



CA Technologies

CA ControlMinder™ Rapid Implementation Guide

Shared Account Management

Contents

References	4
CA ControlMinder References	4
Tibco References	4
Glossary	6
Executive summary	7
Introduction	7
CA ControlMinder Components	9
SAM User and Component Interaction	10
Initial Logon	10
Endpoint Creation	11
Privileged Account Creation	11
Endpoint Logon	12
Endpoint Logoff	12
Architecture	14
Preparing the Environment	15
Suggested Hardware and Software Components	15
Preparing the Database	16
Create MSSQL User	16
Create MSSQL Database	16
Table Sizing	18
Creating Users in Microsoft Active Directory	19
Collect Account DN	19
ENTM Installation	22
Load the Media Containing Required Third-Party Products	22
Install Pre-Requisite Software	23
Install ENTM	28
Installation Validation	36
SAM Endpoint Creation	37
Endpoint Creation	37
Windows Endpoint	39
Windows Endpoint – MS Active Directory Domain	47
UNIX SSH Endpoint	49
MS SQL Endpoint	53
Verify Created Endpoints	56
Privileged Accounts Discovery	58
ENTM Administration Role Scoping	63
Administration Roles	63
Privileged Access Roles	64
Changing the Scope of Default Roles	65
Setting Up Endpoint Tagging and Approvers	71
Tagging Setup	71
Approver Setup	74
Privilege Access Role Definition	76
Role Creation	77
Role Scoping	81
Role Verification	84
Advanced Topics	86

CA ControlMinder Rapid Implementation Guide – Shared Account Management

SAM Endpoint and Account Management Using the Feeder.....	86
The SAM feeder process	86
Import Endpoints using the SAM feeder.....	87
Import Privileged Accounts using the SAM feeder	94
Configure Email Notification for Workflow	97
Verify the Workflow and Email Configuration	103
Enable the CA IdentityMinder Management Console.....	107

References

The references related to CA ControlMinder may be found on the CA support web site in both PDF and HTML format.

<https://support.ca.com>

The references related to Tibco are included in the distribution and may be found in both PDF and HTML format in the following folder:

...\AccessControlServer\MessageQueue\tibco\ems\5.1\doc

CA ControlMinder References

CA ControlMinder Premium Edition Release Notes 12.7
CA ControlMinder Premium Edition Implementation Guide 12.7
CA ControlMinder Premium Edition Enterprise Administration Guide 12.7
CA ControlMinder Reference Guide 12.7
CA ControlMinder Endpoint Administration Guide for UNIX 12.7
CA ControlMinder Endpoint Administration Guide for Windows 12.7
CA ControlMinder selang Reference Guide 12.7
CA ControlMinder Troubleshooting Guide 12.7

Tibco References

TIBCO Enterprise Message Service Installation 5.1
TIBCO Enterprise Message Service User's Guide 5.1
TIBCO Enterprise Message Service Application Integration Guide 5.1
TIBCO Enterprise Message Service C and COBOL Reference 5.1

Copyright ©2013, CA, Inc. All rights reserved. Microsoft, Windows, Windows Server, Active Directory, SQL Server, and Internet Explorer are registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. RACF is a registered trademark of International Business Machines Corporation in the United States, other countries, or both. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries. UNIX is a registered trademark of The Open Group. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies.

This document is for your informational purposes only. CA assumes no responsibility for the accuracy or completeness of the information. To the extent permitted by applicable law, CA provides this document “as is” without warranty of any kind, including, without limitation, any implied warranties of merchantability, fitness for a particular purpose, or non-infringement. In no event will CA be liable for any loss or damage, direct or indirect, from the use of this document, including, without limitation, lost profits, business interruption, goodwill or lost data, even if CA is expressly advised in advance of the possibility of such damages.

Glossary

AC	Access Control
ACNT	Account
ACWS	Access Control Web Service
APM	Advanced Policy Management
APMS	Advanced Policy Management Server
CA	formerly Computer Associates – now CA Technologies
CM	ControlMinder (formerly Access Control)
CMPE	ControlMinder Premium Edition
CMVE	ControlMinder for Virtual Environments
CS	Connector Server
DH	Distribution Host
DMS	Distribution Management Server
DN	Distinguished Name
DR	Disaster Recovery
DS	Distribution Server
ELM	Enterprise Log Manager
ENTM	Enterprise Manager
EP	Endpoint (server)
GECOS	GE Comprehensive Operating System (finger field in passwd file)
GID	Group ID
HA	High Availability
IAM	Identity and Access Manager
JDK	Java Development Kit
MS	Microsoft Corporation
MSADS	Microsoft Active Directory Server / Services
MSSQL	Microsoft SQL/Server
MQ	Message Queue
NSS	Network System Services
OS	Operating System
PAM	Pluggable Authentication Module
PCI	Payment Card Industry
PR	Production
PUPM	Privileged User Password Management
RIA	Rapid Implementation Architecture
RIG	Rapid Implementation Guide
RS	Report Server
RSS	Resident Security System
SAM	Security Account Manager (formerly PUPM)
SeOS	Security for Open Systems
UARM	User Access Reporting Module (formerly ELM)
UAT	User Acceptance Test
UID	User ID
UNAB	UNIX Authentication Broker
W2K3	Windows 2003
W2K8	Windows 2008
WAS	Web Application Server

Executive summary

The purpose of the CA ControlMinder SAM Rapid Implementation Guide is to demonstrate a way to recognize value from Shared Accounts Management (SAM) in a timely manner. A reasonable expectation is to be managing up to 500 privileged accounts across 100 endpoints in 3 weeks or less. Up to 20 users can be using Shared Accounts Management concurrently during this initial implementation. The implementation can readily be expanded as the value becomes apparent, and it is easy to see how this guide also lends itself to proof of concept deployments.

Introduction

This guide provides step-by-step instructions for a successful installation. Tried and true choices like user and object stores have been made. Repeated customer successes drove these choices. Key success factors owned by the customer include:

- Having required hardware and software readily available (described in the [Preparing the Environment](#) section below).
- Identifying the privileged accounts of interest, as well as, the respective endpoints and endpoint types.
- Ensuring the Shared Accounts Management infrastructure can access the endpoints, for example, firewalls are not blocking required ports.

Team members contributing to your rapid implementation need familiarity with:

- Basic SAM functionality and terminology
- Basic Microsoft Windows Server Administration
- Microsoft Active Directory
- Microsoft SQL Server
- Basis Linux Administration.

To demonstrate a quick success, CA Technologies suggests limiting managed endpoints to:

- MS Windows Server 2008 (Local Accounts)
- MS Active Directory 2008 (Domain Accounts)
- MS SQL Server 2008
- Red Hat Linux

These endpoint types are frequently managed by many customers, but this is by no means an all-inclusive list of supported endpoint types. Once the initial bang for the buck has been felt, other

endpoint types can be added. You can view the complete list of managed endpoint types at <https://support.ca.com>.

Some advanced topics of frequent interest to customers covered by this guide include:

- Tagging endpoints and privileged accounts to simplify the process of identifying authorized users.
- Bulk loading endpoints and privileged accounts. This reinforces the need to identify the privileged accounts of interest ahead of time. The accounts used to connect to the endpoints and their respective passwords must also be identified.
- Providing ideas describing how to use roles to enforce separation of duties. After the initial implementation, some customers may choose to tailor the way roles are used.
- Leveraging simple updates to the out-of-the-box workflow configuration that often satisfy customer requirements.
- Using email to provide notifications.

As the success of your initial implementation sinks in, you are likely to want to invest in other advanced features like high availability. We highly recommend becoming familiar with the Enterprise Administration Guide and the Implementation Guide so you can make informed decisions on expanding your Shared Accounts Management implementation. The product Release Notes provide a handy resource for identifying any limitations.

CA ControlMinder Components

The current CA ControlMinder Premium Edition suite version is release 12.7 for the server components and 12.6 SP2 for endpoints. The suite consists of core ControlMinder, Advanced Policy Management, Shared Accounts Management and UNIX Authentication Broker. These components are anchored through a common interface that is known as Enterprise Management.

ControlMinder (CM) is the component that is typically referred to as a server-centric security offering. The intention of CM is to enhance the Resident Security System (RSS) found on all modern operating systems (OS). CM adds a layer of security over and above the RSS that enables the security administrator to effectively define security that is not available with the core OS security.

Advanced Policy Management (APM) is an enterprise security POLICY distribution layer that serves to deliver CM protection to the endpoint using a secure and tamper-proof model. Effectively, it is a management overlay for the enterprise that serves to reduce distribution overhead and enable the security set for the various endpoints to effectively be in place.

Shared Accounts Management (SAM) is a function that provides password management functions for privileged accounts. In the simplest form, SAM is a password vaulting facility that securely manages highly encoded endpoint passwords, and provides various methods of securely delivering those passwords to the user for direct input or through an automatic connection model whereby the user never has direct access to the password. SAM also provides a means to automatically change application passwords for password consumers like ODBC, JDBC, Scheduled Tasks and command line enabled applications. Finally, SAM supports an integration point with Observe IT to provide video-like recording and replay of endpoint activities through either Microsoft RDP, web interfaces for ORACLE or Microsoft SQL/Server or the PuTTY SSH application.

UNIX Authentication Broker (UNAB) provides UNIX endpoint authentication services through Microsoft Active Directory (MSAD).

Enterprise Management (ENTM) is the overarching component that ties the other components together through a unified management portal.

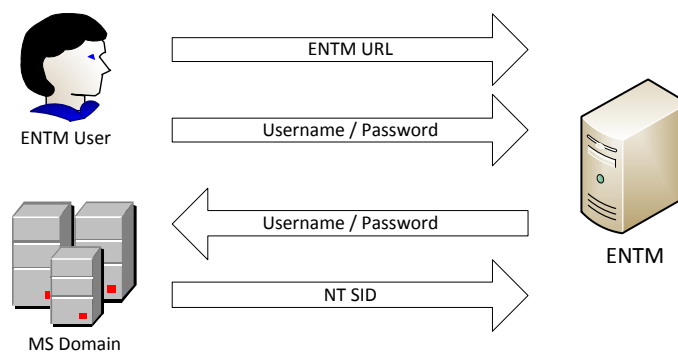
SAM User and Component Interaction

This section presents a high-level overview of the basic dataflow between users and SAM components. The direction of the arrows indicates the overall direction of data flow and the identifiers in each arrow indicate the types of data exchanged. The top-down nature of the arrows indicates that the top arrow is the first data exchange and the bottom arrow is the last data exchange.

Initial Logon

A user starts a browser session with the SAM portal hosted on the ENTM server. Using Active Directory credentials is a supported method of authenticating a user to ENTM. The following example relies on this method.

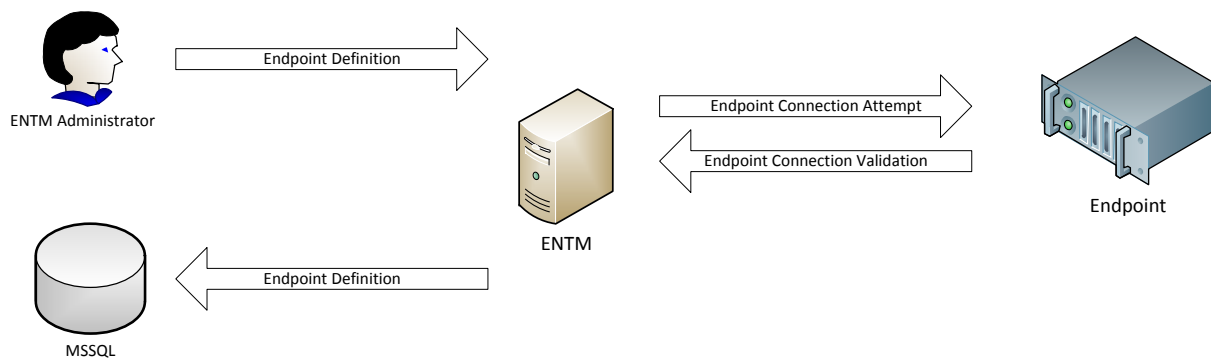
This interaction is through a web browser interface so the initial portal contact is to reference the ENTM URL. This URL is typically defined as `https://<ENTMServer>:18443/iam/ac`, where ENTM_server represents the actual hostname or IP address of the ENTM server.



Endpoint Creation

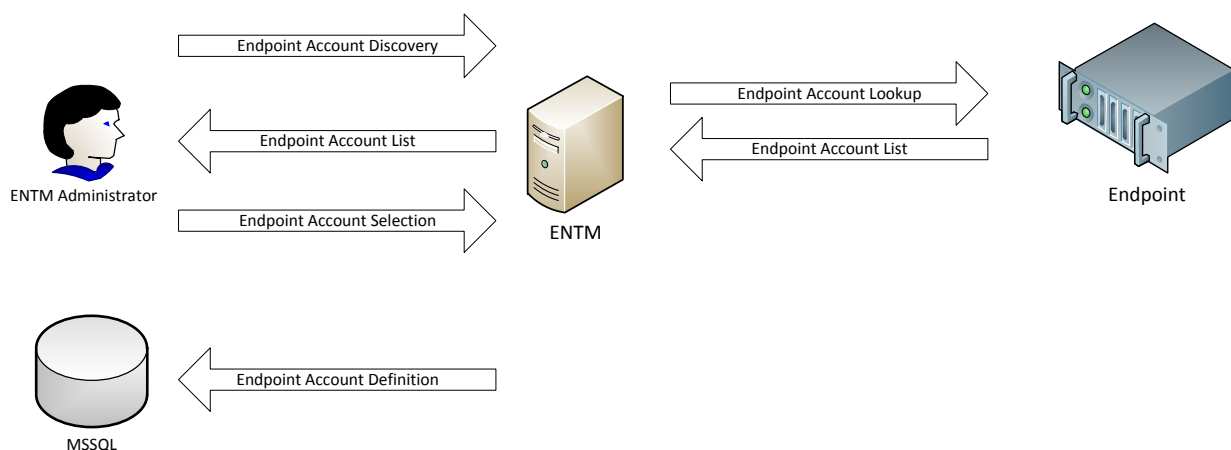
SAM requires two fundamental configuration items to support endpoint access. The first is the definition of the endpoint and the second is the definition of the privileged account. Both of these activities are performed by an ENTM administrator.

The endpoint definition consists of completing a connection form and submitting it to ENTM task processing. If the connection data is correct then ENTM stores the connection data in the RDBMS.



Privileged Account Creation

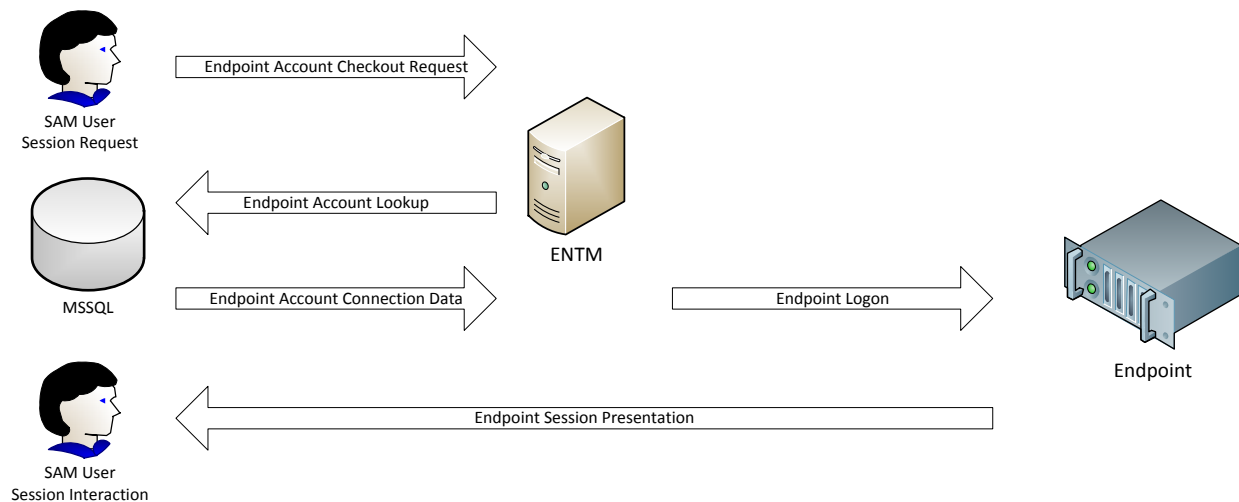
After an endpoint has been defined, the ENTM administrator uses the SAM Account Discovery Wizard to retrieve a list of accounts from the endpoint. The administrator selects a privileged account of interest, and ENTM stores the information in the RDBMS.



Defining the endpoint and privileged account provides sufficient information to manage the account for SAM users.

Endpoint Logon

When a SAM user wants to check out an account and log into an endpoint, the user requests a checkout through the SAM interface. ENTM then processes the request, retrieves the current password for the account from the RDBMS and either displays the password for manual use or executes an automatic logon sequence to the endpoint.

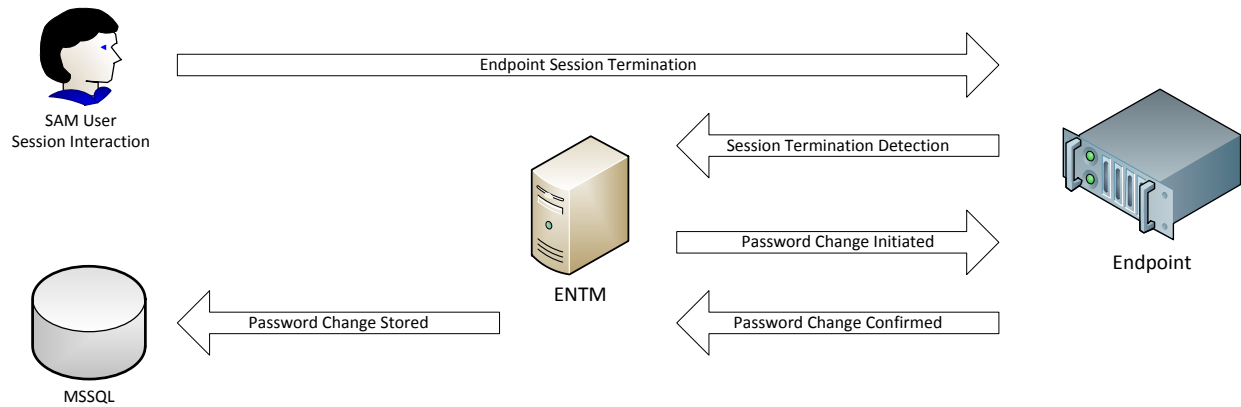


The SAM user then interacts with the endpoint as required. This endpoint interaction is independent of SAM.

Endpoint Logoff

When a SAM user completes endpoint interaction, the privileged account's password is typically changed on the endpoint and stored in the RDBMS for use during the next endpoint logon event.

CA ControlMinder Rapid Implementation Guide – Shared Account Management



Architecture

The base architecture supported in this RIA guide consists of a Microsoft Active Directory Server (MSADS), Microsoft SQL Server (MSSQL), and CA ControlMinder Enterprise Management (ENTM) as shown in Figure 1. Each of these components is hosted on separate servers; although, for demonstration purposes, all three can be hosted on the same server.

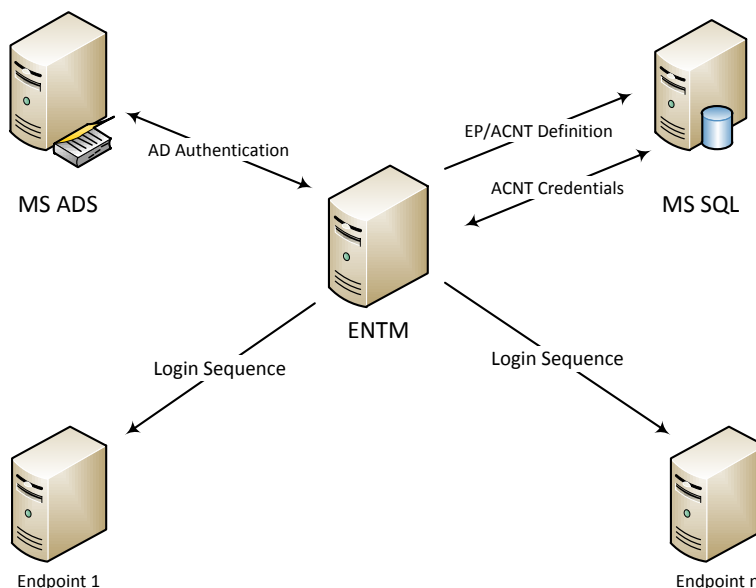


Figure 1 – Rapid Implementation Guide Reference Architecture

MSADS is used for ENTM login authentication and as a user datastore repository to support SAM service accounts.

MSSQL is used to store user/group/task/role assignments, endpoint connection definitions, and endpoint account credentials.

Preparing the Environment

Suggested Hardware and Software Components

The following HW and SW configuration was used for the purpose of this document.

Component	HW Specification	SW Specification
CA ControlMinder ENTM	4x Intel Xeon 2,93 GHz CPU 4 GB RAM HDD1 – 36 GB HDD2 – 72 GB	MS Windows 2008 Enterprise Edition SP2 x64
Directory Server – Uses Store	4x Intel Xeon 2,93 GHz CPU 8 GB RAM HDD1 – 36 GB HDD2 – 72 GB	MS Windows 2008 Enterprise Edition SP2 x64 MS Active Directory Domain Controller
Database Server	4x Intel Xeon 2,93 GHz CPU 8 GB RAM HDD1 – 36 GB HDD2 – 72 GB HDD3 – 128 GB	MS Windows 2008 Enterprise Edition SP2 x64 MS SQL Server 2008

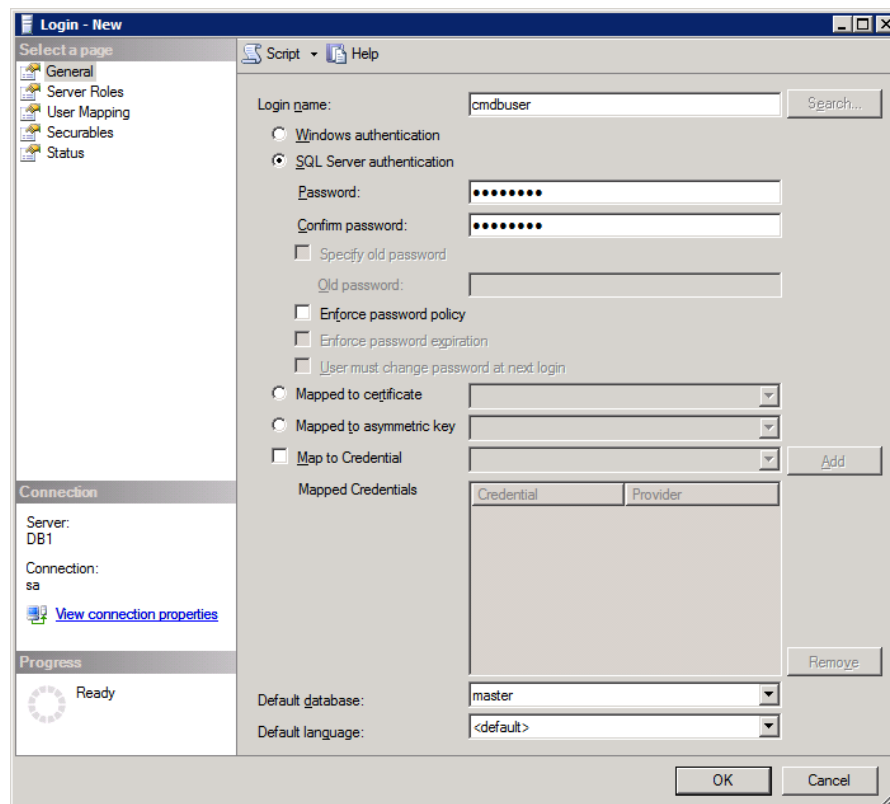
The above HW and SW configuration is sufficient to handle a small scale CA ControlMinder SAM implementation (up to 100 Endpoints and 500 privileged accounts).

Preparing the Database

STEP ONE in deploying SAM is to create an empty MSSQL database using **Microsoft SQL Server Management Studio**, which is typically available from the server where you installed Microsoft SQL Server.

Create MSSQL User

As shown below, an ENTM database user is created using SQL Server authentication. The user in this example is **cmdbuser**. Also note that it is recommended **not to enforce password policy** for this database user.

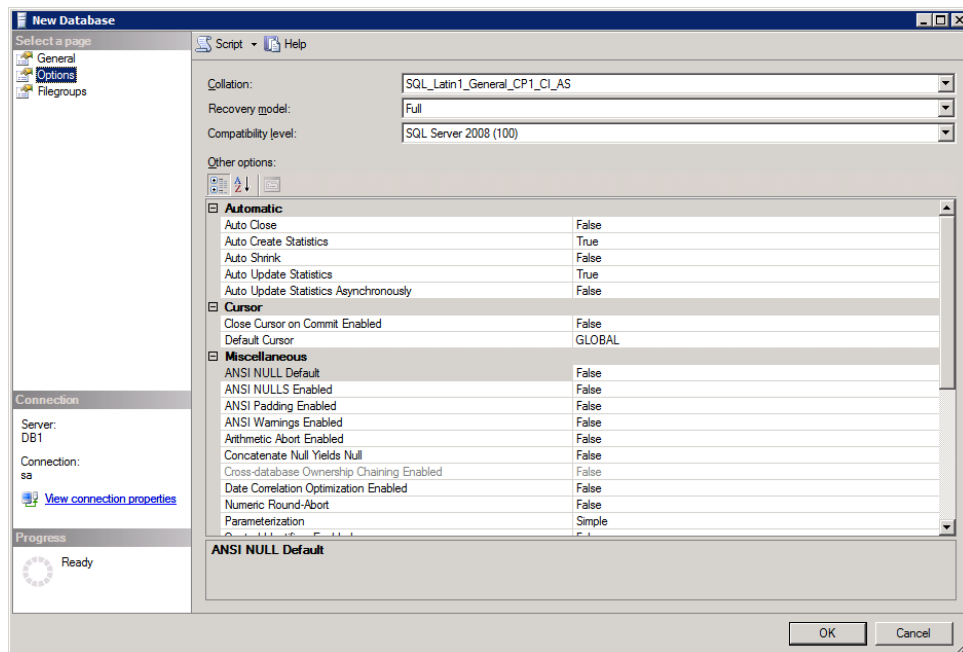


Create MSSQL Database

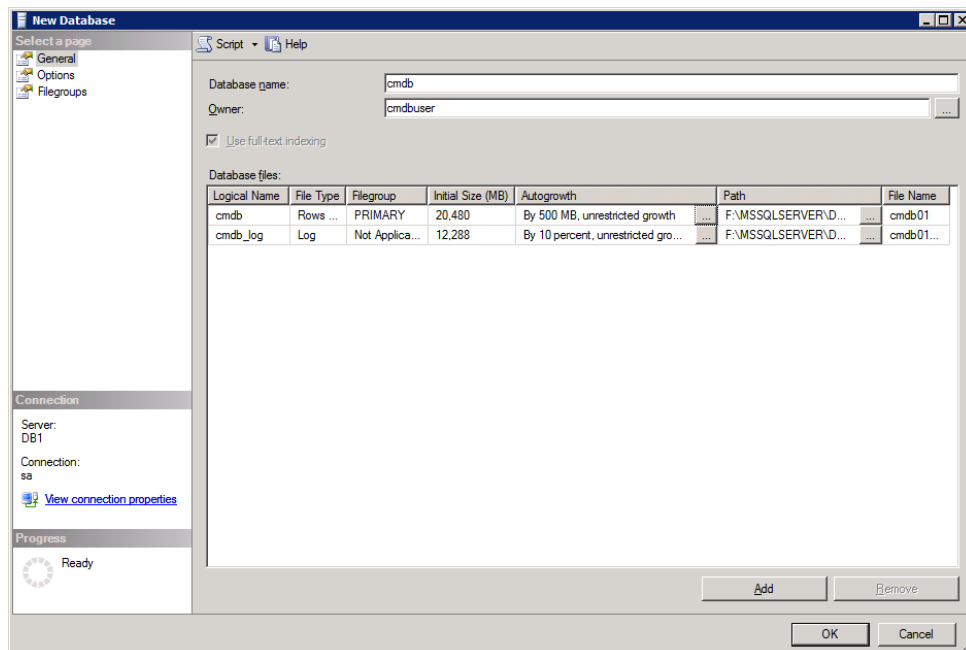
When creating the actual database, define it as a **case-insensitive** database with the item sort order set to **SQL_Latin1_General_CP1_CI_AS**. Failure to configure the correct settings may cause lookup problems later.

When creating the database, set the database owner to the user previously created. If that user is set as the owner (dbo) then no other access rights are required.

CA ControlMinder Rapid Implementation Guide – Shared Account Management



As shown, the database name is **cmdb**.



CA ControlMinder Rapid Implementation Guide – Shared Account Management

Set the newly created database as the default database of cmdbuser.

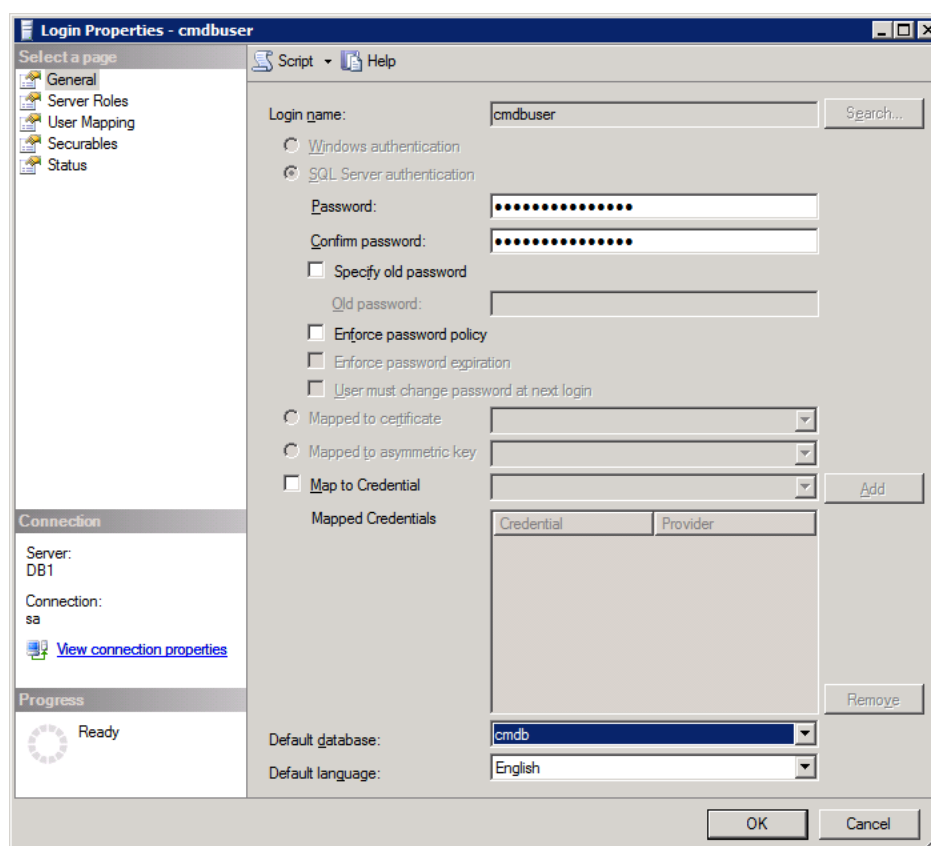


Table Sizing

It is important to pre allocate sufficient database space to hold configuration information and snapshot data.

In the example above we pre-allocated 20 GB of data space and 12 GB of log space. This size is sufficient to hold CM SAM data and reporting data for most environments.

If you do not intend to use the reporting functionality 5 GB of data space and 1 GB of log space will be sufficient.

Please refer to the “Sizing the Implementation” section of the *CA ControlMinder Premium Edition Implementation Guide* for more details.

Creating Users in Microsoft Active Directory

STEP TWO in deploying SAM is to create at least 2 Standard Microsoft user accounts in Active Directory before the installation of ENTM.

The first user will be used by CA ControlMinder Enterprise Management to connect to Active Directory.

User 1: CM ADlink

The best practice is to use a standard user with read-only access to MS Active Directory. Members of the Domain Users group have the necessary privileges by default.

Note: The following Enterprise Management tasks will not work if you use a read-only user (as they require write access to AD):

- modify user.
- create/modify/delete group.
- modify admin roles members.

However, this is not a limitation as you can assign users to roles by using the Modify Role task and specifying users and groups as members of a role in the members tab. This information is stored in the policy store (MSSQL).

The second account will be the super user of ENTM.

User 2: CM Admin

Collect Account DN

For both of the accounts created above you will need to know the Distinguished Name in the following format:

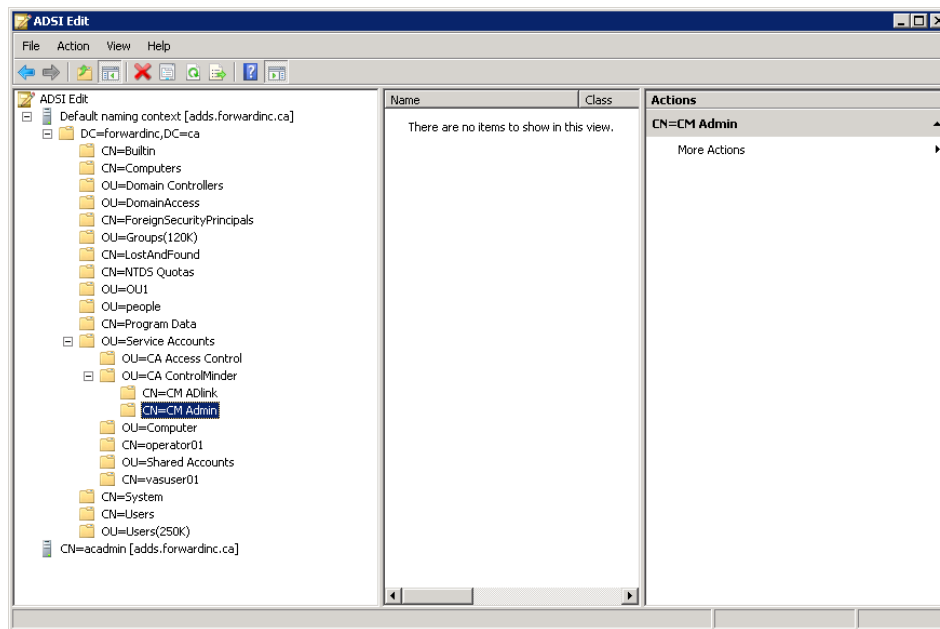
CN=<username>, CN=users, DC=<domain>, DC=<com>

However, if the account was created in another location in the AD tree then the DN may not be obvious. In that case you may use adsiedit.exe to obtain the DN as shown below.

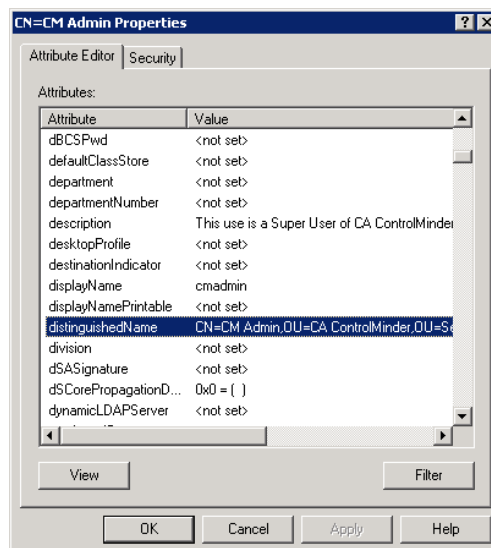
Note that adsiedit.exe is available on all Microsoft domain controllers so there should be no need to find and download the utility.

After selecting the account, right-click the account and select properties to select the DN.

CA ControlMinder Rapid Implementation Guide – Shared Account Management

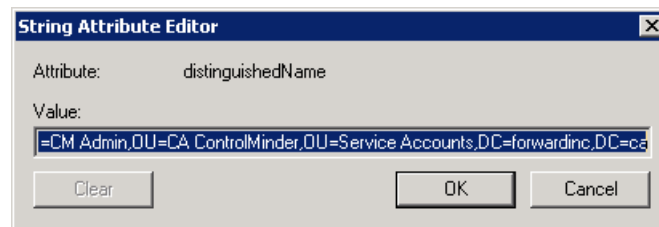


Select distinguishedName as shown.



