CA ControlMinder

Release Notes

12.8

Third-Party Notices

Sample Scripts and Sample SDK Code

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

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

CA Technologies Product References

This document references the following CA Technologies products:

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

Documentation Conventions

The CA ControlMinder documentation uses the following conventions:

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

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

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

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

Example: Command Notation Conventions

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

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

In this example:

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

File Location Conventions

The CA ControlMinder documentation uses the following file location conventions:

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

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

Contact CA Technologies

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

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

Contents

Chapter 6: Feature Support Limitations 35

Chapter 7: Installation Considerations 41

Chapter 1: Welcome

Welcome to CA ControlMinder 12.8. This guide describes new enhancements, changes to existing features, operating system support, system requirements, documentation information, installation and general considerations, published solutions, and known issues for CA ControlMinder.

CA ControlMinder offers enterprise management and reporting capabilities and advanced policy management features.

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

This section contains the following topics:

CA ControlMinder Installation Image Files

CA ControlMinder components are available on the following image files.

The following image files contain Enterprise Management Server and Report Portal components for Windows:

- CA ControlMinder Server Components for Windows

  Contains installation files for CA ControlMinder Endpoint Management, CA ControlMinder Distribution Server, and CA ControlMinder Enterprise Management.

  CA ControlMinder Enterprise Management includes CA ControlMinder Endpoint Management, CA ControlMinder endpoint components for Windows, CA ControlMinder Distribution Server components, and the Deployment Map Server (DMS).

  This image file also includes report packages for import in to CA Business Intelligence.

- CA ControlMinder Third Party Components for Windows

  Contains a prerequisite installer that installs prerequisite third-party software (JDK and JBoss) on Windows. These software applications are required before you can install CA ControlMinder Server Components.

The following image files contain Enterprise Management Server and Report Portal components for Linux:

- CA ControlMinder Server Components for Linux

  Contains installation files for CA ControlMinder Endpoint Management, CA ControlMinder Distribution Server, and CA ControlMinder Enterprise Management.

  CA ControlMinder Enterprise Management includes CA ControlMinder Endpoint Management, CA ControlMinder endpoint components for Linux, CA ControlMinder Distribution Server components, and the Deployment Map Server (DMS).

  This image file also includes report packages for import in to CA Business Intelligence.

- CA ControlMinder Third Party Components for Linux

  Contains prerequisite third-party software (JDK and JBoss) for Linux. These software applications are required before you can install CA ControlMinder Server Components.

Complementary CA User Activity Reporting Module License

As the owner of the CA ControlMinder, you are also entitled to the CA User Activity Reporting Module product for the limited use of collecting, managing and reporting on CA ControlMinder audit logs. First, you must obtain a license for “CA User Activity Reporting Module Server for CA ControlMinder” (Codes ELMSAC99100/ELMSAC991), which is offered to CA ControlMinder customers for a symbolic price.

To obtain your license for CA User Activity Reporting Module in North America, contact your local account representative. If you are outside of North America, call your local account representative or the local CA Technologies office. You can download CA User Activity Reporting Module online through the Download Center on the CA Support Online web site at http://ca.com/support under your CA ControlMinder download links.

A Single Documentation Set

The following describes the documentation for CA ControlMinder:

- Release Notes
- Implementation Guide
- Enterprise Administration Guide
- Upgrade Guide
- Implementation Guide
- Endpoint Administration Guide for Windows

- Endpoint Administration Guide for UNIX
- Reference Guide
- selang Reference Guide
- Troubleshooting Guide

Chapter 2: New and Changed Features

This section contains the following topics:

CA ControlMinder Enhancements

The following CA ControlMinder enhancements and fixes were made since the last release:

- **New CA ControlMinder Enterprise Management User Interface**

  CA ControlMinder Enterprise Management now has a new user interface that provides an improved user experience and ease of use.

- **Active Directory Endpoints Discovery**

  You can use the Active Directory endpoints discovery wizard to quickly configure your environment. For more information, see the *Enterprise Administration Guide*.

- **Endpoints Status and Monitoring**

  CA ControlMinder Enterprise Management now displays the installation, health and enforcement status for each endpoint in your environment. For more information, see the *Enterprise Administration Guide.*

- **Enhanced Shared Accounts Auditing**

  CA ControlMinder Enterprise Management now displays shared accounts audit records for access, request, break-glass and password change events by predefined filters. For more information, see the *Enterprise Administration Guide*.

- **Support for Cloud Operating Systems**

  You can now install CA ControlMinder on Debian and Ubuntu operating systems. For more information, see the *Installation Guide*.

- **Parallel Upgrade on CA ControlMinder Endpoint**

  CA ControlMinder now supports parallel upgrade on Solaris, Linux, AIX operating systems. For more information, see the *Upgrade Guide*.

- **Integration with CA AuthMinder**

  You can now integrate CA ControlMinder with CA AuthMinder to leverage strong authentication capabilities on a UNIX endpoint. For more information, see the *Integration Guide*.

- **CA ControlMinder Support for Microsoft Windows Server 2012 and SQL Server 2012**

  You can now install the Enterprise Management Server on Microsoft Windows Server 2012 and SQL Server 2012. You can also install CA ControlMinder on Microsoft Windows Server 2012.

- **Sepromote Utility**

  You can use the sepromote utility to validate OTP (One-Time-Passwords) generated by CA AuthMinder. For more information, see the *Reference Guide.*

UNAB Enhancements

The following UNAB enhancements and fixes were made since the last release:

- **login Policy for Partial User**

  You can now restrict partial users to log in to endpoints only when a corresponding policy is deployed. To control partial users login you use the partial_user_login_policy token. For more information, refer to the *Reference Guide*.

- **Support for User Name with Tilde (~)**

  You can now use Active Directory user accounts with tilde (~) characters on Linux.

- **Support for AIX PAM Flag pam_silent**

  UNAB now supports AIX PAM module control flag pam_silent to eliminate PAM messages.

- **Check UNAB Database**

  The UNAB agent periodically checks the users and groups database and rebuilds the database if it is corrupted.

- **UNAB Renew Computer Password**

  UNAB agent can now renew the computer object password that was used to register the computer in Active Directory. Use the computer_password_change_interval token. For more information, refer to the *Reference Guide.*

Documentation Enhancements

The following documentation enhancements were made since the last release:

- **Scenario Based Content**

  Added the following scenarios:

  - How to install CA ControlMinder on Debian or Ubuntu Linux

    Describes how to install CA ControlMinder on Debian or Ubuntu Linux operating systems.

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

  - How to Upgrade CA ControlMinder on Linux

    Describes how to perform a parallel upgrade of CA ControlMinder on Linux using RPM.

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

- How to Upgrade CA ControlMinder on AIX

  Describes how to perform a parallel upgrade of CA ControlMinder on AIX.

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

- How to Upgrade CA ControlMinder on Solaris

  Describes how to perform a parallel upgrade of CA ControlMinder on Solaris.

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

- How to Upgrade CA ControlMinder on Solaris Zones

  Describes how to perform a parallel upgrade of CA ControlMinder on Solaris Zones.

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

- Enabling User Password Reset and Resetting a Forgotten Password

  Describes how to configure user accounts and profiles to enable users to reset their password and how users reset a forgotten password.

  Note: For more information, see the *Enterprise Administration Guide*.

- Integration with CA AuthMinder

  Describes how to integrate with CA AuthMinder to provide a strong authentication option for privileged and other native users of the operating system.

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

- Implementing CA ControlMinder High Availability on Linux Using Veritas Cluster Server

  Describes how to implement a high availability deployment on CA ControlMinder on Linux using Veritas cluster server.

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

- How to Upgrade an Enterprise Management Server Deployment

  Describes how to upgrade an Enterprise Management Server deployment to a newer version through migration.

- How to Configure the Apache Load Balancer

  Describes how to configure Enterprise Management Servers for load balancing using Apache HTTPD

Fixed Issues in This Release

Fixes included in this release are documented in the Release FIXLIST. You can access the FIXLIST from the CA ControlMinder Latest Maintenance Release page on CA Support.

Chapter 3: System Requirements

This section contains the following topics:

Operating System Support

For a list of supported operating systems, see the CA ControlMinder Compatibility Matrix that is available from the CA ControlMinder product page on CA Support.

Enterprise Management Server Requirements

The minimum requirements for the Enterprise Management Server are:

- **Processor**—Intel (EM64T) or AM (AMD-V) or newer 64bit processor
- **Memory**—4-GB RAM
- **Available disk space**—10 GB at an installation directory; 2 GB at %TEMP% (Windows) or /tmp (UNIX); 4-GB swap file; 1.5 GB at the JBoss directory.

  Note: For the recommended hardware specifications refer to the *Implementation Guide*, *Planning Your Enterprise Implementation* chapter.

In addition, install the following software in the Enterprise Server:

- **JDK**—Java Development Kit (JDK) 1.7 or higher
- **Application server**—JBoss Application Server version 4.2.3.GA
- **A central database (RDBMS)**—Oracle Database 10g, Oracle Database 11g, Microsoft SQL Server 2005, Microsoft SQL Server 2008 or Microsoft SQL Server 2012.

  Note: You can install the central database on another computer. For information about system requirements for your RDBMS, see the documentation for your product.

On the end-user computer, you need a minimum screen resolution of 1024 x 768 and the following settings as your web browser:

- **Windows**—Microsoft Internet Explorer 8.x; or Mozilla Firefox or Chrome
- **Linux**—Mozilla Firefox

Enterprise Management Server Integration Components

The Enterprise Management Server supports integration with the following products:

- **Active Directory**—(Optional) An enterprise user store.

  Note: You do not need to install the user store on the same computer as the Enterprise Management Server.

- **CA Directory**—(Optional) A CA proprietary user store.
- **Sun ONE**—(Optional) An enterprise user store.

  Note: You do not need to install the user store on the same computer as the Enterprise Management Server.

- **Report Portal**—CA Business Intelligence.

  Note: You do not need to install this software on the same computer as the Enterprise Management Server. For information about system requirements for the Report Portal, see the *CA Business Intelligence Installation Guide*.

  Note: For more information about CA Business Intelligence, see the *CA Business Intelligence Installation Guide*, which is available from CA Technologies Support.

- **CA User Activity Reporting Module**—r12.0

  Note: Do not install this software on the same computer as the Enterprise Management Server. For information about system requirements for CA User Activity Reporting Module, see the *CA User Activity Reporting Module Release Notes*.

- **CA Service Desk**—r12.1

  Note: You do not need to install this software on the same computer as the Enterprise Management Server. For information about system requirements for CA Service Desk, see the *CA Service Desk Release Notes*.

- **CA SiteMinder**

  For more information about the system requirements for CA SiteMinder, see the CA SiteMinder *Release Notes.*

- **CA AuthMinder**

  For more information about the system requirements for CA AuthMInder, see the CA AuthMinder Release Notes.

CA ControlMinder Endpoint Management Requirements

The minimum requirements for the CA ControlMinder Endpoint Management computer are:

- **Processor**—(Windows) Pentium PC 2.66 GHz
- **Memory**—2-GB RAM
- **Available disk space**—2-GB at an installation directory; 3 GB at %TEMP% (Windows) or /tmp (UNIX)

In addition, install the following software in the CA ControlMinder Endpoint Management computer:

- **JDK**—Java Development Kit (JDK) 1.7 or higher
- **Application server**—JBoss Application Server version 4.2.3.GA
- **CA ControlMinder**—Latest version of endpoint installation

On the end-user computer, you need a minimum screen resolution of 1024 x 768 and the following as your web browser:

- **Windows**—Microsoft Internet Explorer 6.x or 7.x or 8.x; or Mozilla Firefox 2.x or 3.0 or 3.5
- **Linux**—Mozilla Firefox 2.x or 3.0 or 3.5

UNIX Endpoint Requirements

The minimum requirements for a CA ControlMinder UNIX endpoint are:

- **Memory**—1 GB RAM (2 GB recommended)
- **Available disk space**—250 MB (300 MB for general installations)

In addition, you need disk space for your CA ControlMinder database, which is the repository of records describing your users and user groups, your protected files and other resources, and the authorizations that permit controlled access to the resources. For example, a database for one thousand users, one thousand files, and five hundred access rules, occupies approximately 2 MB of disk space.

