ONE IDENTITY™

One Identity Management Console for Unix 2.5.3

Administration Guide

Contents

One Identity Privileged Access Suite for Unix

Unix Security Simplified

One Identity Privileged Access Suite for Unix solves the inherent security and administration issues of Unix-based systems (including Linux and Mac) while making satisfying compliance requirements a breeze. It unifies and consolidates identities, assigns individual accountability and enables centralized reporting for user and administrator access to Unix. The Privileged Access Suite for Unix is a one-stop shop for Unix security that combines an Active Directory bridge and root delegation solutions under a unified console that grants organizations centralized visibility and streamlined administration of identities and access rights across their entire Unix environment.

Active Directory Bridge

Achieve unified access control, authentication, authorization and identity administration for Unix, Linux, and Mac systems by extending them into Active Directory (AD) and taking advantage of AD's inherent benefits. Patented technology allows non-Windows resources to become part of the AD trusted realm, and extends AD's security, compliance and Kerberos-based authentication capabilities to Unix, Linux, and Mac. See Authentication Services for more information about the Active Directory Bridge product.

Root Delegation

The Privileged Access Suite for Unix offers two different approaches to delegating the Unix root account. The suite either *enhances* or *replaces* sudo, depending on your needs.

- By choosing to enhance sudo, you will keep everything you know and love about sudo while enhancing it with features like a central sudo policy server, centralized keystroke logs, a sudo event log, and compliance reports for who can do what with Sudo.

  See One Identity Privilege Manager for Sudo for more information about enhancing sudo.

- By choosing to replace sudo, you will still be able to delegate the Unix root privilege based on centralized policy reporting on access rights, but with a more granular permission and the ability to log keystrokes on all activities from the time a user logs

in, not just the commands that are prefixed with "sudo". In addition, this option implements several additional security features like restricted shells, remote host command execution, and hardened binaries that remove the ability to escape out of commands and gain undetected elevated access.

See Privilege Manager for Unix for more information about replacing sudo.

Privileged Access Suite for Unix

Privileged Access Suite for Unix offers two editions - *Standard* edition and *Advanced* edition. Both editions include: **One Identity Management Console for Unix**, a common management console that provides a consolidated view and centralized point of management for local Unix users and groups; and **Authentication Services**, patented technology that enables organizations to extend the security and compliance of Active Directory to Unix, Linux, and Mac platforms and enterprise applications. In addition

- The *Standard* edition licenses you for Privilege Manager for Sudo.
- The *Advanced* edition licenses you for Privilege Manager for Unix.

One Identity recommends that you follow these steps:

1. Install Authentication Services on one machine, so you can set up your Active Directory Forest.
2. Install One Identity Management Console for Unix, so you can perform all the other installation steps from the mangement console.
3. Add and profile hosts using the mangement console.
4. Configure the console to use Active Directory.
5. Deploy client software to remote hosts.

   Depending on which Privileged Access Suite for Unix edition you have purchased, deploy either:

   - **Privilege Manager for Unix** software (that is, Privilege Manager Agent packages)

     -OR-

   - **Privilege Manager for Sudo** software (that is, Sudo Plugin packages)

See Installing Privilege Manager agent or plugin software on page 116 for more information about the two Privilege Manager client software packages available to install onto remote hosts.

NOTE: Refer to Getting Started tab on page 33 for a better understanding of the steps to take to be up and running quickly.

About this guide

Welcome to the One Identity Management Console for Unix Administration Guide. This guide is intended for Windows, Unix, Linux, and Mac system administrators, network

administrators, consultants, analysts, and any other IT professional who will be installing and configuring One Identity Management Console for Unix for the first time.

Introducing One Identity Management Console for Unix

One Identity Management Console for Unix is a web-based console that delivers a consolidated view and centralized point of management for local Unix users and groups, including:

- Local Unix user and group management
- Centralized reporting
- Pre-migration readiness assessment for integrating with Active Directory
- Remote client-agent deployment
- Secure local Unix accounts with Active Directory authentication

Key features and capabilities of the mangement console:

Local Unix User and Group Management

Management Console for Unix enables administrators to use the same tool to manage all Unix account information regardless of its location (within Active Directory or locally on Unix systems). With the mangement console, administrators can remotely manage local users and groups on Unix, Linux, and Mac systems. This functionality is shipped with Authentication Services, Privilege Manager for Unix, and Privilege Manager for Sudo.

Active Directory Integration

Management Console for Unix provides the quickest path to compliance by enabling organizations to quickly, easily, and inexpensively implement Active Directory-based authentication for Unix, Linux, and Mac systems. The mangement console allows remote Unix systems to be profiled and assessed to check their readiness for integration with Active Directory. Once deployed, Management Console for Unix even enables Unix accounts to remain where they are and yet use Active Directory for centralized authentication.

Privilege Manager Integration

Management Console for Unix provides advanced management and reporting capabilities when used with One Identity Privilege Manager. You can install and configure the *Policy Server* as well as the *PM Agent* and the *Sudo Plugin* software to remote hosts. You can also join hosts to a policy group if you have activated it in the *Privilege Manager* settings. This gives you the ability to centrally manage policy and create comprehensive "keystroke logs" that capture forensic-level auditing.

Remote Agent Deployment

Management Console for Unix streamlines deployment of client agent software by empowering administrators to remotely install the software packages and join systems either to Active Directory or a Privilege Manager policy group. The mangement console allows non-Unix administrators to administer and deploy the solution without ever touching the Unix command line.

Role-Based Access Control

Active Directory users and groups can now be granted access to the mangement console and given limited use of console features by means of roles. This means you can configure separation of duties for specific tasks.

Basic Roles:

- Manage Hosts
- Console Administration
- Manage Console Access
- Reporting

Additional Privilege Manager Roles:

- Manage Sudo Policy
- Audit Sudo Policy
- Manage PM Policy
- Audit PM Policy

Reporting

Management Console for Unix enables administrators to quickly and easily provide auditors with granular reports on Unix identity information, including the highly desirable access and privilege reports. By consolidating the generation and viewing of reports within the mangement console, Management Console for Unix reduces the time and effort required to generate key reports that traditionally required multiple data collation and manual processes across multiple Unix systems.

Securing Local Unix Accounts with Active Directory Authentication

Management Console for Unix eases deployments of Authentication Services by providing a birds-eye view of all local Unix accounts and Active Directory accounts with Unix account information. When viewing local Unix accounts, administrators can determine which accounts to configure for Active Directory authentication.

Web Services

Management Console for Unix allows you to access the server by means of Web Services, including Unix command line utilities and Windows Powershell cmdlets that enable you to script common local Unix user and group management tasks. For example, you can write a script to reset a local Unix user's password across multiple Unix systems.

What's new in Management Console for Unix 2.5

Management Console for Unix has continued to add powerful configuration, administration, management, and migration capabilities through a Web-based console. The following is a list of the new features for One Identity Management Console for Unix 2.5.

One Identity Privilege Manager for Unix integration

Support for advanced, centralized Privilege Manager for Unix policy management, remote agent plugin installation and configuration, keystroke logging and replay, and reporting.

- New roles for managing Privilege Manager for Unix
- Remote installation of the Privilege Manager software
- Readiness checks for both server configuration and host joins to policy groups
- Ability to configure both primary and secondary policy servers
- Centralized pmpolicy profile management with reporting and auditing
- Support for the PMRUN elevation credential

One Identity Privilege Manager for Sudo

- Support for Mac OS X

Authentication Services Access Control Management

Support for limiting Active Directory user access to host systems by managing which Active Directory users and groups can access the host systems.

- Manage access control on a single host system

- Add and remove Active Directory users or groups across multiple hosts

Other new Management Console for Unix features

- Reset or change passwords for multiple local accounts across multiple hosts
- Modify certain user properties across multiple hosts
- Support for Tectia SSH
- Context-sensitive help is now available
- New console role for access to all reports
- Product License Usage report

Upgrading from Identity Manager for Unix 1.0

If you are upgrading from Quest Identity Manager for Unix 1.0 to Management Console for Unix 2.*x*, be aware of the following:

- Passwords cached by the ***supervisor*** account or AD users with console access were not migrated during the upgrade process due to changes in encryption. Users will have to re-enter their passwords for hosts they manage the next time they perform tasks on the hosts, and choose to cache their credentials again on the server.
- It is important to re-profile all hosts after an upgrade of any version of Management Console for Unix.
- Existing Active Directory users and groups granted access to the mangement console are added to the **Manage Hosts** role, giving them access to the features they had before the upgrade.

What are the core features of the console

The following summarizes the differences between the core version of Management Console for Unix and what is available when it is used in conjunction with Privilege Manager or Authentication Services.

Core features of Management Console for Unix:

- Provides a central management and reporting console for local Unix hosts.
- Provides up-to-date synchronization between the host and the console.
- Ability to create, delete, and modify local user and group accounts.
- Ability to browse Active Directory
- Ability to assign users to console roles

- Ability to perform console tasks using Windows Powershell and Unix command line tools.

When used with Privilege Manager

- Ability to remotely install Privilege Manager software on a remote host.
- Ability to configure both primary and secondary policy servers.
- Ability to join remote hosts to policy groups.
- Ability to centrally manage the policy file.
- Ability to enable keystroke logging and view captured keystroke logs.
- Ability to provide access and privileges reports to determine which actions users are permitted to perform on Unix hosts.
- Ability to report which commands were executed using sudo on Unix hosts.

When used with Authentication Services:

- Ability to remotely install Authentication Services agents, join systems to Active Directory, and implement AD-based authentication for Unix, Linux, and Mac systems.
- Ability to manage access control on a single host system or across multiple hosts.
- Ability to create reports about Unix-enabled Active Directory users and groups.
- Ability to create access control reports that show which user is permitted to log into which Unix host.

How Management Console for Unix works

Management Console for Unix is a JEE (Java Enterprise Edition) web application that simplifies local user and group management on Unix, Linux, and Mac systems using a "mangement console". You access the mangement console through a supported web browser.

Management Console for Unix is deployed on a web server, or more specifically a Java Servlet container running on a Java Virtual Machine (JVM).

Figure 1: Management Console for Unix Architecture
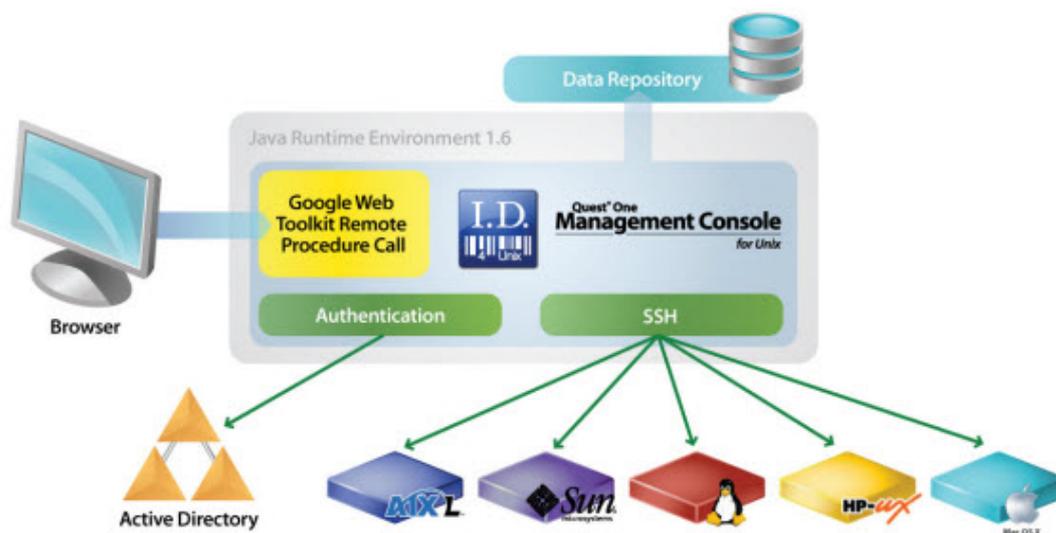
By default, requests are secured by enforcing connections over HTTPS. Communication between the web browser and web server are accomplished through HTTP requests over SSL. Requests from a supported web browser are sent to the web server, which processes the request and returns a response.

The web server fulfills requests by gathering data from one or more locations. These requests are filled from data found in Active Directory, the supplied database, or by collecting data from one or more Unix, Linux, and Mac systems.

The data is stored in a local database on the Management Console for Unix web server. Access to the database is accomplished through JDBC (Java Database Connectivity) technology and is secured by credential authentication (that is, only administrators have access to the Management Console for Unix data directory). Active Directory connections are made through LDAP. These LDAP connections are authenticated with a valid Active Directory user account.

Secure connections to all Unix, Linux, and Mac systems are performed through the SSH protocol. Prior to exchanging SSH credentials, the system's SSH host key is compared against a known SSH host key. If the key validation is successful an authentication attempt is performed. If the key validation determines that the system SSH host key does not match the known SSH host key, authentication will not be attempted until the known SSH host key matches a system SSH host key.

You can run Management Console for Unix separately in a supported web browser or, you can run the mangement console from within the Authentication Services Control Center. You can install it on Windows, Unix, or Linux. One Identity does not advise managing a Unix host by more than one mangement console in order to avoid redundancy and inconsistencies in stored information. If you manage the same Unix host by more than one

mangement console, you should enable auto-profile for that host to minimize inconsistencies that may occur between instances of the mangement consoles.

Installing Management Console for Unix

To remotely manage local users and groups on Unix, Linux, and Mac systems with the mangement console, you must install a Java-based web application that runs on a server which allows you to run a "mangement console" inside a web browser.

The topics in this section explain how to install Management Console for Unix for the first time and how to upgrade it from an older version. It includes the steps for installing and configuring the mangement console on a Windows, Unix, or Linux machine. These instructions assume that you are installing the mangement console from a product ISO.

NOTE: If you already have Quest Identity Manager for Unix installed and are now upgrading it, refer to Upgrade Quest Identity Manager for Unix on page 35.

System requirements

Prior to installing Management Console for Unix, ensure your system meets the minimum hardware and software requirements for your platform.

NOTE: When setting up a virtual environment, carefully consider the configuration aspects such as CPU, memory availability, I/O subsystem, and network infrastructure to ensure the virtual layer has the necessary resources available. Please consult One Identity's Product Support Policies for more information on environment virtualization.

Table 1: System requirements

Component	Requirements
Supported Platforms	Can be installed on the following configurations: - Windows x86 (32-bit) - Windows x86-64 (64-bit) - Unix/Linux systems for which Java 8 is available
Server Requirements	The Management Console for Unix server requires Java 8 (also

Component	Requirements
	referred to as JRE 8, JDK 8, JRE 1.8, and JDK 1.8).
Managed Host Require-ments	Click www.oneidentity.com/products/authentication-services/ to view a list of Unix, Linux, and Mac platforms that support Authentication Services.
	Click www.oneidentity.com/products/privilege-manager-for-unix/ to review a list of Unix and Linux platforms that support Privilege Manager for Unix.
	Click www.oneidentity.com/products/privilege-manager-for-sudo/ to review a list of Unix, Linux, and Mac platforms that support Privilege Manager for Sudo.
	NOTE: To enable the Management Console for Unix server to interact with the host, you must install both an SSH server (that is, sshd) and an SSH client on each managed host. Both OpenSSH 2.5 (and higher) and Tectia SSH 5.0 (and higher) are supported.
	NOTE: Management Console for Unix does not support Security-Enhanced Linux (SELinux).
	NOTE: When you install Authentication Services on Solaris 10 (SPARC - 32/64-bit), the Solaris 10 packages are installed.
Default Memory Requirement:	1024 MB
	NOTE: See JVM memory tuning suggestions on page 214 for information about changing the default memory allocation setting in the configuration file.

Network port requirements

Management Console for Unix must be able to communicate with Active Directory including domain controllers, global catalogs and DNS servers using Kerberos, LDAP and DNS protocols. The following table summarizes the network ports that must be open and their function.

Table 2: Network ports

Port	Protocol	Function
22	TCP	Default TCP port number used for Secure Shell (SSH) access to Unix hosts being managed by the mangement console.
53	TCP and UDP	Used for DNS. Since Management Console for Unix uses DNS to locate domain controllers, DNS servers used by the Unix hosts must serve Active Directory DNS SRV records.

Port	Protocol	Function
88	TCP and UDP	Used for Kerberos authentication and Kerberos service ticket requests against Active Directory Domain Controllers. UDP is used by default, but TCP is also used if the Kerberos ticket is too large for UDP transport.
137	TCP and UDP	Used for resolving NetBIOS names, as per RFC1002. UDP is tried first, with fall back to TCP.
389	TCP and UDP	Used for LDAP searches against Active Directory Domain Controllers. TCP is normally used, but UDP is used when detecting the Active Directory site membership.
3268	TCP	Used for LDAP searches against Active Directory global catalogs. TCP is always used when searching against the global catalog.
9001	TCP	Default TCP port used internally on the loopback interface of the Management Console for Unix server for JDBC connections.
9080	TCP	Non-SSL Port number (http:) for the Management Console for Unix Web server; configurable at install time.
9443	TCP	Default Management Console for Unix Web server TCP port used for HTTPS; configurable at install time.

Before installing the Management Console

Management Console for Unix 2.5.2 requires Java 8 (that is, Java SE 8, Java Platform Standard Edition 8). Before you run the Management Console for Unix installer, ensure that a suitable implementation of Java 8 is installed.

32-bit or 64-bit

- On Unix/Linux, the installer supports both 32-bit and 64-bit Java 8.
- On 32-bit Windows, use 32-bit Java 8 and the 32-bit installer.
- On 64-bit Windows, use 64-bit Java 8 and the 64-bit installer or (if desired) use 32-bit Java 8 for the 32-bit installer.

The 32-bit implementation should only be used for small installations of Management Console for Unix; for most installations, the 64-bit implementation of Java 8 and Management Console for Unix is preferable.

JRE, JDK, or Server JRE

Any configuration of Java 8 — the JRE, the JDK, or the Server JRE — can be used. The Server JRE is ideal but is only available for some platforms. The JRE is sufficient. The JDK,

a superset of the JRE that adds tools for Java development, is also more than sufficient.

Obtaining Java 8

On Unix/Linux, your operating system may provide Java 8, either already installed or available as packages that can be downloaded and installed.

Providers of Java 8 implementations for Windows and for Unix/Linux include:

- Oracle, newest release:

  http://www.oracle.com/technetwork/java/javase/downloads/index-jsp-138363.html

- Oracle, older Java 8 releases:

  http://www.oracle.com/technetwork/java/javase/downloads/java-archive-javase8-2177648.html

- Azul Systems' OpenJDK builds:

  https://www.azul.com/downloads/zulu/

- IBM:

  https://developer.ibm.com/javasdk/downloads/sdk8/

- AdoptOpenJDK:

  https://adoptopenjdk.net/support.html

Java 8 version/update numbers

JDK 8 may also be referred to as JDK 1.8 or JDK 1.8.0. Updates (patch releases) are numbered, and an update such as 181 may be referred to as either JDK 8u181 or JDK 1.8.0_181. The same is true for the JRE. IBM has its own release process and its own numbering scheme.

To stay abreast of Java 8 security fixes, whenever possible the most recent Java 8 update should be used.

Installing the Management Console

You can install Management Console for Unix on Windows, Unix, or Linux computers. Each hosting platform prompts for similar information.

The following install files are located under **console | server**:

- ManagementConsoleForUnix_unix_2_5_2.sh - for Unix and Linux

- ManagementConsoleForUnix_windows_2_5_2.exe - for Windows

- ManagementConsoleForUnix_windows-x64_2_5_2.exe - for Windows

Installing and uninstalling the console on Windows

To install the mangement console from the distribution media on Windows

1. Mount the distribution media.

   Autorun starts automatically.

   > NOTE: To start the Autorun installation wizard, you can also navigate to the root of the distribution media and double-click **autorun** Application file.

2. From the One Identity Privileged Access Suite for Unix Autorun *Home* page, click the **Setup** tab.

3. From the **Setup** tab, click **One Identity Management Console for Unix**.

   The install wizard guides you through these setup dialogs:

   - **Management Console for Unix License Agreement** dialog
   - **Configure TCP/IP Port** dialog
   - **Installing** dialog;

     Please wait while it:

     - extracts and installs Management Console for Unix on your computer
     - configures the database and service on the server
     - copies the Authentication Services client software packages for each platform
     - copies the Sudo Plugin software packages for each platform
     - copies the Privilege Manager for Unix Agent software packages for each platform
     - copies the Privilege Manager Policy Server packages for each platform

       > NOTE: Software packages are only copied if upgrading from a previous version of Management Console for Unix. New installations create a directory structure where the Authentication Servicesand Privilege Manager packages can be placed, but the packages must be set up manually.

   - **Completing the Management Console for Unix installation** dialog

   To continue the installation and configuration process, go to Setting up Management Console for Unix on page 30

To uninstall the mangement console

> BEST PRACTICE: Before you uninstall Management Console for Unix, backup your application database to ensure that you do not lose data. The application database contains information about the hosts, settings, users, groups, passwords, and so forth.

> By default, the application data directory is:

```
%SystemDrive%:\ProgramData\Quest Software\Management Console for Unix
```

1. From the **Start** menu, navigate to **Programs | One Identity Software | Management Console for Unix | Uninstall Management Console for Unix**.

   NOTE: Because One Identity changed the product name for version 2.0, the path to the uninstaller in version 1.0 is **Programs | One Identity Software | Identity Manager for Unix | Quest Identity Manager for Unix Uninstaller**.

2. To preserve your application database, clear the **Remove application database and application logs** option.

3. The default for the uninstaller is to remove everything.

4. Click **Uninstall**.

5. Once the uninstaller has removed the product from your computer, click **Finish** to close the uninstaller program.

Installing the console from the Windows command line

Use this procedure to install the mangement console on the designated Windows computer from the command line.

To install the mangement console on a Windows platform

1. Log in and open a command shell.

2. From the root of the distribution media, navigate to **console | server**.

3. For a 64-bit installation, run the following command:

   ```
   # .\ManagementConsoleForUnix_windows-x64_2_5_2.exe
   ```

   You can use one of the following options:

   - -q option for "quiet" mode, which automatically accepts all the default settings.
   - -c option for "console" mode, which prompts you for information interactively.

   NOTE: Using no option starts the installer in a graphical user interface.

   In "console" mode, it asks you for the following information.

4. Enter **1** to accept the user agreement.

5. Enter the SSL Port number, or press **Enter** to accept the default of 9443.

6. Enter the Non-SSL Port number or press **Enter** to accept the default of 9080.

   The install wizard extracts and copies the files, configures and starts the service, and so forth.

   NOTE: By default, the installation directory is located at:

   ```
   %SystemDrive%:\Program Files\Quest Software\Management Console for Unix
   ```

To continue the installation and configuration process, go to Setting up Management Console for Unix on page 30.

Installing and uninstalling the console on Unix and Linux

Use this procedure to install the mangement console on the designated Unix computer from the command line with the installation script.

To install the mangement console on a Unix platform

1. Log in and open a root shell.
2. Mount the installation media and navigate to **console | server**.
3. Run the following command from the Unix command line as root:

   ```
   # sh ManagementConsoleForUnix_unix_2_5_2.sh
   ```

   You can use one of the following options:

   - -q option for "quiet" mode, which automatically accepts all the default settings.
   - -c option for "console" mode, which prompts you for information interactively.