If the DN is too large to see in the Properties display then select View and a separate pop-up will show the full name.

CA ControlMinder Rapid Implementation Guide – Shared Account Management



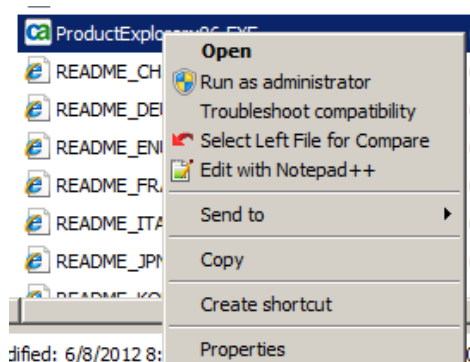
Save the DN to the clipboard for later use during ENTM installation.

ENTM Installation

ENTM installation consists of three steps followed by a **SERVER REBOOT** after the last step. The steps are simply to mount the distribution media, install the pre-requisite components and install the ENTM server software.

The entire installation process may take as little as 15 minutes or as long as 60 minutes, depending on the speed of the selected server.

In all cases, be sure to run the installation utilities as administrator. On Windows 2008 servers, this means to right-click on the installation binary and select **Run as administrator** from the pop-up menu as shown below.



In this RIG, the product media for the pre-requisite and ENTM software is loaded on drive E. The target disk drive for the installation is not important. What is important is to ensure that sufficient disk space is available. The **minimum space** required for each component after installation is listed below:

- JDK 200 MB
- JBoss 850 MB
- ENTM 1.10 GB

Load the Media Containing Required Third-Party Products

Log in to the server where ENTM will be installed as a user that is a member of the local Administrators group.

Mount the DVD or ISO containing CA ControlMinder Third-Party Components for Windows.

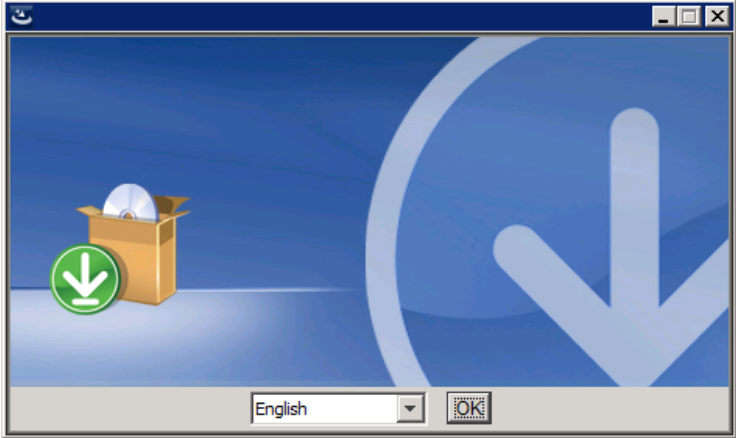
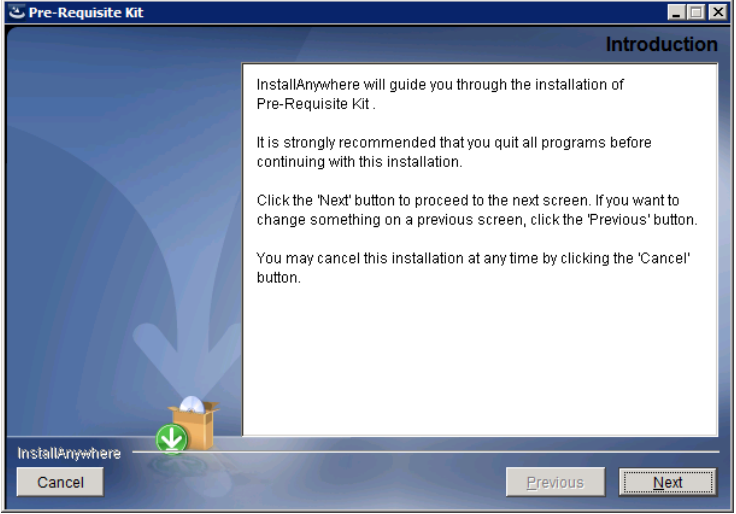
Important: Do not use a UNC path or remote share to specify the software location.

Install Pre-Requisite Software

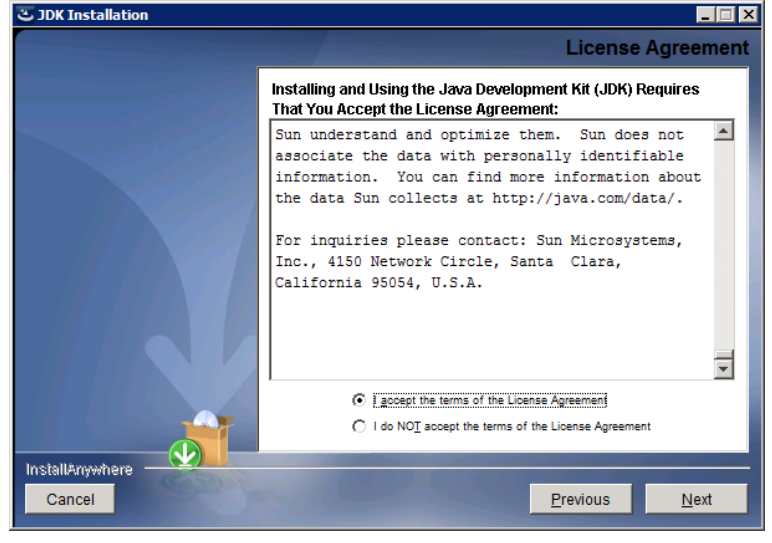
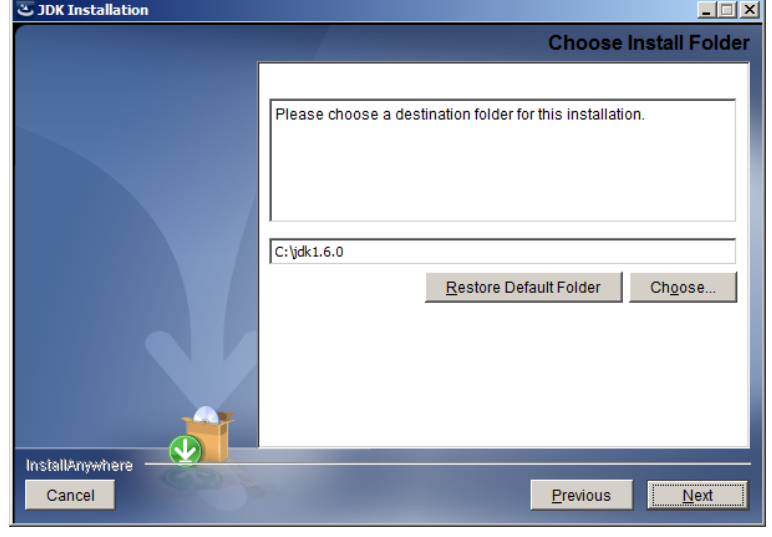
Start the installation of the pre-requisite components by launching **Install_PRK.exe** from the PrereqInstaller directory on the ISO.

Right click and choose “Run as administrator”.

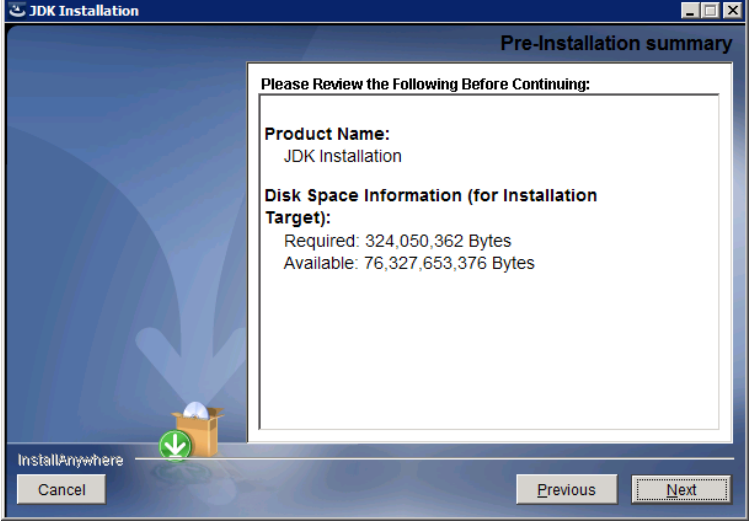

This will install the Java Development Kit and JBoss.

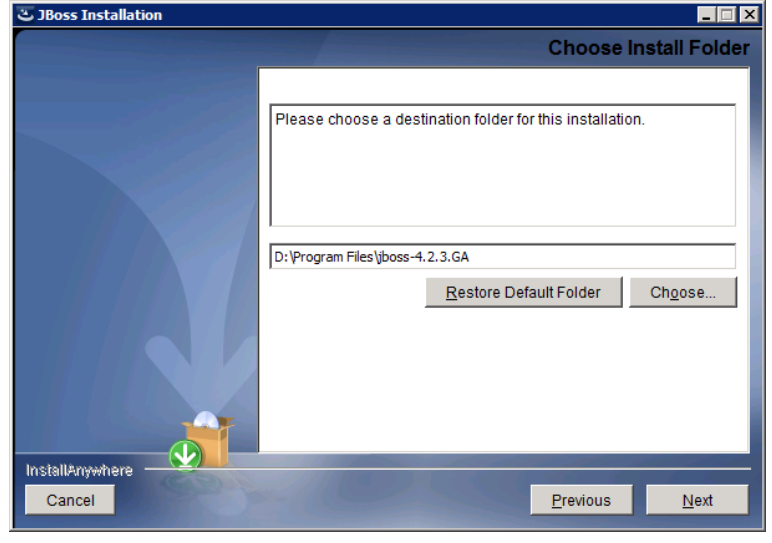
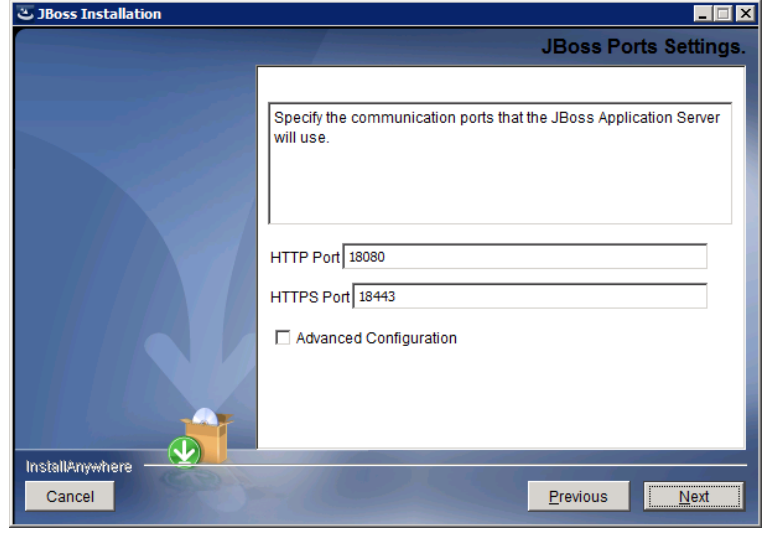
<p>JDK Installation</p> <p>Click OK</p>	
<p>Click Next</p>	

CA ControlMinder Rapid Implementation Guide – Shared Account Management

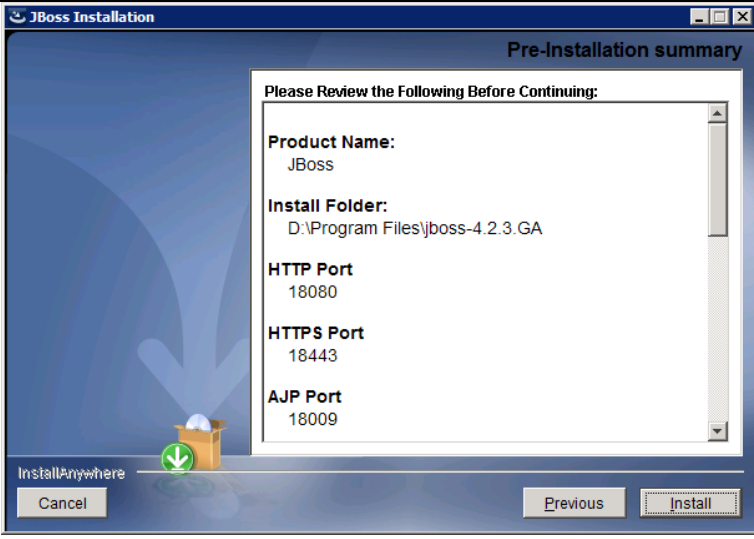
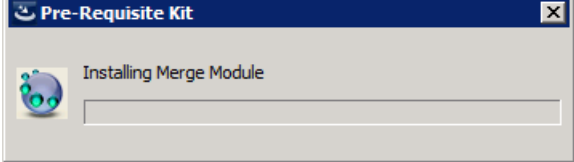
<p>Scroll down on right side of License Agreement and click “I accept...”</p> <p>Click Next</p>	 <p>The screenshot shows the 'JDK Installation' window with the 'License Agreement' tab selected. The agreement text is visible, and the 'I accept the terms of the License Agreement' radio button is selected. The 'Next' button is highlighted.</p>
<p>Select destination folder</p> <p>Click Next</p>	 <p>The screenshot shows the 'JDK Installation' window with the 'Choose Install Folder' tab selected. The text 'Please choose a destination folder for this installation.' is displayed. The folder path 'C:\jdk1.6.0' is entered in the text box. The 'Next' button is highlighted.</p>

CA ControlMinder Rapid Implementation Guide – Shared Account Management

<p>Click Next</p>	 <p>The screenshot shows the 'JDK Installation' window with the 'Pre-Installation summary' tab selected. The window displays the following information:</p> <ul style="list-style-type: none"> Please Review the Following Before Continuing: Product Name: JDK Installation Disk Space Information (for Installation Target): <ul style="list-style-type: none"> Required: 324,050,362 Bytes Available: 76,327,653,376 Bytes <p>At the bottom, there is a green arrow icon pointing down, and buttons for 'Cancel', 'Previous', and 'Next'.</p>
<p>JBoss Installation</p> <p>Scroll down on right side of License Agreement and click "I accept..."</p> <p>Click Next</p>	 <p>The screenshot shows the 'JBoss Installation' window with the 'License Agreement' tab selected. The window displays the following information:</p> <ul style="list-style-type: none"> Installing and Using the JBoss Application Server Requires That You Accept the Following License Agreement: without regard to any conflict of laws provisions, except that the United Nations Convention on the International Sale of Goods shall not apply. Copyright 2006-2007 Red Hat, Inc. All rights reserved. "JBoss" and the JBoss logo are registered trademarks of Red Hat, Inc. All other trademarks are the property of their respective owners. <p>At the bottom, there are two radio buttons: <ul style="list-style-type: none"> <input checked="" type="radio"/> I accept the terms of the License Agreement <input type="radio"/> I do NOT accept the terms of the License Agreement </p> <p>At the bottom, there is a green arrow icon pointing down, and buttons for 'Cancel', 'Previous', and 'Next'.</p>

<p>Select destination folder</p> <p>Click Next</p>	 <p>The screenshot shows the 'JBoss Installation' window with the 'Choose Install Folder' tab selected. The window has a blue header bar with the title 'JBoss Installation'. Below the header, there's a large blue area with a white box containing the text 'Please choose a destination folder for this installation.' Below this box is a text field containing 'D:\Program Files\jboss-4.2.3.GA'. To the right of the text field are two buttons: 'Restore Default Folder' and 'Choose...'. At the bottom of the window, there's a progress bar labeled 'InstallAnywhere' with a green arrow pointing down. Below the progress bar are three buttons: 'Cancel', 'Previous', and 'Next'.</p>
<p>Click Next</p>	 <p>The screenshot shows the 'JBoss Installation' window with the 'JBoss Ports Settings' tab selected. The window has a blue header bar with the title 'JBoss Installation'. Below the header, there's a large blue area with a white box containing the text 'Specify the communication ports that the JBoss Application Server will use.' Below this box are two text fields: 'HTTP Port' with the value '18080' and 'HTTPS Port' with the value '18443'. Below these fields is a checkbox labeled 'Advanced Configuration' which is currently unchecked. At the bottom of the window, there's a progress bar labeled 'InstallAnywhere' with a green arrow pointing down. Below the progress bar are three buttons: 'Cancel', 'Previous', and 'Next'.</p>

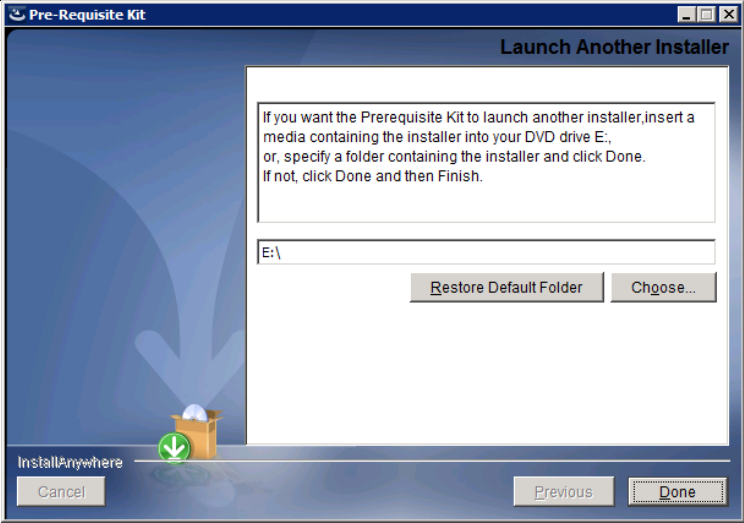
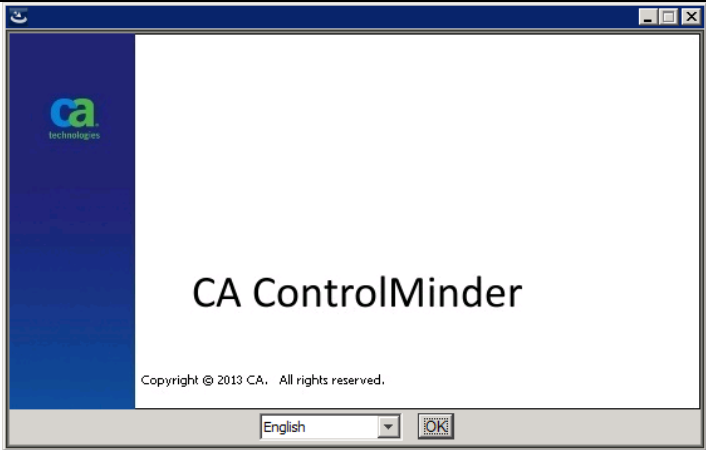
CA ControlMinder Rapid Implementation Guide – Shared Account Management

<p>Click Install</p>	 <p>The screenshot shows the 'JBoss Installation' window with a 'Pre-Installation summary' dialog box. The dialog box contains the following information:</p> <ul style="list-style-type: none"> Product Name: JBoss Install Folder: D:\Program Files\jboss-4.2.3.GA HTTP Port: 18080 HTTPS Port: 18443 AJP Port: 18009 <p>At the bottom of the window, there is a progress bar labeled 'InstallAnywhere' with a green arrow icon. Below the progress bar are 'Cancel', 'Previous', and 'Install' buttons.</p>
<p>Wait for installation to complete</p>	 <p>The screenshot shows a 'Pre-Requisite Kit' window with a progress bar and the text 'Installing Merge Module'.</p>

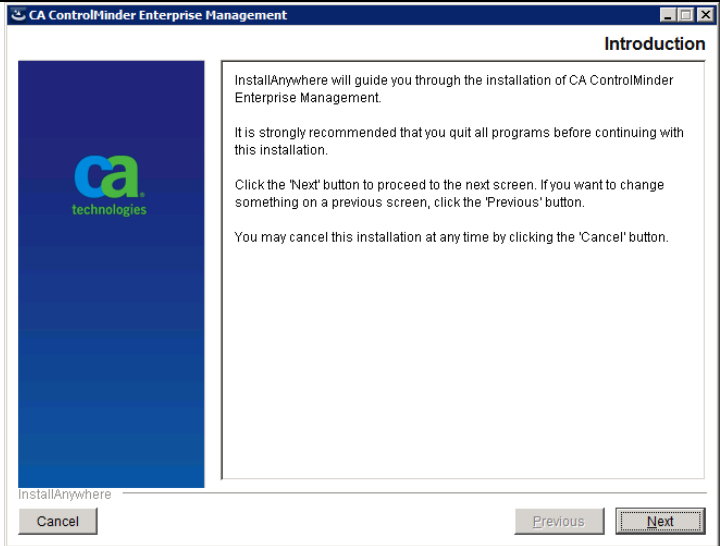
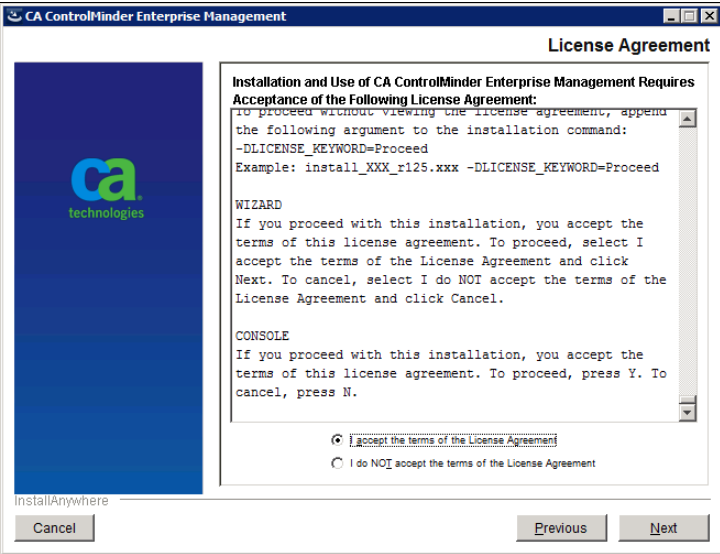
Install ENTM

You can start the installation of ENTM by launching **ProductExplorer** from the ISO or directly from the Prerequisite installer.

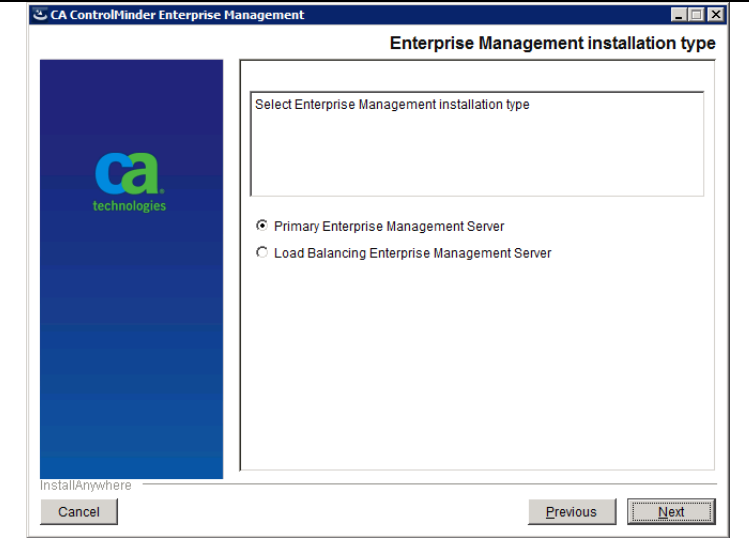
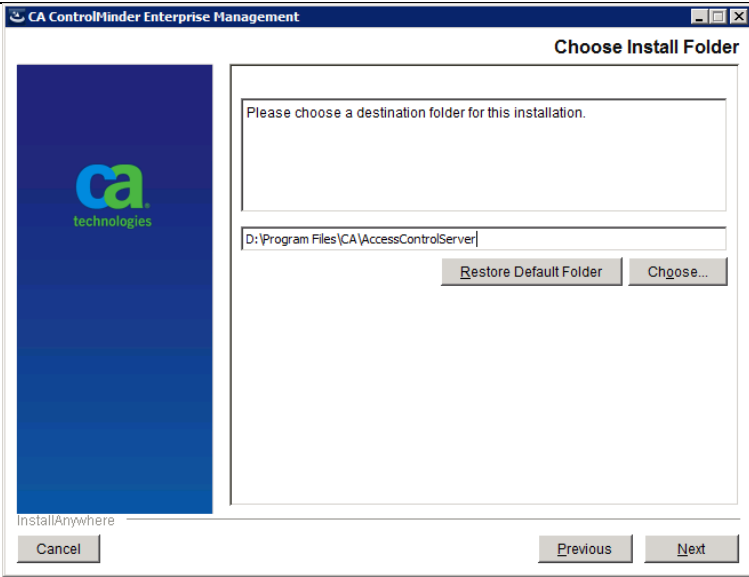
The steps below are for the installation started from the prerequisite installer.

<p>Change the DVD and insert CA ControlMinder Server Components DVD and Click Done.</p> <p>Alternatively, start the installation manually using ProductExplorer.</p>	
<p>If ProductExplorer is started manually, select Enterprise Management from the available choices.</p>	
<p>Click OK</p>	

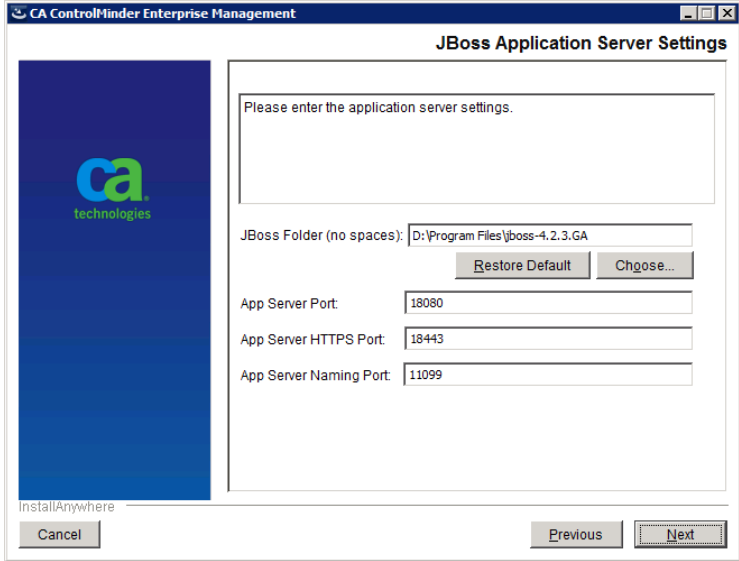
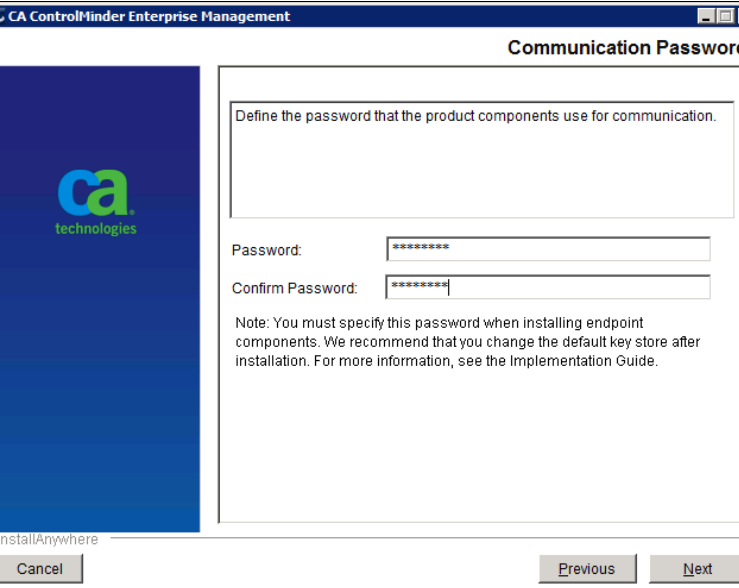
CA ControlMinder Rapid Implementation Guide – Shared Account Management

<p>Click Next</p>	 <p>The screenshot shows the 'Introduction' window of the CA ControlMinder Enterprise Management installer. It features the CA Technologies logo on the left and instructional text on the right. The text explains that InstallAnywhere will guide the installation and recommends quitting all programs. It instructs the user to click 'Next' to proceed, 'Previous' to go back, or 'Cancel' to abort. At the bottom, there are 'Cancel', 'Previous', and 'Next' buttons.</p>
<p>Scroll down on right side of License Agreement and click "I accept..."</p> <p>Click Next</p>	 <p>The screenshot shows the 'License Agreement' window. It contains the CA Technologies logo on the left and the license agreement text on the right. The text includes instructions on how to proceed without viewing the license agreement by using a specific command-line argument. It also provides instructions for accepting or declining the terms. At the bottom, there are two radio buttons: 'I accept the terms of the License Agreement' (which is selected) and 'I do NOT accept the terms of the License Agreement'. Below these are 'Cancel', 'Previous', and 'Next' buttons.</p>

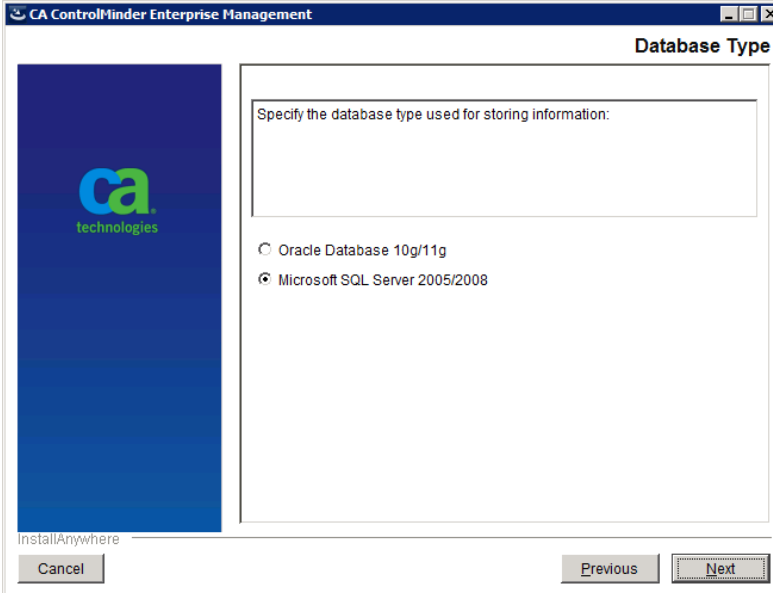
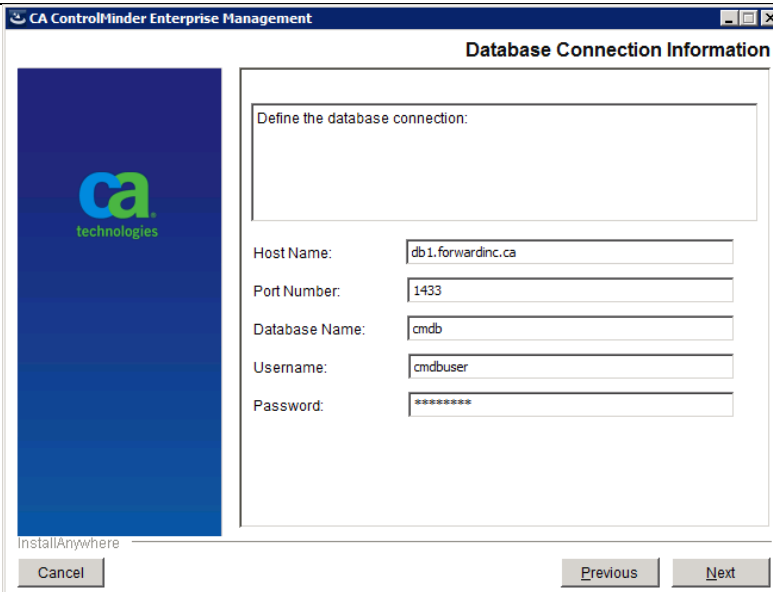
CA ControlMinder Rapid Implementation Guide – Shared Account Management

<p>Select Primary Enterprise Management Server</p> <p>Click Next</p>	
<p>Select destination folder</p> <p>Click Next</p>	

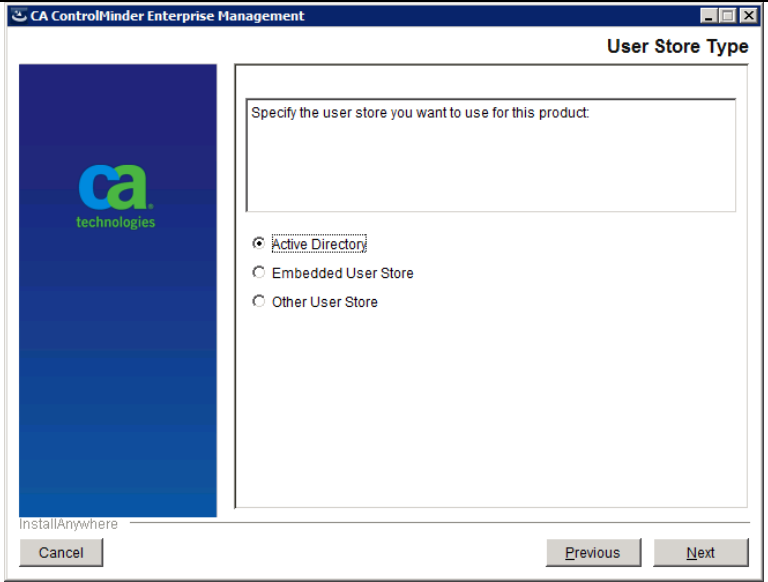
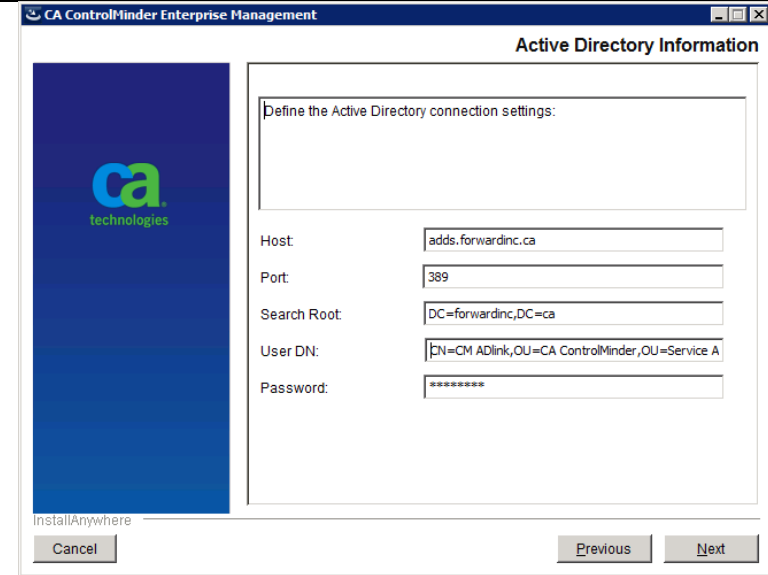
CA ControlMinder Rapid Implementation Guide – Shared Account Management

<p>Click Next</p>	 <p>The screenshot shows the 'JBoss Application Server Settings' window in the CA ControlMinder Enterprise Management application. It features the CA Technologies logo on the left. The main area contains a text box for 'Please enter the application server settings.' Below this, there are input fields for 'JBoss Folder (no spaces):' (with the value 'D:\Program Files\jboss-4.2.3.GA'), 'App Server Port:' (18080), 'App Server HTTPS Port:' (18443), and 'App Server Naming Port:' (11099). There are 'Restore Default' and 'Choose...' buttons next to the JBoss Folder field. At the bottom, there are 'Cancel', 'Previous', and 'Next' buttons. The window title is 'CA ControlMinder Enterprise Management'.</p>
<p>Enter communication password – this password is used by all infrastructure components.</p> <p>Click Next</p>	 <p>The screenshot shows the 'Communication Password' window in the CA ControlMinder Enterprise Management application. It features the CA Technologies logo on the left. The main area contains a text box for 'Define the password that the product components use for communication.' Below this, there are two input fields: 'Password:' and 'Confirm Password:', both masked with asterisks. A note at the bottom states: 'Note: You must specify this password when installing endpoint components. We recommend that you change the default key store after installation. For more information, see the Implementation Guide.' At the bottom, there are 'Cancel', 'Previous', and 'Next' buttons. The window title is 'CA ControlMinder Enterprise Management'.</p>

