CA Access Control

Integration Guide

12.7

Third-Party Notices

CONTAINS IBM(R) 32-bit Runtime Environment for AIX(TM), Java(TM) 2 Technology Edition, Version 1.4 Modules

Sample Scripts and Sample SDK Code

The Sample Scripts and Sample SDK code included with the CA ControlMinder product are provided "as is", for informational purposes only. Adjust them to your specific environment and do not use them in production without running tests and validations.

CA Technologies does not provide support for these samples and cannot be responsible for any errors that these scripts may cause.

CA Technologies Product References

This document references the following CA Technologies products:

- CA Access Control
- CA ControlMinder
- CA Single Sign-On (eTrust SSO)
- CA Top Secret®
- CA ACF2™
- CA Audit
- CA Network and Systems Management (CA NSM, formerly Unicenter NSM and Unicenter TNG)
- CA Software Delivery (formerly Unicenter Software Delivery)
- CA SDM (formerly Unicenter Service Desk)
- CA User Activity Reporting Module (formerly CA Enterprise Log Manager)
- CA Identity Manager

Documentation Conventions

The CA ControlMinder documentation uses the following conventions:

Format	Meaning
`Mono-spaced font`	Code or program output
Italic	Emphasis or a new term
Bold	Text that you must type exactly as shown
A forward slash (/)	Platform independent directory separator used to describe UNIX and Windows paths

The documentation also uses the following special conventions when explaining command syntax and user input (in a mono-spaced font):

Format	Meaning
Italic	Information that you must supply
Between square brackets ([])	Optional operands

Format	Meaning
Between braces ({})	Set of mandatory operands
Choices separated by pipe (|).	Separates alternative operands (choose one). For example, the following means *either* a user name *or* a group name: {*username*|*groupname*}
...	Indicates that the preceding item or group of items can be repeated
Underline	Default values
A backslash at end of line preceded by a space (\)	Sometimes a command does not fit on a single line in this guide. In these cases, a space followed by a backslash (\) at the end of a line indicates that the command continues on the following line. **Note:** Avoid copying the backslash character and omit the line break. These are not part of the actual command syntax.

Example: Command Notation Conventions

The following code illustrates how command conventions are used in this guide:

```
ruler className [props({all|{propertyName1[,propertyName2]...})]
```

In this example:

- The command name (ruler) is shown in regular mono-spaced font as it must be typed as shown.
- The *className* option is in italic as it is a placeholder for a class name (for example, USER).
- You can run the command without the second part enclosed in square brackets, which signifies optional operands.
- When using the optional parameter (props), you can choose the keyword *all* or, specify one or more property names separated by a comma.

File Location Conventions

The CA ControlMinder documentation uses the following file location conventions:

- *ACInstallDir*—The default CA ControlMinder installation directory.
  - Windows—C:\Program Files\CA\AccessControl\
  - UNIX—/opt/Ca/AccessControl/

- *ACSharedDir*—A default directory used by CA ControlMinder for UNIX.
  - UNIX—/opt/CA/AccessControlShared
- *ACServerInstallDir*—The default CA Access Control Enterprise Management installation directory.
  - /opt/CA/AccessControlServer
- *DistServerInstallDir*—The default Distribution Server installation directory.
  - /opt/CA/DistributionServer
- *JBoss_HOME*—The default JBoss installation directory.
  - /opt/jboss-4.2.3.GA

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.

Documentation Changes

The following documentation updates have been made since the last release of this documentation:

- CA ControlMinder REST API—Added the REST requests to communicate between a custom, or third-party programs with the Shared Accounts Management database by-passing the Enterprise Management Server User Interface.

Contents

Chapter 1: About this Guide

This guide provides information about how to integrate CA Access Control with third-party software. These include CA User Activity Reporting Module, CA Directory, CA SiteMinder, RSA SecurID and ObserveIT Enterprise. The chapters in this guide apply to CA Access Control only.

To simplify terminology, we refer to the product as CA ControlMinder throughout the guide.

Chapter 2: Integrating with CA User Activity Reporting Module

This section contains the following topics:

About CA User Activity Reporting Module

CA User Activity Reporting Module focuses on IT compliance and assurance. It lets you collect, normalize, aggregate, and report on IT activity, and generate alerts requiring action when possible compliance violations occur. You can collect data from disparate security and non-security devices.

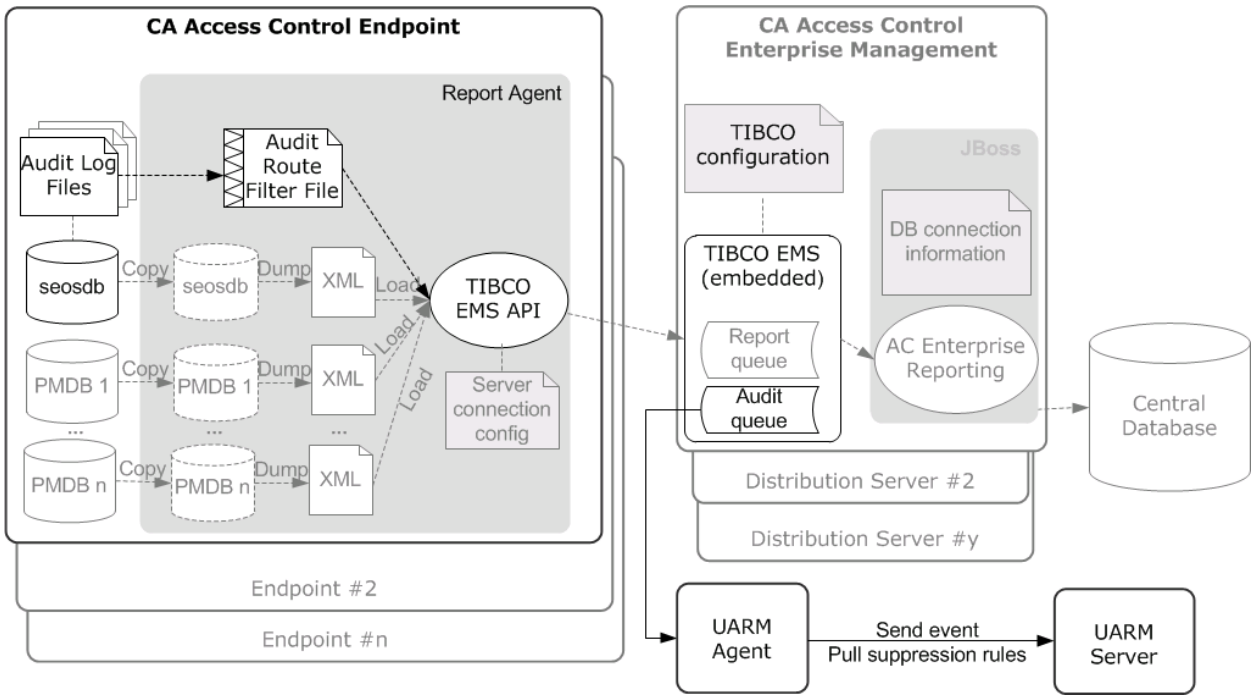
CA User Activity Reporting Module Integration Architecture

Integration with CA User Activity Reporting Module lets you send CA ControlMinder audit events from each of your endpoints for collection and reporting by CA User Activity Reporting Module.

You can configure CA ControlMinder to send audit events from the audit file on the local endpoint to a remote audit queue on the Distribution Server. You can then configure a CA User Activity Reporting Module connector to connect with the audit queue and pull events (messages) from it. CA User Activity Reporting Module processes these events and sends them to the CA User Activity Reporting Module server.

The CA ControlMinder installation supports CA User Activity Reporting Module integration.

The following diagram shows the architecture of CA User Activity Reporting Module integration components:



The preceding diagram illustrates the following:

- Each endpoint, containing a CA ControlMinder database (seosdb), has the Report Agent component installed.
- The Report Agent collects audit data from the endpoint and sends them to the Distribution Server.
- The Distribution Server accumulates the audit data in an audit queue.
- A CA User Activity Reporting Module agent collects events from the audit queue and sends it to the CA User Activity Reporting Module server for processing.

Note: CA User Activity Reporting Module integration relies on reporting service components. As such, your architecture includes other reporting service components and features that are not used for CA User Activity Reporting Module integration. These components and features are dimmed in the diagram.

Note: CA Access Control Enterprise Management installs the Distribution Server on the Enterprise Management Server by default. For high availability purposes, you can install the Distribution Server on a separate computer.

CA User Activity Reporting Module Integration Components

CA User Activity Reporting Module integration uses the following CA ControlMinder components. These components are part of the CA ControlMinder enterprise reporting service:

- A *Report Agent* is a Windows service or a UNIX daemon that runs on each CA ControlMinder or UNAB endpoint and sends information to queues on a configured Message Queue that resides on the Distribution Server. For CA User Activity Reporting Module integration, the Report Agent collects endpoint audit messages from the audit log files on a scheduled basis, and sends these events to the audit queue on a configured Distribution Server.
- A *Message Queue* is a component of the Distribution Server that is configured for receiving endpoint information that Report Agents send. For reporting, the Message Queue forwards endpoint database snapshots to the central database using the CA ControlMinder Web Service. For redundancy and failover, you can have multiple Distribution Servers collecting and forwarding the information.

Note: CA Access Control Enterprise Management installs the Distribution Server on the Enterprise Management Server by default.

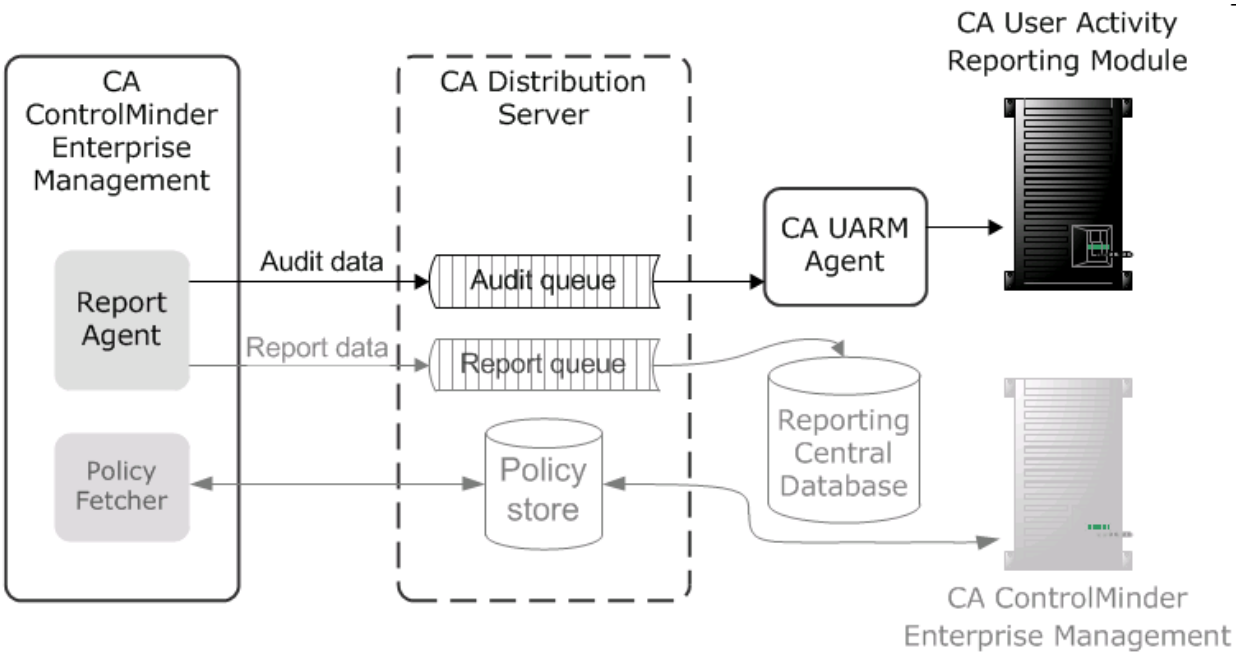
CA User Activity Reporting Module integration also uses the following CA User Activity Reporting Module components:

- A *CA User Activity Reporting Module agent* is a generic service configured with connectors, each of which collects raw events from a single event source and then sends the events to a CA User Activity Reporting Module server for processing. For CA ControlMinder audit data, the agent deploys the CA ControlMinder connector.
- A *CA ControlMinder connector* is an out-of-the-box CA User Activity Reporting Module integration for a CA ControlMinder audit event source. The connector enables raw event collection from a CA ControlMinder Distribution Server and the rule-based transmission of converted events to an event log store, where they are inserted into the hot database.
- A *collection server* is a CA User Activity Reporting Module server that refines incoming event logs, insert them into the hot database, compresses the hot database when it reaches the configured size into a warm database, and auto-archives the warm database to the related management server on the configured schedule.

Note: For more information about CA User Activity Reporting Module components, see the CA User Activity Reporting Module documentation.

How Audit Data Flows from CA ControlMinder to CA User Activity Reporting Module

To understand how CA ControlMinder integrates with CA User Activity Reporting Module, and what to consider when configuring this integration, first consider the flow of audit data between CA ControlMinder and CA User Activity Reporting Module. The following illustration describes how CA ControlMinder routes audit events to a messaging queue on a Distribution Server, where the CA ControlMinder connector of the CA User Activity Reporting Module agent pulls, maps, transforms, and then sends the events to the CA User Activity Reporting Module server:



1. The Report Agent collects audit events from the local endpoint audit files, applies any filtering policies, and places the events on a audit queue located on the Distribution Server.
2. A CA User Activity Reporting Module connector, deployed by the CA User Activity Reporting Module agent, connects with the audit queue and pulls events (messages) from it.
3. The CA User Activity Reporting Module connector and agent maps the events to the Common Event Grammar (CEG) using data mapping and parsing files, and then applies suppression and summarization rules before routing the events to the CA User Activity Reporting Module server.
4. The CA User Activity Reporting Module server receives the events and may apply additional suppression and summarization rules before the events are stored.

Note: For more information about how CA User Activity Reporting Module works, see the CA User Activity Reporting Module documentation.

How to Set Up CA User Activity Reporting Module for CA ControlMinder

To use CA User Activity Reporting Module to create reports that contain audit data from all your CA ControlMinder endpoints, first implement enterprise reporting. You must implement enterprise reporting before you integrate with CA User Activity Reporting Module because implementing enterprise reporting enabled the Report Agents on your endpoints. Once you have enterprise reporting implemented, set up CA User Activity Reporting Module for CA ControlMinder.

To set up CA User Activity Reporting Module for CA ControlMinder, follow these steps:

1. Install the CA User Activity Reporting Module server.

   Note: For more information, see the *CA User Activity Reporting Module Implementation Guide*.

2. Install the CA User Activity Reporting Module agent on or near the Distribution Server.

   The agent must be accessible to the Distribution Server and communicate with it through a specified port. It must also be accessible to the CA User Activity Reporting Module server.

   Note: Verify the operating system support for the CA User Activity Reporting Module agent before you install it. For more information about installing the agent, see the *CA User Activity Reporting Module Agent Installation Guide*.

3. Install CA Access Control Enterprise Management.

   Note: For more information, see the *Implementation Guide*.