Windows Endpoint Requirements

The minimum requirements for a CA ControlMinder Windows endpoint are:

- **Processor**—Intel-based Pentium 4 PC 1.6 GHz
- **Memory**—1-GB RAM
- **Available disk space**—100 MB

In addition, you also need the disk space for your CA ControlMinder database. For example, a database for one thousand users, with one thousand files, and five hundred access rules, occupies approximately 2 MB of disk space.

Enterprise Reporting Requirements

If you use Oracle Database 10g or Oracle Database 11g as your central database (RDBMS), do the following before you install the CA ControlMinder Enterprise Management:

- Verify that the Oracle host and the CA Business Intelligence host can communicate.
- Install Oracle Client software on the CA Business Intelligence host.
- Verify that the Oracle TNS definition on the CA Business Intelligence host points to the central database.

If you use Microsoft SQL Server 2005, Microsoft SQL Server 2008 or Microsoft SQL Server 2012 as your central database (RDMBS), do the following before you install the Report Server:

- Verify that the MS SQL host and the CA Business Intelligence host can communicate.

Important! If you use Microsoft SQL Server as the reporting database, install the Report Portal on a supported Windows operating system.

Distribution Server Requirements

The minimum requirements for the Distribution Server computer are:

- **Processor**—Pentium PC 266 MHz
- **Memory**—2 GB RAM
- **Available disk space**—2 GB at installation; 1 GB at %TEMP% (Windows) or /tmp (UNIX)

In addition, the Distribution Server computer must have the following software installed:

- **JRE**—Java Runtime Environment (JRE) 1.5.0_18 or higher

Policy Model Database Requirements

In addition to endpoint space requirements, you also need additional disk space for each Policy Model you plan to create on the host. Each Policy Model contains a database so you need to calculate the space requirements in the same manner as you did for your CA ControlMinder database.

If you are upgrading and have all your Policy Models databases (PMDBs) in place already, record the space each of the PMDBs uses in the *ACInstallDir*/*policy_model_path*/pmdb_name directory before you upgrade. Use the following calculations to estimate the additional disk space you will need for upgrading each PMDB:

- *ACInstallDir*/policies/pmdb_name/subscribers.dat (size) x 2
- *ACInstallDir*/policies/pmdb_name/updates.dat (size) x 5 + 1000 KB

Chapter 4: Documentation

This section contains the following topics:

Guides

The guides for CA ControlMinder 12.8 are as follows:

- Release Notes
- Implementation Guide
- Endpoint Administration Guide for Windows
- Endpoint Administration Guide for UNIX
- Enterprise Administration Guide
- Integration Guide
- Upgrade Guide
- Reference Guide
- selang Reference Guide
- Troubleshooting Guide

Note: To view PDF files, you must download and install a Portable Document Format (PDF) reader. The CA ControlMinder documentation requires Adobe Reader 7.0.7 or later. You can download Adobe Reader from the Adobe website if it is not already installed on your computer.

In addition to the PDF guides, the CA ControlMinder guides are also available in HTML format and Online Help is accessible from the various web-based interfaces.

Chapter 5: FIPS Compliance

This section contains the following topics:

FIPS Operational Modes

CA ControlMinder has two FIPS operational modes: FIPS-only and regular. In FIPS-only mode, CA ControlMinder uses only those cryptographic functions that are FIPS 140-2 compliant. This means that some CA ControlMinder features are disabled in FIPS-only mode. In regular mode CA ControlMinder uses both FIPS 140-2 cryptographic functions and non-FIPS compliant functions.

Note: To switch between FIPS-only mode and regular, use the *fips_only* configuration setting in the crypto section.

Unsupported Operating Systems for FIPS-only Mode

FIPS-only mode is not supported on the following CA ControlMinder supported operating system architectures:

- Linux s390
- Linux Itanium (IA64)
- Solaris x64
- Windows Itanium (IA64)

FIPS Encryption Libraries

In FIPS-only mode CA ControlMinder uses the CAPKI encryption library. On UNIX systems it uses the OS encryption library for password encryption (“crypt” method). In regular mode, CA ControlMinder uses the CAPKI 4.1.3 encryption library in addition to the non-FIPS encryption libraries.

FIPS Algorithms Used

CA ControlMinder components use the following cryptographic algorithms. Different components use different algorithms.

- In FIPS-only mode:
  - SSL (TLS 1.0)—client/server communication
  - AES in CBC mode—encryption of PMD update file (Windows), bidirectional password history (Windows)
  - SHA-1—Unidirectional password encryption (Windows), Trusted Programs, policy signatures (advanced policy management)
- In regular mode:
  - CA ControlMinder r8 SP1 encryption libraries (DES, Triple DES, AES, MD5, and so on)
  - SSL (SSL V2, SSL V3 and TLS 1.0)—client/server communication
  - SHA-1 (from CAPKI)—used for signatures of trusted programs, signatures of policies
  - AES (from CAPKI)—used for password validation when working with bidirectional password history

Storage of Keys and Certificates

CA ControlMinder stores keys and certificates as follows.

- Symmetric keys are stored as in eTrust Access Control r8 SP1.
- Certificates (subject certificate, private key, and root certificate) are stored on the file system and protected by CA ControlMinder.

  Note: CA ControlMinder encrypts the private key using AES symmetric encryption (from the CAPKI libraries) using CA ControlMinder symmetric key.

Features Affected (UNIX)

The FIPS operational mode can have an effect on the following CA ControlMinder UNIX features:

Feature	Non-FIPS Mode	FIPS Mode
PMD update file encryption	Default symmetric key encryption (two-way)	Disabled

Feature	Non-FIPS Mode	FIPS Mode
Trusted Programs	CAPKI SHA-1 and MD5	CAPKI SHA-1 only
Bidirectional password encryption	Default symmetric key encryption	Disabled
Unidirectional password encryption	Operating system's crypt/bigcrypt method	Operating system's crypt/bigcrypt method
PMD TNG command	Default symmetric key encryption	Disabled
CA ControlMinder TNG daemon	Default symmetric key encryption	Disabled
LDAP password encryption usage (sebuildla -u -n)	Default symmetric key encryption	Disabled
LDAP password encryption generation (seldapcred)	Default symmetric key encryption	Disabled
TCP communication	Default symmetric key encryption (two-way) or CAPKI sockets over SSL V2, SSL V3, or TLS V1	CAPKI sockets over TLS V1
seversion utility	CAPKI SHA-1	CAPKI SHA-1
Trusted Programs (watchdog and seretrust)	CAPKI SHA-1	CAPKI SHA-1
Advanced policy management policy distribution	CAPKI SHA-1 signature, and for backwards compatibility, CA ControlMinder internal SHA-1 signature	CAPKI SHA-1 signature only
selogrd encryption	Default symmetric key encryption and MD5	Disabled
sechkey key change	Default symmetric key encryption	Disabled
iRecorder log file signature	MD5 encryption	Disabled
Report Agent	Enabled	Disabled
SAM Agent	Enabled	Disabled
DMS	Enabled	UNAB endpoints management disabled

Note: Where a feature is disabled as a result of the FIPS operational mode, the relevant program prints an error message and exits, or writes the error message to the system log if a non interactive process occurred. For example: Report Agent or SAM Agent.

Features Affected (Windows)

The FIPS operational mode can have an effect on the following CA ControlMinder Windows features:

Feature	Non-FIPS Mode	FIPS Mode
PMD update file encryption	Default symmetric key encryption (two-way)	CAPKI AES symmetric key encryption
Password history (non-bidirectional)	Saved as CAPKI SHA-1. Password validation with CAPKI SHA-1 and fall through to crypt	Saved as CAPKI SHA-1. Password validation with CAPKI SHA-1 only
Password history (bidirectional)	Default symmetric key encryption. Password validation with default symmetric key encryption	CAPKI AES symmetric key encryption. Password validation with CAPKI AES only.
sechkey key change, password history	Default symmetric key encryption to decrypt and encrypt password history	CAPKI AES symmetric key encryption to decrypt and encrypt password history
sechkey key change, policy model	Default symmetric key encryption to decrypt and encrypt policy model update files	CAPKI AES symmetric key encryption to decrypt and encrypt policy model update files
Trusted Programs	CAPKI SHA-1 and MD5	CAPKI SHA-1 only
Mainframe password synchronization	Enabled	Disabled
iRecorder	Enabled	Disabled
TNG integartion	Enabled	Disabled
Advanced policy management policy distribution	CAPKI SHA-1 signature, and for backwards compatibility, CA ControlMinder internal SHA-1 signature	CAPKI SHA-1 signature only
Report Agent	Enabled	Disabled
SAM Agent	Enabled	Disabled

Feature	Non-FIPS Mode	FIPS Mode
DMS	Enabled	UNAB endpoint management disabled

Note: Where a feature is disabled as a result of the FIPS operational mode, the relevant program prints an error message and exits, or writes the error message to the system log if a non interactive process occurred. For example: Report Agent or SAM Agent.

You should also consider the following:

- When moving from non-FIPS to FIPS, the policy model *cannot* read old commands.
- When moving from FIPS to non-FIPS, the policy model *can* read old commands.
- For non-bidirectional password history, there is no impact when not using crypt in FIPS mode. Crypt is only for backwards compatibility.
- For bidirectional password history, moving from non-FIPS to FIPS, CA ControlMinder cannot decrypt old passwords.

Chapter 6: Feature Support Limitations

This section contains the following topics:

IPv6 Support

CA ControlMinder runs in an IPv4-only environment, an IPv6-only environment, or a mixed environment of both IPv4 and IPv6.

Note: (UNIX) selogrd and selogrcd will not work in IPv6-only environments.

CA ControlMinder does not currently support network access controls on IPv6 networks. This affects the HOST, CONNECT and TCP classes.

You can specify IP addresses to CA ControlMinder in IPv6 format, except that the mask and match feature of HOSTNET class records requires IPv4 format addresses.

Windows Endpoint Limitations

This section describes feature support limitations for Windows endpoints.

x64 Feature Support Limitations

The following are known limitations on Windows 2003 x64:

- Unicenter TNG migration and integration
- Mainframe password synchronization
- Impersonation interception (class SURROGATE functionality), if SurrogateInterceptionMode is set to 1

  Important! Impersonation interception is supported on x64, IA64 and x86 platforms by default via the RunAs plug-in (SurrogateInterceptionMode is set to 0).

  Note: For more information about the SurrogateInterceptionMode registry setting, see the *Reference Guide*.

IA64 Feature Support Limitations

The following features are not supported on IA64 platforms:

- Unicenter TNG migration and integration
- Mainframe password synchronization
- STOP
- Report Agent
- SAM Agent
- SSL
- FIPS 140-2 compliance

Windows Server 2008 Feature Support Limitations

The following are known limitations on Windows Server 2008:

- Impersonation interception (class SURROGATE functionality), if SurrogateInterceptionMode is set to 1

  Important! Impersonation interception is supported on x64, IA64 and x86 platforms by default via the RunAs plug-in (SurrogateInterceptionMode is set to 0).

