CA ControlMinder Premium Edition

Release Notes

12.6.03

Third-Party Notices

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

Sample Scripts and Sample SDK Code

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

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

CA Technologies Product References

This document references the following CA Technologies products:

- CA ControlMinder Premium Edition
- 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 (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 1: Welcome

Welcome to CA ControlMinder Premium Edition 12.6.03. 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 Premium Edition.

This section contains the following topics:

CA ControlMinder Installation Media

CA ControlMinder components are available on the following image files.

The following image files contain endpoint components:

- CA ControlMinder Endpoint Components for Windows

  Contains CA ControlMinder for Windows installation files for endpoint components. These include the core CA ControlMinder functionality required for a standalone Windows computer, additional executables and libraries to extend core functionality (for example, Policy Model support), runtime SDK files and libraries and API samples, mainframe password synchronization, and Stack Overflow Protection (STOP).

- CA ControlMinder Endpoint Components for UNIX

  Contains CA ControlMinder for UNIX installation files for endpoint components. These include the core CA ControlMinder functionality required for a standalone UNIX computer, additional binaries and scripts to extend core functionality (for example, Policy Model support), API libraries and samples, mainframe password synchronization, and Stack Overflow Protection (STOP).

  This image file also contains UNAB installation files for use with CA ControlMinder Enterprise Management.

A Single Documentation Set for All Editions

We supply the same documentation for both editions. Because of that, some sections of some guides apply only to CA ControlMinder Premium Edition. The following describes how the documentation applies to CA ControlMinder:

- Release Notes

  Some information in this guide applies only to CA ControlMinder Premium Edition features.

- Implementation Guide

  Some information in this guide applies only to CA ControlMinder Premium Edition features.

- Enterprise Administration Guide

  The entire guide applies only to CA ControlMinder Premium Edition.

- Upgrade Guide

  Some information in this guide applies only to CA ControlMinder Premium Edition features.

- Implementation Guide

  This entire guide applies to CA ControlMinder Premium Edition.

- Endpoint Administration Guide for Windows

  The entire guide applies to CA ControlMinder.

- Endpoint Administration Guide for UNIX

  The entire guide applies to CA ControlMinder.

- Reference Guide

  Some information in this guide applies only to CA ControlMinder Premium Edition features.

- selang Reference Guide

  Some information in this guide applies only to CA ControlMinder Premium Edition features.

- Troubleshooting Guide

  Some information in this guide applies only to CA ControlMinder Premium Edition features.

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

Chapter 2: New and Changed Features

This section contains the following topics:

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.

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.

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 Premium Edition r12.6.01 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.

Product Re-branding Limitations

The following product components were re-branded to CA ControlMinder:

- Installation messages
- Utility messages
- User interface page titles
- Display names
- Login screens

The following product components were not re-branded and use CA Access Control:

- Product path names
- Selang command prompts
- Product and program file names
- Registry entries
- Package names

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.

Customization Script does not Support Multiple Options Update

The UNAB customized installation script does not support multiple options update. You must customize the installation script twice--once to accept the license and then to customize the installation options.

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.

Chapter 7: Installation Considerations

This section contains the following topics:

Supported Installation Languages

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

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

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

Endpoint Components Release Only

This release of CA ControlMinder contains endpoint components only. The following endpoint components are included with this release:

- CA ControlMinder Endpoint for UNIX
- CA ControlMinder Endpoint for Windows
- UNAB Endpoint

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.

CA ControlMinder Installation Considerations for Solaris 8 and 9

Valid on Solaris 8, Solais 9

To install CA ControlMinder using the native package installation on Solaris 8 and Solaris 9 operating system complete the following procedure before you extract the installation package:

1. Copy the installation package to a temporary directory.
2. Execute the following commands:

   ```
   zcat _SOLARIS_126.tar.Z | tar xof -
   rm -f CAeAC/install/depend
   ```

3. Open the /CAeAC/pkgmap file and locate the line that begins with '1 i depend'.
4. Remove the line from and save the file.

   You can now customize the package and install CA ControlMinder.

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 Enterprise Log Manager.

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).