4. Create a connector for the agent.

   Once you have the CA User Activity Reporting Module agent installed and communicating with the CA User Activity Reporting Module server, create a connector and configure it so that it can access the CA ControlMinder event source (the audit queue on the Distribution Server).

   Note: The following topics describe settings that are required for CA ControlMinder event collection, including the connector details and connector configuration requirements that you must configure for the integration to succeed. For more information about how to create a connector, see the *CA User Activity Reporting Module Administration Guide* and the *Online Help*.

5. Create a connection to CA User Activity Reporting Module from CA Access Control Enterprise Management.

6. (Optional) Configure an audit collector.

7. Configure CA ControlMinder endpoints for audit collection.

Connector Details

After you install the CA User Activity Reporting Module agent on a computer, that computer appears in the CA User Activity Reporting Module server management interface (for example, to view a computer in the Default Agent Group click Administration, Log Collection, Agent Explorer, Default Agent Group, *computer_name*). You must now create a connector. This topic describes the settings that you *must* configure on the Connector Details page of the Connector Creation wizard.

Integration

Specifies the integration you want to use as a template.

Select the appropriate CA ControlMinder integration.

Example: AccessControl_R12SP5_TIBCO

You can optionally change the name of the connector and add a description. You can then apply suppression rules to events handled by the connector.

Note: For information about other optional settings that let you customize your event collection, see the *CA User Activity Reporting Module Administration Guide* and the *Online Help.*

Suppression and Summarization Rules

Once you create the connector and specify the connector details, you can optionally apply suppression rules on the Apply Suppression Rules page of the Connector Creation wizard.

The name of the Ideal Model for the suppression and summarization rules for CA ControlMinder is Host IDS/IPS. When you create rules, select the values for Event Category, Event Class, and Event Action as needed to identify events.

Note: For information about other optional settings that let you customize your event collection, see the *CA User Activity Reporting Module Administration Guide* and the *Online Help.* For more information on field identification or individual values, see the Common Event Grammar Reference in the *CA User Activity Reporting Module Online Help*.

Connector Configuration Requirements

Once you create the connector and specify the connector details, you can configure the connector. This topic describes the settings that you *must* configure on the Connector Configuration page of the Connector Creation wizard to begin event collection.

Note: For information about other optional settings that let you customize your event collection, see the *CA User Activity Reporting Module Administration Guide* and the *Online Help.*

TIBCO Server

Specifies the host name or IP address of the Message Queue (TIBCO server) in the following format:

Protocol://server IP or name:Port number

The Message Queue is installed on CA Access Control Enterprise Management.

- Define the following value:

  `ssl://ACentmserver:7243`

The port values and communication method are the default ports that CA Access Control Enterprise Management uses. If you configured different values after installing CA Access Control Enterprise Management, use that port and communication method values.

TIBCO User

Specifies the user name for Message Queue authentication. CA ControlMinder defines a default user named "reportserver".

TIBCO Password

Specifies the password for Message Queue authentication. Enter the password that you defined in the "Communication Password" dialog when you installed CA Access Control Enterprise Management.

Event Log Name

Specifies the log name for the event source.

Accept the default, "CA ControlMinder".

PollInterval

Specifies the number of seconds the agent waits before polling for events when the Message Queue has become unavailable or disconnected.

SourceName

Specifies the identifier for the Message Queue queue.

Accept the default, "queue_audit".

TIBCO Queue

Specifies the name of the Message Queue queue from which the log sensor is to read messages (events).

Accept the default, "queue/audit".

Number of Collection threads

Specifies the number of threads the log sensor spawns to read Message Queue messages.

You should consider the number of events in the Message Queue queue and the CPU of the CA User Activity Reporting Module agent system when you adjust this value.

Limits: The minimum value is 1. The maximum number of threads that the log sensor can spawn is 20.

How Configuration Settings Affect the Report Agent

For CA User Activity Reporting Module integration, the Report Agent collects endpoint audit messages from the audit log files on a scheduled basis, and routes these events to the audit queue on a configured Distribution Server. You can affect performance by tuning the Report Agent settings.

Note: The Report Agent is part of the CA ControlMinder enterprise reporting service and is also responsible for sending database snapshots for endpoint reporting purposes. This process describes only those actions that the Report Agent takes for audit event routing to CA User Activity Reporting Module.

The Report Agent does the following when you enabled audit collection (set the audit_enabled configuration settings to 1):

- Collects new audit records by reading records from the endpoint audit files and committing them to memory.

  The Report Agent reads the number of audit records that you defined in the audit_read_chunk configuration setting and then waits for the duration that you defined in the audit_sleep configuration setting before reading the audit files again. The Report Agent reads previously unread records in the active audit log *and* all the backup audit files. It then commits to memory those records that pass the audit filter as defined in the audit filter file (audit_filter configuration setting).

- Sends a group of audit records it has in memory to the Distribution Server Message Queue that you defined in the audit_queue configuration setting.

  The Report Agent sends audit records when *one* of the following applies:

  - The number of records in memory reaches the number defined by the audit_send_chunk configuration setting.
  - The amount of time that has passed because the last audit records were sent equals the interval defined by the audit_timeout configuration setting.

Example: Default Report Agent Settings for Audit Collection and Routing

This example illustrates how we set the default Report Agent configuration settings, what environment these are set for, and how they affect performance.

We expect an average environment to have 30 events per second (EPS). Therefore, the Report Agent reads 30 events for every second that passes. To reduce the impact on other running applications (CPU use and context switches) we chose to have the Report Agent read 300 events every 10 seconds, as follows:

```
audit_sleep=10
audit_read_chunk=300
```

The message bus CA ControlMinder uses to transport messages between the Report Agent and the Distribution Server handles large packets that are sent at long intervals better than it handles small packets at short intervals. The following configuration setting specifies that when the number of audit records the Report Agent collects reaches the defined number, the Report Agent sends the records to the Distribution Server. Assuming 30 events per second, if we want the Report Agent to send audit records at approximately one-minute intervals (60 seconds), we et the Report Agent as follows:

```
audit_send_chunk=1800
```

However, at night, or at other times when there are less than 30 events per second, there are less than 1800 events per minute. To verify that the Report Agent still regularly sends audit records to the Distribution Server, we set a maximum interval of 5 minutes between sending audit records, as follows:

```
audit_timeout=300
```

Filter Events from CA User Activity Reporting Module

You can use a filter file to prevent CA ControlMinder from sending every audit record in the log file to CA User Activity Reporting Module. The filter file specifies the audit records that are not sent to CA User Activity Reporting Module.

Note: This filter file prevents CA ControlMinder from sending the specified audit events to the Distribution Server, but does not stop CA ControlMinder from writing the audit events to the local files. To filter out audit events from the local audit file, modifyfilter rules in the file defined be the AuditFiltersFile configuration setting in the logmgr section (by default, audit.cgf).

To filter events from CA User Activity Reporting Module, edit the audit filter file on the endpoint. If you want to apply the same filtering rules to more than one endpoint, we recommend that you create an audit filtering policy and assign the policy to the endpoints where you want it to be effective.

Note: For more information, see the *Reference Guide*.

Example: Audit Filter Policy

This example shows you what an audit filtering policy looks like:

```
env config
er config auditrouteflt.cfg line+("FILE;*;*;R;P")
```

This policy writes the following line to the auditrouteflt.cfg file:

```
FILE;*;*;R;P
```

This line filters audit records that record a permitted attempt by any accessor to access any file resource for reading. CA ControlMinder will not send these audit records to the Distribution Server.

Secure Communications using SSL

When you install CA Access Control Enterprise Management you can select to either secure the communication between the Distribution Server and Report Agent by using SSL or select not to secure the communication. Whichever option you select, specify the same option when you install the Report Agent on the endpoint.

For example, if you use SSL to encrypt the communications between the Report Agent and the Distribution Server (the default), then you must provide authentication information when you install CA Access Control Enterprise Management, such as the password required for the Report Agents to communicate with the Distribution Server.

This is the password you provide when you configure the CA ControlMinder Report Agent on the endpoint and in the CA User Activity Reporting Module agent Connector Configuration page.

You must provide the same information when you install the Report Agent. Only Report Agents that can provide the correct certificate and password information can write events to the audit queue on the Distribution Server and thus be retrieved by CA User Activity Reporting Module.

Audit Log Files Backup for CA User Activity Reporting Module Integration

To collect audit data, the Report Agent reads the CA ControlMinder audit log files according to its configuration settings. The Report Agent reads a configured number of audit records from the audit log files at configured intervals. In a default legacy installation, or when you do not enable audit log routing during installation, CA ControlMinder keeps a single size-triggered audit log backup file. Every time the audit log reaches the configured maximum size, it creates a backup file, overwriting the existing audit log backup file. As a result, it is possible that the backup file will be overwritten before the Report Agent read all of its records.

We strongly recommend that you set CA ControlMinder to keep time-stamped backups of your audit log file. This way, CA ControlMinder does not overwrite the backup audit log files until it reaches a configured maximum of audit log files it should keep. This is the default setting when you enable the audit log routing sub-feature during installation on the endpoint.

Example: Audit Log Backup Settings

This example illustrates how the recommended configuration settings affect CA User Activity Reporting Module integration. When you enable the audit log routing sub-feature during installation on an endpoint, CA ControlMinder sets the following logmgr section configuration settings:

```
BackUp_Date=yes
audit_max_files=50
```

In this case, CA ControlMinder timestamps each backup copy of the audit log file and keeps a maximum of 50 backup files. This provides plenty of opportunity for the Report Agent to read all of the audit records from the files and for you to copy the backup files for safe keeping if required.

Important! If you set audit_max_files to 0, CA ControlMinder does not delete backup files and will keep accumulating the files. If you want to manage the backup files through an external procedure, remember that CA ControlMinder protects these files by default.

Configure an Existing Windows Endpoint for CA User Activity Reporting Module Integration

Once you have CA Access Control Enterprise Management installed and configured, you can configure your endpoints for sending audit data to the Distribution Server by enabling and configuring the Report Agent.

Note: When you install CA ControlMinder, it lets you configure the endpoint for collecting and sending audit data. This procedure illustrates how you configure an existing endpoint for sending audit data if you did not configure this option at install time.

To configure an existing Windows endpoint for CA User Activity Reporting Module integration

1. Click Start, Control Panel, Add or Remove Programs.

   The Add or Remove Program dialog appears.

2. Scroll through the program list and select CA ControlMinder.

3. Click Change.

   The CA ControlMinder installation wizard appears.

   Follow the wizard prompts to modify the CA ControlMinder installation so that you enable the Report Agent feature and the Audit Routing sub-feature.

   Verify that you also specify to keep time-stamped backups of the audit log file.

Note: After you enable the Report Agent and audit routing, you can modify CA ControlMinder configuration settings to change performance-related settings. Before you do this, you should understand how the Report Agent collects audit events and routes them to the Distribution Server (see page 22). For more information about Report Agent configuration settings, see the *Reference Guide*.

Configure an Existing UNIX Endpoint for CA User Activity Reporting Module Integration

Once you have CA Access Control Enterprise Management installed and configured, you can configure your endpoints for sending audit data to the Distribution Server by enabling and configuring the Report Agent.

Note: When you install CA ControlMinder, it lets you configure the endpoint for collecting and sending audit data. This procedure illustrates how you configure an existing endpoint for sending audit data if you did not configure this option at install time.

Follow these steps

1. Run *ACSharedDir*/lbin/report_agent.sh:

   `report_agent config -server hostname [-proto {ssl|tcp}] [-port port_number [-rqueue queue_name] -audit -bak`

   If you omit any configuration options, the default setting is used.

   Note: For more information about the report_agent.sh script, see the *Reference Guide*.

2. Create a *+reportagent* user in database.

   This user should have ADMIN and AUDITOR attributes and *write* access to local terminal. You should also set epassword to the Report Agent Shared Secret (which you defined when you installed the Distribution Server).

3. Create a SPECIALPGM for the Report Agent process.

   The SPECIALPGM maps the root user to the +reportagent user.

Note: After you enable the Report Agent and audit routing, you can modify CA ControlMinder configuration settings to change performance-related settings. Before you do this, you should understand how the Report Agent collects audit events and routes them to the Distribution Server (see page 22). For more information about Report Agent configuration settings, see the *Reference Guide*.

Example: Configure a UNIX Endpoint for CA User Activity Reporting Module Integration Using selang

The following selang commands show you how, assuming you enabled and configured the Report Agent, you create the required Report Agent user and specify special security privileges for the Report Agent process:

```
eu +reportagent admin auditor logical epassword(Report_Agent) nonative
auth terminal (terminal101) uid( +reportagent) access(w)
er specialpgm (/opt/CA/AcessControl/bin/ReportAgent) Seosuid(+reportagent) \

Nativeuid(root) pgmtype(none)
```

Queries and Reports for CA ControlMinder Events

The queries, reports, and action alerts for CA ControlMinder are grouped under the Server Resource Protection tags in the CA User Activity Reporting Module interface.

Note: For information, visit the CA User Activity Reporting Module Product page at http://ca.com/support

How to Enable CA User Activity Reporting Module Reports in CA ControlMinder

Before you can view CA User Activity Reporting Module reports in CA Access Control Enterprise Management, you must enable CA User Activity Reporting Module reporting, export and add the CA User Activity Reporting Module certificate and configure the connection to CA User Activity Reporting Module from CA Access Control Enterprise Management.

1. Enable CA User Activity Reporting Module reporting by configuring advanced settings.
2. Export and add the CA User Activity Reporting Module trusted certificate to the keystore. (see page 29)
3. Configure the Connection to CA User Activity Reporting Module (see page 30)
4. (Optional) Configure an audit collector (see page 32).

   Configure an audit collector if you want to send Shared Accounts Management audit events to CA User Activity Reporting Module.

Add the CA User Activity Reporting Module Trusted Certificate to the Keystore

CA User Activity Reporting Module reports are authenticated using trusted certificates. The certificate verifies that the information displayed in the reports originated from a trusted CA User Activity Reporting Module source, which verifies the authenticity of the data.

To view CA User Activity Reporting Module reports in CA Access Control Enterprise Management, you first export the certificate and add than it to the keystore.

To add the CA User Activity Reporting Module trusted certificate to the keystore

1. Enter the URL of the CA User Activity Reporting Module server in a web browser in the format: https://*host*:*port*

   A security alert dialog appears.

2. Click View Certificate.

   The Certificate dialog appears.

3. Click Details, Copy to File.

   The Certificate Export Wizard appears.

4. Complete the wizard using the following instructions:

   - **Export File Format**—Select Base-64 encoded X.509 (.CER).
   - **File to Export**—Define the full pathname of the exported certificate file.

     For example, C:\certificates\computer.base64.cer

   A message appears indicating that the export completed successfully.

5. Import the certificate to the keystore. For example:

   ```
   C:\jdk1.5.0\jre\lib\security>c:\jdk1.5.0\bin\keytool.exe -import -file
   computer.base64.cer -keystore
   C:\jboss-4.2.3.GA\server\default\deploy\IdentityMinder.ear\custom\ppm\truststo
   re\ssl.keystore
   ```

6. Enter the keystore password. The default password is 'secret'.

7. Click Yes to trust the certificate.

   The certificate is added to the keystore.

