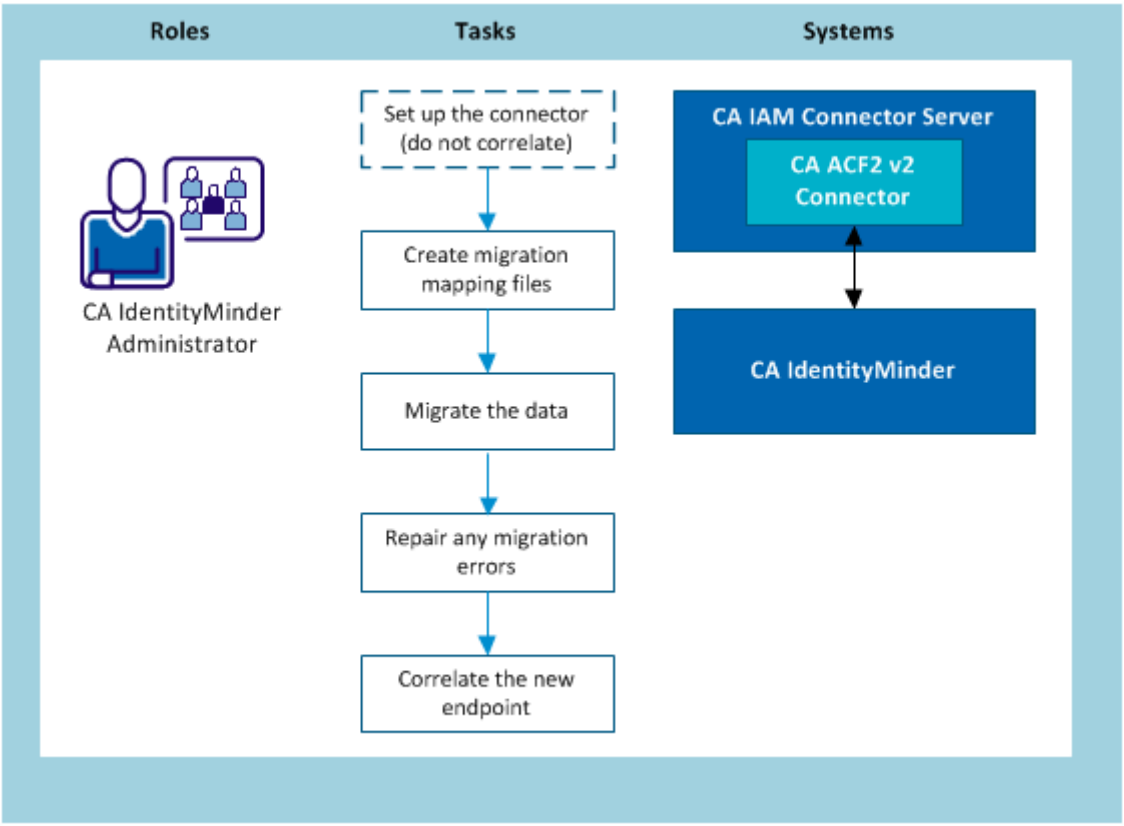
CA IAM CS comes with a tool that helps you migrate account templates and their associations to objects in the new connector. If Identity Management already manages ACF2 endpoints using the plugin connector, you can use the existing ACF2 data with the new connector.

This tool migrates the following data:

- Account templates

  The migrated account templates have the same name as the old account templates.
- Associations between account templates and endpoints, roles, and accounts

You cannot use this tool to migrate endpoint objects. Before you can migrate other data, acquire and explore the endpoints with the new connector.



1. Before you migrate data, set up the connector without correlating, using the steps in How to Connect to ACF2 (see page 81).
2. Create two migration mapping files (see page 89).
3. Migrate the data (see page 90)
4. Repair migration errors (see page 92)
5. Correlate the data (see page 92).

Create Two Migration Mapping Files

The migration tool works with two mapping files:

- (Required) A file that specifies which old endpoints are migrated to which new endpoints.

  The endpoint mapping file uses the following format:

  ```
  OldEndpointName=NewEndpointName
  ```

- (Optional) A file that specifies any custom attributes that you plan to manage.

  The custom attribute mapping file uses the following format:

  ```
  from-custom-attribute=to-endpoint-attribute
  ```

  The mapping file has the same format and contents as the schema_map.txt used in Provisioning Manager and Provisioning Server. You can use schema.txt as the mapping configuration file for the migration.

Follow these steps:

1. Set up any custom attributes in the new endpoint in Identity Management.
2. Prepare the endpoint mapping file. Only the old endpoints that are specified in this mapping file are migrated.

   When you run the mapping tool, use the *–c* option to specify the path to the mapping file.
3. Prepare the mapping file for any custom attributes, if necessary.

   When you run the mapping tool, use the *–m* option to specify the path to the mapping file.

Example: Endpoint mapping file

In the example below, the administrator chooses to keep the endpoint name the same:

```
MFTSS.org.com=MFTSS.org.com
```

Example: Custom attribute mapping file

```
CustomAttribute001=VSE-IES-Dflt-Usercat
CustomAttribute002=VSE-IES-Fld1
```

Migrate the Data

Before you migrate your data, we recommend that you run a simulation first. This generates an HTML report that lists the following items:

- Objects and inclusions that are created
- Potential migration failures

Follow these steps:

1. Open a command prompt and navigate to this location:

   cs_home/bin/ACF2v2Migrate

2. To run a simulated migration, use the acf2v2migrate command with the *-r S* option. For example:

   ```
   ACFv2Migrate -h mycomputer -d im –p 20390 –u admin –c
   c:\endpointconfig.txt –m c:\schema_map.txt –r S
   ```

3. To migrate the data, use the acf2v2migrate command with the *-r R* option. For example:

   ```
   ACF2v2Migrate -h server32 -d im -p 20389  -u etaadmin -n -r R -c
   acf2_endpoints.properties –l logging.properties
   ```

   The tool migrates the data and saves a report in *cs_home*/jcs/resources/acf2.

4. Verify the new account templates and associations.

Migrate Configuration and Data from Old Connector to New

The migration tool converts data from the old plugin connector to the new ACF2 v2 connector.

Note: You cannot migrate the *endpoint* using this tool. Before you can migrate the data, configure the endpoint in Identity Management.

The following command is the syntax used to execute migration:

```
ACF2v2Migrate <options>
```

-h *hostname*

Specifies the computer that hosts Identity Management Provisioning Server.

-d *domain*

Identifies the Identity Management domain that contains the endpoints that you want to migrate. Default: im

-p *port*

Defines the port number of Identity Management Provisioning Server. Default: 20389 for no TLS and 20390 for TLS.

-u *username*

Identifies the administrative user of the Identity Management domain.

-r R

Produces a report that lists the objects and inclusions that would have been migrated, plus any failures.

-n

Disable TLS communication. Default: TLS is enabled.

-r S

Produces a report that lists the objects and inclusions that would have been migrated.

-m *path*

Specifies the file that contains mappings for custom attributes in ACF2. For more information, read Create Two Migration Mapping Files (see page 89).

-c *path*

Defines the path to the endpoints configuration file. For more information, read Create Two Migration Mapping Files.

-l *path*

Specifies the logging configuration file. If this is omitted, the migration tool uses the default logging configuration specified in <JAVA_HOME>/lib/logging.properties. For more information, read Configure the Migration Log File (see page 93).

Repair Migration Errors

After the migration has finished, check the outcome carefully. If the result of the migration is not as desired, you can delete the new data and start again.

Follow these steps:

1. Delete the new endpoints in the ACF2 namespace specified in the endpoint mapping file. This deletes all associated account objects in Identity Management without affecting the endpoint itself. This will also remove all global users – account inclusions.
2. Delete the new account templates in the ACF2 namespace. This removes all associations with the account templates.

   Afterwards, repeat the steps in Create Two Migration Mapping Files (see page 89) and make the necessary modifications to ensure the migration will produce the desired result.

Correlate the Data

If you migrated data from old endpoints, you first explored the data but you did not correlate the data. After the migration is complete, correlate the data.

To correlate the data, follow the instructions in the Identity Management Administration Guide. Search for these steps in *Integrate the Managed Endpoint in Identity Management*, in the Identity Management bookshelf.

For now, include the options for the correlation. The following steps list the actions to perform:

Follow these steps:

1. Create correlation rules.
2. Edit the explore and correlate definition.

   For now, select the correlation checkbox.
3. Explore and correlate the endpoint.

   For now, the data is both explored and correlated.

The endpoint is ready for use in Identity Management.

Troubleshooting

Configure the Migration Log File

This topic applies to all of the mainframe connectors.

The migration tool uses java.util.logging. When you run the tool, you can use the *-l* option to specify the configuration file for the logging system. This file configures the type and format of the information that is logged and the location of log files.

For example, you can configure any of the following log levels:

- Log errors only.
- Log everything, including debugging info.
- Make the timestamps include dates and times down to seconds.
- Make the timestamps include dates only.
- Send the logs to the console.
- Send the logs to a file.

If you do not want to change the default logging configuration, omit the *-l* option.

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 Identity Management or CA CloudMinder 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 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 Identity Management or CA CloudMinder 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

This guide no longer contains information about the CA Arcot connector.

Instead, download the CA AuthMinder endpoint guide from the Download page for Endpoint Guides and Attribute Lists.

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

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 Identity Management 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 Identity Management User Console.

    b. Import the CA_DLP.jar file into the Identity Management 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 Identity Management 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 Identity Management 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 Identity Management 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 Identity Management 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 Identity Management, stop the Identity Management 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 Identity Management Server.

   Identity Management loads the new role, screen, and task definitions for the CA DLP account management screens.
8. Start the Identity Management 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.

    Identity Management 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.

    Identity Management deploys the role definitions, screens, tasks, and roles for the CA DLP Connector and updates the Identity Management environment you selected.

12. Click Continue, then click Restart Environment.
13. Start the Identity Management User Console.
14. Verify that Identity Management has renamed the User Attribute 1 field to City, as follows:
    a. In the Identity Management User Console, view the CA DLP account of a user.
    b. Click the User Attributes 1 Tab.
    c. Verify that Identity Management 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 Identity Management 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 Identity Management User Console.

    b. Import the CA_DLP.jar file into the Identity Management 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 Identity Management 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 Identity Management 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 Identity Management 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 Identity Management 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 Identity Management 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 Identity Management, stop the Identity Management 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 Identity Management Server.

   Identity Management loads the new role, screen, and task definitions for the CA DLP account management screens.
8. Start the Identity Management 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.

    Identity Management 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.

    Identity Management deploys the role definitions, screens, tasks, and roles for the CA DLP Connector and updates the Identity Management environment you selected.
12. Click Continue, then click Restart Environment.
13. Start the Identity Management User Console.
14. Verify that Identity Management has added the user category Assistant Manager to the CA DLP account management screens, as follows:
    a. In the Identity Management User Console, view the CA DLP default template
    b. Click the Account tab.
    c. Verify that Identity Management 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 Identity Management 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 Identity Management, 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 Identity Management 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 Identity Management User Console.

Note: Attempts to delete an email address from a CA DLP account in the Identity Management 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 Identity Management 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 Identity Management.