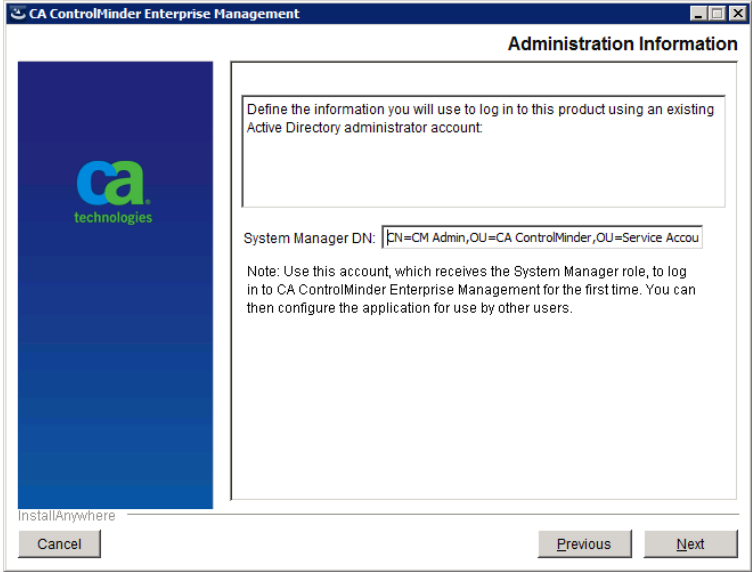
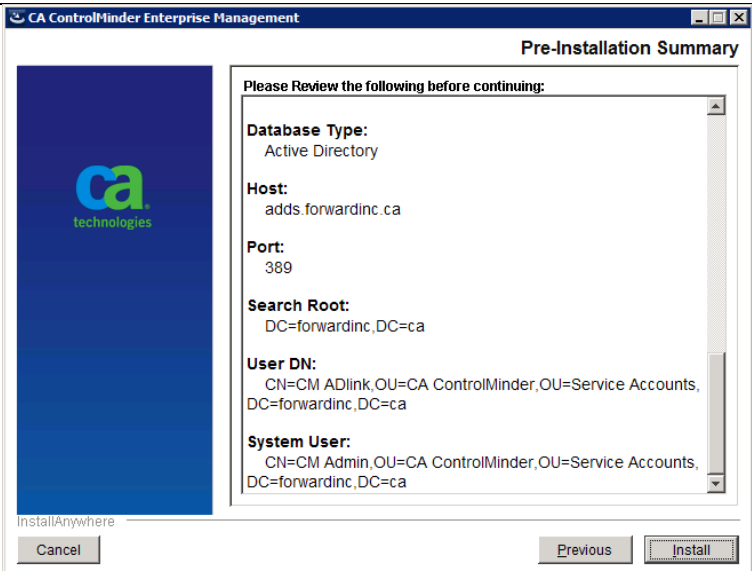
CA ControlMinder Rapid Implementation Guide – Shared Account Management

<p>Select the database type that will be used to store the configuration information of CA ControlMinder Enterprise Management and data for the reports. You will be using MS SQL Server.</p>	 <p>The dialog box titled "CA ControlMinder Enterprise Management" shows the "Database Type" selection screen. It features the CA Technologies logo on the left. The main area contains a text box for specifying the database type and two radio button options: "Oracle Database 10g/11g" and "Microsoft SQL Server 2005/2008". The "Microsoft SQL Server 2005/2008" option is selected. At the bottom, there are "Cancel", "Previous", and "Next" buttons.</p>
<p>Enter the connection data for the MSSQL database connection</p> <p>Click Next</p>	 <p>The dialog box titled "CA ControlMinder Enterprise Management" shows the "Database Connection Information" screen. It features the CA Technologies logo on the left. The main area contains a text box for defining the database connection and several input fields: "Host Name" (db1.forwardinc.ca), "Port Number" (1433), "Database Name" (cmdb), "Username" (cmdbuser), and "Password" (masked with asterisks). At the bottom, there are "Cancel", "Previous", and "Next" buttons.</p>

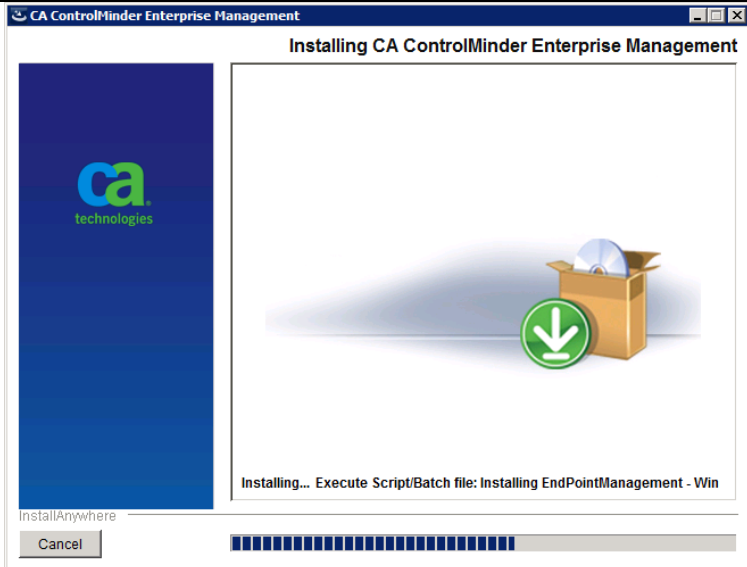
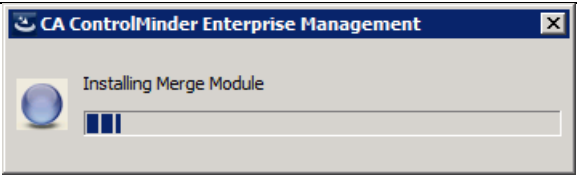
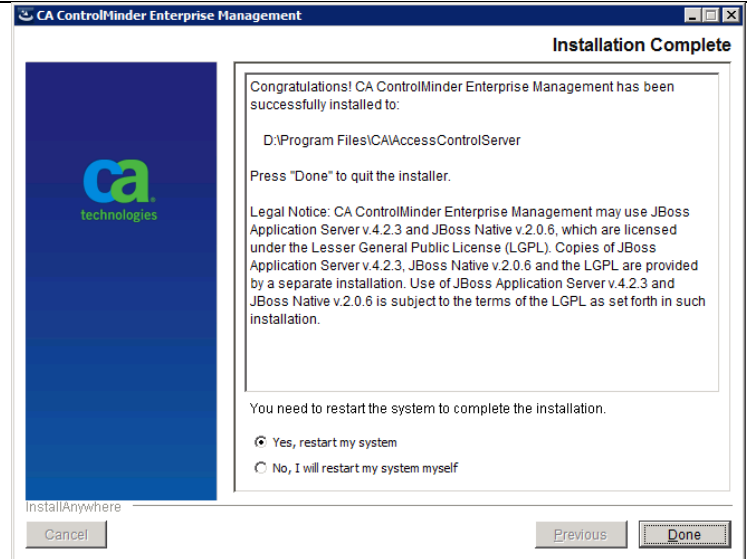
CA ControlMinder Rapid Implementation Guide – Shared Account Management

<p>Select Active Directory for the user store</p> <p>Click Next</p>	 <p>The screenshot shows the 'User Store Type' dialog box. It has a CA Technologies logo on the left. The main area says 'Specify the user store you want to use for this product:' and has three radio buttons: 'Active Directory' (selected), 'Embedded User Store', and 'Other User Store'. At the bottom are 'Cancel', 'Previous', and 'Next' buttons.</p>
<p>Enter the AD connection information. – Enter the DN you obtained from adsiedit for the user you created earlier as the connection account.</p> <p>The User DN for this example is: CN=CM ADlink,OU=CA ControlMinder,OU=Service Accounts,DC=forwardinc,DC=ca</p> <p>Click Next</p>	 <p>The screenshot shows the 'Active Directory Information' dialog box. It has a CA Technologies logo on the left. The main area says 'Define the Active Directory connection settings:' and has several input fields: 'Host' (adds.forwardinc.ca), 'Port' (389), 'Search Root' (DC=forwardinc,DC=ca), 'User DN' (CN=CM ADlink,OU=CA ControlMinder,OU=Service A), and 'Password' (masked with asterisks). At the bottom are 'Cancel', 'Previous', and 'Next' buttons.</p>

CA ControlMinder Rapid Implementation Guide – Shared Account Management

<p>Enter the System Manager DN as noted above. This is the DN of the user you created earlier to be the super user.</p> <p>Click Next</p>	 <p>The screenshot shows the 'Administration Information' dialog box for CA ControlMinder Enterprise Management. It features the CA Technologies logo on the left. The main area contains a text box for 'System Manager DN' with the value 'CN=CM Admin,OU=CA ControlMinder,OU=Service Accounts'. Below this is a note: 'Note: Use this account, which receives the System Manager role, to log in to CA ControlMinder Enterprise Management for the first time. You can then configure the application for use by other users.' At the bottom are 'Cancel', 'Previous', and 'Next' buttons.</p>
<p>Click Install</p>	 <p>The screenshot shows the 'Pre-Installation Summary' dialog box for CA ControlMinder Enterprise Management. It features the CA Technologies logo on the left. The main area is titled 'Please Review the following before continuing:' and lists the following configuration details: <ul style="list-style-type: none"> Database Type: Active Directory Host: adds.forwardinc.ca Port: 389 Search Root: DC=forwardinc,DC=ca User DN: CN=CM Admin,OU=CA ControlMinder,OU=Service Accounts,DC=forwardinc,DC=ca System User: CN=CM Admin,OU=CA ControlMinder,OU=Service Accounts,DC=forwardinc,DC=ca At the bottom are 'Cancel', 'Previous', and 'Install' buttons. </p>

CA ControlMinder Rapid Implementation Guide – Shared Account Management

<p>Wait for installation to complete</p> <p>Important: If the installation does not appear to start then an installation confirmation window may be under the current window. Move the top window and check for an underlying window.</p>	
<p>The installation may take from 15 to 60 minutes to complete</p>	
<p>Click Done to reboot the server</p>	

Installation Validation

After the server has been rebooted, the ENTM components will be automatically started. During the first startup, a few configuration steps are performed to deploy the ENTM components in JBoss and build the required schema in the RDBMS. These activities may take about 5 minutes to fully complete so do not try to log onto the ENTM interface until the post-installation configuration steps have completed. If the server is dedicated to ControlMinder server components, use Task Manager to watch for CPU utilization to drop below 5%.

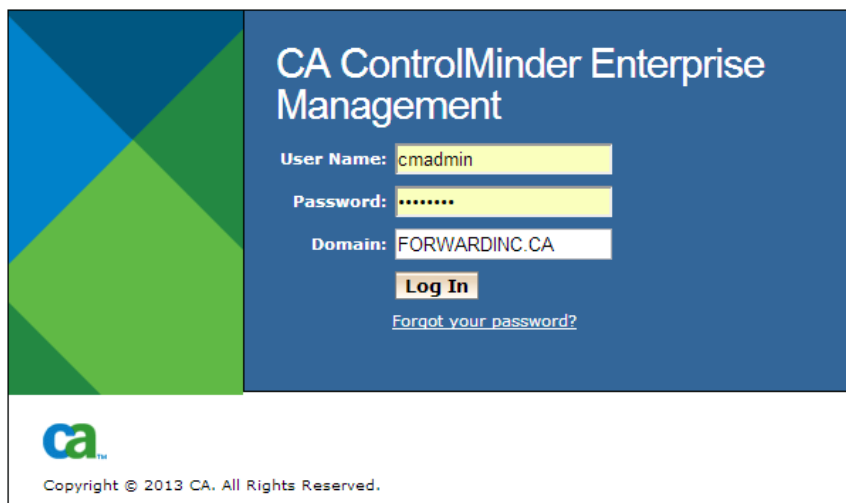
To test the validity of the ENTM installation, use a web browser (Microsoft Internet Explorer, Google Chrome, or Mozilla Firefox) to access the web-based user interface (WebUI).

To access the ENTM interface, use the following URL:

`https://<ENTM_server>:18443/iam/ac`

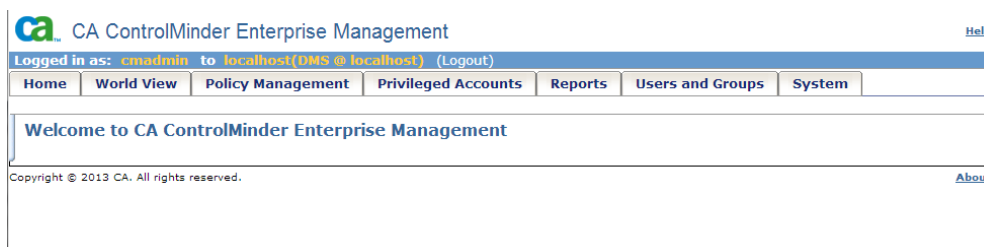
The login page shown below should be displayed. Enter the account name of the super user that you specified during the installation.

Note: This is the account name for the respective DN.



The login page for CA ControlMinder Enterprise Management. It features a blue header with the title "CA ControlMinder Enterprise Management". Below the title are three input fields: "User Name:" with the value "cmadmin", "Password:" with masked characters ".....", and "Domain:" with the value "FORWARDINC.CA". A "Log In" button is positioned below the domain field, and a link "Forgot your password?" is below the button. The footer includes the CA Technologies logo and the text "Copyright © 2013 CA. All Rights Reserved."

After a successful login, note the following dashboard as a simple validation:



The dashboard for CA ControlMinder Enterprise Management. It features a blue header with the title "CA ControlMinder Enterprise Management" and a "Help" link. Below the header is a navigation bar with the text "Logged in as: cmadmin to localhost(DMS @ localhost) (Logout)". The navigation bar includes links for "Home", "World View", "Policy Management", "Privileged Accounts", "Reports", "Users and Groups", and "System". Below the navigation bar is a welcome message "Welcome to CA ControlMinder Enterprise Management". The footer includes the CA Technologies logo and the text "Copyright © 2013 CA. All rights reserved." and an "About" link.

Review server.log located under JBoss_home/server/default/log for errors if the simple validation failed.

SAM Endpoint Creation

The installation and configuration flow of SAM is to create an endpoint definition first and then select privileged accounts of interest from that endpoint to be managed by SAM.

When you create an endpoint, you must define an account used by SAM to connect to the endpoint. This account must have sufficient privilege to list endpoint accounts and change endpoint account passwords. NOTE: The connection account itself can be managed by SAM as a privileged account.

Important: If the password of a connection account expires, SAM cannot manage accounts for this endpoint until the password for the connection account is updated. In support of this rapid implementation we recommend using connection accounts whose passwords do not expire.

Each of the endpoint and account creation methods presented below all use the same starting points. In order to prevent repetition of those items, they are covered once in this section.

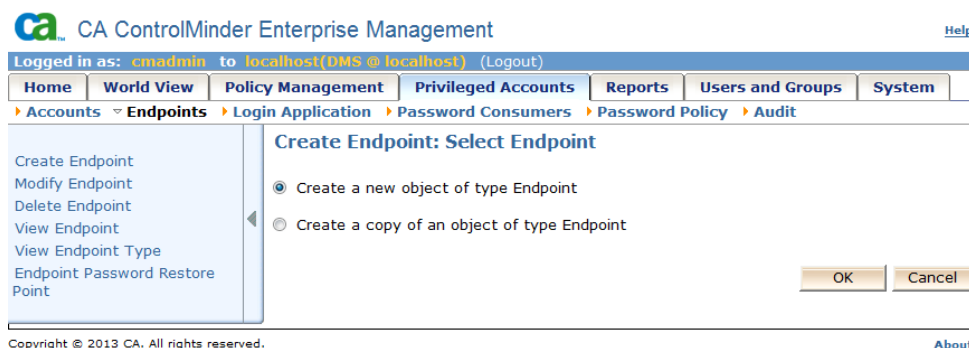
Endpoint Creation

Log into the ENTM WebUI as an administrator that has permission to create endpoint definitions and discover endpoint accounts. At this point, your System Manager user is the only user who can perform these tasks.

From the interface, select the **Privileged Accounts** tab.

From the **Privileged Accounts** tab, select the **Endpoints** menu item.

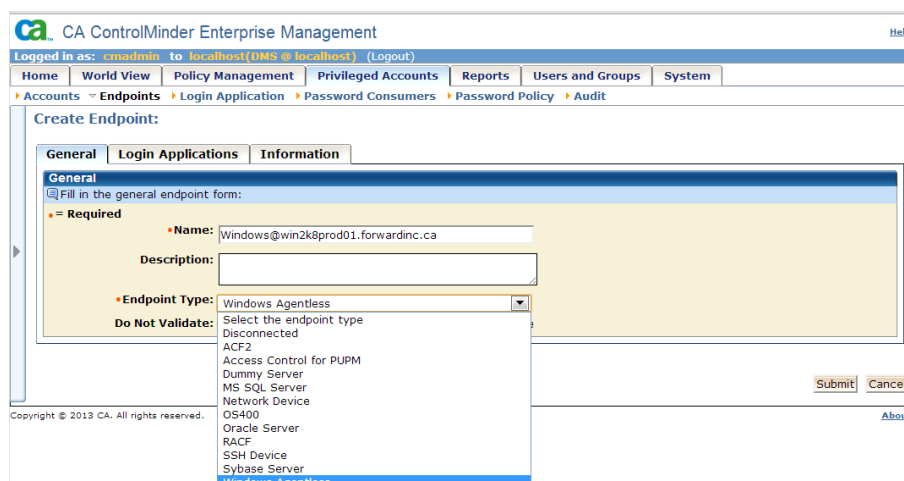
Click on **Create Endpoint** from the **Endpoints** menu. Click the OK button to create a new endpoint.



Provide the name for the endpoint. This name must be unique within an endpoint type.

This field defines how the name of the endpoint appears in CA ControlMinder Enterprise Management. A suggested best practice is to use endpointtype@hostname as the endpoint name. This allows you to distinguish between different endpoint types on the same host (e.g. OS accounts and DB accounts)

CA ControlMinder Rapid Implementation Guide – Shared Account Management



CA ControlMinder Enterprise Management

Logged in as: **cmadmin** to **localhost(DMS @ localhost)** (Logout)

Home | World View | Policy Management | Privileged Accounts | Reports | Users and Groups | System

Accounts > Endpoints > Login Application > Password Consumers > Password Policy > Audit

Create Endpoint:

General | Login Applications | Information

General

Fill in the general endpoint form:

Name: Windows@win2k8prod01.forwardinc.ca

Description:

Endpoint Type: Windows Agentless

Do Not Validate:

Select the endpoint type

- Disconnected
- ACF2
- Access Control for PUPM
- Dummy Server
- MS SQL Server
- Network Device
- OS400
- Oracle Server
- RACF
- SSH Device
- Sybase Server
- Windows Agentless**

Submit Cancel

Copyright © 2013 CA. All rights reserved. About

Select a type from the list of available endpoint types.

You will be presented with the list of options specific to the selected endpoint type.

Windows Endpoint

This topic pertains to Windows endpoints that are not Active Directory domain controllers. Some customers may choose to use a local account to manage these endpoints; whereas, other customers may choose to use a domain account.

The connection model uses the Microsoft Windows Management Instrumentation (WMI) functionality to connect to and manage the endpoint's local privileged account(s).

You need to have the following ports open on a Windows endpoint to successfully manage privileged accounts:

- Port 445
- Port 135

Select Windows Agentless from the list of available endpoint type.

You will be presented with a list of fields for the selected endpoint type.

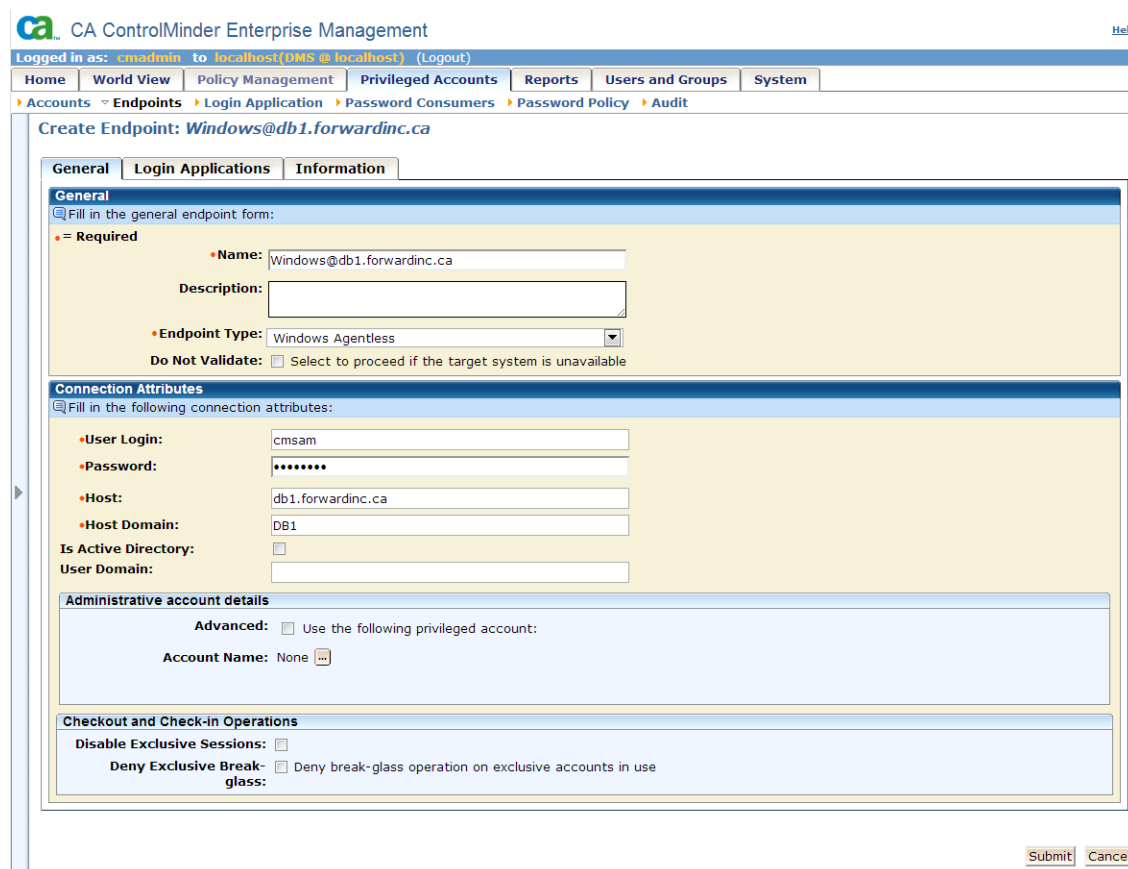
Following is a description of the fields available for the Windows Agentless endpoint type.

Field name	Description	Additional information
User Login	Defines the name of an administrative user who manages the endpoint. SAM uses this account to perform administrative tasks on the endpoint, for example, to connect to the endpoint, discover accounts, and change passwords.	Specify the user name in this field. Do not use the computer name\user name format or the domain name\user name format. Note: If you specify the Advanced option, PUPM ignores the User Login field. Instead, PUPM uses the account that is specified under the Advanced option to perform administrative tasks on the endpoint.
Password	Defines the password of the administrative user of the endpoint.	Note: If you use the Advanced option, this field is ignored.
Host		This option defines the DNS host name of the Windows endpoint Note: You can also use an IP address as a host name.
Host Domain	Provide the NETBIOS name of the endpoint	Note: Do not use the DNS name (computer1.ca.com), use the NETBIOS name (computer1).
Is Active Directory	Do not select this option. This option is valid when managing Active Directory accounts only.	

User Domain	<p>The NETBIOS name of the Active Directory domain of which the administrative privileged account is a member.</p> <p>Required when:</p> <p>LOGIN_USER defines an Active Directory account instead of a local account.</p> <p>The Advanced option is selected and the administrative privileged account is an Active Directory domain user.</p> <p>Not required when:</p> <p>LOGIN_USER defines a local account.</p>	
Advanced	<p>Specifies whether to use a previously defined administrative account to perform administrative tasks on the endpoint. For example, SAM uses the account defined in the Advanced field to manage this endpoint instead of using the account specified in the User Login field. This option is useful when using the same privilege account to manage multiple endpoints.</p>	<p>Note: If you specify this option, SAM ignores the User Login field.</p>

CA ControlMinder Rapid Implementation Guide – Shared Account Management

The following screenshot shows an example of Windows Agentless endpoint definition when a local account is used.



The screenshot displays the CA ControlMinder Enterprise Management web interface. The top navigation bar includes links for Home, World View, Policy Management, Privileged Accounts, Reports, Users and Groups, and System. A breadcrumb trail shows the path: Accounts > Endpoints > Login Application > Password Consumers > Password Policy > Audit. The main title is 'Create Endpoint: Windows@db1.forwardinc.ca'. The form is divided into three tabs: General, Login Applications, and Information. The 'General' tab is active and contains the following sections:

- General:** Includes a 'Fill in the general endpoint form:' section with fields for Name (Windows@db1.forwardinc.ca), Description, Endpoint Type (Windows Agentless), and a checkbox for 'Do Not Validate'.
- Connection Attributes:** Includes a 'Fill in the following connection attributes:' section with fields for User Login (cmsam), Password (masked), Host (db1.forwardinc.ca), Host Domain (DB1), and a checkbox for 'Is Active Directory'.
- Administrative account details:** Includes an 'Advanced' section with a checkbox for 'Use the following privileged account:' and a field for 'Account Name' (None).
- Checkout and Check-in Operations:** Includes checkboxes for 'Disable Exclusive Sessions' and 'Deny Exclusive Break-glass'.

At the bottom right of the form are 'Submit' and 'Cancel' buttons.

Use the local Administrator account or create a new account that is a member of the Administrators group.

If you create a new account as was done in the above example you need to modify the Admin Approval Mode.

This is valid on Windows Server 2008 and Windows 7.

SAM endpoint administration tasks run in the background and require access privileges of a native administrator account. If the SAM endpoint administrators do not have access to this native administrator account, you must allow all endpoint administrators to run in Admin Approval Mode.

Members of the Administrators group run in Admin Approval Mode, which (by default) prompts administrators to confirm actions that require more than Standard privileges.

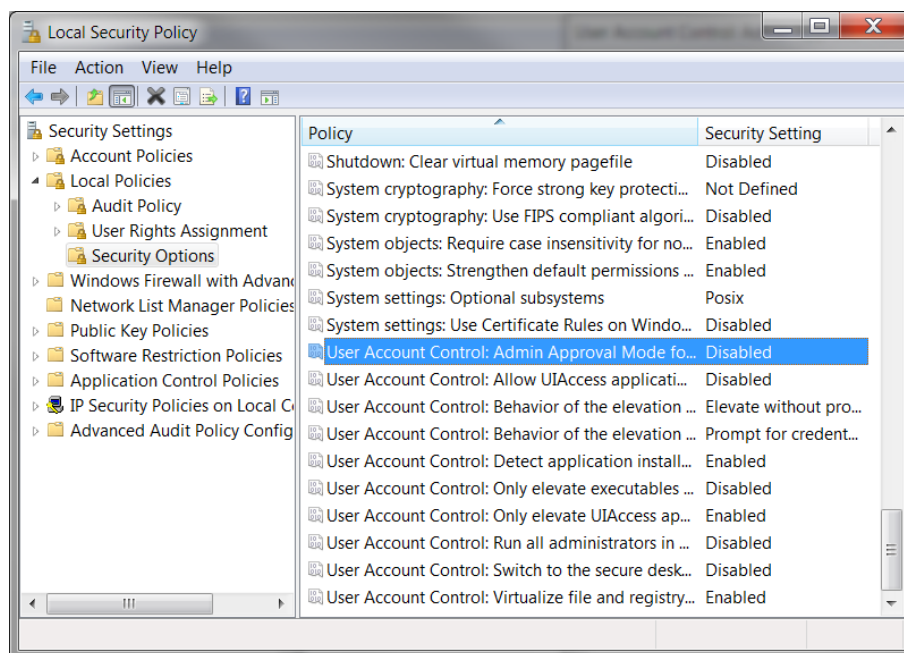
This would block SAM agentless requests if the user is not the Administrator.

Important: If the policy setting is disabled, the Security Center notifies you that the overall security of the operating system has been reduced.

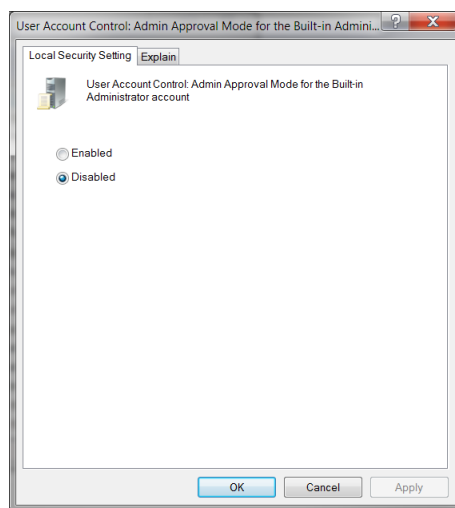
CA ControlMinder Rapid Implementation Guide – Shared Account Management

Follow these steps:

- Select Control Panel, Administrative Tools, Local Security Policy
- The Local Security window opens
- Browse to Local Policies, Security Options
- The Policy Pane opens
- Right-click User Account Control: Run all administrators in Admin Approval Mode and select Properties
- The Properties dialog appears
- Change the operation mode to Disable and click OK
- The Properties dialog closes
- Reboot your computer to apply the change



CA ControlMinder Rapid Implementation Guide – Shared Account Management

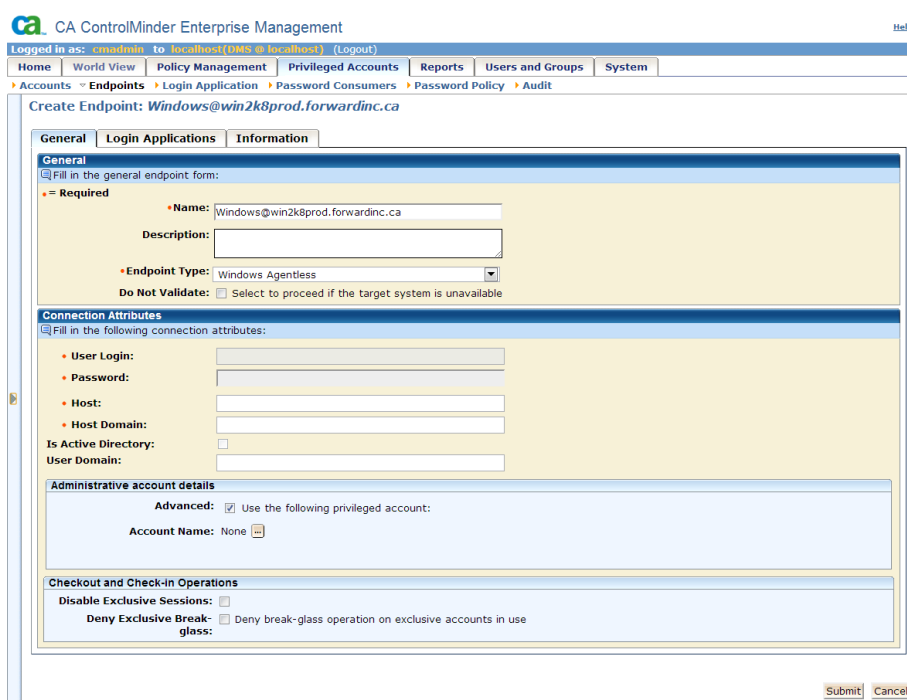


Your background endpoint administration tasks now run successfully.


You can also use a domain account if this endpoint is a member of a MS AD domain.

This account needs to be a member of the local Administrators group.

To use an existing MS AD user select the “Advanced” checkbox.

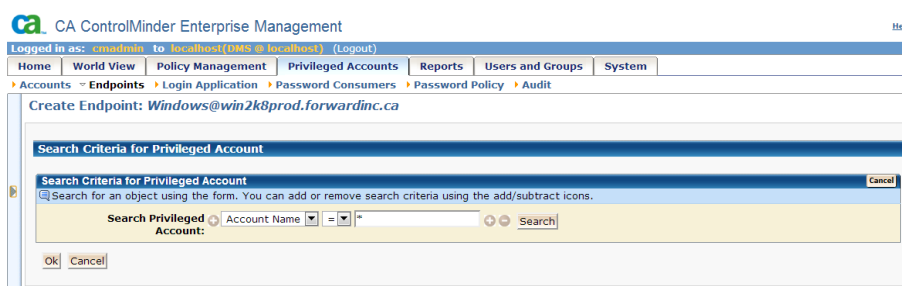


Click the ellipsis button to select the account name to use.

Account Name: None 

CA ControlMinder Rapid Implementation Guide – Shared Account Management

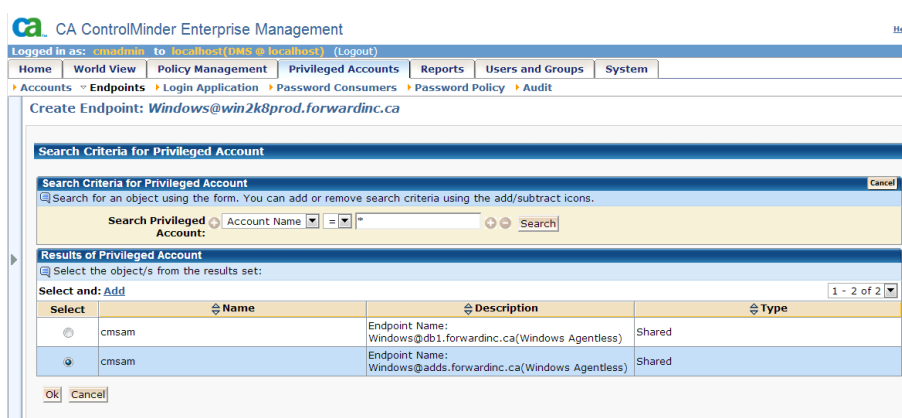
Search for the available accounts.



The screenshot shows the CA ControlMinder Enterprise Management web interface. The user is logged in as 'cmadmin' to 'localhost(DMS @ localhost)'. The breadcrumb trail is: Home > World View > Policy Management > Privileged Accounts > Reports > Users and Groups > System. The current page is 'Create Endpoint: Windows@win2k8prod.forwardinc.ca'. A dialog box titled 'Search Criteria for Privileged Account' is open. It contains a search bar with the text 'Search Privileged Account:' and a dropdown menu set to 'Account Name'. There are 'Add' and 'Subtract' icons, and a 'Search' button. The dialog also has 'Ok' and 'Cancel' buttons at the bottom.

Select an existing account that was already defined to SAM.

A best practice is to use a MS Active Directory account to manage privileged accounts on endpoints that are members of the domain.

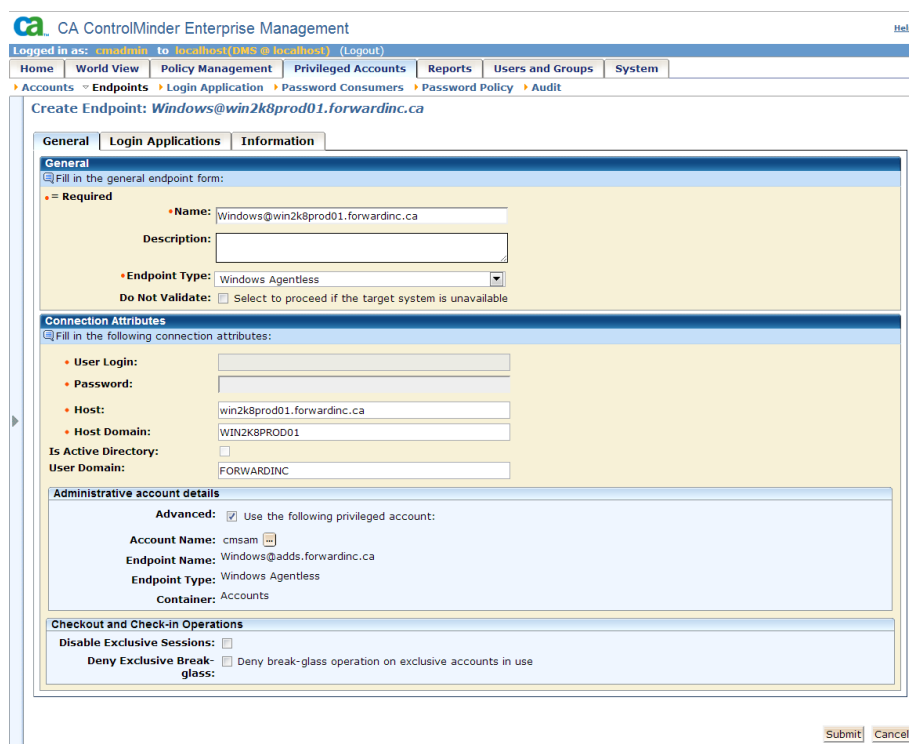


The screenshot shows the same CA ControlMinder Enterprise Management web interface. The 'Search Criteria for Privileged Account' dialog box is now closed, and the 'Results of Privileged Account' dialog box is open. It displays a table of search results. The table has columns for 'Select', 'Name', 'Description', and 'Type'. There are two results listed, both with the name 'cmsam' and type 'Shared'. The first result has the description 'Endpoint Name: Windows@db1.forwardinc.ca(Windows Agentless)'. The second result has the description 'Endpoint Name: Windows@adds.forwardinc.ca(Windows Agentless)'. The dialog also has 'Ok' and 'Cancel' buttons at the bottom.