Configure the Connection to CA User Activity Reporting Module

CA Access Control Enterprise Management communicates with CA User Activity Reporting Module to display reports with CA ControlMinder related information. To display these reports you need to configure the connection to CA User Activity Reporting Module.

To configure the connection to CA User Activity Reporting Module

1. In CA Access Control Enterprise Management, do as follows:
   a. Click System.
   b. Click Connection Management subtab.
   c. Expand the UARM tree in the task menu on the left.

   The Manage CA User Activity Reporting Module Connection task appears in the list of available tasks.
2. Click Manage CA User Activity Reporting Module Connection .

   The Manage CA User Activity Reporting Module Connection: *PrimaryCALMServer* task page appears.
3. Complete the fields in the dialog. The following fields are not self-explanatory:

   Connection name

   Identifies the name of the CA User Activity Reporting Module connection.

   Description

   (Optional) Defines a description for this connection.

   Host Name

   Defines the name of the CA User Activity Reporting Module host you want CA Access Control Enterprise Management to work against.

   Example: host1.comp.com

   Port #

   Defines the port that the CA User Activity Reporting Module host uses for communication.

   Default: 5250

Certificate Authority Signed SSL certificate

Specifies whether the connection to CA User Activity Reporting Module uses an SSL certificate signed by a certificate authority.

Certificate name

Defines the name of the certificate.

Password

Defines the certificate password.

4. Click Submit.

   CA Access Control Enterprise Management saves the CA User Activity Reporting Module connection settings.

Example: Obtain the CA User Activity Reporting Module Certificate Information

The following example shows you how to obtain the CA User Activity Reporting Module certificate information that you need to provide when creating and managing the CA User Activity Reporting Module connection settings in CA Access Control Enterprise Management.

1. Enter the CA User Activity Reporting Module URL in a web browser using the following format:

   `https://host:port/spin/calmapi/products.csp`

   Example: https://localhost:5250/spin/calmapi/products.csp

2. Enter a valid user name and password to log in to CA User Activity Reporting Module.

3. Select the Register option to register a certificate with CA User Activity Reporting Module.

   The New Product Registration screen appears.

4. Enter the certificate name and password and select Register.

   A message appears informing you that the certificate registered successfully.

Configure an Audit Collector

CA Access Control Enterprise Management collects audit events, including Shared Accounts Management audit events, and stores them in the central database. You can configure CA Access Control Enterprise Management to send the audit events to CA User Activity Reporting Module.

To configure an audit collector

1. In CA Access Control Enterprise Management, do as follows:
   a. Click System.
   b. Click Connection Management subtab.
   c. Expand the UARM tree in the task menu on the left.

      The Create Audit Collector task appears in the list of available tasks.
2. Click Create Audit Collector.

   The Create Audit Collector: Audit Collector Search Screen appears.
3. (Optional) Create a copy of an existing audit collector, as follows:
   a. Select Create a copy of an object of type UARM Sender.
   b. Select an attribute for the search, type in the filter value, and click Search.

      A list of UARM Senders that match the filter criteria appear.
   c. Select the object you want to use as a basis for the new audit collector.
4. Click OK.

   The Create Audit Collector task page appears. If you created the audit collector from an existing object, the dialog fields are pre-populated with the values from the existing object.
5. Complete the fields in the dialog. The following fields are not self-explanatory:

   Job Enable

   Specifies whether the audit collector is enabled.

   Name

   Defines the name of audit collector.

   Queue Jndi

   Defines the name of the Message Queue queue that CA Access Control Enterprise Management sends audit event messages to.

   Example: *queue/audit*

   Sleep

   Defines the interval, in minutes, between database queries.

   Default: 1

Time Out

Defines the collector time out period, in minutes, for sending the audit event messages to the messages queue.

Default: 10

Note: Once the timeout period has passed, the collector sends the messages although the number of messages in the queue did not reach the level defined in the Msg Block Size field.

Msg Block Size

Defines the maximum number of messages to accumulate in the database before sending the message to the queue.

Default. 100

6. Click Submit.

   CA Access Control Enterprise Management creates the audit collector.

Chapter 3: Integration with ObserveIT Enterprise

This section contains the following topics:

About this Guide

This chapter instructs you how to integrate CA Access Control with the ObserveIT Enterprise session recording program. This chapter explains the process and procedures that you do to record Shared Accounts Management sessions.

This chapter is intended for security and system administrators using CA ControlMinder that want use the ObserveIT Enterprise session recording capabilities.

To simplify terminology, we refer to the product as CA ControlMinder throughout the guide.

Chapter 4: About ObserveIT Integration

The CA ControlMinder integration with ObserveIT Enterprise extends your control over access attempts by privileged accounts to the servers in your organization. The ObserveIT Enterprise session logging software records user activities on target systems. The recording starts at the moment when a user checks out a privileged account password and logs into the endpoint and ends when the session terminates, for example, when the user checks in the privileged account password.

The recorded sessions are stored on a dedicated database that you prepare. You can replay the recorded sessions directly from CA Access Control Enterprise Management using the ObserveIT viewer.

You can download ObserveIT Enterprise from ObserveIT Systems at the following link:

http://www.observeit-sys.com/download.asp

You can find the ObserveIT Enterprise documentation at the following location:

Product Documentation

Note: For more information about ObserveIT, see the ObserveIT Documentation on the ObserveIT Enterprise installation media.

How to Set Up the Integration

There are several steps you take to integrate CA ControlMinder with the ObserveIT Enterprise session recording software. At the end of the integration, all Shared Accounts Management sessions are recorded by the ObserveIT Enterprise software.

Note: For more information about how to complete Steps 1-5, see the ObserveIT Enterprise documentation on the ObserveIT installation media.

Do the following to set up the integration:

1. Review the ObserveIT Enterprise system and installation requirements.

   Verify that the servers you use meet the minimum system requirements to install ObserveIT Enterprise.

2. Prepare the central database.

   Recorded sessions are stored on a dedicated Microsoft SQL Server.

3. Configure the Internet Information Server (IIS).

   The ObserveIT Enterprise application server uses IIS to process the metadata that the agents send.

4. Install the ObserveIT Enterprise server components.

   The ObserveIT application server, agent, and management console are also installed.

5. Configure the ObserveIT Enterprise application server.

   You configure the recording settings.

6. Deploy the session recording scripts on the Enterprise Management Server.

   The scripts enable the Shared Accounts Management automatic login that triggers the session recording.

7. Create a service account.

   Create a service account for the Enterprise Management Server to use

8. Define the connection to the ObserveIT Enterprise application server in CA Access Control Enterprise Management.

   You configure the connection settings to enable session logging.

How to Prepare the Integration

After you complete the installation of the ObserveIT Enterprise application server, you prepare the server for integration with CA ControlMinder. After you prepare the ObserveIT Enterprise application server, the server is configured to start recording and saving Shared Accounts Management sessions.

Do the following to prepare the integration:

1. Open the management console.
2. Create a service account.

   CA ControlMinder uses the service account to connect to the ObserveIT Enterprise application server.

Open the Management Console

After you install and start ObserveIT Enterprise you can start the web-based management console.

To open the management console

1. Using a browser, open the ObserveIT Enterprise management console. Enter the following URL:

   http://observeit_server_name:port/ObserveIT

   Example:

   `http://observeit_server:4884/ObserveIT`

2. Use the administrator credentials you specified during installation to log in.

   The ObserveIT Enterprise management console opens.

Note: You can also open the ObserveIT Enterprise management console by clicking Start, Programs, ObserveIT, ObserveIT WebConsole.

Create a Service Account

CA Access Control Enterprise Management uses a service account to authenticate the ObserveIT Enterprise application server to record user activities. You supply the service account credentials when you configure the ObserveIT Enterprise application server connection settings in CA Access Control Enterprise Management.

To create a service account

1. From the ObserveIT Enterprise management console, select Configuration, Console Users.

   The console users screen opens.

2. Select Create User.

   The add console user window opens.

3. Enter the user name, password and confirm the password.

4. Set the authentication method to ObserveIT.Authentication and the user role to Admin.

5. Click Add.

   The service account is created.

Note: For more information about users management, see the *ObserveIT Documentation* on the ObserveIT Enterprise installation media.

Deploy the Session Recording Scripts

User session recording works in conjunction with Shared Accounts Management automatic login. When a user checks out a privileged account password and selects to log in to the endpoint, a remote management software opens and automatically logs the user in. CA Access Control Enterprise Management controls the remote management programs by using the session recording scripts, based on the endpoint type.

For example, when a user chooses to log into a Windows endpoint, CA Access Control Enterprise Management uses a script that opens the Remote Desktop software to connect to the endpoint.

To record the sessions on the ObserveIT Enterprise application server, you deploy the session recording scripts on the Enterprise Management Server.

To deploy the session recording scripts

1. From the CA Support web site, download the session recording scripts and save them in a temporary directory.
2. On the Enterprise Management Server, navigate to the following directory, where *JBoss_HOME* specifies the directory JBoss is installed:

   JBoss_HOME/server/default/deploy/IdentityMinder.ear/config/sso_scripts
3. Copy the session recording scripts into the sso_scripts directory.

   We recommend that you back up the files in the directory before you overwrite them.
4. Select to overwrite the existing files with the new files.

You can now configure the connection settings to the ObserveIT Enterprise application server.

Define the Connection to ObserveIT

In order to complete the integration with ObserveIT Enterprise, you configure the connection settings to the ObserveIT Enterprise application server in CA Access Control Enterprise Management.

To define the connection to ObserveIT

1. In CA Access Control Enterprise Management, select System, Connection Management, Session Recording, Create Connection.

   The Create Connection screen appears.

2. Enter the following details:

   Connection description

   Defines a free text description of the connection

   Playback URL

   Define the ObserveIT Enterprise application server URL

   Example:http://observeit_host:4884/observeit/

   User ID

   Define the service account user name

   Password

   Define the service account password

   Advanced

   Specifies the following advanced connection settings:

   Viewer Page

   Specifies whether to display a message indicating that the session is recorded at the top of the screen

   Viewer Parameters

   Specifies the ObserveIt viewer windows width and height

   ActiveX URL

   Specifies the full pathname to the location where the ObserveIT Enterprise ActiveX file is located. By default, you specify the URL to the ObserveIT Application server.

   Example:
   http://observeit_host:4884/ObserveIT/AgentInstall/Agent.cab#version=1,0,0,0

Server URL

Specifies the full pathname of the location where the ObserveIT Enterprise application server stores the recorded sessions. By default, you specify the URL to the ObserveIT Application server.

Example: http://observeit_host:4884/ObserveITApplicationServer

3. Click Submit.

   CA Access Control Enterprise Management creates the connection.

How Sessions Are Logged

Each Shared Accounts Management session is recorded and stored on the ObserveIT Enterprise database. Each session is divided into individual slides that you can reply separately from the entire recorded session.

The following process describes how Shared Accounts Management sessions are logged:

1. A user checks out a privileged account password from CA Access Control Enterprise Management and selects to automatically log into the endpoint.

   If this is the first time that this option is used, the user is required to install ActiveX.

2. A remote management session opens and the user is logged in without entering the password.
3. The ObserveIT agent installed on the endpoint begins to record the user activities and send the slides to the ObserveIT Enterprise application server, which saves the data in the database.
4. The user closes the remote management session and the ObserveIT agent stops the recording.
5. The recorded sessions appear in CA Access Control Enterprise Management.

Important! To enable Internet Explorer to download the ActiveX, specify the ObserveIT Enterprise host name in the Local Intranet Zone or Trusted Zone and set the Download signed ActiveX controls security option to Enable.

Note: For more information about sessions recording, see the *ObserveIT Documentation* on the ObserveIT Enterprise installation media.

Where Sessions Are Logged

The ObserveIT Enterprise application server logs the Shared Accounts Management sessions on a dedicated Microsoft SQL Server. The ObserveIT database server uses two dedicated databases. The first database is named ObserveIT and holds the configuration and metadata. The second database is named ObserveIT_Data and stores the screenshots that the ObserveIT agents collect during the recorded session.

Note: For more information about session logging, see the *ObserveIT Documentation* on the ObserveIT Enterprise installation media.

Play Back Sessions

You play back the recorded Shared Accounts Management sessions from CA Access Control Enterprise Management. When you select to play back a session, CA Access Control Enterprise Management plays the recorded session in a new window. The player window contains control buttons you use to navigate the session. You can also perform a free text search within the recorded sessions.

Note: For more information about free text search, see the *ObserveIT Documentation* on the ObserveIT Enterprise installation media.

To play back sessions

1. In CA Access Control Enterprise Management, select Privileged Accounts, Audit subtask.

   The Audit Privileged Accounts task appears in the list of available task

2. Select Audit Privileged Accounts

   The Audit Privileged Accounts search window opens.

   Note: Verify that the Shared Accounts Management Audit Manager role is assigned to you.

3. Specify the search criteria, enter the number of rows to display and click Search.

   The tasks that satisfy your search criteria are displayed.

4. Click the play back icon in the session details column to play back the session.

   The player window opens and the session is played from the beginning of the session.

   Note: Use the controls at the bottom of the window to navigate the session.

Chapter 5: Integration with RSA SecurID

This section contains the following topics:

How To Integrate CA Access Control Enterprise Management with RSA SecurID

If your organization uses RSA SecurID to authenticate users, you can use the capabilities of RSA SecurID to authenticate users login to CA Access Control Enterprise Management. When you integrate the Enterprise Management Server with RSA SecurID, CA Access Control Enterprise Management does not authenticate users on login. CA Access Control Enterprise Management detects that users authentication is done by a third-party program.

The following process explains how to integrate CA Access Control Enterprise Management with RSA SecurID:

1. Prepare the Enterprise Management Server.
2. Install a supported web server:
   - Windows-Internet Information Server 7.0 with the Application Request Routing (ARR) module.
   - Linux-Apache 2.2.6 web server with the proxy module
3. Configure the Web server as a reverse proxy server (see page 47).

   The web server acts as a reverse proxy server for all login authentication requests.
4. Configure RSA SecurID to block all network access to CA Access Control Enterprise Management except from the web server.

   RSA SecurID prevents users from accessing CA Access Control Enterprise Management directly.
5. Install the Enterprise Management Server components.
6. Define a user account in CA Access Control Enterprise Management for each RSA SecurID user that will log in to CA Access Control Enterprise Management.

   Define only those users that you want to grant access to CA Access Control Enterprise Management.

   Important! If you are using Active Directory you do not need to complete this step.

7. Install the RSA Authentication Agent on the following servers:
   - (Linux) Enterprise Management Server
   - The web server

   RSA Authentication Agent intercepts user access requests and forwards the requests to RSA Authentication Manager.
8. Configure the RSA web Agent to enable Single Sign On (SSO) to CA Access Control Enterprise Management.
9. Install the RSA Authentication Manager on a dedicated host.

   RSA Authentication Manager authenticates users access requests.

