CA Access Control Premium Edition

Integration Guide for ObserveIT Enterprise

r12.5 SP3

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 Access Control product are provided "as is", for informational purposes only. They may need to be adjusted in specific environments and should not be used in production without testing and validating them before deploying them on a production system.

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

CA Product References

This document references the following CA products:

- CA Access Control Premium Edition
- CA Access Control
- CA Single Sign-On (CA 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 Service Desk Manager (formerly Unicenter Service Desk)
- CA Enterprise Log Manager
- CA Identity Manager

Documentation Conventions

The CA Access Control 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
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 Access Control documentation uses the following file location conventions:

- *ACInstallDir*—The default CA Access Control installation directory.
  - Windows—C:\Program Files\CA\AccessControl
  - UNIX—/opt/CA/AccessControl
- *ACSharedDir*—A default directory used by both UNAB and CA Access Control for UNIX.
  - UNIX—/opt/CA/AccessControlShared
- *ACServerInstallDir*—The default CA Access Control Enterprise Management installation directory.
  - Windows—C:\Program Files\CA\AccessControlServer
  - UNIX—/opt/CA/AccessControlServer
- *DistServerInstallDir*—The default Distribution Server installation directory.
  - Windows—C:\Program Files\CA\DistributionServer
  - UNIX—/opt/CA/DistributionServer
- *JBoss_HOME*—The default JBoss installation directory.
  - Windows—C:\jboss-4.2.3.GA
  - UNIX—/opt/jboss-4.2.3.GA

Contact CA

Contact CA Support

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

- 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

Provide Feedback

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

If you would like to provide feedback about CA product documentation, complete our short customer survey, which is available on the CA Support website at http://ca.com/docs.

Documentation Changes

This deliverable was added to the documentation in r12.5 SP3.

Contents

Chapter 1: Introduction

This section contains the following topics:

About this Guide

This guide instructs you how to integrate CA Access Control Premium Edition with the ObserveIT Enterprise session recording program. This guide explains the process and procedures that you do to record PUPM sessions.

This guide was written for security and system administrators using CA Access Control who want to take advantage of the ObserveIT Enterprise session recording program capabilities.

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

About ObserveIT Integration

The CA Access Control 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 obtain the ObserveIT Enterprise session logging program from ObserveIT Systems at the following link:

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

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

Chapter 2: Setting Up the Integration

This section contains the following topics:

How to Set Up the Integration

There are several steps you take to integrate CA Access Control with the ObserveIT Enterprise session recording software. At the end of the integration, all PUPM 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 PUPM 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 Access Control. After you prepare the ObserveIT Enterprise application server, the server is configured to start recording and saving PUPM sessions.

Do the following to prepare the integration:

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

   CA Access Control 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 PUPM 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.

Chapter 3: Logging PUPM Sessions

This section contains the following topics:

How Sessions Are Logged

Each PUPM 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 PUPM 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 PUPM 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 PUPM 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 PUPM 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.