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 Identity Management 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 Identity Management 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
   ```

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 112)

Authentication Method Question (see page 113)

Buffer Size Question (see page 114)

Exploration Questions (see page 114)

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 following sections describe how to use the CA Top Secret connector.

Introduction

This guide describes how to use the following connectors to connect CA IAM CS with CA Top Secret endpoints:

- CA Top Secret v2 Connector with Identity Management and CA CloudMinder (see page 121)

  CA Top Secret v2 is a Java connector that is installed with the CA IAM Connector Server (CA IAM CS). Identity Management and CA CloudMinder can use this connector to gather data and provision users in a CA Top Secret endpoint.

- TSS TSSCFILE Connector with CA GovernanceMinder

  The TSS TSSCFILE connector is a dump file Java connector which is installed with the CA IAM CS. The TSSCFILE utility extracts information from the CA Top Secret system to a security file. CA GovernanceMinder can then read endpoint information from that file.

- CA Top Secret Connector with Identity Management and CA GovernanceMinder

  The CA Top Secret connector is a plug-in component of the Identity Management Provisioning Server. CA GovernanceMinder can access the endpoint through its Identity Management connector.

  Note: The CA Top Secret connector is replaced by the CA Top Secret v2 connector. New deployments should use the CA Top Secret v2 connector.

More Information:

Compare Three Methods for Connecting to CA Top Secret Endpoints (see page 116)

Audience

This guide targets the following people:

- The Identity Management administrators responsible for connecting endpoints to Identity Management
- The CA CloudMinder administrators responsible for connecting endpoints to CA CloudMinder
- The CA GovernanceMinder administrators responsible for integrating CA GovernanceMinder with other products
- The mainframe security administrator responsible for the endpoint

Supported Systems

To see a list of supported systems, use the Platform Support Matrix:

- Platform Support Matrix for Identity Management
- Platform Support Matrix for CA GovernanceMinder

To verify which endpoint versions are supported, see the table "Supported Connector Endpoint Types" in the Platform Support Matrix. This table also lists the version of CA LDAP Server that the mainframe requires.

To verify which operating systems CA IAM CS can run on, see the table "Supported Connector Servers" in Platform Support Matrix.

To see a list of attributes that CA IAM CS handles, see the attribute list on the Download page for Endpoint Guides for Identity Management.

What the Connector Can Do

File Locations

This document refers to the installation location of CA IAM CS as *cs_install*. By default, *cs_install* is in the following locations:

- **Windows:** C:\Program Files (86)\CA\Identity Manager\Connector Server
- **Linux and Solaris:** /opt/CA/IdentityManager/ConnectorServer

The Provisioning Server installation location is referred 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/

For the migration process, the tool uses the default logging configuration path that is specified in *java_home*/lib/logging.properties.

Compare Three Methods for Connecting to CA Top Secret Endpoints

There are three different connectors that you can use to gather data from a CA Top Secret endpoint. The connector named Top Secret TSSCFILE is supplied with CA GovernanceMinder. The connectors named CA Top Secret and CA Top Secret v2 are supplied with Identity Management and CA CloudMinder.

This table compares the methods that are used for connecting CA Top Secret connectors to a CA Top Secret endpoint.

	CA Top Secret v2 Connector	TSS TSSCFILE Connector	CA Top Secret Connector

	CA Top Secret v2 Connector	TSS TSSCFILE Connector	CA Top Secret Connector
Description	A Java connector which is installed with CA IAM CS.	A Java connector which is installed with CA IAM CS.	A plug-in component of Provisioning Server in Identity Management.
Systems that can use this connector	Any system that uses CA IAM CS, including Identity Management and CA CloudMinder.	CA GovernanceMinder only	Existing Identity Management deployments **Note:** New Identity Management deployments should use the CA Top Secret v2 connector. CA GovernanceMinder can access the endpoint through its Identity Management connector.
What can the connector do?	Read and write: Provision users Gather data	Read only: Gather data	Read and write: Provision users Gather data
Method for acquiring data	Connector communicates with CA LDAP Server, which is installed on the CA Top Secret endpoint.	Use the TSSCFILE utility to dump data into a text file. The connector server connects to the file, and CA GovernanceMinder communicates with the connector server.	Connector communicates with CA LDAP Server, which is installed on the CA Top Secret endpoint.
How roles and resources are handled (relevant for CA GovernanceMinder only)	Not supported in this release.	Provides direct and indirect associations between ACIDS, groups, profiles, zones, departments, divisions, and resources.	Provides ACIDS and the attributes, privileges, and resources that are directly associated with them. Provides direct associations between ACIDs and groups, profiles, zones, departments, and divisions.
Type of mapping for CA GovernanceMinder	Not supported in this release.	Shallow and deep mappings	Shallow mappings
Documentation	This guide	This guide	This guide

Feature Comparison of CA Top Secret and CA Top Secret v2 Connectors

The table in Compare Three Methods for Connecting to CA Top Secret Endpoints (see page 116) shows three connectors. The following table contrasts only the connectors that are available in Identity Management.

The differences are important if you currently use the old connector and you plan to migrate to the new connector. Use the following table to verify whether you want to upgrade or not.

Feature	CA Top Secret Connector (Plug-in for Provisioning Server)	CA Top Secret v2 Connector (New Java connector with CA IAM CS)
Uses Provisioning Manager Provisioning Manager is a legacy client of Identity Management. It supports the earlier supported connectors. Provisioning Manager is no longer supported for new connectors.	Yes	No
Use admin credentials for accessing the endpoint The new connector cannot use the logged-in user (Global User) credential to access the endpoint. Instead, it accesses the endpoint using the credentials used to acquire the endpoint.	Yes	No
SSL All communication between the Client and CA LDAP Server for z/OS can be encrypted using SSL.	Yes	Yes
Create, read, update, and delete accounts and ACIDs	Yes	Yes
Create, read, update, and delete the following data: ■ Department ■ Division ■ Group ■ Profile ■ Zone	Yes, in Provisioning Manager only	No
Assign the following data to an account: ■ Department ■ Division ■ Group ■ Profile ■ Zone	Yes	Yes

Feature	CA Top Secret Connector (Plug-in for Provisioning Server)	CA Top Secret v2 Connector (New Java connector with CA IAM CS)
Fetch Suffix List The new connector does not support the Get Suffixes function. Instead, ask the mainframe administrator for the suffix when you ask for the machine name.	Yes	No
Custom attributes The plug-in connector lets you map additional fields to custom attributes using schema_map.txt. The new connector requires you to map custom attributes with Connector Xpress.	Yes	Yes
Multithreading to provide higher processing efficiency	No	Yes
System Options displayed in client System Options is moved from the System Options tab in Provisioning Manager to the System Options tab in User Console.	Yes	Yes
Password Options displayed in client Password Options is moved from the Password Options tab in Provisioning Manager to the Password Options tab in User Console.	Yes	Yes
Password Synch Agent Password Synch Agent is an agent to be installed at the endpoint. This agent propagates a password change from the endpoint to the Global User and to the other endpoint accounts of the same Global User.	Yes	Yes
LDAP Service Wizard LDAP Service wizard sets up password sync parameters on mainframe.	Yes, in Provisioning Manager only	No
Import from Identity Management to CA GovernanceMinder 12.5 SP8/12.6.1 The connector marks a set of objects and attributes as Interesting to Compliance, for CA GovernanceMinder. CA GovernanceMinder connects to Identity Management and extracts users, account templates, provisioning roles and resources.	Yes	No
Export from CA GovernanceMinder 12.5 SP8/ 12.6.1 to Identity Management, and then to the endpoint After CA GovernanceMinder has modified associations on the imported data set, you can push those changes to the endpoint through Identity Management.	Yes	No

Feature	CA Top Secret Connector (Plug-in for Provisioning Server)	CA Top Secret v2 Connector (New Java connector with CA IAM CS)
Reverse Synchronization The process of reverse synchronization let users take actions on endpoint accounts discovered by the explore and correlate process based on a set of defined policies.	Yes	Yes

Chapter 8: Security

Privileges Required to Connect to CA Top Secret

To connect to a CA Top Secret endpoint using CA Top Secret and CA Top Secret v2 connectors, the system administrator must have access to Time Sharing Option (TSO). TSO is used to generate and issue commands for CA LDAP Server.

To connect to the TSSCFILE connector, the system administrator must have read access to the TSSCFILE file that contains the dumped data. The output file TSSCFILE must be moved to the computer that runs CA IAM CS. CA GovernanceMinder can connect to a file on the computer that runs CA IAM CS.

Securing Communication between CA Top Secret and CA IAM CS

We recommend that you use SSL to secure the connection between CA Top Secret and CA IAM CS. Perform the steps in Install CA LDAP and Configure It for SSL (see page 83) and Import the CA LDAP Server Certificate into the CA IAM CS Keystore (see page 85).

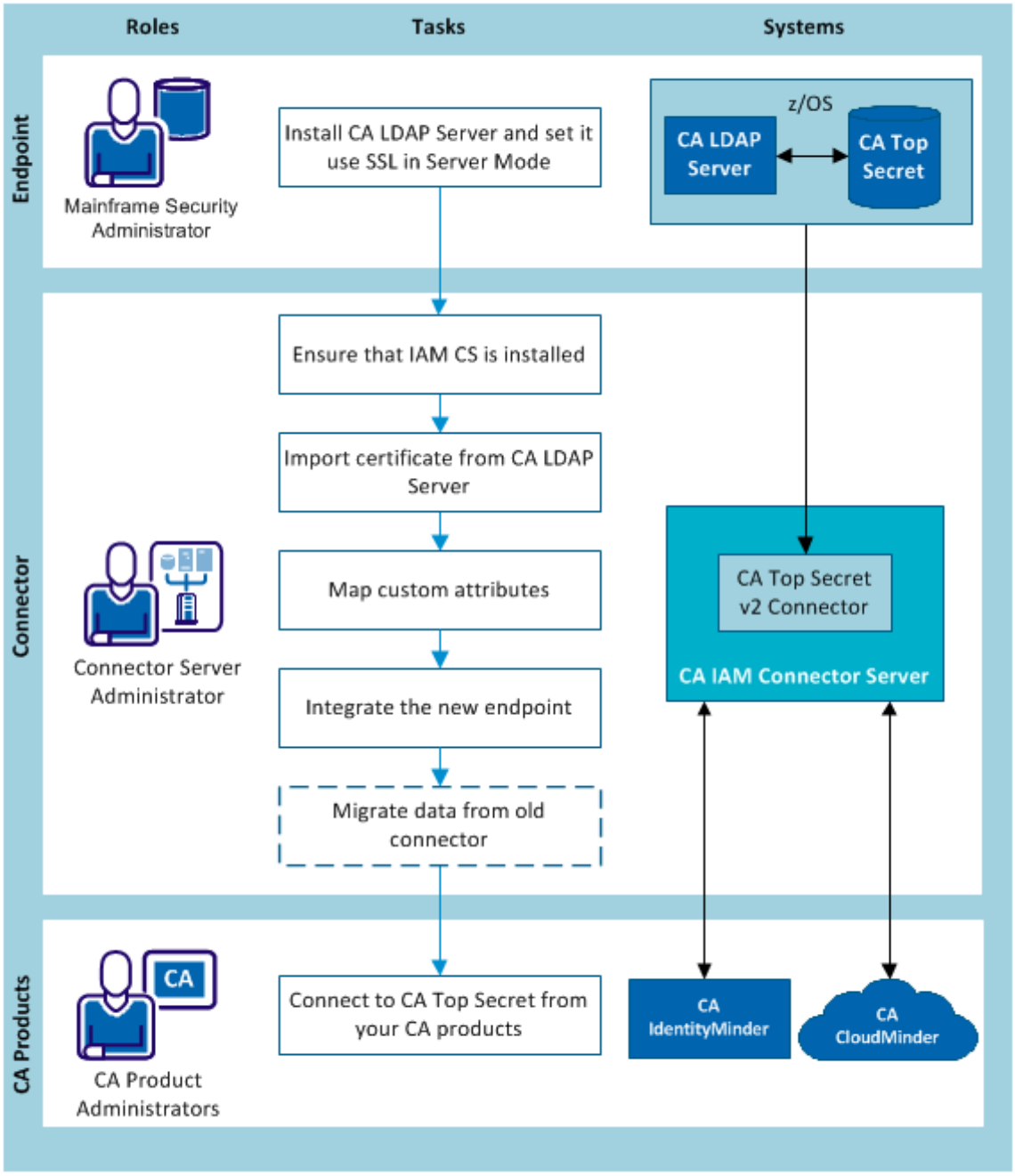
CA Top Secret v2

CA Top Secret v2 is a Java connector that is installed with the CA IAM CS. This chapter describes how to connect to a CA Top Secret v2 connector. You can use the CA Top Secret v2 connector to allow the following products to connect to a CA Top Secret endpoint:

- Identity Management
- CA CloudMinder

In Identity Management, if you are replacing the CA Top Secret connector with the CA Top Secret v2 connector, use the migration tool to migrate account templates and their associations to objects in the CA Top Secret v2 connector. For more information, see Appendix A: How to Migrate Data from the Plug-in Connector (see page 130) section in this guide.

The following diagram shows the tasks that are required to connect to the endpoint, and who does each task.



1. A mainframe security administrator installs CA LDAP Server on the mainframe, then sets it to use SSL in Server Mode (see page 83).
2. The connector server administrator does the following steps:
   a. (If necessary) Ensure that CA IAM CS is installed (see page 84).
   b. (If necessary) Import the CA LDAP Server certificate into the CA IAM CS keystore (see page 85).
   c. (If necessary) Map custom attributes (see page 125).
   d. Integrate the managed endpoints in Identity Management (see page 86).
   e. For CA CloudMinder, configure the cloud-based CA IAM CS for setting up CA IAM CS on the cloud.
   f. (If necessary) the Identity Management administrator migrates data from a CA Top Secret endpoint that used the old plugin connector. These details are described in How to Migrate Data (see page 130).
3. The CA product administrator connects to the endpoint:
   - Connect to the endpoint in Identity Management or CA CloudMinder
   - Connect to the endpoint in CA GovernanceMinder (see page 129)

Install and Configure CA LDAP Server

This procedure is for the mainframe security administrator.

To allow CA IAM CS to communicate with the endpoint, install CA LDAP Server on the mainframe. To keep your data secure, configure CA LDAP Server to use SSL.

For information about CA LDAP Server, use the following links:

- CA LDAP Server r14 bookshelf
- CA LDAP Server r15 bookshelf

Follow these steps:

1. Install CA LDAP Server.

   Instructions for CA LDAP r15 are in the CA LDAP Installation Guide.

   Instructions for CA LDAP r14, are in the Installation chapter in the CA LDAP Product Guide.

2. Configure CA LDAP Server to use SSL in Server mode.

   Instructions are in "Client SSL Setup From the Command Line" in the CA LDAP Product Guide for CA LDAP r15 bookshelf.

   These instructions also apply to CA LDAP r14.

Ensure that CA IAM CS Is Installed

Check that CA IAM CS is installed and running.

CA IAM CS is installed with the following products, unless you deselected the CA IAM CS option:

- **Identity Management r12.6.2 and later**—For details, search for *Install CA IAM CS* in the Identity Management bookshelf.
- **CA GovernanceMinder r12.6 and later**—For details, search for *Connectivity Use Cases* in the CA GovernanceMinder bookshelf.
- **CA CloudMinder 1.1 and later**—Check that CA IAM CS is installed both in the CA CloudMinder cloud and on-premise:
  - CA IAM CS is installed in the CA CloudMinder cloud by the hosting administrator. For details, search for *Provisioning Server and CA IAM Connector Server* in the CA CloudMinder for Service Providers bookshelf.
  - CA CloudMinder also requires an on-premise installation of CA IAM CS for each tenant. For details, search for *How to Set Up On-Premise Provisioning* in the CA CloudMinder for Tenant Administrator bookshelf.

Import the CA LDAP Server Certificate into the CA IAM CS Keystore

This procedure is for the Identity Management and CA CloudMinder administrator. If CA IAM CS already has the CA LDAP Server certificate, ignore this procedure.

After the mainframe security administrator has confirmed that CA LDAP Server is configured to use SSL, you can import the CA LDAP Server certificate into the CA IAM CS keystore.

Follow these steps:

1. Identify the certificate which you want to import into the CA IAM CS keystore as a trusted certificate:
   - The CA LDAP Server certificate.
   - The root certificate of the certificate authority that has issued the CA LDAP Server certificate, and the application server certificate
2. Import the chosen certificates:
   a. Log in to CA IAM CS (see page 21).
   b. At the top, click the Certificates tab.

      The Certificates 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.
   c. To add a certificate, click Add, then enter the details of the certificate:
      - **Certificate**—Enter the path to the certificate file
      - **Alias**—Enter an alias for storing the certificate

Map Custom Attributes for Identity Management

This procedure is for the CA CloudMinder or Identity Management administrator.

When you connect to an endpoint, the objects on the endpoint are mapped to objects in CA CloudMinder or Identity Management. The mapping happens automatically. If you want to make custom mappings, use Connector Xpress.

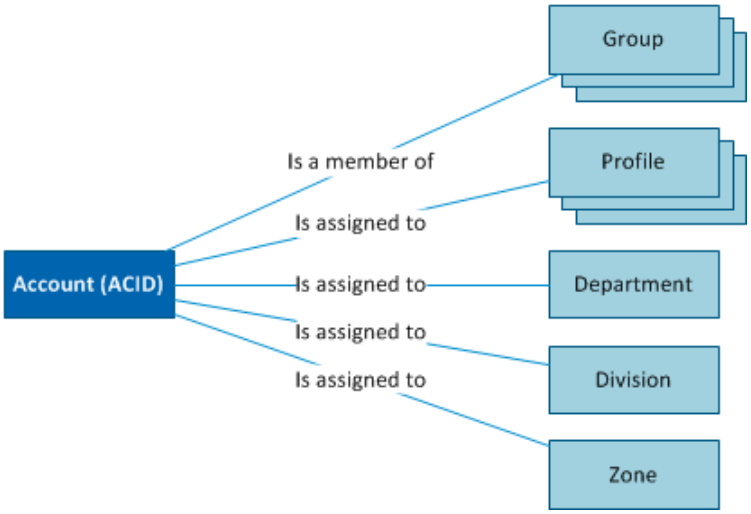
For the instructions about setting up custom mapping with Connector Xpress, search for *Managing Accounts and Groups* in the CA CloudMinder bookshelf or in the Identity Management bookshelf.

To see a list of the objects on the endpoint, download the attribute list from the following page: Download page for Endpoint Guides.

Any LDAP attribute on the mainframe that has a string representation can be exposed as a custom attribute in the connector. To map custom attributes, use Connector Xpress. For information, search for *Managing Accounts and Groups* in the Identity Management bookshelf or CA CloudMinder bookshelf.

Relationships Between Objects

The following diagram illustrates the relationships between accounts and other objects in CA Top Secret v2:



Note: The association between an ACID and a group or profile may have an expiry date.

Only the Groups and Profile attributes are available for use by CA GovernanceMinder. If you set up custom mapping for CA GovernanceMinder, ensure that you use the "Expire Date" attributes only.

Integrate the Managed Endpoint in Identity Management

For the details about the following steps, search for the following topics based on the CA product:

- For CA CloudMinder and Identity Management 12.6 releases, search for *Integrating the Endpoint* in the CA CloudMinder bookshelf or search for *Integrating Managed Endpoints* in the Identity Management bookshelf.
- For CA Identity Manager 12.5 releases, search for *Managed Endpoint Accounts* in the CA Identity Manager bookshelf.

Follow these steps:

1. Navigate to the connectors download page, then open the attribute list for this endpoint type.

   This HTML page lists every endpoint attribute that the connector works with. Use this information in the following steps.

2. Set up the connector:

   a. Import the role definition file.

   b. (CA CloudMinder only) Create a role to manage the endpoint.

   c. Create correlation rules. Skip this step if you plan to migrate data.

   d. (CA CloudMinder only) Configure email notification for the endpoint.

3. Add the endpoint to the environment. In the Endpoint tab, complete the following mandatory fields:

   Endpoint Name

   Specifies the name of the new CA Top Secret endpoint. The endpoint name is the name that appears in the Provisioning Manager. Commas and semi-colons are not allowed.

   Mainframe LDAP IP Address/Machine Name

   Specifies the mainframe LDAP IP Address or machine name of the CA Top Secret.

   Mainframe LDAP Port

   Specifies the Listen Port for the Security Integrator running on the CA Top Secret.

   Use Server-Side SSL

   When checked, specifies that the server's SSL is used.

   Note: Ensure that you have imported the SSL certificate to Provisioning Server (see page 85).

Mainframe LDAP DN Suffix

Specifies valid suffixes that are configured for the current 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.)

Proxy Admin ID

Allows you to specify an ID that is used to issue the password modifications that are requested through the workflow. This provides users with the ability to change or reset their passwords if their password has expired and they cannot be authenticated to the system.

Proxy Admin Password

The password to the Proxy Admin ID on the CA Top Secret endpoint.

When you complete the fields on the Endpoint tab, use the information in the Endpoint section of the attribute list. You can find the details on the Download page.

4. Create an explore and correlate definition. Do not include the correlation if you plan to migrate data.

   Important! If you plan to migrate data from the plug-in connector, explore but **do not correlate**. Correlation of the new endpoint can introduce new associations that conflict with the correlation rules of the old endpoint.

5. Explore and correlate the endpoint.

   Note: If your explore-and-correlate definition does not include correlation, this step explores only.

Connect to the Endpoint in CA GovernanceMinder through Identity Management

This procedure is for the CA GovernanceMinder administrator.

Use this method for a CA GovernanceMinder installation that is associated with a Identity Management installation. In this situation, connect CA GovernanceMinder to Identity Management. CA GovernanceMinder immediately has access to the endpoints that Identity Management connects to.

Follow these steps:

1. Ensure that Identity Management can successfully connect to the endpoint, using the instructions in Connect to the Endpoint in Identity Management.
2. Set up the connection to Identity Management. For instructions, search for *Integrating CA GovernanceMinder and CA IdentityMinder* in the CA GovernanceMinder bookshelf.

   Note: When you come to the setting up mapping between endpoint objects and CA GovernanceMinder resources, we recommend that you use the template that comes with the connector. However you can set up custom mapping for the endpoint.
3. Run an import.

   All endpoint data is imported into CA GovernanceMinder. The selected endpoint permissions are modeled as resources, while provisioning roles and account templates are modeled as roles.

The connection process is complete. The CA GovernanceMinder administrators can now set up a schedule for running the connector job. The role engineers can now use CA GovernanceMinder to model and update roles in the data from the endpoint.

How to Migrate Data from the Plug-in Connector to the New Java Connector

This section applies to Identity Management only.

CA IAM CS comes with a tool that helps you migrate account templates and their associations to objects in the new connector. If Identity Management already manages the CA Top Secret endpoints using the plug-in connector, you can use the existing CA Top Secret data with the new connector.

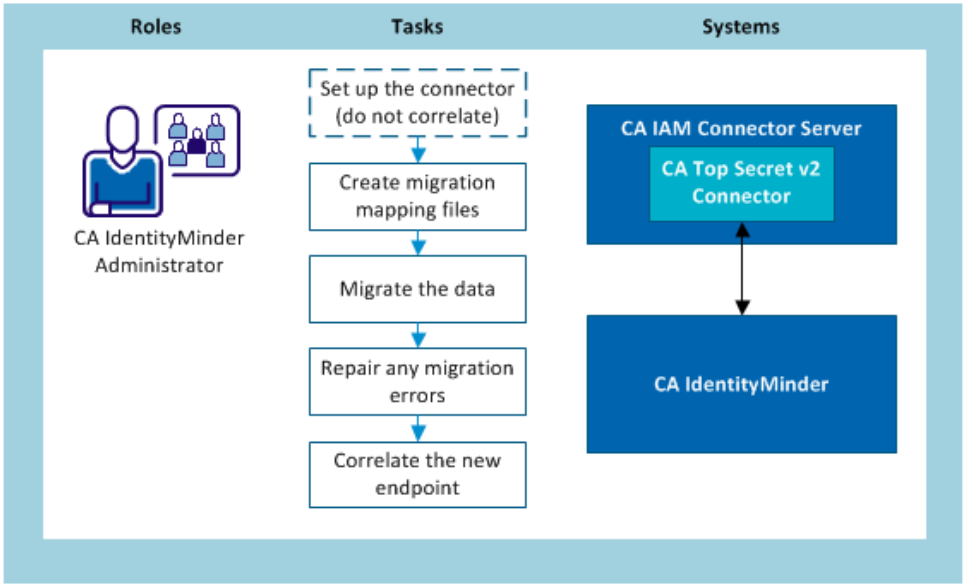
The migration tool migrates data from the CA Top Secret plug-in connector. It cannot migrate from the TSS TSSCFILE connector or from the CA GovernanceMinder import connector.

The migration tool migrates the following data:

- Account templates

  The migrated account templates have the same name as the old account templates.
- Associations between account templates and endpoints, roles, and accounts

You cannot use the migration tool to migrate endpoint objects. Before you can migrate other data, acquire and explore the endpoints with the new connector.



1. After migrating the data, set up the connector without correlating, using the steps in How to Connect to CA Top Secret v2 (see page 121).
2. Create two migration mapping files (see page 89).
3. Migrate the data (see page 132)
4. Repair migration errors (see page 134).
5. Correlate the data (see page 92).

Create Two Migration Mapping Files

The migration tool works with two mapping files:

- (Required) A file that specifies which old endpoints are migrated to which new endpoints.

  The endpoint mapping file uses the following format:

  ```
  OldEndpointName=NewEndpointName
  ```

- (Optional) A file that specifies any custom attributes that you plan to manage.

  The custom attribute mapping file uses the following format:

  ```
  from-custom-attribute=to-endpoint-attribute
  ```

  The mapping file has the same format and contents as the schema_map.txt used in Provisioning Manager and Provisioning Server. You can use schema.txt as the mapping configuration file for the migration.

Follow these steps:

1. Set up any custom attributes in the new endpoint in Identity Management.
2. Prepare the endpoint mapping file. Only the old endpoints that are specified in this mapping file are migrated.

   When you run the mapping tool, use the *–c* option to specify the path to the mapping file.
3. Prepare the mapping file for any custom attributes, if necessary.

   When you run the mapping tool, use the *–m* option to specify the path to the mapping file.

Example: Endpoint mapping file

In the example below, the administrator chooses to keep the endpoint name the same:

```
MFTSS.org.com=MFTSS.org.com
```

Example: Custom attribute mapping file

```
CustomAttribute001=VSE-IES-Dflt-Usercat
CustomAttribute002=VSE-IES-Fld1
```

Migrate the Data

Before you migrate your data, we recommend that you run a simulation first. Simulation generates an HTML report that lists the following items:

- Objects and associations that are created
- Potential migration failures

You can then use the same migration tool to run the real migration.

Follow these steps:

1. Open a command prompt and navigate to the following location:

   cs_home/bin

2. To run a simulated migration, use the tssv2migrate command with the *-r S* option. For example:

   ```
   TSSv2Migrate -h mycomputer -d im –p 20390 –u admin –c
   c:\endpointconfig.txt –m c:\schema_map.txt –r S
   ```

3. To migrate the data, use the tssv2migrate command with the *-r R* option. For example:

   ```
   TSSv2Migrate -h server32 -d im -p 20389  -u etaadmin -n -r R -c
   tss_endpoints.properties –l logging.properties
   ```

   The tool migrates the data and saves a report in *cs_home*/jcs/resources/tss.

4. Verify the new account templates and associations.

tssv2migrate—Migrate Data from Old Plugin Connector to New Connector

The migration tool converts data from the old plug-in connector to the new CA Top Secret v2 connector.

Note: You cannot migrate the *endpoint* using the migration tool. Before you can migrate the data, configure the endpoint in Identity Management.

```
TSSv2Migrate <options>
```

-c *path*

Specifies the file that lists which endpoints have their data that migrated. For more information, read Create Two Migration Mapping Files (see page 89).

-d *domain*

Identifies the Identity Management domain that contains the endpoints that you want to migrate. Default: *im*.

-h *hostname*

Specifies the computer that hosts Provisioning Server.

-l *path*

Specifies the logging configuration file. If you omit this option, the migration tool uses the default available logging configuration from the following path: *java_home*/lib/logging.properties.

For more information, read Configure the Migration Log File (see page 93).

-m *path*

Specifies the file that contains mappings for custom attributes in CA Top Secret. For more information, read Create Two Migration Mapping Files (see page 89).

-n

Disable TLS communication. Default: TLS is enabled.

-p *port*

Defines the port number of the Provisioning Server. Default for no TLS: *20389*. Default for TLS: *20390*.

-r S

Produces a report that lists the objects and associations that would have been migrated.

-r R

Migrates data and produces a report that lists the objects and associations that would have been migrated, plus any failures.

-u *username*

Identifies the administrative user of the Identity Management domain.

Repair Migration Errors

After the migration has finished, verify the outcome carefully. If the result of the migration is not correct, delete the new data and start again.

Follow these steps:

1. Delete the new endpoints that are specified in the endpoint mapping file.

   Deletes all associated account objects in Identity Management without affecting data on the endpoint itself. This step also removes all associations between global users and accounts.

2. Delete the new account templates.

   Removes all associations with the account templates.

You are ready to migrate again.

Correlate the Data

If you migrated data from old endpoints, you first explored the data but you did not correlate the data. After the migration is complete, correlate the data.

To correlate the data, follow the instructions in the Identity Management Administration Guide. Search for these steps in *Integrate the Managed Endpoint in Identity Management*, in the Identity Management bookshelf.

For now, include the options for the correlation. The following steps list the actions to perform:

Follow these steps:

1. Create correlation rules.
2. Edit the explore and correlate definition.

   For now, select the correlation checkbox.

3. Explore and correlate the endpoint.

   For now, the data is both explored and correlated.

The endpoint is ready for use in Identity Management.

Troubleshooting

Configure the Migration Log File

This topic applies to all of the mainframe connectors.

The migration tool uses java.util.logging. When you run the tool, you can use the *-l* option to specify the configuration file for the logging system. This file configures the type and format of the information that is logged and the location of log files.

For example, you can configure any of the following log levels:

- Log errors only.
- Log everything, including debugging info.
- Make the timestamps include dates and times down to seconds.
- Make the timestamps include dates only.
- Send the logs to the console.
- Send the logs to a file.

If you do not want to change the default logging configuration, omit the *-l* option.

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 Identity Management or CA CloudMinder 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 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 Identity Management or CA CloudMinder 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.

Cannot Set the Administer MLS Attribute on an Account

This section applies to the plugin CA Top Secret connector.

Symptom:

My CA Top Secret endpoint has CA LDAP Server for z/OS r12. When I attempt to set the *Administer MLS* attribute on an account, I see the following message:

```
[LDAP: error code 17 – ettsssm5-mlsadmin: attribute type undefined]
```

Solution:

This error appears because eTTSSM5-MLSADMIN is supported only in CA LDAP Server for z/OS r14+.

You can avoid this problem in the following ways:

- Upgrade to a later version of CA LDAP Server.
- Update the problem attribute, using Connector Xpress. Change the value of the *Connector Map To for the Administer MLS* attribute from eTTSSM5-MLSADMIN to eTTSSAdminMisc5.

  The attribute lets you set the “Administer MLS” privilege with its value as write only.

IBM 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 Identity Management
- 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 (see page 138).

Set Up License Files for the DB2 for z/OS Connector

The DB2 for z/OS connector uses JDBC, and it requires a license file to connect to the DB2 endpoint. The license file is available only if you already have a license for DB2 Connect.

For information, see the following IBM technotes:

- IBM technote: Location of the db2jcc_license_cisuz.jar file
- IBM technote: DB2 JDBC driver is not licensed for connectivity

Follow these steps:

1. Install or upgrade CA IAM CS.

   The installation registers CA IAM CS with the provisioning server, creates the DBZ endpoint type, and populates it with its associated metadata.

2. Find *db2jcc_license_cisuz.jar*, which is in the following location on the DB2 Connect activation CD:

   `/db2/license`

3. Copy the license file to the following location on the CA IAM CS computer:

   `cs_home``/jcs/resources/jdbc`

4. Run the *jdbc_db2_zos* script in the same location.

   This script creates a bundle that contains the license file, which you deploy using CA IAM CS.

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:

   Note: You can deploy the OSGI bundle from the connector server GUI or copy the jar files to ca-home/jcs/data/bundles/restore. Then restart the connector server and wait up to ten minutes for it to load.

   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 select Refresh Imports from the popup menu.

CA IAM CS can now connect to DB2 endpoints.

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 Identity Management.

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, Identity Management 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 Identity Management 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 Identity Management based on the explore and correlate definition you created.

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.

Chapter 9: 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.

Google Apps Connector guide describes how to install, configure, and manage the Google Apps Connector for Google Apps endpoints.

This guide is for the following people:

- Identity Management administrators
- CA GovernanceMinder administrators
- CA CloudMinder tenant administrators

Configure Google Apps Provisioning API Access

To manage a Google Apps endpoint with Identity Management, log in to the Google Apps Control Panel and enable the provisioning API in your Google Apps settings.

Identity Management 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 Identity Management, configure the minimum and maximum length for passwords in Google Apps and in Identity Management so they match.

Note: For more information, see Password Policies in the Ide*ntity Management 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 Identity Management 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 Identity Management 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 Identity Management, 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 Identity Management.

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, Identity Management 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 Identity Management 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 Identity Management based on the explore and correlate definition you created.

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.

DB2 UDB Users

In Identity Management DB2 UDB Users give users access to the resources on an endpoint. Identity Management 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

Identity Management 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.

IBM RACF v2 Connector

The following sections describe how to use the RACF v2 connector.

Introduction

This guide describes how to use the following connectors to connect CA IAM CS with IBM RACF (RACF) endpoints:

- RACF v2 Connector for Identity Management and CA CloudMinder (see page 155)

  RACF v2 is a Java connector that is installed with the CA IAM Connector Server (CA IAM CS). Identity Management and CA CloudMinder can use this connector to gather data and provision users in a RACF endpoint.

- IRRDBU00 Connector for CA GovernanceMinder

  The IRRDBU00 connector is a dump file Java connector which is installed with the CA IAM CS. The IRRDBU00 utility extracts information from the RACF system to a security file. CA GovernanceMinder can then read endpoint information from that file.

- RACF Connector with Identity Management, CA CloudMinder, and CA GovernanceMinder

  The RACF connector is a plug-in component of the Identity Management Provisioning Server. CA GovernanceMinder can access the endpoint through its Identity Management connector.

  Note: The RACF connector is replaced by the RACF v2 connector. New deployments should use the RACF v2 connector.

Audience

This guide targets the following people:

- Identity Management administrators responsible for connecting endpoints to Identity Management
- CA CloudMinder administrators responsible for connecting endpoints to CA CloudMinder
- CA GovernanceMinder integrators responsible for integrating CA GovernanceMinder with other products
- The mainframe security administrator responsible for the endpoint.

Supported Systems

To see a list of supported systems, use the Platform Support Matrix:

- Platform Support Matrix for Identity Management
- Platform Support Matrix for CA GovernanceMinder

To verify which endpoint versions are supported, see the table "Supported Connector Endpoint Types" in the Platform Support Matrix. This table also lists the version of CA LDAP Server that the mainframe requires.

To verify which operating systems CA IAM CS can run on, see the table "Supported Connector Servers" in Platform Support Matrix.

To see a list of attributes that CA IAM CS handles, see the attribute list on the Download page for Endpoint Guides for Identity Management.

RACF v2 and Identity Management

The RACF v2 connector can create, read, update, and delete accounts.

This table lists the tasks that the connector lets applications do:

Task	Identity Management
Create, read, update, and delete an user on the RACF endpoint	Yes
Assign and unassign groups to user	Yes
Map custom attributes	Yes

File Locations

This document refers to the installation location of CA IAM CS as *cs_install*. By default, *cs_install* is in the following locations:

- **Windows:** C:\Program Files (86)\CA\Identity Manager\Connector Server
- **Linux and Solaris:** /opt/CA/IdentityManager/ConnectorServer

The Provisioning Server installation location is referred 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/

For the migration process, the tool uses the default logging configuration path that is specified in *java_home*/lib/logging.properties.

Feature Comparison of RACF and RACF v2 Connectors

The table in Compare Three Methods for Connecting to RACF Endpoints shows three connectors. The following table contrasts only the connectors that are available in Identity Management.

The RACF connector is hosted by the Provisioning Server as a server plug-in. The new connector (RACF v2) is hosted by CA IAM CS.

The differences are important if you currently use the old connector and you plan to migrate to the new connector. Use this table to check whether you want to upgrade.

Feature	RACF Connector (Plugin for Provisioning Server)	RACF v2 Connector (New Java connector with CA IAM CS)
Explore & Correlate Explore and Correlate is used by the connector to discover objects in the endpoint.	Yes	Yes
Provisioning Manager Provisioning Manager is the legacy client of Identity Management. It provides limited access to the functionalitiy in the RACF v2 connector.	Yes	No
Fetch Suffix List "Get Suffixes" feature is not available in RACF v2 connector. Alternatively, when you enter the attributes and submit, an error message is displayed. The error message displays a list of available suffixes at the endpoint.	Yes	On Error
Use Logged on Administrator Credentials Legacy mainframe connectors can use logged-in user (Global User) credential to access the endpoint. RACF v2 connector uses the endpoint administrator's login credentials to access the endpoint.	Yes	No
SSL All communication between the Client and the CA LDAP Server for z/OS can be encrypted using SSL (Secure Socket Layers).	Yes	No
Display System Options The System Options tab in the Provisioning Manager Endpoint screen displays endpoint specific information such as version. For supported v2 connectors, endpoint information is available on the endpoint screen of the Identity Management User Console.	Yes	No
Account Create, Read, Update, and Delete	Yes	Yes
Assign Group to Account	Yes	Yes

Feature	RACF Connector (Plugin for Provisioning Server)	RACF v2 Connector (New Java connector with CA IAM CS)
Group Create, Read, Update, and Delete	Yes, in Provisioning Manager only	No
Account Custom Attributes	Yes	Yes
Reverse Sync Reverse sync is a process that allows users to take actions on endpoint accounts discovered by the explore & correlate process based on set of defined policies.	Yes	Yes
Multithreading An execution model that provide higher processing efficiency.	No	Yes
Password Options On the Provisioning Manager Endpoint screen, the Password Options tab displays endpoint password related information. A similar tab is available in the User Console endpoint screen. It is available if the relevant mainframe 'v2' connector supports this feature.	No	No
Password Synch Agent Password Synch Agent is installed at the endpoint. When the Global user is enabled for the password synchronization agent (Available at the Provisioning Manager Global user screen, Password tab), the password change at the endpoint, using the native tool, can be propagated back to the Global User and to the other endpoint accounts of the same Global User.	No	No
Import from Identity Management 12.6.2 to CA GovernanceMinder 12.5 SP8, 12.6 SP1 The connector marks a set of objects and attributes as 'Interesting to compliance' for the CA GovernanceMinder. CA GovernanceMinder (RCM) connects to Identity Management and extracts Users, Account Templates, Provisioning Roles and Resources.	Yes	No
Export from CA GovernanceMinder 12.5 SP8, 12.6 SP1 to Identity Management 12.6.2 CA GovernanceMinder can modify associations on the imported data set. These changes can be pushed to the endpoint through Identity Management. This process is called an export.	Yes	No

Chapter 10: Security

Privileges Required to Connect to RACF

To connect to a RACF endpoint, the Identity Management administrator must have access to Time Sharing Option (TSO) to generate and issue commands for CA LDAP Server.

Securing Communication between RACF and CA IAM CS

Identity Management can send passwords and other security information across the network.

When you do not set up SSL communication, these details are sent without encryption, creating a security risk.

We recommend that you use SSL to secure the connection between RACF and CA IAM CS, using the steps in Install CA LDAP and Configure It for SSL (see page 83) and Import the CA LDAP Server Certificate into the CA IAM CS Keystore (see page 85).

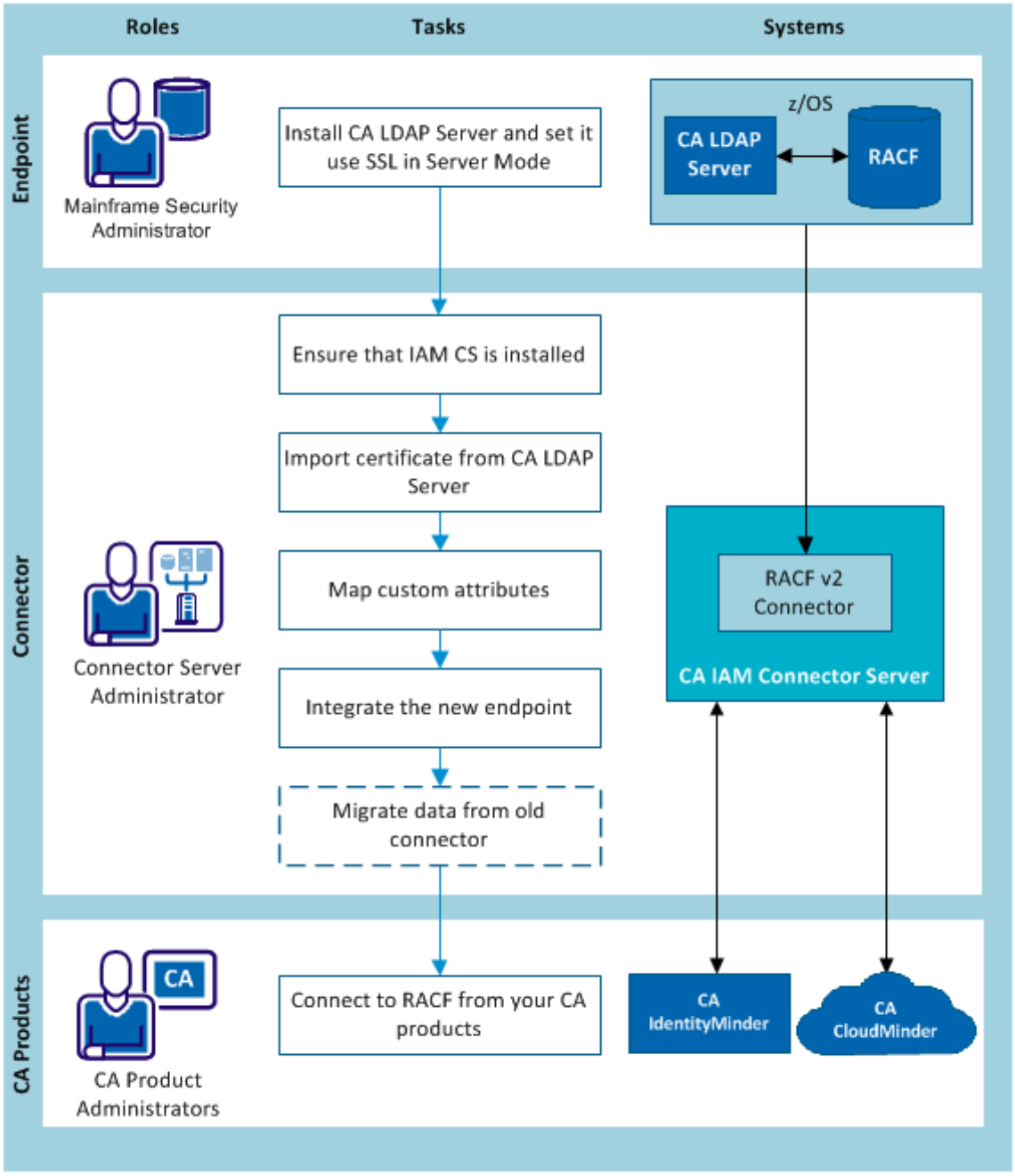
RACF v2 Connector

RACF v2 is a Java connector that is installed with the CA IAM CS. This chapter describes how to connect to a RACF v2 connector. You can use the RACF v2 connector to allow the following products to connect to a RACF endpoint:

- Identity Management
- CA CloudMinder

In Identity Management, if you are replacing the RACF connector with the RACF v2 connector, use the migration tool to migrate account templates and their associations to objects in the RACF v2 connector. For more information, see Appendix A: How to Migrate Data from the Plug-in Connector (see page 161) section in this guide.

The following diagram shows the tasks that are required to connect to the endpoint, and who does each task.



1. A mainframe security administrator installs CA LDAP Server on the mainframe, then sets it to use SSL in Server Mode (see page 157).
2. The connector server administrator does the following steps:
   a. (If necessary) Install CA IAM CS. For details, search for *Install CA IAM CS* in the Identity Management bookshelf.
   b. (If necessary) Import the CA LDAP Server certificate into the CA IAM CS keystore (see page 85).
   c. (If necessary) Map custom attributes (see page 159).
   d. Integrate the managed endpoints in Identity Management.
   e. For CA CloudMinder, configure the cloud-based CA IAM CS for setting up CA IAM CS on the cloud.
   f. If necessary, the Identity Management administrator migrates data from a RACF endpoint that used the old plug-in connector. This is described in How to Migrate Data (see page 161).
3. The CA product administrators connect to the endpoint in Identity Management or CA CloudMinder.

Install CA LDAP

This procedure is for the mainframe security administrator.

To allow CA IAM CS to communicate with RACF, install CA LDAP Server on the mainframe. To keep your data secure, configure CA LDAP Server to use SSL.

1. Install CA LDAP Server. Use the following links to see instructions:
   - Install CA LDAP Server r15
   - Install CA LDAP Server r14
2. Configure CA LDAP Server to use SSL in Server mode. These instructions apply to both r15 and r14.

Ensure that CA IAM CS Is Installed

Check that CA IAM CS is installed and running.

CA IAM CS is installed with the following products, unless you deselected the CA IAM CS option:

- **Identity Management r12.6.2 and later**—For details, search for *Install CA IAM CS* in the Identity Management bookshelf.
- **CA GovernanceMinder r12.6 and later**—For details, search for *Connectivity Use Cases* in the CA GovernanceMinder bookshelf.
- **CA CloudMinder 1.1 and later**—Check that CA IAM CS is installed both in the CA CloudMinder cloud and on-premise:
  - CA IAM CS is installed in the CA CloudMinder cloud by the hosting administrator. For details, search for *Provisioning Server and CA IAM Connector Server* in the CA CloudMinder for Service Providers bookshelf.
  - CA CloudMinder also requires an on-premise installation of CA IAM CS for each tenant. For details, search for *How to Set Up On-Premise Provisioning* in the CA CloudMinder for Tenant Administrator bookshelf.

Import the CA LDAP Server Certificate into the CA IAM CS Keystore

This procedure is for the Identity Management and CA CloudMinder administrator. If CA IAM CS already has the CA LDAP Server certificate, ignore this procedure.

After the mainframe security administrator has confirmed that CA LDAP Server is configured to use SSL, you can import the CA LDAP Server certificate into the CA IAM CS keystore.

Follow these steps:

1. Identify the certificate which you want to import into the CA IAM CS keystore as a trusted certificate:
   - The CA LDAP Server certificate.
   - The root certificate of the certificate authority that has issued the CA LDAP Server certificate, and the application server certificate
2. Import the chosen certificates:
   a. Log in to CA IAM CS (see page 21).
   b. At the top, click the Certificates tab.

      The Certificates 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.
   c. To add a certificate, click Add, then enter the details of the certificate:
      - **Certificate**—Enter the path to the certificate file
      - **Alias**—Enter an alias for storing the certificate

Map Custom Attributes for Identity Management

This procedure is for the CA CloudMinder or Identity Management administrator.

When you connect to an endpoint, the objects on the endpoint are mapped to objects in CA CloudMinder or Identity Management. This happens automatically. If you want to make custom mappings, use Connector Xpress.

For instructions about setting up custom mapping with Connector Xpress, search for *Managing Accounts and Groups* in the CA CloudMinder bookshelf or in the Identity Management bookshelf.

To see a list of the objects on the endpoint, download the attribute list from this page: Download page for Endpoint Guides.

Any LDAP attribute on the mainframe that has a string representation can be exposed as a custom attribute in the connector. To map custom attributes, use Connector Xpress. For information, search for *Managing Accounts and Groups* in the Identity Management bookshelf or CA CloudMinder bookshelf.

Integrate the Managed Endpoint in Identity Management

For the details about the following steps, search for the following topics based on the CA product:

- For CA CloudMinder and Identity Management 12.6 releases, search for *Integrating the Endpoint* in the CA CloudMinder bookshelf or search for *Integrating Managed Endpoints* in the Identity Management bookshelf.
- For CA Identity Manager 12.5 releases, search for *Managed Endpoint Accounts* in the CA Identity Manager bookshelf.

Follow these steps:

1. Navigate to the connectors download page, then open the attribute list for this endpoint type.

   This HTML page lists every endpoint attribute that the connector works with. Use this information in the following steps.

2. Set up the connector:

   a. Import the role definition file.

   b. (CA CloudMinder only) Create a role to manage the endpoint.

   c. Create correlation rules. Skip this step if you plan to migrate data.

   d. (CA CloudMinder only) Configure email notification for the endpoint.

3. Add the endpoint to the environment. In the Endpoint tab, complete the following mandatory fields:

   Endpoint Name

   Specifies the name of the new CA Top Secret endpoint. The endpoint name is the name that appears in the Provisioning Manager. Commas and semi-colons are not allowed.

   Mainframe LDAP IP Address/Machine Name

   Specifies the mainframe LDAP IP Address or machine name of the CA Top Secret.

   Mainframe LDAP Port

   Specifies the Listen Port for the Security Integrator running on the CA Top Secret.

   Use Server-Side SSL

   When checked, specifies that the server's SSL is used.

   Note: Ensure that you have imported the SSL certificate to Provisioning Server (see page 85).

Mainframe LDAP DN Suffix

Specifies valid suffixes that are configured for the current 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.)

Proxy Admin ID

Allows you to specify an ID that is used to issue the password modifications that are requested through the workflow. This provides users with the ability to change or reset their passwords if their password has expired and they cannot be authenticated to the system.

Proxy Admin Password

The password to the Proxy Admin ID on the CA Top Secret endpoint.

When you complete the fields on the Endpoint tab, use the information in the Endpoint section of the attribute list. You can find the details on the Download page.

4. Create an explore and correlate definition. Do not include the correlation if you plan to migrate data.

   Important! If you plan to migrate data from the plug-in connector, explore but **do not correlate**. Correlation of the new endpoint can introduce new associations that conflict with the correlation rules of the old endpoint.

5. Explore and correlate the endpoint.

   Note: If your explore-and-correlate definition does not include correlation, this step explores only.

How to Migrate Data from the Plug-in Connector to the New Java Connector

This section applies to Identity Management only.

CA IAM CS comes with a tool that helps you migrate account templates and their associations to objects of the new connector. If Identity Management already manages RACF endpoints using the plugin connector, you can use the existing RACF data with the new connector.

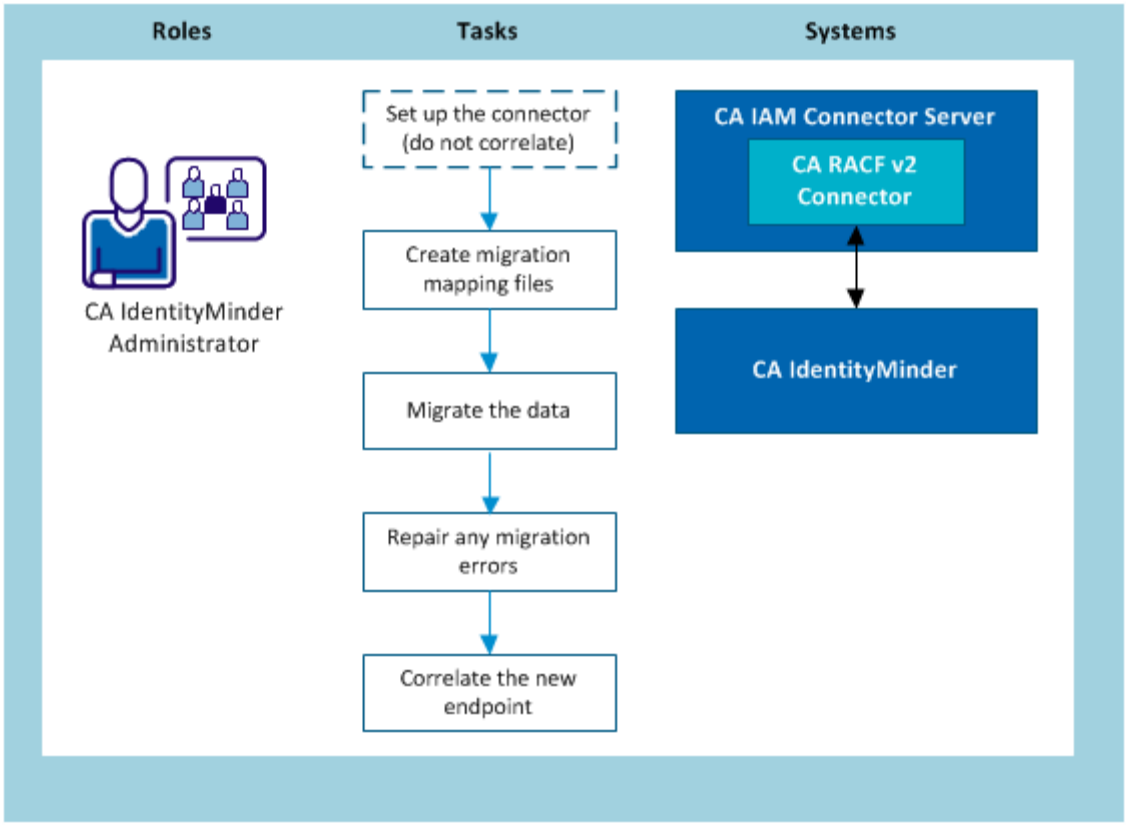
This tool migrates the following data:

- Account templates

  The migrated account templates have the same name as the old account templates.

- Associations between account templates and endpoints, roles, and accounts

You cannot use this tool to migrate endpoint objects. Before you can migrate other data, acquire and explore the endpoints with the new connector.



1. Before you migrate data, set up the connector without correlating, using the steps in How to Connect to RACF (see page 155).
2. Create two migration mapping files (see page 89).
3. Migrate the data (see page 164)
4. Repair migration errors (see page 166)
5. Correlate the data (see page 92).

Create Two Migration Mapping Files

The migration tool works with two mapping files:

- (Required) A file that specifies which old endpoints are migrated to which new endpoints.

  The endpoint mapping file uses the following format:

  ```
  OldEndpointName=NewEndpointName
  ```

- (Optional) A file that specifies any custom attributes that you plan to manage.

  The custom attribute mapping file uses the following format:

  ```
  from-custom-attribute=to-endpoint-attribute
  ```

  The mapping file has the same format and contents as the schema_map.txt used in Provisioning Manager and Provisioning Server. You can use schema.txt as the mapping configuration file for the migration.

Follow these steps:

1. Set up any custom attributes in the new endpoint in Identity Management.
2. Prepare the endpoint mapping file. Only the old endpoints that are specified in this mapping file are migrated.

   When you run the mapping tool, use the *–c* option to specify the path to the mapping file.
3. Prepare the mapping file for any custom attributes, if necessary.

   When you run the mapping tool, use the *–m* option to specify the path to the mapping file.

Example: Endpoint mapping file

In the example below, the administrator chooses to keep the endpoint name the same:

```
MFTSS.org.com=MFTSS.org.com
```

Example: Custom attribute mapping file

```
CustomAttribute001=VSE-IES-Dflt-Usercat
CustomAttribute002=VSE-IES-Fld1
```

Run a Migration Report

Before you migrate your data, we recommend that you run a simulation first. This generates an HTML report that lists the following items:

- Objects and inclusions that are created
- Potential migration failures

You can then use the same migration tool to run the real migration.

Follow these steps:

1. Open a command prompt and navigate to this location:

   cs_home/bin/RACFv2Migrate

2. To run a simulated migration, use the racfv2migrate command with the *-r S* option. For example:

   ```
   RACFv2Migrate -h mycomputer -d im –p 20390 –u admin –c
   c:\endpointconfig.txt –m c:\schema_map.txt –r S
   ```

3. To migrate the data, use the racfv2migrate command with the *-r R* option. For example:

   ```
   RACFv2Migrate -h server32 -d im -p 20389  -u etaadmin -n -r R -c
   tss_endpoints.properties –l logging.properties
   ```

   The tool migrates the data and saves a report in *cs_home*/jcs/resources/racfv2.

4. Verify the new account templates and associations.

Migrate Configuration and Data from Old Connector to New

The migration tool converts data from the old plugin connector to the new RACF v2 connector.

Note: You cannot migrate the *endpoint* using this tool. Before you can migrate the data, configure the endpoint in Identity Management.

`RACFv2Migrate <options>`

-h *hostname*

Specifies the computer that hosts IMPS.

-d *domain*

Identifies the Identity Management domain that contains the endpoints that you want to migrate. Default: im

-p *port*

Defines the port number of IMPS. Default: 20391.

-u *username*

Identifies the administrative user of the Identity Management domain.

-r S

Produces a report that lists the objects and inclusions that would have been migrated.

-r R

Migrates data and produces a report that lists the objects and associations that would have been migrated, plus any failures.

-m *path*

Specifies the file that contains mappings for custom attributes in RACF.

One of the pre-requisites of the migration tool is the administrator has to migrate the custom attributes to the new namespace manually before running the tool. The tool has no knowledge of the custom attributes added to the new namespace, hence the user is also responsible to create a mapping file and supply the location of the file when running the tool.

The mapping file should contain the from-custom-attribute=to-endpoint-attribute information, for example:

```
eTRACCustomAttribute001=eTRACAddressLine1
eTRACCustomAttribute002=eTRACAddressLine2
```

Note that the contents and format are the same as that used in schema_map.txt, and that file can be used as is as the mapping configuration file for migration.

-c *path*

Specifies the file that lists which endpoints have their data migrated. For more information, read Create Two Migration Mapping Files. (see page 89)

-l *path*

Specifies the logging configuration file. If this is omitted, the migration tool uses the default logging configuration specified in <JAVA_HOME>/lib/logging.properties. For more information, read Configure the Migration Log File (see page 93).

Repair Migration Errors

After the migration has finished, check the outcome carefully. If the result of the migration is not correct, delete the new data and start again.

Follow these steps:

1. Delete the new endpoints specified in the endpoint mapping file.

   This step deletes all associated account objects in Identity Management without affecting data on the endpoint itself. This step also removes all associations between global users and accounts.

2. Delete the new account templates.

   This step removes all associations with the account templates.

You are now ready to migrate again.

Correlate the Data

If you migrated data from old endpoints, you first explored the data but you did not correlate the data. After the migration is complete, correlate the data.

To correlate the data, follow the instructions in the Identity Management Administration Guide. Search for these steps in *Integrate the Managed Endpoint in Identity Management*, in the Identity Management bookshelf.

For now, include the options for the correlation. The following steps list the actions to perform:

Follow these steps:

1. Create correlation rules.
2. Edit the explore and correlate definition.

   For now, select the correlation checkbox.

3. Explore and correlate the endpoint.

   For now, the data is both explored and correlated.

The endpoint is ready for use in Identity Management.

Troubleshooting

Configure the Migration Log File

This topic applies to all of the mainframe connectors.

The migration tool uses java.util.logging. When you run the tool, you can use the *-l* option to specify the configuration file for the logging system. This file configures the type and format of the information that is logged and the location of log files.

For example, you can configure any of the following log levels:

- Log errors only.
- Log everything, including debugging info.
- Make the timestamps include dates and times down to seconds.
- Make the timestamps include dates only.
- Send the logs to the console.
- Send the logs to a file.

If you do not want to change the default logging configuration, omit the *-l* option.

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 Identity Management or CA CloudMinder 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 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 Identity Management or CA CloudMinder 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.

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 171)
- Password Policy Naming Conventions (see page 171)
- Password Limitations (see page 171)

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).

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:

- Kerberos authentication (see page 175)
- SSH authentication

Install and Deploy the Connector

The Kerebros connector is installed automatically when you install the CA IAM CS. However, there is some additional configuration to complete before you use the connector.

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 178)
- CA IAM CS principal and a custom keytab (see page 179)
- A principal other than CA IAM CS host principal and the default keytab (see page 180)
- A principal other than CA IAM CS host principal and a custom keytab (see page 182)
- Principal and password authentication (see page 183)

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 computer 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. Ensure that the SSH server is a member of the realm.
2. 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.
3. Modify the logging and appdefaults sections in the /etc/krb5/krb5.conf file as required.
4. 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`*

5. Set up authentication to use one of the following:
   - CA IAM CS host principal (see page 178)
   - CA IAM CS host principal and a custom keytab (see page 179)
   - A principal other than CA IAM CS host principal and the default keytab (see page 180)
   - A principal other than CA IAM CS host principal and a custom keytab (see page 182)
   - Principal and password authentication (see page 183)

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 178)
- If the default keytab file does not exist, create a new keytab file. (see page 179)

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.

Acquire a Kerberos Machine Using the User Console

You must acquire the Kerberos machine before you can administer it with Identity Management.

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, Identity Management 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 Identity Management 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 Identity Management based on the explore and correlate definition you created.

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.

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.

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
-ticket lives	Connector specified defaults
-flags	Default Kerberos flags
-password policy	None

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.

Known Issues

This section contain the following topics:

Account Creation Fails with Invalid Date Specification (see page 187)

Account Creation Fails with Parameter is Incorrect (see page 187)

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.

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.

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 189).
4. Add encryption keys to the server ID (see page 190).
5. Configure remote access to the Domino Server (see page 191).
6. Sign the agents used by the connector (see page 192).
7. Enable SSL between Lotus Domino and CA IAM CS (see page 193).
8. Add NCSO.jar to the Lotus Domino connector (see page 194).

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.

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.

To allow the connector to access the Lotus Domino endpoints, 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 Identity Management 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:

   Note: You can deploy the OSGI bundle from the connector server GUI or copy the jar files to ca-home/jcs/data/bundles/restore. Then restart the connector server and wait up to ten minutes for it to load.

   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 select Refresh Imports from the popup menu.

The Lotus Domino connector can now use NCSO.jar.

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 Identity Management.

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, Identity Management 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 Identity Management 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 Identity Management based on the explore and correlate definition you created.

Managed Objects

Identity Management 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 Identity Management. 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. **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. **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 Identity Management 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. 2. Specify the absolute path (on the LND server) and filename as follows: ■ Windows: C:\Program Files\Lotus\Domino\data\user.id ■ 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. 2. Enter the full UNC path, including the drive as follows: \\server\c$\share\user.id Do not omit the c$.
Certifier ID	On LND Server	1. Select the Specify a Location for the Certifier ID check box on the Organization Certifiers tab. 2. Specify the absolute path (on the LND server) and filename as follows: ■ Windows: C:\Program Files\Lotus\Domino\data\certifier.id ■ Unix: /local/notedata/certifier.id
	On separate system	1. Select the User ID File Path check box on the UserID tab. 2. Enter the full UNC path, including the drive as follows: \\server\c$\share\certifier.id Do not omit the c$.

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’.

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.

Identity Management 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 Identity Management, 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 Identity Management 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.

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 Identity Management 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, Identity Management cannot create the new user.

To allow Identity Management 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.

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 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.

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 Identity Management, 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 Identity Management, 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 Identity Management 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>
```

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 Identity Management 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 Identity Management.