   NOTE: Using no option starts the installer in a graphical user interface if you have an X server, making the installation experience similar to running it from the Windows autorun. See Installing and uninstalling the console on Windows on page 26 for details.

   In "console" mode, it asks you for the following information.

4. Enter **1** to accept the user agreement.
5. Enter the SSL Port number, or press **Enter** to accept the default of 9443.
6. Enter the Non-SSL Port number or press **Enter** to accept the default of 9080.

   The install wizard extracts and copies the files, configures and starts the service, and so forth.

   NOTE: On Unix, the install location is /opt/quest/mcu and you cannot specify an alternate path.

   To continue the installation and configuration process, go to Setting up Management Console for Unix on page 30.

To uninstall Management Console for Unix from Unix

NOTE: The default for the uninstaller is to remove everything. Before you uninstall Management Console for Unix, if you plan to re-install Management Console for Unix and want to preserve your data, backup your application database. The application database contains information about the hosts, settings, users, groups, passwords, and so forth.

By default, the database directory is at: /var/opt/quest/mcu.

1. Run the following command as root:

   - To uninstall version 1.0, run:

     /opt/quest/imu/uninstall

   - To uninstall version 2.*x*, run:

     /opt/quest/mcu/uninstall

   You can use one of the following options with the `uninstall` command:

   - `-q` option for "quiet" mode, which automatically accepts all the default settings, including removing the application database and logs.
   - `-c` option for "console" mode, which prompts you for information interactively.

   | NOTE: Using no option starts the uninstaller in a graphical user interface.

2. If in "console" mode, confirm whether you want to remove the application database and application logs or not.

   This option is useful if you plan to re-install Management Console for Unix and want to preserve your data. The default for the uninstaller is to remove everything.

The wizard uninstalls Management Console for Unix.

Launching the Management Console

Use one of the following methods to launch the mangement console:

1. If you selected the **Create desktop shortcut** option on the **Complete** dialog, select the Management Console for Unix shortcut from your Windows desktop.

2. If you selected the **Create Start menu item** option on the **Complete** dialog, from your Windows desktop, navigate to **Start | Programs | Quest Software | Management Console for Unix | Management Console for Unix**.

3. You can also open your web browser and enter the URL of the web application server by entering:

   ```
   https://<Hostname or IP address>:<port>
   ```

   For example, entering **https://localhost:9443** launches the mangement console that was installed locally using the default port of 9443.

   NOTE: Management Console for Unix requires that all connections to the browser are secured with the SSL/TLS protocol. Therefore, you must use the https URL. If you accidentally enter the http URL, you may encounter unexpected behavior (for example, on Firefox, you are asked to save a file to disk). See Installing a production certificate on page 182 for details.

To launch the mangement console from Unix or Linux

1. Open your web browser and enter the URL of the web application server:

   ```
   https://<Hostname or IP address>:<port>
   ```

   For example, entering **https://localhost:9443** launches the mangement console that was installed locally using the default port of 9443.

NOTE: If you are using Management Console for Unix with Authentication Services 4.*x*, you can also launch the mangement console from within the Control Center.

1. Select **Management Console** from the left-hand navigation pane of the **Home** page.

Setting up Management Console for Unix

The first time you launch the mangement console, the **Setup One IdentityManagement Console for Unix** wizard leads you through some post-installation configuration steps.

Choose one of these options:

- **Skip the Active Directory configuration, I'll do that later from the console**

  This option allows you to use the core features of the console and limits access to the console to the default *supervisor* account only. See What are the core features of the console on page 18 for details.

- **Walk me through the configuration steps for using AD user accounts for logon to the console**

  When you configure the console for Active Directory, you unlock additional Active Directory features.

  NOTE: To use the mangement console with Authentication Services, or to use roles to allow access to the console using Active Directory, you must configure the console for Active Directory log on.

Choose an option and click **Next**.

NOTE: If you choose the "Skip" option, the **Identify Console** dialog displays. See Identify console on page 32.

If you choose the "Walk" option, it allows you to configure the console for Active Directory log on. See Configure console for Active Directory logon on page 31.

NOTE: If you can not configure the console for Active Directory during your initial installation of Management Console for Unix, choose the "Skip" option. After the installation, log into the console as *supervisor* and configure the console for Active Directory from **System Settings**. See Active Directory configuration on page 165 for details.

Configure console for Active Directory logon

The **Setup Management Console for Unix** wizard opens the **Configure Console for Active Directory Logon** dialog when you choose the **Walk me through the configuration steps for using AD user accounts for logon to the console** option.

To configure the mangement console for Active Directory logon

1. On the **Configure Console for Active Directory Logon** dialog, enter a valid Active Directory domain in the forest, in the form **example.com**.

2. Enter the credentials for an Active Directory account that has log-on rights.

   Enter a sAMAccountName, which uses the default domain or a User Principal Name, as in **username@domain**. The wizard uses these credentials to configure the mangement console for use with Active Directory.

   NOTE: This is a read-only operation; no changes are made to Active Directory.

3. Click **Connect to Active Directory**.

4. When you see the message that indicates the console connected to Active Directory successfully, click **Next**.

   The **Set up console access by role** dialog opens.

Set up console access by role

After you **Configure Console for Active Directory Logon**, the setup wizard displays the **Set up console access by role** dialog.

To add Active Directory users or groups to the console access list

1. On the **Set up console access by role** dialog, click **Add** to specify the Active Directory users and groups that you want to have access to the features available in Management Console for Unix.

2. On the **Select Users and Groups** dialog, use the search controls to find and select Active Directory users or groups. Select one or more objects from the list and click **OK**.

   The mangement console adds the selected objects to the list on the **Set up console access by role** dialog.

   By default the mangement console assigns users to **All Roles**, which gives those accounts permissions to access and perform all tasks within the console. (See Console Roles and Permissions system settings on page 161 for details.)

3. Click in the **Roles** cell to activate a drop-down menu from which you can choose a role for the user account.

   NOTE: During the initial set up, you can only assign one role per user. Add additional roles to a user in **System Settings**. See Adding (or Removing) role

| members on page 164 for details.

4. Click **Next** to save your selections.

    The **Identify Console** dialog opens.

Identify console

The setup wizard displays the **Identify Console** dialog during the post-installation configuration steps. The Authentication Services Control Center uses this information to identify this mangement console. Hosts configured for automatic profiling or automatic QAS agent status also use this information to contact the mangement console server.

To identify the mangement console

1. On the **Identify Console** dialog, modify the information about this mangement console, if necessary, and click **Next** to open the **Set supervisor password** dialog.

    NOTE: You can modify these settings from **Settings | System settings | General | Console Information**. See Console Information settings on page 158 for details.

Set Supervisor Password dialog

The *supervisor* account is the default account for accessing all features of the mangement console. The *supervisor* is a member of all roles and no permissions can be removed from *supervisor*. However, the *supervisor* does not have Active Directory credentials and therefore is blocked from performing Active Directory tasks.

To set the supervisor password

1. On the **Set supervisor password** dialog, enter a password for the *supervisor* account and click **Next**.

    The **Summary** dialog displays.

2. To log on using the console supervisor account, use **supervisor** as the user name.

NOTE: The *supervisor* is the only account that has rights to change the *supervisor* account password in *System Settings*. See Reset the supervisor password on page 206 for details.

Summary dialog

To complete the Management Console for Unix Setup wizard

1. On the **Summary** dialog, click **Finish**.

   The Management Console for Unix log-in screen opens.

Management Console for Unix Log On page

Whenever you launch the mangement console, you must enter an authorized account to proceed. The Management Console for Unix features that are available depend on the account with which you log in.

To use the core version of the mangement console to manage local Unix users and groups and to access system settings, you must use the *supervisor* account (that is, you must log on with the **supervisor** user name). However, to use the Active Directory features of Management Console for Unix, you must log on with an Active Directory account that has been granted access to the mangement console. That is, defined during the post-installation configuration. See Set up console access by role on page 31 for details. To add additional accounts to this access list, see Adding (or Removing) role members on page 164.

To log on to the mangement console

1. Enter the user name and password and click **Sign In**.

   Enter:

   - the **supervisor** account name
   - a sAMAccountName, which uses the default domain
   - a User Principal Name in the form, **username@domain**

   The mangement console opens and displays the user name you specified in the upper right-hand corner of the screen.

2. To log on using a different account, click the authenticated user's login name and click **Sign Out**. Then sign back on using a different account.

   The Log-on page redisplays, allowing you to enter a different account.

Getting Started tab

The first time you start Management Console for Unix, it opens the **Getting Started** tab which describes the new features in mangement console and provides you with a self-

directed introduction to the basics of managing your hosts within the mangement console.

> NOTE: If the **Getting Started** tab does not open, you can access it from the **Help** drop-down menu located in the upper-right corner of the console.

It's simple. Just follow the tasks on the left, in order. As you complete each task your progress is tracked. The right panel explains the procedures that you would do on the mangement console. Click **Next** to go to the next step within a task. Click the ❓ help icon in the upper right-hand corner of the mangement console to access context-sensitive help. For more information, open the help drop-down menu to access the user documentation.

> NOTE: It's important to understand that this is not just a "test drive". You will be adding and configuring a remote host in your environment and adding real data to the database. The only way to restart the *Getting Started* session to repeat the procedures is to stop the service, delete the database, and restart Management Console for Unix.

There are three main tasks: *General*, *Authentication Services*, and *Privilege Manager*.

The *General* task introduces you to the new features of the mangement console since the last release, shows you an overview of the basic console functions, and then directs you to perform these tasks:

1. Add a Host.
2. Profile a Host.
3. Configure Active Directory for Authentication Services; that is, prepare Active Directory to store the configuration settings that it uses.

The *Authentication Services* task introduces you to Authentication Services, and then directs you to perform these tasks:

1. Verify the path to the Authentication Services software on your server.
2. Install the Authentication Services software on the host you set up in the *General* task.

The *Privilege Manager* task introduces you to Privilege Manager for Unix, and then directs you to perform these tasks:

1. Verify the path to the Privilege Manager software on your server.
2. Install the Privilege Manager Policy Server software on the host you set up in the *General* task.
3. Configure the host as a primary policy server.
4. Join a PM Agent or Sudo Plugin host to the policy group,

We hope this experience gives you a quick start to using Management Console for Unix.

Upgrade Quest Identity Manager for Unix

The process for upgrading Identity Manager for Unix to Management Console for Unix is similar to installing it for the first time. The installer detects an older version of the console and automatically upgrades the components.

NOTE: The procedures in this topic assume you have Quest Identity Manager for Unix 1.0.1 or greater installed. If you are upgrading a previous version of Identity Manager for Unix, you must uninstall the web console and do a fresh install of Management Console for Unix; you can not upgrade 1.0.0.

Before you begin the upgrade procedure,

- Delete your browser's cached *Temporary Internet Files* and *Cookies*.
- Close the console and make a backup of your database, as explained in step 1.

To upgrade Identity Manager for Unix to Management Console for Unix

1. Backup the 1.0.*x* database files:

    a. Shutdown the service. See Start/stop/restart Management Console for Unix service on page 215 for details.

        NOTE: The mcu_service was called the imu_service in the Identity Manager for Unix 1.0.x console.

        Management Console for Unix uses a HSQLDB (Hyper Structured Query Language Database) to store its data such as information about the hosts, settings, users, groups, and so forth.

    b. Copy the `/var/opt/quest/imu` data directory to a backup location.

        NOTE: Refer to Database maintenance on page 237 for more information about the database locations and filenames.

    c. After backup is complete restart the service. See Start/stop/restart Management Console for Unix service on page 215 for details.

        Once you backup the database files, you are ready to start the upgrade.

2. To start the upgrade, follow the instructions for a first-time installation. See the *Installing and Uninstalling* topic for your platform under Installing the Management Console on page 25 to start the installation procedure.

    When the installer detects a previous version of the mangement console is already installed, it asks if you want to continue.

3. Click **Yes** at the **Install Management Console for Unix** dialog.

    The **Install Management Console for Unix** dialog displays.

4. Accept the terms of the license agreement and click **Next**.

5. Modify the installation directory path, if necessary, and click **Next**.

6. Modify the default SSL (https) and Non-SSL (http) port numbers, if necessary, and click **Install**.

   The installation wizard installs Management Console for Unix 2.*x* and upgrades the database.

7. When the installer asks if you want to uninstall the previous version of the console, you can opt to leave the older version installed and continue the 2.*x* installation.

   Once you are satisfied with the upgrade, you can uninstall the previous version at a later time. See the *Installing and Uninstalling* topic for your platform under Installing the Management Console on page 25 for details about the uninstall procedure.

   > NOTE: While you can have both the older and the newer versions of the mangement console installed, you can not run both at the same time.

8. On the **Complete** dialog, select the **Launch the Management Console** option and click **Finish**.

9. Log into the mangement console as *supervisor* to complete the post-upgrade configuration.

   You can not login as an Active Directory user until you log in as *supervisor* and reassign your Active Directory accounts to specific roles.

10. On the **Complete Upgrade** dialog, enter your Active Directory credentials and click **Continue** to perform the post-upgrade configuration.

    After upgrading from 1.0.x, Active Directory accounts are assigned to the **Manage Host** role. To assign Active Directory users to other roles, log in to the console as *supervisor* and go to **Settings | System Settings | Console Roles and Permissions**. See Adding (or Removing) role members on page 164 for details.

11. On the **Summary** dialog, click **Logout** to log back in using an Active Directory account or click **Close** to open the mangement console with the *supervisor* account.

NOTE: After an upgrade from version 1.0.x to 2.x, please note the following:

- Passwords cached by the *supervisor* account or AD users with console access were not migrated during the upgrade process due to changes in encryption. Users will have to re-enter their passwords for hosts they manage the next time they perform tasks on the hosts, and choose to cache their credentials again on the server.

- It is important to re-profile all hosts after an upgrade of any version of Management Console for Unix.

- Existing Active Directory users and groups granted access to the mangement console are added to the **Manage Hosts** role, giving them access to the features they had before the upgrade.

- Because the encryption mechanism was changed, cached host credentials (that is, passwords cached by the *supervisor* account or Active Directory users with console access) are not migrated when you upgrade from 1.0.x to 2.x. Users will have to re-enter their passwords for hosts they manage the next time they perform tasks on the hosts and choose to cache them again on the server.

- The host address in the **Console host address** box on the **Console Information** settings may have been entered as a simple address in version 1.0.x. To perform some tasks in without error, such as auto-profiling, the **Console host address** must be a Fully Qualified Domain Name.

Reset custom configuration settings

When upgrading from version 1.0.x to 2.x or higher, there are some steps you must take to reset any custom configuration settings you had in the previous version.

The upgrade procedure makes a `.bak` copy of your configuration file (`jvmargs.cfg.bak`) at the root of your installation directory. After you upgrade the mangement console from version 1.0.*x*, to reset any custom configuration settings you may have made in the previous version, compare the `jvmargs.cfg.bak` file with the new `jvmargs.cfg` file to see if you had any custom settings. For example, if you had increased the JVM Memory size in the previous version, you must add the JVM Memory setting argument to the `custom.cfg` file. See Setting custom configuration settings on page 208 for more information about customizing configuration settings for the mangement console.

NOTE: Do not change the `jvmargs.cfg` directly; the settings in the `custom.cfg` file always take precedence over the default settings in `jvmargs.cfg`. And, next time you upgrade Management Console for Unix, changes in the `jvmargs.cfg` file will be overwritten.

Upgrade Management Console for Unix

The process for upgrading Management Console for Unix from an older version is similar to installing it for the first time. The installer detects an older version of the console and automatically upgrades the components.

NOTE: The procedures in this topic assume you have Management Console for Unix 2.0.x or greater installed.

Before you begin the upgrade procedure, review the upgrade notes in the release notes, close the console and make a backup of your database, as explained in step 1.

To upgrade Management Console for Unix

1. Backup the database files:

   a. Shutdown the service. See Start/stop/restart Management Console for Unix service on page 215 for details.

   Management Console for Unix uses a HSQLDB (Hyper Structured Query Language Database) to store its data such as information about the hosts, settings, users, groups, and so forth.

ONE IDENTITY™

b. Copy the `/var/opt/quest/mcu` data directory to a backup location.

   Refer to Database maintenance on page 237 for more information about the database locations and filenames.

c. After backup is complete restart the service. See Start/stop/restart Management Console for Unix service on page 215 for details.

   Once you backup the database files, you are ready to start the upgrade.

2. To start the upgrade, follow the instructions for a first-time installation. See the *Installing and Uninstalling* topic for your platform under Installing the Management Console on page 25 to start the installation procedure.

   When the installer detects a previous version of the mangement console is already installed, it asks if you want to continue.

3. Click **Yes** at the **Install Management Console for Unix** dialog.

4. Accept the terms of the license agreement and click **Next**.

5. Modify the default SSL (https) and Non-SSL (http) port numbers, if necessary, and click **Install**.

   The installation wizard uninstalls the old version and configures the server database and service.

NOTE: After an upgrade from any version of Management Console for Unix, it is important to re-profile all managed hosts.

Preparing Unix hosts

The mangement console provides a central management and reporting console for local Unix users and groups.

Whether you have the core version of the mangement console or are managing hosts with Authentication Services or Privilege Manager for Unix, once you have successfully installed Management Console for Unix, you must first add your hosts to the console, and then profile them to gather system information. Once a host is added and profiled you can then manage users and groups on the hosts and run reports.

NOTE: Installing Authentication Services on hosts that you manage with the console unlocks many additional features for managing Unix systems with Active Directory, such as Active Directory user management and Access and Privileges reports.

Installing Privilege Manager on hosts that you manage with the console allows you to view and edit centrally stored policies, as well as search and replay keystroke logs. See What are the core features of the console on page 18 for a list of these additional features.

Adding hosts to the Management Console

In order to manage a Unix host from the mangement console, you must first add the host. Go to the **Hosts** tab of the mangement console to either manually enter hosts or import them from a file.

To add hosts to the mangement console

1. Click the **Add Hosts** toolbar button to display the **Add Hosts** dialog.

2. To manually add one or more hosts, enter the FQDN, IP address, or short name of a host you want to add to the mangement console and either click the **Add** button or press **Enter**.

   Once added, the **Host** column displays the value you enter. The mangement console uses that value to connect to the host. You can rename the host if it has not been profiled using the **Rename Host** command on the **Host** panel of the toolbar. After a host is profiled the only way to change what is displayed in the **Host** column is to

remove the host from the console and re-add it. For example, if you add a host by its IP address, the IP address displays in the **Host** column (as well as in the **IP Address** column); to change what is displayed in the **Host** column, you must use the **Remove from console** toolbar button to remove the host from the console; then use the **Add Hosts** button to re-add the client by its host name. If you had profiled the host before removing it, you will have to re-profile it after re-adding it.

3. To add hosts from a *known_hosts* file, click the **Import** button.

   a. On the **Import hosts from file** dialog, browse to select a .txt file containing a list of hosts to import.

      Once imported, the host addresses display in the **Add Host** dialog list.

      NOTE: The valid format for an import file is:

      - .txt file - contains the *IP address* or *DNS name*, one per line
      - known_hosts file - contains *address algorithm hostKey* (separated by a space), one entry per line

      See Known_hosts file format on page 188 for more information about the supported *known_hosts* file format.

4. Once you have a list of one or more hosts to add, if you do not wish to profile the hosts at this time, clear the **Profile hosts after adding** option.

   NOTE: If you add more hosts to the list than selected in the *Rows to show* drop-down menu in the *View* panel of the toolbar, this option is disabled.

5. If you do not clear the **Profile hosts after adding** option on the **Add Hosts** dialog, when you click **OK**, the **Profile Host** dialog prompts you to enter the user credentials to access the hosts. (Refer to Profiling hosts on page 41 which walks you through the host profile steps.)

6. If you clear the **Profile hosts after adding** option on the **Add Hosts** dialog, when you click **OK**, the **Add Hosts** dialog closes and control returns to the mangement console.

   The mangement console lists hosts that were successfully added on the **All Hosts** view by the FQDN, IP address, or short name of the hosts you entered on the **Add Hosts** dialog.

Renaming hosts

NOTE: You can only rename a host that has not been profiled.

To rename hosts

1. Select a host on the **All Hosts** view and click **Rename Host** from the **Host** panel of the toolbar.

2. In the **Rename Host** dialog, enter the FQDN, IP address or short name to use to connect to that host.

3. Optionally, you can clear the **Profile host now** option.

4. Click **OK**.

If the **Profile host now option** option was selected, the mangement console starts the *Profile Host* procedure. See for details.

Profiling hosts

Profiling imports information about the host, including local users and groups, into the mangement console. It is a read-only operation and no changes are made to the host during the profiling operation. Profiling does not require elevated privileges.

To profile hosts

1. Select one or more hosts on the **All Hosts** view and click **Profile** from the **Prepare** panel of the toolbar, or open the **Profile** menu and choose **Profile**.

2. In the **Profile Host** dialog, enter user credentials to access the hosts.

   If you selected multiple hosts, you are asked if you want to use the same credentials for all the hosts (default) or enter different credentials for each host.

3. If you selected multiple hosts and the **Use the same credentials for all selected hosts** option, enter the following information:

   a. Enter the user name and password to log onto the selected hosts.

   b. (Optional) Enter the SSH port to use. It uses port 22 by default.

   c. To save the credentials entered for the host, select the **Save my credentials on the server** option.

      Once saved, the mangement console uses these credentials to access the host during this and subsequent sessions.

   NOTE: If you do not save a password to the server, the user name and password fields will be blank the first time the mangement console needs credentials to complete a task on the host during a log on session. Once entered, the mangement console caches the user name and password and reuses these credentials during the current session, and pre-populates the user name and password fields in subsequent tasks during the current log on session.

   If you choose to save a host's credentials to the server, the mangement console encrypts the credentials and saves them in the database. Saved user names and passwords persist across log on sessions, and when needed, the mangement console pre-populates the user name and password fields the first and subsequent times it needs them to perform a task. See Caching Unix host credentials on page 189 for more information.

4. If you selected multiple hosts and the **Enter different credentials for each selected host** option, a grid displays allowing you to enter different credentials and specify different settings for each host.

a. To enter different credentials, place your cursor in the **Username** and **Password** columns to the right of the **Host** column and enter the credentials to use.

b. To change the SSH port for a host, place your cursor in the **SSH Port** column and enter the new SSH port number.

c. To save the credentials entered for a host, select the check box in the **Save** column.

5. If you want the mangement console to prompt you to review and accept new SSH keys for the selected hosts (that do not have previously cached SSH keys), clear the **Automatically accept SSH keys** option before you click **OK**.

   NOTE: When profiling one or more hosts, you must accept at least one key before continuing. The mangement console only profiles hosts with accepted keys.

   By default the **Automatically accept SSH keys** option is checked. This enables the mangement console to automatically accept SSH key for all selected hosts that do not have a previously cached key. When it accepts the key, the console adds it to the accepted-keys cache on the Management Console for Unix server. If you clear the **Automatically accept SSH keys** option, when the mangement console encounters a modified key, it opens the **Validate Host SSH Keys** dialog, allowing you to manually accept keys that are encountered. Once you have manually verified the fingerprint, the console adds the SSH host keys to the accepted-keys cache.