Select	Name	Description	Type
<input type="radio"/>	cmsam	Endpoint Name: Windows@db1.forwardinc.ca(Windows Agentless)	Shared
<input checked="" type="radio"/>	cmsam	Endpoint Name: Windows@adds.forwardinc.ca(Windows Agentless)	Shared

CA ControlMinder Rapid Implementation Guide – Shared Account Management

As shown below, set the “User Domain” field to the NETBIOS name of the Active Directory domain of the user defined by the “Account Name” field associated with the “Advanced” option.



The screenshot displays the CA ControlMinder Enterprise Management web interface. The breadcrumb trail indicates the path: Accounts > Endpoints > Login Application > Password Consumers > Password Policy > Audit. The current page is titled 'Create Endpoint: Windows@win2k8prod01.forwardinc.ca'.

The form is divided into several sections:

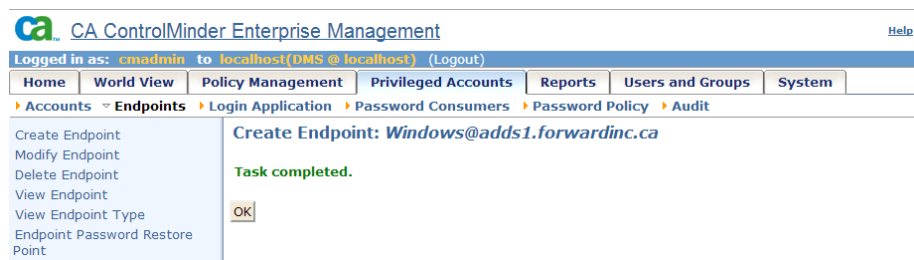
- General:** Contains fields for Name (Windows@win2k8prod01.forwardinc.ca), Description, Endpoint Type (Windows Agentless), and a checkbox for 'Do Not Validate'.
- Connection Attributes:** Contains fields for User Login, Password, Host (win2k8prod01.forwardinc.ca), Host Domain (WIN2K8PROD01), Is Active Directory (unchecked), and User Domain (FORWARDINC).
- Administrative account details:** Includes an 'Advanced' checkbox (checked) and fields for Account Name (cmsam), Endpoint Name (Windows@adds.forwardinc.ca), Endpoint Type (Windows Agentless), and Container (Accounts).
- Checkout and Check-in Operations:** Includes checkboxes for 'Disable Exclusive Sessions' and 'Deny Exclusive Break-glass'.

At the bottom right of the form, there are 'Submit' and 'Cancel' buttons.

CA ControlMinder Rapid Implementation Guide – Shared Account Management

Click **Submit**

You will see the following screen if the endpoint creation is successful.



Windows Endpoint – MS Active Directory Domain

SAM can be used to manage domain users in Active Directory.

You need to have the following ports open to manage MS Active Directory account passwords:

- Port 389
- Port 445

To manage the Active Directory accounts, define a Windows Agentless Endpoint.

You will be presented with the list of options for the selected endpoint type. These options are the same as those described above for Windows endpoints that are not domain controllers.

However, as the managed target is a domain you need to select the “Is Active Directory” option.

The below options are filled in differently in case of MS Active Directory endpoint.

Field name	Description	Additional information
Host	Defines the Active Directory DC name or IP address or DNS domain name.	Note: SAM attempts to resolve the Active Directory domain controller from the domain name. If SAM fails to resolve this name, specify the Active Directory Domain Controller (DC) DNS name or IP address.
Host Domain	Specifies the domain name (NETBIOS name).	Example: domain1 Note: Do not use the DNS name (domain1.ca.com), use the NETBIOS name (domain1).

In the screenshot below we used a domain controller name.

Select a member of the “Domain Admins” group since such an account can manage the password of any domain user.

CA ControlMinder Rapid Implementation Guide – Shared Account Management

CA ControlMinder Enterprise Management Help

Logged in as: cmsadmin to localhost (DMS @ localhost) (Logout)

Home World View Policy Management Privileged Accounts Reports Users and Groups System

Accounts Endpoints Login Application Password Consumers Password Policy Audit

Create Endpoint: *Windows@adds.forwardinc.ca*

General Login Applications Information

General
 Fill in the general endpoint form:

Name: Windows@adds.forwardinc.ca

Description:

Endpoint Type: Windows Agentless

Do Not Validate: ☐ Select to proceed if the target system is unavailable

Connection Attributes
 Fill in the following connection attributes:

User Login: cmsam

Password: *****

Host: adds.forwardinc.ca

Host Domain: FORWARDINC

Is Active Directory: ☒

User Domain:

Administrative account details
 Advanced: ☐ Use the following privileged account:
 Account Name: None

Checkout and Check-in Operations
 Disable Exclusive Sessions: ☐
 Deny Exclusive Break-glass: ☐ Deny break-glass operation on exclusive accounts in use

Submit Cancel

Click “Submit”

UNIX SSH Endpoint

You can manage privileged accounts on UNIX and Linux over ssh or telnet protocols.

You must have the ssh or telnet port to manage SSH Device endpoints.

Field name	Description	Additional information
User Login	Defines the name of an administrative user of the endpoint. SAM uses this account to perform administrative tasks on the endpoint, for example, to connect to the endpoint, discover accounts, and change passwords.	Note the following points: If you specify the Advanced option, SAM does not use the User Login account to perform administrative tasks. Instead, SAM uses the specified privileged account to perform administrative tasks on the endpoint. If you specify an operation administrator account, SAM uses that account to perform administrative tasks on the endpoint, but the account specified by User Login is still used as the connection account unless the “Advanced” option was specified.
Password	Defines the password of the user defined by the above User Login field.	
Host	Defines the host name of the endpoint.	
Use Telnet	Specifies to use Telnet rather than SSH to connect to the SSH device.	Note: The communication to the endpoint is not encrypted in this case.
Operation Administrator User Login	(Optional) Defines the name of an operation administrator user of the endpoint. SAM uses this account to perform administrative tasks on the endpoint, for example, discovering and changing the password of privileged accounts. If you do not specify an operation administrator user, SAM uses the User Login account to perform administrative tasks on the endpoint.	
Operation Administrator Password	(Optional) Defines the password of the operation administrator user.	

Field name	Description	Additional information
Configuration File	Specifies the name of the SSH Device XML configuration file. You can customize the XML files according to your needs.	Note: If you do not specify a value for this field, CA ControlMinder Enterprise Management uses the ssh_connector_conf.xml file.
Advanced	Specifies whether you want to use a privileged administrative account to perform administrative tasks on the endpoint, for example, to connect to the endpoint, discover accounts, and change passwords. For example, you can specify a privileged domain account that can perform administrative tasks on multiple endpoints.	If you specify this option, SAM does not use the User Login account to perform administrative tasks.

When you create an endpoint, you specify the administrator account that SAM uses to connect to the endpoint and perform administrative tasks, such as discovering and changing the password of privileged accounts. For UNIX accounts, the most suitable administrator account is often root. However, SAM uses SSH to connect to UNIX endpoints, and some organizations prohibit users and applications from making SSH connections as the root user.

To overcome this problem, you can specify both a connection account and an operation administrator account when you create an SSH Device endpoint. (SAM uses SSH Device as the endpoint type for UNIX endpoints.) Using two accounts also lets you use a connection account that has fewer privileges than the operation administrator account.

The following process explains how SAM uses these accounts to connect to an SSH Device endpoint:

SAM uses the credentials of the connection account to connect to the endpoint. This is defined by “User Login” field or “Account Name” if “Advanced” option is used.

Using the credentials of the operation administrator account, the connection account connects to the endpoint and switches (su) to the operation administrator account.

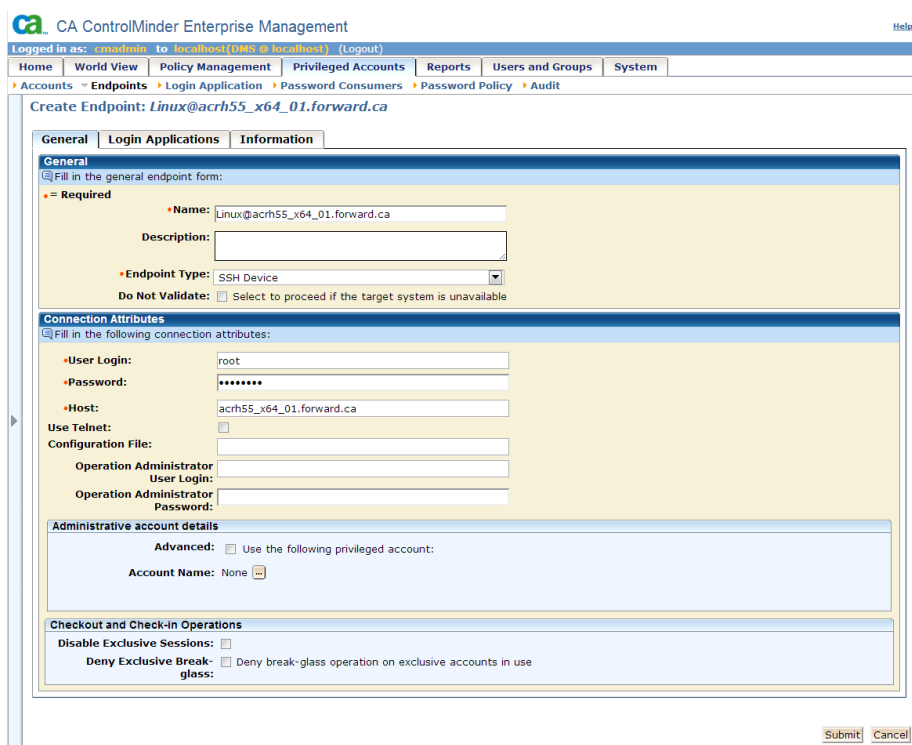
Administrative tasks such as getting a list of accounts and changing passwords are performed by the operation administrator.

For example, if the operation administrator account is root, SAM performs administrative tasks as root.

When you view the privileged accounts on an SSH Device endpoint, both the connection and the operation administrator account are listed as endpoint administrator accounts.

CA ControlMinder Rapid Implementation Guide – Shared Account Management

The first screenshot shows an example where you use the root user account to login directly.



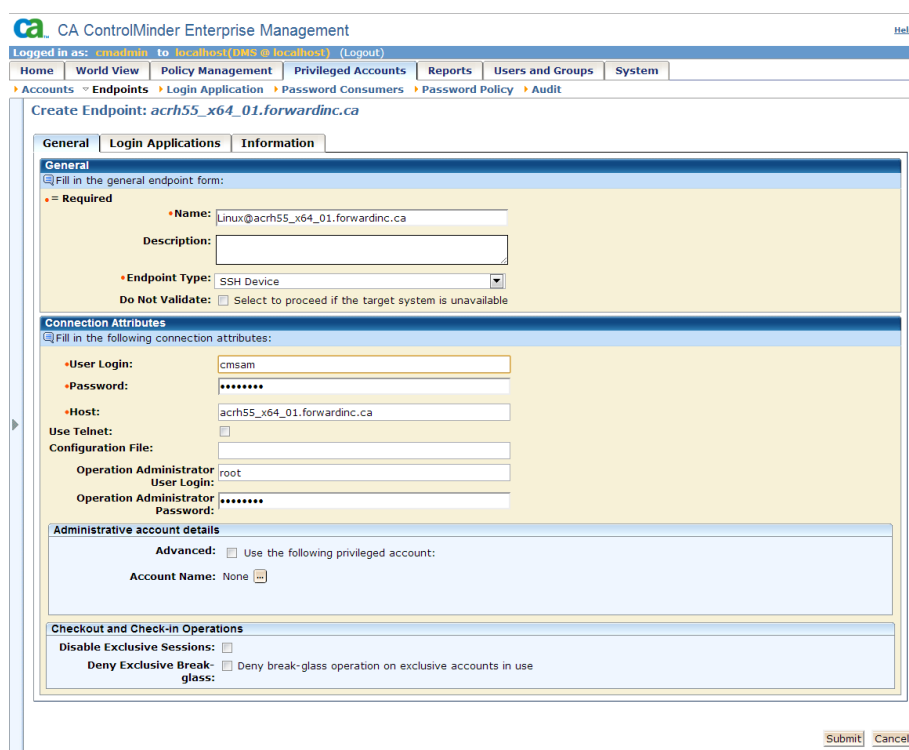
The screenshot displays the CA ControlMinder Enterprise Management web interface. The top navigation bar includes links for Home, World View, Policy Management, Privileged Accounts, Reports, Users and Groups, and System. The main content area is titled 'Create Endpoint: Linux@acrh55_x64_01.forward.ca' and contains several sections:

- General:** Contains fields for Name (Linux@acrh55_x64_01.forward.ca), Description, Endpoint Type (SSH Device), and a checkbox for 'Do Not Validate'.
- Connection Attributes:** Contains fields for User Login (root), Password (masked), Host (acrh55_x64_01.forward.ca), and a checkbox for 'Use Telnet'. It also includes fields for Configuration File, Operation Administrator User Login, and Operation Administrator Password.
- Administrative account details:** Contains an 'Advanced' checkbox and an 'Account Name' field (set to None).
- Checkout and Check-in Operations:** Contains checkboxes for 'Disable Exclusive Sessions' and 'Deny Exclusive Break-glass'.

At the bottom right of the form, there are 'Submit' and 'Cancel' buttons.

CA ControlMinder Rapid Implementation Guide – Shared Account Management

The second screenshot shows the use of an operation administrator account.



The screenshot displays the 'Create Endpoint' form in the CA ControlMinder Enterprise Management web interface. The interface includes a top navigation bar with the CA logo and the title 'CA ControlMinder Enterprise Management'. Below the navigation bar, there is a breadcrumb trail: 'Home > World View > Policy Management > Privileged Accounts > Reports > Users and Groups > System > Accounts > Endpoints > Login Application > Password Consumers > Password Policy > Audit'. The main content area is titled 'Create Endpoint: acr55_x64_01.forwardinc.ca' and contains three tabs: 'General', 'Login Applications', and 'Information'. The 'General' tab is active and shows the following fields:

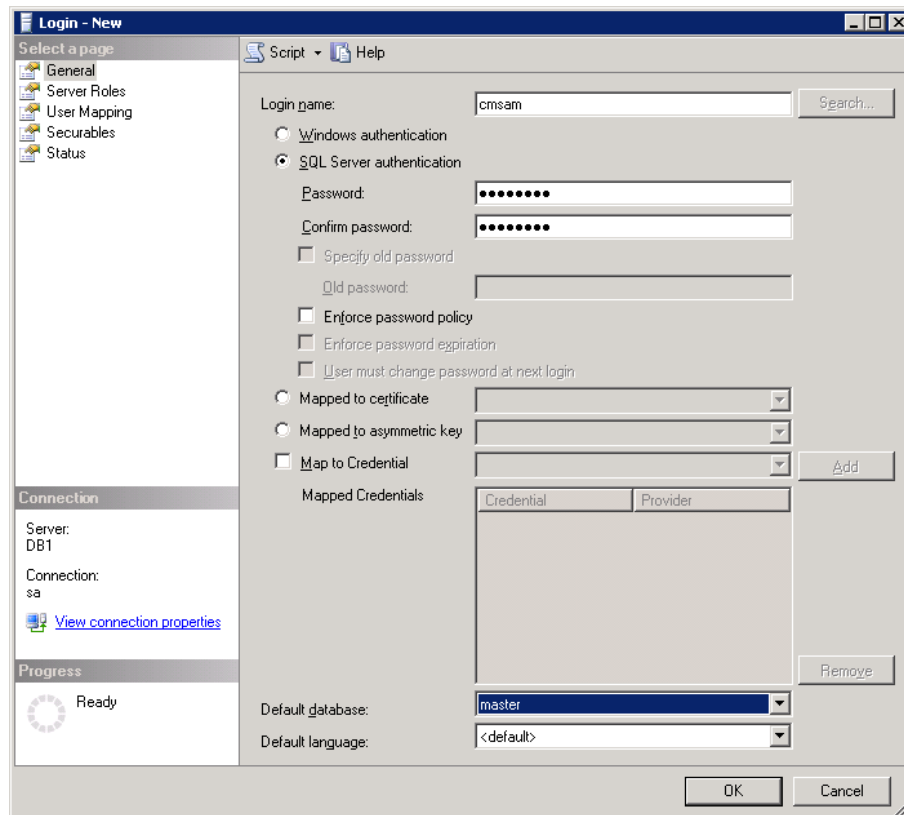
- General**
 - Fill in the general endpoint form:
 - Name:** linux@acr55_x64_01.forwardinc.ca
 - Description:** (empty text box)
 - Endpoint Type:** SSH Device (dropdown menu)
 - Do Not Validate:** ☐ Select to proceed if the target system is unavailable
- Connection Attributes**
 - Fill in the following connection attributes:
 - User Login:** cmsam
 - Password:** (masked with dots)
 - Host:** acr55_x64_01.forwardinc.ca
 - Use Telnet:** ☐
 - Configuration File:** (empty text box)
 - Operation Administrator**
 - User Login: root
 - Password: (masked with dots)
- Administrative account details**
 - Advanced:** ☐ Use the following privileged account:
 - Account Name:** None (dropdown menu)
- Checkout and Check-in Operations**
 - Disable Exclusive Sessions:** ☐
 - Deny Exclusive Break-glass:** ☐ Deny break-glass operation on exclusive accounts in use

At the bottom right of the form, there are 'Submit' and 'Cancel' buttons.

MS SQL Endpoint

The MS SQL Server endpoint type lets you manage privileged Microsoft SQL Server accounts.

The administrative user that you specify for an MS SQL Server endpoint must have the securityadmin server role. Use MS SQL Server Management Studio to create the user as shown below.



Login - New

Select a page: General, Server Roles, User Mapping, Securables, Status

Script Help

Login name: cmsam Search...

☐ Windows authentication

☒ SQL Server authentication

Password:

Confirm password:

☐ Specify old password

Old password:

☐ Enforce password policy

☐ Enforce password expiration

☐ User must change password at next login

☒ Mapped to certificate

☐ Mapped to asymmetric key

☐ Map to Credential

Mapped Credentials

Credential	Provider
------------	----------

Add Remove

Default database: master

Default language: <default>

OK Cancel

Connection

Server: DB1

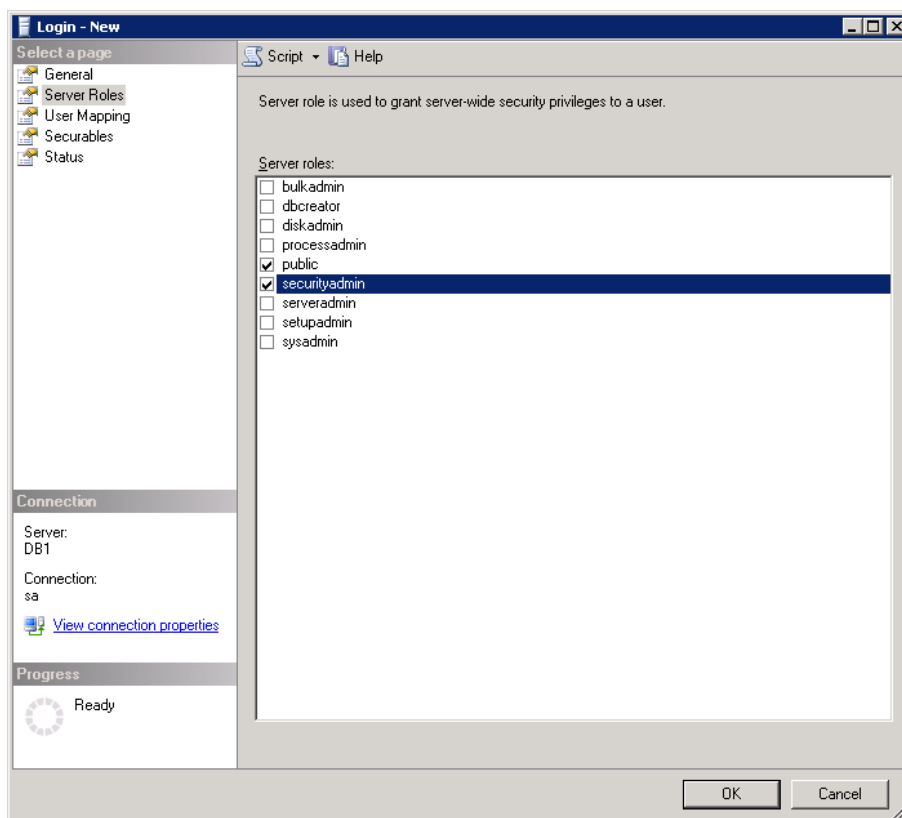
Connection: sa

[View connection properties](#)

Progress

Ready

From the Server roles definition, select **securityadmin**.



Click “OK”.

Select MS SQL Server when creating an endpoint.

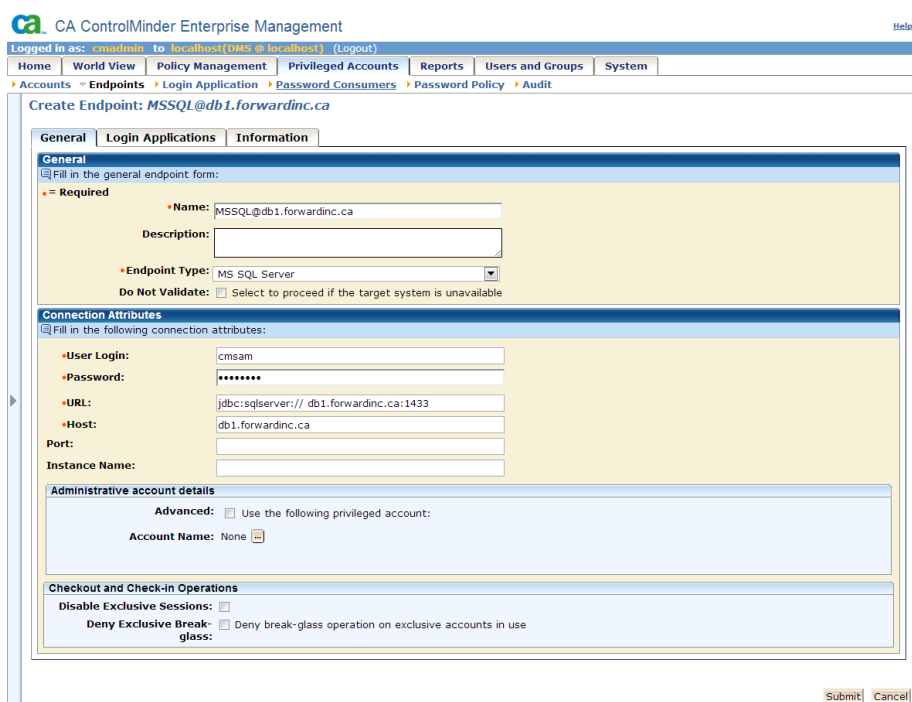
The below fields are specific to MS SQL Server endpoint.

Field name	Description	Additional information
URL	Defines the URL that CA ControlMinder Enterprise Management can use to connect to the endpoint. The URL specifies a particular type of database server.	Format: jdbc:sqlserver://servername:port Example: jdbc:sqlserver://db_hostname:1433
Port	(Optional) Specifies the server listening port number. The port number that you specify must match the port number that you specify in the URL.	The port number is required when you use login applications.

CA ControlMinder Rapid Implementation Guide – Shared Account Management

Field name	Description	Additional information
Instance Name	(Optional) Specifies the MS SQL Server instance name.	

The screenshot below shows an example of MS SQL Server endpoint configuration.



The screenshot displays the 'Create Endpoint: MSSQL@db1.forwardinc.ca' configuration page in the CA ControlMinder Enterprise Management web interface. The page is divided into several sections:

- General:** Contains fields for 'Name' (MSSQL@db1.forwardinc.ca), 'Description', 'Endpoint Type' (MS SQL Server), and a 'Do Not Validate' checkbox.
- Connection Attributes:** Contains fields for 'User Login' (cmsam), 'Password' (masked), 'URL' (jdbc:sqlserver://db1.forwardinc.ca:1433), 'Host' (db1.forwardinc.ca), 'Port', and 'Instance Name'.
- Administrative account details:** Includes an 'Advanced' checkbox and an 'Account Name' dropdown set to 'None'.
- Checkout and Check-in Operations:** Includes checkboxes for 'Disable Exclusive Sessions' and 'Deny Exclusive Break-glass'.

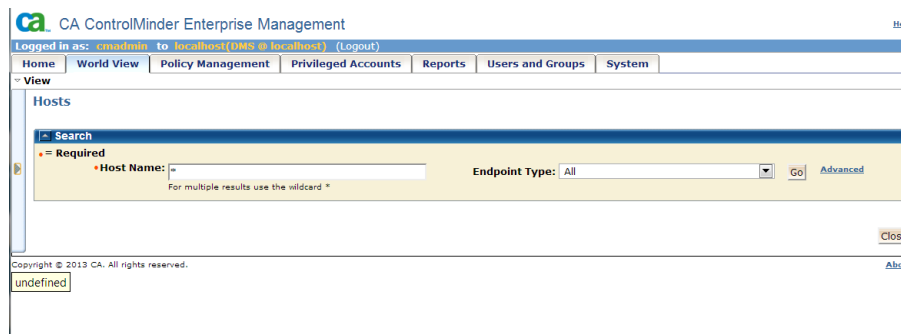
At the bottom right, there are 'Submit' and 'Cancel' buttons.

CA ControlMinder Rapid Implementation Guide – Shared Account Management

Verify Created Endpoints

Navigate to WorldView -> View -> Hosts

Click “Go” to search for all the available endpoints.



CA ControlMinder Enterprise Management

Logged in as: [cmadmin](#) to [localhost\(DMS @ localhost\)](#) (Logout)

Home World View Policy Management Privileged Accounts Reports Users and Groups System

View

Hosts

Search

Required

Host Name: Endpoint Type: All

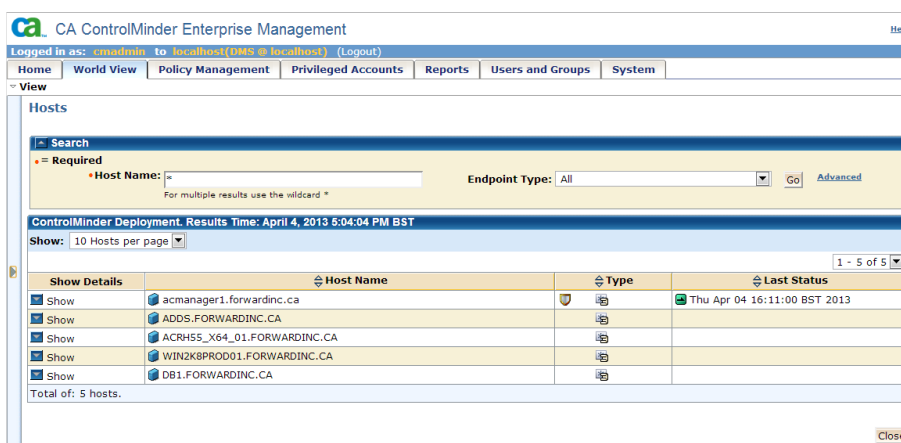
For multiple results use the wildcard *

Close

Copyright © 2013 CA. All rights reserved.

About

You should see all the endpoints you have already defined.



CA ControlMinder Enterprise Management

Logged in as: [cmadmin](#) to [localhost\(DMS @ localhost\)](#) (Logout)

Home World View Policy Management Privileged Accounts Reports Users and Groups System

View

Hosts

Search

Required

Host Name: Endpoint Type: All

For multiple results use the wildcard *

ControlMinder Deployment. Results Time: April 4, 2013 5:04:04 PM BST

Show: 10 Hosts per page

1 - 5 of 5

Show Details	Host Name	Type	Last Status
Show	acmanager1.forwardinc.ca	Agentless	Thu Apr 04 16:11:00 BST 2013
Show	ADDS.FORWARDINC.CA	Agentless	
Show	ACRH55_X64_01.FORWARDINC.CA	Agentless	
Show	WIN2K8PROD01.FORWARDINC.CA	Agentless	
Show	DB1.FORWARDINC.CA	Agentless	

Total of: 5 hosts.

Close

And you can verify these endpoints are managed devices in SAM.

Click “Show” to display the devices.

Note that the ENTM server was defined as a managed endpoint during product installation.

You can see in the screenshot below that for db1.forardinc.ca there are 2 managed devices (Windows Agentless and MS SQL Server).

CA ControlMinder Rapid Implementation Guide – Shared Account Management

CA ControlMinder Enterprise Management Help

Logged in as: cadmin to localhost (DMS @ localhost) (Logout)

Home World View Policy Management Privileged Accounts Reports Users and Groups System

View

Hosts

Search

Host Name: Endpoint Type: All [Advanced](#)

For multiple results use the wildcard *

ControlMinder Deployment Results Time: April 4, 2013 5:25:22 PM BST

Show: 10 Hosts per page 1 - 5 of 5

Show Details	Host Name	Type	Last Status
<input checked="" type="checkbox"/> Show	acmanager1.forwardinc.ca		Thu Apr 04 16:11:00 BST 2013
<input checked="" type="checkbox"/> Hide	ADDS.FORWARDINC.CA		
	Managed Devices: Total of 1 managed devices @Windows@adds.forwardinc.ca (Windows Agentless) Modify View Accounts Add		
<input checked="" type="checkbox"/> Hide	ACRH55_X64_01.FORWARDINC.CA		
	Managed Devices: Total of 1 managed devices @Linux@acrh55_x64_01.forwardinc.ca (SSH Device) Modify View Accounts Add		
<input checked="" type="checkbox"/> Hide	WIN2K8PROD01.FORWARDINC.CA		
	Managed Devices: Total of 1 managed devices @Windows@win2k8prod01.forwardinc.ca (Windows Agentless) Modify View Accounts Add		
<input checked="" type="checkbox"/> Hide	DB1.FORWARDINC.CA		
	Managed Devices: Total of 2 managed devices @Windows@db1.forwardinc.ca (Windows Agentless) Modify View Accounts Add @MSSQL@db1.forwardinc.ca (MS SQL Server) Modify View Accounts Add		

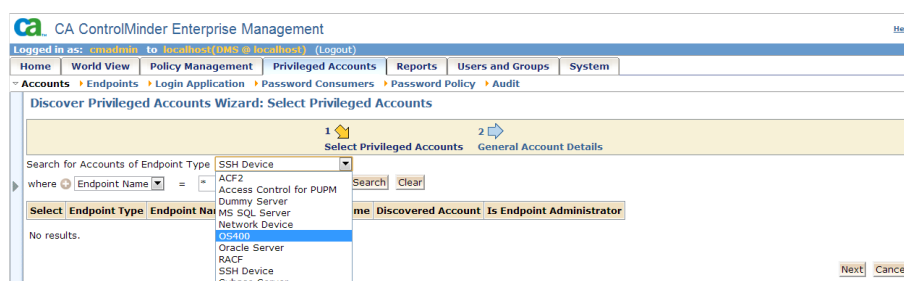
Total of: 5 hosts.

Privileged Accounts Discovery

You can run the privileged accounts discovery process to scan for new privileged accounts on the endpoints. Discovering privileged accounts lets you create multiple privileged accounts at the same time. CA ControlMinder Enterprise Management presents the accounts that it discovers in a table, so that you can easily tell which accounts you already manage with SAM.

Navigate to Privileged Accounts/Accounts/Discover Privileged Accounts

Select Endpoint Type from the drop down.



CA ControlMinder Enterprise Management

Logged in as: [cmadmin](#) to [localhost \(DM3 @ localhost\)](#) (Logout)

Home | World View | Policy Management | Privileged Accounts | Reports | Users and Groups | System

Accounts > Endpoints > Login Application > Password Consumers > Password Policy > Audit

Discover Privileged Accounts Wizard: Select Privileged Accounts

1 Select Privileged Accounts 2 General Account Details

Search for Accounts of Endpoint Type SSH Device

where Endpoint Name = *

Select Endpoint Type Endpoint Name

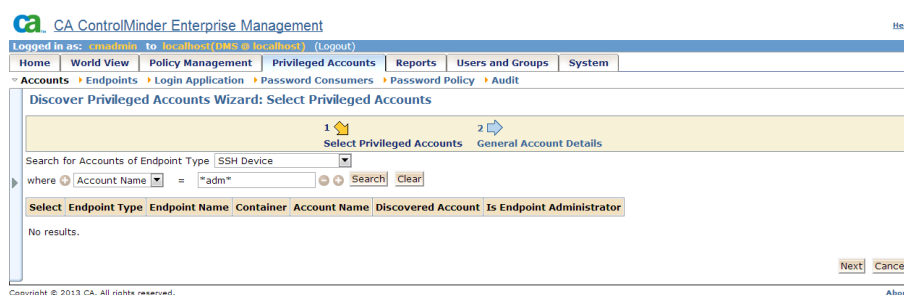
No results.

me Discovered Account Is Endpoint Administrator

Next Cancel

Fill in the search criteria you want to use when discovering the accounts.

Using wildcards, you can limit the accounts that are returned by your search.



CA ControlMinder Enterprise Management

Logged in as: [cmadmin](#) to [localhost \(DM3 @ localhost\)](#) (Logout)

Home | World View | Policy Management | Privileged Accounts | Reports | Users and Groups | System

Accounts > Endpoints > Login Application > Password Consumers > Password Policy > Audit

Discover Privileged Accounts Wizard: Select Privileged Accounts

1 Select Privileged Accounts 2 General Account Details

Search for Accounts of Endpoint Type SSH Device

where Account Name = *adm*

Select Endpoint Type Endpoint Name Container Account Name Discovered Account Is Endpoint Administrator

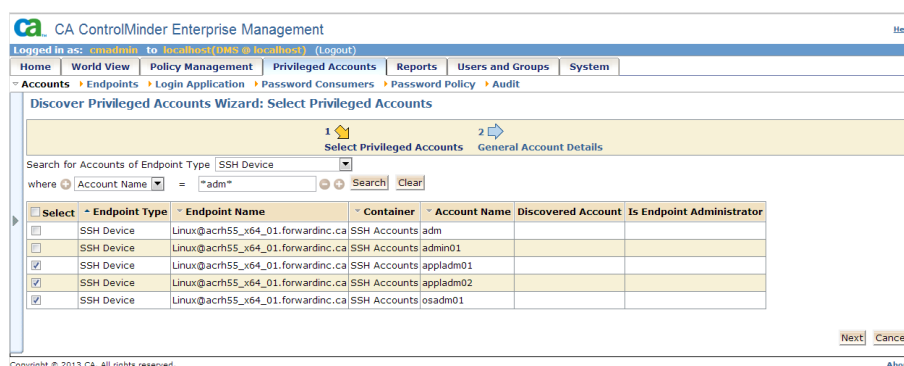
No results.

Next Cancel

Copyright © 2013 CA. All rights reserved. About

You will get the accounts from the managed systems that match the criteria.

Select the accounts you want to manage as privileged accounts and click “Next”.