  Note: For more information about the SurrogateInterceptionMode registry setting, see the *Reference Guide*.

SAN Support

CA ControlMinder supports a SAN (storage area network) environment when you install CA ControlMinder on:

- A local file system and use it to protect files on a SAN, when the SAN is accessible from a single host.

  Note: If the SAN is accessible from multiple hosts, install CA ControlMinder on each host that can access the SAN and use each installation to protect files on the SAN.

- A SAN disk, subject to the following limitations:

  - CA ControlMinder drivers must be installed on the local file system.
  - You must manually start CA ControlMinder on the SAN disk each time you start or restart the computer. Do not start CA ControlMinder automatically when you start or restart the computer.

    Note: The previous condition only applies when you install CA ControlMinder on a SAN disk. If you install CA ControlMinder on a local file system and use it to protect files on a SAN, you do *not* need to manually start CA ControlMinder each time you restart the computer.

If the SAN is accessible from multiple hosts and CA ControlMinder is installed on the SAN, and you want to install CA ControlMinder from a different host to the same location on the SAN, consider the following before you begin:

- The new installation of CA ControlMinder replaces the existing installation of CA ControlMinder and overwrites the existing CA ControlMinder configuration files and database.
- You must stop the existing installation of CA ControlMinder before you begin the new installation.

McAfee Entercept Buffer Overflow

The CA ControlMinder STOP feature is incompatible with the McAfee Entercept buffer overflow technology.

Turn off the CA ControlMinder STOP feature or the McAfee Entercept buffer overflow protection feature.

Short File Name Rules (8.3 Format) Are Not Supported

CA ControlMinder does not support rules created as short file names (8.3 format). When you define any of the following classes, you must enter the full path name of the file or directory:

FILE, PROGRAM, PROCESS, SECFILE, SPECIALPGM

The following is an example of a rule using a full path name:

```
nr file ("C:\program files\text.txt")
```

The following is an example of a rule using a short path name that is *not* supported:

```
nr file ("C:\progra~1\test.txt")
```

UNIX Endpoint Limitations

This section describes feature support limitations for UNIX endpoints.

HP-UX Feature Support Limitations

The following is a known UNAB and CA ControlMinder limitation on HP-UX operating systems:

- seversion utility does not display SHA-1 signature.

Unicenter Integration is Not Supported on HP-UX Itanium and RHEL Itanium

Unicenter integration is not supported on HP-UX Itanium (IA64) and Red Hat Linux Itanium IA64.

SAM Agent Are Not Supported on Linux IA64

The SAM Agent is not supported on Linux Itanium (IA64). CA ControlMinder does not install the SAM Agent on these operating systems regardless of the selections you make during installation.

Note: UNAB is also not supported on Linux IA64.

SAN Support

CA ControlMinder supports a SAN (storage area network) environment when you install CA ControlMinder on a local file system and use it to protect files on a SAN, when the SAN is accessible from the single host where CA ControlMinder is installed.

Note: If the SAN is accessible from multiple hosts, install CA ControlMinder on each host that can access the SAN and use each installation to protect files on the SAN.

If the SAN is accessible from multiple hosts and CA ControlMinder is installed on the SAN, and you want to install CA ControlMinder from a different host to the same location on the SAN, consider the following before you begin:

- The new installation of CA ControlMinder replaces the existing installation of CA ControlMinder and overwrites the existing CA ControlMinder configuration files and database.
- You must stop the existing installation of CA ControlMinder before you begin the new installation.

Note: CA ControlMinder behavior is unspecified when you install it on a SAN and it is executed from multiple connected hosts.

UNAB Limitations

This section describes feature support limitations for UNAB endpoints.

Account Password Format in a One-Way Trust Domain Environment

When you change your Active Directory account password in a different domain than the registration domain using the uxconsole utility, you must use the following command format:

```
uxconsole -krb -passwd user@DOMAIN
```

Important! the domain name must appear in capital letters.

UNAB Not Supported on Linux IA64

Currently, you cannot install UNAB on Linux IA64 operating system.

UNAB is not FIPS140-2 and IPV6 Compliant

Currently, UNAB is not FIPS140-2 and IPV6 compliant.

SAM Limitations

This section describes feature support limitations for SAM endpoints and server components.

SAM Is Not FIPS140-2 and IPV6 Compliant

Currently, SAM is not FIPS140-2 and IPV6 compliant.

Chapter 7: Installation Considerations

This section contains the following topics:

Supported Installation Languages

You can specify the language in which the Enterprise Management Server and CA ControlMinder are installed. The following language IDs are supported, you can specify and their respective languages:

The Enterprise Management Server supports the following languages:

- 1033—English
- 1041—Japanese
- 1042—Korean
- 2052—Chinese(Simplified)
- 1031—German
- 1040—Italian
- 1036—French
- 1046—Portuguese(Brazilian)
- 1034—Spanish

  Note: You can generate CA ControlMinder reports in English, Japanese and Korean only.

CA ControlMinder for Windows, CA ControlMinder for UNIX and UNAB support the following languages:

- 1033—English
- 1041—Japanese
- 1042—Korean
- 2052—Chinese(Simplified)

Windows Endpoint Installation Considerations

This section describes items you should consider when installing CA ControlMinder on Windows endpoints.

Restart Message Pops Up During Installation, Uninstallation or Upgrade on Windows Server 2008

When you install, uninstall or upgrade CA ControlMinder on Windows Server 2008, a dialog box may appear informing you that a restart is required after the process is complete. To continue, close the dialog box by selecting OK.

UNIX Endpoint Installation Considerations

This section describes items you should consider when installing CA ControlMinder on UNIX endpoints.

AIX 6.1 Requires TL3 or Later for CA ControlMinder to Start

Valid on AIX 6.1

To load CA ControlMinder on AIX 6.1, verify that TL3 or later is installed.

Message Queue for Linux390 Requires J2SE Version 5.0

To use Message Queue functionality on Linux s390 and s390x endpoints, verify that J2SE version 5.0 or later is installed on the endpoint. Message Queue functionality lets you send report data to the Report Portal and audit data to CA User Activity Reporting Module.

Note: You may need to configure the java_home configuration setting in the accommon.ini file. For more information, see the *Implementation Guide*.

Compatibility Library Missing on x86_64bit Linux

By default x86_64 Linux operating systems should not include 32bit compatibility libraries when installed. CA ControlMinder endpoint requires that the library libstdc++.so.6 exists under the usr/lib directory from rpm libstdc++.

Verify that this library exists on the endpoint before you install CA ControlMinder.

CA ControlMinder Installation and Uninstallation Restarts UNAB

When CA ControlMinder is installed or uninstalled from an endpoint that UNAB is running on, the UNAB agent, uxauthd, is stopped and started.

Propagating CA ControlMinder and UNAB to a New Solaris Zone

When you setup a new Solaris zone, you must complete several post installation steps before the native operating system completely propagate and run the post installation part of the package and you can propagate CA ControlMinder and UNAB to the new zone.

Note: For more information on setting up a new zone correctly, see Sun's System Administration Guide: Solaris Containers--Resource Management and Solaris Zones, which is available at the Sun Microsystems Documentation website.

Installing CA ControlMinder on Solaris 11 Limitation

Due to a Solaris 11 limitation, CA ControlMinder package is not propagated into nonglobal zones during installation. We recommend you to install CA ControlMinder in each zone individually using the Solaris native packaging tool (pkgadd).

CA ControlMinder on RHEL 7x86_64 Considerations

When you install CA ControlMinder on the RHEL 7x86_64 endpoint, the following limitations are applicable:

- RHEL 7x86_64 supports CA ControlMinder 64-bit installation only.
- When you start the CA ControlMinder services, the system generates the following messages. You can locate the messages at /var/log/messages.

  ```
  seos: module license 'Proprietary' taints kernel
  Disabling lock debugging due to kernel taint
  seos: module verification failed: signature and/or required key
  missing - tainting kernel
  ```

  Note: The system messages are normal and cause no problem.
- CA ControlMinder fails to detect users using Telnet, when you set the loginflags(PAMLogin) property for the LOGINAPPL record.
- The serevu utility fails to disable a user login using Telnet, when the failed login count exceeds the configured maximum value. However, the serevu utility behaves correctly for the SSH logins.
- When CA ControlMinder denies an incoming Telnet connection, the system Telnet service can transition to the failed state. When the Telnet service fails, restart the Telnet service.

UNAB Endpoint Installation Considerations

This section describes items you should consider when installing UNAB endpoints.

UNAB for Linux 390 Requires J2SE Version 5.0 for Remote Management

To remotely manage Linux s390 and s390x endpoints, verify that J2SE version 5.0 or later is installed on the endpoint. Remote management lets you use CA ControlMinder Enterprise Management to manage UNAB endpoints.

Note: You may need to configure the java_home configuration setting in the accommon.ini file. For more information, see the *Implementation Guide*.

Server Component Installation Considerations

This section describes items you should consider when installing server components (the Enterprise Management Server, CA ControlMinder Endpoint Management, and Enterprise Reporting).

Required 32-bit Packages for Installing Enterprise Management Server on Red Hat Linux 6

Valid on Red Hat Linux 6

Before you install the Enterprise Management Server on Red Hat Linux 6:

1. Verify that the minimum hardware requirement of 4 GB RAM and 4 GB swap space is available.
2. Install the following packages:
   `audit-libs, compat-libstdc++, glibc, libgcc, libSM, libXext, LibXp, LibXt, ncurses, pam, libstdc++, Ksh, dos2unix`

Note: Use the rpm --requires and the rpm --whatprovides commands to verify package dependencies, and install missing packages.

rpm --requires—Detect Library Dependencies

When installing Enterprise Management on Linux, you want to know on which libraries the CAeAC package depends.

The command uses the following syntax:

```
rpm -qp --requires package
```

The command has the following parameters:

-q

Specifies that you want to query RPM package information.

-p

Query a RPM package file. Also retrieves information on packages that are not installed.

--requires *package*

Retrieves the dependencies that are required by the package.

Example

You want to retrieve dependency information on CA ControlMinder 12.8 SP0.

```
root> rpm -qp --requires CAeAC-1280-0.0.1275.i386.rpm
rpm >= 4.0
libcrypt.so.1
libc.so.6
libdl.so.2
libgcc_s.so.1
libm.so.6
libnsl.so.1
libpam.so.0
libpthread.so.0
libresolv.so.2
libstdc++.so.6
rpmlib(PayloadFilesHavePrefix) <= 4.0-1
rpmlib(CompressedFileNames) <= 3.0.4-1
```

Continue running the rpm command on the listed packages one by one to retrieve further dependencies.

```
root> rpm -qp --requires libcrypt
```

More information:

rpm --whatprovides—Verify That a Library Exists (see page 46)

rpm --whatprovides—Verify That a Library Exists

Before installing Enterprise Management on Linux, verify that all required libraries are present on the target system.

The command uses the following syntax:

```
rpm -q --whatprovides capability
```

The command has the following parameters:

-q

Specifies that you want to query RPM package information.

--whatprovides *capability*

Specifies that you want to retrieve information which packages provide the capability.

Example: Verify that a library is installed

In this example, you want to verify that libcrypt.so.1 is installed. You receive a positive answer ($? is 0) and you learn that its is the glibc-2.5-42 package that provides libcrypt.so.1.

```
root> rpm -q --whatprovides libcrypt.so.1
glibc-2.5-42
root> echo $?
0
```

Example: Detect that a library is not installed

In this example, you want to find out whether libexample.so.1 is installed. You receive a negative answer ($? is 1), because no package is installed that provides this capability.

```
root> rpm -q --whatprovides libexample.so.1
no package provides libexample.so.1
root> echo $?
1
```

If a required library is missing, install it before proceeding the installation.