   NOTE: Once you profile a host, all future tasks that involve an SSH connection will verify the SSH host key against the accepted-keys cache. When profiling, if the console encounters a modified key, the profile task prompts you to accept new or changed keys. When performing any other SSH action, other than profile, if the console encounters a different SSH key, the task will fail. To update the accepted-keys cache for the host, you can either profile or re-profile the host, accept the new key, and try the task again. Or, you can import a new SSH host key from the host's properties or from the **All Hosts** view.

   See Importing SSH host key on page 57 or Managing SSH host keys on page 187 for more information.

A progress bar displays in the **Task Progress** pane. The final status of the task displays, including any failures or advisories encountered.

Automatically profiling hosts

To keep the Management Console for Unix database up to date with accurate information about users, groups, and One Identity products, you can configure the mangement console to profile hosts automatically.

BEST PRACTICE: As a best practice, configure newly added hosts for auto-profiling before you perform any other actions so that the mangement console dynamically updates user and group information. See UID or GID conflicts on page 218.

Configuring a host for auto-profiling sets up a cron job on the client that runs every five minutes. If it detects changes on the host, it triggers a profile operation.

The cron job detects changes to the following:

- local users, groups, or shells
- installed Authentication Services or Privilege Manager software
- Authentication Services access control lists
- Authentication Services mapped user information
- Privilege Manager configuration
- Authentication Services configuration
- Privilege Manager licenses

The cron job also sends a heartbeat every day. This updates the **Last profiled** date displayed on the host properties. If the **Last profiled** date is more than 24 hours old, the host icon changes to ![icon] to indicate no heartbeat.

To configure automatic profiling

1. Select one or more hosts on the **All Hosts** view, open the **Profile** menu from the **Prepare** panel of the toolbar, and choose **Profile Automatically**

   NOTE: The **Profile Automatically** option is only available for multiple hosts if all hosts are in the same 'Auto-profile' state; that is, they all have 'Auto-profile' turned on, or they all have 'Auto-profile' turned off.

2. In the **Profile Automatically** dialog, select the **Profile the host automatically** option.

3. Choose the user account you want to use for profiling, either:

   a. **Create a user service account on the host**

      When you choose to create the user service account on the host, if it does not already exist, the mangement console, does the following:

      i. Creates "questusr", the user service account, and a corresponding "questgrp" group on the host that the mangement console uses for automatic profiling.

      ii. Adds *questusr* as an implicit member of *questgrp*.

      -OR-

   b. **Use an existing user account (user must exist on all selected hosts)**

      (Click **Select** to browse for a user.)

4. Click **OK** on the **Profile Automatically** dialog.

   Whether you choose to create the user service account or use an existing user account, the mangement console,

   - Adds the user account (the "questusr" or your existing user account) to the `cron.allow` file, if necessary. For example, the console takes no action if the `cron.allow` file does not already exist, but there is a `cron.deny` file:

     When the user is added to the cron.allow file:

cron.allow	cron.deny	Console's action	Resultant User Access
NO	NO	Creates `cron.allow` and adds root and *questusr* to it	Both root and *questusr* have access.
NO	YES	No action	All users have access except those in `cron.deny`; *questusr* has access unless explicitly denied.
YES	NO	Adds *questusr* to `cron.allow`	Users in `cron.allow` have access.
YES	YES	Adds *questusr* to `cron.allow`	Users in `cron.allow` have access unless in `cron.deny`.

- Adds a cron job to the *questusr* account to execute `chgfmon` utility that monitors changes. `chgfmon` logs change events to syslog.
- Creates a second cron job to monitor the host connectivity to the server.
- Adds the auto-profile SSH key to *questusr*'s authorized_keys, `/var/opt/quest/home/questusr/.ssh/authorized_keys`.
- Verifies the user service account can login to the host.

NOTE: If you receive an error message saying you could not log in with the user service account, please refer to Service account login fails on page 208 to troubleshooting this issue.

The *questusr* account is a non-privileged account that does not require root-level permissions. This account is used by the console to gather information about existing user and groups in a read-only fashion, however, the mangement console does not use *questusr* account to make changes to any configuration files.

If *questusr* is inadvertently deleted from the console, the console turns 'Auto-profiling' off.

To recreate the "questusr" account,

a. Re-profile the host.

b. Reconfigure the host for automatic profiling.

5. On the **Log on to Host** dialog, enter the user credentials to access the selected hosts and click **OK**.

NOTE: This task requires elevated credentials.

If you select multiple hosts, you are asked if you want to use the same credentials for all the hosts (default) or enter different credentials for each host.

a. If you selected multiple hosts and the **Use the same credentials for all selected hosts** option, enter your credentials to log on to access the selected

hosts and click **OK**.

b. **selected host** option, it displays a grid which allows you to enter different credentials for each host listed. Place your cursor in a cell in the grid to activate it and enter the data.

To disable automatic profiling

1. Select one or more hosts on the **All Hosts** view and choose **Profile Automatically**

2. Clear the **Profile the host automatically** option and click **OK**.

3. On the **Log on to Host** dialog, enter the user credentials to access the selected hosts and click **OK**.

When you disable auto-profiling for a host, the mangement console,

1. leaves the "questusr" and the corresponding "questgrp" accounts on the host, if they were previously created.

2. leaves *questusr* as an implicit member of *questgrp*, if it exists.

3. removes the user account (the "questusr" or your existing user account) from the `cron.allow` file.

4. removes the auto-profile SSH key from that user's `authorized_keys` file.

Viewing the auto-profile status

You can view the automatic profile failures or warnings on the **Host Notification** tab.

To view the auto-profile status

1. From the **Host Notifications** tab, select the **Auto-Profile Status** tab.

   NOTE: If the **Host Notifications** tab is not currently available on the mangement console, open the **Open views** menu from the Tab bar (represented by a "tab" icon ▬) and choose the **Host Notifications** option.

   The **Auto-Profile Status** tab displays the following alert for hosts where there has been a failure to auto-profile:

   ⚠ - Auto-profile failed

2. To re-profile or re-set the auto-profile settings for one or more hosts, select the hosts on the **Auto-Profile Status** tab, open the **Profile** menu from the toolbar, and choose either **Profile** or **Profile Automatically**.

   NOTE: The **Profile Automatically** option is only available for multiple hosts if all hosts are in the same 'Auto-profile' state; that is, they all have 'Auto-profile' turned on, or they all have 'Auto-profile' turned off.

Viewing the auto-profile heartbeat errors

When configured for automatic profiling, the host sends a heartbeat every 24 hours. If the server does not receive a heartbeat in over 24 hours, it displays an alert on the **Auto-Profile Heartbeat** tab.

To view auto-profile heartbeat notifications

1. From the **Host Notifications** tab, select the **Auto-Profile Heartbeat** tab.

   The **Auto-Profile Heartbeat** tab displays alerts for hosts where a auto-profile heartbeat has not been reported in the last 24 hours using this icon:

    - Profiled, but no heartbeat in last 24 hours

Checking readiness

Once you add and profile hosts, the mangement console allows you to perform a series of tests to verify that a host meets the minimum requirements to configure a policy server or join a remote host to either a Privilege Manager policy group or an Active Directory domain. Running the readiness checks does NOT require elevated privileges.

To check readiness

1. Select one or more hosts on the **All Hosts** view of the **Hosts** tab.

2. Open the **Check** menu from the **Prepare** panel of the task bar and choose

   a. Check Policy Server Readiness

   b. Check Client for Policy Readiness

   c. Check Host for AD readiness

   d. Check QAS agent status

   e. Check QAS agent status automatically

   NOTE: You must add and profile a Privilege Manager Policy Server to the mangement console and set it as **Active** before the **Check Client for Policy Readiness** option is available on the **Check** menu.

   You must be logged on as the *supervisor* or an Active Directory account in the **Manage Hosts** Role to perform any task on the **Check** menu.

   See the following topics for more information about these options:

   - Checking policy server readiness on page 108
   - Checking client for policy readiness on page 114
   - Checking host for AD readiness on page 84

- Check QAS Agent Status on page 93
- Automatically checking QAS agent status on page 94

Working with host systems

Management Console for Unix simplifies local host management on Unix, Linux, and Mac systems.

Install software on hosts

Once a you have successfully added and profiled one or more hosts, you can remotely deploy software products to them from the mangement console.

The **Install Software** dialog displays when you select the **Install Software** toolbar button.

From this dialog, select the software products you want to deploy and install on the selected hosts.
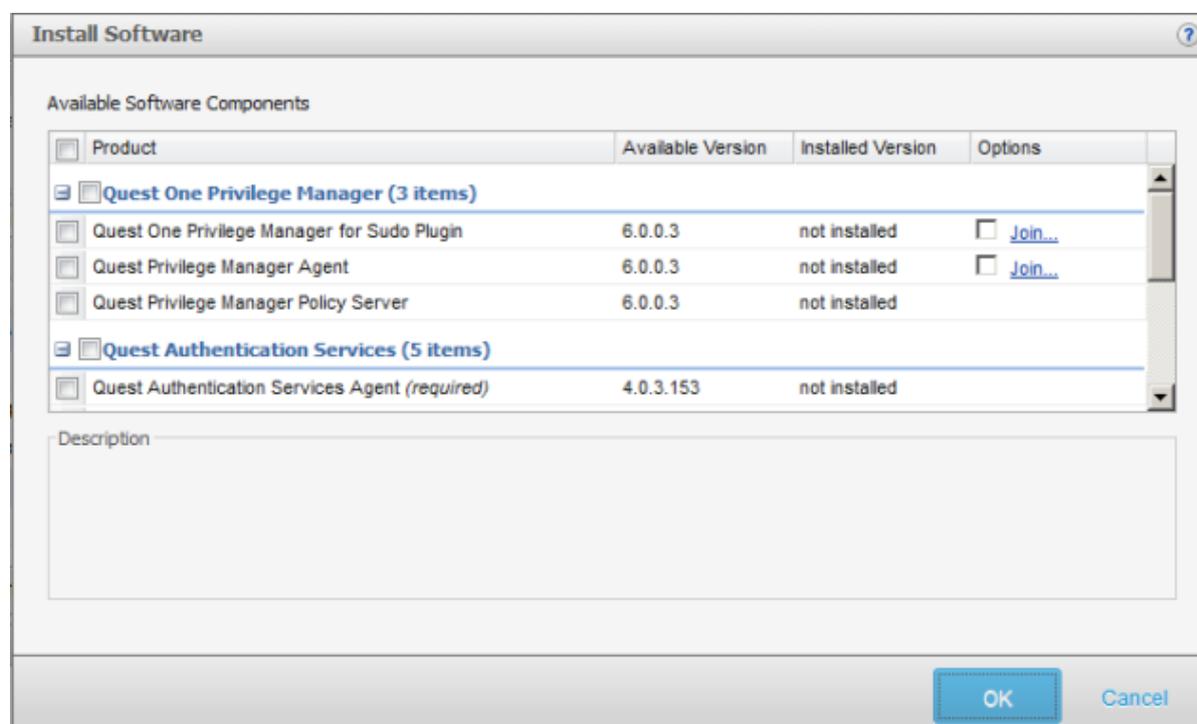
NOTE: If you do not see all of these software packages, verify that the path to the software packages is correctly set in **System Settings**. Refer to:

- Setting Authentication Services software path on page 82
- Setting the Privilege Manager software path on page 172.

Available software components

You can install the following software products remotely from the mangement console:

- **Privilege Manager (3 items)**

  - **Sudo Plugin** - Select to install a component that enables the host to use a centrally managed sudoers policy file located on the Privilege Manager primary server from the mangement console.

    NOTE: Before installing the **Sudo Plugin**, please see Configuring a service account on page 169.

  - **Privilege Manager Agent** - Select to install a component that enables the host to use a centrally managed pmpolicy policy file located on the primary policy server from the mangement console.

    NOTE: Before installing the **Privilege Manager Agent**, please see Configuring a service account on page 169.

  - **Privilege Manager Policy Server** - Select to install the Privilege Manager Policy Server which provides central policy management, granular access control reporting, as well as the ability to enable, gather, store and playback keystroke logs.

    NOTE: Centralized policy management and keystroke logging are licensed separately.

  NOTE: When you install the **Privilege Manager Policy Server** it installs all three Privilege Manager for Unix packages on that host. However, once you have installed the Sudo Plugin onto a remote host, the mangement console will not allow you to install the PM Agent on that host; and once you have installed the PM Agent onto a remote host, the mangement console will not allow you to install the Sudo Plugin on that host.

- **Authentication Services (5 items)**

  - **Authentication Services Agent (*Required*)** - Select to allow Active Directory users access to selected host. Authentication Services provides centralized user and authentication management. It uses Kerberos and LDAP to provide secure data transport and an authentication framework that works with Microsoft Active Directory. Components include: vasd, nss_vas, pam_vas, and vastool.

  - **Authentication Services for Group Policy (*Required*)** - Select to install the Group Policy component which provides Active Directory Group Policy support for Unix, Linux, and Mac platforms.

- **Authentication Services for NIS** - Select to install the NIS Proxy component which provides the NIS compatibility features for Authentication Services. `vasyp` is a NIS daemon that acts as a `ypserv` replacement on each host.

- **Authentication Services for LDAP** - Select to install the LDAP Proxy component which provides a way for applications that use LDAP bind to authenticate users to Active Directory without using secure LDAP (LDAPS). Instead of sending LDAP traffic directly to Active Directory domain controllers, you can configure applications to send plain text LDAP traffic to `vasldapd` by means of the loopback interface. `vasldapd` proxies these requests to Active Directory using Kerberos as the security mechanism.

- **Dynamic DNS Updater** - Select to install the Dynamic DNS Updater component which provides a way to dynamically update host records in DNS and can be triggered by DHCP updates.

- **Defender (1 item)**

  - **Defender PAM Module** - Select to install the Defender authentication components for PAM based Unix/Linux systems. Includes PAM module, documentation and utilities to appropriately configure the PAM subsystem for Active Directory/Defender OTP authentication.

For more information about installing software components:

- See Installing the Privilege Manager packages on page 109 for general information about installing the Privilege Manager components.

- See Configuring a secondary policy server on page 113 for details about installing a Secondary Policy Server.

- See Installing Privilege Manager agent or plugin software on page 116 for details about installing Privilege Manager client packages.

- See Installing Authentication Services software packages on page 87 for details about installing the Authentication Services packages.

Using the console search options

Management Console for Unix provides both basic and advanced search options to help you find and select hosts from the **All Hosts** view or user accounts from the **All Local Users** tab.

Performing a basic search

To search for hosts on the **All Hosts** view based on the values in any of the mangement console columns, use the **Search for hosts** box under the toolbar. To search for users on the **All Local Users** tab based on the values in any of the columns on that view, use the **Search for users** box.

To perform a basic search

1. Place your cursor in the **Search** box and enter one or more characters. As you enter characters into the search field, the mangement console displays only the items that contain the search criteria. For example, if you enter the letter "a", the console displays all items that have the letter "a" in one of the columns.

   NOTE: You cannot use wildcards in basic search strings.

2. Optionally, to sort within the displayed items, click a column title to arrange it into either ascending or descending order.

3. To clear the search and display all items, click the ☒ to the right of the **Search for hosts** box.

Using the advanced search options

Use the **Advanced Search Options** to search for hosts or users based on various property values.

To use the advanced search options

1. Click the ☒ arrow icon next to the **Search** box to open the advanced search options.

   NOTE: The advanced search button toggles to expand or collapse based on its current state.

   All Hosts view Advanced Search Options

   When you expand the **All Hosts** view advanced search options, it displays four search fields.

   By default, the search field labels are the first four column titles:

   - Host
   - IP Address
   - OS
   - Version

   Each search field has a drop-down menu that allows you to change the search criteria to search for information in another available column:

   - Joined to Domain
   - Version
   - Joined to Policy Group

   All Local Users tab Advanced Search Options

   When you expand the **All Local Users** tab advanced search options, it displays four search fields. By default, the search field labels are the first four column titles:

- Name

- UID

- Comment (GECOS)

- Host

Other available advanced search options on the **All Local Users** tab are:

- AD User

- GID

- Home Directory

- Joined Domain

- Login Shell

NOTE: You can choose to display or hide these columns from view. Open any column menu, navigate to **Columns**, and select the columns you want available. If you do not see the items you searched for, it may be because that column is hidden.
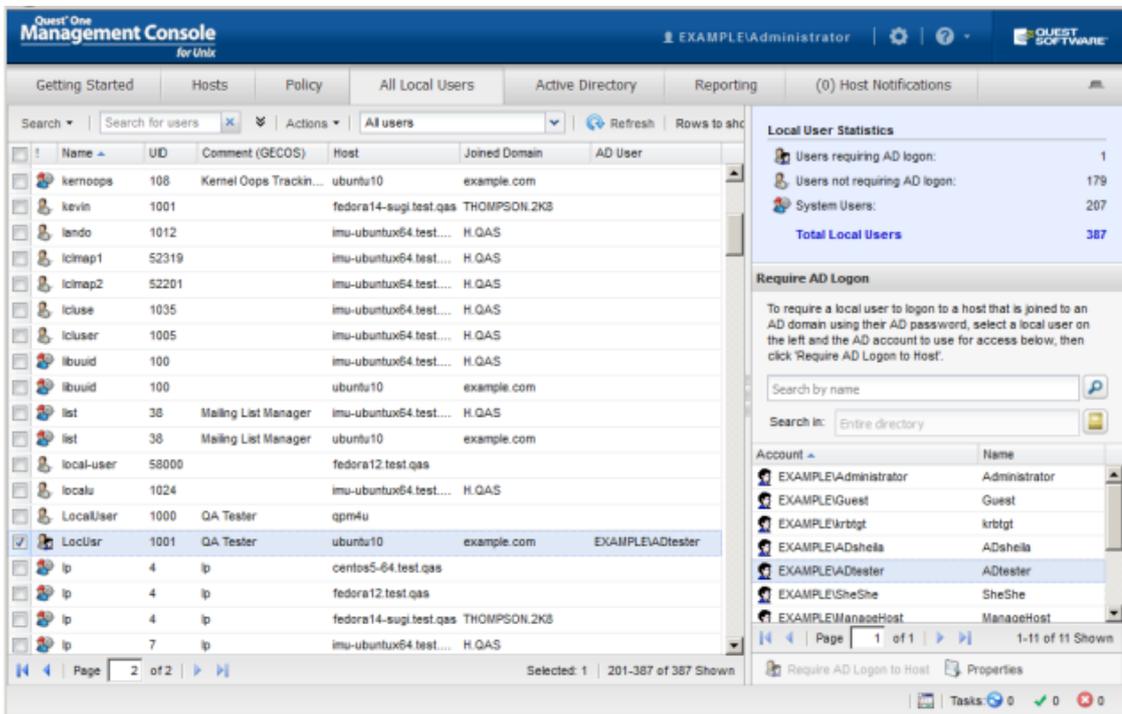
2. Set the search field labels and enter search criteria into the text boxes.

   NOTE: **SEARCH TIPS**

   Wildcards: You can use wildcards in text strings, such as * and ?. If the text string actually contains one of these characters, precede the character with the backslash (\) escape character.

   Ranges: You can specify a range of positive or negative numbers using a colon (:) as a range separator character. For example, to search for all users with UIDs

from 0 to 499, enter **0:499** in the **Search** box. You cannot use wildcards in numbers.

Groups: You can search for more than one text string or more than one number range. For example,

- From the **All Hosts** view, you can find all hosts that match these strings:

    Host ▾ | fedora*,linux

    Separate multiple names with a comma; do not add extra spaces.

- From the **All Local Users** tab, you can find all the users in the following **UID** ranges on all managed hosts:

    UID ▾ | 0:499,501,555:600

    Separate multiple number ranges with a comma; do not add extra spaces.

3. Optionally, to sort within the displayed items, click a column title to arrange it into either ascending or descending order.

4. To clear the search, click the ✕ to the right of the **Search** box.

NOTE: As you type search criteria into the text boxes, the top-level **Search** box reflects the values you specify for searching.

Note that spaces display as question marks (?), as in: Search ▾ | host=Red?Hat ✕

As you become more familiar with the search query syntax, you can type your query directly into the *Search* box instead of using the search fields. For example,

- On the **All Hosts** view, to search for hosts with "red" as part of the operating system, type **os=red*** into the **Search** box or to search for hosts that have Authentication Services 4.0 installed, type **qasversion=4.0***.

- On the **All Local Users** tab, to search for users with a Group Identification Number (GID) of "100", type **gid=100**.

Saving search criteria

You can save search criteria for reuse later and manage the list of saved searches. The mangement console saves searches on a per-user basis; it does not save system-wide searches.

To save search criteria for reuse later

1. Open the **Search** menu and choose **Save search**.

2. Enter a name for the search and click **OK**.

    It adds the new search to the **Search** menu.

To use a saved search

1. Open the **Search** menu and choose a saved search.

Removing saved searches

To remove a saved host search

1. Open the **Search** menu and choose **Saved searches**.
2. From the **Saved Searched** dialog, select one or more saved searches and click **Remove**.
3. Click **OK** to save your changes and return to the mangement console.

Filtering All Hosts view content

By default, all of the managed hosts display on the **All Hosts** view regardless of their status or state. You can filter the hosts listed in the **All Hosts** view by using filters.

Each column has a drop-down menu from which you can choose which columns you want to view on the mangement console. In addition, the drop-down menus for the two *state* columns (represented by the exclamation points), **Joined to Domain**, and **Status** columns allow you to filter the items displayed by various criteria.

- Use the **Host state** column drop-down menu to filter the hosts by profiled or heartbeat state.
- Use the **Authentication Services state** column drop-down menu to filter the hosts QAS agent status.
- Use the **Installed state** column drop-down menus to filter the hosts by type of Privilege Manager product.
- Use the **Status** column drop-down menus to filter the hosts by "joined" or "ready" state.

NOTE: When you set a filter for one of these columns, the mangement console italicizes and bolds the column heading.