CA ControlMinder Enterprise Management

Logged in as: [cmadmin](#) to [localhost \(DM3 @ localhost\)](#) (Logout)

Home | World View | Policy Management | Privileged Accounts | Reports | Users and Groups | System

Accounts > Endpoints > Login Application > Password Consumers > Password Policy > Audit

Discover Privileged Accounts Wizard: Select Privileged Accounts

1 Select Privileged Accounts 2 General Account Details

Search for Accounts of Endpoint Type SSH Device

where Account Name = *adm*

Select Endpoint Type Endpoint Name Container Account Name Discovered Account Is Endpoint Administrator

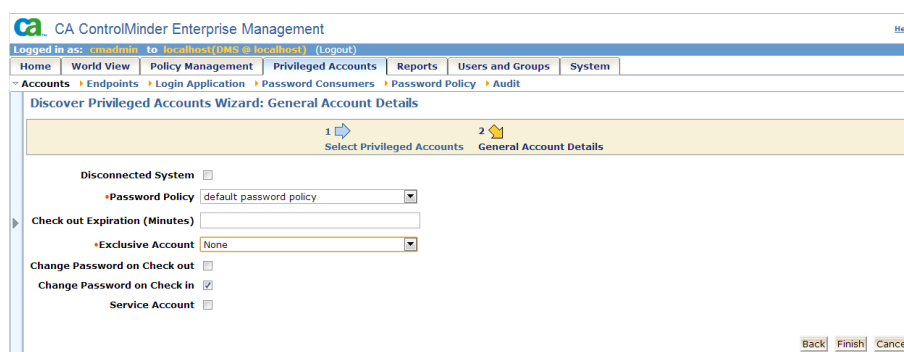
<input type="checkbox"/>	SSH Device	Linux@acr55_x64_01.forwardinc.ca	SSH Accounts	adm		
<input type="checkbox"/>	SSH Device	Linux@acr55_x64_01.forwardinc.ca	SSH Accounts	admin01		
<input checked="" type="checkbox"/>	SSH Device	Linux@acr55_x64_01.forwardinc.ca	SSH Accounts	appladm01		
<input checked="" type="checkbox"/>	SSH Device	Linux@acr55_x64_01.forwardinc.ca	SSH Accounts	appladm02		
<input type="checkbox"/>	SSH Device	Linux@acr55_x64_01.forwardinc.ca	SSH Accounts	osadm01		

Next Cancel

Copyright © 2013 CA. All rights reserved. About

CA ControlMinder Rapid Implementation Guide – Shared Account Management

You will see a screen with privileged account properties.



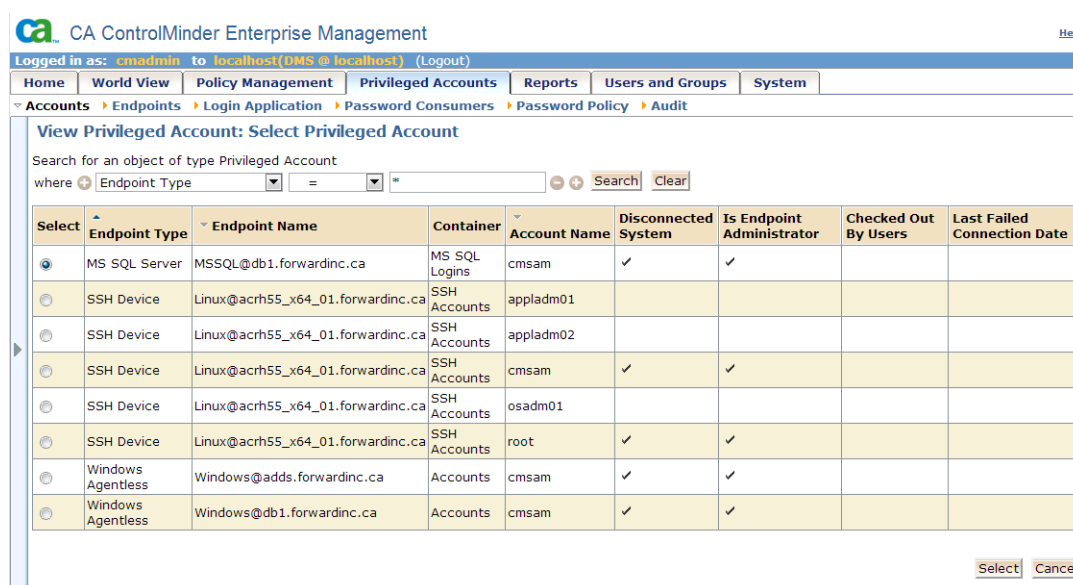
The table below describes the meaning of the attributes.

Field name	Description	Additional information
Disconnected System	Specifies whether the account originates from a disconnected system.	If you select this option, SAM does not manage the account. Instead, it acts only as a password vault for privileged accounts of the disconnected system. Every time you change the password, you also need to manually change the account password on the managed endpoint.
Password Policy	Specifies the password policy you want to apply to the privileged or service account.	Make sure that the password policy meets the requirements of the target system. You can create multiple password policies.
Check out Expiration	Defines the duration, in minutes, before the checked out account expires.	
Exclusive Account	Specifies whether only a single user can use the account at any one time. An <i>exclusive account</i> is a restriction imposed on a privileged account that limits use of the account to a single user at a time.	Exclusive Session specifies that only a single user can use the account, if no open sessions are currently running on the endpoint.
Change Password on Check Out	Specifies whether you want CA ControlMinder Enterprise Management to change the password of the privileged account every time it is checked out.	Note: This option does not apply to service accounts.

CA ControlMinder Rapid Implementation Guide – Shared Account Management

Field name	Description	Additional information
Change Password on Check In	Specifies whether you want CA ControlMinder Enterprise Management to change the password of the privileged account every time it is checked in by a user or a program, or when the checkout period expires.	Note: If the account is not exclusive, CA ControlMinder Enterprise Management generates a new privileged account password only when <i>all</i> users have checked in the account. This option does not apply to service accounts.
Service Account	Specifies whether the discovered account is a service account.	Note: You can also use the Discover Service Accounts Wizard to discover service accounts.

To verify that the accounts were added successfully go to Privileged Account/Accounts/View Privileged Accounts.



CA ControlMinder Enterprise Management

Logged in as: **cmadmin** to **localhost(OHMS @ localhost)** (Logout)

Home World View Policy Management Privileged Accounts Reports Users and Groups System

Accounts Endpoints Login Application Password Consumers Password Policy Audit

View Privileged Account: Select Privileged Account

Search for an object of type Privileged Account
where Endpoint Type = Search Clear

Select	Endpoint Type	Endpoint Name	Container	Account Name	Disconnected System	Is Endpoint Administrator	Checked Out By Users	Last Failed Connection Date
<input checked="" type="radio"/>	MS SQL Server	MSSQL@db1.forwardinc.ca	MS SQL Logins	cmsam	✓	✓		
<input type="radio"/>	SSH Device	Linux@acrh55_x64_01.forwardinc.ca	SSH Accounts	appladm01				
<input type="radio"/>	SSH Device	Linux@acrh55_x64_01.forwardinc.ca	SSH Accounts	appladm02				
<input type="radio"/>	SSH Device	Linux@acrh55_x64_01.forwardinc.ca	SSH Accounts	cmsam	✓	✓		
<input type="radio"/>	SSH Device	Linux@acrh55_x64_01.forwardinc.ca	SSH Accounts	osadm01				
<input type="radio"/>	SSH Device	Linux@acrh55_x64_01.forwardinc.ca	SSH Accounts	root	✓	✓		
<input type="radio"/>	Windows Agentless	Windows@adds.forwardinc.ca	Accounts	cmsam	✓	✓		
<input type="radio"/>	Windows Agentless	Windows@db1.forwardinc.ca	Accounts	cmsam	✓	✓		

Select Cancel

You will see the accounts you discovered listed.

The accounts marked “Disconnected System” and “Is Endpoint Administrator” are the accounts you used to acquire the endpoints. These are so called connection accounts and by default CM SAM is not managing the passwords of these accounts.

Repeat this process for all endpoints that contain privileged accounts of interest.

CM SAM can also manage passwords of the connection accounts.

We suggest that you keep the connection accounts as disconnected (passwords are not managed) while user acceptance testing is in progress.

CA ControlMinder Rapid Implementation Guide – Shared Account Management

You can edit the accounts later to change an Administrative account from Disconnected to Connected.

Navigate to Privileged Accounts\Accounts\Modify Privileged Account to change an account from connected to disconnected.

Search for an account you want to modify.

Select the account and click “Next”.

CA ControlMinder Enterprise Management Help

Logged in as: **cmadmin** to **localhost(DMS @ localhost)** (Logout)

Home | World View | Policy Management | **Privileged Accounts** | Reports | Users and Groups | System

Accounts > Endpoints > Login Application > Password Consumers > Password Policy > Audit

Modify Privileged Account: Select Privileged Account

Search for an object of type Privileged Account
 where Endpoint Type = *

Select	Endpoint Type	Endpoint Name	Container	Account Name	Disconnected System	Is Endpoint Administrator	Checked Out By Users	Last Failed Connection Date
<input type="radio"/>	MS SQL Server	MSSQL@db1.forwardinc.ca	MS SQL Logins	cmsam	✓	✓		
<input type="radio"/>	SSH Device	Linux@acrh55_x64_01.forwardinc.ca	SSH Accounts	appladm01				
<input type="radio"/>	SSH Device	Linux@acrh55_x64_01.forwardinc.ca	SSH Accounts	appladm02				
<input type="radio"/>	SSH Device	Linux@acrh55_x64_01.forwardinc.ca	SSH Accounts	cmsam	✓	✓		
<input type="radio"/>	SSH Device	Linux@acrh55_x64_01.forwardinc.ca	SSH Accounts	osadm01				
<input type="radio"/>	SSH Device	Linux@acrh55_x64_01.forwardinc.ca	SSH Accounts	root	✓	✓		
<input checked="" type="radio"/>	Windows Agentless	Windows@adds.forwardinc.ca	Accounts	cmsam	✓	✓		
<input type="radio"/>	Windows Agentless	Windows@db1.forwardinc.ca	Accounts	cmsam	✓	✓		
<input type="radio"/>	Windows Agentless	Windows@win2k8prod01.forwardinc.ca	Accounts	appladm01				
<input type="radio"/>	Windows Agentless	Windows@win2k8prod01.forwardinc.ca	Accounts	osadm01				

1 2 >

Uncheck the “Disconnected Account” check box.

Click “Submit”.

CA ControlMinder Rapid Implementation Guide – Shared Account Management

CA ControlMinder Enterprise Management Help

Logged in as: **cmadmin** to **localhost(DMS @ localhost)** (Logout)

Home World View Policy Management Privileged Accounts Reports Users and Groups System

Accounts Endpoints Login Application Password Consumers Password Policy Audit

Modify Privileged Account: name: "cmsam" on "Windows@adds.forwardinc.ca" Accounts ("Windows Agentless").

General Password Consumers Information

General

Fill in the privileged account form:

• **Required**

• **Account Name:** cmsam

Disconnected Account: ☐

• **Account Type:** Shared

• **Endpoint Name:** Windows@adds.forwardinc.ca

• **Endpoint Type:** Windows Agentless

• **Container:** Accounts

Do Not Validate: ☐ Select to proceed if the target system is unavailable

Password

• **Password Policy:** default password policy

Password Last Modified Date (GMT):

Check-out and Check-in Operations

Check out Expiration (Minutes):

Exclusive Account: None Exclusive Sessions are not available for administrative account

Change Password on Check out: ☐ Generate a new password for the check-out session

Change Password on Check in: ☒

Login Application Checkout Only: ☐

[Return to Search](#) [Submit](#) [Cancel](#)

Note that CA SAM will change the password of this account periodically based on the assigned password policy.

If you do not want the account password to be changed keep this account as disconnected.

ENTM Administration Role Scoping

Administration Roles

Predefined admin roles in CA ControlMinder Enterprise Management provide a basic set of admin roles that you can assign to administrators in your enterprise according to your requirements. Admin roles of interest to Shared Account Management customers include:

- **System Manager**—Responsible for managing CA ControlMinder Enterprise Management. A user with this admin role can perform, create, and manage all tasks in CA ControlMinder Enterprise Management. Use this role for the implementation phase to define the actual admin roles in your organization and for emergency situations. We recommend that you assign this role to a minimal number of users, ideally only one user, and closely monitor this user's actions.
- **Customized System Manager**—Consider creating a Customized System Manager role because the out-of-the-box System Manager role has all privileged accounts available for checkout.
- **Reporting**—Responsible for managing English reports. A user with this role can schedule and view reports.
- **CA Enterprise Log Manager User**—Responsible for viewing CA Enterprise Log Manager Reports. A user with this role can view CA Enterprise Log Manager Reports.
- **CA Enterprise Log Manager Admin**—Responsible for managing CA Enterprise Log Manager Reports. A user with this role can administer the CA Enterprise Log Manager reports in CA ControlMinder Enterprise Management and manage the connection to the CA Enterprise Log Manager server.
- **Self Manager**—Responsible for managing their own user account. A user with this role can perform administrative actions on their account: change the account password, modify their user profile, view their assigned roles, submitted tasks, and the items that are waiting for their approval.

Note: By default, every user in the system is assigned the Self Manager role.

Privileged Access Roles

The following roles are relevant to SAM.

- **SAM User**—A user with this role can check out and check in privileged account passwords to which the user is permitted. This role is assigned by default to all the users in CA ControlMinder Enterprise Management. The three ways a user can check out a privileged account are:
 - By always being granted access to a privileged account(s). No approval is required.
 - Through approval of a user's Privileged Account Request. When approved, access is granted as a Privileged Account Exception.
 - By always being granted access to a privileged account via Break Glass. By default, the Privileged Account owner is notified when a privileged account password is checked out via Break Glass. Under normal circumstances the user would submit a Privileged Account Request for approval. Under emergency situations, the user can check out a privileged account password without having to wait for approval.
- **Privileged Account Request**— A user with this role can submit or delete requests for privileged account passwords. This role is assigned by default to all the users in CA ControlMinder Enterprise Management.
- **SAM Approver**— A user with this role can respond to privileged access requests that CA ControlMinder Enterprise Management users have submitted. Approving the request grants the requestor a Privileged Account Exception. This role is assigned by default to all the users in CA ControlMinder Enterprise Management, but, by default, only the owner of a privileged account can approve or deny access to that privileged account. Beginning with CA ControlMinder r12.7, the owner can be a specific user or a group of users. NOTE: A user with the System Manager role can approve or deny any Privileged Account Request.
- **Break Glass**— This role allows a user to check out a privileged account password via Break Glass for those privileged accounts to which the user has been granted Break Glass access. By default, all users are assigned this role but have no Break Glass access to any privileged account.
- **Endpoint Privileged Access Role**— A user with this role can perform privileged account tasks on the specified endpoint type. The first time that you define a new type of endpoint, CA ControlMinder creates a corresponding endpoint privileged access role. For example, the first time you create a Windows endpoint in CA ControlMinder Enterprise Management, CA ControlMinder creates the Windows Agentless Connection endpoint privileged access role.
- **SAM Audit Manager**— A user with this role can audit privileged account activity and manage the CA Enterprise Log Manager audit collection parameters.

- **SAM Policy Manager**— A user with this role can manage role members and member polices, assign role owners, and create and delete roles.
- **SAM Target System Manager**—A user with this role can administer password policies and privileged accounts, and can execute the privileged accounts discovery wizard to discover privileged accounts on endpoints. This role also provides the means to delete a Privileged Account Exception. Deleting a Privileged Account Exception results in voiding a previously approved Privileged Account Request.
- **SAM User Manager**—A user with this role can administer CA ControlMinder Enterprise Management users and groups and password policies, and manage the work items of users.

Changing the Scope of Default Roles

By default, some of the predefined roles have membership rules set to “all”. This means that all the users are members of these roles.

The roles where the default of “all” is relevant are listed below:

- Break Glass
- Privileged Account Request
- SAM Approver
- SAM User
- Self-Manager

This means that all the users that are defined in the ENTM user store are allowed to:

- Login into ENTM.
- Request any account password through a predefined workflow process.
- Approve privileged account requests if processed via workflow. This is just for requests that are routed to the user for approval.
- Use the Break Glass task within the defined scope. (The default scope is that no accounts are allowed to use the break glass functionality.)

It is a best practice to modify the membership rules of the above roles to allow only a predefined set of users to access roles listed above by limiting the membership with respect to users, groups and other criteria.

As an example, we shall limit the membership by AD group by creating a new group in AD and assigning all SAM users to this group. You can also use an existing AD group if a suitable group already exists.

We created a group named “CA CM Users” that all the users of CA CM SAM will be members of.

CA ControlMinder Rapid Implementation Guide – Shared Account Management

Login to ENTM using an account with System Manager permissions.

Click on **Users and Groups** tab

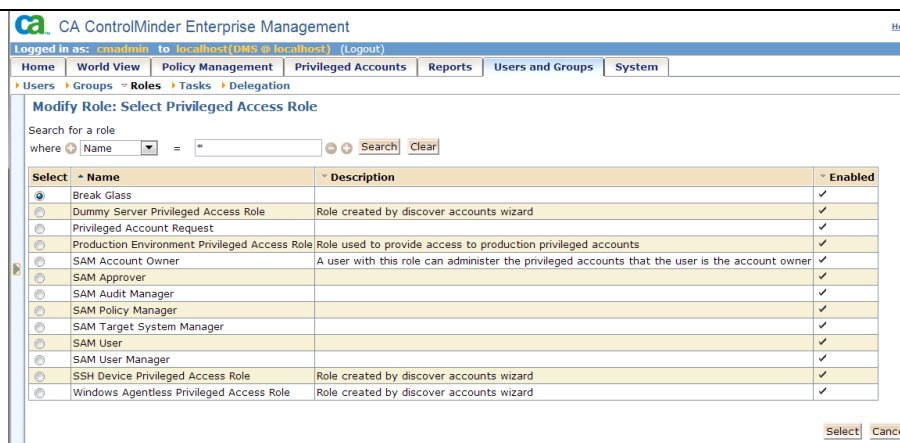
Select Roles

Select Privileged Access Role

Select Modify Role

Select one of the above mentioned roles.

The “Break Glass” role was used as an example.



CA ControlMinder Enterprise Management

Logged in as: **cmadmin** to **localhost(DMS @ localhost)** (Logout)

Home | World View | Policy Management | Privileged Accounts | Reports | Users and Groups | System

Users > Groups > Roles > Tasks > Delegation

Modify Role: Select Privileged Access Role

Search for a role where

Select	Name	Description	Enabled
<input type="radio"/>	Break Glass		<input checked="" type="checkbox"/>
<input type="radio"/>	Dummy Server Privileged Access Role	Role created by discover accounts wizard	<input checked="" type="checkbox"/>
<input type="radio"/>	Privileged Account Request		<input checked="" type="checkbox"/>
<input type="radio"/>	Production Environment Privileged Access Role	Role used to provide access to production privileged accounts	<input checked="" type="checkbox"/>
<input type="radio"/>	SAM Account Owner	A user with this role can administer the privileged accounts that the user is the account owner	<input checked="" type="checkbox"/>
<input type="radio"/>	SAM Approver		<input checked="" type="checkbox"/>
<input type="radio"/>	SAM Audit Manager		<input checked="" type="checkbox"/>
<input type="radio"/>	SAM Policy Manager		<input checked="" type="checkbox"/>
<input type="radio"/>	SAM Target System Manager		<input checked="" type="checkbox"/>
<input type="radio"/>	SAM User		<input checked="" type="checkbox"/>
<input type="radio"/>	SAM User Manager		<input checked="" type="checkbox"/>
<input type="radio"/>	SSH Device Privileged Access Role	Role created by discover accounts wizard	<input checked="" type="checkbox"/>
<input type="radio"/>	Windows Agentless Privileged Access Role	Role created by discover accounts wizard	<input checked="" type="checkbox"/>

Login to ENTM using an account with System Manager permissions.

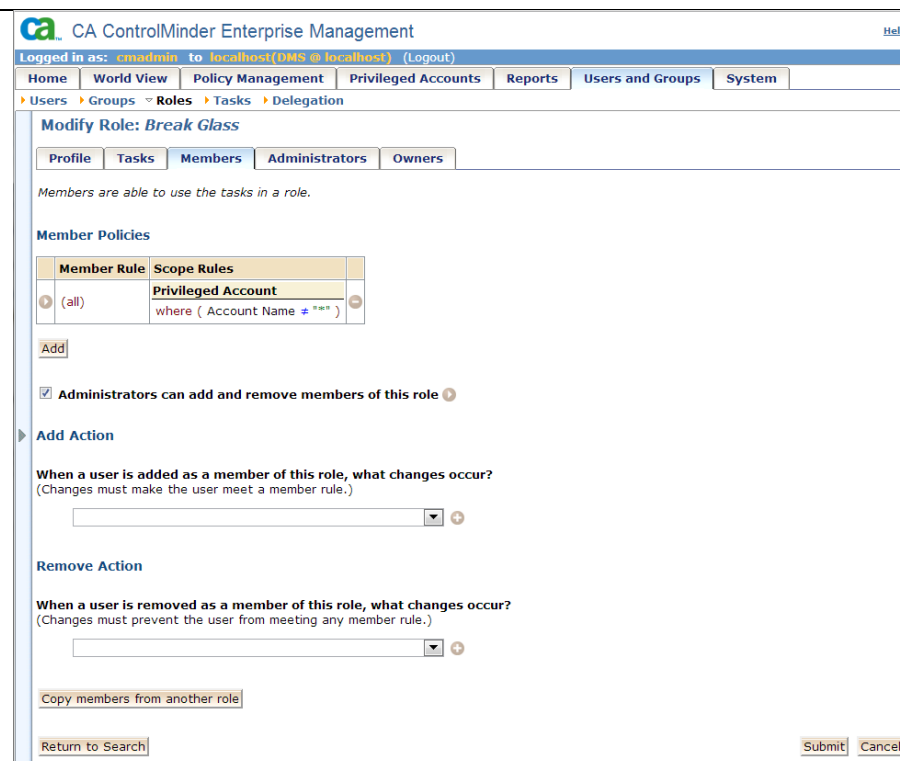
Click on **Users and Groups** tab

Select Roles

Select Privileged Access Role

Select Modify Role

Click on Members tab



CA ControlMinder Enterprise Management

Logged in as: **cmadmin** to **localhost(DMS @ localhost)** (Logout)

Home | World View | Policy Management | Privileged Accounts | Reports | Users and Groups | System

Users > Groups > Roles > Tasks > Delegation

Modify Role: Break Glass

Profile | Tasks | Members | Administrators | Owners

Members are able to use the tasks in a role.

Member Policies

Member Rule	Scope Rules
<input type="radio"/> (all)	Privileged Account where (Account Name = "SAM")

☒ Administrators can add and remove members of this role

Add Action

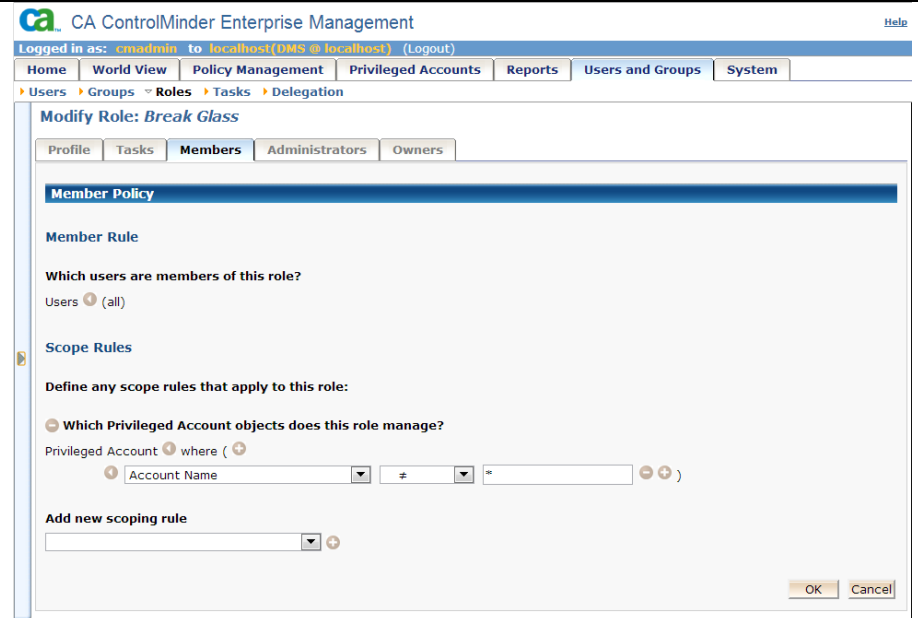
When a user is added as a member of this role, what changes occur?
(Changes must make the user meet a member rule.)

Remove Action

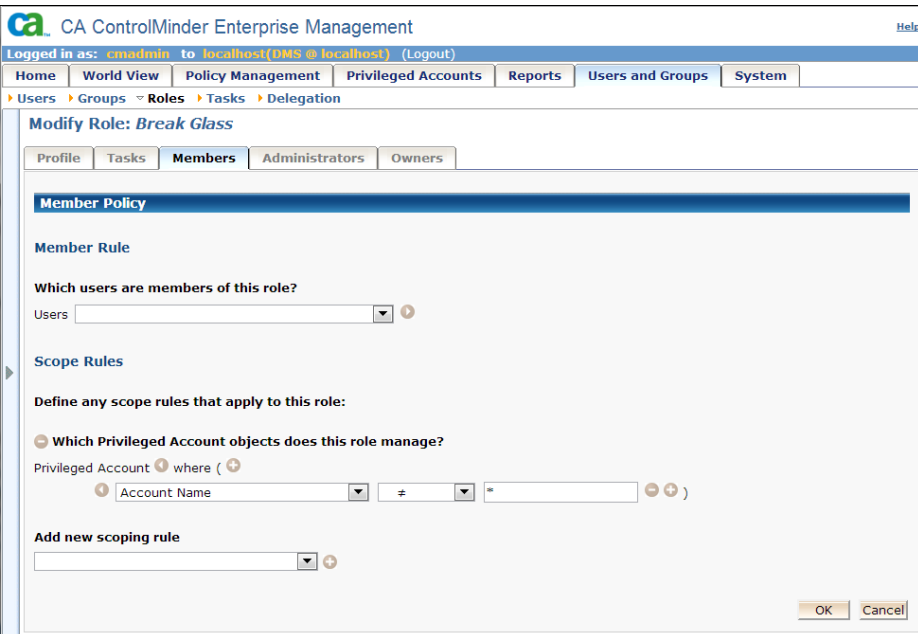
When a user is removed as a member of this role, what changes occur?
(Changes must prevent the user from meeting any member rule.)

CA ControlMinder Rapid Implementation Guide – Shared Account Management

Click the **Edit** button
(right facing triangle)
under Member Policies
(next to (all))



Click the **Edit** button next
to Users under Member
Rule



CA ControlMinder Enterprise Management

Logged in as: [cmmadmin](#) to [localhost\(DMS @ localhost\)](#) (Logout)

Home World View Policy Management Privileged Accounts Reports Users and Groups System

Users Groups Roles Tasks Delegation

Modify Role: *Break Glass*

Profile Tasks **Members** Administrators Owners

Member Policy

Member Rule

Which users are members of this role?

Users

(all)
where <user-filter>
in <org-rule>
where <user-filter> and who are in <org-rule>
who are members of <group-member-rule>
who are members of <role-rules>
who are administrators of <role-rule>
who are owners of <role-rule>

Scope

Definition

Privilege

returned by the query <LDAP-query>

Account Name =

Add new scoping rule

OK Cancel

CA ControlMinder Enterprise Management

Logged in as: [cmadmin](#) to [localhost\(DMS @ localhost\)](#) (Logout)

Home | World View | Policy Management | Privileged Accounts | Reports | Users and Groups | System

Users > Groups > Roles > Tasks > Delegation

Modify Role: Break Glass

Profile | Tasks | **Members** | Administrators | Owners

Member Policy

Member Rule

Which users are members of this role?

Users who are members of

group

Scope Rules

Define any scope rules that apply to this role:

Which Privileged Account objects does this role manage?

Privileged Account where

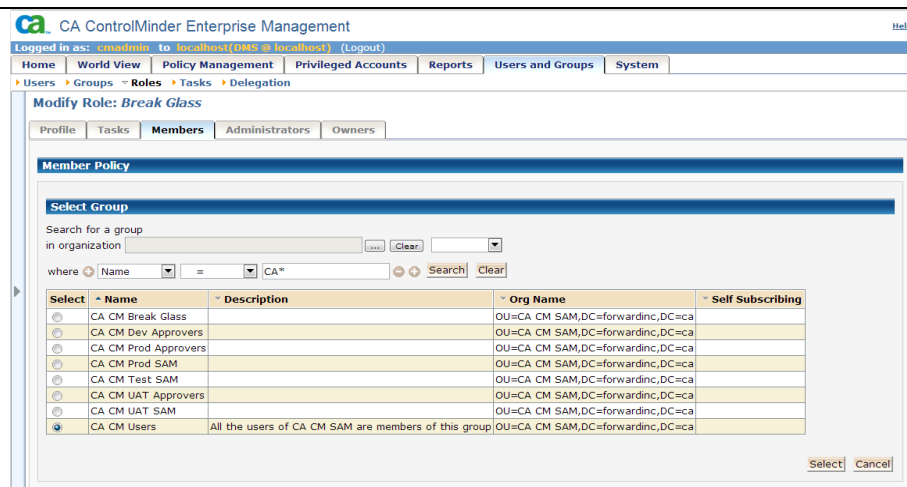
Account Name =

Add new scoping rule

OK Cancel

CA ControlMinder Rapid Implementation Guide – Shared Account Management

Choose the group and click **Select**.



CA ControlMinder Enterprise Management

Logged in as: cmanadmin to localhost(DMS @ localhost) (Logout)

Home | World View | Policy Management | Privileged Accounts | Reports | Users and Groups | System

Users > Groups > Roles > Tasks > Delegation

Modify Role: Break Glass

Profile | Tasks | **Members** | Administrators | Owners

Member Policy

Select Group

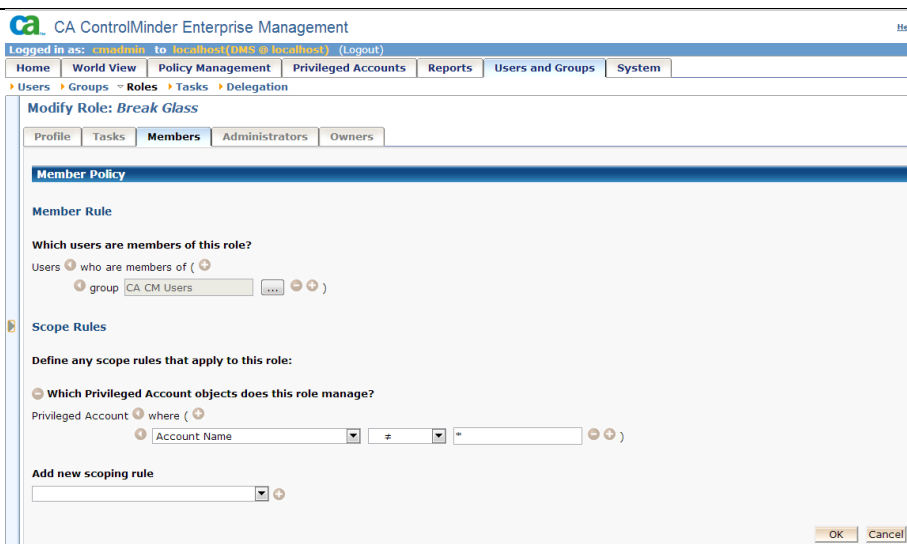
Search for a group in organization

where Name = CA* Search Clear

Select	Name	Description	Org Name	Self Subscribing
<input type="radio"/>	CA CM Break Glass		OU=CA CM SAM,DC=forwardinc,DC=ca	
<input type="radio"/>	CA CM Dev Approvers		OU=CA CM SAM,DC=forwardinc,DC=ca	
<input type="radio"/>	CA CM Prod Approvers		OU=CA CM SAM,DC=forwardinc,DC=ca	
<input type="radio"/>	CA CM Prod SAM		OU=CA CM SAM,DC=forwardinc,DC=ca	
<input type="radio"/>	CA CM Test SAM		OU=CA CM SAM,DC=forwardinc,DC=ca	
<input type="radio"/>	CA CM UAT Approvers		OU=CA CM SAM,DC=forwardinc,DC=ca	
<input type="radio"/>	CA CM UAT SAM		OU=CA CM SAM,DC=forwardinc,DC=ca	
<input checked="" type="radio"/>	CA CM Users	All the users of CA CM SAM are members of this group	OU=CA CM SAM,DC=forwardinc,DC=ca	

Select Cancel

Click **OK**



CA ControlMinder Enterprise Management

Logged in as: cmanadmin to localhost(DMS @ localhost) (Logout)

Home | World View | Policy Management | Privileged Accounts | Reports | Users and Groups | System

Users > Groups > Roles > Tasks > Delegation

Modify Role: Break Glass

Profile | Tasks | **Members** | Administrators | Owners

Member Policy

Member Rule

Which users are members of this role?

Users who are members of (group "CA CM Users")

Scope Rules

Define any scope rules that apply to this role:

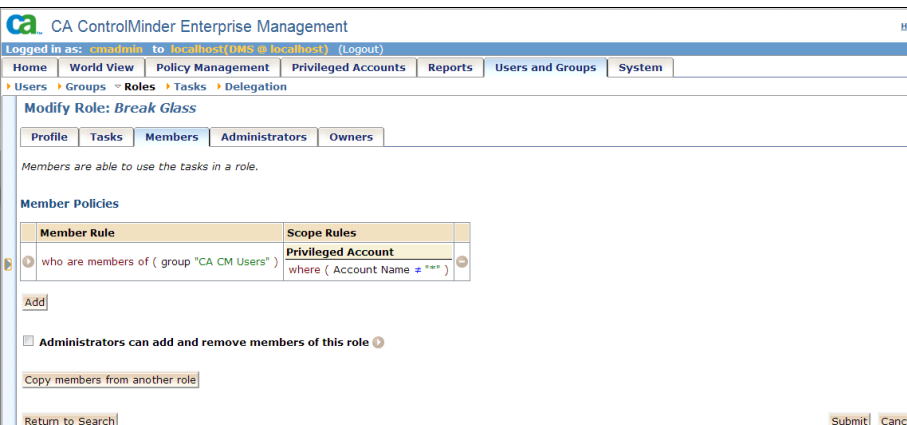
Which Privileged Account objects does this role manage?

Privileged Account where (Account Name = *)

Add new scoping rule

OK Cancel

Click **Submit** to submit the modify role task to the ENTM workflow processor



CA ControlMinder Enterprise Management

Logged in as: cmanadmin to localhost(DMS @ localhost) (Logout)

Home | World View | Policy Management | Privileged Accounts | Reports | Users and Groups | System

Users > Groups > Roles > Tasks > Delegation

Modify Role: Break Glass

Profile | Tasks | **Members** | Administrators | Owners

Members are able to use the tasks in a role.

Member Policies

Member Rule	Scope Rules
who are members of (group "CA CM Users")	Privileged Account where (Account Name = *)

Add

☐ Administrators can add and remove members of this role

Copy members from another role

Return to Search

Submit Cancel

If desired you may repeat the steps shown above for the Break Glass role modification to modify the role membership of the SAM default role definitions – Privileged Account Request, SAM Approver, SAM User and Self-Manager.

Note: Because of a current limitation in the product all the users that need access to accounts through “My Privileged Accounts” must be members of “Break Glass Role”. They will not be able to see the privileged account they are allowed to use otherwise.

You can specify which accounts would be available for break glass by changing the scoping rules of this role.

Please note that no accounts are available for break glass by default.

Setting Up Endpoint Tagging and Approvers

Endpoint tagging provides a method to assign meaningful attributes to endpoints that may be used to group those endpoints into like collectives. For example, in a typical enterprise environment servers exist in various environments such as test, user acceptance / quality assurance and production. Using tagging it is possible to set servers into a test group, user acceptance test (UAT) group and production group.

Once a server set is tagged it is possible to assign a set of approvers to be associated with each group. Using the designations from above one may set up approvers for test servers, UAT servers and production servers.

In the methodology shown in this section, the tags Test, UAT and Prod will be used to associate servers into those groups.

For the actual set up, the Custom 1 field will be used to hold the tag.

AD groups will be used to hold the list of approvers. These will be CA CM Test Approvers, CA CM UAT Approvers and CA CM Prod Approvers. The group names will be specified in the Owner field.

These are representations used for discussion and may be changed in an actual rapid implementation to more closely match the model of the enterprise.