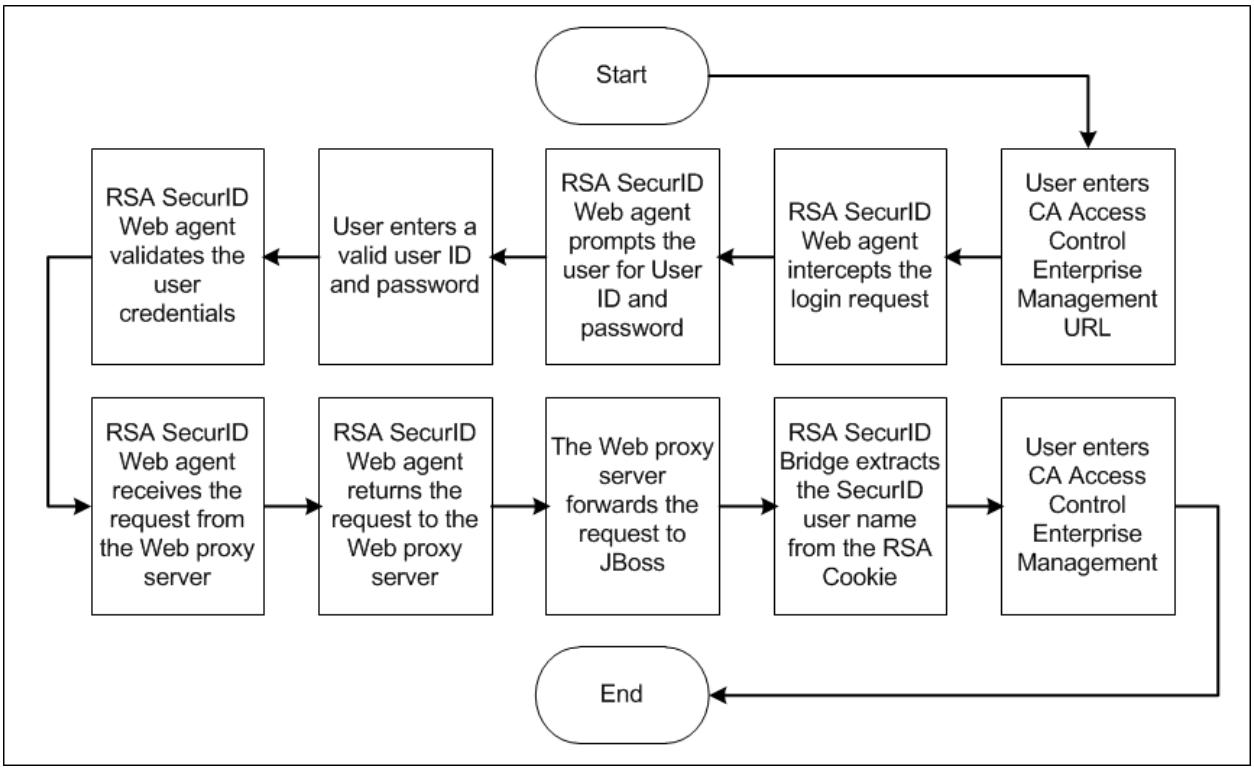
Each time a user tries to log in to CA Access Control Enterprise Management, RSA SecurID prompts the user for a valid RSA SecurID credentials instead of CA Access Control Enterprise Management user account details. If authenticated, RSA SecurID logs the user in to CA Access Control Enterprise Management.

Note: For more information about the RSA SecurID web Agent and Authentication Manager, refer to the RSA SecurID website.

How RSA SecurID Authenticates Users Login

When you integrate the Enterprise Management Server with RSA SecurID, each time a user logs into CA Access Control Enterprise Management,RSA SecurID authenticates the login request.If RSA SecurID validates the user login, the user automatically gains access to CA Access Control Enterprise Management.

The following diagram illustrates how RSA SecurID authenticates user logins to CA Access Control Enterprise Management:



Configuring a Web Server as a Reverse Proxy Server

When a user attempts to login to CA Access Control Enterprise Management, RSA SecurID intercepts the request and prompts the user for a valid SecurID user name and password. The Web server you installed acts as a reverse proxy server that receives login requests from the RSA Authentication Web agent on the Enterprise Management Server and forwards the requests to the RSA Authentication Manager.

A *reverse proxy* is a gateway for other servers that enables one web server to provide content from another.

Example: Configuring Internet Information Services 7.0 on Windows Server 2008 as a Reverse Proxy Server

In this example, Steve the system administrator installed the Enterprise Management Server and Internet Information Services (IIS) 7.0 on a Windows Server 2008 with the Application Request Routing (ARR) module installed. The ARR module enables the IIS to act as a proxy server.

1. Steve enables the IIS proxy settings on the internet Information Services server:
   a. Selects Start, Administrative Tools, internet Information Services (IIS) Manager

      The internet Information Services (IIS) Manager console opens.

   b. Selects the host from the left pane to expend the actions pane and selects the Application Request Routing Cache icon.

      The Application Request Routing Cache management console opens.

   c. Selects Server Proxy Settings from the actions pane.

   d. Marks the Enable Proxy check box and clicks Apply.

      Steve has enabled the IIS proxy settings.

2. Steve configures the IIS to forward requests to the Enterprise Management Server:
   a. Expands the Sites menu and selects the default website.

   b. Highlights the URL Rewrite icon and selects Open Feature from the Actions menu.

      The URL Rewrite configuration console opens.

   c. Selects Add Rules from the Actions menu.

      The Add Rules window opens.

   d. Under the Inbound Rules, selects Blank Rule and clicks Ok.

      The Edit Inbound Rule configuration window opens.

   e. Specifies the rule name and selects (iam.+) from the Patterns menu.

   f. Scrolls down to the Action section and selects Rewrite from the Action type menu.

   g. Enters the CA Access Control Enterprise Management URL in the URL Rewrite filed using the following format.

      ```
      http://enterprise_host:8080/{R:0}
      ```

   h. Clicks Apply to create the rule.

      The new inbound rule is created.

   i. Repeats steps c to h using (castyles.+) from the Patterns menu.

      Steve has configured the IIS to forward requests to the Enterprise Management Server.

3. Steve configures RSA SecurID to secure the web server:
   a. Selects the Default Web Site in the internet Information Services (IIS) Manager console and double clicks the RSA SecurID icon.

      The RSA SecurID settings window opens.

   b. Selects the following check boxes:
      - Enables RSA SecurID Web Access Authentication Feature on This Server
      - Protect This Resource

   c. Selects apply from the Actions menu
4. Steve configures the RSA Web Agent to enable Single Sign Off (SSO) for CA Access Control Enterprise Management
   a. Opens the regedit utility and navigates to the following location:

      `HKEY_LOCAL_MACHINE\SOFTWARE\SDTI\RSAWebAgent`

   b. Creates a registry key of type DWORD under the name RSAUSERCustomHeader.

   c. Sets the registry key value to 1

   Steve has configured Internet Information Services as a reverse proxy server.

Example: Configuring the Apache Web server 2.2.6 as a Reverse Proxy Server on a Red Hat Enterprise Linux 5.0

In this example, Steve the system administrator installed the Enterprise Management Server on a Red Hat Enterprise Linux 5.0. Steve now needs to install and configure the Apache Web Server 2.2.6 as a reverse proxy server.

1. Steve does the following to install and configure the Apache Web Server 2.2.6 with the proxy module:

   a. Configures the Apache Web Server 2.2.6 installation to install the proxy module, as follows:

   ```
   tar -zxvf httpd_2.2.6.tar.gz
   ./configure --prefix=/usr/local/apache --enable-proxy
   --enable-proxy-http
   make
   make install
   ```

   The Apache Web Server 2.2.6 is installed with the proxy module.

2. Steve does the following to configure the reverse proxy:

   a. Navigates to the conf directory of the Apache web server.

   b. Opens the httpd.conf file for editing.

   c. Locates the LoadModule list of entries and adds the following section:

   ```
   # Used for proxy to the Enterprise Management Server
   ProxyPass    /iam http://196.168.1.1:8080/iam
   ProxyPass    /castylesr5.1.1
   http://192.168.1.1:8080/castylesr5.1.1
   ProxyPassReverse    /iam http://192.168.1.1:8080/iam
   ```

   d. Saves and closes the file.

   e. Restarts the Apache Web Server.

   Steve configured the Apache Web Server 2.2.6 to act as a reverse proxy server.

3. Steve configures the RSA web agent to ignore the web browser IP address for cookie validation:

   a. Navigates to the RSA web agent installation directory:

   ```
   /usr/local/apache/rsawebagent/
   ```

   b. Runs the RSA web agent configuration utility.

   c. Selects the RSA server that is currently in use from the list.

   d. Browses to the second configuration screen.

   e. Verifies that the Ignore browser IP address for cookie validation is enabled.

   Steve has configured the RSA web agent to ignore the web browser IP address for cookie validation.

4. Steve configures the RSA web agent to enable Single Sign Off (SSO) for CA Access Control Enterprise Management:

   a. Opens the Linux web agent distribution and locates the following file:

      `rsacookieapi.tar`

   b. Copies the file to a temporary directory and extracts the content of the file.

   c. Locates the following files:

      - RSACookieAPI.jar
      - librsacookieapi.so

   d. Copies the librsacookieapi.so file to the following location, where *JBOSS_HOME* indicates the location where Steve installed Jboss:

      JBOSS_HOME`/server/default/deploy/IderntityMinder.ear/library`

   e. Copies the RSACookieAPI.jar file to the following location:

      `JBOSS_HOME/server/default/deploy/IderntityMinder.ear/user_console.war/WEB-INF/lib/`

   Steve configured the RSA web agent to enable SSO for CA Access Control Enterprise Management.

Chapter 6: Working with Multiple LDAP Servers

This section contains the following topics:

Introduction

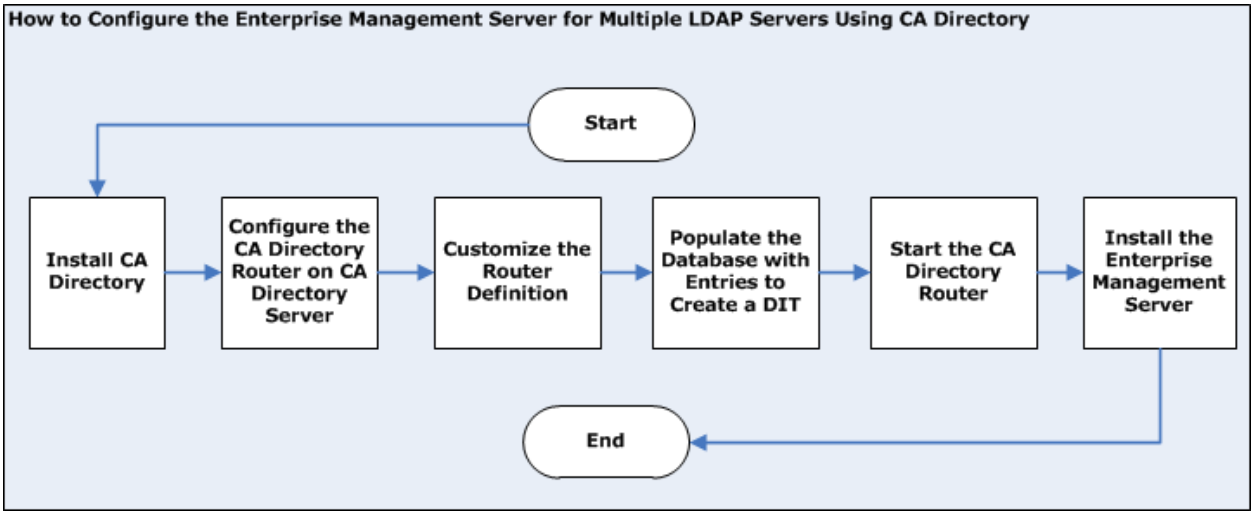
This information in this chapter describes how a system or a database administrator configures CA Access Control Enterprise Management with multiple LDAP servers using CA Directory. Working with multiple LDAP servers, enables the administrator to integrate multiple LDAP user stores into a single enterprise-wide user store.

How to Configure Multiple LDAP Servers

CA Directory supports the integration of LDAP servers into a distributed directory backbone.

CA Directory provides a utility called DXlink,that enables searches over a number of LDAP directory servers.

The following diagram illustrates how to configure CA Access Control Enterprise Management for multiple LDAP servers using CA Directory:



You perform the following steps to configure the Enterprise Management Server for multiple LDAP servers using CA Directory:

1. Install CA Directory
2. Configure the CA Directory router (see page 55)
3. Customize the CA Directory router definitions (see page 57)
4. Populate the database with entities to create a DIT (see page 60)
5. Start CA Directory
6. Install the Enterprise Management Server with Active Directory as the user store

   Important! When you install the Enterprise Management Server, specify the following:

   - Host name—Specify CA Directory host name
   - Port number—Specify 25389
   - Base DN—Specify a DN that is common to all Active Directory servers in the environment. Leave this field blank if not applicable.
   - (Linux) Search Root—Specify a DN that is common to all Active Directory servers in the environment. Leave this field blank if not applicable.
   - Administrative account—Specify an administrative account from one of the Active Directory domains.

Note: When you log in to CA Access Control Enterprise Management, verify that you specify the domain name that the administrative account you are using is a member.

Configure the CA Directory Router

CA Directory routes requests to the Active Directory that correspond to the suffix defined in the client request to the Active Directory used by CA ControlMinder. CA Directory uses the DXlink utility to route the request.

Before you completed this procedure, you installed two Active Directory user stores, for example: acdir1 and acdir2 and CA Directory, named dsarouter.

Follow these steps:

1. From the CA Directory server, open a Command Prompt window
2. Run the following command:

   `dxnewdsa -s 1 cadirhost-adrouter 25389`

   -s *1*

   Specify the database size of 1 MB

   cadirhost -adrouter

   Defines the name of the router

   25389

   Specifies the router port
3. Stop the router using the following command:

   `dxserver stop cadirhost-adrouter`
4. Install the router using the following command:

   `dxserver install cadirhost-adrouter`

5. Navigate to the following directory, where *DXHOME* is the name of the directory where you installed the router:

   DXHOME/config/knowledge

6. Duplicate the cadirhost-router.dxc file, as follows:

   a. Rename one file to acdir1-dxlink.dxc

   b. Rename the second file to acdir2-dxlink.dxc

   c. Edit the acdir1-dxlink.dxc file to appear as follows:

```
set dsa "acdir1-dxlink" =
{
    prefix            = <dc "acdir1"><dc "com">
    dsa-name          = <cn "acdir1-dxlink">
    dsa-password      = "secret"
    ldap-dsa-name     = <dc "acdir1"><dc "com"><cn "users"><cn
"Administrator">
    ldap-dsa-password = "{CADIR}yKW2cVbG"
    address           = tcp "acdir1" port 389
    auth-levels       = clear-password
    trust-flags       = allow-check-password, no-server-credentials
    link-flags        = dsp-ldap, ms-ad
};
```

   ldap-dsa-name

   Specifies the Distinguished Named (DN) used to bind to Active Directory

   ldap-dsa-password

   Defines the encrypted password for the DN

   Note: Use the dxpassword utility to encrypt the password. For example: dxpassword -P CADIR <*password*>.

   address

   Specifies the Active Directory domain controller address

   d. Edit the acdir2-dxlink.dxc to appear as follows:

```
set dsa "aclabcail-dxlink" =
{
    prefix            = <dc "acdir2"><dc "com">
    dsa-name          = <cn "acdir2-dxlink">
    dsa-password      = "secret"
    ldap-dsa-name   = <dc "acl"><dc "aclab"><cn "users"><cn "Administrator">
    ldap-dsa-password = "{CADIR}yKW2cVbG"
    address           = tcp "acdir2" port 389
    auth-levels       = clear-password
    trust-flags       = allow-check-password, no-server-credentials
    link-flags        = dsp-ldap, ms-ad
};
```

You have configured the CA Directory router.