1. To filter the hosts by profiled or heartbeat state, open the **Host status** column drop-down menu, navigate to **Filters** and choose one of the following options:
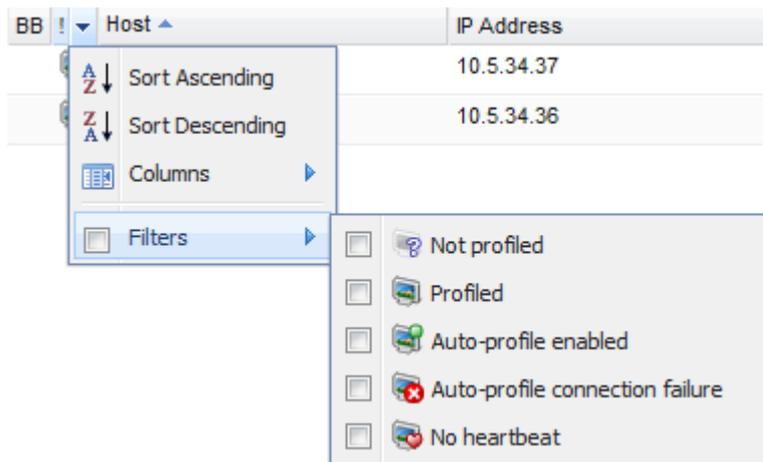
2. To filter the hosts by QAS Agent Status, open the **Authentication Services state** column (next to the *Version* column), navigate to **Filters** and choose one of the following options:
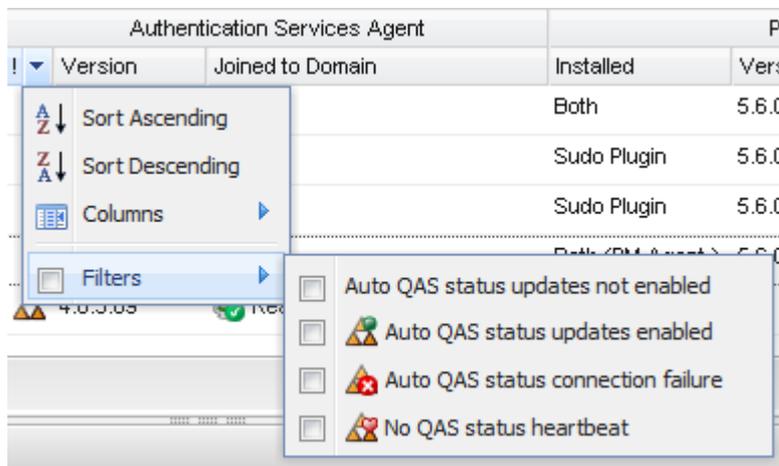
3. To filter the hosts by the type of Privilege Manager product installed: Sudo Plugin, PM Agent, or Server, open the **Installed** column drop-down menu, navigate to **Filters** and choose one of the following options:
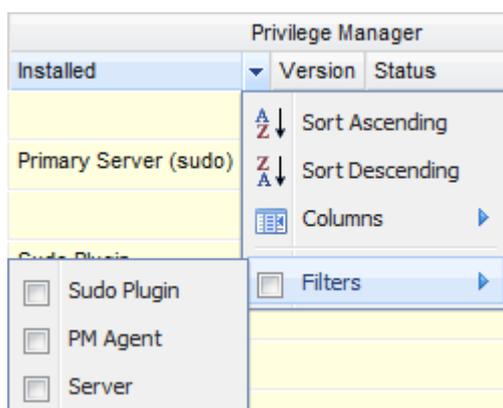
NOTE: When you select a filter, only the hosts that match that criteria display.

However, when you install the **Privilege Manager Policy Server** it installs all three Privilege Manager for Unix packages on that host. Thus, if you filter by either the PM Agent or the Sudo Plugin, the console displays all the server hosts, as well.

4. To filter the Privilege Manager hosts by "joined" or "ready" state, open the **Status** column drop-down menu, navigate to **Filters** and choose one of the following options:
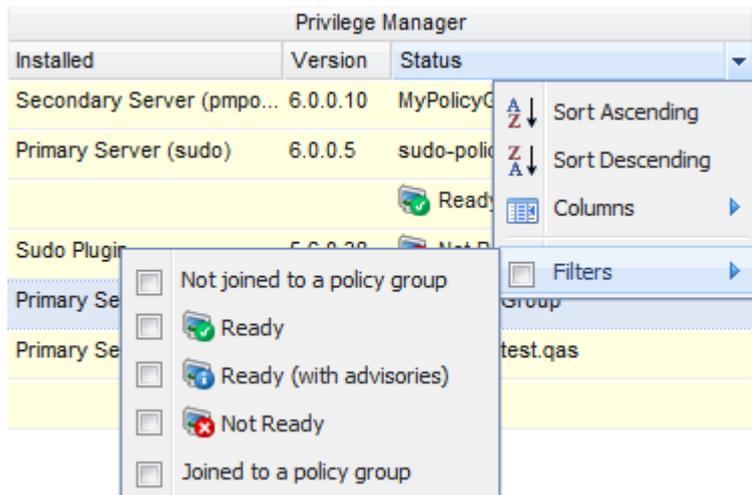
NOTE: When you select a filter, only the hosts that match that criteria display. It is important to understand that when you set multiple filters, the console only displays the hosts that meet all of the criteria you have selected.

If you want the mangement console to temporarily ignore the filter options for a column, clear the **Filters** option box in the drop-down menu. Then, re-select the **Filters** option, to re-enable those filter settings.

To clear host filters, deselect the individual options or click the **Clear column filters** button in the **View** pane of the task bar.

Reviewing host properties

Once you add and profile a host you can review the system, user, and group information, as well as the current status of the host.

To review host properties

1. Select the host and click the **Properties** toolbar button from the **Host** panel of the toolbar.

   NOTE: You can also double-click a host name to open its **Properties** or right-click the host and choose **Properties** from the context menu.

2. The mangement console adds a tab to the **All Hosts** view for the selected host with these tabs:

- Details

- Users

- Groups

- Readiness Check Results

- Software

- Host Access Control (console must be configured for AD and host must be joined to AD)

3. To close a host properties, click the close button ![x] in the right-hand corner of the host's properties.

Removing hosts from Management Console

Removing a host means that you will no longer be able to access information about the host or manage the host's local users and groups from the mangement console. The host is removed from the database, but this does not change the configuration of the Authentication Services Agent, PM Agent, or Sudo Plugin host, or prevent further Active Directory log on.

To remove hosts from mangement console

1. Select one or more hosts from the **All Hosts** view and click the **Remove Host** toolbar button.

2. Confirm you want to remove the selected hosts from the mangement console.

   Once removed, the mangement console no longer lists the Unix hosts on the **All Hosts** view. In addition, associated users and groups for these hosts are removed from the mangement console and you will lose the system user markings identified for any of these users.

Importing SSH host key

You can upload a new SSH key and replace the one that is cached for a host on the server by importing an SSH host key.

To import SSH host key

1. Select a managed host from the **All Hosts** view and click the **Import SSH Host Key** toolbar button.

2. At the **Import SSH host key from file** dialog, browse to select an SSH host key

file.

See Known_hosts file format on page 188 for details.

For more information, see Managing SSH host keys on page 187.

ONE IDENTITY™

Managing local groups

The profiling operation imports system information about the local groups so you can remotely manage them through the mangement console.

A host's properties contains a **Groups** tab, from which you can manage the local groups.

The topics in this section step you through the local group management tasks you can perform from the **Groups** view. For a detailed description of these tasks, please refer to the online help.

Adding a local group

You can use the mangement console to remotely add a local group to the host.

> NOTE: This topic instructs you to set up a local group by the name of "localgroup" referred to by other examples in this guide.

To add a local group to the host

1. From the **All Hosts** view, double-click a host name to open its properties.

2. Select the **Groups** tab and click **Add Group**.

3. In the **Add New Group** dialog, enter **localgroup** as a local group name in the **Group Name** box and click **Add Group**.

4. In the **Log on to Host** dialog, enter your credentials and click **OK**.

   > NOTE: This task requires elevated credentials. Credential information is entered by default from the cache.

   The new local group account is added to the system and mangement console.

Searching for groups

Use the **Search for groups** control to search for a particular group or groups on a host's **Groups** tab.

To search for groups

1. Place your cursor in the **Search for groups** box and enter one or more characters. As you enter characters into the text box, the mangement console displays the groups whose name matches (contains) the criteria entered.

2. To clear the text box and redisplay the original groups list, click the ☒ to the right of the search box.

Modifying a local group's properties

Modify the general properties of a local Unix group from the **Groups** tab of a host's properties.

To modify a local group's properties

1. Right-click the group name and choose **Properties**.

   You can also double-click a group from the list to open its properties.

2. On the **General** tab of the group's properties, modify the group information.

3. On the **Members** tab, add or remove users from the local group.

4. Click **OK**.

5. On the **Log on to Host** dialog, enter the user credentials and click **OK**.

   NOTE: This task requires elevated credentials.

Adding users to a local group

Add local or Active Directory users to a local group from a local group's properties.

To add users to a local group

1. From the **Groups** tab on the host's properties, right-click a group name and choose **Properties**.

   You can also double-click the group name to open its properties.

2. Select the **Members** tab, open the **Add** menu and choose **Local user**.

   NOTE: The **AD user** option is only available when you are logged in as an Active Directory user for a host that is joined to Active Directory. See Adding AD user to a local group on page 97 for details.

3. On the **Select Local User** dialog, search for and select a local user from the list and click **OK**.

   NOTE: To find a particular user you can filter the list of users. Enter one or more

characters in the **Search for users** box. The mangement console automatically displays the users whose name contains the characters you enter. To redisplay the original list, click the ✕ button on the **Search for users** box.

You can also select one of the following options from the user type drop-down menu:

- All users

- All non-system users

- System users

- Users requiring AD logon (requires Authentication Services 4.x)

- Users not requiring AD logon (requires Authentication Services 4.x)

4. Click **OK** on the **Members** tab to save your selections.

   The mangement console adds the users with an icon to the list on the **Members** tab.

5. On the **Log on to Host** dialog, enter the user credentials and click **OK**.

   NOTE: This task requires elevated credentials.

Removing user from local group

Remove local or Active Directory users from a group from the **Groups** tab of a host's properties.

To remove a user from a local group

1. Right-click a group name and choose **Properties**.

   You can also double-click a group from the list to open its properties.

2. From the **Members** tab, select one or more users and click **Remove User**.

   The mangement console adds a icon to the user names to indicate they are ready to remove from the list.

3. Click **OK** on the **Members** tab to save your selections.

4. On the **Log on to Host** dialog, enter the user credentials and click **OK**.

   NOTE: This task requires elevated credentials.

Deleting local group

Any users belonging to a deleted group will no longer have access to the resources previously owned by that group.

To delete a local group

1. From the **Groups** tab, select one or more groups to delete and click **Delete Group**.

2. Confirm that you want to delete the selected groups.

3. On the **Log on to Host** dialog, enter the user credentials and click **OK**.

   | NOTE: This task requires elevated credentials.

   The **Groups** view is automatically refreshed and no longer lists the deleted groups.

Reviewing the Local Unix Groups report

The **Local Unix Groups** report lists all the groups on a host and the group's membership.

NOTE: This report is available when you are logged on as the *supervisor* or an Active Directory account in the **Manage Hosts** role.

To create the Local Unix Groups report

1. From the mangement console, navigate to **Reporting**.

2. From the **Reports** view, double-click the **Local Unix Groups** report name.

   The report opens a new **Local Unix Groups** tab on the **Reporting** view.

3. To locate a specific group, use a combination of the following report parameters:

   - Group Name contains
   - GID Number is
   - Member contains
   - Include all group members in report (Always included when exporting to CSV)

   NOTE: The **Member contains** field accepts multiple entries separated by a comma. Spaces are taken literally in the search. For example, entering:

   - **adm, user** searches for members whose name contains 'adm' or ' user'
   - **adm,user** searches for members whose name contains 'adm' or 'user'.

   NOTE: When you specify multiple report parameters (for example, **Group Name contains**, **GID Number is**, and **Member contains**), it uses the AND expression; therefore, ALL of the selected parameters must be met in order to locate a group.

   If you do not specify a group, it includes all local groups on each profiled host in the report. In addition, it includes all of the group members in the report by default, but you can clear the **Include all group members in report** option.

4. Open the **Export** drop-down menu and select the format you want to use for the report: **PDF** or **CSV**.

   It launches a new browser or application page and displays the report in the selected format.

NOTE: When generating multiple reports simultaneously or generating a single report that contains a large amount of data, One Identity recommends that you increase the JVM memory. See JVM memory tuning suggestions on page 214 for details.

Managing local users

The profiling operation imports system information about the local users so you can remotely manage them through the mangement console.

The console's **All Local Users** tab provides a consolidated view of all users on all hosts. In addition, a host's properties contains a **Users** view, from which you can manage the local users.

The topics in this section step you through the local user management tasks you can perform from the **Users** and **All Local Users** tabs. For a detailed description of these tasks, please refer to the online help.

Adding a local user

You can use the mangement console to remotely add a local user to a host.

NOTE: This topic instructs you to set up a local user by the name of "localuser" referred to by other examples in this guide.

To add a local user account

1. From the **All Hosts** view, double-click a host name to open its properties.

   You can also right-click the host name and choose **Users**.

2. Select the **Users** tab and click **Add User**.

3. In the **Add New user** dialog,

   a. Enter **localuser** as a new local user name in the **Name** box.

   b. Click the **Select Group** browse button next to the **GID** box to select the primary group of the user.

      The **Select Local Group** dialog opens.

   c. Find and select a local group account and click **OK**.

      By default, the **Select Local Group** dialog displays all groups discovered on the host. You can filter the groups by entering text in the filter area or use the navigation buttons at the bottom of the list to find and select a group.

> NOTE: See Adding a local group on page 59 for details about adding local groups.

    d. Click the **Select Shell** browse button to select the login shell of the user.

       The **Select local login shell** dialog opens.

    e. Find and select a local login shell and click **OK**.

       By default, the **Select local login shell** dialog displays all login shells discovered on the host. You can filter the login shells by entering text in the filter area.

    f. Enter and re-enter a password of your choice and click **Add User** to add this new local user and click **OK**.

4. On the **Log on to Host** dialog, enter your credentials to log onto the host and click **OK**.

> NOTE: This task requires elevated credentials. The mangement console enters this information by default from the cache.

   The new local user account is added to the system and mangement console.

At this point the new local user is valid for local authentication with the password you just set.

Searching for users

Use the **Search for users** control to locate particular users on a host's **Users** tab or the **All Local Users** tab.

To search for users

1. From the **All Hosts** view, double-click a host name to open its properties and select the **Users** tab.

2. Place your cursor in the **Search for users** box and enter one or more characters. As you enter characters into the text box, the mangement console redisplays only the users whose Name, UID, GID, GECOS, Login Shell, or AD User matches (contains) the criteria entered.

3. To clear the text box and redisplay the original list, select ☒ to the right of the **Search for users** box.

4. To further filter the list by type of user, open the user type drop-down menu and choose one of the following:

    • All users

    • All non-system users

    • System user

ONE IDENTITY™

- Users requiring AD logon (requires Authentication Services 4.x)

- Users not requiring AD logon (requires Authentication Services 4.x)

Modifying user properties

Modify a local Unix user's properties from either the **Users** view of a host's properties or the **All Local Users** tab.

To modify a user's properties

1. Right-click the user name and choose **Properties**.

   You can also double-click the user name to open its properties.

2. On the **General** tab, modify the user information.

3. On the **Member Of** tab, add or remove local groups.

4. On the **AD Logon** tab, specify if this user is required to use an Active Directory password to log on to the host. This allows you to "map" a local user to an Active Directory account.

   NOTE: This feature is only available when you are logged in as an Active Directory user for a host that is joined to Active Directory.

5. Click **OK** to save the changes.

6. On the **Log on to Host** dialog, enter the user credentials and click **OK**.

   NOTE: This task requires elevated credentials.

Modifying multiple user's properties

Modify multiple local Unix user's properties from either the **Users** view of a host's properties or the **All Local Users** tab.

To modify multiple user's properties simultaneously

1. Select two or more user names and right-click to reveal the context menu.

2. Choose the **Properties** option.

   The **Properties: Multiple Users** dialog displays.

3. On the **General** tab, modify:
    a. Comments (GECOS)
    b. Login shell

        Optionally, you can click the **Select Shell** button to browse for a local login shell.
4. Click **OK** to save the changes.
5. On the **Log on to Host** dialog, enter the user credentials and click **OK**.

    NOTE: This task requires elevated credentials.

Resetting local user's password

Change a user's password from either the **Users** view of a host's properties or from the **All Local Users** tab.

NOTE: The **Set Local User Password** option is not available for users required to log in with Active Directory authentication because *root* does not have permission to change a password stored in Active Directory.

To change a local user's password

1. Select one or more user names, right-click and choose **Set Local User Password** from the context menu.
2. Enter the new password for the users and click **OK**.
3. On the **Log on to Host** dialog, enter the user credentials and click **OK**.

    NOTE: This task requires elevated credentials.

System users

You can mark local user accounts that are not associated with an actual user, as "system users" from either the **Users** view of a host's properties or from the **All Local Users** tab. The mangement console allows you to manually mark (or unmark) *system users*, or you can mark (or unmark) a range of *system users*. Once you mark a user as a *system user*, you can filter the **Users** list by displaying only the *system users* or only the *non-system users*.

You can also choose to mark a range of system users automatically when profiling a host by setting the **Host System Users** option in **System Settings**. See Automatically marking host system users on page 157 for details.

Manually marking system users

You can mark multiple local user accounts that are not associated with an actual user, as "system users" from either the **Users** view of a host's properties or from the **All Local Users** tab. You mark system users for a specific host from the **Users** view of a host's properties and you mark system users for all hosts from the **All Local Users** tab.

To mark specific system users manually

1. Select one or more users from the list that you want to identify as system users.

2. Right-click the selected users and choose **Mark as system user** from the context menu.

   The status column icon changes to 🧑, the **system user** icon.

   When you mark a user as a "system user", the mangement console updates the number of **System Users** in the **Local User Statistics** pane of the **All Local Users** tab.

   > NOTE: The **Local User Statistics** pane only displays if you have Authentication Services 4.x installed and when you are logged on as an Active Directory account in the **Manage Hosts** role.

To unmark specific system users manually

1. Select one or more users from the list that you want to identify as system users.

2. Right-click the selected users and choose **Unmark as system user**.

   The status column icon reverts to 🧑, the regular user icon.

Marking multiple system users

To mark multiple system users

1. Open the **User** drop-down menu on either the **Users** view of a host's properties or from the **All Local Users** tab, and choose **Mark system users**.

   > NOTE: To unmark multiple system users, choose **Unmark system users**.

2. On the **Mark System Users** dialog, enter a UID number or range of numbers to mark.

   Use a colon (:) to signify a range of numbers; comma delimit multiple numbers or ranges. For example,

   ```
   0:499,501,555:600
   ```

   > NOTE: Do not add extra spaces.

ONE IDENTITY™

3. Enter specific account names you want to mark. For example,

```
root,web*,*nobody,ma?k
```

> NOTE: Comma delimit multiple names; do not add extra spaces. You can use wildcards in the text string, such as * and ?.

The status column icon changes to 🧑‍💼, the system user icon. It reverts to 👤 , the regular user icon, when you unmark system users.

> NOTE: You can enable the mangement console to mark local user accounts as "system users" when it profiles hosts.

> See Automatically marking host system users on page 157 for details.

Deleting a local user

When you delete a local user, all files or processes owned by the user will no longer have an owner.

To delete a local user

1. Select one or more users from the **Users** tab of a host's properties and click **Delete User**.
2. Confirm that you want to delete the selected users.
3. On the **Log on to Host** dialog, enter the user credentials and click **OK**.

   > NOTE: This task requires elevated credentials.

   The **Users** view is automatically refreshed and no longer lists the deleted users.

> NOTE: When you delete a local user, the mangement console does not delete the user's home directory.

Reviewing the Local Unix Users report

The **Local Unix Users** report lists all users on all hosts.

> NOTE: This report is available when you are logged on as the *supervisor* or an Active Directory account in the **Manage Hosts** role.

To create the Local Unix Users report

1. From the mangement console, navigate to **Reporting**.
2. From the **Reports** view, double-click the **Local Unix Users** report name.

   The report opens a new **Local Unix Users** tab on the **Reporting** view.

3. To locate a specific user, use a combination of the following report parameters:

- User Name contains
- UID Number is
- Primary GID Number is
- Comment (GECOS) contains
- Home Directory contains
- Login Shell contains

NOTE: When you specify multiple report parameters, it uses the AND expression; therefore, ALL of the selected parameters must be met in order to locate the user account.

If you do not define a specific user, it includes all local users on each profiled host in the report.

Active Directory integration

You can configure mangement console for Active Directory so that you can perform basic Active Directory operations, such as searching for Active Directory users, groups, or computers. With Active Directory credentials that have proper permissions, you can also modify specific properties of these Active Directory objects.

NOTE: Management Console for Unix is limited to managing users, security groups, and computers. Other Active Directory object types (such as distribution groups and contacts) are not displayed by the console.

The topics in this section explain how to search for and locate Active Directory users, groups and computers, and how to manage the Active Directory users who are permitted to authenticate to your non-Windows systems. For a detailed description of these tasks, please refer to the online help.

Enabling Active Directory features

If you initially configured the Management Console for Unix core features to manage local Unix users and groups and now want to use the Active Directory features, you must configure the mangement console for Active Directory.

NOTE: See Active Directory configuration on page 165 for more information.

When you configure the mangement console for Active Directory, you can perform these basic Active Directory operations:

- Search for Active Directory objects
- View or modify Active Directory user, security group, and computer object properties

    NOTE: You must have permissions in Active Directory to modify Active Directory object properties.

You can unlock these additional Active Directory features when you install Authentication Services 4.*x* on hosts you manage with Management Console for Unix:

- Join systems to Active Directory and implement AD-based authentication for Unix, Linux, and Mac systems.

- Activate the **Unix Account** and **Local User Accounts** tabs on Active Directory user properties dialog.
- Activate the **Unix Account** tab on the Active Directory group properties dialog.
- Map a Unix user to an Active Directory user.
- Create reports about Active Directory Unix-enabled users and groups.
- Create **Logon Policy for AD User** and **Logon Policy for Unix Host** reports that show which user is permitted to log into which Unix host.

NOTE: See Configure Active Directory for Authentication Services on page 78 for more information about setting up the console for full Active Directory functionality.

Adding an Active Directory group account

NOTE: The following procedure instructs you to use ADUC (Active Directory Users and Computers) to set up an Active Directory group by the name of "UNIXusers" referred to by other examples in this guide.

To create a new group in Active Directory

1. From the **Start** menu navigate to **Administrative Tools | Active Directory Users and Computers**.

   The **Active Directory Users and Computers** Console opens.

   NOTE:
   - Windows Vista/Windows 7 or 8: You must have the Remote Server Administration Tools installed and enabled.
   - Windows 2003/Windows XP: You must have the Windows 2003 Server Administration Tools installed.

2. Expand the *domain* folder and select the **Users** folder.

3. Click the **New Group** button.

   The **New Object – Group** dialog opens.

4. Enter **UNIXusers** in the **Group name** box and click **OK**.

Authentication Services provides additional tools to help you manage different aspects of migrating Unix hosts into an Active Directory environment. Links to these tools are available from **Tools** in the Control Center.

Adding an Active Directory user account

NOTE: The following procedure instructs you to use ADUC (Active Directory Users and

Computers) to set up an Active Directory user by the name of "ADuser" referred to by other examples in this guide.

To create an Active Directory user account

1. In the **Active Directory Users and Computers** console, select the **Users** folder and click the **New User** button.

2. On the **New Object - User** dialog, enter information to define a new user named **ADuser** and click **Next**.

   The **New Object - User** wizard guides you through the user setup process.

3. When you enter a password, clear the **User must change password at next logon** option, before you click **Next**.

4. Click **Finish**.

5. Close **Active Directory Users and Computers** and return to the mangement console.

Searching for Active Directory objects

Using the controls at the top of the mangement console's **Active Directory** tab, you can search Active Directory for users, groups and computers. With proper credentials, you can also search for Unix-enabled users and groups (requires Authentication Services 4.x).