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 Identity Management

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 Identity Management 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 Identity Management 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\Identity Management\Provisioning Server\bin
```

Note: ADSLDAPDiag should be run on the same machine as the C++ Connector Server. If ADSLDAPDiag fails, this indicates that the Identity Management-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.

Using Failover

IMPORTANT! By default, ADS failover is disabled. Before you enable failover, review the following list carefully to prevent unexpected behavior.

- If you wish to activate Failover, you must set the environment variable ADS_FAILOVER to 1on the system where the C++ Connector Server and ADS connector run.
- The server name that you specify in the connector server user interface should match the fully qualified DNS server name.
- Enable logging.
- 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 Identity Management 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 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 Identity Management 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 Identity Management 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 Identity Management. 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, Identity Management 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.
- When you change the order of the controllers, 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 sequence, 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.

Identity Management 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 Identity Management. For example, a hypothetical AD forest has three domains, D1, D2 and D3. You have two Identity Management-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 Identity Management-managed domains (D1 and D2). If you choose to have the new global catalog search feature only deal with Identity Management-managed domains, then Identity Management 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 Identity Management-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 Identity Management).

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 Identity Management or not).
- 1 - Deal with groups in Identity Management-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 Identity Management 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 Identity Management 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.
- Identity Management assumes that these extensions are in effect for the entire enterprise.

Once the extended ADS schema has been configured in Identity Management, 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.

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 Identity Management.

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, Identity Management 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 Identity Management 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 Identity Management based on the explore and correlate definition you created.

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 Identity Management 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.

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>'
```

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.

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.

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.

Follow these steps:

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 CCS.

Incomplete or Truncated Search Results When Searching for or Importing more than 20000 Users in Identity Management or RCM

Symptom:

When I search for more than 20000 users in Identity Management, 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

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 Identity Management, 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.

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 Identity Management. 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 Identity Management 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.

For Exchange 2010, specify the Mail Server in all mailbox-enabled account templates in the User Console. You cannot make this change in the Provisioning Manager.

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.