Customize the CA Directory Router Definitions

After configuring the CA Directory router, you need to customize the CA Directory router definitions.

Follow these steps:

1. Navigate to the following directory, where *DXHOME* is the directory where CA Directory is installed:

   DXHOME/config/limits

2. Do the following:

   a. Create a copy of the default.dxc file and renames the original file to dsarouter-adrouter.dxc

   b. Remove the ReadOnly flag from the file

   c. Open the dsarouter-adrouter.dxc file and modify the following fields as follows:

   ```
   # size limits
   set max-users = 255;
   set max-local-ops = 100;
   set max-op-size = 0;

   # time limits
   set max-bind-time = none;
   set bind-idle-time = 3600;
   set max-op-time = 600;
   ```

   Save and close the file.

3. Navigate to the following directory:

   DXHOME/config/settings

4. Do the following:

   a. Create a copy of the default.dxc file and rename the original file to dsarouter-adrouter.dxc

   b. Remove the ReadOnly flag from the file

   c. Open the dsarouter-adrouter.dxc file and modify the following fields as follows:

   ```
   # directory information base
   set alias-integrity = true;
   # distribution controls
   set multi-casting = true;
   set always-chain-down = false;
   ```

```
# security controls
set min-auth = clear-password;
set allow-binds = true;
set ssl-auth-bypass-entry-check = false;
# general controls
set op-attrs = true;
set transparent-routing = true;
```

Save and close the file

5. Navigate to the following directory:

   ```
   DXHOME/config/knowledge
   ```

6. Open, or create, the dsarouter-adrouter.dxc file and remove the auth-levels string value "anonymous" to enable clear password login only. For example:

   ```
   set dsa "cadirhost-adrouter" =
   {
   prefix        = <>
   dsa-name      = <cn "cadirhost-adrouter">
   dsa-password  = "secret"
   address       = tcp "cadirhost" port 25389
   disp-psap     = DISP
   snmp-port     = 25389
   console-port  = 25390
    auth-levels   = clear-password
   ```

   Save and close the file.

   Important! If you installed CA Directory on a server where both IPv4 and IPv6 addresses are defined, specify IPv6 and IPv4 address types in the tcp value. For example: address = tcp "fe80::20d:56ff:fed4:8300%5" port 19389, tcp "192.168.1.1" port 19389

7. Create a file named adrouter.dxa and add the following lines, then save and close the file:

   ```
   source "dsarouter-adrouter.dxc";
   source "acdir1-dxlink.dxc";
   source "acdir2-dxlink.dxc";
   ```

8. Navigate to the following directory:

   ```
   DXHOME/config/logging
   ```

9. Do the following:

   a. Create a copy of the default.dxc file

   b. Rename the original file to dsarouter-adrouter.dxc

   c. Remove the ReadOnly tag.

10. Navigate to the following directory:

    ```
    DXHOME/config/servers
    ```

11. Do the following:

    a. Edit the *cadirhost*-adrouter.dxi, modify the following lines as follows then save and close the file:

```
#
# Initialization file written by DXnewdsa
#
# logging and tracing
source "../logging/cadirhost-adrouter.dxc";
# schema
clear schema;
source "../schema/default.dxg";
# knowledge
clear dsas;
source "../knowledge/adrouter.dxg";
# operational settings
source "../settings/cadirhost-adrouter.dxc";
# service limits
source "../limits/cadirhost-adrouter.dxc";
# access controls
clear access;
source "../access/default.dxc";
# ssl
source "../ssld/default.dxc";
# replication agreements (rarely used)
# source "../replication/";
# multiwrite DISP recovery
set multi-write-disp-recovery = false;
# grid configuration
set dxgrid-db-location = "data";
set dxgrid-db-size = 1;
set cache-index = all-attributes;
set lookup-cache = true;
```

Note: Replace *cadirhost* with the CA Directory host name.

You have customized the CA Directory router definitions.

Populate the CA Directory Database to Create a DIT

You can choose to populate the CA Directory database with entities to create a Directory Informational Tree (DIT). A DIT enables you to browse the organizational hierarchy from the top down.

Follow these steps:

1. On the server hosting the CA Directory router, create a file named input.ldif and enter the following entities, for example:

```
dn: dc=com
objectClass: domain
objectClass: top
dc: com

dn: dc=company,dc=com
objectClass: domain
objectClass: top
dc: company

dn: dc=demo
objectClass: domain
objectClass: top
dc: demo
```

2. Save and close the file.
3. Open a Command Prompt window and run the following command:

   `dxloaddb cadirhost-adrouter input.ldif`
4. Run the following command to start up the CA Directory router:

   `dxserver start cadirhost-adrouter`

   Note: Replace *cadirhost* with the CA Directory host name.

You have populated the CA Directory database with entities to create a DIT.

Chapter 7: Integrating with CA SiteMinder

This section contains the following topics:

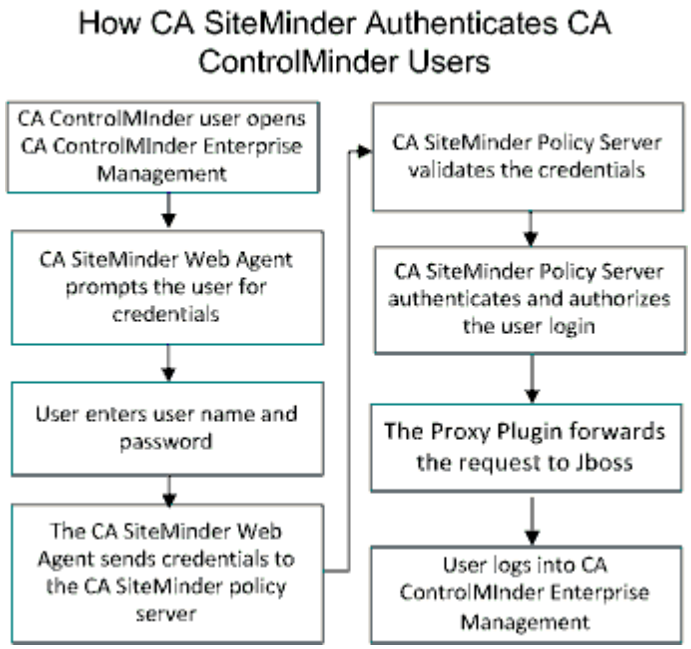
Integration with CA SiteMinder

The information in this chapter describes how system, network or security administrators secure CA Access Control Enterprise Management with CA SiteMinder. CA SiteMinder can authenticate users from a CA SiteMinder directory and allow CA ControlMinder users only to log in to CA Access Control Enterprise Management. Securing CA Access Control Enterprise Management with CA SiteMinder enables the administrator to use CA SiteMinder advanced user authentication methods.

How CA SiteMinder Authenticates CA ControlMinder Users

When you use CA SiteMinder to secure CA Access Control Enterprise Management, each time a user logs in to CA Access Control Enterprise Management, CA SiteMinder authenticates the login request. If CA SiteMinder authorizes the login request, the user gains access to CA Access Control Enterprise Management.

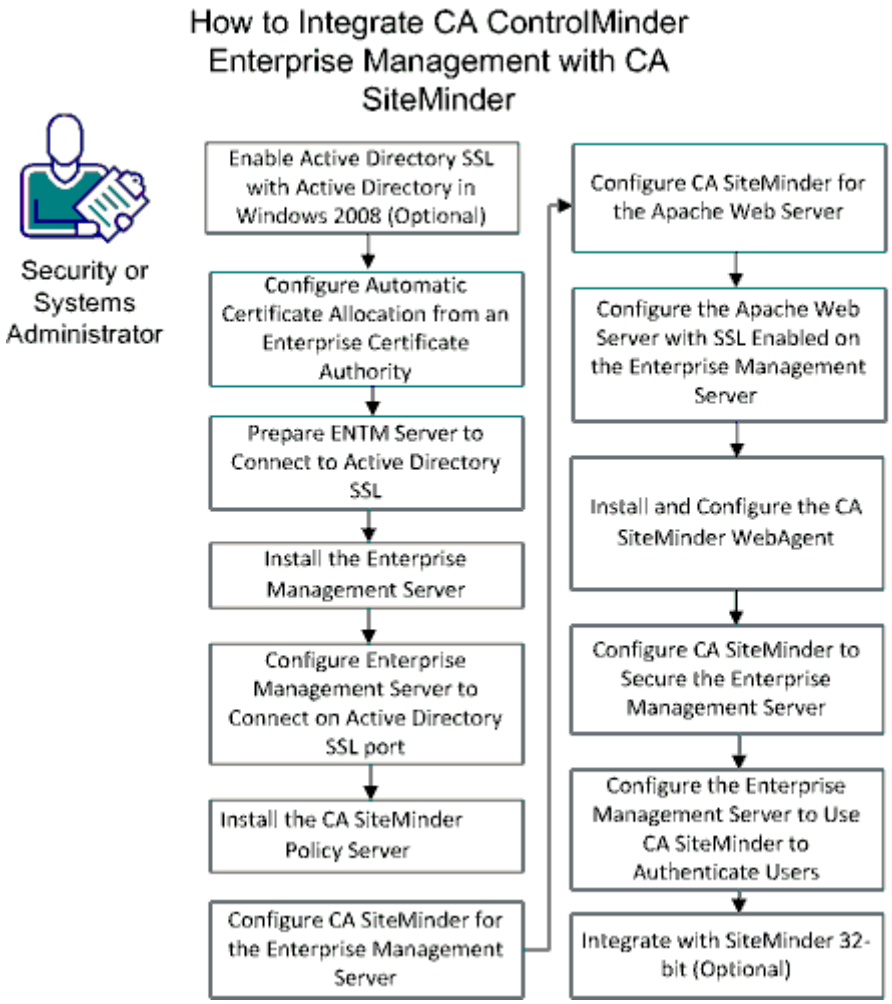
The following diagram illustrates how CA SiteMinder authenticates and authorizes CA ControlMinder users to log in to CA Access Control Enterprise Management:



How to Integrate with CA SiteMinder

You can integrate CA Access Control Enterprise Management with CA SiteMinder to leverage CA SiteMinder advanced user authentication and authorization capabilities.

The following diagram illustrates how a system or a security administrator integrates CA Access Control Enterprise Management with CA SiteMinder:



Follow these steps:

1. Enable Active Directory SSL with Active Directory in Windows 2008 (see page 64) (Optional)
2. Configure Automatic Certificate Allocation from an Enterprise Certificate Authority (see page 65)
3. Prepare Enterprise Management Server to connect to Active Directory SSL (see page 66)
4. Install the Enterprise Management Server (see page 67)

   Note: Before you install the Enterprise Management Server, prepare the computer by installing and configuring the prerequisites.
5. Configure Enterprise Management Server to connect on Active Directory SSL port (see page 72)
6. Install the CA SiteMinder Policy Server (see page 74)
7. Configure CA SiteMinder for the Enterprise Management Server (see page 75)
8. Configure the Apache Web Server Proxy Plug In on the Enterprise Management Server (see page 76)
9. Configure CA SiteMinder for the Apache Web Server (see page 78)
10. Configure the CA SiteMinder Web Agent (see page 79)
11. Configure CA SiteMinder to Secure the Enterprise Management Server (see page 80)
12. Configure the Enterprise Management Server to Use CA SiteMinder To Authenticate Users (see page 82)
13. Integrate with CA SiteMinder 32-bit (see page 85)

Note: For more information about CA SiteMinder Policy Server, Web Agent, and Administrator UI, see the CA SiteMinder documentation.

Enable Active Directory SSL with Active Directory in Windows 2008 (Optional)

To encrypt the communication between CA ControlMinder Enterprise Management and users when using Active Directory, configure Enterprise Management to use SSL.

Note: This step is optional if you are using Active Directory on Windows 2008.

Follow these steps:

1. On the Active Directory Computer, open Server Manager. Select Roles and Add Roles from the drop-down menu and click Next.

   The Add Roles Wizard Before you Begin Window opens.

2. Complete the wizard as follows:

   a. Check the Skip this page by default box and click Next.

   b. Select Active Directory Certificate Services and Click Next.

      The Select Role Services window opens.

   c. Select Certification Authority and click Next.

      The Specify Setup Type window opens.

   d. Select Enterprise and click Next.

      The Specify CA Type window opens.

   e. Select Root CA and click Next.

      The Set Up Private Key window opens.

   f. Select Create a new private key and click Next.

      The Configure Cryptography for CA window opens.

   g. Select the appropriate cryptographic service provider, hash algorithm, and key length and click Next.

      The Configure CA Name window opens.

   h. Enter a common name and click Next.

      The Validity Period screen opens.

   i. Use the default validity period (five years) and click Next.

      The Certificate Database screen opens.

   j. Use the default certificate database and login location and click Next.

      The Confirm Installation Selections screen opens.

   k. Review the installation selections and click Install.

      The roles are installed and the installation is complete.

3. Click Finish and restart the computer.
4. Click Start, select Administrative Tools, and Certification Authority.

   The Certification Authority application is launched and the Certificate Authority window opens.
5. In the Certification Authority drop-down menu on the left, locate your certificate in the Certificates folder to confirm that a certificate is issued.

Configure Automatic Certificate Allocation from an Enterprise Certificate Authority

You can use auto-enrollment to install computer certificates. For the automatic allocation of computer certificates, configure the Group Policy on the Active Directory domain.

Follow these steps:

1. On the domain controller, open the Active Directory Users and Computers console.
2. Double-click Active Directory Users and Computers, right-click your CA domain name, and click Properties.
3. On the Group Policy tab, click Default Domain Policy and Edit.
4. Navigate to Computer Configuration, Windows Settings, Security Settings, Public Key Policies, Automatic Certificate Request Settings.
5. Right-click Automatic Certificate Request Settings.
6. Select New, and click Automatic Certificate Request.

   The Automatic Certificate Request wizard opens.
7. Click Next.
8. In Certificate templates, click Computer and Next.

   Your enterprise root CA appears on the list.
9. Click CA, Next, and Finish.

   You can now import certificates into Enterprise Management. To create a computer certificate for the CA computer, type the following command at the command prompt:

   ```
   gpupdate /target:Computer.
   ```

Prepare Enterprise Management Server to connect to Active Directory SSL

When working with Active Directory, you can configure CA ControlMinder Enterprise Management to use SSL to encrypt the communication between Enterprise Management and users.