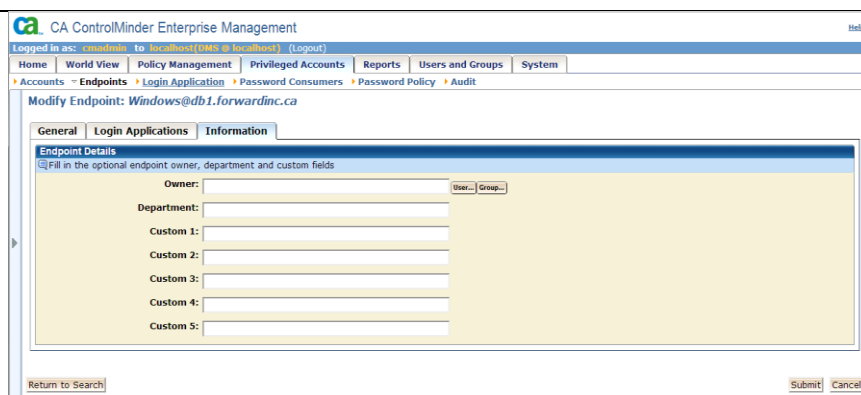
Tagging Setup

Set custom attributes and owners by navigating to:

Privileged Accounts ->
Endpoints ->
Modify Endpoint

Search for the endpoint you want to modify.

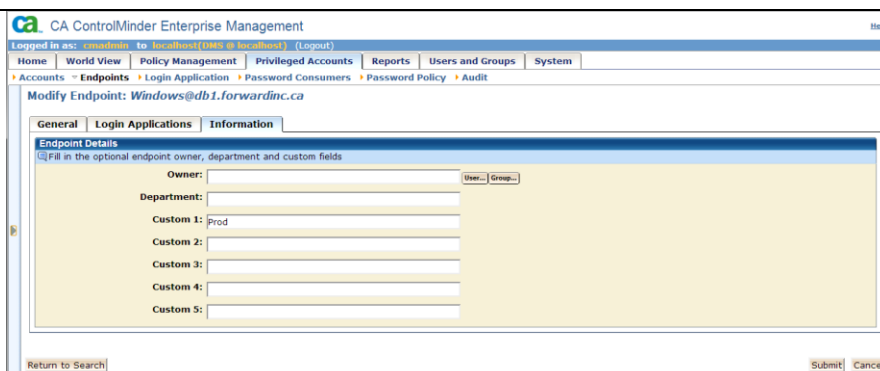
Select the endpoint and click on the **Information** tab.



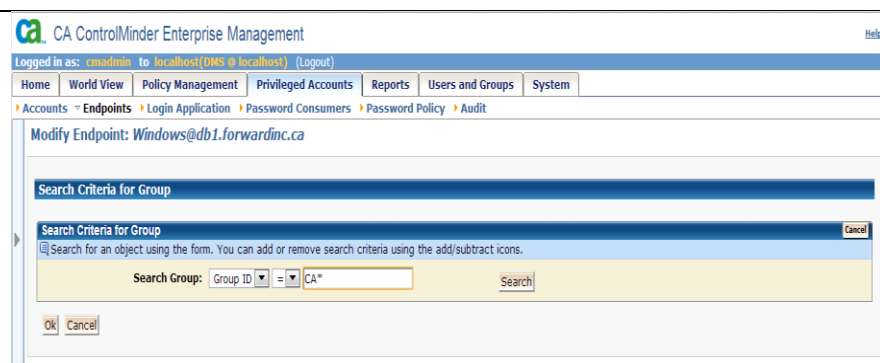
CA ControlMinder Rapid Implementation Guide – Shared Account Management

Update the custom attributes with tagging information as shown. In this case we set the entry of the Custom 1 field to “Prod” (to indicate production).

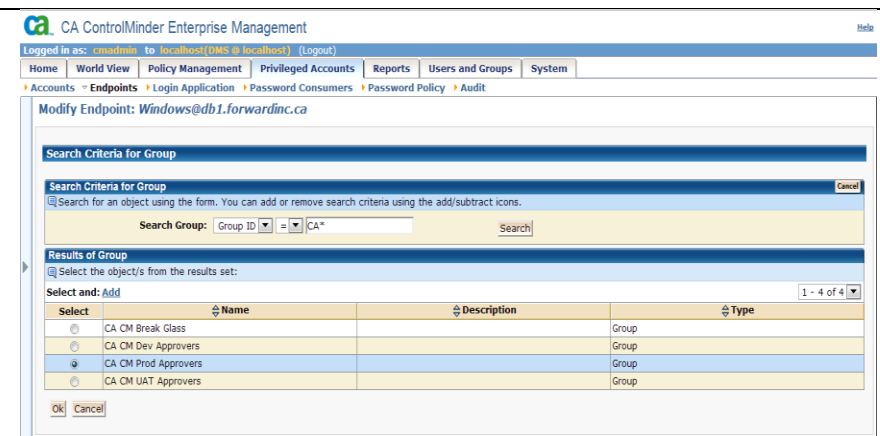
Click the **Group** button next to the **Owner** field. This allows the setting of the search criteria as shown.



After entering the desired search group, click the **Search** button to perform the group search.



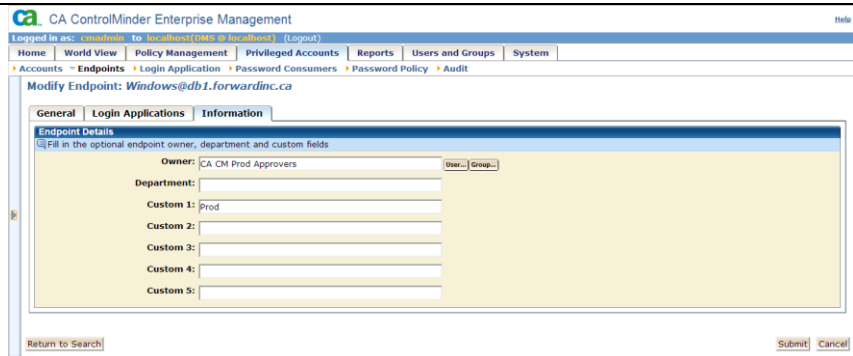
When the list of groups is returned, select the desired group and click **OK** to use the selected group.



Select	Name	Description	Type
<input type="radio"/>	CA CM Break Glass		Group
<input type="radio"/>	CA CM Dev Approvers		Group
<input checked="" type="radio"/>	CA CM Prod Approvers		Group
<input type="radio"/>	CA CM UAT Approvers		Group

CA ControlMinder Rapid Implementation Guide – Shared Account Management

Click **Submit** to enter the changes.



The screenshot displays the CA ControlMinder Enterprise Management web application. The user is logged in as 'casadmin' to 'localhost(OMS to localhost)' and is viewing the 'Modify Endpoint' page for 'Windows@db1.forwardinc.ca'. The interface includes a navigation menu with options like Home, World View, Policy Management, Privileged Accounts, Reports, Users and Groups, and System. The main content area shows the 'Endpoint Details' form with fields for Owner (CA CM Prod Approvers), Department, Custom 1 (Prod), Custom 2, Custom 3, Custom 4, and Custom 5. There are 'Return to Search', 'Submit', and 'Cancel' buttons at the bottom.

Repeat the preceding steps for all of the tags that you want to define in your environment.

CA ControlMinder Rapid Implementation Guide – Shared Account Management

Approver Setup

This section is informational only. You do not need to go through the steps unless you want to modify the default workflow process.

The task that is used to request and approve privileged accounts is the **Privileged Account Request** task.

Navigate to:

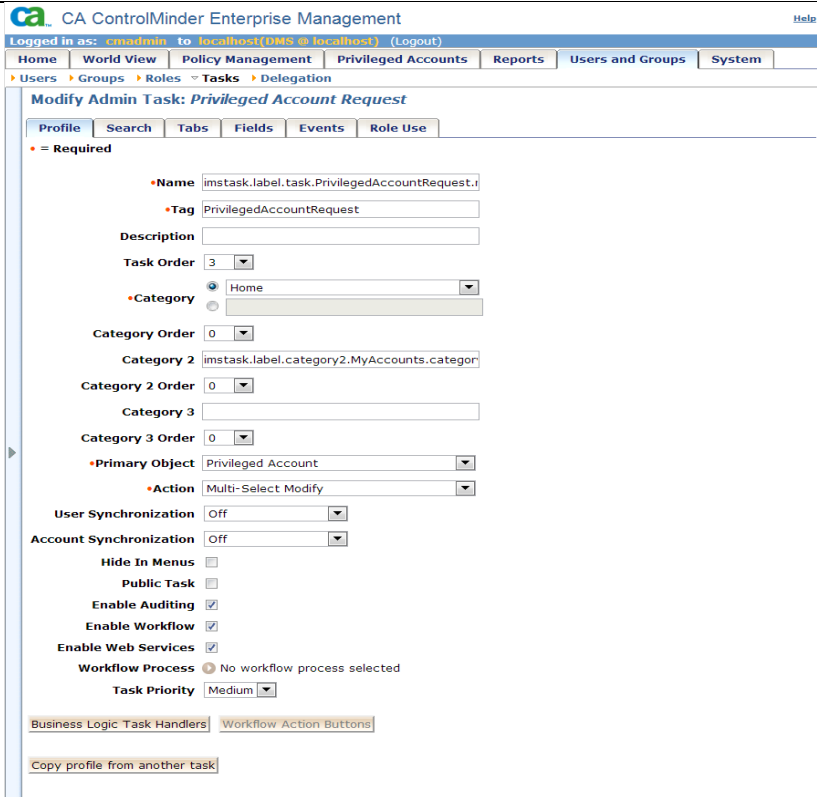
User and Groups ->

Tasks ->

Modify Task

Search for

PrivilegedAccountRequest



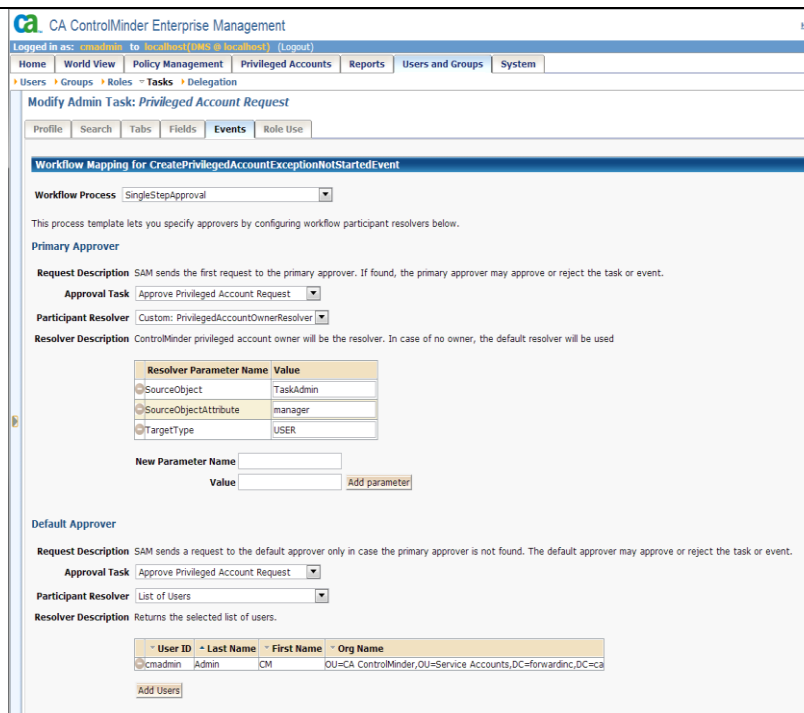
CA ControlMinder Rapid Implementation Guide – Shared Account Management

Click on the **Events** panel.

You can see that workflow process is set to **SingleStepApproval** and the participant resolver is set to **PrivilegedAccountOwnerResolver**

This means that the list of approvers will be retrieved based on the data in the **Owner** attribute of the Privileged Account or Endpoint.

We specified an AD group as an owner in our case. The list of owners will serve as list of approvers.



CA ControlMinder Enterprise Management

Logged in as: cmadmin to localhost (MS 8 localhost) (Logout)

Home | World View | Policy Management | Privileged Accounts | Reports | Users and Groups | System

Users | Groups | Roles | Tasks | Delegation

Modify Admin Task: Privileged Account Request

Profile | Search | Tabs | Fields | **Events** | Role Use

Workflow Mapping for CreatePrivilegedAccountExceptionNotStartedEvent

Workflow Process: SingleStepApproval

This process template lets you specify approvers by configuring workflow participant resolvers below.

Primary Approver

Request Description SAM sends the first request to the primary approver. If found, the primary approver may approve or reject the task or event.

Approval Task Approve Privileged Account Request

Participant Resolver Custom: PrivilegedAccountOwnerResolver

Resolver Description ControlMinder privileged account owner will be the resolver. In case of no owner, the default resolver will be used

Resolver Parameter Name	Value
SourceObject	TaskAdmin
SourceObjectAttribute	manager
TargetType	USER

New Parameter Name: Value: Add parameter

Default Approver

Request Description SAM sends a request to the default approver only in case the primary approver is not found. The default approver may approve or reject the task or event.

Approval Task Approve Privileged Account Request

Participant Resolver List of Users

Resolver Description Returns the selected list of users.

User ID	Last Name	First Name	Org Name
cmadmin	Admin	CM	OU=CA ControlMinder, OU=Service Accounts, DC=forwardinc, DC=ca

Add Users

If the owner field is blank or no approver is specified then the “default” approver will be used. The default approver is the super admin user that was specified during the SAM installation.

If desired, you may modify the default approver to add multiple users to the default approver list.

Privilege Access Role Definition

In ENTM, you assign privileges to users and administrators by assigning admin and privileged access roles. A role contains tasks that correspond to application functions in CA ControlMinder Enterprise Management.

Roles simplify privilege management. Instead of associating a user with each task that they perform, you can assign a role to the user. The user can perform all the tasks in their assigned role. You can then edit the role by adding tasks. Every user who has the role can now perform the new task. If you remove a task from a role, the user can no longer perform that task.

When a user logs in to ENTM, they see tabs based on their role(s). The user can see only the tabs and tasks that are assigned to their role(s).

You can assign separate roles to different users to prevent one user being able to complete every task. This may help your organization comply with separation of duties requirements. However, you can assign more than one role to a user.

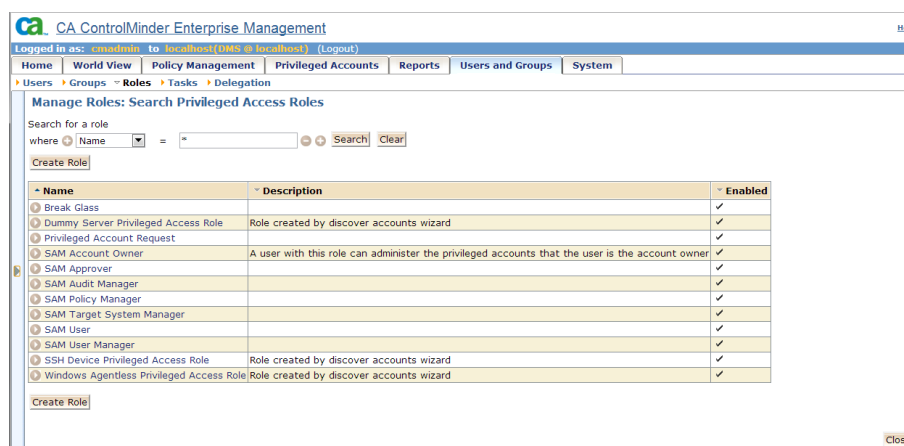
It is suggested to use the properties of the endpoints and accounts for tagging as described previously. In this case every endpoint will have the application and environment assigned listed in one of the custom fields. This will allow the rule sets to be simplified. When a new endpoint is acquired and tagged it will automatically be available to a user defined with the associated role.

The first time that you discover privileged accounts on an endpoint type, CA ControlMinder Enterprise Management automatically creates an endpoint privileged access role for using privileged accounts on that endpoint type. For example, the first time you discover privileged accounts on a Windows Agentless endpoint, CA ControlMinder Enterprise Management automatically creates the Windows Agentless Privileged Access Role.

You can see the created role if you go to Users and Groups/Roles/Privileged Access Roles/Manage Roles.

The SSH Device Privileged Access Role and Windows Agentless Privileged Access Role in the screenshot below were created by the discovery process.

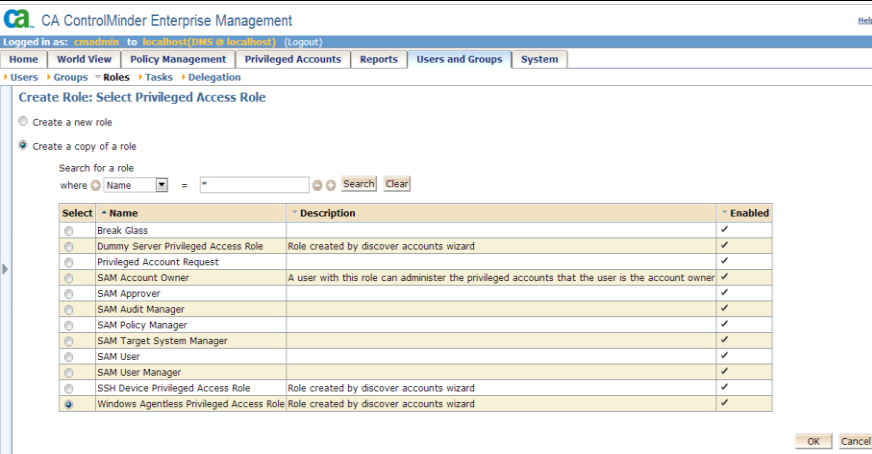
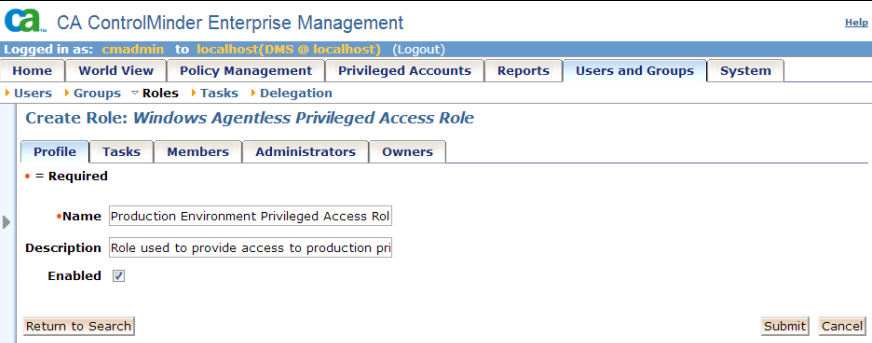
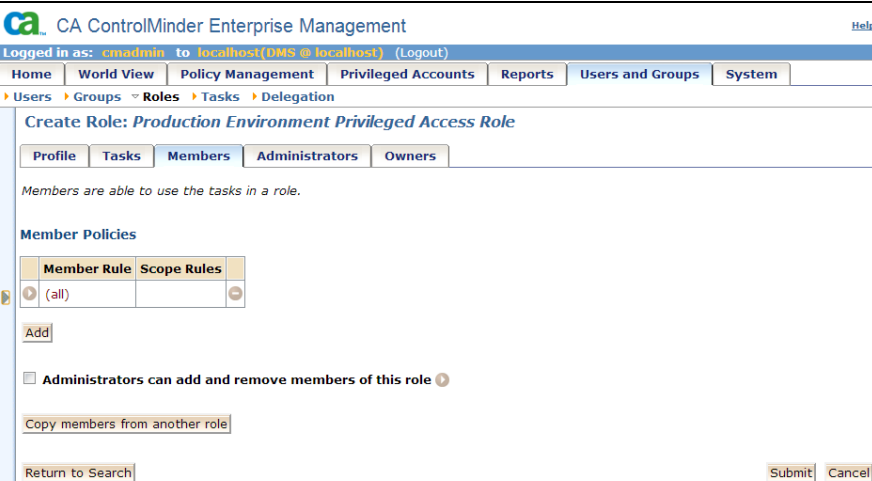
This role can be used to give access to all the accounts of a given type. It can also be used as a template when you create new roles.



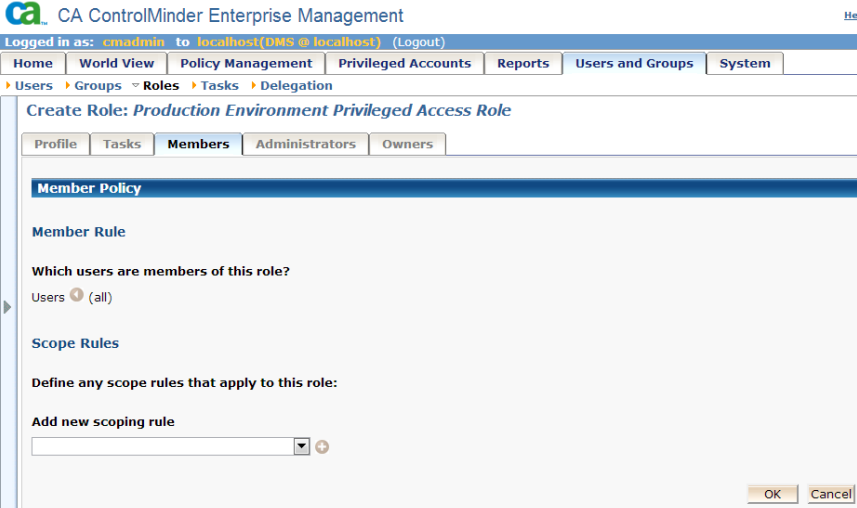
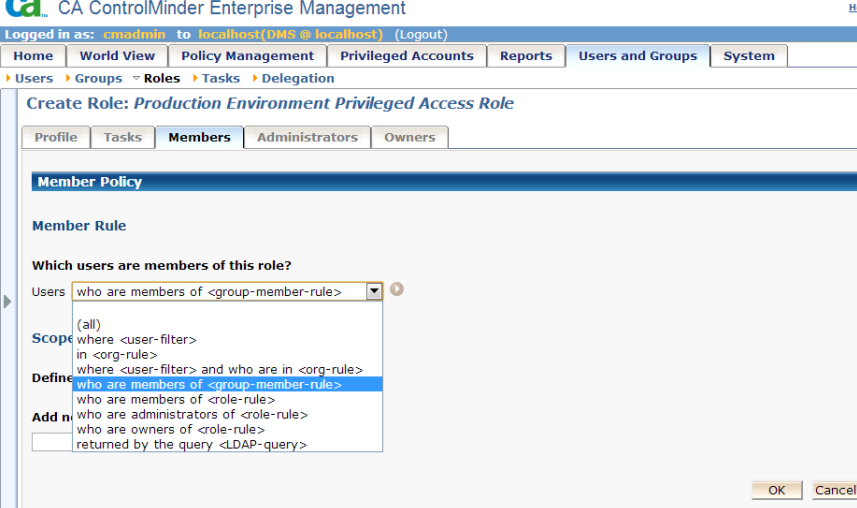
CA ControlMinder Rapid Implementation Guide – Shared Account Management

You can use the automatically created roles as a starting point when creating new roles.

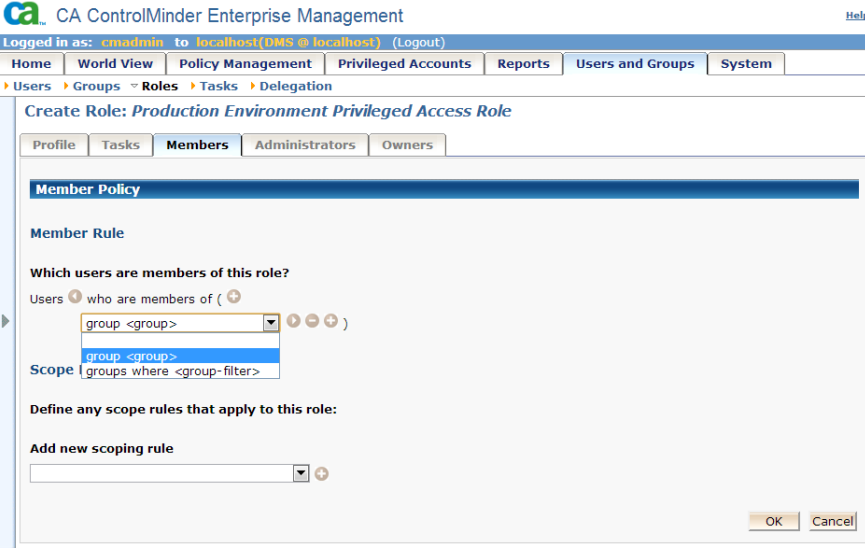

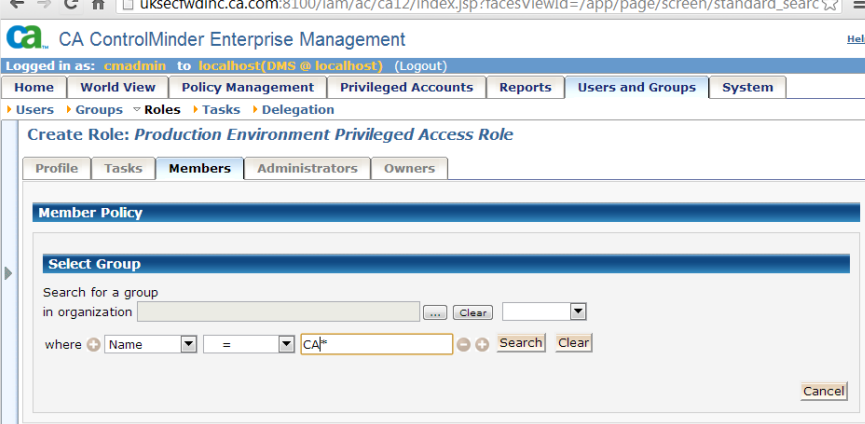
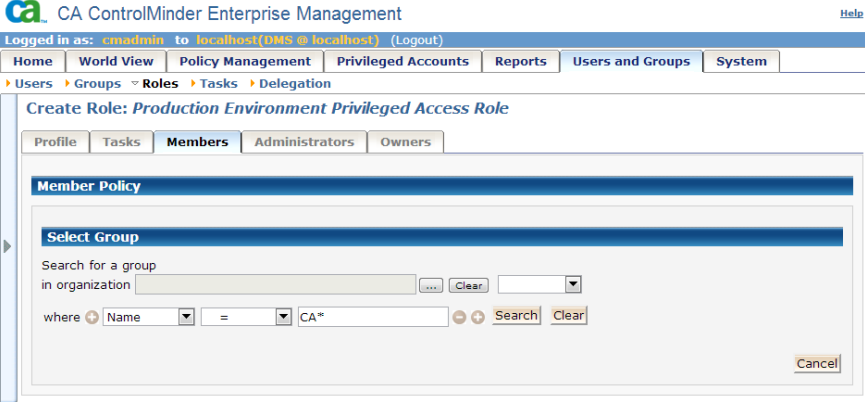
Role Creation

<p>Navigate to:</p> <p>User and Groups -> Roles -> Privileged Access Roles/Create Role</p> <p>Select Create a copy of a role and click Search.</p> <p>Select one of the roles that were created by the discover accounts wizard.</p>	 <p>CA ControlMinder Enterprise Management</p> <p>Logged in as: cmadmin to localhost(DMS @ localhost) (Logout)</p> <p>Home World View Policy Management Privileged Accounts Reports Users and Groups System</p> <p>Users > Groups > Roles > Tasks > Delegation</p> <p>Create Role: Select Privileged Access Role</p> <p><input type="radio"/> Create a new role</p> <p><input checked="" type="radio"/> Create a copy of a role</p> <p>Search for a role where Name = [] Search Clear</p> <table border="1"> <thead> <tr> <th>Select</th> <th>Name</th> <th>Description</th> <th>Enabled</th> </tr> </thead> <tbody> <tr> <td><input type="radio"/></td> <td>Break Glass</td> <td></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td><input type="radio"/></td> <td>Dummy Server Privileged Access Role</td> <td>Role created by discover accounts wizard</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td><input type="radio"/></td> <td>Privileged Account Request</td> <td></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td><input type="radio"/></td> <td>SAM Account Owner</td> <td>A user with this role can administer the privileged accounts that the user is the account owner</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td><input type="radio"/></td> <td>SAM Approver</td> <td></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td><input type="radio"/></td> <td>SAM Audit Manager</td> <td></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td><input type="radio"/></td> <td>SAM Policy Manager</td> <td></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td><input type="radio"/></td> <td>SAM Target System Manager</td> <td></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td><input type="radio"/></td> <td>SAM User</td> <td></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td><input type="radio"/></td> <td>SAM User Manager</td> <td></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td><input type="radio"/></td> <td>SSH Device Privileged Access Role</td> <td>Role created by discover accounts wizard</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td><input checked="" type="radio"/></td> <td>Windows Agentless Privileged Access Role</td> <td>Role created by discover accounts wizard</td> <td><input checked="" type="checkbox"/></td> </tr> </tbody> </table> <p>OK Cancel</p>	Select	Name	Description	Enabled	<input type="radio"/>	Break Glass		<input checked="" type="checkbox"/>	<input type="radio"/>	Dummy Server Privileged Access Role	Role created by discover accounts wizard	<input checked="" type="checkbox"/>	<input type="radio"/>	Privileged Account Request		<input checked="" type="checkbox"/>	<input type="radio"/>	SAM Account Owner	A user with this role can administer the privileged accounts that the user is the account owner	<input checked="" type="checkbox"/>	<input type="radio"/>	SAM Approver		<input checked="" type="checkbox"/>	<input type="radio"/>	SAM Audit Manager		<input checked="" type="checkbox"/>	<input type="radio"/>	SAM Policy Manager		<input checked="" type="checkbox"/>	<input type="radio"/>	SAM Target System Manager		<input checked="" type="checkbox"/>	<input type="radio"/>	SAM User		<input checked="" type="checkbox"/>	<input type="radio"/>	SAM User Manager		<input checked="" type="checkbox"/>	<input type="radio"/>	SSH Device Privileged Access Role	Role created by discover accounts wizard	<input checked="" type="checkbox"/>	<input checked="" type="radio"/>	Windows Agentless Privileged Access Role	Role created by discover accounts wizard	<input checked="" type="checkbox"/>
Select	Name	Description	Enabled																																																		
<input type="radio"/>	Break Glass		<input checked="" type="checkbox"/>																																																		
<input type="radio"/>	Dummy Server Privileged Access Role	Role created by discover accounts wizard	<input checked="" type="checkbox"/>																																																		
<input type="radio"/>	Privileged Account Request		<input checked="" type="checkbox"/>																																																		
<input type="radio"/>	SAM Account Owner	A user with this role can administer the privileged accounts that the user is the account owner	<input checked="" type="checkbox"/>																																																		
<input type="radio"/>	SAM Approver		<input checked="" type="checkbox"/>																																																		
<input type="radio"/>	SAM Audit Manager		<input checked="" type="checkbox"/>																																																		
<input type="radio"/>	SAM Policy Manager		<input checked="" type="checkbox"/>																																																		
<input type="radio"/>	SAM Target System Manager		<input checked="" type="checkbox"/>																																																		
<input type="radio"/>	SAM User		<input checked="" type="checkbox"/>																																																		
<input type="radio"/>	SAM User Manager		<input checked="" type="checkbox"/>																																																		
<input type="radio"/>	SSH Device Privileged Access Role	Role created by discover accounts wizard	<input checked="" type="checkbox"/>																																																		
<input checked="" type="radio"/>	Windows Agentless Privileged Access Role	Role created by discover accounts wizard	<input checked="" type="checkbox"/>																																																		
<p>Provide a unique name for the role and a description.</p>	 <p>CA ControlMinder Enterprise Management</p> <p>Logged in as: cmadmin to localhost(DMS @ localhost) (Logout)</p> <p>Home World View Policy Management Privileged Accounts Reports Users and Groups System</p> <p>Users > Groups > Roles > Tasks > Delegation</p> <p>Create Role: Windows Agentless Privileged Access Role</p> <p>Profile Tasks Members Administrators Owners</p> <p><input checked="" type="radio"/> Required</p> <p>Name: Production Environment Privileged Access Rol</p> <p>Description: Role used to provide access to production pri</p> <p>Enabled: <input checked="" type="checkbox"/></p> <p>Return to Search Submit Cancel</p>																																																				
<p>To select members, Click on the Members tab.</p>	 <p>CA ControlMinder Enterprise Management</p> <p>Logged in as: cmadmin to localhost(DMS @ localhost) (Logout)</p> <p>Home World View Policy Management Privileged Accounts Reports Users and Groups System</p> <p>Users > Groups > Roles > Tasks > Delegation</p> <p>Create Role: Production Environment Privileged Access Role</p> <p>Profile Tasks Members Administrators Owners</p> <p>Members are able to use the tasks in a role.</p> <p>Member Policies</p> <table border="1"> <thead> <tr> <th>Member Rule</th> <th>Scope Rules</th> </tr> </thead> <tbody> <tr> <td>(all)</td> <td></td> </tr> </tbody> </table> <p>Add</p> <p><input type="checkbox"/> Administrators can add and remove members of this role</p> <p>Copy members from another role</p> <p>Return to Search Submit Cancel</p>	Member Rule	Scope Rules	(all)																																																	
Member Rule	Scope Rules																																																				
(all)																																																					

CA ControlMinder Rapid Implementation Guide – Shared Account Management

<p>Modify the member rule that only members of a specified MS Active Directory group will belong to this role.</p> <p>Click the triangle sign next to (all).</p>	
<p>Click the triangle sign next to Users.</p> <p>Select who are members of <group-member-rule> from the drop down list.</p>	

CA ControlMinder Rapid Implementation Guide – Shared Account Management

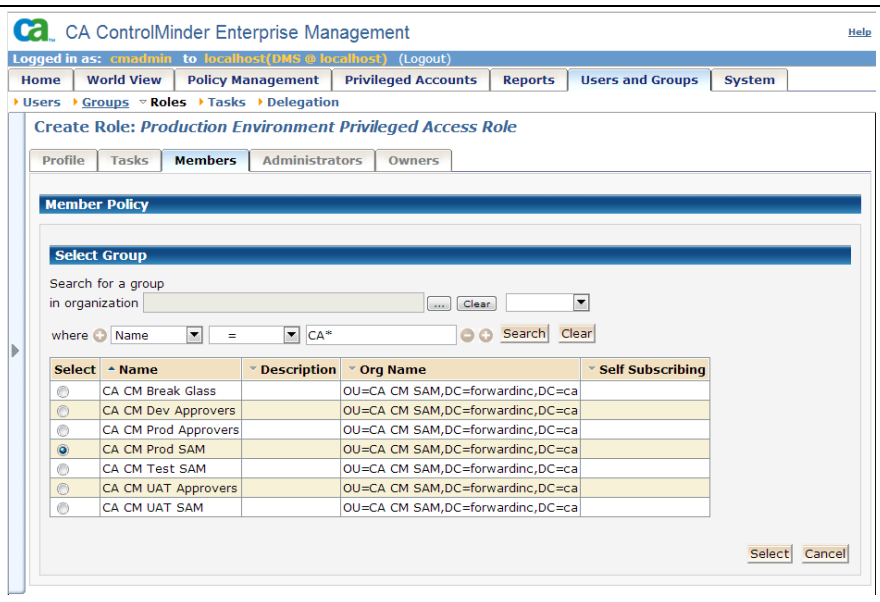
<p>Select group <group> from the drop down list.</p>	
<p>Click  to search for a group.</p>	
<p>Specify search criteria and click Search.</p>	

CA ControlMinder Rapid Implementation Guide – Shared Account Management

You will be provided with a list of MS Active Directory groups.

Select a group whose members will have access to privileged accounts that you will define in the scope.

Click **Select**.



CA ControlMinder Enterprise Management

Logged in as: cadmin to localhost(DMS @ localhost) (Logout)

Home World View Policy Management Privileged Accounts Reports Users and Groups System

Users Groups Roles Tasks Delegation

Create Role: Production Environment Privileged Access Role

Profile Tasks **Members** Administrators Owners

Member Policy

Select Group

Search for a group in organization

where Name = CA*

Select	Name	Description	Org Name	Self Subscribing
<input type="radio"/>	CA CM Break Glass		OU=CA CM SAM,DC=forwardinc,DC=ca	
<input type="radio"/>	CA CM Dev Approvers		OU=CA CM SAM,DC=forwardinc,DC=ca	
<input type="radio"/>	CA CM Prod Approvers		OU=CA CM SAM,DC=forwardinc,DC=ca	
<input checked="" type="radio"/>	CA CM Prod SAM		OU=CA CM SAM,DC=forwardinc,DC=ca	
<input type="radio"/>	CA CM Test SAM		OU=CA CM SAM,DC=forwardinc,DC=ca	
<input type="radio"/>	CA CM UAT Approvers		OU=CA CM SAM,DC=forwardinc,DC=ca	
<input type="radio"/>	CA CM UAT SAM		OU=CA CM SAM,DC=forwardinc,DC=ca	

Role Scoping

You use privileged access roles to specify the SAM tasks that each user can perform in ENTM and the privileged accounts that each user can check in and check out. ENTM comes with predefined privileged access roles. You can modify the predefined roles to suit your enterprise, or create new roles entirely.