Configuring the Exchange Remote Agent

Step 1. Configure the CAM and CAFT Service

You must configure CAFTHOST to recognize the C++ Connector Server and the Identity Management 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/Identity Management/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. Identity Management 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'
```

Exchange 2010

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)	Organization Administrators
All other Exchange Tasks (Not required if a member of Exchange Organization Administrator)	Discovery Management

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

Identity Management 1.5 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 Identity Management 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 Remote Agent for Exchange

The CAM and CAFT Service is a Windows service. You can control this process using the Services dialog on your Control Panel. The CAM and CAFT Service is called CA Message Queuing Server.

Note: The CAM and CAFT Service allows encryption using certificates.

View the Remote Agent Process

Follow these 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 Identity Management 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 Identity Management can communicate with the Microsoft Exchange Remote Agent.

Managing Exchange Users

The Active Directory connector can manage mailboxes on Active Directory endpoints. Information about these mailboxes is stored in the Active Directory endpoint that is associated with the Microsoft Exchange server. For this reason, you must acquire the Active Directory endpoint before you can manage Microsoft Exchange users.

When you acquire an Active Directory endpoint, the Endpoint Content dialog displays the following containers:

- **Builtin** contains all security groups that are built into Active Directory, such as Administrators and Backup Operators
- **Computers** contains computers that belong to the Active Directory directory
- **Microsoft Exchange System Objects** contains Microsoft Exchange system mailboxes
- **Users** contains all Active Directory accounts and groups, including those with mailboxes

Other organizational containers may appear in this dialog. These containers reflect the structure that exists within the Active Directory directory. For example, an Active Directory 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, Identity Management attempts to read the necessary data. If it fails, Identity Management 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 Identity Management 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 Active Directory, the members of these groups are subject to Active Directory account templates.

If an Active Directory 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, you should add the Active Directory group that represents the Microsoft Exchange distribution list to the account template.

Sometimes you cannot add the distribution lists to the Active Directory account template. 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. Identity Management 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 through etautil or through an LDAP browser such as 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

To manage the Office Communications Server 2007, do the following:

1. Extend the Active Directory schema for Identity Management.
2. Determine the correct ADS common attribute values. (see page 254)

Extend the Active Directory Schema for Office Communications Server

To manage Office Communications Server 2007, extend the Active Directory schema for Identity Management.

Follow these steps:

1. Add the following attributes to the *PS_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 CCS service.
3. Next, determine the correct ADS common attribute values (see page 254).

Note: For more information about extending the schema, see the sections *Extend the ADS Schema* and *Modify the schema.ext File* in the *Identity Management 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.

Follow these steps:

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 Identity Management 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*. Identity Management 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 Office 365 Connector

The following sections describe how to use the Office 365 connector.

Introduction

The Office 365 connector communicates with a Microsoft Office 365 domain in the cloud using PowerShell (installed on-premise) to perform provisioning tasks. The provisioning tasks include:

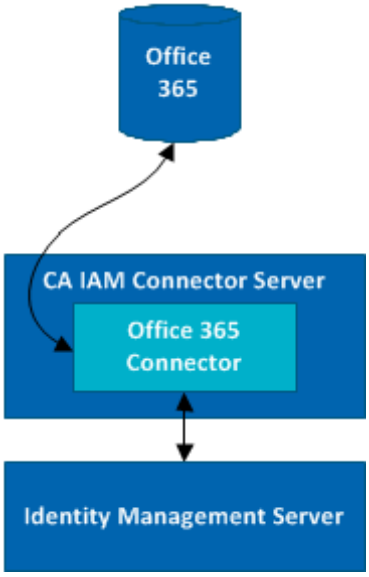
- User account management
- License assignment
- Role assignment
- Group assignment

This guide describes how Identity Management can provision users and manage credentials on Office 365 endpoints.

Office 365 Connector and Identity Management

After you set up a connection between Identity Management and an Office 365 endpoint, you can use Identity Management to do the following tasks:

- Add, lookup, search, modify, and delete Office 365 endpoints
- Add, lookup, search, modify, and delete and explore Office 365 accounts
  - Manage account basic attributes
  - Manage license assignment, include license options granularity
  - Add/remove account as a member of Outlook admin/user role groups
  - Add/remove account as a member/owner of Outlook distribution groups
- Lookup and search license options
- Lookup and search exchange admin/user role groups
- Lookup and search exchange distribution groups.



To check which versions of the endpoint are supported, see the Platform Support Matrix available at CA Technologies Support Online.

Audience

This guide targets the following people:

- The Identity Management administrator responsible for integrating Identity Management with other CA products.
- The administrator responsible for the Office 365 endpoint.

Limitations

The following table lists the limitations of Office 365 connector:

Limitation	Description
Suspension or Deletion	Identity Management keeps an Office 365 account that has been soft-deleted from the domain for 30 days. During this time, an administrator can restore the account, including the Exchange mailbox. The connector treats a soft-deleted account as a suspended account. The account is soft-deleted or restored when the Suspended checkbox is selected or cleared, respectively. You cannot modify account attributes when an account is suspended. If you delete an account via the connector, the account, including the Exchange mailbox is permanently deleted. These accounts cannot be restored. Account suspension and deletion should be exercised with caution as a suspended account will be permanently removed by Office 365 after 30 days and a deleted account will be permanently removed from the domain. The recommended approaches are: ■ Use the Block Credential checkbox to block or unblock user access to the portal. ■ Remove the license option assigned to an account to deny the user access to the service. For example, when the Exchange Online license option is removed from the account, the user will not be able to access the mailbox.

Limitation	Description
Setting Mailbox Attributes	Mailbox attributes are processed only when the mailbox exists. Assign the Exchange Online license option to the account to trigger mailbox creation. Since it takes a while for the Exchange server to create the mailbox, the connector waits until the mailbox is successfully created before setting the mailbox attribute. If the wait exceeds configured limits, the connector reports an error, informing the caller that the mailbox does not exist. You can configure the limits in the connect.xml file: ■ maxHaltExecution – The maximum number of wait period of the connector. ■ haltExecutionTimeMillis – The duration of each wait period in milliseconds. ■ keepConnectionWhileHalting – When true, the connector holds on to the connection during the wait period.
Left-behind PowerShell Processes	If CA IAM CS is forcefully closed, the native PowerShell processes started by the connector continue to run on the machine. These processes are removed when the CA IAM CS starts again. Alternatively, you can end the process manually using Windows Task Manager. The process PIDs are stored in the following path: *cs_home*\jcs\data\o365.
"Partner_Managed" Admin Role Groups	Admin role group that has the "Partner_Managed" capability is a read-only group. You cannot add a member to this group directly. The connector does not return these groups when performing an admin role groups search. For example, these groups are not returned during an explore operation, and therefore, cannot be assigned to an account.
License Options	Once the domain is set up, license options can change. To improve the connector performance, the connector caches license option data when a domain license plan changes. Explore the license options sub-tree again to get the latest license option data.
User Name	User Name of the account does not support non-ASCII characters (foreign characters).
User Password	*Force Change Password* must be set in conjunction with Password field otherwise the value does not apply. Even when *Strong Password Required* is not selected, the account's password must be 8-16 characters.

File Locations

This document refers to the CA IAM CS installation location as *cs_install*. By default, *cs_install* is in the following locations:

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

More Information

To check which versions of the endpoint are supported, see the Platform Support Matrix available at CA Technologies Support Online.

To see the objects and attributes that this connector provides, navigate to the connectors download page, then open the attribute list for this endpoint type.

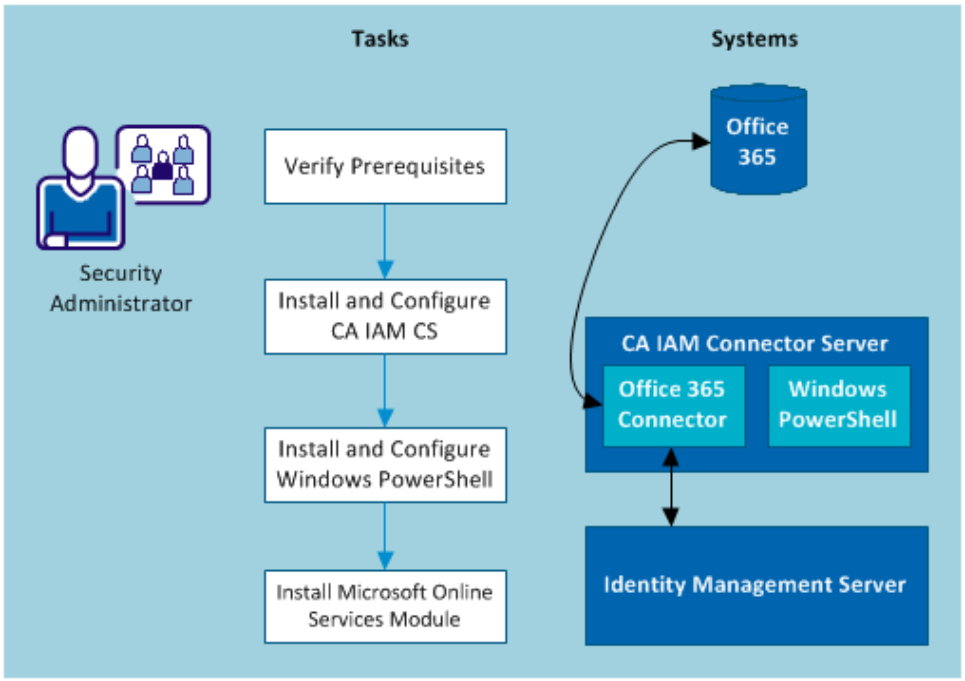
Chapter 11: Security

Privileges Required to Connect to Office 365

The administrator account that is used to acquire the Office 365 endpoint must have the Global Administrator role.

How to Connect Identity Management to Office 365

The following diagram shows the tasks that are required to connect to the endpoint, and who does each task.



- The security administrator does the following steps:
  - Verify prerequisites (see page 264)
  - Install and configure CA IAM CS. (see page 84)
  - Install and configure Windows PowerShell (see page 266)
  - Install Microsoft Online Services Module (see page 267)

Prerequisites for Connecting to Office 365

Before the connector server can be connected to Office 365, the office 365 administrator must verify that the following prerequisites are met:

- Register a domain with Microsoft Office 365.
- Windows PowerShell for Office 365 is installed. In order to make sure the Windows PowerShell for Office 365 is properly set up, perform the following steps:

  1. Connect Windows PowerShell on your local computer to the cloud-based service.
  2. Install the Office 365 cmdlets.

     Note: If you are running Windows 7, re-install the Microsoft Online Services Module in order to ensure that you are using the latest version. This is because some cmdlets are not supported in the earlier version.

     Also make sure that you install the version of JDK or JRE that is compatible with the Microsoft Online Module installed. If you have installed 64-bit module, make sure that you are running on 64-bit JVM.

Install CA IAM CS

When you install CA IAM CS, be sure to record the values you enter. The port name, password, and URL are required in other parts of the process.

Note: This procedure assumes that you do not already have a local instance of CA IAM CS installed. If you have installed it as part of an Identity Management installation, the default username is set to "admin".

Follow these steps:

1. Check the time settings for your on-premise Connector Server host. They must match the setting information that you received from the System Administrator for the two servers to connect successfully.

   Note: The cloud-based and on-premise Connector Server time zones need not match, only the settings. For example, daylight savings time must be enabled on both.

2. Download CA IAM CS from support.ca.com, and launch the installer.
3. Select the C++ connector option you want, depending on your environment.
4. Clear the "Register this installation with a Provisioning Server" checkbox if it is selected. This setting is not required for an on-premise installation.
5. On the Cloud Connector Server screen, enter the following information:
   - Server URL - The URL of the cloud-based CA IAM CS messaging interface, for example: https://*cloudcs_hostname*:22002. The System Administrator provides the URL information.
   - Tenant Name
   - Tenant Host ID - Optional identification for an environment with multiple on-premise server installations.
   - Username - The user name that the System Administrator created for this tenant.
   - Password - The password that the System Administrator created for this tenant.

   Note: To connect to a cloud-based Connector Server, enter details in this step. The details are required for the installer to create a key pair and self-signed certificate. If for some reason you cannot enter details on initial installation, rerun the installer and add details before completing the connection.
6. Enter the admin password on the Connector Server Configuration screen, and accept the default LDAP port values.

   Note: If you install multiple connector servers, be sure to set the same password for each. This practice avoids a password synch issue.
7. On the Port Configuration screen, accept the default values.
8. Enter HTTP Proxy credentials if your environment uses an HTTP proxy.

9. Complete the wizard. You can install multiple connector servers in your environment, depending on your needs.

Install and Configure Windows PowerShell

Set up Windows PowerShell on the on-premise environment where the connector is running. For details, see the following link:

http://help.outlook.com/en-us/140/cc952756.aspx

Follow these steps:

1. Install the latest version of Windows PowerShell in the on-premise environment where the connector is running.
2. Open Windows PowerShell and run the following command:

   ```
   Get-ExecutionPolicy
   ```

   The command specifies the execution policy which is currently in-use.
3. To set the ExecutionPolicy to RemoteSigned, run the following command:

   ```
   Set-ExecutionPolicy RemoteSigned
   ```

   The execution policy is now set to RemoteSigned. This indicates that the downloaded scripts require a trusted publisher to sign before they can be run.
4. Exit the Windows PowerShell.
5. Open command prompt and run the following command:

   ```
   net start winrm
   ```

   Windows Remote Management (winrm) starts.
6. In the command prompt, run the following command:

   ```
   winrm get winrm/config/client/auth
   ```

   Note: If the value returned does not contain *Basic=true*, run the following command:

   ```
   winrm set winrm/config/client/auth @[Basic="true"]
   ```
7. To stop winrm, run the following command:

   ```
   net stop winrm
   ```

Install Windows Azure Active Directory Module for Windows PowerShell

Install Windows Azure Active Directory Module for Windows PowerShell to connect to your local PowerShell session and create your Microsoft Online Office365 Administration session.

Note: Make sure that Microsoft PowerShell is installed before you install this module.

Follow these steps:

1. Check that the module is already installed.

   To do this, open Windows PowerShell and run the following command:

   ```
   Import-Module MsOnline
   ```

   A list of cmdlets appear.

2. If the module MsOnline is not found use the instructions on the following page to install the latest version of the module:

   http://aka.ms/aadposh

3. Repeat Step 1 to check that the module has installed correctly.

Troubleshooting

Error When Creating/Modifying an Office 365 Account

Symptom:

An error that resembles the following messages occurs when I create/modify an Office 365 account and assign one or more attributes of mailbox:

[… Failed to modify account mailbox attributes because account's mailbox does not exist …]

[… Failed to modify account mailbox attributes because account is not licensed …]

Solution:

Mailbox attributes cannot be set without the existence of the account's mailbox. The error might be due to one of the following reasons:

- No Exchange Online license is assigned to the Office 365 account
- The mailbox creation is still in progress
- There is an error on Exchange Online license assignment or the mailbox creation.

In order to rectify the issue, follow one of the steps below:

- Assign the Exchange Online license to the account, if not already assigned.
- Wait until the license option status has changed from *PendingInput* to *Success,* before proceeding to setting up the mailbox attributes
- Contact Microsoft regarding the license assignment or mailbox creation failure.

License Violation When Creating/Modifying an Office 365 Account

Symptom:

Error that resemble the following message occurs when I create/modify an Office 365 account and assign the Office Web Apps license option to the account, without assigning the SharePoint Online license option:

[… Unable to assign this license set because it would cause a license violation …]

Solution:

An Office 365 account is required to have SharePoint Online license option in order to have Office Web Apps license option.

Make sure SharePoint Online license option is already assigned or to be assigned when assigning the Office Web Apps license option.

Exceeded Concurrent Shells Limit

Symptom:

An error that resembles the following message occurs when I have sent a request to the connector that involves contacting the endpoint:

[…This user is allowed a maximum number of 3 concurrent shells, which has been exceeded …]

Solution:

Exchange Online server has a limit of three sessions per user per machine. For better performance, the connector is expecting to have access to all the three available sessions. The error might be due to one of the following reasons:

- An active session has been created manually on the same machine using the same administrator credential.
- A session created by the connector is not cleaned-up.

To resolve this issue, perform one of the following actions below:

- Close the active session which are created manually.
- Manually ending all running PowerShell processes that are started by the connector.
- Restart the CA IAM CS.
- Override the *maxActive* property in connector.xml to reflect the number of sessions available for the connector to use.

Microsoft SQL Server Connector

After you have set up a connection to a Microsoft Office 365 endpoint, you can use Identity Management to do the following tasks:

- 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 Identity Management, 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.

Acquire an MS SQL Server Using the User Console

You must acquire the MS SQL server before you can administer it with Identity Management.

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, Identity Management 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 Identity Management 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 Identity Management 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 Identity Management. 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 Identity Management 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.

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 Identity Management 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 Identity Management 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 Identity Management installation is using the CAM/CAFT encryption, ask your Identity Management 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 Identity Management Agent, and you want to activate CAM/CAFT encryption for the communication between the Provisioning Server and other Identity Management 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 Identity Management 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 Identity Management can communicate with the Windows NT Remote Agent.

Windows NT Support for FIPS and IPv6

For this release of Identity Management, 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 Identity Management.

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, Identity Management 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 Identity Management 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 Identity Management based on the explore and correlate definition you created.

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

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 Identity Management, 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 Identity Management.

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, Identity Management 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 Identity Management 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 Identity Management based on the explore and correlate definition you created.

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 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.

Required Oracle Administrator Account Privileges

The Oracle administrator account that you use with Identity Management is the account name that you enter in the System Logon field of the Endpoint tab of the Oracle Endpoint property sheet.

Give this account at least the following privileges:

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

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

Sufficient privileges to Oracle accounts for packages and procedures

Grant these privileges in ONE of the following ways:

- The account is the owner of these packages and procedures.
- The account has execute privileges with the Admin Option for these packages and procedures.

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 Identity Management, the Oracle Connector does not support FIPs or IPv6.

Limitations

Connector Cannot Manage Some Privileges

You cannot use the Oracle connector manage the following operations:

- Manage system privileges or object privileges that apply to Oracle accounts
- Manage system privileges or object privileges that apply to Oracle roles

Instead, use native Oracle administrative tools to work with these privileges.

Suspend Operation Locks User Accounts

After suspending an Oracle account from 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 cannot 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.

Enable the Fix for Oracle Bug 6376915

The Oracle bug 6376915 causes high water (HW) enqueue contention when the database is busy handling large objects (LOB) and the database is configured to use automatic segments space management (ASSM).

This bug causes performance and scalability problems with CA software, including Identity Management and CA CloudMinder.

The fix for this problem introduces a mandatory event. Set this new event to make the ASSM architecture allocate LOB chunks more efficiently.

This bug was introduced in Oracle 10.2.0.3. It was fixed in both Oracle 10.2.0.4 and Oracle 11.1.0.7. However, the fix is not enabled by default.

The steps in this procedure assume that spfile is used for configuration.

Follow these steps:

1. Enter the following command:

   ```
   ALTER SYSTEM SET EVENT='44951 TRACE NAME CONTEXT FOREVER, LEVEL
   1024' scope=spfile;
   ```

2. Restart the database.
3. To test the fix, use the following measures:
   - Use Bulk Loader to measure the task throughput in Identity Management and CA CloudMinder.
   - Measure the wait time for HW enqueue contention.

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

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.

Well-Known Attribute %ENDPOINT_DESCRIPTION%

This applies to the following connectors: Windows, Oracle RDBMS, Siebel, UNIX NIS, MS SQL Server, and OpenVMS.

These endpoint types do not define the endpoint description in the eTDescription attribute. This means that until recently, you could not search on the endpoint description. In addition, the search screen did not display the endpoint description.

You can now use the new well-known attribute %ENDPOINT_DESCRIPTION% for the affected connectors.

The DefaultEndpointSearch role definition has been updated, to allow the Default Endpoint Search screen to use the new well-known attribute. If you are upgrading from an older version of Identity Management, import this modified screen after upgrading. For more information, see the Environment Changes section in your Upgrade Guide.

IBM i5/OS (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

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 Identity Management. For more information, see the Identity Management *Administrator's Guide*.

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) Management Console.
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 an 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.

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 Identity Management.

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, Identity Management 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 Identity Management 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 Identity Management based on the explore and correlate definition you created.

OS/400 Cascading Delete

In previous versions, if an OS400 account owned objects, the account could not be deleted from Identity Management. 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 Identity Management 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

PeopleSoft Connector

This guide does not contain information about the PeopleSoft connector.

Instead, download the endpoint guide from the Download page for Endpoint Guides and Attribute 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, and copy the compintfc.jar you generated previously into the same location.

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:

   Note: You can deploy the OSGI bundle from the connector server GUI or copy the jar files to ca-home/jcs/data/bundles/restore. Then restart the connector server and wait up to ten minutes for it to load.

   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 select 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 Identity Management.

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, Identity Management 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 Identity Management 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 Identity Management based on the explore and correlate definition you created.

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.

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 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.

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 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 Identity Management, 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 Identity Management.

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, Identity Management 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 Identity Management 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 Identity Management based on the explore and correlate definition you created.

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 337)
- Administrative roles
- RADIUS profiles
- Tokens
- Security domains
- Trusted groups
- User groups

In addition, you can view read-only information about the following objects on RSA SecurID endpoints:

- Authentication agents
- Authentication grade policies
- Identity sources
- Lockout policies
- Off-line authentication policies
- Password policies
- Self-service troubleshooting policies
- Token policies
- Trusted realms

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:

    Note: You can deploy the OSGI bundle from the connector server GUI or copy the jar files to ca-home/jcs/data/bundles/restore. Then restart the connector server and wait up to ten minutes for it to load.

    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 select 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.

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 Identity Management 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:

- Identity Management 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:
  - Identity Management 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 Identity Management 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 Identity Management 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:

- Identity Management 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 Identity Management Provisioning Directory with RSA 7.1 tokens, run the RSA7Migrate utility with the -token command-line parameter.

To migrate tokens

1. Stop the Identity Management 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 Identity Management 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.

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 333), 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 Identity Management 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

Known Issues

This section contains the following known issues for the RSA SecurID 7 Connector.

- Non-English Character Support for RADIUS Profiles (see page 337)
- Attempting to Create a Security Domain Above the Top Level Security Domain Fails (see page 338)
- Attempting to Create a Security Domain Above the Top Level Security Domain Fails (see page 338)

More information:

Non-English Character Support for RADIUS Profiles (see page 337)
Properties of RADIUS Profile Created with Japanese Characters (see page 338)
RADIUS Profiles with French Characters (see page 338)
Trusted Groups with More than 25 French or Japanese Characters (see page 338)
Attempting to Create a Security Domain Above the Top Level Security Domain Fails (see page 338)
RADIUS Profiles with Japanese Characters (see page 338)
Connector Data Migration Fails in Interactive Mode (see page 339)

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 338)
- Displaying properties of RADIUS profiles created with Japanese characters (see page 338)
- Creating RADIUS profiles with French characters (see page 338)
- Creating a Trusted Group with more than 25 French or Japanese characters (see page 338)

RADIUS Profiles with Japanese Characters

If you try to delete a RADIUS profile on an RSA7 server using Identity Management 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 Identity Management 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 Identity Management 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 Identity Management 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 Identity Management, 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 Identity Management 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 *Identity Management 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 Identity Management 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 Identity Management 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, Identity Management 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 Identity Management 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

This section applies to CA CloudMinder and Identity Management. It does not apply to CA GovernanceMinder.

The Salesforce connector supports the creation of custom attributes. You can customize the metadata of the Salesforce connector to create additional attributes for a Salesforce user object, including custom Salesforce 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 User Console

This section applies to CA CloudMinder and Identity Management. It does not apply to CA GovernanceMinder.

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 create custom attributes only for attributes that have a *string* data type. Strings include text fields, integer fields, and date and time fields.

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 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 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 is displayed in the User Console.
5. Generate the Account Management screens for the Salesforce.com connector.

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 Identity Management as the client 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 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.

The example shows you how to display a custom Salesforce.com text attribute named *MyCustomAttribute*, and then how to change the length of the field.

Follow these steps:

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 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 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 Identity Management User Console.

10. Deploy the Salesforce connector to the Provisioning Server.

11. Use the Role Definition Generator to generate the User Console Salesforce account management screens.

    The custom attribute appears in the Organization section of the User tab of the Salesforce Account dialog in the User Console.

Note: For more information about how to add and configure a provisioning server, create a project, and generate Identity Management User Console account screens, see the *Connector Xpress Guide*.

Deleting Salesforce.com Accounts

This section applies to CA CloudMinder and Identity Management. It does not apply to CA GovernanceMinder.

You cannot use the Salesforce.com connector to delete a Salesforce.com user, as Salesforce.com does not support account deletion.

The connector 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, the connector removes the Suspended membership and modifies the account, instead of adding a new account.

During an explore and correlate, the connector 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.

SAP R/3 Connector

The SAP R/3 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 Identity Management 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 Identity Management to manage an SAP 4.6C system, the following limitations apply:

- Identity Management 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 R/3 4.6C (see page 369)

Install JCo for SAP ERP

The SAP ERP connector requires SAP Java Connector 3 (SAP JCo). Before you use the SAP ERP connector, create a bundle that contains the JCo files, and then add the bundle to the connector.

Follow these steps:

1. 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 3 from the menu, then select the appropriate 64-bit download from the list.
   d. Extract the following files:
      - **Windows:** sapjco3.jar, sapjco3.dll
      - **UNIX:** sapjco3.jar, libsapjco3.so
   e. Send the files to the CA IAM CS computer.

   You can now follow the remaining steps.
2. 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 following location:

   `cs-home/jcs/resources/sap/sapConnectorLibsOsgi.jar`
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:

   Note: You can deploy the OSGI bundle from the connector server GUI or copy the jar files to ca-home/jcs/data/bundles/restore. Then restart the connector server and wait up to ten minutes for it to load.
   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 select Refresh Imports from the popup menu.

You can now use the SAP ERP connector to connect to an endpoint.

Load the Bundle for SAP r3 Prerequisites

The SAP R3 connector requires SAP Java Connector (SAP JCo). CA IAM CS comes with a bundle that contains the JCo files. Before you use the SAP R3 connector, add this bundle to the connector.

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.

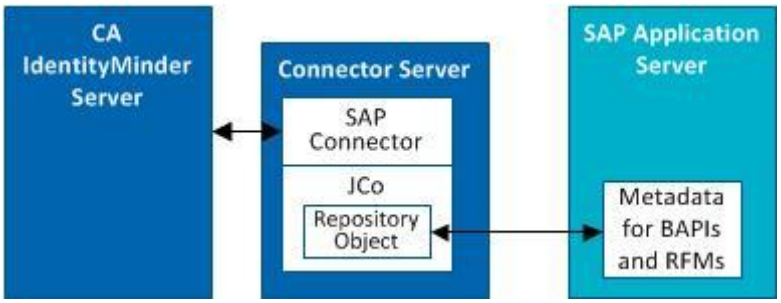
   CA IAM CS loads the bundle and lists it as a fragment.
5. Right-click the SAP R3 connector bundle (not the fragment!) and select Refresh Imports.

   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 the SAP ERP Connector to Read SUSPENDED and LOCKED States

This section applies to SAP R/3 4.6C only.

To allow the SAP ERP 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 Identity Management.

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, Identity Management 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 Identity Management 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 Identity Management based on the explore and correlate definition you created.

Changed SAP ERP Passwords are Expired

This section applies to SAP R/3 4.6C only. It is relevant for Identity Management and CA CloudMinder. It is not relevant for CA GovernanceMinder.

When you create or modify an SAP ERP endpoint, you can check the Changed Passwords Are Expired box. The user is then 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 behavior that SAP recommends for password changes. The box is checked by default for new endpoints.

More information:

Account Password Management (see page 365)
Account Password Management in CUA Environment (see page 367)

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.

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 Identity Management, 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.

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. You can prevent non-dialog accounts from being correlated to a global user

Follow these 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 correlation.

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.

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, an endpoint called CUAMAST (CUA master) can grant an account the following roles:

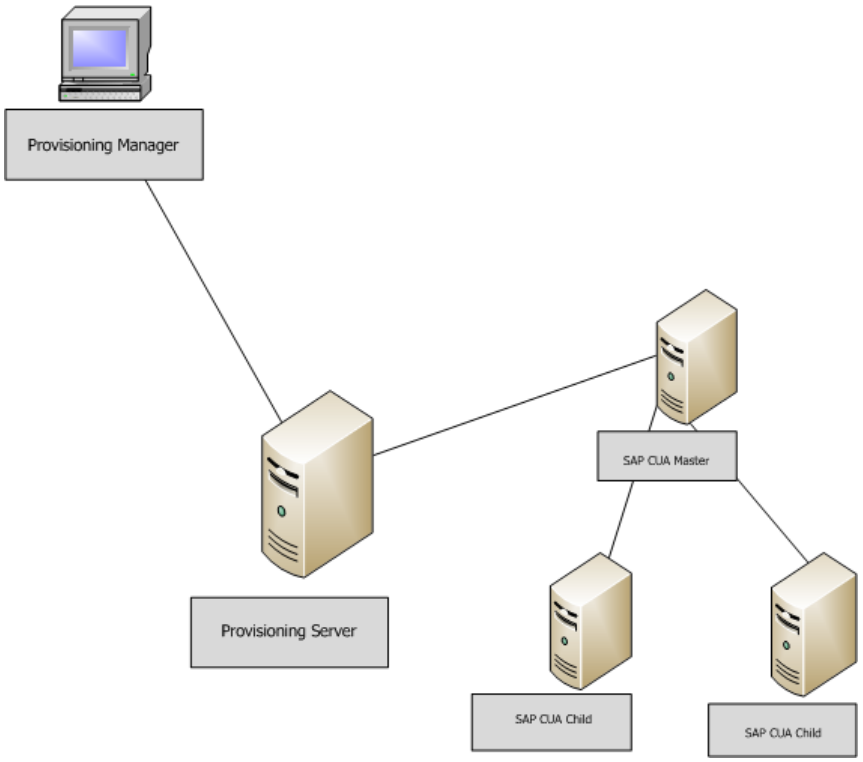
- role1
- CUACHI1/role3
- CUACHI2/role4

The following then occurs:

- An account is created on the CUA master system by Identity Management.
- The SAP CUA mechanism grants this account role1 privilege on the master system.
- The SAP CUA mechanism propagates the account to both CUACHI1 and CUACHI2 child systems.
- 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:

Figure 4: 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.

Distribution Settings in SAP CUA

Some distribution settings in your CUA environment can cause unexpected results.

If you use the SAP connector to change an attribute in a way that conflicts with the CUA distribution model, the modification attempted by the connector may be ignored. In some cases, SAP returns an error. However, in other cases you receive no notification that your change was ignored.

In addition, the User Console may not give a visual indication that the attribute change is permitted under the current distribution settings.

With the exception of password management, we recommend that where possible, the distribution settings be set to "Global".

Use the following advice to design your system:

- When the distribution model for an attribute has been set to "Global", this attribute must be managed by the connector 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.
- 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.

Note: 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.

Passwords on SAP R/3 4.6C

This section applies to SAP R/3 4.6C only. It is relevant for Identity Management and CA CloudMinder. It is not relevant for CA GovernanceMinder.

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, Identity Management ignores this flag.

Note: This flag only applies to passwords entered when adding new accounts or changing existing accounts.

true

(Default) Identity Management 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

Identity Management does not convert the password, if the SAP basis version is lower than 700.

More information:

Support for SAP (see page 357)

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 Identity Management 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 Identity Management 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 Identity Management User Console to do the following provisioning tasks:

- Create, update, and delete SAP UME users

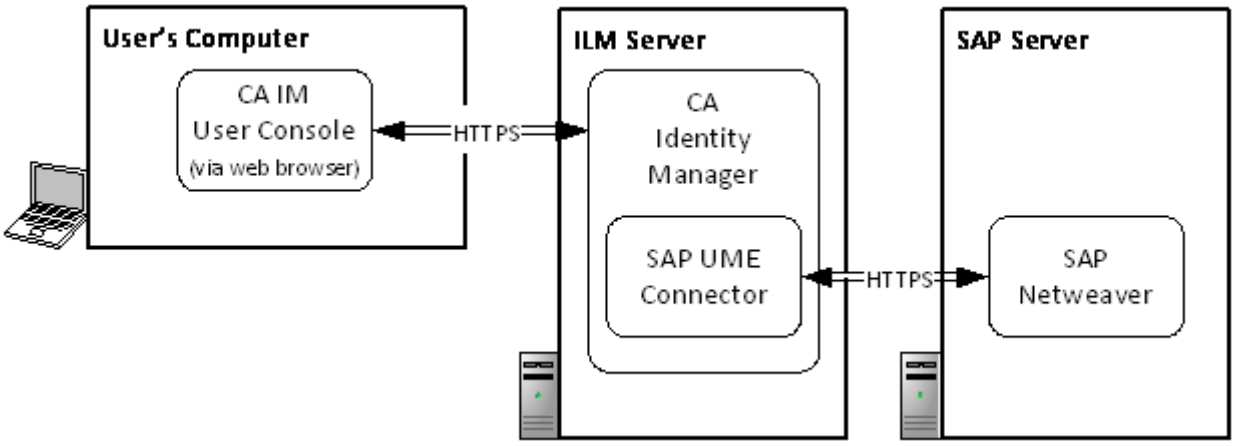
  Note: You cannot rename a user using the Identity Management User Console.
- Change a user's password
- Lock and unlock accounts
- Assign and unassign roles to users
- Assign and unassign groups to users

For known issues related to the SAP UME connector, see the Ide*ntity Management Release Notes* distributed with the Identity Management bookshelf.

How the SAP UME Connector Works

The following diagram shows how the connector links the endpoint (an SAP Netweaver server) with Identity Management:

Equation 1: The SAP UME Connector uses HTTPS to connect to SAP Netweaver on the SAP server.



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.

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 Identity Management .
2. The administrator for Identity Management does the following:
   a. To add the certificate to CA IAM CS keystore as a trusted certificate, enter one of the following commands:

      Windows:

      ```
      jcs_install\conf..\jvm\bin\Keytool.exe –importcert –keystore
      ssl.keystore –storepass <keystore_password> -file <cert_file>
      ```

      UNIX:

      ```
      jcs_install/conf../jvm/bin/keytool -import -keystore
      ssl.keystore -storepass <keystore_password> -file <cert_file>
      ```

      The keystore is in *jcs-install*/conf/ssl.keystore.
   b. Restart CA IAM CS.
   c. Verify that the Use HTTPS check box is selected for each SAP UME endpoint that you create. This check box is selected by default.

Troubleshooting

Locked and Suspended Passwords

Identity Management 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 Identity Management 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, Identity Management 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 Identity Management User Console

Symptom:

I created an SAP UME account with Japanese characters in Identity Management. 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 Identity Management, 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 Identity Management 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 Identity Management 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, Identity Management 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.

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 Identity Management 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.

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 Identity Management.

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, Identity Management 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 Identity Management 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 Identity Management based on the explore and correlate definition you created.

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.

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.

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 manage NIS slave servers or clients.

Installing the UNIX Connector

The UNIX connector comes with C++ Connector Server (CCS). You do not need to install it separately.

After you install CCS, install and configure the UNIX agents and the CAM Service.

LSM handles the installation process for these supporting components, including reference counting.

Note: Each package can be installed using the script installation (.sh) method.

Important! For HP-UX, install the latest Gold Quality Pack.

The installation process for the UNIX agents and the CAM service have two modes:

- 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.

Set Up the Installation Files for the UNIX Remote Agent

The connectors for UNIX ETC and UNIX NIS use a remote agent to communicate with the connector server, and to perform operations on the endpoint. You install the remote agent on each endpoint.

Follow these steps:

1. Choose an installation method:
   - **LSM**—Uses a .@pif file.
   - **Script**—Uses a .sh script. Use the script if LSM is not available, for example when no other CA products are installed on the system.
2. Locate the installation package for your platform. The packages are in the following location in the installation files:

   RemoteAgent/UNIX/*platform*/IdentityManager.*platform*.sh

   platform

   Identifies one of the following platforms:

   - AIX
   - HPUX
   - Solaris
   - SolarisIntel
   - Linux
   - LinuxS390
   - Tru64
3. If required, copy the installation files to the UNIX computer on which you intend to install. To do this, copy the entire contents of the directory for your platform.

You can now choose an installation method: interactive or silent.

Installation Commands

The installation options are described in the following table:

Installation Option	Description
% sh IdentityManager.[Platform].sh -r [Response File] [-F]	Installs the product. A response file can be added to customize unattended installation. The switch '-F' performs a forced installation and prevents the backup of the previous version of the product.
lsm -e *product name* [-s]	Removes the installed product. Switch '-s' runs the uninstallation in unattended mode. 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. 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. 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. 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 Commands (see page 383)

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 Commands (see page 383)

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 Identity Management 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:

   ```
   PATHIdentity Management=/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 Identity Management