Follow these steps:

1. On the Active Directory (AD) computer, do the following:

   A. Copy the ldp.exe file from “c:\Windows\system32\” and paste it in the same location on the Enterprise Management Server.

   B. Copy the ldp.exe.mui file from “C:\Windows\System32\en-US” and paste it in the same location on the Enterprise Management Server.

   Note: These steps are required to start the ldp.exe tool on the Enterprise Management server.

2. Click Start, Run, and type ldp.exe.

   The ldp.exe connection Window opens.

3. Click Connection and Connect.

   The Connect screen opens.

4. Enter your Active Directory hostname and Non-SSL port number (For example: Server:ad1.forward.inc, Port: 389) and click OK.

   The connection is complete.

5. Check the SSL box and click OK.

   The connection to the Active Directory is confirmed.

   Note: Before you check the Active Directory SSL connection, import the Active Directory certificate and install it in Root Certificate on the Enterprise Management server. To import the AD certificate, SSL must be configured on your Active Directory. For more information, refer to the *Implementation Guide*.

6. On the Active Directory computer, click Start, Administrative Tools, Certification Authority.

7. Click Certification, right click RootCA, and click Properties from the drop-down menu.

   The RootCA Properties window opens.

8. Click the View Certificate button.

9. On the Details tab, click the Copy to File button.

   The Certificate Export Wizard opens.

10. Complete the Certificate Export Wizard.

    When the Certificate Export wizard is complete, the Certificate file is copied to your Active Directory computer.

11. Browse to the certificate location on the Active Directory computer and copy the certificate file to your Enterprise Management Server.

12. On your Enterprise Management Server, double-click the copied certificate.

13. Click Install Certificate Wizard and click Next.

14. Select Place all certificates in the following store and click Browse.

    The Select Certificate Store window opens.

15. Select Trusted Root Certification Authorities, Click OK, and Next.

    The Completing the Certificate Import Wizard window opens.

16. Click Finish and OK.

    The Certificate Import wizard is complete.

17. To check the SSL Active Directory connection, select Start, Run, ldp.exe on the Enterprise Management Server.

    The ldp.exe connection Window opens.

18. Click Connection in the tool bar and click Connect.

    The Connect window opens.

19. Specify the Server and SSL port number, check the SSL box, and click OK.

    The ldaps://(server name) window opens confirming the connection to the Active Directory is successful.

Install CA Access Control Enterprise Management on Windows

Installing CA Access Control Enterprise Management installs all the Enterprise Management Server components. Prepare the Enterprise Management Server before you install CA Access Control Enterprise Management.

We recommend that you use the Prerequisite Kit installer to initiate the CA Access Control Enterprise Management installation. This installer installs the prerequisite third-party software and then starts the CA Access Control Enterprise Management installation.

Note: You cannot install CA Access Control Enterprise Management by network install. Copy the entire contents of the Disk 1 directory of the CA Access Control Server Components DVD to your installation directory or map a drive to the DVD instead.

Follow these steps:

1. Stop JBoss Application Server if it is running.
2. Stop CA ControlMinder services if you are installing CA Access Control Enterprise Management on a computer that already has CA ControlMinder installed.
3. Insert the CA Access Control Server Components DVD for Windows into your optical disc drive.
4. Expand the Components folder in the Product Explorer, select CA Access Control Enterprise Management, then click Install.

   The InstallAnywhere installation program starts.

   a. (Optional) Specify the full pathname of a custom FIPS key to use during the installation.

   b. Open a command prompt window and navigate to the CA Access Control Enterprise Management installation executable on the CA Access Control Server Components DVD for Windows. This file is located under:

      `\EnterpriseMgmt\Disk1\InstData\NoVM`

   c. Run the CA Access Control Enterprise Management install executable with the following argument:

      `-DFIPS_KEY=`*`full_pathname_to_FIPS_key`*

      For example, to install with a custom FIPS key located at C:\tmp\FIPS.key:

      ```
      E:\EnterpriseMgmt\Disk1\InstData\NoVM\install_EntM_r125.exe
      -DFIPS_KEY=C:\tmp\FIPSkey.dat
      ```

   Important! If you install CA Access Control Enterprise Management for High Availability, specify the same FIPS key on the primary and secondary Enterprise Management Servers. Specify a custom FIPS key if you install CA Access Control Enterprise Management for High Availability with FIPS support.

   The InstallAnywhere installation program starts.

5. Complete the wizard as required. The following installation inputs are not self-explanatory:

   Choose Install Folder

   Defines the full path of the installation folder.

   Default: \ProgramFiles\CA\AccessControlServer\

   Note: On 64 bit operating systems the default installation folder is:

   `\Program Files(x86)\CA\AccessControlServer\`

Java Development Kit (JDK)

Defines the location of an existing JDK.

Note: If you launch the CA Access Control Enterprise Management installation immediately after you use the CA Access Control Third Party Component DVDs to install the prerequisite software, this wizard page does not appear. The installation utility configures the installation settings on this page based on the values you provided in the prerequisite software installation process.

JBoss Application Server Information

Defines the JBoss instance that you want to install the application on.

To do this, define the:

- JBoss folder, which is the top directory where you have JBoss installed.

  For example, C:\jboss-4.2.3.GA on Windows or /opt/jboss-4.2.3.GA on Solaris.

- URL, which is the IP address or host name of the computer you are installing on.
- Port JBoss uses.
- Port JBoss uses for secure communications (HTTPS).
- Naming port number.

Note: If you launch the CA Access Control Enterprise Management installation immediately after you use the CA Access Control Third Party Component DVDs to install the prerequisite software, this wizard page does not appear. The installation utility configures the installation settings on this page based on the values you provided in the prerequisite software installation process.

Communication Password

(Primary Enterprise Management Server Only) Defines the password used for CA ControlMinder Enterprise Management Server inter-component communication.

Note: CA Access Control Enterprise Management uses the communication password to manage the Message Queue keystore and administrator account, handle communication between CA Access Control Enterprise Management and the endpoints and manage the Java Connection Server.

Database Information

Defines the connection details to the RDBMS:

- **Database Type**—Specifies a supported RDBMS.
- **Host Name**—Defines the name of the host where you have the RDBMS installed.
- **Port Number**—Defines the port used by the RDBMS you specified. The installation program provides the default port for your RDBMS.

- **Service Name**—(Oracle) Defines the name that identifies your RDBMS on the system. For example, for Oracle Database 10g this is *orcl* by default.
- **Database Name**—(MS SQL) Defines the name of the database you created.
- **Username**—Defines the name of the user that you created when you prepared the database.

  Note: You granted this user the appropriate database permissions when you prepared the database.
- **Password**—Defines the RDBMS password of the user that you created when you prepared the database.

The installation program checks the connection to the database before it continues.

User Store Type

Defines the user store type CA Access Control Enterprise Management uses. Select *one* of the following:

- **Embedded User Store**—CA Access Control Enterprise Management stores user information in the RDBMS.
- **Active Directory—**you specify the connection information details in the next screen.
- **Other User Store**—you specify the user store configuration information after the CA Access Control Enterprise Management installation completes.

Note: To deploy login authorization policies to UNAB, you must select either Active Directory or Other User Store as the user store. If you select Active Directory or Other User Store as the user store, you cannot create or delete users and groups in CA Access Control Enterprise Management. For more information about UNAB and Active Directory restrictions, see the *Enterprise Administration Guide*.

Active Directory Settings

Defines the Active Directory user store settings:

- **Host**—Defines the Domain Controller host name of Active Directory.
- **Port**—Defines the port used by default for LDAP queries against Active Directory, for example, 389.
- **Search Root**—Defines the search root, for example, ou=DomainName, DC=com.

  Note: Set the Search Root at least one node higher in the directory tree than the Distinguished Names (DNs) for the users specified for User DN and System User. Otherwise, Enterprise Management might launch without displaying any tabs.

- **User DN**—Defines the Active Directory user account name that is used to manage CA Access Control Enterprise Management. For example: CN=Administrator, cn=Users, DC=DomainName, DC=Com.

  Note: This user issues LDAP queries against Active Directory. You can choose to define a user with read-only privileges for this parameter. However, if you define a user with read-only privileges, you cannot assign admin roles or privileged access roles to users in CA Access Control Enterprise Management. Instead, you modify the member policy for each role to point to an Active Directory group.

- **Password**—Defines the password of the Active Directory user account that is used to manage CA Access Control Enterprise Management.

The installation program checks the connection to Active Directory before continuing.

Note: You can use the DSQUERY directory querying utility to discover the user Distinguished Name (User DN). You must run this query on the Active Directory server. For example:

```
dsquery user -name administrator
"CN=Administrator,CN=Users,DC=lab.DC=demo"
```

System User

(Active Directory only) Defines the DN of the Active Directory user who is assigned the System Manager admin role in CA Access Control Enterprise Management.

Example: CN=SystemUser, ou=OrganizationalUnit, DC=DomainName, DC=Com

Note: By default, a user with the System Manager admin role can perform, create, and manage all tasks in CA Access Control Enterprise Management. For more information about the System Manager admin role, see the *Enterprise Administration Guide*.

Administrator Password

(Embedded user store only) Defines the password of *superadmin*, the CA Access Control Enterprise Management administrator. Make a note of the password so you can log in to CA Access Control Enterprise Management when the installation is complete.

Note: In this step you create the superadmin user in the embedded user store. The superadmin user is assigned the System Manager admin role in CA Access Control Enterprise Management. You log in as superadmin the first time you log in to CA Access Control Enterprise Management. For more information about the System Manager admin role, see the *Enterprise Administration Guide*.

CA Access Control Enterprise Management is installed after you complete the wizard.

6. To complete the installation, reboot the computer.

   After you reboot the computer, you can configure CA Access Control Enterprise Management for your enterprise.

Configure Enterprise Management Server to connect on Active Dirctory SSL port

Follow these steps:

1. Stop the JBoss service and set the service Startup Type to Manual.
2. Navigate to the following directory:

   JBoss_HOME/default/deploy/IdentityMinder.ear/management_console.war/WEB-INF

3. Open the web.xml file in edit mode.
4. Set the <param-value>true</param-value> for the AccessFilter section and save and close.

   Note: This step is required to enable the CA Identity Manager Management console.

5. Start the JBoss service.
6. Using a Web browser, open the CA Identity Manager Management console and click Continue.
7. Click Directories, ac-dir, Export, and click then Save.
8. Specify the location where you want to save the ac-dir.xml file and back up the xml file.

9. Open one of the ac-dir.xml files in the edit mode and make the following changes:

   ```
   <LDAP searchroot="DC=cmlab,DC=ca,DC=corp" secure="true"/>
   <Connection host="KUMVI10-TEST.cmlab.ca.corp" port="636"/>
   <Container objectclass="top,organizationalUnit" attribute="ou"
   value=""/>
   ```

10. Click Directories, ac-dir, and the Update button.

11. Browse to the ac-dir.xml file you edited and click Finish.

    The ac-dir is updated with the new port values. Errors are noted at the bottom.

12. Click Continue.

13. Stop the JBoss service.

14. Back up the ssl.keystore file from the following location:

    JBoss_HOME`/server/default/deploy/IdentityMinder.ea/custom/ppm/truststore.`

15. Import the certificate into the JBoss key store with the following command:

    ```
    keytool -import -keystore
    "jBoss_HOME/server/default/deploy/IdentityMinder.ear/custom/ppm
    /truststore/ssl.keystore" -alias "<ALIAS NAME>" -file
    "<Certificate File Name>.cer"
    ```

16. Enter the certificate password,“secret”.

    Note: The certificate must be trusted during the import.

17. Update the run.bat file with the following line:
    ```
    set JAVA_OPTS=%JAVA_OPTS% -Xms256m –Xmx1408m
    -Djavax.net.ssl.trustStore="%SYSTEMDRIVE%\jboss-4.2.3.GA\server
    \default\deploy\IdentityMinder.ear\custom\ppm\truststore\ssl.ke
    ystore".
    ```

18. Save the file and start JBoss.

19. Using a web browser, open the CA Identity Manager Management Console.

20. Go to Directory, ac-dir to check and verify that your Enterprise Management environment is connecting with SSL.

21. Access the Enterprise Management URL with the SSL port and verify that you are able to log in to Enterprise Management.

Install the CA SiteMinder Policy Server

To manage the User Interface, use the installation wizards to install the following components:

- The CA SiteMinderAdministrative Prerequisites
- The Administrative User Interface (UI)
- The Policy server

Follow these steps:

1. From the Admin UI, double-click "adminui-pre-req-12.51-win32" and click Next.

   The Administrative UI Prerequisite Installer opens.

2. Complete the wizard.

   The Administrative UI Installer wizard opens.

3. Complete the Administrative UI Installer wizard.

   The Administrative UI installation is complete. The CA SiteMinder Administrative UI opens automatically and you are ready to install the Policy server.

4. In the Administrative UI, double-click "ca-ps-12.51-win32" and click Next.

   The Police Server Wizard is launched.

5. Complete the Policy Server Install wizard. The following installation inputs are not self-explanatory:

   - In the Choose Features window, select the Policy Store box.
   - In the Policy Store window, select the Relational Database box.
   - In the Choose Password Services window, select the Basic Password Services box.

   The Policy Serve installation is complete.

   Note: The initial login to the Admin UI requires registering the Admin UI with the Policy Server to create a trusted relationship between both components. To register the Admin UI with the Policy Server, run the XPSRegClient utility to supply the registration super user account name and Siteminder user password (*password*-adminui-setup). When you connect for the first time, the Policy Server verifies the credentials and it creates the trusted relationship with the Admin UI.

Configure CA SiteMinder for the Enterprise Management Server

The following procedure explains how you configure CA SiteMinder for the Enterprise Management Server to leverage CA SiteMinder advanced users authentication and authorization capabilities.

Follow these steps:

1. Complete the following using the CA SiteMinder Administrator interface:
    1. Go to Start, All Programs, CA, CA SiteMinder, CA SiteMinder Administrative UI.

        The CA SiteMinder Administrative UI opens, prompting the user for a user name and password.
    2. Log in to the CA SiteMinder Administrative UI.
    3. Select Infrastructure, Hosts, Host Configuration, Create Host Configuration, Create a copy of an object of type Host Configuration.
    4. Select the DefaultHostSettings object and click OK.
2. Complete the following fields:
    - **Name**—*acentmnode*-HCO
3. Move to the Configuration Values frame, click Add and enter the host name of the CA SiteMinder Policy Server as follows:

    Host: *policyserver.company.com*
4. Click Submit.

You have configured the agent object. Next, you install and configure the CA SiteMinder Web Agent.

Configure the Apache Web Server with SSL Enabled on the Enterprise Management Server

The steps below explain how you install the Enterprise Management Server on a Windows (2003, 2008, or 2012) Server.

First, use the wizard to install Apache HTTP Server 2.2.22.

Follow these steps:

1. To Configure Apache Web Server with SSL, run the "httpd-2.2.22-win32-x86-openssl-0.9.8t.msi" installer of apache2.x with openssl.
2. Complete the Apache HTTP Server 2.2 installation wizard as instructed. The following installation inputs are not self-explanatory:
   - **Server Information** - Use all default values.
   - **Select Type** - Select Typical.