When a user logs in to ENTM, they see only the tasks and privileged accounts that correspond to their role. Out-of-the-box, ENTM assigns the Break Glass, SAM Approver, Privileged Account Request, and SAM User roles to all users. You can modify this by defining the specific endpoints and privileged accounts that the role can access. Scope rules let you implement fine-grained access to privileged accounts across the enterprise and are defined by the member policy of a role.

In our example we have three groups for SAM users:

- CA CM Prod SAM
- CA CM UAT SAM
- CA CM Test SAM

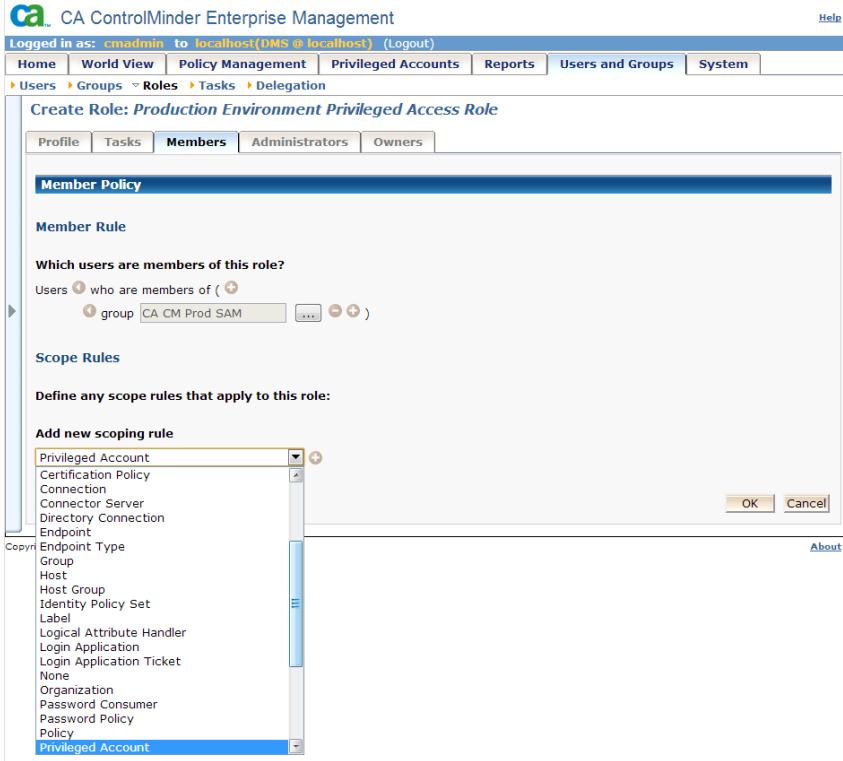
These groups were created to be able to give access to three sample environments:

- Production
- User Acceptance Testing
- Test

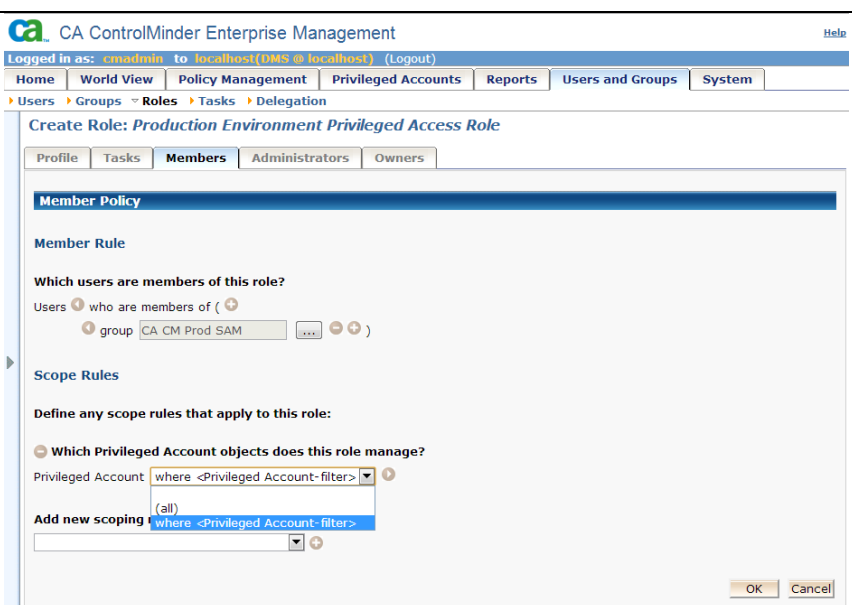
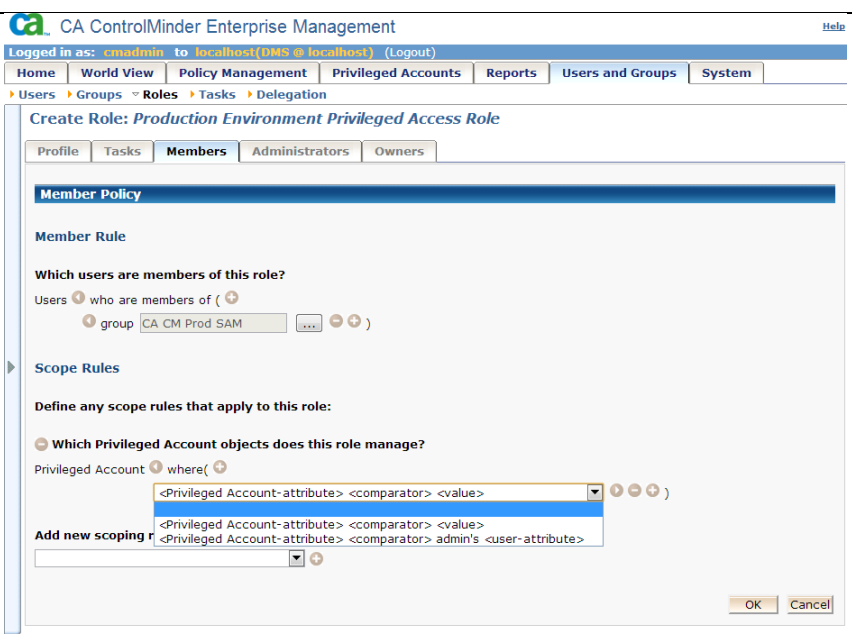
Navigate to:

Create Role -> Members

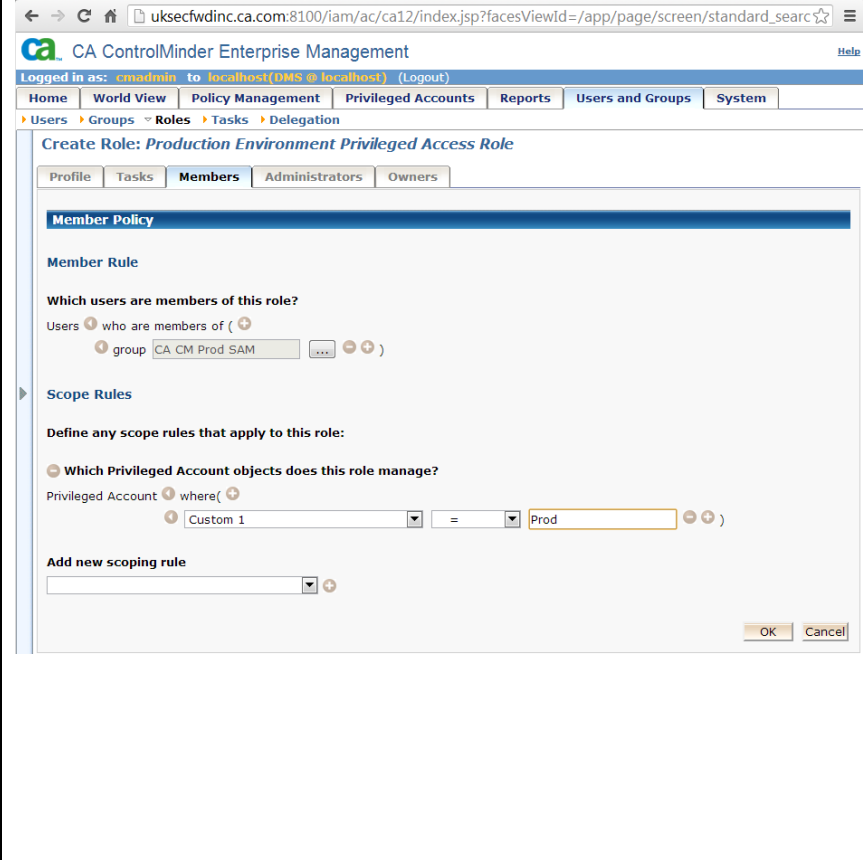

Select **Privileged Account** from the drop down list



CA ControlMinder Rapid Implementation Guide – Shared Account Management

<p>Select <Privileged Account-filter> as the filter scoping rule</p>	
<p>Select <Privileged Account – attribute> <comparator> <value></p>	

CA ControlMinder Rapid Implementation Guide – Shared Account Management

<p>Select Custom 1 from the list of available attributes and specify a tag name you used previously for the environment you are creating a role for.</p> <p>In our document we use the following tags:</p> <p>Prod</p> <p>UAT</p> <p>Test</p> <p>The custom attribute values are inherited from an endpoint to its accounts.</p> <p>This value can be overwritten on the account level if required.</p> <p>Click OK to confirm.</p>	
<p>Verify the member rule and scoping rules on the next screen and click Submit</p>	

The members of this rule will be able to access the privileged accounts that have “Prod” tag set on the endpoint or account levels.

Repeat the above steps for each environment (group of servers).

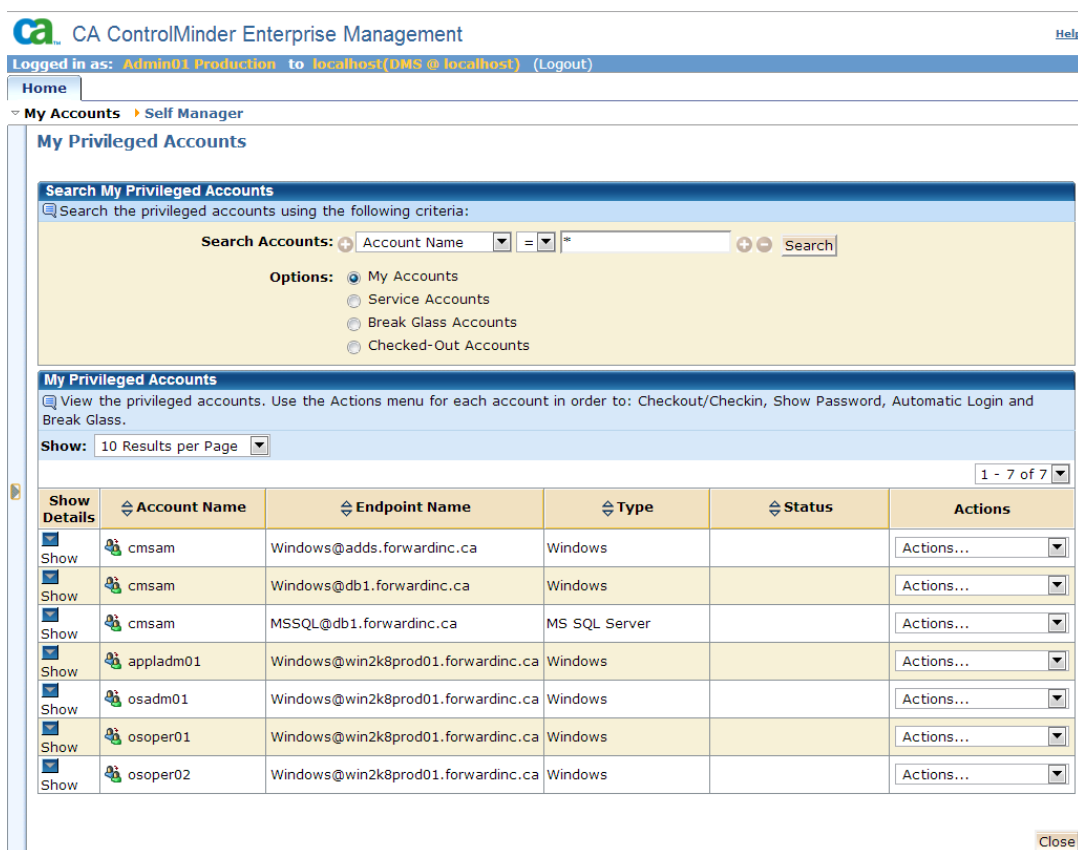
CA ControlMinder Rapid Implementation Guide – Shared Account Management

Role Verification

Login to ENTM as a user that is member of a MS Active Directory group defined on the member rules of the defined roles.

In the example below the user was a member of “CM Prod SAM” group that is member of “Production Environment Privileged Access Role”. This roles gives access to all the accounts that are tagged as production - have “Prod” in their “Custom 1” field.

Navigate to Home -> My Privileged Accounts



CA ControlMinder Enterprise Management

Logged in as: Admin01 Production to localhost(DMS @ localhost) (Logout)

Home

My Accounts Self Manager

My Privileged Accounts

Search My Privileged Accounts

Search the privileged accounts using the following criteria:

Search Accounts: Account Name = *

Options:

- ☒ My Accounts
- ☐ Service Accounts
- ☐ Break Glass Accounts
- ☐ Checked-Out Accounts

My Privileged Accounts

View the privileged accounts. Use the Actions menu for each account in order to: Checkout/Checkin, Show Password, Automatic Login and Break Glass.

Show: 10 Results per Page

1 - 7 of 7

Show Details	Account Name	Endpoint Name	Type	Status	Actions
Show	cmsam	Windows@adds.forwardinc.ca	Windows		Actions...
Show	cmsam	Windows@db1.forwardinc.ca	Windows		Actions...
Show	cmsam	MSSQL@db1.forwardinc.ca	MS SQL Server		Actions...
Show	appladm01	Windows@win2k8prod01.forwardinc.ca	Windows		Actions...
Show	osadm01	Windows@win2k8prod01.forwardinc.ca	Windows		Actions...
Show	osoper01	Windows@win2k8prod01.forwardinc.ca	Windows		Actions...
Show	osoper02	Windows@win2k8prod01.forwardinc.ca	Windows		Actions...

Close

You can see the list of accounts this user is allowed to “Check Out” without a need for an approval.

Navigate to Home -> Privileged Account Request and click Search.

CA ControlMinder Rapid Implementation Guide – Shared Account Management

CA ControlMinder Enterprise Management [Help](#)

Logged in as: Admin01 Production to localhost(DMS @ localhost) (Logout)

[Home](#)

My Accounts ▸ Self Manager

Privileged Account Request: Select Privileged Account

Search for objects of type Privileged Account

where Endpoint Type = * [Search](#) [Clear](#)

Select	Endpoint Type	Endpoint Name	Container	Account Name	Disconnected System	Is Endpoint Administrator	Checked Out By Users	Last Failed Connection Date
<input type="checkbox"/>	SSH Device	Linux@acrh55_x64_01.forwardinc.ca	SSH Accounts	appladm01				
<input type="checkbox"/>	SSH Device	Linux@acrh55_x64_01.forwardinc.ca	SSH Accounts	appladm02				
<input type="checkbox"/>	SSH Device	Linux@acrh55_x64_01.forwardinc.ca	SSH Accounts	cmsam	✓	✓		
<input type="checkbox"/>	SSH Device	Linux@acrh55_x64_01.forwardinc.ca	SSH Accounts	osadm01				
<input type="checkbox"/>	SSH Device	Linux@acrh55_x64_01.forwardinc.ca	SSH Accounts	root	✓	✓		

[Select](#) [Cancel](#)

You can see all the other account listed. These are the accounts that the user is able to request and if approved then “Check Out” the password.

The default behavior of CA ControlMinder SAM is that all accounts are available for request by any SAM user. Of course, there is no need to request a privileged account that is always available to a user for check-out.

Advanced Topics

SAM Endpoint and Account Management Using the Feeder

In addition to the manual creation of endpoints and accounts using the ENTM WebUI, SAM provides a method to automatically create and update endpoints and associated accounts using technology known as a “feeder”.

The SAM feeder lets you import many SAM endpoints and shared accounts into CA ControlMinder Enterprise Management in a single step. You can also use the SAM feeder to create, modify, or delete SAM endpoints and privileged accounts.

While interviewing your application owners and system administrators to identify privileged accounts, you can add the endpoints and privileged accounts of interest to a feeder file. The feeder file is a simple CSV file. Copy your feeder files to a folder that is periodically polled by the feeder process of CA SAM. This enables an automated and unattended process. The feeder output can be monitored for conflict/errors.

The SAM feeder process

You, or an automated process, create and save one or more CSV files in the polling folder.

Each line in the CSV file represents a task to create or modify a SAM endpoint or privileged account.

You need to create separate CSV files for endpoints and for privileged accounts.

When the polling task starts, the SAM feeder uploads the CSV files in the polling folder to CA ControlMinder Enterprise Management. You can configure the polling task to run at a specified time, or you can start the polling task manually.

CA ControlMinder Enterprise Management renames the CSV file `original_timestamp.csv`, and moves the file to the processed files folder.

Note: `original` is the name of the original CSV file, and `timestamp` is a timestamp that indicates when the file was processed. For example, if you name the original CSV file `endpoints.csv`, CA ControlMinder Enterprise Management names the file in the processed file folder `endpoints_091209130256.csv`.

CA ControlMinder Enterprise Management processes each line in the CSV file in turn. For each line in the CSV file, the following happens:

As CA ControlMinder Enterprise Management successfully processes a line from the CSV file:

- The action is committed, for example, an endpoint is created.
- An audit event is written noting the action taken.

If CA ControlMinder Enterprise Management fails to process a line from the CSV file:

- The line from the CSV file is copied to a CSV file in the error files folder.
- A column named `FAILURE_REASON` is added to the CSV file in the error files folder.

- The reason why the task failed is added to the FAILURE_REASON column for the affected line.
- An audit event is written noting the failure.

The CSV file in the error files folder provides an easy way for you to review failures. The name of this file is also original_timestamp.csv.

Note: The CSV file in the processed files folder lists all processed lines, but it does not note success or failure.

Import Endpoints using the SAM feeder

Each row or line in the endpoint CSV file, after the header row or line, represents a task to create, modify, or delete an endpoint in CA ControlMinder Enterprise Management.

Create a CSV file and give it an appropriate name.

There are sample files located in the following directory, where <ACServer> is the directory in which you installed the Enterprise Management Server:

<ACServer>\IAM Suite\Access Control\tools\samples\feeder

Create a header row or line that specifies the names of the endpoint attributes.

The names of the endpoint attributes are as follows. Some endpoint attributes are valid only for certain endpoint types. If you specify an attribute in the header of the CSV file and there is no value used for a specific line in the file you need to leave a placeholder there (,,)

Note: The list below is not all inclusive. You can find additional information in the product documentation.

Attribute name	Description	Additional information
OBJECT_TYPE	Specifies the type of the object to import.	Value: ENDPOINT
ACTION_TYPE	Specifies the type of action to perform	Value: CREATE, MODIFY, DELETE
%FRIENDLY_NAME%	Defines the name that you use to refer to this endpoint within CA ControlMinder Enterprise Management.	
DESCRIPTION	Defines any descriptive information that you want to record for this endpoint.	
DO_NOT_VALIDATE	(Optional) Identifies whether or not to connect to the endpoint when creating the endpoint. If the endpoint is offline, you may not want the connection to be validated because this results in an error.	Values: TRUE, FALSE Default: TRUE
ENDPOINT_TYPE	Specifies the type of the endpoint.	You can view the available endpoint types in CA ControlMinder Enterprise

		Management.
HOST	Defines the host name of the endpoint.	It is a best practice to use the DNS fully qualified domain name
LOGIN_USER	<p>Defines the name of an administrative user of the endpoint.</p> <p>This field is ignored when the IS_ADVANCE attribute has a value of TRUE.</p> <p>Setting the IS_ADVANCE attribute to TRUE is recommended when possible because the password does not have to be provided in the PASSWORD attribute.</p>	<p>Valid for all endpoint types</p> <p>LOGIN_USER identifies the administrative account that connects to the endpoint and performs administrative tasks unless the IS_ADVANCE attribute has a value of TRUE. For the latter case, an already existing privileged administrative account is used.</p> <p>For the SSH Device endpoint type, the administrative accounts described above only connect to the endpoint when the OPERATION_ADMIN_USER_NAME is defined. The OPERATION_ADMIN_USER_NAME attribute defines the account that performs administrative tasks.</p> <p>When the OPERATION_ADMIN_USER_NAME is not defined, the SSH Device endpoint type behaves like all other endpoint types.</p>
PASSWORD	Defines the password of LOGIN_USER.	When “IS_ADVANCE” identifies the administrative user, “PASSWORD” is ignored, but a placeholder is still required in the feeder file. There are advantages to not identifying the password.
URL	Defines the URL that CA ControlMinder Enterprise Management uses to connect to the endpoint. This attribute is valid for the MS SQL Server and Oracle Server endpoint types.	<p>Format: (MS SQL Server) jdbc:sqlserver://servername:port;</p> <p>Format: (Oracle Server) jdbc:oracle:drivername:@hostna</p>

		me:port:service
DOMAIN	<p>Provides the NETBIOS name of the endpoint when an account local to the endpoint will be managed as a privileged account.</p> <p>Provide the NETBIOS name of the Active Directory domain when a domain account will be managed.</p>	<p>Valid for the endpoint types:</p> <p>Access Control for SAM</p> <p>Windows Agentless</p>
IS_ACTIVE_DIRECTORY	<p>Specifies whether the endpoint is an Active Directory domain or an Active Directory domain controller.</p>	<p>Valid only for the Windows Agentless endpoint type.</p> <p>Limits: TRUE, FALSE</p>
USER_DOMAIN	<p>The NETBIOS name of the Active Directory domain of which the administrative privileged account is a member.</p> <p>Required when:</p> <p>LOGIN_USER defines an Active Directory account instead of a local account.</p> <p>The Advanced option is selected and the administrative privileged account is an Active Directory domain user.</p> <p>Not required when:</p> <p>LOGIN_USER defines a local account.</p>	<p>Valid for the Windows Agentless endpoint type.</p>
CONFIGURATION_FILE	<p>Specifies the name of the SSH Device XML configuration file that you are defining.</p>	<p>Valid only for the SSH Device and the Network Device endpoint types.</p> <p>Note: If you do not specify a value for this attribute, CA ControlMinder Enterprise Management uses the default configuration file (ssh_connector_conf.xml).</p> <p>Some endpoints require a different XML file. Refer to the product documentation for additional information.</p>
OPERATION_ADMIN_USER_NAME	<p>(Optional) Defines the name of the operation administrator user of the</p>	<p>Valid only for the SSH Device</p>

	<p>endpoint. SAM uses this account to perform administrative tasks on the endpoint, for example, discovering and changing the password of privileged accounts.</p> <p>The purpose is to allow an account with less privilege to connect to the endpoint but perform administrative tasks with another account having enough privileges.</p>	<p>endpoint type.</p> <p>‘LOGIN_USER’ defines the connection account unless you use the “IS_ADVANCE” and related attributes to identify the connection account.</p>
OPERATION_ADMIN_USER_PASSWORD	(Optional) Defines the password for the operation administrator user of the endpoint.	Valid only for the SSH Device endpoint type.
IS_ADVANCE	(Optional) Specifies whether you want to use an existing privileged administrative account already known to SAM to connect to the endpoint and to perform administrative tasks on the endpoint, for example, to discover accounts and change passwords.	<p>Valid for all endpoint types.</p> <p>Limits: TRUE, FALSE</p> <p>Note: When the IS_ADVANCE attribute has a value of TRUE, the LOGIN_USER attribute is ignored, but you must provide values for: PROPERTY_ADMIN_ACCOUNT_ENDPOINT_TYPE, PROPERTY_ADMIN_ACCOUNT_ENDPOINT_NAME, PROPERTY_ADMIN_ACCOUNT_CONTAINER, and PROPERTY_ADMIN_ACCOUNT_NAME.</p>
PROPERTY_ADMIN_ACCOUNT_ENDPOINT_TYPE	(Optional) Defines the endpoint type on which the privileged administrative account is defined.	IS_ADVANCE must be TRUE.
PROPERTY_ADMIN_ACCOUNT_ENDPOINT_NAME	(Optional) Defines the name of the endpoint on which the privileged administrative account is defined. The endpoint must already exist in CA ControlMinder Enterprise Management.	IS_ADVANCE must be TRUE.
PROPERTY_ADMIN_ACCOUNT_CONTAINER	(Optional) Defines the container in which the privileged administrative account is defined. A container is a class whose instances are collections of other objects.	<p>IS_ADVANCE must be TRUE.</p> <p>Values by endpoint type:</p> <p>(Windows Agentless and Oracle Server): Accounts</p> <p>(SSH Device): SSH Accounts</p> <p>(MS SQL Server): MS SQL Logins</p>

PROPERTY_ADMIN_ACCOUNT_NAME	(Optional) Defines the name of the privileged administrative account that SAM uses to perform administrative tasks on the endpoint, for example, to discover accounts and change passwords. The privileged account must already exist in CA ControlMinder Enterprise Management.	IS_ADVANCE must be TRUE.
LOGIN_APPLICATION	Specify the name of the login application to associate with the endpoint.	<p>When a SAM user checks out a privileged account, a session can be automatically started, for example, RDP could start a session on a Windows endpoint using the privileged account's credentials.</p> <p>The login application must already be defined to SAM.</p>
OWNER_INFO	Specifies the name of the endpoint owner.	This can be either a user or group name that is defined in the user store used by CM ENTM.
OWNER_TYPE	Specify if the owner is a group or user.	Values: GROUP, USER
DEPARTMENT_INFO	Specifies the name of the department.	The intent is to identify the department associated with the endpoint or privileged account, but this field can be used for any purpose.
CUSTOM1.....5_INFO	Specifies up to five customer-specific attributes.	<p>These are free-form fields that can be used for any purpose.</p> <p>As described earlier, we used CUSTOM1_INFO to store information used for endpoint tagging.</p>
ADMIN_ACCOUNT_IS_DISCONNECTED	Specifies if the endpoint administrator account is disconnected.	<p>When TRUE, the password of the account used to connect to the endpoint is not managed (changed) by CM SAM.</p> <p>Values: TRUE, FALSE; Default: TRUE</p>
DISABLE_EXCLUSIVE_SESSIONS	Specifies whether or not to disable the exclusive sessions option on this endpoint.	Values: TRUE, FALSE; Default: FALSE

DENY_BREAKGLASS_EXCLUSIVE	Specifies whether or not to prevent checkout of an exclusive account that is already checked out via break glass.	Values: TRUE, FALSE; Default: FALSE
----------------------------------	---	-------------------------------------

You can use a spreadsheet or text editor of your choice to create the SAM feeder CSV file.

We suggest using a spreadsheet editor and exporting the file to CSV format (comma delimited).

Here as an example of an endpoint import CSV file.

```
OBJECT_TYPE,ACTION_TYPE,%FRIENDLY_NAME%,DESCRIPTION,ENDPOINT_TYPE,HOST,LOGIN_USER,DOMAIN,IS_ACTIVE_DIRECTORY,USER_DOMAIN,IS_ADVANCE,PROPERTY_ADMIN_ACCOUNT_ENDPOINT_TYPE,PROPERTY_ADMIN_ACCOUNT_ENDPOINT_NAME,PROPERTY_ADMIN_ACCOUNT_CONTAINER,PROPERTY_ADMIN_ACCOUNT_NAME,OWNER_INFO,OWNER_TYPE,CUSTOM1_INFO
ENDPOINT,CREATE,Windows@win2k8uat02.forwardinc.ca,Created by the SAM feeder,Windows
Agentless,win2k8uat02.forwardinc.ca,,WIN2K8UAT01,FALSE,FORWARDINC,TRUE,Windows Agentless,Windows@adds.forwardinc.ca,Accounts,cmsam,"CA CM UAT Approvers","GROUP","UAT"
ENDPOINT,CREATE,Windows@win2k8test02.forwardinc.ca,Created by the SAM feeder,Windows
Agentless,win2k8test02.forwardinc.ca,,WIN2K8TESTD01,FALSE,FORWARDINC,TRUE,Windows Agentless,Windows@adds.forwardinc.ca,Accounts,cmsam,"CA CM Test Approvers","GROUP","Test"
ENDPOINT,CREATE,Windows@win2k8prod02.forwardinc.ca,Created by the SAM feeder,Windows
Agentless,win2k8prod02.forwardinc.ca,,WIN2K8PROD02,FALSE,FORWARDINC,TRUE,Windows Agentless,Windows@adds.forwardinc.ca,Accounts,cmsam,"CA CM Prod Approvers","GROUP","Prod"
```

This file includes the header record and 3 endpoint records.

This will create 3 Windows Agentless Endpoints – OBJECT_TYPE = ENDPOINT, ACTION_TYPE = CREATE.

The IS_ADVANCE property is set to TRUE, which means that a privileged account already defined to SAM is used to connect to and manage the endpoint. The previously discovered administrative account is the “cmsam” Active Directory account from the [Windows@adds.forwardinc.ca](#) endpoint. The examples assume that the three new endpoints are members of the Active Directory domain, and “cmsam” has administrative rights on these endpoints.

For all three endpoints, the OWNER_INFO attribute is set to an Active Directory group, CA CM Prod Approvers, and the CUSTOM1_INFO attribute is set to Prod per our need to have a way to tag the endpoints’ environment.

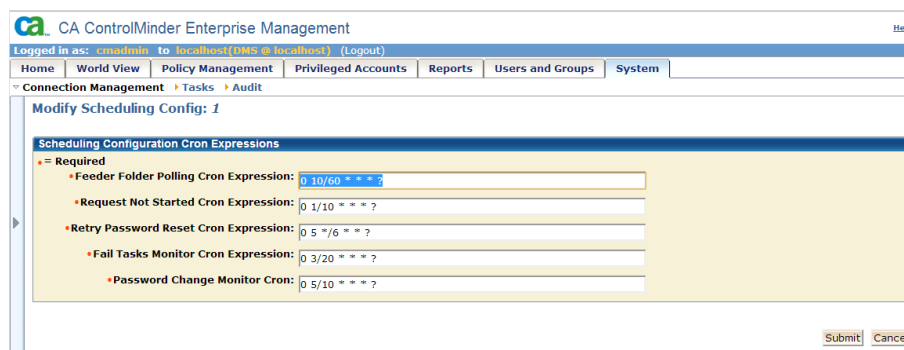
When you are ready to add these endpoints to SAM, copy the CSV file to the following location:

JBoss_home/server/default/deploy/IdentityMinder.ear/custom/ppm/feeder/waitingToBeProcessed

where JBoss_home provides the drive and path to the JBoss installation on the Enterprise Management server. By default, the feeder checks the folder every hour.

CA ControlMinder Rapid Implementation Guide – Shared Account Management

Go to System\Connection Management\Modify Scheduling Config to view or modify the feeder's schedule.



CA ControlMinder Enterprise Management

Logged in as: cmanadmin to localhost (DMS @ localhost) (Logout)

Home World View Policy Management Privileged Accounts Reports Users and Groups System

Connection Management Tasks Audit

Modify Scheduling Config: 1

Scheduling Configuration Cron Expressions

Required

- Feeder Folder Polling Cron Expression: 0 10/60 * * * ?
- Request Not Started Cron Expression: 0 1/10 * * * ?
- Retry Password Reset Cron Expression: 0 5 */6 * * * ?
- Fail Tasks Monitor Cron Expression: 0 3/20 * * * ?
- Password Change Monitor Cron: 0 5/10 * * * ?

Submit Cancel

From the above example, the Feeder Folder Polling Cron Expression is set to:

0 10/60 * * * ?

The previous expression implies that the feeder polling job runs automatically every 60 minutes, starting on the 10th minute. This is a standard expression as used for cron scheduling. You can modify this expression to suit your needs.

Go to Privileged Accounts\Accounts\Feeder Folder Polling to start the polling manually.

The Feeder Folder Polling screen appears.



CA ControlMinder Enterprise Management

Logged in as: cmanadmin to localhost (DMS @ localhost) (Logout)

Home World View Policy Management Privileged Accounts Reports Users and Groups System

Accounts Endpoints Login Application Password Consumers Password Policy Audit

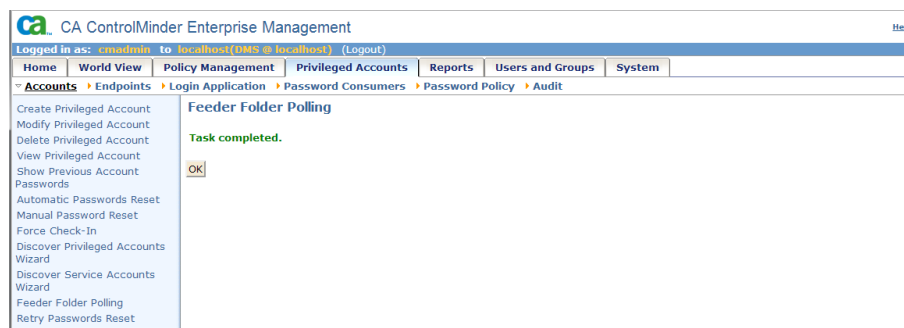
Feeder Folder Polling

Submit Cancel

Click Submit.

The SAM feeder processes the CSV files in the polling folder.

You will see the screen below when the task is submitted.



CA ControlMinder Enterprise Management

Logged in as: cmanadmin to localhost (DMS @ localhost) (Logout)

Home World View Policy Management Privileged Accounts Reports Users and Groups System

Accounts Endpoints Login Application Password Consumers Password Policy Audit

Feeder Folder Polling

Task completed.

OK

Create Privileged Account
Modify Privileged Account
Delete Privileged Account
View Privileged Account
Show Previous Account
Passwords
Automatic Passwords Reset
Manual Password Reset
Force Check-In
Discover Privileged Accounts
Wizard
Discover Service Accounts
Wizard
Feeder Folder Polling
Retry Passwords Reset

You can check files in the following folders for processed records and failures.

CA ControlMinder Rapid Implementation Guide – Shared Account Management

Files in the following directory include all the processed records (failures AND successes).

JBoss_home/server/default/deploy/IdentityMinder.ear/custom/ppm/feeder/processed

Files in the following directory include the records that resulted only in failure. The reason for the failure is noted at the end of each record:

JBoss_home/server/default/deploy/IdentityMinder.ear/custom/ppm/feeder/failedToSubmit

You can also view the results in the UI at System/Audit/ View Submitted Tasks.

You can also use the feeder to delete or modify the endpoints. Set ACTION_TYPE in the CSVfile to DELETE or MODIFY, as appropriate.

The following example modifies OWNER_INFO (used to store approvers) to "CA CM Prod Approvers" and CUSTOM1_INFO to "PROD" (used for tagging). Other attributes stay the same as populated by the feeder in the above mentioned CREATE action.

```
OBJECT_TYPE,ACTION_TYPE,%FRIENDLY_NAME%,DESCRIPTION,ENDPOINT_TYPE,HOST,LOGIN_
USER,DOMAIN,IS_ACTIVE_DIRECTORY,USER_DOMAIN,IS_ADVANCE,PROPERTY_ADMIN_ACCOUNT_
_ENDPOINT_TYPE,PROPERTY_ADMIN_ACCOUNT_ENDPOINT_NAME,PROPERTY_ADMIN_ACCOUNT_CO
NTAINER,PROPERTY_ADMIN_ACCOUNT_NAME,OWNER_INFO,OWNER_TYPE,CUSTOM1_INFO
ENDPOINT,MODIFY,Windows@win2k8uat02.forwardinc.ca,Modified by the SAM
feeder,Windows
Agentless,win2k8uat02.forwardinc.ca,,WIN2K8UAT01,FALSE,FORWARDINC,TRUE,Window
s Agentless,Windows@adds.forwardinc.ca,Accounts,cmsam,"CA CM Prod
Approvers","GROUP","PROD"
```

Import Privileged Accounts using the SAM feeder

You can also use the feeder to create, modify and delete privileged accounts.

The process is the same as for the endpoints, but the attributes are different.

You need to create a CSV file and give it an appropriate name.

Each row or line in the privileged account CSV file, after the header row or line, represents a task to create, modify, or delete a privileged account in CA ControlMinder Enterprise Management.