More information:

rpm --requires—Detect Library Dependencies (see page 45)

Libc Library Missing When Installing CA ControlMinder on Linux

Symptom:

When installing CA ControlMinder using a native Linux package, it fails with the following error message.:

```
Binary file cannot be executed
Reason: The platform does not match or some necessary libraries are missing.
Action: Please check that the correct system libraries are used (libc).
```

Solution:

The CA ControlMinder installation on Linux requires a 32-bit libc library to be installed and configured in libpath, independent of the system architecture. If your Linux system is a 64-bit minimal installation with no 32-bit version of libc, the installation fails.

Install the 32-bit version of libc, and rerun the installation.

Does Not Support RDP Hardening

CA ControlMinder does not support an RDP Hardening server component configuration. If a deployed hardening policy that includes the “Always prompt for password” option is selected, PUPM automatic login does not work.

Install Primary and Load Balancing Enterprise Management Server on Same Time Zone

When configuring Enterprise Management Server for high availability, verify that both the primary and the load balancing servers are installed on the same time zone.

Installing Endpoint Management on 64-bit Linux

To install Endpoint Management on a 64-bit Linux server, install CA ControlMinder Endpoint Management 32-bit version. The 32-bit version is required as Endpoint Management installs a 32-bit web service.

Special Characters in Administrator Name

Valid on Windows

The administrative account user name must not include any special characters. For example: '-' character.

Supported JDK and JBoss Versions

You can find supported JDK and JBoss versions on the CA ControlMinder Third Party Components DVDs.

Prerequisite Kit Installer Considerations

When using the Prerequisite Kit installer utility to install CA ControlMinder Enterprise Management from the media, after you are prompted to insert the CA ControlMinder Enterprise Management DVD, you must select Done to continue. You may also need to close the ProductExplorer window that appears when you insert the DVD.

Superuser Account Required for Server Components Installations

To install any of the CA ControlMinder server components (such as Endpoint Management and Enterprise Management), you must log in as the superuser (root on UNIX or a member of the Administrators group on Windows).

RDBMS Connection Fails During Installation if Java Cannot Be Found

During CA ControlMinder Enterprise Management installation, when it tries to connect to the RDBMS, a connection failure may suggest that java.exe cannot be located.

Make sure that the full pathname to java.exe is in the system's PATH environment variable.

Enterprise Management Server Installation Does Not Support Spaces in Installation Path

Valid on UNIX

Do not enter spaces in the installation path when you install the Enterprise Management Server.

Set Up CA ControlMinder Enterprise Management to Work with Active Directory on Another Domain

If you want to work with an Active Directory that is located outside of the domain that you installed CA ControlMinder Enterprise Management on, you must change the host TCP/IP settings.

To set up CA ControlMinder Enterprise Management to work with Active Directory on another domain

On Windows

1. Click Start, Control Panel, Network Connections.

   The Network Connections window appears.

2. Right-click the active network connection and click Properties.

   The Connection Properties dialog appears with the General tab open.

3. Select Internet Protocol (TCP/IP) and click Properties

   The Internet Protocol (TCP/IP) Properties General tab appears.

4. Click Advanced and click the DNS tab in the open dialog.

   The Advanced TCP/IP Settings DNS tab appears.

5. Click Add and enter the IP address of the DNS server of the domain that Active Directory is located on.

6. Select Append these DNS suffices (in order) and click Add to add a suffix.

   The TCP/IP Domain Suffix dialog appears.

7. Enter the domain suffix.

   Example: *company.com*

8. Click OK on all open dialogs to confirm your changes and exit.

On UNIX

Verify that the DNS server name of the domain that Active Directory is located on is set to the correct value.

To verify that the DNS domain name, open the file /etc/resolv.conf and verify that the domain is set to the correct value.

CA ControlMinder Endpoint Management Installation Instructions Refer to Both Editions of CA ControlMinder

The CA ControlMinder Endpoint Management installation instructions that are documented in the Installing CA ControlMinder Endpoint Management chapter of the Implementation Guide apply to both CA ControlMinder and CA ControlMinder. Non-CA ControlMinder users that want to install CA ControlMinder Endpoint Management should follow these instructions and use the non-Premium Server DVD.

CA ControlMinder Endpoint Management Shortcut Points to Port Number 8080

By default, the CA ControlMinder Endpoint Management installer sets the shortcut to port number 8080. To change the default settings, you must run the CA ControlMinder Endpoint Management installer directly from the CA ControlMinder DVD and not from the ProductExplorer.

Use the following command line to define the port to use when installing CA ControlMinder Endpoint Management:

```
install_EM.exe -DJBOSS_PORT=<18080>
```

Alternatively, you can edit the CA ControlMinder Endpoint Management shortcut to point to a different port after the installation.

CA User Activity Reporting Module Supports Only Trusted SSL Connection

When defining the connection settings of the CA User Activity Reporting Module server, define the SSL connection settings. CA User Activity Reporting Module does not support non-SSL connection.

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

Special Subscription Needed to View CA User Activity Reporting Module Reports from CA ControlMinder Enterprise Management

To use view CA User Activity Reporting Module reports from the CA ControlMinder Enterprise Management interface, apply a special subscription update to your CA User Activity Reporting Module server.

To apply the subscription update

1. In CA User Activity Reporting Module, click the Administration tab, the Services subtab, and select the Subscription Module.
2. Provide the following RSS feed URL:

   ```
   http://securityupdates.ca.com/CA-ELM/r12/OpenAPI/RSSFeed.xml
   ```
3. Download and apply all of the modules to CA User Activity Reporting Module.

   You can now view CA User Activity Reporting Module reports from CA ControlMinder Enterprise Management.

Synchronize the System Time of the CA ControlMinder Enterprise Management and Report Portal Computers

If you install the Report Portal on a separate computer to CA ControlMinder Enterprise Management, you must synchronize the system time of the computers. If you do not synchronize the system times, reports that CA ControlMinder Enterprise Management generates will remain in a pending or recurring status.

Uninstall Fails if You Are Not the Superuser

To uninstall any of the CA ControlMinder server components (such as Endpoint Management and Enterprise Management), you must log in as the superuser (root on UNIX or Administrator on Windows). If you are not logged in as the superuser, the uninstall fails.

Chapter 8: Upgrade Considerations

This section contains the following topics:

Versions You Can Upgrade From

You can upgrade your CA ControlMinder endpoints to 12.8 from the following versions:

- 12.7
- 12.6.02
- 12.6.01
- 12.6
- 12.5.5
- 12.5 SP4
- 12.5 SP3

You cannot upgrade your CA ControlMinder endpoints to 12.8 from the following versions:

- 8.0 SP1 GA

  To upgrade an 8.0 SP1 GA endpoint, install the latest CR for 8.0 SP1 before you upgrade to 12.8.

- 5.2 and 5.3

  To upgrade an 5.2 or 5.3 endpoint, install the latest CR for 8 SP1 before you upgrade to 12.8.

Windows Endpoint Upgrade Considerations

This section describes items you should consider when upgrading CA ControlMinder on Windows endpoints.

Change in Default Access to Database

The default access to seosdb, the CA ControlMinder database, is now none. In r12.5 SP2 and earlier, the default access to the database was read.

Note: CA ControlMinder internal processes have full access to the database and the NT AUTHORITY\System user has read access to the database.

UNIX Endpoint Upgrade Considerations

This section describes items you should consider when upgrading CA ControlMinder on UNIX endpoints.

Default Installation Location

The default installation location has changed in r12.0 and is as follows:

```
/opt/CA/AccessControl
```

FIPS 140-2 Library Upgrade

This release of CA ControlMinder uses CAPKI 4.1.2 instead of ETPKI 3.2. The upgrade is automatic and keeps the ETPKI 3.2 libraries on your computer if they are used by other components. To determine whether other components are using ETPKI 3.2, CAPKI uses an internal reference count. When this count equals 0, ETPKI 3.2 uninstalls on upgrade.

Systemwide Audit Mode for UNIX Upgrades

The SYSTEM_AAUDIT_MODE property in the SEOS class specifies the default audit mode for users and enterprise users (systemwide audit mode). When you upgrade to CA ControlMinder r12.5 SP1 or later, CA ControlMinder sets the value of the SYSTEM_AAUDIT_MODE property to the value of the DefaultAudit configuration setting in the [newusr] section of the lang.ini file.

Note: The default value of both the SYSTEM_AAUDIT_MODE property and the DefaultAudit configuration setting is Failure LoginSuccess LoginFailure.

Authorization Recognizes Resource Group Ownership

CA ControlMinder takes into account resource group ownership when checking user authorization to a resource. This behavior was introduced in r12.0. In earlier releases, the authorization process considered only the resource's owner.

For example, you define a FILE resource with a default access of none and no owner that is a member to a GFILE resource with a named owner. In CA ControlMinder r12.0 and later, the named group owner has full access to the file. In earlier releases, nobody has access to the file.

syslog Messages That Have a Reduced Priority

The following syslog messages have been reduced to informational priority (INFO rather than ERROR):

- CA ControlMinder daemon going down.
- START-UP: CA ControlMinder PID=%d
- SEOS_load: use_streams=$use_streams unload_enable=$unload_enable
- Loading CA ControlMinder kernel extension.
- $prodname kernel extension is already loaded.
- Starting $SeosBinDir/seosd daemon. (CA ControlMinder)
- Watchdog started.
- Watchdog initialized Watchdog extensions.

Server Component Upgrade Considerations

This section describes items you should consider when upgrading server components (the Enterprise Management Server, CA ControlMinder Endpoint Management, and Enterprise Reporting).

Required Hot Fixes Before Upgrade on Linux

Valid on Linux

Symptom:

After I upgraded the Enterprise Management Server on Linux, I noticed that the effective and assigned policies on the HNODE objects were not upgraded and that commands was missing.

Solution:

During upgrade of the DMS or DH databases the procedure exports the current database (using 'dbmgr -export') into a selang command file which is then imported by the new version.

Due to a defect that was introduced in a previous fix the assigned and effective policies on the HNODE objects (in the case there is more than one policy assigned to the HNODE) are not exported. The result is information loss and the new database is not updated properly during upgrade.

To resolve the issue you must be apply the corresponding hot fixes before before you upgrade to CA ControlMinder 12.8:

- CA ControlMinder 12.7: RO65652
- CA ControlMinder 12.6SP1:RO65612
- CA ControlMinder 12.6: RO65615
- CA ControlMinder 12.5SP5 :RO65774
- CA ControlMinder 12.5SP4: RO65611

You can find the hot fixes in the following link.

12.8 Enterprise Management Server Requires 12.8 Distribution Servers

If you upgrade the Enterprise Management server to 12.8, you must also upgrade its Distribution Servers to 12.8.

Enterprise Management UI Login Fails When Upgrading from CA ControlMinder 12.6SP1 or lower.

Symptom:

When I upgrade from CA ControlMinder 12.6SP1 or lower to 12.7 or higher, I am not able to log in to the Enterprise Management UI.

Solution:

Update the server.xml file in JBOSS (<<jboss-4.2.3.GA>>\server\default\deploy\jboss-web.deployer) to enable the Enterprise Management UI login. Set the emptysessionpath attribute to True for all connector entries.

Requirements for Upgrading from 12.6 to 12.8

In case your Enterprise Management environment includes Distribution Server hosts, perform the following steps before upgrading to release 12.8:

Follow these steps:

1. Log in to the Enterprise Management database.
2. Browse to table the named ENDPOINT.
3. Look into the FRIENDLY_NAME column and verify that the Distribution Server host name is not duplicated.