   Note: To resolve a port conflict error, provide a unique port number in the next step.

Next, configure the Apache web server proxy plug-in:

Follow these steps:

1. Stop the JBoss application server on the Enterprise Management Server.
2. Navigate to the following directory:

   APACHE_HOME/conf

   APACHE_HOME

   The directory where the Apache web server is installed.
3. To enable the proxy modules and include the proxy configuration, edit the httpd.conf file:
   a. Uncomment the following lines:

   ```
   LoadModule proxy_module modules/mod_proxy.so
   LoadModule proxy_http_module modules/mod_proxy_http.so
   ServerName
   ```

   b. Add the following line at the end of the Global configuration section:

   ```
   Include conf/extra/httpd-proxy-entm.conf
   ```
4. Navigate to the following directory:

   APACHE_HOME/conf/extra

5. Create a file named httpd-proxy-entm.conf, and add the following content, then save and close the file:

```
# Proxy to CA AC ENTM
<IfModule proxy_module>
  <IfModule proxy_http_module>
       # /iam section BEGIN
    <Proxy /iam>
      Order allow,deny
      Allow from all
    </Proxy>
    ProxyPass /iam http://acentmnode.example.com:8080/iam
    ProxyPassReverse /iam
http://acentmnode.example.com:8080/iam
    ProxyPass /iam/ http://acentm.examplenode.com:8080/iam/
    ProxyPassReverse /iam/
http://acentmnode.example.com:8080/iam/
       # /iam section END
       # /castylesr5.1.1 section BEGIN
    <Proxy /castylesr5.1.1>
      Order allow,deny
      Allow from all
    </Proxy>
    ProxyPass /castylesr5.1.1
http://acentmnode.example.com:8080/castylesr5.1.1
    ProxyPassReverse /castylesr5.1.1
http://acentmnode.example.com:8080/castylesr5.1.1
    ProxyPass /castylesr5.1.1/
http://acentmnode.example.com:8080/castylesr5.1.1/
    ProxyPassReverse /castylesr5.1.1/
http://acentmnode.example.com:8080/castylesr5.1.1/
       # /castylesr5.1.1 section END
  </IfModule>
</IfModule>
```

   Note: Replace the *acentmnode.example.com:port* with the actual hostname and port of the server where you installed the Enterprise Management server.

6. Restart the Apache web server.

7. Start the JBoss application server.

8. To verify that the Apache web server forwards the requests successfully, browse to the Enterprise Management Server. Use the following URL:

   `http://enterprise_host:port/iam/ac`

You have configured the Apache web server proxy plug-in with SSL enabled on the Enterprise Management Server.

Configure CA SiteMinder for the Apache Web Server

After you configure the Apache web server proxy plug-in on the Enterprise Management Server, you configure CA SiteMinder for the Apache web server

Follow these steps:

1. In the CA SiteMinder Administrator interface, select Infrastructure, Agent, Agents, Create Agent, Create a new object of type Agent.
2. Complete the following fields and click Submit:
   - **Name**—webserver-agent
   - **Description**—web server node web agent
   - **Select an Agent type**—SiteMinder
   - **Agent type**—web agent
   - **Supports 4.x Agents**—check

   You have configured the web agent object.
3. Select Infrastructure, Agents, Agent Configuration Objects, Create Agent Configuration, Create a copy of an object of type Agent Configuration.
4. Select ApacheDefaultSettings, click OK, and do the following:
   a. Complete the following field:
      - **Name**—webservernode-ACO

   b. From the Parameters list, edit the #DefaultAgentName field and remove the # character in the name value.

   c. Set the agent name value as follows:
      - **DefaultAgentName**—webserver-agent

   d. Edit #LogoffUri and #LogOffURI and remove the # characters in the name value.

   e. Set the value as follows:
      - **LogoffUri**—/iam/logout.jsp
      - **LogOffURI**—/iam/logout.jsp

   Note: For more information about the agent parameters, see the CA SiteMinder Agent Configuration Guide.
5. Click Submit.

   You have created the agent configuration object.

Install and Configure the CA SiteMinder Web Agent

The following explains how to install and configure the CA SiteMinder WebAgent for the Apache web server.

Follow these steps:

1. Do the following to install the CA SiteMinder WebAgent:
   a. Install the CA SiteMinder WebAgent on your Enterprise Management server using the "ca-wa-12.51-win32.exe" file.
   b. Complete the installation wizard as instructed and restart the computer.

      The CA SiteMinder web agent is installed.
2. Next, do the following to Configure the CA SiteMinder WebAgent using the host and agent objects configuration that you previously defined:
   a. Go to Start, All Programs, CA, SiteMinder, Web Agent Configuration Wizard.
   b. When prompted, select: Yes, I would like to do Host Registration now.
   c. Enter the CA SiteMinder Admin user name and password.
   d. In the Trust Host Name and Configuration Object window, do the following steps:
      a. Define the Trusted Host Name as the Enterprise Management Server that you are registering with CA SiteMinder.
      b. Define the Host Configuration Object that you previously created. Example: webservernode-HCO
   e. Define the Policy Server IP address and click Add.
   f. Select FIPS Compatibility Mode.
   g. Click Next at Host Configuration File Location.

      The Web Agent registers with the CA SiteMinder server.
   h. Select Web Server:Apache 2.2.xx.
   i. Select the Agent Configuration Object that you previously created on the CA SiteMinder server.
   j. Select SSL Authentication as "No Advanced Authentication".
   k. Select Yes to enable the Web Agent.

      The Web Agent installs.
   l. Restart the Apache web server

      The CA SiteMinder web agent is configured.

Configure CA SiteMinder to Secure the Enterprise Management Server

The following explains how to configure CA SiteMinder to secure the Enterprise Management Server log in session. Configure the user store so that CA SiteMinder secures the authentication scheme and the domain policy.

Follow these steps:

1. Do the following:
   a. Go to Start, All Programs, CA, SiteMinder, CA SiteMinder Administrative UI.

      The CA SiteMinder Administrative UI opens prompting you for a username and password.

   b. Enter the credentials for the CA SiteMinder administrator user account.
   c. Select Infrastructure, Directory, User Directory, Create User Directory.
   d. Complete the following fields in the General frame:
      - **Name**—ac-dir
      - **Description**—Access Control User Store
   e. Move to the Directory Setup frame and complete the following fields:
      - **Namespace**—LDAP
      - **Server**—*directory_hostname:port*
   f. Move to the Administrator Credentials and complete the following fields:
      - **Require credentials**—check
      - **Username**—Bind user full DN
      - **Password**—*password*
      - **Confirm Password**—*password*
   g. Move to the LDAP Settings frame and complete the following fields:
      - **Root**—*searchroot*
      - **Scope**—Sub-Tree
      - **Start**—(&(sAMAccountName=
      - **End**—)(objectclass=top)(objectclass=person)(objectclass=organizationalperson)(objectclass=user))
   h. Move to the User Attributes frame and complete the following fields:
      - **Universal ID**—Attribute name corresponding to %USER_ID%
2. Click Submit.

   CA SiteMinder creates the user directory object.
3. Select View User Directory, ac-dir, View Content.

The user store entries appear.

4. Select Infrastructure, Authentication, Authentication Scheme, Create Authentication Scheme, complete the following fields:
   - **Name**—ac-basic-auth
   - **Description—**CA Access Control Enterprise Management basic authentication
   - **Authentication Scheme Type**—Basic Template
   - **Protection Level**—5
   - **Library**—smauthdir
5. Click Submit

   CA SiteMinder creates the authentication scheme object.
6. Select Policies, Domains, Domain, Create Domain.
7. Specify the name of the domain.
8. Move to the User Directories frame and clicks Add/Remove.
9. Move ac-dir from the Available Members list to the Selected Members list, and then click OK.
10. Select Policy, Realms, Create Realm and complete the following fields:
    - **Name**—ac-realm
    - **Agent**—*webserver*-agent
    - **Resource Filter**—/iam/
    - **Default Resource Protection**—Protected
    - **Authentication Scheme**—ac-basic-auth
11. Move to the Rules frame, select Create and complete the following fields:
    - **Name**—ac-rule
    - **Resource**—*
    - **Allow Access**—select
    - **Web Agent Actions**—Get, Post
12. Click OK and Finish.
13. Select Policies, Domain, Domain Policies, Create, and complete the following field in the General tab:
    - **Name**—ac-policy
14. Move to the Users tab and select Add All

15. Move to the Rules tab, click Add Rule, select ac-rule, and click OK.
16. Click OK and Submit to create the domain.

You have configured the domain and realm policy.

Configure the Enterprise Management Server to Use CA SiteMinder To Authenticate Users

The following steps explain how to configure the Enterprise Management Server for CA SiteMinder integration.

Note: Complete the following steps on Windows x64 operating system before you begin this procedure:

- Install 32bit Java from DVD06142621E\JDK-1.6.30_x86
- To point to the 32bit Java, locate the run_idm.bat file in \jboss-4.2.3.GA\bin and modify the JAVA_HOME value.
- Copy the following files from \Program Files (x86)\CA\webagent\java: `smconapi.jar, smjavaagentapi.jar, smjavasdk2.jar`
- Place the files in the following directory: \jboss-4.2.3.GA\server\default\lib

Follow these steps:

1. On the Enterprise Management Server:
   a. Stop the JBoss application server.
   b. Navigate to the following directory, where *JBOSS_HOME* is the directory where you installed JBoss:

      JBOSS_HOME`/server/default/deploy/IdentityMinder.ear/user_console.war/WEB-INF`

   c. Open the web.xml file and locate the FrameworkAuthFilter section.
   d. Modify the value to false, then save and close the file. For example:

```
<filter>
  <filter-name>FrameworkAuthFilter</filter-name>

<filter-class>com.netegrity.webapp.authentication.FrameworkLoginFilter</filter-class>
  <init-param>
    <param-name>Enable</param-name>
    <param-value>false</param-value>
  </init-param>
</filter>
```

2. Navigate to the following directory:

   JBOSS_HOME/server/default/deploy/IdentityMinder.ear/policyserver.rar/META-INF

3. Do the following:

   a. Open the ra.xml file and set the value to true to enable the connection, as follows:

   ```
   <config-property>
    <config-property-name>Enabled</config-property-name>

   <config-property-type>java.lang.String</config-property-type>
    <config-property-value>true</config-property-value>
   </config-property>
   ```

   b. Configure the FIPS mode according to the CA SiteMinder Policy Server configuration, as follows:

   ```
   <config-property>
     <config-property-name>FIPSMode</config-property-name>

   <config-property-type>java.lang.String</config-property-type>
     <config-property-value>false</config-property-value>
   </config-property>
   ```

   c. Define the CA SiteMinder Policy Server hostname, IP address, and port number, as follows:

   ```
   <config-property>

   <config-property-name>ConnectionURL</config-property-name>

   <config-property-type>java.lang.String</config-property-type>

   <config-property-value>policyservernode.example.com,44441,44442,44443</config-property-value>
   </config-property>
   ```

   d. Define the administrative user account settings, as follows:

   ```
   <config-property>
     <config-property-name>UserName</config-property-name>

   <config-property-type>java.lang.String</config-property-type>
     <config-property-value>siteminder</config-property-value>
   </config-property
   ```

e. Run the password tool that is located in the following directory:

```
/CA/AccessControlServer/IAMSuite/AccessControl/tools/PasswordTool
```

For example:
pwdTools -FIPS -p <clear_*text_password*> -k JBoss_HOME/server/default/deploy/IdentityMinder.ear/config/com/netegrity/config/keys/FIPSKey.dat

f. Define AdminSecret as the output of the following encryption command,as follows:

```
<config-property>
  <config-property-name>AdminSecret</config-property-name>

<config-property-type>java.lang.String</config-property-type>

<config-property-value>{AES}:gSez2/BhDGzEKWvFmzca4w==</config-property-value>
</config-property>
```

g. Define AgentName as the CA Access Control Enterprise Management node agent name:

```
<config-property>
  <config-property-name>AgentName</config-property-name>

<config-property-type>java.lang.String</config-property-type>

<config-property-value>webserver-agent</config-property-value>
</config-property>
```

h. Encrypt the CA Access Control Enterprise Management shared secret using the following password tool command:
ACServerInstallDir/IAMSuite/AccessControl/tools/Passwordtool/pwdtools.bat -FIPS -p <*your_shared_secret*> -k *JBoss_HOME*/server/default/deploy/IdentityMinder.ear/config/com/netegrity/config/keys/FIPSKey.dat

i. Define AgentSecret as the encrypted output of the following command:

```
<config-property>
  <config-property-name>AgentSecret</config-property-name>

<config-property-type>java.lang.String</config-property-typ
e>

<config-property-value>{AES}:gSez2/BhDGzEKWvFmzca4w==</conf
ig-property-value>
</config-property>
```

4. Save and close the file.
5. Navigate to the following directory:

   JBoss_HOME/bin

6. Edit the run_idm.bat and set the %PATH% variable to the JBoss installation path: For example:

```
set
PATH=%PATH%;C:\jboss-4.2.3\server\default\deploy\IdentityMinder
.ear\library;%SystemRoot%\SYSTEM32;%SystemRoot%;%SystemRoot%\SY
STEM32\WBEM
```

7. Save and close the file.
8. Start the JBoss application server.

   You have configured the Enterprise Management Server for CA SiteMinder integration. You can now browse to the CA Access Control Enterprise Management URL and verify that CA SiteMinder secures the login session.

Integrating with CA SiteMinder 32-bit

To integrate CA ControlMinder 12.8 64-bit with CA SiteMinder 32-bit, follow the basic configuration steps excluding the step to configure the WebAgent. After completing the basic configuration, do the following steps to allow the CA ControlMinder 64-bit dlls to communicate with CA SiteMinder 32-bit dll files:

Follow these steps:

1. Download the latest web agent version (12.51 CR01 32-bit).
2. Install the WebAgent and continue with the configuration as instructed skipping the Install WebAgent step.

   Note: After the installation, JBoss will produce errors due to a DLL mismatch.

3. Stop the JBoss service.
4. Install the latest CA SiteMinder SDK (12.51 CR01) on the JBoss computer.

5. After the installation, navigate to the folder \Program Files (x86)\CA\sdk and copy all DLLs from the bin64 folder to *JBoss folder*/server/default/deploy/IdentityMinder.ear/library.
6. Copy the contents of the lib64 folder to *JBoss folder*/server/default/deploy/IdentityMinder.ear/library.
7. Copy the following five jars from java64 to *JBoss folder*/server/default/deploy/IdentityMinder.ear/library:
   - smagentapi.jar
   - smjavaagentapi.jar
   - SmJavaApi.jar
   - smjavasdk2.jar
   - imsjavasdk.jar
8. Remove the msvcr71.dll if it appears in the /server/default/deploy/IdentityMinder.ear/library.
9. Ensure that the first path of the PATH env variable is \Program Files (x86)\CA\sdk\bin64.
10. Download the latest web agent version (12.51 CR01 64-bit).
11. Install but do not configure the WebAgent (Select Configure Later).
12. Restart the computer.
13. Remove the \Program Files\CA\webagent\win32\bin path from the PATH env variable.
14. Restart the Apache server.