Attribute name	Description	Additional information
OBJECT_TYPE	Specifies the type of the object to import.	Value: ACCOUNT_PASSWORD
ACTION_TYPE	Specifies the type of action to perform	Value: CREATE, MODIFY, DELETE
ACCOUNT_NAME	Defines the name by which the endpoint refers to the account.	Note: Use upper case for mainframe privileged accounts, for example, RACF, ACF2, and Top Secret accounts and for Oracle accounts. Use the proper case for

		the SSH Device endpoint type because it is case-sensitive.
ENDPOINT_NAME	Specifies the name of the endpoint on which the privileged account resides.	NOTE: The endpoint must already exist before creating any privileged accounts for the endpoint.
NAMESPACE	Specifies the endpoint type of the endpoint.	Note: You can view the available endpoint types in CA ControlMinder Enterprise Management.
CONTAINER	Specifies the name of the container for the shared account. A container is a class whose instances are collections of other objects. Containers are used to store objects in an organized way following specific access rules.	Values: Windows Agentless and Oracle Server endpoints: Accounts SSH Device endpoints: SSH Accounts MS SQL Server endpoints: MS SQL Logins.
DISCONNECTED_SYSTEM	Specifies if the shared account originates from a disconnected system.	If you specify TRUE, SAM does not manage the account password. Instead, SAM acts only as a password vault for the privileged account. Anytime the account's password is changed on the endpoint, someone must manually update the password in SAM. Values: TRUE, FALSE
EXCLUSIVE_ACCOUNT	Specifies if the account can only be checked out by one user at a time.	EXCLUSIVE – SAM lets a single user check-out the account at any time. EXCLUSIVE_SESSIONS – SAM verifies that the privileged account is not already in use on the endpoint before allowing the account to be checked out. NONE – SAM allows multiple users to check-out the account concurrently. Values: EXCLUSIVE_SESSIONS, EXCLUSIVE, NONE
NEW_PASSWORD	Defines the password for the shared account. If you do not	Note: The password must comply with the password policy.

	specify a value for this attribute, CA ControlMinder Enterprise Management generates a password that complies with the specified password policy.	
PASSWORD_POLICY	Specifies the password policy for the shared account.	Note: If you specify a password policy that does not exist, the task fails and CA ControlMinder Enterprise Management does not create the account.
OWNER_INFO	Specifies the name of the account owner.	This attribute is inherited from the endpoint if not specified.
OWNER_TYPE	Specify if the owner is a group or user	Values: GROUP or USER
DEPARTMENT_INFO	Specifies the name of the department.	This attribute is inherited from the endpoint if not specified.
CUSTOM1....5_INFO	Specifies up to five customer-specific attributes.	These attributes are inherited from the endpoint if not specified.
CHANGE_PASSWORD_ON_CHECKOUT	Specifies if you want CA ControlMinder Enterprise Management to change the password of the account every time it is checked out.	Values: TRUE, FALSE Default: FALSE Use this option if there is a possibility that the account password might be changed outside of SAM. This is to ensure that the checked out password matches the one on the target system.
CHANGE_PASSWORD_ON_CHECKIN	Specifies whether you want CA ControlMinder Enterprise Management to change the password of the account every time it is checked in by a user, program, or when the checkout period expires.	Values: TRUE, FALSE Default: TRUE It is a best practice to change the account password on check in.

The following CSV file snippet imports 3 privileged accounts to CM SAM.

The account passwords will be managed by SAM. Multiple users can checkout these privileged accounts since EXCLUSIVE_ACCOUNT is set to NONE.

Note that NEW_PASSWORD attribute is empty so the account password will be generated by CA SAM using the specified password policy.


```
OBJECT_TYPE,ACTION_TYPE,ACCOUNT_NAME,ENDPOINT_NAME,NAMESPACE,CONTAINER,DISCONNECTED_SYSTEM,EXCLUSIVE_ACCOUNT,NEW_PASSWORD,PASSWORD_POLICY
ACCOUNT_PASSWORD,CREATE,osprodadm02,Windows@win2k8prod02.forwardinc.ca,Windows Agentless,Accounts,FALSE,NONE,,Windows password policy
ACCOUNT_PASSWORD,CREATE,osuataadm02,Windows@win2k8uat02.forwardinc.ca,Windows Agentless,Accounts,FALSE,NONE,,Windows password policy
ACCOUNT_PASSWORD,CREATE,ostestadm03,Windows@win2k8test03.forwardinc.ca,Windows Agentless,Accounts,FALSE,NONE,,Windows password policy
```

Set ACTION_TYPE to DELETE or MODIFY to delete or update an account.

The following CSV file snippet modifies PASSWORD_POLICY to “Windows password policy – Strong”

```
OBJECT_TYPE,ACTION_TYPE,ACCOUNT_NAME,ENDPOINT_NAME,NAMESPACE,CONTAINER,DISCONNECTED_SYSTEM,EXCLUSIVE_ACCOUNT,NEW_PASSWORD,PASSWORD_POLICY
ACCOUNT_PASSWORD,MODIFY,osprodadm02,Windows@win2k8prod02.forwardinc.ca,Windows Agentless,Accounts,FALSE,NONE,,Windows password policy - Strong
```

The manual feeder polling instructions are the same for endpoints and accounts.

Configure Email Notification for Workflow

CA ControlMinder Enterprise Management can send email notifications when a specific event occurs.

Email notifications inform CA ControlMinder Enterprise Management users of events in the system, and are generated from email templates. If you enable email notifications, CA ControlMinder Enterprise Management can generate email notifications when one of the following occurs:

- An event that requires approval or rejection is pending.
- An approver approves an event.
- An approver rejects an event.
- An event starts, fails, or completes.
- A CA ControlMinder Enterprise Management user is created or modified.

It is a best practice to enable email notifications for events related to approval workflows.

The two events of interest include:

BreakGlassCheckOutAccountEvent

CreatePrivilegedAccountExceptionEvent

It is also possible to have a notification for “CheckOutAccountPasswordEvent” if you require a notification to be received every time a password is checked out.

To configure email notification settings follow these steps:

Stop the JBoss service from the Services panel.

Open the mail-service.xml file. By default, the file is located in the following directory:

JBoss_HOME/server/default/deploy

Locate the following entry in the file:

```
<property name="mail.smtp.host" value="smtp.nosuchhost.nosuchdomain.com"/>
```

Change the smtp.nosuchhost.nosuchdomain.com value to the full DNS domain name of the outgoing email server host. For example:

```
<property name="mail.smtp.host" value="mysmtpserver.mydomain.com"/>
```

Note: The Enterprise Management Server must resolve the IP address of the SMTP server to the full DNS domain name that you specify for this property.

Update the smtp port if required.

```
<property name="mail.smtp.port" value="25"/>
```

Open the corresponding email templates for the privileged account password request

CreatePrivilegedAccountExceptionEvent.tmpl file in the following directories:

JBoss_HOME/server/default/deploy/IdentityMinder.ear/custom/emailTemplates/default/approved

JBoss_HOME/server/default/deploy/IdentityMinder.ear/custom/emailTemplates/default/completed

JBoss_HOME/server/default/deploy/IdentityMinder.ear/custom/emailTemplates/default/pending

JBoss_HOME/server/default/deploy/IdentityMinder.ear/custom/emailTemplates/default/rejected

Modify the template host name and port from "localhost:8080" to the Enterprise Management Server host name and port, for example: myentmserver.mydomain.com:18443

Do the same for the following template BreakGlassCheckOutAccountEvent.tmpl for the break glass event located under:

JBoss_HOME/server/default/deploy/IdentityMinder.ear/custom/emailTemplates/default/pending

Save and close the files.

Open the email.properties file. The file is located in the following directory:

JBoss_HOME/server/default/deploy/IdentityMinder.ear/config/com/netegrity/config/

Edit the following entry:

```
admin.email.address=IMS
```

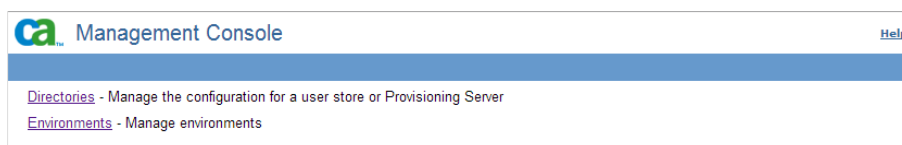
Specify the sender email address then save and close the file. For example:

```
admin.email.address=SAMadmin@mycompany.com
```

CA ControlMinder Rapid Implementation Guide – Shared Account Management

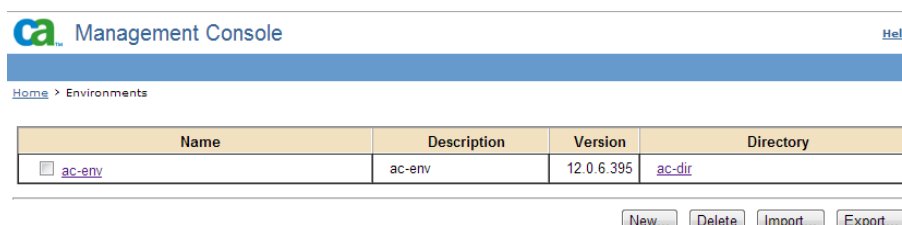
Start JBoss.

In the CA IdentityMinder™ Management Console, click Environments.

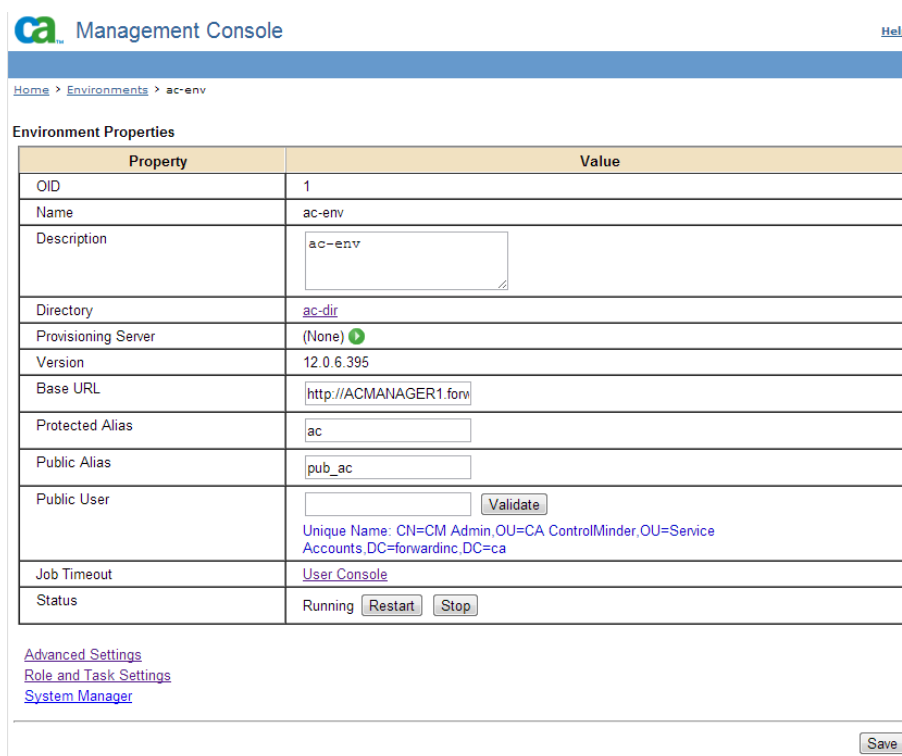


Note: See the “Enable the CA IdentityMinder Management Console” section of this document for the steps to enable and start the console.

Select “ac-env”.

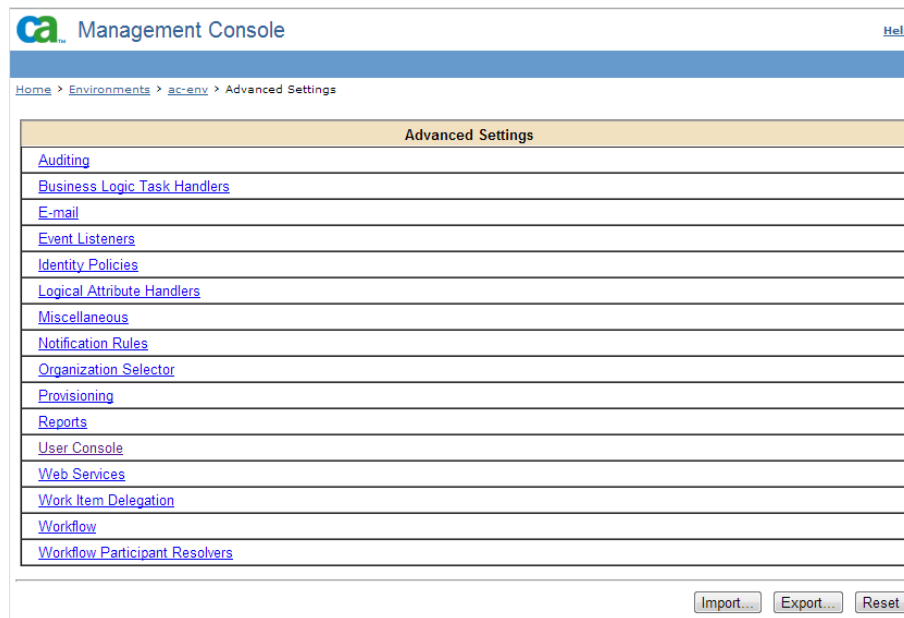


Select “Advanced Settings”.




Select “E-mail”.

CA ControlMinder Rapid Implementation Guide – Shared Account Management



The E-mail Properties window appears.

CA ControlMinder Rapid Implementation Guide – Shared Account Management


Management Console
[Help](#)

[Home](#) > [Environments](#) > [ac-env](#) > [Advanced Settings](#) > [E-mail](#)

E-mail Properties

Property	Value
Events e-mail Enabled	<input type="checkbox"/>
Tasks e-mail Enabled	<input type="checkbox"/>
Template Directory	default

Send e-mail when the following events are completed or during workflow:

Event: [Add](#)

Event
<input type="checkbox"/> AddGrantorOnSharedAccountRoleEvent
<input type="checkbox"/> AddToGroupEvent
<input type="checkbox"/> AssignAdminRoleEvent
<input type="checkbox"/> AssignSharedAccountRoleEvent
<input type="checkbox"/> BreakGlassCheckOutAccountEvent
<input type="checkbox"/> CheckOutAccountPasswordEvent
<input type="checkbox"/> CreateGroupEvent
<input type="checkbox"/> CreateOrganizationEvent
<input type="checkbox"/> CreatePrivilegedAccountExceptionEvent
<input type="checkbox"/> CreatePrivilegedAccountExceptionNotStartedEvent
<input type="checkbox"/> CreateUserEvent
<input type="checkbox"/> DeleteGroupEvent
<input type="checkbox"/> DeleteUserEvent
<input type="checkbox"/> ModifyGroupEvent
<input type="checkbox"/> ModifyUserEvent
<input type="checkbox"/> RemoveFromGroupEvent
<input type="checkbox"/> RevokeAdminRoleEvent
<input type="checkbox"/> RevokeSharedAccountRoleEvent
<input type="checkbox"/> SelfRegisterUserEvent

[Delete](#)

Select the check box next to “Events e-mail Enabled”

This enables email notifications for CA ControlMinder Enterprise Management events, including SAM events.

The Template Directory is set to “default” out of the box.

Do not modify this entry.

Note: The email templates are located in the following directory:

jboss_dir/server/default/deploy/IdentityMinder.ear/custom/emailTemplates/default

Specify the events for which email notifications are sent.

We recommend that you specify only SAM events for which email templates are provided.

Select the check box next to every event, except the following SAM events:

BreakGlassCheckOutAccountEvent

CA ControlMinder Rapid Implementation Guide – Shared Account Management

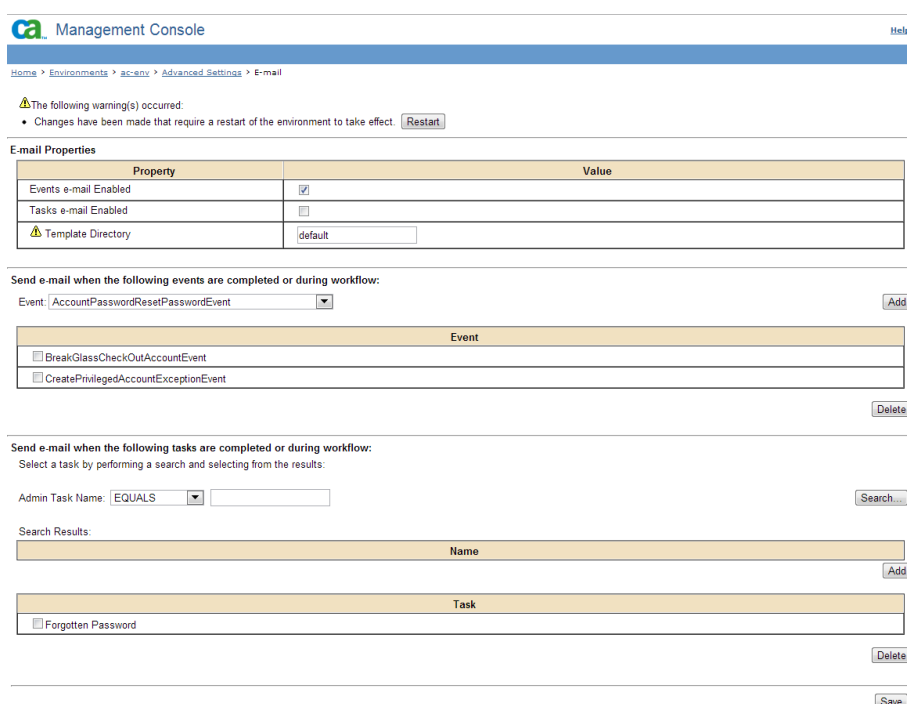
CreatePrivilegedAccountExceptionEvent

Click Delete.

Note: You can also keep “CheckOutAccountPasswordEvent” in if you want to receive a notification every time a password is checked out.

All notifications, other than these two SAM events, are deleted.

You have configured CA ControlMinder Enterprise Management to send email notifications for these two SAM events.



CA Management Console Help

Home > Environments > ac-env > Advanced Settings > E-mail

Warning: The following warning(s) occurred:
 • Changes have been made that require a restart of the environment to take effect. [Restart](#)

E-mail Properties

Property	Value
Events e-mail Enabled	<input checked="" type="checkbox"/>
Tasks e-mail Enabled	<input type="checkbox"/>
Template Directory	default

Send e-mail when the following events are completed or during workflow:

Event: AccountPasswordResetPasswordEvent [Add](#)

Event
<input type="checkbox"/> BreakGlassCheckOutAccountEvent
<input type="checkbox"/> CreatePrivilegedAccountExceptionEvent

[Delete](#)

Send e-mail when the following tasks are completed or during workflow:

Select a task by performing a search and selecting from the results:

Admin Task Name: EQUALS [Search](#)

Search Results:

Name
Add

Task
<input type="checkbox"/> Forgotten Password

[Delete](#)

[Save](#)

Click Save.

The email notification properties are saved.

You are warned that there are changes that require a restart.

Click “Restart.”

The CA IdentityMinder Management Console restarts the environment and applies your changes.

Note: For more information about email notifications, see the Enterprise Administration Guide.

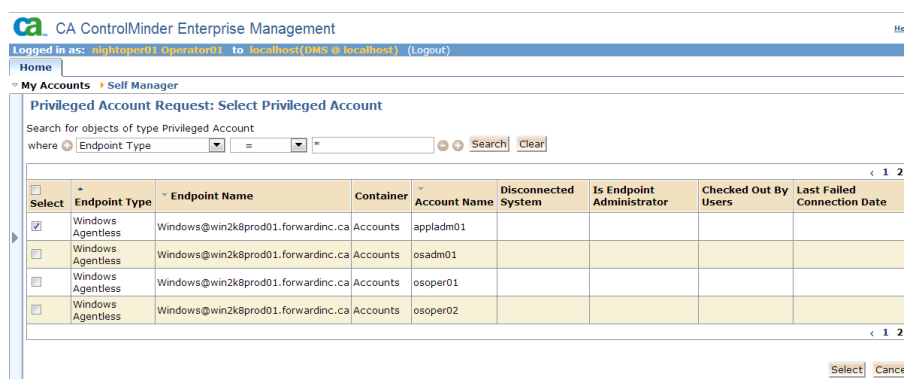
CA ControlMinder Rapid Implementation Guide – Shared Account Management

Verify the Workflow and Email Configuration

Login to Enterprise Management as a user that has no direct access to privileged accounts.

Go to Home\My Accounts\Privileged Account Request.

Search for the account you want to request and select the account.

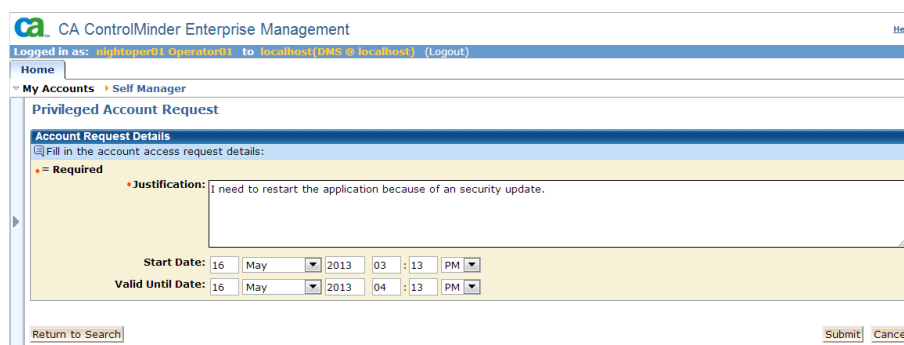


Select	Endpoint Type	Endpoint Name	Container	Account Name	Disconnected System	Is Endpoint Administrator	Checked Out By Users	Last Failed Connection Date
<input checked="" type="checkbox"/>	Windows Agentless	Windows@win2k8prod01.forwardinc.ca	Accounts	appladm01				
<input type="checkbox"/>	Windows Agentless	Windows@win2k8prod01.forwardinc.ca	Accounts	osadm01				
<input type="checkbox"/>	Windows Agentless	Windows@win2k8prod01.forwardinc.ca	Accounts	osoper01				
<input type="checkbox"/>	Windows Agentless	Windows@win2k8prod01.forwardinc.ca	Accounts	osoper02				

Click “Select”.

Provide a justification, start date and valid until date.

Click “Submit”.



Account Request Details

Fill in the account access request details:

Required


Justification: I need to restart the application because of an security update.

Start Date: 16 May 2013 03 :13 PM

Valid Until Date: 16 May 2013 04 :13 PM

Return to Search Submit Cancel

The request is sent for approval.



Privileged Account Request

Task pending.

Return to Search OK

In our case we selected one of the accounts from a production server.

A request for approval will be sent to all the member of the group specified in the “Owner” property of the requested accounts.

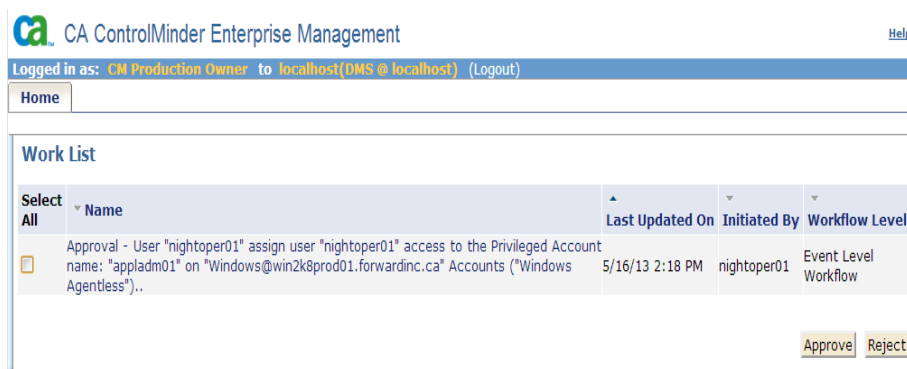
This property is inherited from the endpoint.

CA ControlMinder Rapid Implementation Guide – Shared Account Management

Log in to the user interface as one of the approvers – a member of the AD group specified in the owner field of the privileged account.

You should see a request awaiting an approval.

Click on the hyperlink.



CA ControlMinder Enterprise Management

Logged in as: CM Production Owner to localhost(DMS @ localhost) (Logout)

Home

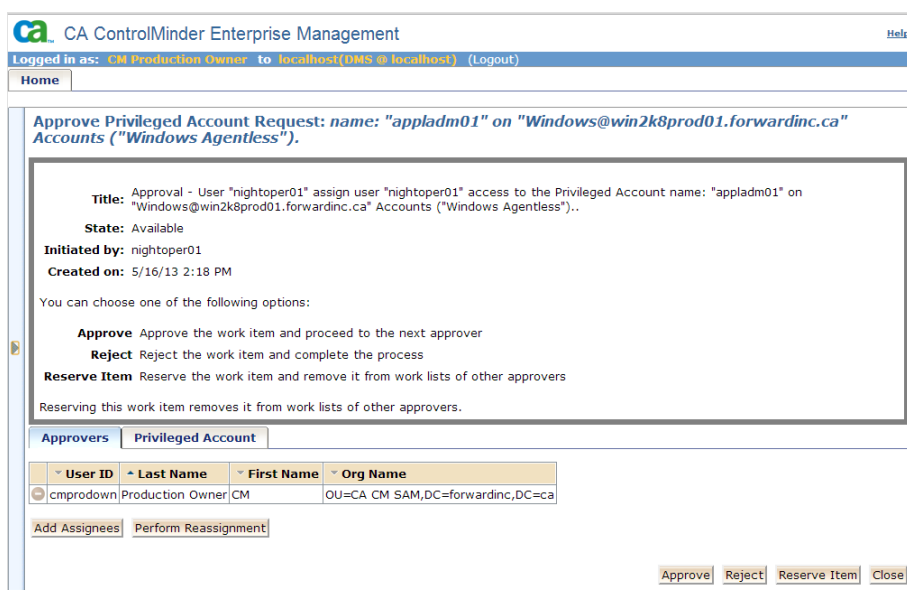
Work List

Select	Name	Last Updated On	Initiated By	Workflow Level
<input type="checkbox"/>	Approval - User "nightoper01" assign user "nightoper01" access to the Privileged Account name: "appladm01" on "Windows@win2k8prod01.forwardinc.ca" Accounts ("Windows Agentless")..	5/16/13 2:18 PM	nightoper01	Event Level Workflow

Approve Reject

You will see the details of the request.

Click "Privileged Accounts" tab for more information about the request.



CA ControlMinder Enterprise Management

Logged in as: CM Production Owner to localhost(DMS @ localhost) (Logout)

Home

Approve Privileged Account Request: name: "appladm01" on "Windows@win2k8prod01.forwardinc.ca" Accounts ("Windows Agentless").

Title: Approval - User "nightoper01" assign user "nightoper01" access to the Privileged Account name: "appladm01" on "Windows@win2k8prod01.forwardinc.ca" Accounts ("Windows Agentless")..

State: Available

Initiated by: nightoper01

Created on: 5/16/13 2:18 PM

You can choose one of the following options:

Approve Approve the work item and proceed to the next approver

Reject Reject the work item and complete the process

Reserve Item Reserve the work item and remove it from work lists of other approvers

Reserving this work item removes it from work lists of other approvers.

Approvers Privileged Account

User ID	Last Name	First Name	Org Name
cmprdown	Production Owner	CM	OU=CA CM SAM,DC=forwardinc,DC=ca

Add Assignees Perform Reassignment

Approve Reject Reserve Item Close

You can add a comment or change the start and valid until dates.

Click "Approve".

CA ControlMinder Rapid Implementation Guide – Shared Account Management

Approvers

Privileged Account

Endpoint Type Windows Agentless
Endpoint Name Windows@win2k8prod01.forwardinc.ca
Container Accounts
Account Name appladm01
Justification I need to restart the application because of an security update.
Start Date 16 May 2013 03 : 18 PM
Valid Until Date 16 May 2013 04 : 18 PM
Comment


Approve

Reject

Reserve Item

Close

Click “OK”.


CA ControlMinder Enterprise Management

Help

Logged in as: CM Production Owner to localhost(DMS @ localhost) (Logout)

Home

Approve Privileged Account Request: name: "appladm01" on "Windows@win2k8prod01.forwardinc.ca" Accounts ("Windows Agentless").
Task pending.

OK

Log out and log in as the user that requested the account.

Go to Home/My Accounts/ My Privileged Accounts.

The requested and approved account is listed.


CA ControlMinder Enterprise Management

Help

Logged in as: nightoper01 Operator01 to localhost(DMS @ localhost) (Logout)

Home

My Accounts Self Manager

My Privileged Accounts

Search My Privileged Accounts
Search the privileged accounts using the following criteria:
Search Accounts: Account Name = * Search
Options:

- ☒ My Accounts
- ☐ Service Accounts
- ☐ Break Glass Accounts
- ☐ Checked-Out Accounts

My Privileged Accounts
View the privileged accounts. Use the Actions menu for each account in order to: Checkout/Checkin, Show Password, Automatic Login and Break Glass.
Show: 10 Results per Page

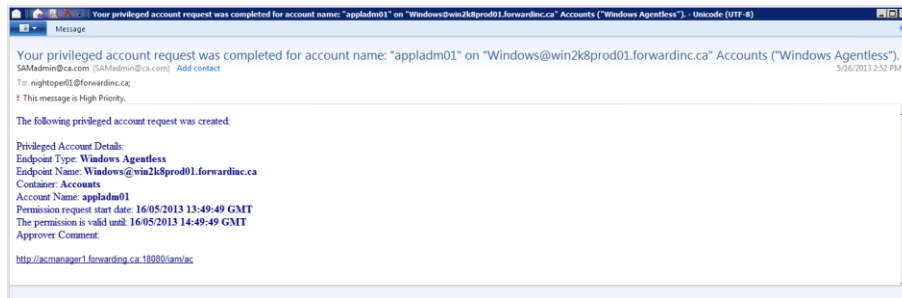
Show Details	Account Name	Endpoint Name	Type	Status	Actions
Show	appladm01	Windows@win2k8prod01.forwardinc.ca	Windows		Actions...

Close

CA ControlMinder Rapid Implementation Guide – Shared Account Management

The user will get an email that the account request was approved if the notification is enabled.

Below is an example of such an email.



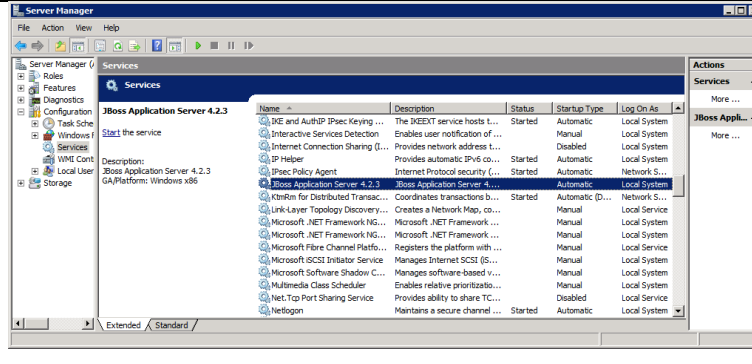
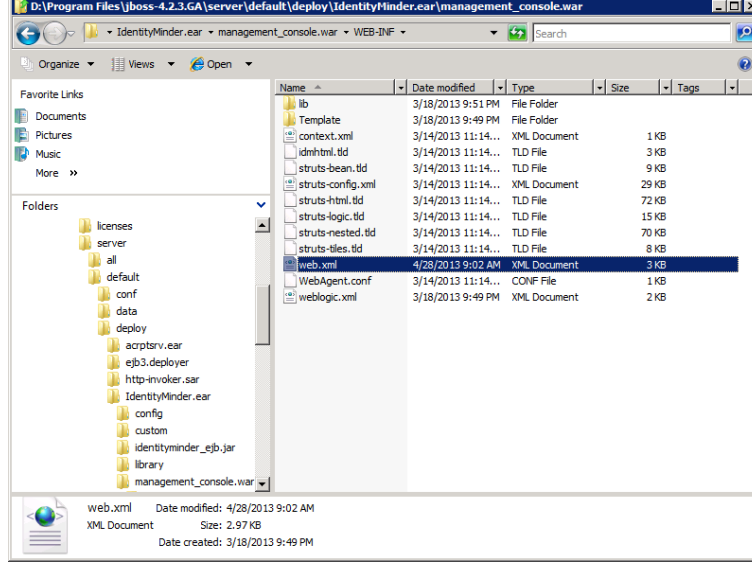
CA ControlMinder Rapid Implementation Guide – Shared Account Management

Enable the CA IdentityMinder Management Console

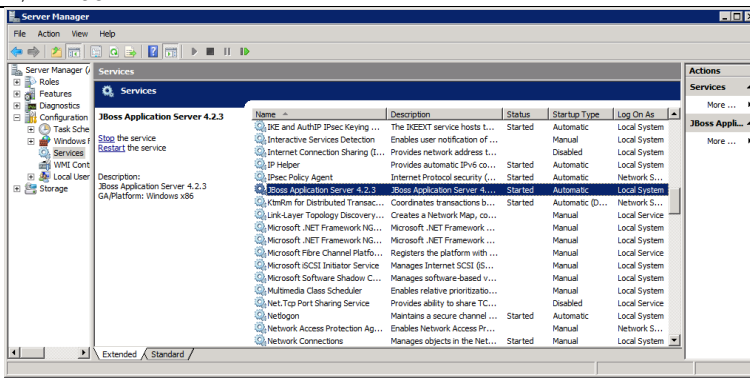
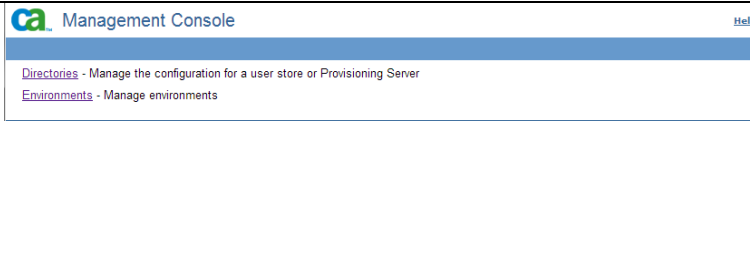
You use the CA IdentityMinder Management Console to perform advanced configuration tasks, such as CA ControlMinder Enterprise Management to send email notifications when a specific event occurs.

When you install the Enterprise Management Server, the CA IdentityMinder Management Console option is disabled.

To enable the CA IdentityMinder Management Console follow these steps:

<p>Stop the JBoss Application Server service from the Services Panel.</p>	
<p>Navigate to the following directory, where JBoss_HOME is the directory where you installed JBoss: JBoss_HOME\server\default\deploy\IdentityMinder.ear\management_console.war\WEB-INF</p>	
<p>Open the web.xml file in an editable form.</p>	
<p>Search for the following section: AccessFilter</p>	<pre><filter> <filter-name>AccessFilter</filter-name> <filter- class>com.netegrity.ims.manage.filter.AccessFilter< /filter-class> <init-param> <param-name>Enable</param-name> <param-value>False</param-value> </init-param></pre>

CA ControlMinder Rapid Implementation Guide – Shared Account Management

	<pre></filter></pre>
<p>In the <param-value> field, change the value to True.</p> <p>Save and close the file.</p>	<pre><filter> <filter-name>AccessFilter</filter-name> <filter- class>com.netegrity.ims.manage.filter.AccessFilter< / filter-class> <init-param> <param-name>Enable</param-name> <param-value>True</param-value> </init-param> </filter></pre>
<p>Restart the JBoss Application Server service from the Services Panel.</p>	 <p>The screenshot shows the Windows Server Manager 'Services' console. The 'JBoss Application Server 4.2.3' service is selected in the list. The 'Actions' pane on the right shows 'Stop the service' and 'Restart the service' options. The service description indicates it is a JBoss Application Server 4.2.3 GA Platform on Windows x64.</p>
<p>The CA IdentityMinder Management Console is enabled.</p> <p>To access the console go to:</p> <p><a href="https://<ENTMserver>:18443/idmmanage">https://<ENTMserver>:18443/idmmanage</p>	 <p>The screenshot shows the CA Management Console web interface. It has a blue header with the CA logo and 'Management Console' text. Below the header, there are two main sections: 'Directories - Manage the configuration for a user store or Provisioning Server' and 'Environments - Manage environments'. A 'Help' link is visible in the top right corner.</p>