NOTE: The **Active Directory** tab is only available when you are logged onto the console as an Active Directory user. See Active Directory configuration on page 165 for details.

To search for Active Directory objects

1. On the **Active Directory** tab of the mangement console, place your cursor in the **Search by name** box and enter a search expression to locate Active Directory objects. By default, when you click the 🔎 button without entering any search criteria, Management Console for Unix searches for all users in the forest.

   NOTE: The mangement console uses Ambiguous Name Resolution (ANR) as the search algorithm to search Active Directory. This allows you to enter limited or partial input to find multiple objects in Active Directory. Use one of the following methods to enter your search expression:

   - Enter a partial string to return exact matches or a list of possible matches
   - Enter a string preceded by the equal sign to return only exact matches, for example, **=Administrator**

   See Ambiguous Name Resolution for more information.

2. In the **Find** box, open the drop-down menu and select the type of Active Directory object to locate:

   a. Users (default)

   b. Groups

c.　Computers

　　　d.　Users, Groups, Computers

　　　e.　Unix-enabled Users

　　　f.　Unix-enabled Groups

　　　g.　Non Unix-enabled Users

　　　h.　Non Unix-enabled Groups

To search for *all* objects matching the object type you specify in the **Find** box, do not enter any characters in the **Search by name** field.

For example, to search for all groups in the forest, do not enter anything in the **Search by name** box, select **Groups** from the **Find** box menu, and click 🔎.

3. To narrow the search, select the container where you would like to start the search, by clicking the ▣ button next to the **In** box.

By default, the mangement console searches the entire forest configured for Active Directory.

4. Once you have defined your search expression, the type of objects to locate, and where you want to conduct your search, click the 🔎 button to initiate the search.

5. The mangement console displays the Active Directory objects whose names match (starts with) the characters you entered, are of the object type you specified, and are located in the directory or container you specified.

> NOTE: To clear the search criteria and results, click the | ⊗ Clear All | button.

Viewing or modifying Active Directory user properties

When logged in with an Active Directory account in the **Manage Hosts** role, you can view the properties of Active Directory user accounts from the **Active Directory** tab. However, you must have permissions in Active Directory to modify Active Directory user properties.

To view or modify the properties of an Active Directory user

1. From the **Active Directory** tab of the mangement console, use the search controls to locate an Active Directory user.

2. Double-click the user name to open the Active Directory user's properties.

You can also right-click the user name and choose **Properties**.

3. Use the **General** tab to view or modify the following properties:

- First Name
- Initial
- Last Name

- Display Name
- Description

4. Use the **Account** tab to view or modify the following settings:

   - User logon name
   - User logon name (pre-Windows 2000)
   - Account is locked out option (view only)
   - Account options

   NOTE: Please review the following notes regarding the account options:

   - You cannot modify the **User cannot change password** option through the mangement console. Use Active Directory Users and Computers (ADUC) to enable/disable this option, as needed.
   - If the **User cannot change password** option is enabled in ADUC, you cannot require the user to change their password at next log on.
   - If the **Password never expires** option is enabled in ADUC, you cannot require the user to change their password at the next log on.

5. Use the **Member Of** tab to view the groups of which this Active Directory user is a member.

   NOTE: You cannot make modifications to this view through the mangement console.

6. Use the **Unix Account** tab to enable or disable Unix access of the Active Directory user.

7. Use the **Local User Accounts** tab to display a list of all the local Unix users required to log on using the selected Active Directory user account.

8. Click **OK** to save your changes and close the Active Directory user's properties.

Viewing or modifying Active Directory group properties

When logged in with an Active Directory account in the **Manage Hosts** role, you can view the properties of Active Directory group accounts from the **Active Directory** tab. However, you must have permissions in Active Directory to modify Active Directory group properties.

To view or modify the properties of an Active Directory group

1. From the **Active Directory** tab of the mangement console, use the search controls to locate an Active Directory group.

2. Double-click the group name to open the Active Directory group's properties.

   You can also right-click the group name and choose **Properties**.

3. Use the **General** tab to view or modify the following properties:

    - Group name
    - Description

4. Use the **Member** tab to view the Active Directory objects (users, groups, computers) that are members of the group.

   NOTE: Searching for the members of an Active Directory group works most efficiently when there is a global catalog for the group's domain. If a global catalog for the group's domain cannot be found, the search may be slower.

    a. To add a member to the Active Directory group, click the **Add Members** button.

       The **Add Members To Group** dialog displays.

       Use the search controls to display a list of Active Directory users or groups available to add to the Active Directory group.

       Select the users or groups you wish to add and click **OK**.

    b. To remove a member from the Active Directory group, select that member and click the **Remove Members** button.

5. Use the **Member Of** tab to view the groups of which this Active Directory group is a member.

   NOTE: You cannot make modifications to this view through the mangement console.

6. Use the **Unix Account** tab to enable or disable Unix access for the Active Directory group.

7. Click **OK** to save your changes and close the Active Directory group's properties.

Authentication Services integration

You can unlock these additional Active Directory features when you install Authentication Services 4.*x* on hosts you manage with the mangement console:

- Join systems to Active Directory and implement AD-based authentication for Unix, Linux, and Mac systems.
- Activate the **Unix Account** and **Local User Accounts** tabs on Active Directory user properties.
- Activate the **Unix Account** tab on the Active directory group properties.
- Map a Unix user to an Active Directory user.
- Create reports about Unix-enabled Active Directory users and groups.
- Create **Logon Policy for AD User** and **Logon Policy for Unix Host** reports that show which user is permitted to log into which Unix host.

NOTE: See Configure Active Directory for Authentication Services on page 78 for more information about setting up the console for full Active Directory functionality.

After you install the core version of Management Console for Unix, add and profile at least one host, and enable the Active Directory features (as explained in Enabling Active Directory features on page 71), take these steps to configure the mangement console for Authentication Services:

1. Install Authentication Services on the Active Directory domain for which the console is configured.
2. Configure Active Directory for Authentication Services.
3. Choose to view the Authentication Services information in the mangement console.
4. Check for AD Readiness.
5. Install Authentication Services Software Packages on Hosts.
6. Discover the Authentication Services license in the mangement console.
7. Join to Active Directory.
8. Configure Host Access Control

The following topics walk you through these steps.

Installing Authentication Services

Install Authentication Services on each Windows workstation you plan to use to administer Unix data in Active Directory.

To install the Authentication Services Windows components

1. Mount the distribution media.

   Autorun starts automatically.

   > NOTE: To start the Autorun installation wizard, you can also navigate to the root of the distribution media and double-click **autorun** Application file.

2. From the Autorun **Setup** tab, click **Authentication Services** to launch the **Setup** wizard.

   The **Authentication Services Setup Wizard** starts automatically.

3. Click **Next** at the **Welcome** dialog and follow the wizard prompts.

   The wizard leads you through the following dialogs:

   - **License Agreement**
   - **Choose Destination Location**
   - **Ready to Install the Program**
   - **InstallShield Wizard Complete**

4. Leave the **Launch Authentication Services** option selected on the **InstallShield Wizard Complete** dialog, and click **Finish** to automatically start the Control Center.

> NOTE: The first time you install Authentication Services in your environment, the **Authentication Services Active Directory Configuration Wizard** starts automatically to walk you through the process of configuring Active Directory for Authentication Services. If the configuration has already been performed when you click **Finish**, the Control Center launches.

Configure Active Directory for Authentication Services

To utilize full Active Directory functionality, when you install Authentication Services in your environment, One Identity recommends that you prepare Active Directory to store the configuration settings that it uses. Authentication Services adds the Unix properties of Active Directory users and groups to Active Directory and allows you to map a Unix user to an Active Directory user. This is a one-time process that creates the Authentication Services application configuration in your forest.

> NOTE: To use the **Authentication Services Active Directory Configuration Wizard**, you must have rights to create a container in Active Directory.

If you do not configure Active Directory for Authentication Services, you can run your Authentication Services client agent in "Version 3 Compatibility Mode" which allows you to join a host to an Active Directory domain. See *Version 3 Compatibility Mode* in the *Authentication Services Administration Guide* for details.

When running Authentication Services in "Version 3 Compatibility Mode", you have the option in Management Console for Unix to set the schema configuration to use Windows 2003 R2. See Configuring Windows 2003 R2 schema on page 179 for details. The Windows 2003 R2 schema option extends the schema to support the direct look up of Unix identities in Active Directory domain servers.

Configuring Active Directory for Authentication Services

This topic walks you through the Active Directory configuration process. If the Authentication Services application configuration already exits in your forest, skip this section.

To configure Active Directory for Authentication Services

1. At the Authentication Services Active Directory Configuration Wizard **Welcome** dialog, click **Next**.

2. At the **Connect to Active Directory** dialog:

   a. Provide Active Directory login credentials for the wizard to use for this task:

   - Select **Use my current AD logon credentials** if you are a user with permission to create a container in Active Directory.

   - Select **Use different AD logon credentials** to specify the Active Directory credentials of another user and enter the User name and Password.

   NOTE: The wizard does not save these credentials; it only uses them for this setup task.

   b. Indicate how you want to connect to Active Directory:

   Select whether to connect to an Active Directory Domain Controller or ActiveRoles Server.

   NOTE: If you have not installed the ActiveRoles Server MMC Console on your computer, the **ActiveRoles Server** option is not available.

   c. Optionally enter the Domain or domain controller and click **Next**.

3. At the **License Authentication Services** dialog, browse to select your license file and click **Next**.

   NOTE: You can add additional licenses later. See Importing Authentication Services licenses on page 179 for details.

4. At the **Configure Settings in Active Directory** dialog, accept the default location

in which to store the configuration or browse to select the Active Directory location where you want to create the container and click **Setup**.

| NOTE: You must have rights to create a container in the selected location.

5. Once you have configured Active Directory for Authentication Services, click **Close**.

    The Control Center opens. You can now begin using Control Center to manage your Unix hosts.

6. From the Control Center, click the **Management Console** navigation link to open the mangement console log in page.

    | NOTE: Refer to Launching the Management Console on page 29 for other ways to open the mangement console

7. To take advantage of the additional Active Directory features you get when you use the mangement console with Authentication Services, log in as Active Directory account in the **Manage Hosts** role and proceed to Displaying Authentication Services agent information on page 82.

    If you have not configured the mangement console for Active Directory as explained in Active Directory configuration on page 165, you will have to log in as *supervisor*.

About Active Directory configuration

The first time you install or upgrade the Authentication Services 4.*x* Windows tools in your environment, One Identity recommends that you configure Active Directory for Authentication Services. This is a one-time Active Directory configuration step that creates the Authentication Services application configuration in your forest. Authentication Services uses the information found in the Authentication Services application configuration to maintain consistency across the enterprise.

NOTE: Without the Active Directory configuration you can join Unix machines to Active Directory and if your domain supports Windows 2003 R2 Unix naming attributes, you can store Unix identity information in Active Directory. See Configuring Windows 2003 R2 schema on page 179 for details.

The Authentication Services application configuration stores the following information in Active Directory:

- Application Licenses
- Settings controlling default values and behavior for Unix-enabled users and groups
- Schema configuration

The Unix agents use the Active Directory configuration to validate license information and determine schema mappings. Windows management tools read this information to determine the schema mappings and the default values it uses when Unix-enabling new users and groups.

The Authentication Services application configuration information is stored inside a container object with the specific naming of: cn={786E0064-A470-46B9-83FB-

C7539C9FA27C}. The default location for this container is cn=Program Data,cn=Quest Software,cn=Authentication Services,dc=<your domain>. This location is configurable.

There can only be one Active Directory configuration per forest. If multiple configurations are found, Authentication Services uses the one created first as determined by reading the *whenCreated* attribute. If another group in your organization has already created an application configuration, use the existing configuration. The only time this would be a problem is if different groups are using different schema mappings for Unix attributes in Active Directory. In that case, standardize on one schema and use local override files to resolve conflicts. You can use the Set-QasUnixUser and Set-QasUnixGroup PowerShell commands to migrate Unix attributes from one schema configuration to another. Refer to the PowerShell help for more information.

You can modify the settings using the Control Center**Preferences**. To change Active Directory configuration settings, you must have rights to Create Child Object (container) and Write Attribute for *cn*, *displayName*, *description*, *showInAdvancedViewOnly* for the Active Directory configuration root container and all child objects.

In order for Unix clients to read the configuration, authenticated users must have rights to read *cn*, *displayName*, *description*, and *whenCreated* attributes for container objects in the application configuration. For most Active Directory configurations, this does not require any change.

This table summarizes the required rights:

Table 3: Required rights

Rights Required	For User	Object Class	Attributes
Create Child Object	Authentication Services Administrators Only	Container	
Write Attribute	Authentication Services Administrators Only	Container	cn, displayName, description, showInAdvancedViewOnly
Read Attribute	Authenticated Users	Container	cn, displayName, description, whenCreated

At any time you can completely remove the Authentication Services application configuration using the Remove-QasConfiguration cmdlet. However, without the Authentication Services application configuration (or Windows 2003 R2 schema),

- Unix agents will not load Unix identity from Active Directory
- The mangement console will not find any Authentication Services licenses
- The mangement console will not know which schema to use; thus, it will run as if Authentication Services had never been installed.
- Authentication Services Active Directory-based management tools will not function

Displaying Authentication Services agent information

If the information related to Authentication Services does not display in the mangement console, you can use the **Columns** menu in the **View** panel of the task bar to expose the Authentication Services-related columns in the mangement console; that is, the Authentication Services state column, represented with the ! icon, the **Version**, and **Joined to Domain** columns.

To display the Authentication Services-related information

1. From the **All Hosts** view, open the **Columns** menu, in the **View** panel, and choose **Authentication Services**.

   The **Authentication Services** columns display in the mangement console; that is, the Authentication Services state column, represented with the ! icon, the Authentication Services**Version** and **Joined to Domain** columns.

NOTE: Once you have opened (or closed) a column group, the mangement console remembers the setting from session to session. However, if you reinstall Management Console for Unix, it reverts back to the default of showing all columns.

Setting Authentication Services software path

During the installation process, the setup wizard copies the Authentication Services software packages to a default location on the local computer

The default `client` directories are:

- On Windows platforms:

  ```
  %SystemDrive%:\Program Files\Quest Software\Management Console for
  Unix\software\qas\<version#>
  ```

- On Unix/Linux platforms:

  ```
  /opt/quest/mcu/software/qas/<version#>
  ```

If you plan to install Authentication Services or Defender client software packages, or run the AD Readiness check, you must ensure the path to the software packages is correctly set in *System Settings*.

To ensure the path to the Authentication Services software packages is correctly set

1. Make note of where your Authentication Services client software packages are located.
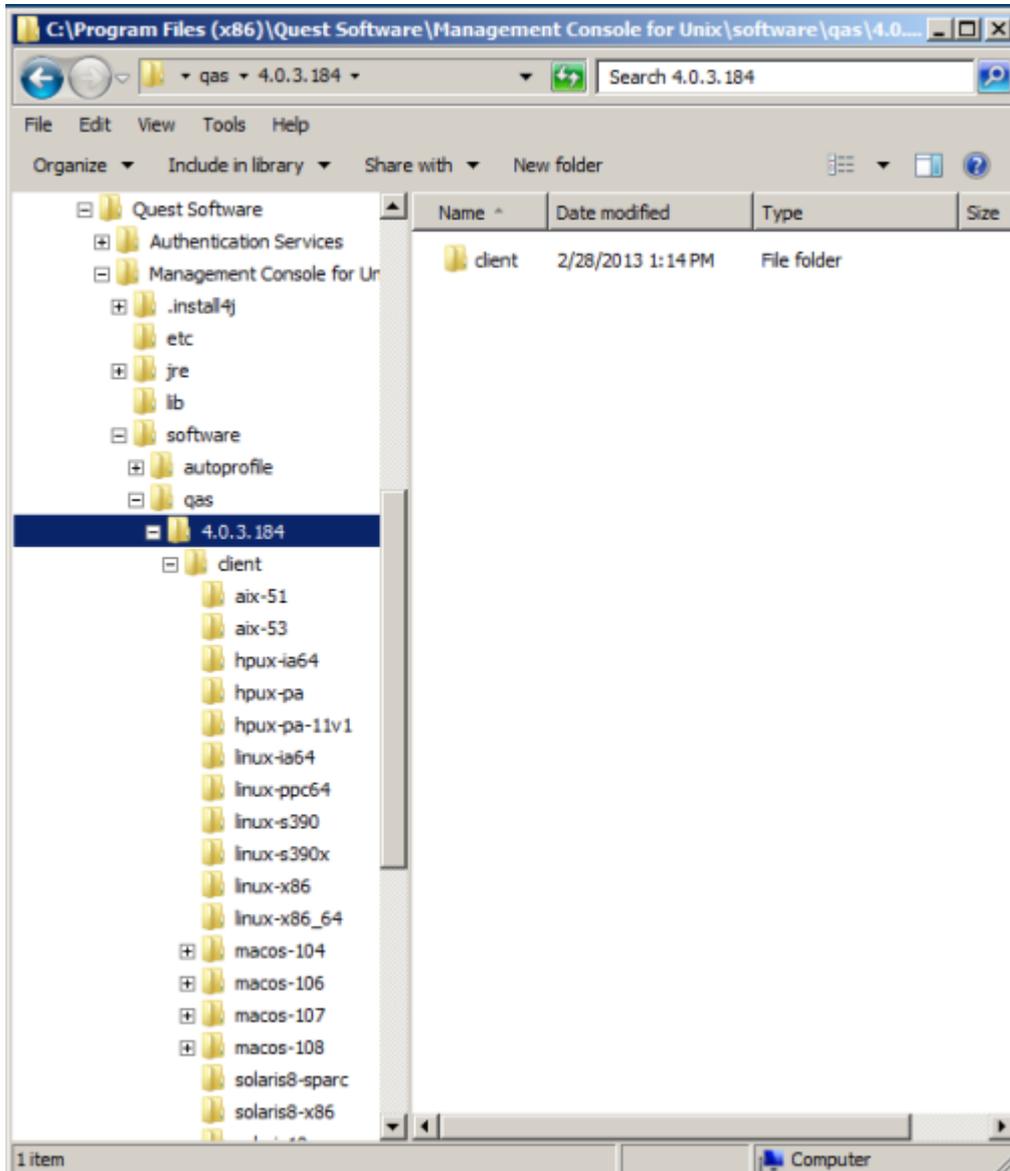
2. Ensure that **System Settings** points to that location:

    a. Log in with the *supervisor* account or an Active Directory account with rights to change **System Settings**; that is, an account in the **Console Administration** role. See Console Roles and Permissions system settings on page 161 for details.

    b. From the top-level **Settings** menu, navigate to **System settings | Authentication Services**.
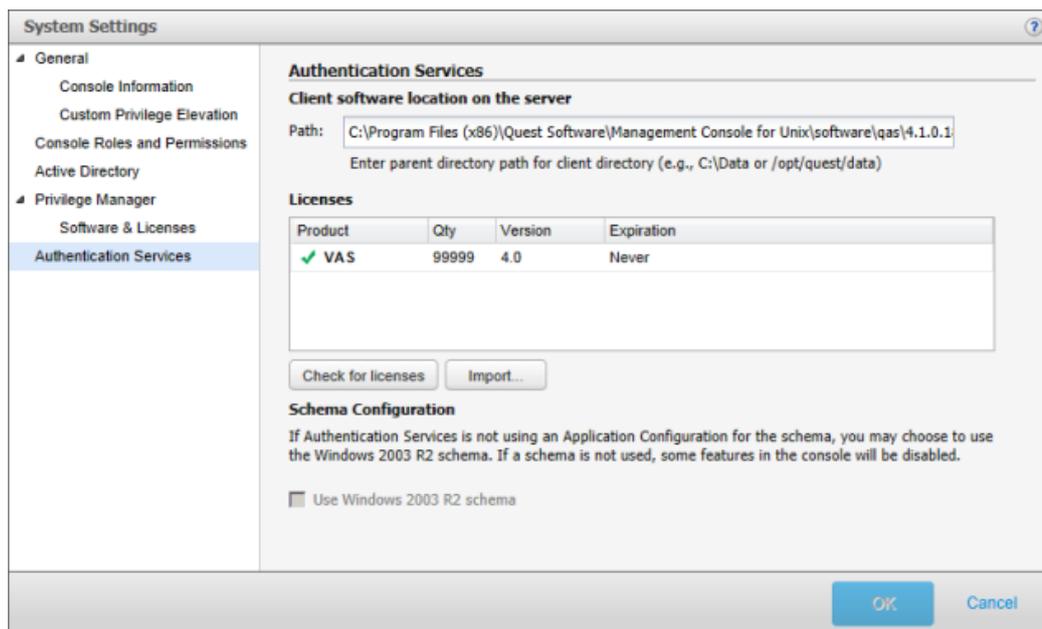
c. In the **Path** box, enter the path where the Authentication Services client software packages are located on the server and click **OK**.

NOTES: The path to the software packages must point to the folder containing the `client` directory. If the path to the software packages is not pointing to where the `client` files are, you can either change the path or copy the files to the location.

When running Management Console for Unix on Windows, the location of the Authentication Services software packages must be accessible to the mangement console service which runs as 'NT AUTHORITY\NetworkService'.

Checking host for AD readiness

The **Check for AD Readiness** command performs a series of tests to verify that a host meets the minimum requirements to join an Active Directory domain.

NOTE:

- This task is only available when you are logged on as *supervisor* or an Active Directory account in the **Manage Hosts** role. See Console Roles and Permissions system settings on page 161 for more information.

- You must have the software path set for the AD Readiness check to work properly. See Setting the Authentication Services software path on page 176 for details.

To check hosts for Active Directory Readiness

1. Select one or more hosts on the **All Hosts** view of the **Hosts** tab, open the **Check** menu from the **Prepare** panel of the toolbar, and choose **Check for AD Readiness**.

2. In the **Check AD Readiness** dialog, enter the Active Directory domain to use for the readiness check.

3. Enter Active Directory user credentials, and click **OK**.

4. On the **Log on to Host** dialog, enter the user credentials to access the selected hosts and click **OK**.

   If you selected multiple hosts, it asks whether you want to use the same credentials for all the hosts (default) or enter different credentials for each host.

   a. If you selected multiple hosts and the **Use the same credentials for all selected hosts** option, enter your credentials to log on to access the selected hosts and click **OK**.

   b. If you selected multiple hosts and the **Enter different credentials for each selected host** option, it displays a grid which allows you to enter different credentials for each host listed. Place your cursor in a cell in the grid to activate it and enter the data.

5. To check the results of the readiness check,

   a. Right-click the host on the **All Hosts** view of the **Hosts** tab, and choose **Properties**.

   b. Select the **Readiness Check Results** tab on the properties.

   c. Choose **AD Readiness** from the drop-down menu, if necessary.