Chapter 8: CA ControlMinder REST API

This section contains the following topics:

REST-based API

REST (Representational State Transfer) describes an architectural style characteristic of software that relies on the inherent properties of hypermedia to create and modify the state of an object that is accessible at a URL.

In a RESTful scenario, documents (representing the state of an object) are passed back and forth between a client and a service with the assumption that neither knows anything about any entity other than what is in a single request or response.

To get the schema for the REST-based API, navigate to the following URL and View the source of the empty page:

`https://hostname:18443/iam/api/1.0/restapi/schemas`

Note: For more information about the schema, see the examples in this section.

You can use the REST requests to communicate between your custom, or third-party programs with the Shared Accounts Management database by-passing the Enterprise Management Server User Interface.

HTTP Verbs

Where possible, CA ControlMinder REST API uses the following appropriate HTTP verbs for each action.

GET

Used for retrieving accounts, endpoints, and account requests.

POST

Used for creating accounts, endpoints, and account requests.

PUT

Used for updating accounts, endpoints, and account requests.

DELETE

Used for deleting accounts, endpoints, and account requests.

Examples: HTTP Operations

The following are schema examples for the supported REST-based API commands:

- HTTP POST:

```
POST /iam/api/1.0/restapi/environments/ac/endpoints/endpointname/accounts
HTTP/1.1
Content-type: application/xml; charset=UTF-8
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Cache-Control: no-cache
Pragma: no-cache
Host: 10.112.196.244
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Content-Length: 79
```

The following example is an HTTP POST body content to create an account:

```
<Account>
<Name>myaccount_name</Name>
<Disconnected>true</Disconnected>
<Type>Shared</Type>
<Container>MS SQL Logins</Container>
<PasswordPolicy>default password policy</PasswordPolicy>
<PasswordState>CheckedIn</PasswordState>
<Exclusive>false</Exclusive>
<ChangePasswordOnCheckOut>false</ChangePasswordOnCheckOut>
<ChangePasswordOnCheckIn>false</ChangePasswordOnCheckIn>
<LoginApplicationCheckoutOnly>false</LoginApplicationCheckoutOnly>
<Owner ownerType="Group">my_group</Owner>
</Account>
```

- HTTP GET:

```
GET /iam/api/1.0/restapi/environments/ac/endpoints/endpointname HTTP/1.1
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host: 10.112.196.169:9998
```

- HTTP PUT:

```
PUT /iam/api/1.0/restapi/environments/ac/endpoints/endpointname/accounts
HTTP/1.1
Content-type: application/xml; charset=UTF-8
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Cache-Control: no-cache
Pragma: no-cache
Host: 10.112.196.244
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Content-Length: 959
```

The following example is an HTTP PUT body content to update an account:

```
<Account>
```

```
<Name>myaccount_name</Name>
<Disconnected>true</Disconnected>
<Type>Shared</Type>
<Container>MS SQL Logins</Container>
<PasswordPolicy>default password policy</PasswordPolicy>
<PasswordState>CheckedIn</PasswordState>
<Exclusive>false</Exclusive>
<ChangePasswordOnCheckOut>false</ChangePasswordOnCheckOut>
<ChangePasswordOnCheckIn>false</ChangePasswordOnCheckIn>
<LoginApplicationCheckoutOnly>false</LoginApplicationCheckoutOnly>
<Owner ownerType="Group">my_group</Owner>
</Account>
```

- HTTP DELETE:

```
DELETE /iam/api/1.0/restapi/environments/ac/endpoints/endpointname HTTP/1.1
Content-type: application/xml; charset=UTF-8
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Cache-Control: no-cache
Pragma: no-cache
Host: 10.112.196.244
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
```

REST-based Authentication

The CA ControlMinder REST requests include the authentication information as part of the request information. CA ControlMinder supports the HTTP basic authentication method. You can use the following basic authentication, for example:

```
Authorization: Basic
c3VwZXJhZG1pbjpkZWZhdWx0c3VwZXJhZG1pbjpkZWZhdWx0
```

The previous example represents the Base 64 encoding of the user “superadmin” and the password “default”.

Get Schema

To retrieve the account requests schema, send the HTTP GET request to the following URL:

`https://<host_name>:18443/iam/api/1.0/restapi/schemas`

host_name

Specifies the host name.

Create an Account

To create an account, send the HTTP POST request to the following URL:

`https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts`

host_name

Specifies the host name.

endpoint_name

Specifies the endpoint name.

The following example shows the HTTP body content to create an account:

```
<Account>
<Name>myaccount_name</Name>
<Disconnected>true</Disconnected>
<Type>Shared</Type>
<Container>MS SQL Logins</Container>
<PasswordPolicy>default password policy</PasswordPolicy>
<PasswordState>CheckedIn</PasswordState>
<Exclusive>false</Exclusive>
<ChangePasswordOnCheckOut>false</ChangePasswordOnCheckOut>
<ChangePasswordOnCheckIn>false</ChangePasswordOnCheckIn>
<LoginApplicationCheckoutOnly>false</LoginApplicationCheckoutOnly>
<Owner ownerType="Group">my_group</Owner>
</Account>
```

Name

Specifies the account name.

Disconnected

Specifies if the account is disconnected.

Type

Specifies the type of account.

Container

Specifies the container.

PasswordPolicy

Specifies the password policy that is implemented for the account.

PasswordState

Specifies the password state of the account.

Exclusive

Specifies if the account is exclusive or not.

ChangePasswordOnCheckOut

Specifies if the password is changed when the account is checked out.

ChangePasswordOnCheckIn

Specifies if the password is changed when the account is checked in.

LoginApplicationCheckoutOnly

Specifies if the login application checks out the account.

Owner

Specifies the owner type.

Update an Account

To update an account, send the HTTP PUT request to the following URL:

`https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>`

host_name

Specifies the host name.

endpoint_name

Specifies the endpoint name.

account_name

Specifies the account name.

The following example shows the HTTP body content to update an account:

```
<Account>
<Name>myaccount_name</Name>
<Disconnected>true</Disconnected>
<Type>Shared</Type>
<Container>MS SQL Logins</Container>
<PasswordPolicy>default password policy</PasswordPolicy>
<PasswordState>CheckedIn</PasswordState>
<Exclusive>false</Exclusive>
<ChangePasswordOnCheckOut>false</ChangePasswordOnCheckOut>
<ChangePasswordOnCheckIn>false</ChangePasswordOnCheckIn>
<LoginApplicationCheckoutOnly>false</LoginApplicationCheckoutOnly>
<Owner ownerType="Group">my_group</Owner>
</Account>
```

Name

Specifies the account name.

Disconnected

Specifies if the account is disconnected.

Type

Specifies the type of account.

Container

Specifies the container.

PasswordPolicy

Specifies the password policy that is implemented for the account.

PasswordState

Specifies the password state of the account.

Exclusive

Specifies if the account is exclusive or not.

ChangePasswordOnCheckOut

Specifies if the password is changed when the account is checked out.

ChangePasswordOnCheckIn

Specifies if the password is changed when the account is checked in.

LoginApplicationCheckoutOnly

Specifies if the login application checks out the account.

Owner

Specifies the owner type.

Delete an Account

To delete an account, send the HTTP DELETE request to the following URL:

`https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>`

host_name

Specifies the host name.

endpoint_name

Specifies the endpoint name.

account_name

Specifies the account name.

Get an Account

Use the GET command to retrieve a specific account.

Note: If the account is checked out, you can view the password.

To retrieve a specific account, send the HTTP GET request to the following URL:

`https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>`

Use the account-container query parameter to specify a container for supporting endpoints while retrieving accounts.

To retrieve accounts which have a non-default account-container such as an Active Directory, send the HTTP GET request to the following URL:

`https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>`

host_name

Specifies the host name.

endpoint_name

Specifies the endpoint name.

account_name

Specifies the account name.

Get Accounts

To retrieve privileged accounts on an endpoint, send the HTTP GET request to the following URL:

`https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts`

host_name

Specifies the host name.

endpoint_name

Specifies the endpoint name.

Check In an Account

To check in an account, send the HTTP PUT request to the following URL:

`https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>`

host_name

Specifies the host name.

endpoint_name

Specifies the endpoint name.

account_name

Specifies the account name.

The following example shows the HTTP body content to check in an account:

```
<Account>

<PasswordState>Checked In</PasswordState>

</Account>
```

Checkout an Account

To check out an account, send the HTTP PUT request to the following URL:

`https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>`

host_name

Specifies the host name.

endpoint_name

Specifies the endpoint name.

account_name

Specifies the account name.

The following example shows the HTTP body content to check out an account:

```
<Account>

<PasswordState>Checked Out</PasswordState>

</Account>
```

Breakglass Accounts

A user performs a break glass check out when they need immediate access to an account that they are not authorized to manage.

To break glass an account, send the HTTP request to the following URL:

`https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>?breakglass-accounts=true`

host_name

Specifies the host name.

endpoint_name

Specifies the endpoint name.

account_name

Specifies the account name.

The following example shows the HTTP body content to break glass an account:

```
<Account>

<PasswordState justification="my
justification">BreakGlass</PasswordState>

</Account>
```

Note: Only users with the break glass privileged access role can perform the break glass process.

Reset Password

To reset the password manually, send the HTTP PUT request to the following URL:

`https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>`

host_name

Specifies the host name.

endpoint_name

Specifies the endpoint name.

account_name

Specifies the account name.

The following example shows the HTTP body content to reset the password:

```
<Account>

<Password auto="false">password</Password>

</Account>
```

Reset Password Auto

To reset the password to an account automatically, send the HTTP PUT request to the following URL:

`https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>`

host_name

Specifies the host name.

endpoint_name

Specifies the endpoint name.

account_name

Specifies the account name.

The following example shows the HTTP body content to reset the password automatically:

```
<Account>

<Password auto="true"/>

</Account>
```

Create an Endpoint

To create an endpoint, send the HTTP POST request to the following URL:

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints
```

host_name

Specifies the host name.

The following example shows the HTTP body content to create an endpoint:

```
<Endpoint>
   <Name>endpoint_name</Name>
   <EndpointType>MS SQL Server</EndpointType>
   <EndpointTypeProperties>
      <UserLogin>user1</UserLogin>
      <URL>URL Value</URL>
      <Host>Endpoint_Host_Address</Host>
      <Password>User_Password</Password>
   </EndpointTypeProperties>
   <AdministrativeAdvanced>false</AdministrativeAdvanced>

</Endpoint>
```

Name

Specifies the endpoint name.

EndpointType

Specifies the endpoint type.

UserLogin

Specifies the user login for the endpoint.

URL

Specifies the URL Value for the endpoint.

Host

Specifies the endpoint host address.

Password

Specifies the password for the endpoint user that is specified in the UserLogin tag.

AdministrativeAdvanced

Specifies if the endpoint is enabled for advanced administration.

Note: The *EndpointTypeProperties* tag is dynamic and determined by the input that is given for the *EndpointType* tag. See the get endpoint types (see page 102) topic for the description on how to get the property schema for dynamic endpoint type properties.

Update an Endpoint

To update an endpoint, send the HTTP PUT request to the following URL:

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints
```

host_name

Specifies the host name.

The following example shows the HTTP body content to update an endpoint:

```
<Endpoint>
    <Name>endpoint_name</Name>
    <EndpointType>Endpoint_type</EndpointType>
    <EndpointTypeProperties>
        <UserLogin>user1</UserLogin>
        <URL>URL Value</URL>
        <Host>Endpoint_Host_Address</Host>
        <Password>User_Password</Password>
    </EndpointTypeProperties>
<AdministrativeAdvanced>false</AdministrativeAdvanced>
</Endpoint>
```

Name

Specifies the endpoint name.

EndpointType

Specifies the endpoint type.

UserLogin

Specifies the user login for the endpoint.

URL

Specifies the URL Value for the endpoint.

Host

Specifies the endpoint host address.

Password

Specifies the password for the endpoint user that is specified in the UserLogin tag.

AdministrativeAdvanced

Specifies if the endpoint is enabled for advanced administration.

Delete an Endpoint

To delete an endpoint, send the HTTP DELETE request to the following URL:

`https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>`

host_name

Specifies the host name.

endpoint_name

Specifies the endpoint name.

Get Endpoint

To retrieve all the endpoints, send the HTTP GET request to the following URL:

`https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>`

host_name

Specifies the host name.

endpoint_name

Specifies the endpoint name.

Get Endpoints

Use the get endpoints command to retrieve all endpoints.

To retrieve all endpoints, send the HTTP GET request to the following URL:

`https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints`

host_name

Specifies the host name.

Get Endpoint Types

Use the get endpoint types command to retrieve all endpoint types.

To retrieve all endpoint types, send the HTTP GET request to the following URL:

`https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoint-types`

The EndpointTypeProperties tag is dynamic and determined by the input that is given for the EndpointType tag. Use the following URL to get the properties schema:

`https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoint-types/<host_name>/properties-schema`

host_name

Specifies the host name.

Create Account Request

To create an account request, send the HTTP POST request to the following URL:

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>/accountrequest
```

host_name

Specifies the host name.

endpoint_name

Specifies the endpoint name.

account_name

Specifies the account name.

The following example shows the HTTP body content to create an account request:

```
<AccountRequest>
    <StartTime>Start_Time</StartTime>
    <ValidUntilTime>Valid_Until_Time</ValidUntilTime>
    <User>
        <Name>user1</Name>
    </User>
    <Approver>
    <User>
        <Name>superadmin</Name>
    </User>
    </Approver>
    <Justification>user1 requests</Justification>

</AccountRequest>
```

StartTime

Specifies the start time from when a requester user can perform shared account request tasks.

Enter the date in the following format:
`yyyy-mm-ddThh:mm:sec`

ValidUntilTime

Specifies the valid time, after which the user cannot perform shared account request tasks.

Enter the date in the following format:
`yyyy-mm-ddThh:mm:sec`

Name

Specifies the user name of the requester.

<Approver><User>Name

Specifies the user name of the approver.

Justification

Specifies the justification comments.

Delete Account Request

To delete an account request, send the HTTP DELETE request to the following URL:

`https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>/accountrequest/<account_request_name>`

host_name

Specifies the host name.

endpoint_name

Specifies the endpoint name.

account_name

Specifies the account name.

account_request_name

Specifies the account request name.

Get Account Password to Request

To retrieve all the account passwords which a user can request, send the HTTP GET request to the following URL:

`https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts?to-request=true`

host_name

Specifies the host name.

endpoint_name

Specifies the endpoint name.

Get Account Request

To retrieve a specific account request, for example: *exc-113*, send the HTTP GET request to the following URL:

`https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>/accountrequests/exc-113`

To retrieve all account requests, which have access to the privileged account (account_name), send the HTTP GET request to the following URL:

`https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>/accountrequests`

To retrieve all account requests in the entire environment, send the HTTP GET request to the following URL:

`https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints?display=accountrequests`

host_name

Specifies the host name.

endpoint_name

Specifies the endpoint name.

account_name

Specifies the account name.