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.

Follow these steps:

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. Identity Management 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 Identity Management 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

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.

-i

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.

-m

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.

blank

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.

3. Restart the CAM Service on each computer on which you installed the new key, using hte following commands:

```
camclose
cam start
```

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 Identity Management, 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 Identity Management.

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, Identity Management 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 Identity Management 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 Identity Management 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 Identity Management.

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, Identity Management 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 Identity Management 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 Identity Management based on the explore and correlate definition you created.

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 Identity Management 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.

Managing Passwords

Identity Management can intercept an account password change on a UNIX or Linux system, and propagate it to all other accounts associated with its Global User. Identity Management Pluggable Authentication Module (PAM) lets Identity Management authenticate passwords against external security systems so that global users can use their existing system passwords to log on to Identity Management.

For more information, see the *Administration Guide*.

Appendix A: Bulk Load Client

This section contains the following topics:

Introduction

The Bulk Load Client is a command line utility that you use to remotely access the Identity Management 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 Identity Management 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 Identity Management authentication.

Note: The user must be authorized to use the Identity Management 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.

Configure the Environment for the Bulk Load Client

After you create a tenant environment, you configure it to work with the bulk load client.

Follow these steps:

Important! Perform this procedure only once. If you repeat these steps, other issues can occur.

1. In the Management Console, complete the following steps:
   a. Navigate to Environments, *your_environment*, Advanced Settings, Web Services.
   b. Select the following options:

      Enable Execution

      Enable WSDL Generation

      Enable admin_id (allow impersonation)

   c. Select Basic Authentication in the SiteMinder Authentication field.
   d. Click Save.
   e. Restart the environment.

2. In the Administrative UI, complete the following steps:
   a. Navigate to Policies, Domain, Domains, then click the domain name that applies to the environment.
   b. Open the Realms tab, and verify that the *tenant_name*_TEWS6_realm appears in the list of realms.
   c. Navigate to the Administration tab at the top of the screen.
   d. Select Policy Server, Cache Management.
   e. Click Flush All in the All Caches section.
3. In the User Console, enable Web Services for the Bulk Loader task as follows:
   a. Log in as a user with rights to use the Modify Admin Task.

      For example, the CSP admin role includes this task.
   b. Navigate to Modify Admin Task.
   c. Search for and select the Bulk Loader task.
   d. On the Profile tab, select Enable Web Services.
   e. Click Submit.

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 Identity Management 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 Identity Management Server

Bulk Load Client uses a user name and a password to authenticate to the Identity Management Server.

When the Identity Management 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 Identity Management, configure the Identity Management Server to accept HTTPS requests, then setup the Bulk Load Client:

Follow these steps:

1. Import the Identity Management 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:

- Identity Management 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:

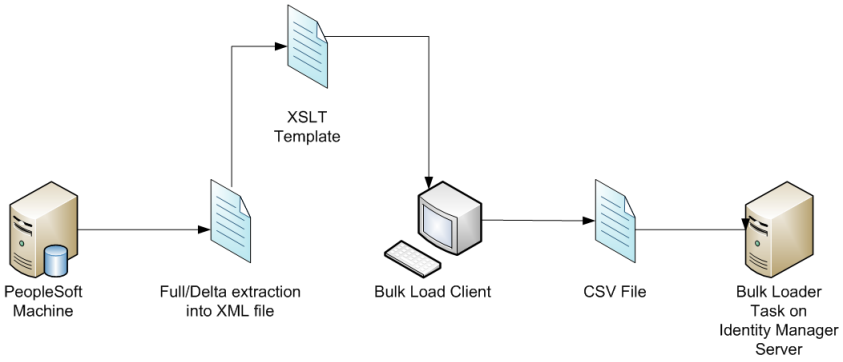
```
#
# These are the connection details of the Identity Management Server
#

# 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 Identity Management ObjectsFeeder task
#

# Identity Management 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 Identity Management 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 2: 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 Identity Management Bulk Loader task.
3. Convert the XML file using XSLT template with the Identity Management Bulk Load Client.

   Bulk Load Client internally transforms the XML file into CSV format required by the Identity Management 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 *Identity Management 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 Identity Management 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 Identity Management log files.

The Bulk Loader task can be monitored as any other task using VST. Each nested Identity Management 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 Identity Management 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.