AD Readiness Check runs these tests:

- Checks for supported operating system and correct OS patches
- Checks for sufficient disk space to install software
- Checks that the host name of the system is not 'localhost'
- Checks if the name service is configured to use DNS
- Checks /etc/resolv.conf for proper formatting of name service entries and that the name servers can be resolved *example.com*
- Checks for a name server that has the appropriate DNS SRV records for Active Directory *example.com*
- Selects a writable DC with port 389 (UDP) open to use for the checks *example.com*
- Displays AD site of user running checks, if available
- Checks if port 464 (TCP) is open for Kerberos Kpasswd *windows.example.com*
- Checks if port 88 (UDP and TCP) is open for Kerberos Traffic *windows.example.com*
- Checks if port 389 (TCP) is open for LDAP *windows.example.com*
- Checks for Global Catalog and port 3268 (TCP) is open to the GC *example.com*
- Checks for a valid time skew against Active Directory DC *windows.example.com*

- Checks for Authentication Services Application Configuration *windows.example.com*

- Checks if port 445 (TCP) is open for Microsoft Directory Services *windows.example.com*

A progress bar displays in the **Task Progress** pane. The final status of the task displays, including any failures or advisories encountered.

6. If the Readiness Check completed with failures or advisories, correct the issues and rerun the Readiness Check until all tests pass.

Reviewing the Authentication Services Readiness report

The **Authentication Services Readiness** report provides a snapshot of the readiness of each host to join Active Directory.

NOTE: This report is available when you are logged on as the *supervisor* or an Active Directory account in the *Manage Hosts* role.

To create the Authentication Services Readiness report

1. From the mangement console, navigate to **Reporting**.

2. From the **Reports** view, double-click the **Authentication Services Readiness** report name.

   The report opens a new **Authentication Services Readiness** tab on the **Reporting** tab.

3. Select or deselect the report parameters to define which details to include in the report:

   - Joined to AD

   - Ready to Join AD

   - Ready to Join AD with Warnings

   - Not Ready to Join AD

   - Not Checked for Readiness

4. Open the **Export** drop-down menu and select the format you want to use for the report: **PDF**, or **CSV**.

   It launches a new browser or application page and displays the report in the selected format.

NOTE: When generating multiple reports simultaneously or generating a single report that contains a large amount of data, One Identity recommends that you increase the JVM memory. See JVM memory tuning suggestions on page 214 for details.

Installing Authentication Services software packages

Once you have added and profiled one or more hosts, and checked them for AD Readiness, you can remotely deploy software products to them from the mangement console.

NOTE: This task is only available when you are logged on as **supervisor** or an Active Directory account in the *Manage Hosts* role.

To install Authentication Services software on hosts

1. Select one or more profiled hosts on the **All Hosts** view and click the **Install Software** toolbar button.

   NOTE: The **Install Software** toolbar menu is enabled when you select hosts that are profiled; the toolbar button will not be active if you have not selected any hosts.

2. On the **Install Software** dialog, select the software products you want to install and click **OK**.

   - **Authentication Services Agent**
   - **Authentication Services for Group Policy**
   - (Optional) **Authentication Services for NIS**
   - (Optional) **Authentication Services for LDAP**
   - (Optional) **Dynamic DNS Updater**
   - (Optional) **Defender Pam Module**

   NOTES:

   - Both the **Authentication Services Agent** and the **Authentication Services Group Policy** packages are required.
   - If you do not see all of these software packages, verify that the path to the software packages is correctly set in **System Settings**. (Refer to: Setting Authentication Services software path on page 82)

3. On the **Log on to Host** dialog, enter the user credentials to access the selected hosts and click **OK**.

   NOTE: This task requires elevated credentials.

   If you selected multiple hosts, it asks whether you want to use the same credentials for all the hosts (default) or enter different credentials for each host.

   a. If you selected multiple hosts and the **Use the same credentials for all selected hosts** option, enter your credentials to log on to access the selected hosts and click **OK**.

   b. If you selected multiple hosts and the **Enter different credentials for each selected host** option, it displays a grid which allows you to enter different

credentials for each host listed. Place your cursor in a cell in the grid to activate it and enter the data.

Upgrading Authentication Services

The process for upgrading the Authentication Services software packages from an older version is similar to installing it for the first time. The installer detects an older version and automatically upgrades the components.

To upgrade Authentication Services

1. Create a directory where you want to store the new Authentication Services client files.

   For example, create C:\Program Files\Quest Software\Management Console for Unix\Software\4.n.n.nn

   where "4.n.n.nn" is the Authentication Services version number to which you are upgrading.

   > NOTE: Refer to Setting Authentication Services software path on page 82 for more information about the default client directories.

2. Copy the client directory from the ISO to the directory you just created.

3. Log into the mangement console using the *supervisor* account.

4. From the top-level **Settings** menu, navigate to **System Settings | Authentication Services**.

5. In the **Authentication Services software path** box, enter the location of the directory where you copied the Authentication Services client files and click **OK**.

6. On the mangement console, select the host you want to upgrade and click **Install Software**.

7. Select the Authentication Services agent software components to upgrade and click **OK**.

8. On the **Log on to Host** dialog, enter the user credentials to access the selected hosts and click **OK**.

   If you selected multiple hosts, it asks whether you want to use the same credentials for all the hosts (default) or enter different credentials for each host.

   a. If you selected multiple hosts and the **Use the same credentials for all selected hosts** option, enter your credentials to log on to access the selected hosts and click **OK**.

   b. If you selected multiple hosts and the **Enter different credentials for each selected host** option, it displays a grid which allows you to enter different credentials for each host listed. Place your cursor in a cell in the grid to activate it and enter the data.

9. Wait for the task to finish successfully.

ONE IDENTITY™

Joining host to Active Directory

In order to manage access to a host using Authentication Services for Active Directory, you must join the host to an Active Directory domain. Joining a host to a domain creates a computer account in Active Directory for that host. Once you have deployed and installed the Authentication Services Agent software on a host, use the **Join to Active Directory** command on the **All Hosts** view's **Join or configure** menu to join the host to an Active Directory domain.

NOTE: This task is only available when you are logged on as an Active Directory account in the **Manage Hosts** role. See Console Roles and Permissions system settings on page 161 for details.

To join hosts to Active Directory

1. Select one or more hosts from the list on the **All Hosts** view, open the **Join or Configure** menu toolbar button and choose **Join to Active Directory**.

   NOTE: The **Join to Active Directory** option is only enabled when you select hosts that have the Authentication Services Agent installed.

   If you select a host that is already joined to Active Directory, you can 'rejoin' the host to the same Active Directory domain.

2. On the **Join Host to Active Directory** dialog, enter the following information to define how and where you want to join the host to Active Directory:

   a. Select the Active Directory domain to use for the join operation or enter the FQDN of the Active Directory domain.

      Use the same domain you entered when you performed the Check for AD Readiness.

   b. Optionally enter a name for the computer account for the host.

      Leave this field blank to generate a name based on the host's DNS name.

   c. Click the 🖼 button to locate and select a container in which to create the host computer account.

   d. Enter the optional join commands to use.

      See Optional join commands on page 90 for a list of commands available.

   e. Enter the user name and password to log onto Active Directory.

      The user account you enter must have elevated privileges in Active Directory with rights to create a computer account for the host.

3. On the **Log onto Host** dialog, enter the user credentials to access the selected host (s) and click **OK**.

   NOTE: This task requires elevated credentials. The mangement console pre-populates this information.

   The task progress pane on the **All Hosts** view displays a progress bar and the final status of the tasks, including any failures or advisories encountered.

Optional join commands

You can enter one or more of the following `join` commands on the **Join Host to Active Directory** dialog. Separate multiple commands with a single space.

Table 4: Optional join commands

Option	Description
-I *cache export filename*	Load users and groups from the specified cache export file instead of from the network.
-c *computer_ name*	Specify a different name for the computer object than the one usually generated from your host name. Specify either the FQDN or NetBIOS name for the computer object. NOTE: If you specified a computer account on the **Join Host to Active Directory** dialog, the mangement console ignores this command and uses the computer account you specify on the dialog.
-c *container*	Specify the LDAP DN of the container where the computer will be created. NOTE: If you specified a container on the **Join Host to Active Directory** dialog, the mangement console ignores this command and uses the container you specify on the dialog.
-l	Do not apply Group Policy Settings (if Authentication Services for Group Policy is installed).
-w	Enable workstation mode where users are not cached until they log on.
-U	Load all users from the global catalog. The mangement console loads all Unix-enabled users in the forest, regardless of location and domain.
-G	Load all groups from the global catalog. The mangement console loads all Unix-enabled groups in the forest, regardless of location and domain.
-r *domain_ list*	Specify a comma-separated list of alternate authentication domains, used for resolving simple names.
-u *search_ path*	Specify an alternate search path from which to populate the user's cache. You must specify a container object within your Active Directory forest in this search path.
-g *search_ path*	Specify an alternate search path from which to populate the group's cache. You must specify a container object within your Active Directory forest in this search path.
-s *siteName*	Manually specify the site name for the selected host.
-p *UPM_ search_path*	Specify the path of the Primary Personality Container. This command supersedes the `-u` and `-g` settings. If the specified UPM search path does not exist, the join command will fail.

Option	Description
--skip-config	Skip automatic system configuration of PAM, NSS, LAM and SIA subsystems.
--preload-nested-memberships	After loading users or groups, query tokenGroups for all cached users to process nested group membership information.
--site-only-usn	For USN queries, only use site servers. Use this command when non-site servers are unavailable, for example, blocked by a firewall.
--no-timesync	Skip automatic time synchronization.

Unjoining host from Active Directory

Unjoining a host from the mangement console removes the computer object from Active Directory, preventing further Active Directory user log on. This task does not remove the Authentication Services Agent software installed on the unjoined host.

NOTE: This task is only available when you are logged on as an Active Directory account in the **Manage Hosts** role.

To unjoin hosts from Active Directory

1. Select one or more hosts from the list on the **All Hosts** view, open the **Unjoin** menu toolbar button and choose **Unjoin from Active Directory**.

   NOTE: If unjoining multiple hosts, all hosts must be joined to the same domain.

2. On the **Unjoin Host from Active Directory** dialog, enter the user credentials of an Active Directory user that has rights to delete computer objects from the Active Directory domain and click **OK**.

3. On the **Log on to Host** dialog, enter the user credentials to access the selected hosts and click **OK**.

   NOTE: To unjoin the host from Active Directory, Authentication Services requires you to have elevated (root) credentials to complete the task on the host side.

   A progress bar displays in the **Task Progress** pane. The final status of the task displays, including any failures or advisories encountered. If successfully unjoined, the Active Directory domain, previously listed in the **Joined to Domain** column, is replaced with the 🌐 **Ready to join** icon if you have previously run **Check for AD readiness**; otherwise the **Joined to Domain** column is left empty.

Configuring host access control

The mangement console allows you to modify Authentication Services access settings. You can add Active Directory users or groups to the `users.allow` file for a single host or a selected group of hosts. This allows you to control Active Directory user access on Authentication Services hosts.

NOTE: The mangement console does not allow you to view or modify the `users.deny` file.

To view the users.allow file for a single host

1. From the **All Hosts** view, right-click a host that is joined to an Active Directory domain.

2. Select the **Host Access Control** option from the context menu.

   The **Host Access Control** tab lists the content of the `users.allow` file.

   NOTE: Users and Groups displayed in red text indicate that Authentication Services could not resolve the user/group in Active Directory.

To allow additional Active Directory users or groups to access a single host

1. From the **Host Access Control** tab, click **Manage Access**.

2. On the **Host Access Control** dialog, specify the names you want to allow access to the selected host.

   You can either:

   - Type a name into the text box and click **Add**.

     -OR-

   - Click **Select** to browse for the Active Directory user or group name.

     Clicking **Select** opens the **Select AD Object** dialog.

   Once you have the names listed on the **Host Access Control** dialog, click **OK**.

3. On the **Log on to Host** dialog, enter the user credentials to access the selected host and click **OK**.

   The console updates the `users.allow` file and the database accordingly.

To add or remove access for Active Directory users or groups on multiple hosts

1. From the **All Hosts** view, select and right-click multiple hosts that are joined to an Active Directory domain.

2. Select the **Host Access Control** option from the context menu.

   The **Host Access Control** dialog displays two list boxes: one in which to add users or groups, the other to specify users and groups to remove from the `users.allow` file.

3. Specify or select names to add or remove and click **OK**.

4. On the **Log on to Host** dialog, enter the user credentials to access the selected

hosts and click **OK**.

The console updates the `users.allow` file and the database accordingly.

Check QAS Agent Status

You can either check the health status of Authentication Services agents manually, or you can configure the mangement console to automatically check the QAS agent status and report any warnings or failures to the console.

NOTE: Running the **Check QAS Agent Status** commands requires:

- you are logged on as an Active Directory account in the **Manage Hosts** role
- the hosts have Authentication Services 4.0.3.78 (or later) Agent software installed

For more information, see Check QAS agent status commands not available on page 197.

Manually checking QAS agent status

To check QAS agent status

1. Select one or more hosts on the **All Hosts** view, open the **Check** menu from the **Prepare** panel of the toolbar and choose **Check QAS agent status**.

2. In the **Log on to Host** dialog, enter the user credentials to access the selected hosts and click **OK**.

   A progress bar displays in the task progress pane and the **Host Notifications** tab indicates the number of hosts with warnings or failures detected.

   NOTE: This task requires elevated credentials.

   If you select multiple hosts, you are asked if you want to use the same credentials for all the hosts (default) or enter different credentials for each host.

   - If you selected multiple hosts and the **Use the same credentials for all selected hosts** option, enter your credentials to log on to access the selected hosts and click **OK**.
   - If you selected multiple hosts and the **Enter different credentials for each selected host** option, it displays a grid which allows you to enter different credentials for each host listed. Place your cursor in a cell in the grid to activate it and enter the data.

3. Select the **Host Notifications** tab to view the reported warnings or failures.

   See Viewing the QAS status errors on page 95 for details.

Automatically checking QAS agent status

To have updated information about the status of Authentication Services agents, you can configure the mangement console to periodically check the QAS agent status automatically. If it detects a status change on the host, it reports the following warnings or failures to the **Host Notifications** tab:

- Critical Failure
- Failure
- Warning

To configure the console to automatically check the QAS agent status

1. Select one or more hosts on the **All Hosts** view, open the **Check** menu from the **Prepare** panel of the toolbar, and choose **Check QAS agent status automatically...**

   NOTE: This option is only available for multiple hosts if all hosts are in the same "Check QAS agent status" state; that is, they all have automatic status checking turned on, or they all have automatic status checking turned off.

2. Select the **Check status automatically** option, set the frequency for the health status check, and click **OK**.

   NOTE: Use standard crontab syntax when entering Advanced schedule settings.

3. On the **Log on to Host** dialog, enter the user credentials to access the selected hosts and click **OK**.

   NOTE: This task requires elevated credentials.

   When configured for automatic checking, the **QAS state** column on the **All Hosts** view displays the ⚠ icon. Then, if the server does not receive a heartbeat in over 4 hours (by default), it displays the ⚠ icon. No icon in the **QAS state** column indicates the host is not configured to check the QAS agent status automatically.

   If you select multiple hosts, you are asked if you want to use the same credentials for all the hosts (default) or enter different credentials for each host.

   - If you selected multiple hosts and the **Use the same credentials for all selected hosts** option, enter your credentials to log on to access the selected hosts and click **OK**.

   - If you selected multiple hosts and the **Enter different credentials for each selected host** option, it displays a grid which allows you to enter different credentials for each host listed. Place your cursor in a cell in the grid to activate it and enter the data.

   NOTE: If you receive a GID conflict error, see UID or GID conflicts on page 218.

4. View the QAS Agent status for each host on the **Host Notification** tab.

   See Viewing the QAS status errors on page 95 for details.

   When you configure a host to check the QAS agent status automatically, the mangement console,

ONE IDENTITY™

a. Creates "questusr" (the user service account), if it does not already exist, and, a corresponding "questgrp" group on the host that the mangement console uses for automatic QAS agent status checking.

b. Adds *questusr* as an implicit member of *questgrp*.

c. Adds the auto-check SSH key to *questusr*'s authorized_keys, /var/opt/quest/home/questusr/.ssh/authorized_keys.

d. Verifies the user service account can login to the host.

e. Creates a Authentication Services cron job that runs QAS status according to the specified interval.

NOTE: If you receive an error message saying you could not log in with the user service account, please refer to Service account login fails on page 208 to troubleshooting this issue.

The *questusr* account is a non-privileged account that does not require root-level permissions. This account is used by the console to gather information about existing users and groups in a read-only fashion, however, the mangement console does not use the *questusr* account to make changes to any configuration files.

NOTE: If *questusr* is inadvertently deleted from the console, the console will not be updated. To recreate the "questusr" account, re-configure the host for automatic QAS agent status checking.

To disable automatic status checking

1. Select one or more hosts on the **All Hosts** view and choose **Check QAS agent status automatically…**.

2. Clear the **Check status automatically** option on the **Check QAS Agent Status Automatically** dialog and click **OK**.

3. On the **Log on to Host** dialog, enter the user credentials to access the selected hosts and click **OK**.

When you disable auto-status checking for a host, the mangement console

1. Leaves the "questusr" and the corresponding "questgrp" accounts on the host.

2. Leaves *questusr* as an implicit member of *questgrp*.

3. Removes the auto-check SSH key from that user's authorized_keys file.

4. Removes the cron job on the host.

Viewing the QAS status errors

After you have checked the status of the Authentication Services hosts, you can view the reported failures or warnings on the **Host Notifications** tab.

To view QAS agent status

1. From the **Host Notifications** tab, select the **QAS Status** view.

   NOTE: If the **Host Notifications** tab is not currently available on the mangement console, open the **Open Views** menu and choose **Host Notifications**.

2. Expand the host to see the warning and failure messages.

   The **QAS Status** view indicates the health status of the listed Authentication Services hosts using these icons:

   - 🛑 - Critical Failure

   - ❌ - Failure

   - ⚠️ - Warning

3. **To list only the hosts of one or more status levels**

   a. Open the **QAS Status state** column drop-down menu, indicated with ! icon.

   b. Navigate to the **Filters** option.

   c. Choose one or more of the status levels.

   NOTE: The mangement console does not preserve the filter settings across log-on sessions. To clear the filter settings, click the **Clear column filters** button in the toolbar. If the **Clear column filters** button is not enabled, no status filters are set.

4. To see the details about a particular warning or failure message, double-click it and open the *Properties* window.

   NOTE: You can also click the 🖼 icon in the toolbar to show status properties.

5. To close the status **Properties** window, click the **Show status properties** icon.

6. To re-check the QAS agent status for a host, select any warning or failure for that host and click the **Check QAS agent status** button on the toolbar.

   NOTE: The **Check QAS Status** button is only available when a warning or failure is selected.

7. To change the auto-status configuration, open the **Check** menu and choose **Check QAS agent status automatically**.

   NOTE: You can also right-click any warning or failure to access the two **Check QAS** options.

Viewing the QAS status heartbeat errors

The host sends a heartbeat every four hours by default. If the server does not receive a heartbeat in over four hours, it displays an alert on the **QAS Heartbeat** tab.

NOTE: The **QAS Status Heartbeat** tab only lists hosts that fail to send a heartbeat in four hours.

To view QAS agent heartbeat

1. From the **Host Notifications** tab, select the **QAS Status Heartbeat** view.

   The **QAS Status Heartbeat** view shows alerts for hosts that have failed to send a QAS agent status heartbeat using this icon:

   🔥 - No heartbeat received in over 4 hours

   > NOTE: You can customize the heartbeat interval for the automatic QAS Status update. See Customize auto-task settings on page 209 for details.

   When a host, configured for automatic checking, receives a QAS agent status heartbeat error, in addition to displaying the alert on the **QAS Status Heartbeat** view, it displays the 🔥 icon in the **Authentication Services state** column on the **All Hosts** view.

Adding AD user to a local group

Once you have successfully joined a host to an Active Directory domain, use the **Groups** view on the host's properties to add an Active Directory user to a local group (or remove users from a group).

> NOTE: This feature is only available when you are logged on as an Active Directory account in the **Manage Hosts** role. See Console Roles and Permissions system settings on page 161 for details.

To add an Active Directory user to a local group

1. On the **All Hosts** view, right-click a host that is joined to an Active Directory domain and choose the **Groups**.

   You can also double-click the host name to open its properties, then click the **Groups** tab.

2. Double-click a local group name or right-click the group name and choose **Properties** to open its properties.

3. On the group's properties, click the **Members** tab, open the **Add** menu and choose **AD user**.

4. On the **Select Unix-Enabled AD User** dialog, search Active Directory to locate users to add.

   > NOTE: When searching Active Directory, the mangement console only lists Unix-enabled users. See Unix-Enable an Active Directory User for details.

   To find a particular user you can filter the list of users. Enter one or more characters in the **Search by name** box. The mangement console automatically displays the users whose name contains the characters you enter.

   You can also click 📁 to select the container where you want to being the search.

5. Select one or more users from the list and click **OK**.

   The mangement console adds the selected users to the list on the **Members** tab with an ![icon] icon.

6. Click **OK** on the **Members** tab to save your selections.

7. On the **Log on to Host** dialog, enter the user credentials to access the selected host and click **OK**.

   This information is pre-populated if you saved the credentials for the host.

NOTE: To remove objects from a local group, select one or more objects from the list on the **Members** tab and click **Remove User**.

Mapping local users to Active Directory users

Management Console for Unix provides a feature called "Require AD Logon" where you can map local Unix user accounts to Active Directory users accounts. In other words, you can specify an Active Directory user account with which local users can authenticate, or login to a Unix host. Active Directory password policies are enforced requiring that these users use their Active Directory password with their local user name or Active Directory log on name. Local users retain all of their local Unix attributes such as UID Number and Login Shell, but they authenticate using their Active Directory password.

NOTE: This feature is only available if you meet these criteria:

- Authentication Services 4.*x* is installed on the client host
- Your client host is joined to Active Directory
- You are logged on as an Active Directory account in the **Manage Hosts** role. See Console Roles and Permissions system settings on page 161 for details.

Advantages of Requiring Users to Log in with Active Directory Authentication:

- Provides a rapid deployment path to take advantage of Active Directory authentication
- Kerberos authentication provides stronger security
- Enables centralized access control
- Enforces Active Directory Password policies
- Provides a path for consolidating identities in Active Directory with the Ownership Alignment Tool (OAT)
- Low impact to existing applications and systems on the Unix host
- Easy to deploy with Authentication Services self enrollment

By "mapping" a local user to an Active Directory account, the user can log in with his Unix user name and Active Directory password.

Enabling local user for AD authentication

This feature, also known as user mapping, allows you to associate an Active Directory user account with a local Unix user. Allowing a local user to log into a Unix host using Active Directory credentials enables that user to take advantage of the benefits of Active Directory security and access control.

To enable a local user for Active Directory authentication

1. In the mangement console, navigate to **Hosts | All Hosts**.

2. Double-click a host to open its properties.

3. From a host's properties, select the **Users** tab and double-click a local user account to open its **Properties**.

   NOTE: To set up the local user, see Adding a local user on page 64.

4. On the **AD Logon** tab, select the **Require an AD Password to logon to Host** option, and click **Select**.

5. On the **Select AD User** dialog, select the **ADuser** account and click **OK**.

   NOTE: To set up the Active Directory user, see Adding an Active Directory user account on page 72.

6. On the local user's properties, click **OK**.

7. On the **Log on to Host** dialog, verify your credentials to log onto the host and click **OK**.

   NOTE: This task requires elevated credentials.