UNAB Endpoint Installation Considerations

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

Error Message Appears if CA_LIC Installed in a Non-Default Directory

Valid on Solaris

Symptom:

After I installed CA_LIC in to a non-default directory I attempted to install CA ControlMinder and UNAB on the Solaris host. The installation completed successfully but the registration process ended with an error message.

Solution:

The error message appears when you specify to install the CA_LIC component into a non-default directory, for example you specified the LIC_INSTALL_DIR parameter to /work/CA directory. To workaround this problem specify the following parameter CASHCOMP=/work/CA and install UNAB.

Users Log in Fail When UNAB SELinux is Enabled on Red Hat Enterprise Linux 5.8

Valid on Red Hat Enterprise Linux 5.8

Active Directory users cannot log in to a Red Hat Enterprise Linux 5.8 if UNAB SELinux is enabled.

UNAB Installation Considerations for Solaris 8 and 9

Valid on Solaris 8, Solais 9

To install UNAB on Solaris 8 and Solaris 9 operating system, you must complete the following procedure before you extract the installation package:

1. Copy the installation package to a temporary directory.
2. Execute the following commands:

   ```
   zcat _SOLARIS_Ux_PKG_126.tar.Z | tar xof -
   rm -f uxauth/install/depend
   ```
3. Open the pkgmap file and locate the line that begins with '1 i depend'.
4. Remove the line from and save the file.

   You can now customize the package and install UNAB.

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*.

Chapter 8: Upgrade Considerations

This section contains the following topics:

Versions You Can Upgrade From

You can upgrade your CA ControlMinder endpoints to 12.6.03 from the following versions:

- 12.6.02
- 12.6.01
- 12.6
- 12.5.5

You cannot upgrade your CA ControlMinder endpoints to 12.6.03 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 12.6.03.

- 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 12.6.03.

Windows Endpoint Upgrade Considerations

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

Reboot May Be Required When Upgrading

When you upgrade an endpoint to this release from r12.0 SP1 or later, it is not mandatory that you reboot the computer. After the upgrade, CA ControlMinder preserves backwards compatibility. However, the upgrade is not complete until you reboot the computer, and all new functionality may not be supported until after the reboot.

When you upgrade an r8.0 SP1 or r12.0 endpoint to this release, you must reboot the computer.

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.

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.

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.

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.

Native Package Customization on Non-English Locales Fails When Customizing Package for Several Locales

Symptom:

When I customize the CA ControlMinder or UNAB native packages for several locales on a non-English operating system the customization process fails.

Solution:

Currently, you cannot customize the CA ControlMinder and UNAB native packages to support several non-English locales. To fix this issue contact CA Support to obtain a fix that you deploy before customizing the packages.

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.

seaudit, sebuildla Permission Denied Messages After Upgrade

Valid on AIX

After you upgrade using the native package, you may receive permission denied error messages when using the seaudit and sebuildla utilities.

To work around this problem, re-trust the utilities after the upgrade completes.

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.

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 Enterprise Log Manager Reports

A rename HOST event performed in selang is displayed as an unknown event in CA Enterprise Log Manager reports.

UNIX Endpoint Known Issues

This section describes known issues for CA ControlMinder for UNIX.

FTP Login on Solaris 8 Fails

Symptom:

I'm on a Solaris 8 machine and FTP logins fail for AD users.

```
530 Login incorrect.
Login failed.
```

The same account credentials work fine for native users.

Solution:

None. The ftpd on Solaris 8 verifies the existence of the account in /etc/shadow and NIS. The FTP implementation on newer Solaris versions does not have this limitation.

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.

SSH Login Not Audited by CA ControlMinder or by Audit Log if SElinux Enabled

Valid on RedHat Linux Advanced Server 6

On RedHat Linux Advanced Server 6, SSH user log ins are not audited by CA ControlMinder because the SElinux default policy does not allow SSHD to access the /proc file system.

To workaround this issue, run the /opt/CA/AccessControl//lbin/sshd_policy.sh script to load a SElinux policy module to allow access to /proc.

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.

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.

Failed to Change Password at First Login

Valid on Solaris 10

When a user attempts to log in to a UNAB host using SSH and tries to change the account password on first login, the password change operation fails.

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.

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.