   If the host name is duplicated, delete one of the two rows.

Enterprise Management Server Upgrade Fails to Preserve Tasks Assigned to the Built-in Roles

When you upgrade the Enterprise Management Server, the upgrade fails to preserve the tasks that you assign to the built-in roles. With an upgrade, you can preserve the configurations of the custom roles, and only the membership policies of the built-in roles.

CA ControlMinder r12.6.01 Requires Hot Fix to Manage Policy Models on CA ControlMinder r12.5 and r12.0.01

If you are using CA ControlMinder 12.7 Server to manage policy models on CA ControlMinder r12.5 or r12.0.01 endpoints, then install the following hot fixes:

- For r12.5 endpoint, install hot fix T537526
- For r12.0.01 endpoint, install hot fix T537569

Note: For more information, contact CA Support at http://ca.com/support.

Software Patch Required to Deploy Policies on Endpoints

To deploy policies on CA ControlMinder r12.5 endpoints from CA ControlMinder Enterprise Management r12.6, you must install patch T537526 on the Enterprise Management Server.

Download the software patch from the CA Support website.

Chapter 9: General Considerations

This section contains the following topics:

Windows Endpoint Considerations

This section describes items you should consider when using CA ControlMinder on Windows endpoints.

The WINSERVICE Class is not Support on Microsoft Windows Server 2012

Applies to Windows Server 2012

The WINSERVICE class is not supported on Microsoft Windows Server 2012.

RunAs Administrator to Start CA ControlMinder on Windows Server 2008

Valid on Windows Server 2008

To start CA ControlMinder using the command line options (seosd -start), you must have administrator privileges if the User Account Control (UAC) option is enabled. Run the command prompt using the RunAs option and specify a user account with administrative privileges.

Uninstall Does Not Remove CA License Files

When you uninstall CA ControlMinder, the CA License files are not deleted. By default, the CA License files are in the CA_license directory (for example, C:\Program Files\CA\SharedComponents\CA_LIC).

UNAB Considerations

This section describes items you should consider when using UNAB.

Home Directory Not Created on Log In When SELinux is Enabled

Valid on Linux

Symptom:

When I log in to a Linux host using an SSH client the home directory for my account is not created when SELinux is enabled.

Solution:

The home directory is not created when attempting to log in using an SSH client. To work around this problem do the following:

1. Open the password-auth file. This file is located in the following directory by default:

   ```
   \etc\pam.d\
   ```

2. Locate the session section.
3. Add the following line before the pam_uxauth section:

   ```
   session required pam_makehomedir.so
   ```

4. Save and close the file.

Change Password Attempt Fails on Red Hat Linux

Valid on Red Hat Linux

Symptom:

When asked to change my password I cannot continue to work on the host after the password change processes completed. The problem occurs when I log in using an SSH client or Telnet.

Solution:

To overcome the problem change the account password, log out of the host and log in with the new password.

Disable Local User Account After Migration

After fully migrating user accounts to Active Directory, you can disable the local UNIX account by adding an asterisk (*) at the beginning of the account entry in the /etc/passwd file.

Do Not Set the unab_refresh_interval Token Value to a Short Interval

To avoid performance issues in UNAB, do not set the value of the unab_refresh_interval token value to a short interval.

Do not Set Kerberos dns_lookup_realm to True

Valid for SSO mode

We recommend that unless required, do not set the Kerberos dns_lookup_realm value to true. When set to true, Kerberos initiates unnecessary DNS searches that can result in a substantial slowdown of UNAB login processing.

UNAB Users Cannot Change Account Password According to Specified Password Policy

If UNAB users cannot change their account passwords, verify that the Domain Controller security policy you use does not prohibit users from changing their account passwords.

sepass Integration with UNAB Endpoints

The sepass utility is integrated with UNAB. The integration lets users change their Active Directory passwords on endpoints on which both CA ControlMinder and UNAB are installed.

To integrate sepass with UNAB:

- Verify that you set the "change_pam" token value, in the seos.ini file, to **yes.** Configure this token to instruct sepass to change passwords using the PAM interface.
- Verify that you set the "auth_login" token value, in the seos.ini file, to **pam.** Configure this token to instruct sepass to validate existing passwords using the PAM interface.

Note: For more information about seos.ini initialization file tokens, see the *Reference Guide*.

Log In to UNAB with Active Directory Account

If you want to log in to UNAB with an Active Directory account that did not previously exist on the local host, follow these steps:

1. Register the UNAB host with Active Directory as follows:

   ```
   uxconsole -register
   ```

2. Activate UNAB as follows:

   ```
   uxconsole -activate
   ```

3. Create a UNAB login authorization (login policy) or local login policy (users.allow, users.deny, groups.allow, groups.deny) to enable Active Directory users to log in.

You Cannot Log In to CA ControlMinder for UNIX Using 'Administrator' Account When UNAB Is Installed

You cannot log in to a CA ControlMinder endpoint for UNIX with the 'Administrator' Active Directory user account if UNAB is installed on the endpoint. To work around this problem, you can create userPrincipleName for this account.

Server Components Considerations

This section describes items you should consider when using CA ControlMinder server components (CA ControlMinder Endpoint Management, CA ControlMinder Enterprise Management, and Enterprise Reporting).

Communication Issues between CA ControlMinder Components and CA ControlMinder Message Queue

The following CA ControlMinder components rely on communications with the CA ControlMinder Message Queue for some functionality:

- Enterprise Management Server
- Report Agent
- DMS
- DH
- UNAB
- SAM Password Consumers
- Agent Manager

These components may not be able to communicate with the Message Queue if it is not running, the configuration options are not set correctly for the Message Queue host or queue, or a generic network error is present.

If communication between any of these components and the Message Queue cannot be established or breaks down, the communication does not resume automatically when the problem is fixed. To work around this issue you must fix the communication issue and then restart the CA ControlMinder component.

Upgrade With Oracle

Before the upgrade is performed with an Oracle database, execute the following steps and run the noted commands on Oracle:

1. Open SQLPLUS from a command line
2. Connect to the database.
3. Log in as a system or sysdba user.
4. Run the following commands:
   ```
   GRANT EXECUTE ON SYS.DBMS_CRYPTO TO vpm20;
   GRANT UNLIMITED TABLESPACE TO vpm20;
   ALTER SYSTEM SET transactions=275 SCOPE=SPFILE;
   ALTER SYSTEM SET sessions=250 SCOPE=SPFILE;
   ALTER SYSTEM SET processes=200 SCOPE=SPFILE;
   ```

CA ControlMinder Host Name Limitation

The host name of the CA ControlMinder endpoint must be 15 characters or less. If the host name of the CA ControlMinder computer exceeds 15 characters, you cannot use CA ControlMinder Endpoint Management to log into the endpoint.

Automatic Generation of Policy Undeploy Script

When you undeploy a policy that does not have an associated undeploy script, CA ControlMinder automatically generates the required script to remove the policy. This script is based on the deployment script.

If you want to remove the policy but *keep* the policy rules (from the deployment script), provide an undeployment script with a rule that does not modify anything (for example, er GPOLICY *policyName*).

Specify the SAM Endpoint NETBIOS Name and Not the DNS Domain Name

When you create a SAM endpoint in CA ControlMinder Enterprise Management, the host name that you specify in the Name field must match the host name that appears in World View.

If the endpoint is an Active Directory endpoint, specify the NETBIOS domain name in the Host Domain field. If the endpoint is not an Active Directory endpoint, specify the NETBIOS host name in the Host Domain field, not the DNS domain name. For example, if an endpoint is not an Active Directory endpoint, specify the NETBIOS host name (ACSERVER) in the Host Domain field and not the endpoint DNS domain name (acserver.company.com).

If you specify the DNS domain name, advanced features, such as SAM Automatic Login, fail.

Using the Login Application Script to log on to a Member of a Domain

Symptom:

When I log in to a server that is a member of a domain using the CA ControlMinder Endpoint Management login application script, I can log in to FTP but the FTP user command indicates “Not connected”.

Solution:

FTP and PuTTY do not support domain users. You cannot use the automatic login application script to enable FTP and PuTTY automatic user logins to a server that is a domain member. To check out a password to log in to a domain member server using FTP or PuTTY, create a new automatic login script.

Follow these steps:

1. Locate the FTP or PuTTY script on the server.
2. Copy the FTP or PuTTY script.
3. Create another login application script that is based on the existing script.
4. Modify the script with the full user name and domain attributes as follows:

   ```
   userName = "#userName#"

   userDomain = "#userDomain#"

   password = "#password#"

   serverName = "#host#"

   fullUserName = userDomain & "\" & username

   Set pupmObj = CreateObject("ACLauncher.ACWebLauncher")

   hwnd = pupmObj.LaunchePUTTY(serverName, fullUserName, password)
   ```

5. Assign the new login application to the endpoint.

For more information on the automatic login application script, see The SAM Automatic Login Application Visual Basic Script.

You Cannot Configure More Than a Single CA IdentityMinder Provisioning Connector Server

Do not configure more than a single CA IdentityMinder provisioning connector server in CA ControlMinder Enterprise Management.

Cannot Configure CA IdentityMinder Provisioning Connector Server Using SSL Port

When you configure an CA IdentityMinder provisioning connector server, do not specify the CA IdentityMinder provisioning server SSL port (20390). If you specify the connector server SSL port, the connection to the connector server fails.

Cannot Use SAM to Change Password for the Expert Account

If you use a Check Point firewall on an SSH endpoint, you cannot use SAM to change the password for the expert account on the endpoint. This restriction means that the expert account must be a disconnected account in SAM.

SQLCMD Utility Does Not Support Blank Passwords

Valid on SQL Server

The SQL Server command utility sqlcmd does not support blank passwords. If you defined the SQL Server endpoint as a password consumer in CA ControlMinder Enterprise Management and check out a password from SAM, do not leave the password field empty. You can specify the account password or any other string as the password.

Oracle11g Server Certificate Required

To connect to an Oracle 11g server using auto login with ORACLE_11G_WEB.vbs, you must install a server certificate on the endpoint.

Note: To connect to the server without SSL, remove the SSL restriction from the Oracle server.

Special Characters in Installation Directory Paths

Special characters are not supported in the product installation directory paths.

Chapter 10: Known Issues

This section contains the following topics:

Installation Known Issues

This section describes installation known issues for CA ControlMinder components.

Windows Endpoint Installation Known Issues

This section describes installation known issues for Windows endpoints.

"No Valid Source Could Be Found" Message When Installing From MSI File

A "no valid source could be found" message appears when you upgrade CA ControlMinder. The message appears if the media that you currently use and the media that was originally used to install CA ControlMinder have the MSI file at different paths.

To work around this issue, add a registry string named "MediaPackage" and specify the relative path to the CA ControlMinder msi package. Add the registry string in the following path:

```
HKLM\Software\Classes\Installer\Products\
CDAFB228040EC5F40AA08B5E852A6D61\SourceList\Media
```

For example, if you install CA ControlMinder on a 32-bit Windows operating system, the full path to the msi file is: E:\x86\, where E: is the removable media drive. In the MediaPackage value you specify the value: \x86\

UNIX Endpoint Installation Known Issues

This section describes installation known issues for UNIX endpoints.

RPM Package Verification May Return Errors

When verifying RPM package installations you may receive some verification errors.

These errors do not indicate that there are issues with the functionality of the installed product and you can safely ignore them.

Client-Server Communication Mode Incompatibility

A client set up with non_ssl or all_modes cannot communicate with a server set up with fips_only communication mode.

API Libraries for Linux Z-series Are 32-bit

The API libraries that CA ControlMinder supplies for Linux Z-series (s390x) are 32-bit.