   You have now "mapped" a local user to an Active Directory user and the mangement console indicates that the local user account requires an Active Directory password to log onto the Host in the **AD User** column.

You can also map multiple Unix users to use a single Active Directory account using the **Require AD Logon** pane on the **All Local Users** tab.

To assign (or "map") a Unix user to an Active Directory user

1. From the **All Local Users** tab, select one or more local Unix users.

2. In the **Require AD Logon** pane, click the 🔍**Search** button to populate the list of Active Directory users.

   (Click the 📁**Directory** button to search in a specific folder.)

3. Select an Active Directory user and click the **Require AD Logon to Host** button at the bottom of the **Require AD Logon** pane.

4. On the **Log on to Host** dialog, verify your credentials to log onto the host and click **OK**.

   NOTE: This task requires elevated credentials.

The Active Directory user assigned to the selected local Unix user displays in the **AD User** column of the **All Local Users** tab.

Listing local users required to use AD authentication

You can view a list of the host accounts that are required to log on using a particular Active Directory account from the **All Local Users** tab of the mangement console.

NOTE: This feature is only available when you are logged on as an Active Directory account in the **Manage Hosts** role. See Console Roles and Permissions system settings on page 161 for details.

To view local user accounts required to log on with an Active Directory Account

1. From the **All Local Users** tab of the mangement console, click the **AD User** column title to sort the list of users by those required to log on with an Active Directory user account.

2. Right-click a user name and choose **Properties** to open its properties.

3. Select the **AD Logon** tab to view or modify the Active Directory user properties.

To see which local user accounts are enabled to use Active Directory account credentials

1. From the **Active Directory** tab, search for users.

2. Double-click a user name to open its properties.

3. Select the **Local User Accounts** tab to display a list of all the local user accounts that are required to log on using the selected Active Directory user account.

NOTE: The **Local Unix Users with AD Logon** report is another way to identify the local user accounts that are required to use Active Directory credentials. See Reports on page 143.

Testing the mapped user login

Once you have "mapped" a local user to an Active Directory user, you can log into the local Unix host using your local user name and the Active Directory password of the Active Directory user to whom you are "mapped". The Control Center offers a simple way to log into the host.

To test the mapped user login

1. From the Control Center, under **Login to remote host**:

   - **Host name**: Enter the Unix host name.
   - **User name**: Enter the local user name, **localuser**.

   Click **Login** to log onto the Unix host with your local user account.

2. If the **PuTTY Security Alert** dialog opens, click **Yes** to accept the new key.

3. Enter the password for *ADuser*, the Active Directory user account you mapped to *localuser*, when you selected the **Require an AD Password to logon to Host** option on the user's properties.

4. At the command line prompt, enter **id** to view the Unix account information.

5. Enter /opt/quest/bin/vastool klist to see the credentials of the Active Directory user account.

6. Enter **exit** to close the command shell.

You just learned how to manage local users and groups from themangement console by mapping a local user account to an Active Directory user account. You tested this by logging into the Unix host with your local user name and the password for the Active Directory user account to whom you are "mapped".

Configuring the console to recognize Unix attributes in AD

Configuring the mangement console to recognize Unix attributes in Active Directory, enables these features:

- **Unix Account** tab on the user and group properties
- Ability to query Unix-enabled users or groups
- Reports that include Active Directory Unix information

There are two ways to configure the mangement console to recognize Unix attributes in Active Directory:

1. Installing Authentication Services 4.0 or greater in your Active Directory domain and creating the Authentication Services application container in your forest. See Configure Active Directory for Authentication Services on page 78 for details.

   Authentication Services adds the Unix properties of Active Directory users and groups to Active Directory and allows you to map a Unix user to an Active Directory user.

2. If you are running Authentication Services without a Authentication Services application configuration in your forest, to configure the console to recognize Active Directory objects, enable Management Console for Unix to use the default Windows 2003 R2 schema to recognize Unix naming attributes. See Configuring Windows 2003 R2 schema on page 179 for details.

   The Windows 2003 R2 schema option extends the schema to support the direct look up of Unix identities in Active Directory domain servers.

Unix-enable an Active Directory group

You can Unix-enable an Active Directory group from a group's properties on the **Active Directory** tab.

NOTE: This feature is only available if:

- you have configured the mangement console to recognize Active Directory objects See Configuring the console to recognize Unix attributes in AD on page 101 for details.
- you are logged into the mangement console as an Active Directory account in the **Manage Hosts** role
- you have rights in Active Directory to Unix-enable groups

To Unix-enable an Active Directory group

1. On the mangement console's **Active Directory** tab, open the **Find** drop-down menu and choose **Groups**.

2. Enter a group name, such as **UNIX** in the **Search by name** box and press **Enter**.

3. Double-click the group name, such as **UNIXusers** to open its properties.

    NOTE: To set up the Active Directory group account, see Adding an Active Directory group account on page 72.

4. On the **Unix Account** tab, select the **Unix-enabled** option and click **OK**.

Reviewing the Unix-enabled AD Groups report

The **Unix-enabled AD Groups** report identifies all Active Directory groups that have Unix group attributes.

To create the Unix-enabled AD Groups report

1. From the mangement console, navigate to **Reporting**.

2. From the **Reports** view, double-click the **Unix-enabled AD Groups** report name.

    The report opens a new **Unix-enabled AD Groups** tab on the **Reports** view.

    NOTE: This report is only available if you have configured the mangement console to recognize Active Directory objects (see Configuring the console to recognize Unix attributes in AD on page 101), and you are logged on as an Active Directory account in the **Manage Hosts** role.

3. Choose the base container for the report.

4. Open the **Export** drop-down menu and select the format you want to use for the report: **PDF** or **CSV**.

It launches a new browser or application page and displays the report in the selected format.

NOTE: When generating multiple reports simultaneously or generating a single report that contains a large amount of data, One Identity recommends that you increase the JVM memory. See JVM memory tuning suggestions on page 214 for details.

Unix-enable an Active Directory user

An Active Directory user object is considered to be Unix-enabled when it has the following Unix user attributes assigned: UID Number, Primary GID Number, Home Directory and Login Shell.

NOTE: This feature is only available if:

- you have configured the mangement console to recognize Active Directory objects. See Configuring the console to recognize Unix attributes in AD on page 101 for details.
- you are logged into the mangement console as an Active Directory account in the **Manage Hosts** role
- you have rights in Active Directory to Unix-enable users.

To Unix-enable an Active Directory user

1. On the mangement console's **Active Directory** tab, open the **Find** drop-down menu and choose **Users**.

2. Click the 🔎 **Search by name** box to search for all Active Directory users. Or, enter a portion of your **ADuser** log on name in the **Search by name** box and press **Enter**.

3. Double-click **ADuser**, the Active Directory user name, to open its **Properties**.

4. On the **Unix Account** tab, select the **Unix-enabled** option.

   It populates the **Properties** with default Unix attribute values.

5. Make other modifications to these settings, if necessary, and click **OK** to Unix-enable the user.

   NOTE: You can use PowerShell to apply additional settings. PowerShell allows you to validate entries for the GECOS, Home Directory and Login Shell attributes. Please refer to the Authentication Services user documentation for more information on defining these additional settings using PowerShell cmdlets.

   Once enabled for Unix, you can log on to the host with that Active Directory user's log on name and password.

You can also Unix-enable Active Directory users from the **Require AD Logon** pane on the **All Local Users** tab.

To Unix-Enable an Active Directory user

1. In the **Require AD Logon** pane, click the 🔍**Search** button to populate the list of Active Directory users.

   Click the ▢ **Directory** button to search in a specific folder.

2. Select an Active Directory user and click the **Properties** button at the bottom of the **Require AD Logon** pane.

3. Select the **Unix Account** tab from the user's properties.

4. Select the **Unix-enabled** option and click **OK**.

Reviewing the Unix-enabled AD Users report

The **Unix-enabled AD Users** report identifies all Active Directory users with Unix user attributes.

To create the Unix-enabled AD Users report

1. From the mangement console, navigate to **Reporting**.

2. From the **Reports** view, double-click the **Unix-enabled AD Users** report name.

   The report opens a new **Unix-enabled AD Users** tab on the **Reports** view.

   NOTE: This report is only available if you have configured the mangement console to recognize Active Directory objects (see Configuring the console to recognize Unix attributes in AD on page 101), and you are logged on as an Active Directory account in the **Manage Hosts** role.

3. Choose the base container for the report.

4. Open the **Export** drop-down menu and select the format you want to use for the report: **PDF** or **CSV**.

   It launches a new browser or application page and displays the report in the selected format.

NOTE: When generating multiple reports simultaneously or generating a single report that contains a large amount of data, One Identity recommends that you increase the JVM memory. See JVM memory tuning suggestions on page 214 for details.

Testing the Active Directory user login

Now that you have Unix-enabled an Active Directory user, you can log into a local Unix host using your Active Directory user name and password.

To test the Active Directory login

1. From the Control Center, under **Login to remote host**:

   - **Host name**: Enter the Unix host name.
   - **User name**: Enter the Active Directory user name, such as **ADuser**.

   Click **Login** to log onto the Unix host with your Active Directory user account.

2. Enter the password for the Active Directory user account.

3. At the command line prompt, enter **id** to view the Unix account information.

4. After a successful log in, verify that the user obtained a Kerberos ticket by entering:

   ```
   /opt/quest/bin/vastool klist
   ```

   The `vastool klist` command lists the Kerberos tickets stored in a user's credentials cache. This proves the local user is using the Active Directory user credentials.

5. Enter **exit** to close the command shell.

You just learned how to manage Active Directory users and groups from the mangement console by Unix-enabling an Active Directory group and user account. You tested this out by logging into the Unix host with your Active Directory user name and password. Optionally, you can expand on this tutorial by creating and Unix-enabling additional Active Directory users and groups and by testing different Active Directory settings such as account disabled and password expired.

Privilege Manager integration

Management Console for Unix allows you to install the *Privilege Manager Policy Server* as well as the *Privilege Manager Agent* and the *Sudo Plugin* software to remote hosts; it also allows you to join hosts to a policy group activated in the Privilege Manager**System Settings**. See Configuring a service account on page 169 for details.

The policy management and keystroke logging features are available when the mangement console is configured in **System Settings** for one or more policy groups.

NOTE: To use the policy editor, you must log in either as the *supervisor* or an Active Directory account with rights to manage policy; that is, an account in the **Manage Sudo Policy** or **Manage PM Policy** roles.

To replay keystroke logs, you must log in either as the *supervisor* or an Active Directory account with rights to audit policy; that is, an account in the **Audit Sudo Policy** or **Audit PM Policy** console roles.

After you install Management Console for Unix, you are ready to enable the Privilege Manager features.

Getting started

To enable the mangement console's Privilege Manager features

1. Set up a user in the **Manage Sudo Policy** or **Manage PM Policy** role to edit the policy and a user in the **Audit Sudo Policy** or **Audit PM Policy** role to replay keystroke logs. See Adding (or Removing) role members on page 164 for details.

    NOTE: The default *supervisor* account is a member of all roles and therefore has the permissions to both edit policy and replay keystroke logs.

2. Download the Privilege Manager for Unix software packages to the server.

3. Set the Privilege Manager software location in **System Settings**.

    See Setting the Privilege Manager software path on page 172.

4. Configure the Primary Policy server:

a. Add and profile a host intended to be the primary policy server.

b. Check the server for configuration readiness. See Checking policy server readiness on page 108.

c. Install the Privilege Manager Policy Server package. See Installing the Privilege Manager packages on page 109.

d. Configure the primary policy server. See Configuring the primary policy server on page 109.

e. Join the PM Agent or Sudo Plugin to the policy group. See Joining the host to a policy group on page 111.

5. Configure a Secondary Policy server:

a. Add and profile a host intended to be a secondary policy server used for load balancing.

b. Check the server for configuration readiness. See Checking policy server readiness on page 108.

c. Install the Privilege Manager Policy Server package. See Installing the Privilege Manager packages on page 109.

d. Configure the secondary policy server. See Configuring a secondary policy server on page 113.

e. Join the PM Agent or Sudo Plugin to the policy group. See Joining the host to a policy group on page 111.

6. Install the PM Agent or Sudo Plugin software on a remote host:

a. Add and profile a remote host where you plan to install the PM Agent or Sudo Plugin software.

b. Configure a console service account on the primary policy server and activate the policy groups you want to use. See Configuring a service account on page 169 for details.

c. Check the remote host for policy readiness. See Checking client for policy readiness on page 114.

d. Install the Privilege Manager software on the remote host. See Installing Privilege Manager agent or plugin software on page 116.

e. Join the PM Agent or Sudo Plugin to the policy group. See Joining the host to a policy group on page 111.

Configure a primary policy server

The first thing you must do is configure the host you want to use as your primary policy server.

Checking policy server readiness

Check Policy Server Readiness performs a series of tests to verify that the specified hosts meet the minimum requirements to be configured as a policy server.

NOTE: This command is only available, if no Privilege Manager software is installed on the selected hosts.

For the readiness check to finish successfully, the path to the Privilege Manager software packages must be correctly set in **System Settings**. See Setting the Privilege Manager software path on page 172 for details.

To check for policy server readiness

1. Select one or more hosts on the **All Hosts** view of the **Hosts** tab, open the **Check** menu from the **Prepare** panel of the toolbar, and choose **Check Policy Server Readiness**.

2. In the **Check Policy Server Readiness** dialog, enter user credentials to access the hosts and click **OK**.

   NOTE: This task does not require elevated credentials.

   If you select multiple hosts, you are asked if you want to use the same credentials for all the hosts (default) or enter different credentials for each host.

   a. If you selected multiple hosts and the **Use the same credentials for all selected hosts** option, enter your credentials to log on to access the selected hosts and click **OK**.

   b. If you selected multiple hosts and the **Enter different credentials for each selected host** option, it displays a grid which allows you to enter different credentials for each host listed. Place your cursor in a cell in the grid to activate it and enter the data.

3. To check the results of the readiness check,

   a. Right-click the host on the **All Hosts** view of the **Hosts** tab, and choose **Readiness Check Results**.

   b. Choose **Policy Readiness** from the drop-down menu, if necessary.

   Running the readiness check on a policy server performs these tests:

   - Basic Network Conditions:
       - Hostname is configured
       - Hostname can be resolved
       - Reverse lookup returns it own IP
   - Privilege Manager for Unix Server Network Requirements
       - Policy server port is available (TCP/IP port 12345)
   - Privilege Manager for Unix Prerequisites
       - SSH keyscan is available

ONE IDENTITY™

A progress bar displays in the **Task Progress** pane. The final status of the task displays, including any failures or advisories encountered.

4. If the readiness check completed with failures or advisories, correct the issues and run the policy server readiness check again.

   After you make sure your primary policy server host meets the system requirements, you are ready to install the Privilege Manager packages.

Installing the Privilege Manager packages

The mangement console allows you to install three Privilege Manager software components which provide central policy management, granular access control reporting, as well as the ability to enable, gather, store and playback keystroke logs.

NOTE: Centralized policy management and keystroke logging are licensed separately. See Software & Licenses settings on page 172 for details.

To install the Privilege Manager packages

1. Select one or more profiled hosts on the **All Hosts** view.

2. Click **Install Software** from the **Prepare** panel on the **All Hosts** view.

   NOTE: The **Install Software** toolbar menu is enabled when you select hosts that are profiled.

   The toolbar button will not be active if

   - You have not selected any hosts.
   - You have selected hosts that are not profiled.

3. On the **Install Software** dialog, select a Privilege Manager package and click **OK**.

   a. Sudo Plugin

   b. Privilege Manager Agent

   c. Privilege Manager Policy Server

   NOTE: If you do not see these software packages, verify the path to the software packages is correctly set in **System Settings**. Refer to Setting the Privilege Manager software path on page 172 for details.

4. On the **Log on to Host** dialog, enter your host credentials and click **OK** to start the installation process.

   NOTE: This task requires elevated credentials.

Configuring the primary policy server

The first policy server you configure is the primary policy server which holds the master copy of the policy file. Additional policy servers configured in the policy group are secondary policy servers. The primary policy server and any number of additional

secondary policy servers share a common policy. Adding secondary policy servers to a policy group allows you to load-balance the authorization requests on the policy servers.

To configure a primary policy server

1. From the **All Hosts** view, open the **Join or Configure** toolbar menu and navigate to **Configure Policy Server | As Primary Policy Server...**.

2. On the **Configure Primary Policy Server** dialog,

   a. Enter a policy group name in the text box.

      NOTE: When the configuration is complete, this new policy group will be automatically configured and activated in the Privilege Manager system settings. See Configuring a service account on page 169 for details.

   b. Choose the policy type: either sudo policy type (Privilege Manager for Sudo) or pmpolicy type (Privilege Manager for Unix).

      See Security policy management on page 118 for more information about the policy types.

3. Click **Advanced** to import an existing policy or a license file.

   If you configure Privilege Manager for Sudo using the default sudo policy type, Privilege Manager uses a copy of the /etc/sudoers file as its initial security policy if the file exists, otherwise it creates a generic sudoers file.

   NOTE: When you join a Sudo Plugin to a policy server, Privilege Manager for Sudo adds the following lines to the current local sudoers file, generally found in /etc/sudoers.

   ```
   ##
   ## WARNING: Sudoers rules are being managed by QPM4Sudo
   ## WARNING: Do not edit this file, it is no longer used.
   ##
   ## Run "/opt/quest/sbin/pmpolicy edit" to edit the actual sudoers
   rules.
   ##
   ```

   When you unjoin the Sudo Plugin, Privilege Manager for Sudo removes those lines from the local sudoers file.

   If you configure Privilege Manager for Unix using the pmpolicy type, Privilege Manager creates a profile-based (or role based) policy. This security policy simplifies setup and maintenance through use of easy-to-manage profile (or role) templates.

   a. In the Import policy data from box, enter a path to the policy data to override the default and import the initial security policy from the specified location.

      For example, enter

      ```
      /tmp/pmpolicy/pm.conf
      ```

   b. In the **Import license file from** box, click **Browse** to select a product

license file from the local file system.

You can skip this step initially. Privilege Manager comes with a 30-day trial license. After 30 days, Privilege Manager continues to allows you to run ten Sudo Plugin clients without a license, but requires a license for the PM Agents. See Software & Licenses settings on page 172 for details.

4. Enter the `pmpolicy` service account password in the **Join Password** box.

   NOTE: You will use this password when you add secondary policy servers or join remote hosts to this policy group.

5. Select the **Join agent or plugin to policy group** option if you want to join primary policy server to the policy group at this time.

   When you join a policy server to a policy group, you are indicating which policy group you want to use for policy verification. That is, you are enabling that host to validate security privileges against a single common policy file located on the primary policy server, instead of a policy file located on the local host.

   NOTE: Policy servers can only be joined to policy groups they host (that is, manage). You cannot join a Sudo Plugin host to a pmpolicy server group or the PM Agent host to a sudo policy server group.

   You can join the agent or plugin to the policy group later. See Joining the host to a policy group on page 111 for details.

6. On the **Log on to Host** dialog, enter the user credentials to access the selected host and click **OK**.

   This information is pre-populated if you saved the credentials for the host.

Joining the host to a policy group

When you join a host to a policy group, it enables that host to validate security privileges against a single common policy file located on the primary policy server, instead of on the host.

NOTE: To join a host to a policy group, the host must meet all of these conditions:

- When using a sudo policy type, to join a policy group, the selected hosts must have Sudo 1.8.1 (or higher), the Sudo Plugin software installed, and be added and profiled to the mangement console.

- When using pmpolicy type, the host must have the PM Agent software installed on it. See Installing Privilege Manager agent or plugin software on page 116.

- A service account must be configured. See Configuring a service account on page 169.

- A policy group must be active. See Activating policy groups on page 171.

- If you select multiple hosts to join, they must be of the same type (sudo or pmpolicy). However, when selecting multiple primary servers, the **Join** option will be disabled because each primary server belongs to a different policy group.

Policy servers can only be joined to policy groups they host (that is, manage). You cannot join a Sudo Plugin host to a pmpolicy server group or the PM Agent host to a sudo policy server group.

To join a host to a policy group

1. From the list on the **All Hosts** view, select one or more hosts that have the Privilege Manager software installed, open the **Join or Configure** toolbar menu, and choose **Join to Policy Group**.

   NOTE: The **Join to Policy Group** option is enabled when you select hosts that have the Privilege Manager software installed and are not already joined to a policy group.

   The toolbar button will not be active if

   - You have not selected any hosts.
   - You have selected hosts that are already joined.

2. On the **Policy Group** tab,

   a. Select the policy group to use for the policy verification.

      The **Policy group** drop-down menu lists the configured policy groups with the policy server type in parenthesis, either **pmpolicy** or **sudo**.

   b. Enter the pmpolicy service account password in the **Join password** box.

      NOTE: The **Join password** is the password for the pmpolicy service account that was set when you configured the primary server. See Configuring the primary policy server on page 109 for details.

3. On the **Failover** tab,

   a. Set the failover parameters, if you desire, and click **OK**.

      NOTE: If you set the failover parameter to random order, Privilege Manager ignores the ordering of the policy servers.

   b. Set the default policy server failover order within the policy group by ordering the hosts in the **Policy Server** list using the up and down arrows.

      Where there are two or more policy servers, Privilege Manager connects to the next available server when it cannot make a connection to a policy server.

      NOTE: To change the failover order, unjoin the host from the policy group and then rejoin it using new settings.

4. On the **Log onto Host** dialog, enter the user credentials to access the selected hosts and click **OK**.

   NOTE: This task requires elevated credentials. The mangement console pre-populates this information if you saved the credentials for the host.

   The **Task Progress** pane on the **All Hosts** view displays a progress bar and the final status of the tasks, including any failures or advisories encountered.

Unjoining host from policy group

When you unjoin a host from a policy group, the host will no longer check for privileges against the policy in the policy group.

To unjoin hosts from the policy group

1. Select one or more hosts that are joined to a policy group from the list on the **All Hosts** view.

2. Open the **Unjoin** toolbar menu and choose **Unjoin from Policy Group**.

3. On the **Unjoin host from policy group** dialog, enter your credentials to log on to the host and click **OK**.

   NOTE: This task requires elevated credentials.

Configure a secondary policy server

The *primary* policy server is always the first server configured in the policy server group; *secondary* servers are subsequent policy servers set up in the policy server group to help with load balancing. The "master" copy of the policy is kept on the primary policy server.

All policy servers (primary and secondary) maintain a working copy of the security policy stored locally. The initial working copy is initialized by means of a checkout from the repository when you configure the policy server. Following this, the policy servers automatically retrieve updates as required.

Configuring a secondary policy server

After you install and configure a primary policy server, you are ready to configure additional policy servers for load balancing purposes.

To configure a secondary policy server

1. Check the Policy Server for configuration readiness.

   See Checking policy server readiness on page 108 for details.

2. Install the *Privilege Manager Policy Server* package on the secondary server host.

   See Installing the Privilege Manager packages on page 109 for details.

3. From the **All Hosts** view, open the **Join or Configure** toolbar menu and navigate to **Configure Policy Server | As Secondary Policy Server**.

4. On the **Configure Secondary Policy Server** dialog,

a. Choose the policy group you want to associate with the secondary policy server.

b. Enter the `pmpolicy` service account password in the **Join password** box.