CA ControlMinder does not supply 64-bit libraries for Linux Z-series (s390x).

HP-UX requires an Updated Patch Level

On HP-UX, CA ControlMinder requires an updated patch level to install properly. We recommend the following OS patches:

- 11.23 on IA64—Patch PHSS_37492 or OS QPK1123 Bundle that is dated September 2006 or later.
- 11.11 on PA-RISC—OS Path with support for "dld_getenv" or OS QPR Bundle dates December 2006 or later.
- 11.23 on PA-RISC—OS QPK Bundle that is dated December 2006 or later.

PAM Does Not Work on Linux s390x with Older /lib64/libc.so.6 Library

PAM on Linux s390 and s390x does not work if the /lib64/libc.so.6 library on the host is older than the version CA ControlMinder PAM library was compiled with.

The library version should be 2.3.2 or later.

UNAB Endpoint Installation Known Issues

This section describes installation known issues for UNAB endpoints.

UNAB Restarts Twice When Installing CA ControlMinder

Valid on IBM AIX

When installing CA ControlMinder on IBM AIX and UNAB is already running, UNAB restarts twice. This behavior is because AIX performs additional Kernel checks.

Uninstalling Fails When Native Installation Is Customized to Install CA ControlMinder and UNAB in The Same Non-Default Location [UNAB]

Valid on AIX, and HP-UX

Symptom:

Uninstalling UNAB fails after I installed CA ControlMinder and UNAB using native installation and customized the installation directory to the same path on a nondefault location.

Solution:

Uninstalling CA ControlMinder corrupts and fails the UNAB installation. Uninstalling fails as both CA ControlMinder and UNAB are installed on the same directory. While customizing native installation to a nondefault destination folder, we recommend that you concatenate the product name (uxauth or UNAB) to the destination path.

UNAB Does Not Support CA ControlMinder r8.0 SP1 and r12.0 SP1

Currently, you cannot install UNAB on CA ControlMinder r8.0 SP1 and r12.0 SP1 endpoints. Also, UNAB and CA ControlMinder must be of identical version or service pack.

Upgrade Known Issues

This section describes upgrade known issues for CA ControlMinder components.

Windows Endpoint Upgrade Known Issues

This section describes upgrade known issues for Windows endpoints.

"Insufficient Privileges to Modify File" Message Appears During Upgrade

If you upgrade a CA ControlMinder endpoint and a message appears that informs you that the installer has insufficient privileges to modify a file, acknowledge the message and continue with the upgrade.

UNIX Endpoint Upgrade Known Issues

This section describes upgrade known issues for UNIX endpoints.

Pre-r12.0 Versions Must Use a Maximum of 54 Characters for the Encryption Key

If your environment includes versions of CA ControlMinder earlier than r12.0, you must use a maximum of 54 characters for the encryption key.

General Known Issues

This section describes general known issues for CA ControlMinder components.

Windows Endpoint Known Issues

This section describes known issues for CA ControlMinder for Windows.

"CA Access Control for ActiveX" Appears in Add/Remove Programs

Valid on Windows

Symptom:

The following application appears in the Add/Remove Programs list:

```
CA Access Control for ActiveX
```

Solution:

This application belongs to CA ControlMinder, don't remove it.

General Tab on Endpoint Creation Screen Loses Information

Symptom:

On the Endpoint creation screen's General tab, I fill in the endpoint name, host, account name, and password. On the Information tab, I choose the owner or select administrative accounts. When I return to the General tab, the data I had already entered is lost.

Solution:

Click Submit on the General tab before filling in the Information tab.

Uninstall Does not Remove the Data and Log Directories

Valid on Windows

Symptom:

After I removed CA ControlMinder from the system I noticed that the uninstall process did not remove Data and Log directories from the following path:

```
\ProgramFiles\CA\AccessControl\
```

Solution:

The uninstallation process does not remove the Data and Log directories. You can manually remove them after the processes completed.

Microsoft Internet Explorer 7.0 Compatibility Issues with CA ControlMinder

Due to compatibility issues of Microsoft Internet Explorer 7.0 with CA ControlMinder, the browser may stop responding. To work around the issue, Install Microsoft Internet Explorer 8.0 or do the following:

Important! Apply Microsoft software patch KB957388 before you begin this procedure. You can download the software patch from the Microsoft web site.

1. Stop all CA ControlMinder services.
2. Open a command line window and run the following command:

   ```
   net stop cainstrm
   ```
3. Open the regedit utility from the Run command line window.
4. Navigate to the following path:

   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSset\Services\cainstrm\parameters
   ```
5. Modify the ExcludeProcess registry entry value to include the iexplorer.exe file.
6. From the command line window, run the following command:

   ```
   net start cainstrm
   ```
7. Start the CA ControlMinder services.

Privileged Processes Can Save and Restore a Registry Tree Without Authorization

On Window Server 2003 and later, when a process obtains the special privileges SE_BACKUP_NAME and SE_RESTORE_NAME, it can save and restore a registry tree without CA ControlMinder authorization.

FIPS Only Mode on Windows x64

CAPKI 4.1.2 is now supported on x64 CA ControlMinder endpoint for Windows. However, due to a known issue with RSA, when running the CAPKI 4.1.2 in FIPS enabled mode, communication is significantly delayed.

Rename HOST Event in selang Marked as Unknown Event in CA User Activity Reporting Module Reports

A rename HOST event performed in selang is displayed as an unknown event in CA User Activity Reporting Module reports.

UNIX Endpoint Known Issues

This section describes known issues for CA ControlMinder for UNIX.

CAWIN Installation Requires Ncurses

Valid on Linux 64-bit Server

Install Ncurses 32-bit before installing CAWIN on Linux 64-bit servers.

Failed Login Events Not Audited When serevu Daemon Running

Valid on VMware vCenter 4.0 u2

When CA ControlMinder is installed on VMware vCenter version 4.0 u2, the following occurs when the serevu daemon is running:

- A LOGIN records for failed login events do not appear in audit file
- The pam_seos_failed_login.log file size is 0

To work around this issue, do the following:

1. Stop all CA ControlMinder daemons.
2. Navigate to the following directory:

   ```
   /etc/pam.d/
   ```

3. Edit the system-auth file to remove all references to pam_seos.so. For example:

   ```
   account required pam_per_user.so /etc/pam.d/login.map
   auth required pam_per_user.so /etc/pam.d/login.map
   password required pam_per_user.so /etc/pam.d/login.map
   session required pam_per_user.so /etc/pam.d/login.map
   ```

4. Edit the system-auth-generic file to add reference to pam_seos.so. For example:

   ```
   password  sufficient  pam_seos.so
   auth       optional     pam_seos.so
   account    optional     pam_seos.so
   session    optional     pam_seos.so
   ```

5. Edit the system-auth-local file to add references to pam_seos.so. For example:

   ```
   password  sufficient  pam_seos.so
   auth       optional     pam_seos.so
   account    optional     pam_seos.so
   session    optional     pam_seos.so
   ```

6. Save and close the files.
7. Start CA ControlMinder daemons.

Cannot Configure JBoss JDBC Password Consumer on Linux

Valid on Linux

Currently, you cannot configure a JBoss JDBC password consumer on LInux.

Log in to CA ControlMinder Requires PAM_Login Flag Enabled

Valid on AIX

If the PAM_login flag is not enabled, CA ControlMinder cannot detect the Active Directory user account correctly.

To work around this problem, enable the PAM_login flag in the log in program (LOGINAPPL) you set. Verify that seosd daemon accepts log in requests from PAM modules by setting the PamPassUserInfo token to 1 in seos.ini under the [pam_seos] section.

You can use the following command to set the login flags:

```
er LOGINAPPL SSH loginflags(pamlogin)
```

User Sessions Are Not Logged when Default Shell Is Not Defined in /etc/shells

Valid for Keyboard Logger

CA ControlMinder does not record user sessions when a user logs in with a shell that is not defined in /etc/shells.

When PAM is Active segrace Is Not Called for FTP and SSH Grace Login

When PAM is activated, segrace is not called automatically for a grace login to FTP and SSH services.

To work around this issue on FTP, change the value of the LOGINFLAGS property to nograce in the LOGINAPPL record for the FTP service.

To work around this issue on SSH, do not call segrace from PAM. Instead, call segrace from the user or operating system startup script.

CA ControlMinder Does Not Reset Passwords Once the Grace Period Expires

Valid on HPUX, and AIX

If UNAB is installed on the CA ControlMinder endpoint, CA ControlMinder PAM does not invoke the 'sepass' utility to reset the account password when the user password grace period expires.

This problem affects login applications that use loginflags(pamlogin), for example, SSH login, rlogin, FTP, and Telnet. SSH login is not recognized as a login action by CA ControlMinder on HPUX and AIX. To work around this problem, use loginflags(none) for SSH login applications.

Run the following command to set the token:

```
er LOGINAPPL SSH loginflags(none)
```

Solaris Network Event Bypass Does Not Work for Some Processes

CA ControlMinder on Solaris does not bypass network events (bypass type PBN of SPECIALPGM records) for processes that start before CA ControlMinder starts.

Stat Interception Calls Not Supported on AIX Systems

File access check on a stat system call with the STAT_intercept token set to “1” is not supported on AIX systems.

UNAB Known Issues

This section describes known issues for UNAB.

One-Way Trust Functionality Fails After UNAB Upgrade

Symptom:

After I upgraded UNAB from 12.6 ,12.6.1 or 12.6.2 to 12.8, the one-way trust functionality did not work.

Solution:

To resolve this issue, you must register UNAB with the one-way trust domain after you upgrade to 12.8.

UNAB Agent Lost Connection to Trusted Domain

Symptom:

The UNAB agent (uxauthd) lost connection to the trusted domain after I configured the domain security policy Kerberos service ticket lifetime to expire before the user ticket expires.

Solution:

Set the tgt_renew_lifetime token value the in uxauth.ini to less than the Kerberos service ticket maximum lifetime.

AD Users are Prompted Twice for Current Password on HP-UX

Valid on HP-UX IA64

To change a password, Active Directory users are prompted for and must provide the current password twice instead of once.

Failed Login Attempt of Mapped Users to AIX Not Logged

Valid on AIX

Symptom:

When I try to login to an AIX UNIX host using SSH as a mapped user the failed attempt is not logged by uxaudit.

Solution:

Seaudit does not log the first failed log in attempt of a mapped user if the user entered an incorrect password. Subsequent login attempts are logged by uxaudit..

Password Change at Next Login Fails on HP-UX

Valid on HP-UX

In Active Directory I selected the "User must change password at next login" option. When I use SSH or Telnet to login, users cannot login or change the password.

PAM Configuration Changes Blocks Users Login

Valid on Red Hat Linux 5.0 and up

Symptom:

I installed UNAB and CA ControlMinder on a Red Hat Linux and configured the PAM configuration files to use the "value=action" syntax in the control field. When I attempt to log in to a Linux host, the log in action is denied.

Solution:

UNAB does not support the "value=action" syntax of the control field in the PAM configuration files.

Incorrect User ID Displayed After Un-registering UNAB in a One-Way Trust Domain Environment

After un-registering UNAB from Active Directory in a one-way trust domain environment user ID details from the one-way trusted domain are displayed even though they should not appear.

Trusted User SSH Login Failed on AIX

Symptom:

I tried to log in to an AIX 5.3 endpoint using SSH, however the login attempt failed.

Solution:

This error is a known IBM issue with several combinations of AIX and SSH versions. The issue has been logged with IBM development as APAR (Authorized Program Analysis Report) number IV10231.

uxauthd Starts Even When watchdog_enabled Token is Set to No

Symptom:

When I set the token watchdog_enabled to no and restart UNAB, uxauthd starts.

Solution:

The watchdog script ignores changes made to the watchdog_enabled token after starting uxauthd for the first time. We recommend you to specify *-n* during the registration process, make changes to the token, and start uxauthd.sh script separately.

Audit Log Records Login With Local Account Password As Attempt Login

Symptom:

When I log in to UNAB and my user account is present in the local password file and the Active Directory, the audit log shows the following record:

```
<audit_record_date_and_time> A LOGIN map3
```

Solution:

This is a known issue with UNAB. The audit log records A LOGIN instead of P LOGIN.

Rlogin Entries Logged Twice

Valid on Linux

If you log in to a host that has UNAB installed using rlogin, the login attempt appears in the audit twice.

Hot Fix for Microsoft Windows Server 2003 to Improve Performace

Valid on Windows Server 2003 SP1, Windows Server 2003 64 Bit

LDAP queries fails to return Active Directory queries results for extended search using LDAP_MATCHING_RULE_IN_CHAIN.

To workaround this issue, install the latest service pack for MIcrosoft Windows 2003 Server or disable the UNAB group update during log in by setting the wingrp_update_login token to no.

Note: For more information, see Microsoft Knowledge Base article 914828.

Uxpreinstall Utility Fails to Verify Host Name Resolution

The uxpreinstall utility fails to verify the host name resolution after you install UNAB and before you register with Active Directory.

To work around this problem, use the -d argument to specify the Active Directory domain name. For example:

```
./uxpreinstall -d domain_name
```

Telnet and rlogin Programs Not Displayed in Audit Records

Valid on Linux, HP-UX

The UNAB audit records do not display the telnet and rlogin login programs. In LInux, the UNAB audit records show "remote" instead of telnet or rlogin. On HP-UX the UNAB audit records show "login" instead of telnet or rlogin.

Interval between uxconsole -register and -deregister Commands

If you register then deregister a UNAB host in Active Directory, after you register the host, we recommend that you wait the time necessary for domain controller replication before you deregister the host.

Note: If you deregister a UNAB host, policies that were not distributed are deleted.

New Domain User Login May Fail on First Attempt

Valid for SSH

If you create a user in Active Directory and the new user immediately tries to log in to a UNAB endpoint, the first login attempt fails but subsequent login attempts succeed. The first login attempt fails because the user is not known to the endpoint. However, during the failed login process, uxauthd updates the local NSS storage with the user information. Subsequent login attempts succeed because the user is now known to the endpoint.

By default, uxauthd updates the user information in the NSS storage every hour. If the new user tries to log in to the endpoint after uxauthd updates the NSS storage, the login succeeds.

Login Services Bypass PAM on SSO Login

Several login services bypass PAM on SSO login. The login policy is not applied and audit events are not generated.

Successful Login to Host Generates an Error Message

Valid for Linux, AIX, HP-UX

A limitation in the UNIX PAM flow results in logging a successful login to a UNAB host as an error message, indicating that account authentication failed in the syslog file.

Password Mismatch Message When Changing Password Using sepass

Valid on AIX 5.3

A password mismatch error message appears when a mapped user attempts to change an account password using sepass. Regardless of the error message, the account password is changed on Active Directory.

Active Directory User Cannot Change Password on Solaris

Due to Sun Solaris password limitations, users that are logging in to the UNIX host with Active Directory account, cannot change their account password using Solaris passwd tool. If the user must change the account password on the first login, the user must login from a system other than Solaris.

If UNAB is running on the UNIX host, use the following command to change the local account password:

```
passwd -r files username
```

If CA ControlMinder is running on the UNIX host, use the sepass utility to change the local account password.

Impersonating an Active Directory User Does Not Create Audit Record

If you impersonate an Active Directory user using su, the impersonation attempt is not audited.

sshd Program Name Appears in Audit Records of SFTP Sessions

The audit records of login sessions done using sftp program can display the sshd daemon in the program field and not the sftp program.

UNAB Entries Contain Blank Fields in Event Viewer

UNAB events are displayed in the Windows Event Viewer with blank fields.

FTP SSO Login of Enterprise Users Not Audited

Valid for Solaris

Kerberized FTP and telnet programs bypass the PAM stack and therefore, UNAB does not audit FTP and telnet SSO logins of enterprise users.

Deregistering SSO Enabled UNAB Does Not Delete Records from Keytab File

When you deregister a UNAB host that was previously registered with SSO enabled, the computer object is removed from Active Directory, but the corresponding records are not deleted from the keytab file. If you attempt to register the UNAB host again, the Kerberos ticket is not created.

To overcome this problem, we recommend that you do not deregister UNAB hosts, or remove the keytab file if it is used by UNAB hosts only.

HP-UX Does Not Support @ Symbol in Passwords

Valid on HP-UX

Due to an HP-UX limitation, do not use the @ symbol in passwords on HP-UX endpoints.

HP-UX Does Not Support Fully Qualified Domain Name Login

Valid on HP-UX

You cannot log into a HP-UX host with a fully qualified domain name, for example: user@domain.

Server Components Known Issues

This section describes known issues for CA ControlMinder server components (CA ControlMinder Endpoint Management, CA ControlMinder Enterprise Management, and Enterprise Reporting).

Error Message Appears When Attempting to Check Out an Operation Administrator Account Password

Symptom:

When I check out an operation administrator account password of from an SSH endpoint type, the following message appear:

```
java.lang.Exception: too many results found for account
handle:ACCOUNT_HANDLE_NOT_INITIALIZED
```

Solution:

This is a known issue with the SAM feeder. The problem occur when you attempt to check out a connected operation administrator account password that you created using the feeder (ADMIN_ACCOUNT_IS_DISCONNECTED=false) when more than one operation administrator account is defined.

To workaround this issue, do the following:

- Run the SAM feeder polling task to create the SSH endpoint type and set the operation administrator accounts as disconnected (ADMIN_ACCOUNT_IS_DISCONNECTED=true).
- Run the SAM feeder polling for each of the operation administrator accounts and modify them to specify that the accounts originated for a disconnected system (DISCONNECTED_SYSTEM=false).

Error Messages Appear in JBoss Server Log File After Enterprise Management Server Installation

Symptom:

When I restart the Enterprise Management Server after installing the third-party components and the Enterprise Management Server, the server.log file shows the following errors:

- 593 ERROR
- 597 ERROR
- 604 ERROR
- 737 ERROR
- 229 ERROR
- 329 ERROR
- 805 ERROR

Solution:

This behavior is a known issue. Verify that CA ControlMinder services are started. The Enterprise Management requires that CA ControlMinder is running. If the JBoss Application Server services are not started, perform one of the following:

- (Windows) Click Start, Programs, CA, ControlMinder, Start Task Engine.

  Note: The Task Engine may take some time to load the first time you start it.
- (Windows) Start the JBoss Application Server service from the Services panel.
- (Linux) Enter ./JBOSS_HOME/bin/run.sh -b 0.0.0.0

Active Directory Users with Japanese Characters Cannot Be Disabled

Symptom:

When I disable an Active Directory user with Japanese characters in the CA ControlMinder Enterprise Management, the task fails. The user can still log in to the Enterprise Management Server.

Solution:

This behavior is a known issue.

Modify Password Consumer Event Action Appears as Unknown Action

Symptom:

When I modify a password consumer event and verify the action, it appears as Unknown Action.

Solution:

This behavior is a known issue.

Wrong Time Zone in SAM Password History

Symptom:

The privileged account password history change date is displayed in the time zone of the JBoss server, and not the time zone of the client that is running the web browser.

Solution:

None.

dbmgr -export Function Fails to Export Effective and Assigned Policies After Upgrade

Valid on Linux

Symptom:

After I upgraded the Enterprise Management Server, I cannot locate the assigned and effective policies on the hosts.

Solution:

During the Enterprise Management Server upgrade process, the installation uses the dbmgr -export function to export the existing policies to selang commands. Due to an error in the process, the installation did not import the policies back in to the database.

To fix this issue, install the following test fixes before you upgrade the Enterprise Management Server:

- For 12.7--T537745
- For 12.6.01--T537746
- For 12.5SP5--T537747
- For 12.5SP4-T537738

.NET Framework Error Message Displayed During Installation

During Installation of CA Enterprise Management, the following error message is displayed in the Add Roles and Features Wizard: "The following feature could not be installed: NET Framework3.5 (includes .NET2.0 and 3.0)"

Close the error message pop-up box and continue with the installation. This error message does not affect the server installation.

Privileged Account Requests and Daylight Savings Time (DST)

If either the Enterprise Management Server or the requester are in daylight savings time (DST), the following occurs when submitting a privileged account request:

- If the Enterprise Management Sever *is* in daylight savings time and the requester is not then the requested time period is one hour later than in the original request.
- If the Enterprise Management Server *is not* in daylight savings time and the requester is in daylight savings time then the requested period is one hour earlier than in the original request.

Uninstall Does Not Delete JBoss and JDK Files

Symptom:

Following an Endpoint Management uninstall of a nondefault drive installation, all JBoss and JDK files are not deleted due to JBoss and JDK package limitations.

Solution:

After the Enterprise Management uninstall, manually remove the JBoss and JDK ControlMinder folders.

How to Delete Old Hosts From the Database Report Tables

Symptom:

When I remove one of two CA ControlMinder endpoints or a CA ControlMinder DNS, data from the removed component still appears in the Policy Management reports.

Solution:

To delete endpoint snapshot data from the reports, run the following command on the Enterprise Management database:

```
Delete from SNAPSHOTINFO where HOSTID = host_to_delete_name
```

To delete endpoint snapshot data for Oracle, run the following commands on the Enterprise Management database:

```
Delete from GROUPINFO where hostid = host_to_delete_name
Delete from resac where hostid = host_to_delete_name
Delete from UACC where hostid = host_to_delete_name
Delete from USERREVACL where hostid = host_to_delete_name
Delete from NODE where hostid = host_to_delete_name
Delete from SPECIALPGMTYPE where hostid =host_to_delete_name
Delete from ACL where hostid = host_to_delete_name
Delete from resinfo where hostid =host_to_delete_name
Delete from seos where hostid = host_to_delete_name
Delete from USERACMODE  where hostid = host_to_delete_name
Delete from USERAC where hostid = host_to_delete_name
Delete from userinfo where hostid = host_to_delete_name
```

For Example:

- To delete endpoint data:
  ```
  Delete from SNAPSHOTINFO where HOSTID = 'hostname@ca.com
  ```
- To delete DMS data:
  ```
  Delete from SNAPSHOTINFO where HOSTID = DMS__@hostname@ca.com
  ```

Searching in View Recorded Sessions

The following known issues occur when you click View to search View Recorded Sessions in the CA ControlMinder Endpoint Management Recorded Sessions tab:

- When you search for Activity Log Contains (default), no results or messages are displayed.
- When you search for UserID or LoginID, the UserName field displays n\a/n\a.

Open Session Does Not Work In iOS 5

Open session does not work in iOS 5 due to a problem with iOS. The command to select open sessions in iOS, returns closed sessions as well.

PMDB Subscribers Not Listed When PMDB Name Exceeds Than 25 Characters

Symptom:

If a PMDB is created with more than 25 characters, then its subscribers are not listed when, you view it using the Endpoint Management user interface.

Solution:

This is a known issue with the Endpoint Management user interface. Use the sepmd utility to view the list of subscribers. The command has the following format:

```
sepmd -l pmd
```

-l

Lists the subscribers of the Policy Model.

pmd

Specifies the name of the Policy Model.

Telnet Session is Not Supported by Open Sessions

Valid on Windows

Open session does not detect and recognize the Telnet session as a login. The Telnet session is not supported by open sessions on Windows.

Default Request Approver Not Configured

Valid on SunOne and CA Directory

If you use SunOne or the CA Directory user directory, configure the default request approver. You define the default request approver that all privileged account passwords requests are submitted to.

Follow these steps:

1. Log in to CA ControlMinder Enterprise Management as a System Manager.
2. Select Users and Groups, Tasks, Modify Admin Task.

   The Modify Admin Task: Search Admin Task window opens.
3. Enter Privileged Account Request in the Name field, then click Search.

   CA ControlMinder Enterprise Management displays the results that match the search criteria.
4. Select the Privileged Account Request and click Select.

   The Modify Admin Task: Privileged Account Request window opens.
5. Navigate to the Events tab and select the workflow process.

   The Workflow Process screen opens.
6. In the Default Approver section, select Add Users.

   The Select User screen opens.
7. Enter the name of the user you want to assign as a default approver and select Search.

   CA ControlMinder Enterprise Management displays the results according to the search criteria.
8. Click Select.

   The user that you selected is added as a default request approver.
9. Click OK to exit.

Note: The default request approver that you defined does not apply to users that you created before you installed the Enterprise Management Server. The default request approver for users that previously existed in the user directory is superamdin.

"No Managed Connections Available Within Configured Blocking Timeout" Error Message When Running Batch Operations

"Managed Connections Available Within Configured Blocking Timeout" error message received when you run batch tasks. For example, you attempt to run the automatic reset password task on a large group or accounts. The error message indicates that the JBoss application server has exhausted the available connections and cannot complete the task.

To work around this problem you need to increase the number of available connections in the pool:

1. Stop the JBoss application server.
2. Navigate to the following directory, where *JBoss_HOME* indicates the directory where you installed JBoss:

   ```
   JBoss_HOME/server/default/deploy/
   ```
3. Open the file imtaskpersistencedb-ds.xml for editing.
4. Locate the <max-pool-size> tag and set the value to 40.
5. Locate the <idle-timeout-minutes> tag and set the value to 1.
6. Comment out (<!--) the <blocking-timout-millis> tag as follows:

   ```
   <!--blocking-timeout-millis>5000</blocking-timeout-millis-->
   ```
7. Save and close the file.
8. Start the JBoss application server.

   You have increased the number of available connections in the pool. You can now run the task.

JBoss for Windows Sample Policy Failed to Deploy

The JBoss for Windows sample policy fails to deploy on an endpoint. The policy deployment process terminates with an internal error message indicating that a PROGRAM resource already exists.

To work around the problem, use the JBoss sample policy and modify the policy before you deploy it to create PROGRAM resources explicitly.

Error Message Displayed When Viewing Policy Management Reports in CA ControlMinder Enterprise Management

CA ControlMinder Enterprise Management displays a message that the task failed when attempting to view policy management reports.

To work around this problem, restart the JBoss application server and the CA Business Intelligence server (Report Portal).

A CA ControlMinder User Not Defined a Password Cannot Log Into the CA ControlMinder Enterprise Management Server

An CA ControlMinder user account without a password cannot log into the CA ControlMinder Enterprise Management Server.

Access Roles Are Not Supported in CA ControlMinder Enterprise Management

When you define admin role rules, select users that are members of admin roles. CA ControlMinder Enterprise Management does not support access roles. The access roles option should not appear in the interface.

"No Operation Required" Message When Modifying UNAB Host or Host Group

When modifying UNAB host or host group settings and submitting the changes, CA ControlMinder Enterprise Management displays the following message: "No operation required". Although this message indicates that no action was taken, the modifications you made to the UNAB host or host group were applied.

Control Characters May Cause an Application Exception

Control characters in the CA ControlMinder database may cause an application exception or render incorrectly in CA ControlMinder Endpoint Management and CA ControlMinder Enterprise Management.

Incomprehensible Characters In the User Interface

Symptom:

When I log into the CA ControlMinder Enterprise Management user interface, I see incomprehensible characters.

Solution:

The problem is that the database instance you are using does not fully support UTF8 international characters set. To correct this problem, you must reinstall CA ControlMinder Enterprise Management on a fully internationalized database instance.

Cannot Change the Trust Property of a Monitored File

In CA ControlMinder Endpoint Management, clearing the Trust check box on the Audit tab of a monitored file (SECFILE) resource fails when you try to save the changes.

To work around this issue and change this resource attribute, use selang.

CA ControlMinder Enterprise Management Time-Out When Creating Large Policies

The CA ControlMinder Enterprise Management user interface times out when you create a policy that contains more than 6000 commands. You cannot continue working in the user interface until CA ControlMinder Enterprise Management creates the policy. To work around this problem, open a new session by logging in to CA ControlMinder Enterprise Management from a new browser.

Cannot Deploy Policies That Contain a Trailing Backslash

Conventions for selang let you use a backslash character (\) as the last character of a line to indicate that the command continues on the following line. This is not supported by advanced policy management. Make sure that policy commands do not span multiple lines.

Note: The following sample policies CA ControlMinder provides contain a trailing backslash: _AC_WEBSERVICE, _APACHE, _JBOSS, _MS_SQL_SERVER, and _ORACLE.

Policy Script Validation Error Messages Are in a Different Language

Valid in CA ControlMinder Enterprise Management

If a policy deploys with errors, the selang result messages you see in CA ControlMinder Enterprise Management are in the installation language of the CA ControlMinder endpoint on the Enterprise Management server and not that of the CA ControlMinder Enterprise Management installation.

To see these messages in a localized language, you must install the CA ControlMinder endpoint on the Enterprise Management computer in the desired localized language before you install CA ControlMinder Enterprise Management.

Cannot View Audit Records for Terminals with Names Longer than 30 Characters

You cannot view audit records if the terminal name has more than 30 characters. This happens when CA ControlMinder Endpoint Management running on a Windows computer manages a UNIX endpoint.

PMDB Audit Records Are Not Visible When Managing the PMDB

When you manage a PMDB using CA ControlMinder Endpoint Management, you cannot see the PMDB’s audit records.

To work around this issue and view the audit records for the PMDB, connect to host where the PMDB resides.

Open Session For Network Devices Fails

If the privileged account name contains more than ten characters, open session for Network Devices fails.

"No Such Method" or "Failed to Reset Password" Error Message for Access Control for SAM Endpoint Types

Valid on Linux

When you install the Enterprise Management Server on a Linux computer, you receive the following error message when you define Access Control for SAM endpoints: "No Such Method".

If you specify that CA ControlMinder Enterprise Management resets a privileged account password on check in, when a user checks in a privileged account on an Access Control for SAM endpoint they receive the following error message: "Failed to Reset Password".

Follow these steps:

1. Stop the Java Connector Server. Do the following:

   a. Navigate to the following directory, where *ACServerInstallDir* refers to the directory where the Enterprise Management Server is installed:

      ```
      ACServerInstallDir/Connector_Server/bin
      ```

   b. Run the following command:

      ```
      ./im_jcs stop
      ```

      The Java Connector Server stops.

2. Open the im_jcs script for editing.

3. Locate and remove the following line from the script:

   ```
   PREJAR="$FULLBASEPATH/bin/jcs-bootstrap.jar:$FULLBASEPATH/
   conf:$FULLBASEPATH/lib/jcs.jar:"`echo $FULLBASEPATH/
   lib/apacheds-server-main-*-app.jar`
   ```

4. Copy the following line and paste it into the script:

   ```
   PREJAR="$FULLBASEPATH/bin/jcs-bootstrap.jar:$FULLBASEPATH/
   conf:$FULLBASEPATH/lib/jcs.jar:$FULLBASEPATH/
   lib/nlog4j__V1.2.25.jar:"`echo
   $FULLBASEPATH/lib/apacheds-server-main-*-app.jar`
   ```

   Important! Delete the carriage returns in the line after you paste it into the script.

5. Save the file.
6. Start the Java Connector Server.

   ```
   ./im_jcs start
   ```

   The Java Connector Server starts. You can now configure the Access Control for SAM endpoint type.

Telnet Automatic Login Not Supported on Solaris After Upgrade

Valid on Solaris

The Telnet automatic login is not supported on Solaris after you upgrade to CA ControlMinder 12.7.

Changes to Windows Services and Scheduled Tasks Are Not Discovered

Valid on Windows Server 2003

Symptom:

When you change a Windows Service or Windows Scheduled Task, the changes cannot be discovered.

Solution:

This is a known Microsoft issue. After you change the service or task on the endpoint, delete the existing password consumer. Use the Service Account Discovery Wizard to create a password consumer.

Approval of Service Account Password Request Fails

After you submit a request for a service account password, the request is not sent to the request approver and you cannot check out the service account password.

No Audit Record for Password Retrieval by JDBC Password Consumer

The Enterprise Management Server does not write an audit record when a JDBC password consumer gets a password from CA ControlMinder Enterprise Management.

Error Message When You Use Automatic Login to Log in to Oracle Enterprise Manager

Valid on Oracle

An error message appears when you use the automatic login option to log into the Oracle Enterprise Manager after you checked out an administrator account password. The error message appears if you terminated the last session by closing the browser window without logging off.

Remote Desktop Connection Fails When Endpoint Prompts for Password

Valid on Windows

The Windows Remote Desktop automatic login script fails to log into the endpoint if the endpoint Terminal Services settings are configured to always prompt for password on login.

SAM Accepts Ticket Numbers for Closed CA Service Desk Tickets

Valid for integration with CA Service Desk

If you specify the number for a closed CA Service Desk issue or request ticket (ticket type=iss or cr) when you request access to a privileged account, CA ControlMinder Enterprise Management forwards the request to the approver.

Cannot Specify CA Service Desk Change Order Ticket Number

Valid for integration with CA Service Desk

If you specify the number for a CA Service Desk change order ticket (ticket type=ch) when you request access to a privileged account, CA ControlMinder Enterprise Management does not forward the request to the approver.

Cannot Verify Exclusive Sessions to Prevent Check In

Symptom:

In Linux Enterprise Management or with a Linux Distribution Server, I cannot verify exclusive sessions to prevent check-in if open sessions are available to that endpoint.

Solution:

Follow these steps:

1. Stop CA ControlMinder services.
2. On the Linux Enterprise Management Distribution Server, go to directory (AccessControlServer_HOME/APMS/AccessControlShared) and open accommon.ini for editing.
3. Go to the [AccountManager] section and search for 'exclude_endpoint_types'.
4. Enter the 'Windows Agentless' value after the '=' symbol. For example, exclude_endpoint_types = Windows Agentless. Separate multiple endpoint types with commas.
5. Start CA ControlMinder services.

Note: This change is recommended only if one of the Distribution Server/Enterprise Management operating systems is Windows.

New Topic (183)

Valid on Windows

After I change an Active Directory requester organizational unit, tasks that were submitted under the old organizational unit do not appear in My View Submitted Task.

This is a known issue that results from limitations in the Active Directory search method.

Documentation Known Issues

This section describes known issues for the CA ControlMinder documentation set.

No Alternate Text for Graphics In the SDK Guide

There is no alternate text for graphics in the SDK Guide. The SDK Guide was first published with a previous release of CA ControlMinder and is provided as a courtesy with the CA ControlMinder r12.5 documentation.

PDF Documentation Requires Adobe Reader 7.0.7

To read the documentation for CA ControlMinder in print format (PDF files), you must install Adobe Reader 7.0.7 or later. You can download Adobe Reader from the Adobe website if it is not already installed on your computer.

Note: Adobe Reader is not available on HP-UX Itanium (IA64) and Red Hat Linux Itanium IA64.