    NOTE: The **Join password** is the password for the `pmpolicy` service account that was set when the primary policy server was configured. See Configuring the primary policy server on page 109 for details.

c. Select the **Join agent or plugin to policy group** option, if you want to join the secondary policy server to the policy group at this time.

    When you join a policy server to a policy group, you are indicating which policy group you want to use for policy verification. That is, you are enabling that host to validate security privileges against a single common policy file located on the primary policy server, instead of a policy file located on the local host.

    NOTE: Policy servers can only be joined to policy groups they host (that is, manage). You cannot join a Sudo Plugin host to a pmpolicy server group or the PM Agent host to a sudo policy server group.

    You can join the server to the policy group later. See Joining the host to a policy group on page 111 for details.

5. On the **Log on to Host** dialog, enter the user credentials to access the selected host and click **OK**.

    This information is pre-populated if you saved the credentials for the host.

Install PM agent or Sudo plugin on a remote host

Once you have installed and configured the primary policy server, you are ready to install a PM Agent or Sudo Plugin on a remote host.

Checking client for policy readiness

Check Client for Policy Readiness performs a series of tests to verify that the specified hosts meet the minimum requirements to be joined to a policy server.

This command is only available, if

- a primary policy server is active in **System Settings**. See Configuring a service account on page 169 for details.

  -AND-

- the selected hosts are not already joined to a policy group.

NOTE: For the readiness check to finish successfully, the path to the Privilege Manager software packages must be correctly set in **System Settings**. See Setting the Privilege

To check hosts for policy readiness

1. Select one or more hosts on the **All Hosts** view of the **Hosts** tab, open the **Check** menu from the **Prepare** panel of the toolbar, and choose **Check Client for Policy Readiness**.

2. In the **Check Client for Policy Readiness** dialog, choose a policy group to use for the check and click **OK**.

3. On the **Log on to Host** dialog, enter user credentials to access the hosts and click **OK**.

   NOTE: This task requires elevated credentials.

   If you select multiple hosts, you are asked if you want to use the same credentials for all the hosts (default) or enter different credentials for each host.

   1. If you selected multiple hosts and the **Use the same credentials for all selected hosts** option, enter your credentials to log on to access the selected hosts and click **OK**.

   2. If you selected multiple hosts and the **Enter different credentials for each selected host** option, it displays a grid which allows you to enter different credentials for each host listed. Place your cursor in a cell in the grid to activate it and enter the data.

4. To check the results of the readiness check,

   a. Right-click the host on the **All Hosts** view of the **Hosts** tab, and choose **Readiness Check Results**.

   b. Choose **Policy Readiness** from the drop-down menu, if necessary.

The results of the **Check Client for Policy Readiness** check depend on whether you run it on a Sudo Plugin or PM Agent host.

Running the readiness check on a Sudo Plugin host performs these tests:

- Basic Network Conditions:
    - Hostname is configured
    - Hostname can be resolved
    - Reverse lookup returns it own IP
- Policy Server Connectivity:
    - Hostname of policy server can be resolved
    - Can ping the policy server
    - Can make a connection to policy server
    - Policy server is eligible for a join

- Sudo Installation:
    - sudo is present on the host
    - sudo is in a functional state
    - sudo is version 1.8.1 (or greater)
- Prerequisites to support off-line policy caching:
    - SSH keyscan is available
    - Policy server port is available

Running the check on a PM Agent host runs these tests:

- Basic Network Conditions:
    - Hostname is configured
    - Hostname can be resolved
    - Reverse lookup returns it own IP
- Privilege Manager for Unix Client Network Requirements
    - PM Agent port is available (TCP/IP port 12346)
    - Tunnel port is available (TCP/IP port 12347)
- Policy Server Connectivity:
    - Hostname of policy server can be resolved
    - Can ping the policy server
    - Can make a connection to policy server
    - Policy server is eligible for a join
    - Policy server can make a connection to the PM Agent on port 12346

A progress bar displays in the **Task Progress** pane. The final status of the task displays, including any failures or advisories encountered.

5. If the readiness check completed with failures or advisories, correct the issues and run the policy server readiness check again.

Installing Privilege Manager agent or plugin software

There are two Privilege Manager client software packages available to install onto a remote host that provide central policy management, granular access control reporting, as well as the ability to enable, gather, store and playback keystroke logs.

NOTE: Centralized policy management and keystroke logging are licensed separately.

- **Sudo Plugin** is a plug-in to Sudo 1.8.1 (or higher). With the Sudo Plugin installed, when you execute a command using sudo, the plugin sends the command to the policy server for evaluation rather than to the local host. This allows you to centrally

ONE IDENTITY™

manage a sudoers policy file located on the primary policy server that is used by all the Sudo Plugin clients.

NOTE: Before you install the Sudo Plugin on the host, ensure the host has Sudo 1.8.1 or higher installed on it. While you can install the Sudo Plugin without Sudo 1.8.1, you cannot join the host to a policy server without it.

- **Privilege Manager Agent**. With the PM Agent installed, when you execute a command, the client sends the command to the policy server for evaluation rather than to the local host. This allows you to centrally manage a pmpolicy file located on the primary policy server that is used by all the PM Agent clients.

To install the Privilege Manager client software and join to a policy group

1. Select one or more profiled hosts on the **All Hosts** view.

2. Click **Install Software** from the **Prepare** panel on the **All Hosts** view.

    NOTE: The **Install Software** toolbar menu is enabled when you select hosts that are profiled.

    The toolbar button will not be active if

    - You have not selected any hosts.

    - You have selected hosts that are not profiled.

        Note: When you install the **Privilege Manager Policy Server** it installs all three Privilege Manager packages on that host. However, once you have installed the Sudo Plugin onto a remote host, the mangement console will not allow you to install the PM Agent on that host; and once you have installed the PM Agent onto a remote host, the mangement console will not allow you to install the Sudo Plugin on that host.

3. On the **Install Software** dialog, select **Sudo Plugin** or **Privilege Manager Agent** and, optionally, select the **Join** option if you want to join the remote host to the policy group at this time. You can only install one package or the other.

    NOTE: If you do not see these software packages, verify the path to the software packages is correctly set in **System Settings**. Refer to Setting the Privilege Manager software path on page 172 for details.

    NOTE: When you join a remote host to a policy group, you are indicating which policy group you want to use for policy verification. That is, you are enabling that host to validate security privileges against a single common policy file located on the primary policy server, instead of a policy file located on the local host.

    You can join the remote host to the policy group later. See Joining the host to a policy group on page 111 for details.

    The *Join* process configures the host to run the Privilege Manager software with a policy group that you have previously activated in **System Settings**. If you have not already activated a policy group (as explained in Configuring a service account on page 169), you can install the Privilege Manager software without "joining" the host to a policy group at this time. Later, you can use the **Join to Policy Group** option from the **Join or Configure** menu to join the host to a policy group.

4. On **Join to Policy Group** tab,

a. Select the policy group to use for the policy verification.

b. Enter the `pmpolicy` password in the **Join password** box.

   The **Join password** is the password for the `pmpolicy` user that was setup when the Policy Server was configured. See Configuring the primary policy server on page 109 for details.

c. Set the default policy server failover order within the policy group by ordering the hosts in the *Policy Server* list using the up and down arrows.

   Where there are two or more policy servers, Privilege Manager connects to the next available server when it cannot make a connection to a policy server.

   NOTE: To change the failover order, unjoin the host from the policy group and then rejoin it using new settings.

5. At the **Install Software** dialog, click **OK**.

6. On the **Log on to Host** dialog, enter your host credentials and click **OK** to start the installation process.

   NOTE: This task requires elevated credentials.

   The mangement console displays the version of Privilege Manager in the **Version** column; and, if it is joined, the name of the policy group to which the host is joined in the **Status** column.

Security policy management

The security policy lies at the heart of Privilege Manager. It stipulates which users may access which commands with escalated privileges. Privilege Manager guards access to privileged functions on your systems according to rules specified in the security policy.

Privilege Manager for Unix supports two security policy types:

- **sudo policy type** – (default) uses a standard sudoers file as its security policy; that is, the **sudo policy** is defined by the `sudoers` file which contains a list of rules that control the behavior of `sudo`. The `sudo` command allows users to get elevated access to commands even if they do not have `root` access.

- **pmpolicy type** – uses an advanced security policy which employs a high-level scripting language to specify access to commands based on a wide variety of constraints. Privilege Manager policy is defined by `pm.conf`, the default Privilege Manager policy configuration file which contains statements and declarations in a language specifically designed to express policies concerning the use of `root` and other controlled accounts.

Management Console for Unix gives you the ability to centrally manage policy located on the primary policy server. You view and edit both types of policy from the **Policy** tab on the mangement console.

NOTE: To manage policy, you must log in either as the ***supervisor*** or an Active Directory account with rights to edit the policy file; that is, an account in the **Manage Sudo Policy**

or **Manage PM Policy** roles.

Opening a policy file

To open a policy

1. From the mangement console, navigate to the **Policy** tab and select either the **Sudo Policy Editor** view or the **PM Policy Editor** view.

    To use the **Sudo Policy Editor** or the **PM Policy Editor**, you must first add and profile a Privilege Manager policy server, configure the service account, and activate the policy group in the mangement console. See Activating policy groups on page 171 for details.

2. From the **Open** menu, select either:

    a. **Current version** to open the latest saved version of the policy that is currently in use by the mangement console for a policy group.

    b. **Version** to open the **Open Version** dialog from which you select a policy group and a version of a policy and click **OK** to open the file.

3. Once the policy is open you can modify it.

    NOTE: See Edit panel commands on page 119 for more information about editing the policy in the text editor.

4. After you modify the policy, save it.

    The policy is saved as a new version.

Rolling back the policy file

To revert back to a specific version of the policy file

1. From the **Open** menu, select **Version** to open the **Open Version** dialog.

2. Select a policy group and a version of a policy and click **OK**.

3. After you modify the policy, save it, accepting the warning message to save over the existing policy.

    The policy file is saved as a new version; not as the version number that you opened.

Edit panel commands

You can make changes to the policy in the text editor by either typing in changes or using the commands in the **Edit** panel to insert, copy, or paste text; check for errors; or disable and enable syntax highlighting.

As you edit a policy, the **Errors** pane lists syntax errors by line and column number. You can double click an error to navigate directly to the line containing the error.

To use the commands in the Edit panel to modify the policy file

1. Open the **Insert** menu and select one of these options:

   a. **Insert Local User** to open the **Select Local User** dialog.

   b. **Insert Local Group** to open the **Select Local Group** dialog.

   c. **Insert AD User** to open the **Select AD User** dialog.

   d. **Insert AD Group** to open the **Select AD Group** dialog.

      NOTE: The **Select AD** dialogs allow you to select a container from which to begin the search.

      The AD options are only available if you are logged in as an Active Directory user with rights to edit the policy file; that is, an account in the **Manage Sudo Policy** or **Manage PM Policy** role. Non-Unix-enabled groups require that you configure the Authentication Services sudo_vas group provider module. See *Configuring Sudo Access Control* in the *Authentication Services Administration Guide* for details.

   e. **Insert Host** to open the **Select host** dialog.

   f. **Insert Alias** to open the **Select Alias** dialog (only available in the Sudo Policy Editor.)

      NOTE: The **Select Alias** dialog allows you to filter the list of Alias names by:
      - All Aliases
      - Command Alias
      - Host Alias
      - Runas Alias
      - User Alias

   g. **Insert List** to open the **Edit Entries** dialog (only available in the PM Policy Editor).

      The **Edit Entries** dialog allows you to insert lists of data either manually, pasted from another file, or imported from a file. Separate multiple items with commas, for example:

      ```
      Fred, Ethel, Lucy
      ```

      The **Insert List** option allows you to copy and paste a comma-delimited lists into the text box and will automatically add the list of data objects with quotes around each individual entry. For example, if you paste the following into the **Add entries** box:

      ```
      /usr/bin/kill,/usr/bin/cp,/usr/bin/passwd,/usr/bin/head
      ```

when you click **Add**, the console lists the entries and puts quotes around each one, like this:
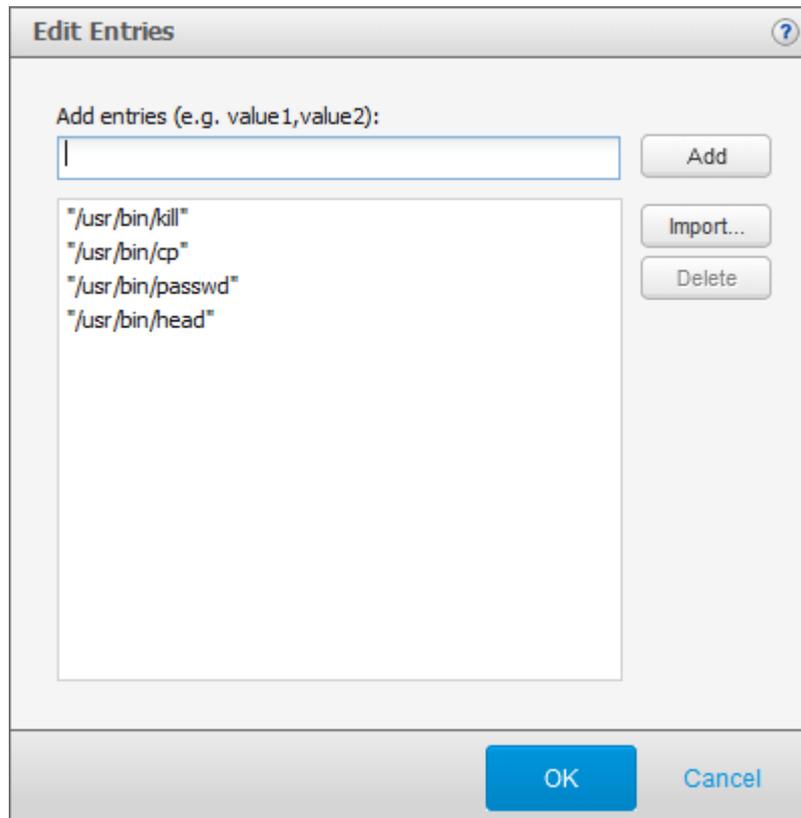
Once you have the objects listed on the **Edit Entries** dialog, click **OK** to include them in the policy.

> NOTE: For more information about the **Edit Entries** dialog, click the help link.

2. Click the **Error Check** button to validate the formatting and syntax of the policy file.

> NOTE: When checking sudo policy for errors, note that the `#include` and `#includedir` directives are currently ignored by Privilege Manager for Sudo. Remove or comment out any `#include` or `#includedir` directives in your sudo policy. Error-checking of policy files that contain a `#include` or `#includedir` may generate false errors. It is safe to ignore such errors when saving the sudo policy, but it is best practice to remove or comment out such directives.

The **Errors** pane is located across the bottom of the **Edit Policy** view and provides feedback on any syntax errors encountered when you click the **Error Check** button. You can double click an error to navigate directly to the line containing the error.

3. Select the **Highlight Syntax** option to view color-coded syntax.

> NOTE: Managing large policy files may affect the policy editor performance.

4. Use the controls in the **Search** panel to search for keywords in the policy file.

Type a text string and click **Next** or **Previous**.

Editing PM policy files

Privilege Manager roles (or profiles) define who, what, where, when, and how users are permitted to perform various privileged account actions.

When you open a PM Policy file for editing, it lists the roles associated with the policy using the following icons:

- Privilege Manager Role

- Privilege Manager Restricted Shell Role

NOTE: If a role is disabled, it is grayed out; if a role currently has an error, it displays .

From the **Privilege Manager Roles** view, you can perform the following tasks:

1. **Properties**

   View and modify privileged account actions for a role.

2. **Add Role**

   Type of roles you can add include:

   - Privilege Manager Roles
   - Privilege Manager Restricted Shell Roles

     Shell roles manage host access with secure shells.

   - New role based on an existing template

3. **Delete Role**

4. **Change Version**

   Opens a different version of the policy making that version the active policy.

5. **Policy Change Report**

   Review all policy modifications.

6. **Manage Defaults**

   Define policy defaults as global settings for all Privilege Manager roles.

Default roles (or profiles)

By default, Privilege Manager for Unix provides the following role profiles:

- **Privilege Manager Roles**

  - **admin**

Permits the root user on any host to submit any standard or 'normal' (that is, not a Privilege Manager Shell program) command as the root user on the local host.

- **demo**

  Permits any user on any host to submit the `id` and the `whoami` commands as the root user on the local host.

- **helpdesk**

  Permits users in the *helpdesk* UNIX group, on any host, to reset (change) any user's password on the local host by running the `passwd` command as root.

- **webadmin**

  Permits users in the *webadmin* UNIX group to start and stop the Apache webserver on the local host.

- **Privilege Manager Restricted Shell Roles**

  - **qpm4u_login**

    Permits any user to run a 'wrapped' standard shell program which enables keystroke logging for all commands the user runs.

  - **restricted**

    Permits any user to run any restricted Privilege Manager Shell program as the `root` user on the local host.

    NOTE: Because the shell runs in restricted mode, the following restrictions apply:

    - PATH, ENV and SHELL variables are read-only
    - User cannot change directory
    - User can only run programs in $PATH
    - User cannot run a command identified by an absolute/relative path
    - User cannot use I/O redirection

    NOTE:

    - Shell built-in commands are checked as well as normal executable commands.
    - A specified list of "dangerous" commands are forbidden, such as `passwd`, `shutdown`, and `kill`.
    - A specified list of benign commands are permitted without authorization.
    - A specified list of benign commands are permitted without authorization if the input to the command is from a pipe.

  - **root**

    Permits the `root` user to run any Privilege Manager Shell program in unrestricted mode, as the `root` user on the local host.

    NOTE:

- Shell built-in commands are permitted without authorization.
- Certain benign commands are permitted without authorization if the input to the command is from a pipe.
- Commands within a specified list are forbidden without authorization.

NOTE:

- Only the **admin**, **demo**, **root**, and **qpm4u_login** profile roles are enabled by default. You can enable (or disable) a profile role by selecting the **Enable keystroke logging** option in the role **General** Settings.

- The Access & Privilege reports provide information about what commands a user is allowed to run from each profile. See for details.

Modifying Privilege Manager role properties

Once you open a Privilege Manager policy, the console lists the roles and restricted shell roles associated with it.

To modify Privilege Manager role properties

1. From the **PM Policy Editor** view, double-click a role, select it and click **Properties**, or right-click the role and choose **Properties** from the context menu.

   To find a particular policy role,

   - Type a string in the **Search for role** box for either a name or a description. (This is case sensitive and searches dynamically.)
   - Sort or filter the list of roles by type (enabled roles, disabled roles, enabled shell roles, or disabled shell roles) from the **Role state** column represented with the exclamation mark (!).
   - Click a column title to sort the list of roles by name or description.

   NOTE: Disabled roles are greyed out. However, you can modify or delete disabled roles.

   When a role opens, the **Edit Role** dialog displays.

   See or for details about the role properties.

Overriding role property defaults

If a role property has a global default, it will be indicated by the "default override" check box to the left of the property, in a green background, and the default role property to the right, in a disabled state. If a property does not have a "default override" check box, there is no global default for that property. For example, the following screen indicates the **Enable role** property does not have a global default, but the **Enable keystroke logging** property does. The default for the **Enable keystroke logging** property is **Enabled**.

To override a global default

1. Select the override check box, change the role property, as needed, and click **OK**.

   When you override the global default, the value you specify takes precedence over the global default and remains effective even if the global default changes.

   > NOTES:
   >   - If you leave the global override check box deselected, the role uses the global default automatically. In the example above, the new role will have keystroke logging enabled and create the keystroke log in /var/opt/quest/qpm4u/iolog/ even though the override check boxes are not selected. If you *always* want keystroke logging to be enabled for this role even if the global default is changed in the future, select the override check box and leave the **Enable keystroke logging** option selected.
   >   - You can set a global default for the **Enable role** property, applicable to all roles, using the text editor. See Managing role defaults on page 133 for details.

Role property variables

Privilege Manager roles (or profiles) define who, what, where, when, and how users are permitted to perform various privileged account actions using variable values in the policy configuration file. You set the values for these user-defined variables in global_ profile.conf, the default Privilege Manager policy configuration file, using either a GUI editor or a text editor.

The following tables identify the policy variables associated with each GUI editor setting for both Privilege Manager roles and restricted shell roles. The **Manage Defaults** column

indicates which variables you can set as global defaults using the **Manage Defaults** button on the GUI editor; you must use the text editor to set global defaults for variables marked **No**. See Managing role defaults on page 133 for details.

Table 5: General Settings

GUI Editor Setting	Role/Shell	Policy Variable	Manage Defaults
General			
Description	Both	pf_profiledescription	No
Enable role	Both	pf_enableprofile	No
Trace level	Both	pf_tracelevel	Yes
Enable keystroke logging	Both	pf_enablekey-strokelogging	Yes
Keystroke log path	Both	pf_iologdir	Yes
Disable password logging	Both	pf_logpasswords	Yes
Password prompts	Both	pf_passprompts	Yes
Authentication			
Require authentication	Both	pf_enableau-thentication	Yes
Authenticate on host running command	Both	pf_authen-ticateonclient	Yes
PAM service	Both	pf_pamservice	Yes
Command line prompt	Both	pf_pamprompt	Yes
Allow scp / non-interactive SSH	Shell	pf_allowscp	Yes

Table 6: What Settings

GUI Editor Setting	Role/Shell	Policy Variable	Manage Defaults
Commands			
Path on host	Role	pf_authpaths	Yes
Commands	Role	pf_authcmds	Yes
Allow commands from authorized submit hosts	Role	pf_enablere-motecmds	Yes
Shell Commands			

ONE IDENTITY™

GUI Editor Setting	Role/Shell	Policy Variable	Manage Defaults
Accept only commands	Shell	pf_shellcom-mandsaccept	No
Reject commands	Shell	pf_shellcom-mandsreject	No
Authorize shell builtins	Shell	pf_checkbuiltins	No
Command rejection message	Shell	pf_shellreject	No
Pre-authorized Commands			
Commands allowed by shell	Shell	pf_shellallow	Yes
Commands allowed only from pipe	Shell	pf_shellallowpipe	Yes
Commands rejected by shell	Shell	pf_shellforbid	Yes

Table 7: Where Settings

GUI Editor Setting	Role/Shell	Policy Variable	Manage Defaults
Run Hosts			
Hosts where commands can run	Both	pf_authrunhosts	No
Submit Hosts			
Hosts where commands can be submitted	Role	pf_authsub-mithosts	No
Forbidden Run Hosts			
Hosts where members are forbidden to run commands	Role	pf_forbidrun-hosts	No
Forbidden Submit Hosts			
Hosts where members are forbidden to submit commands	Role	pf_forbid-submithosts	No

Table 8: Who Settings

GUI Editor Setting	Role/Shell	Policy Variable	Manage Defaults
Users			
Users authorized to run commands	Both	pf_authusers	No
Runas User	Both	pf_authuser	No

GUI Editor Setting	Role/Shell	Policy Variable	Manage Defaults
Groups			
Local and Unix-enabled AD groups	Both	pf_authgroups	No
Runas Group	Both	pf_authgroup	No
User must be member of author-ized group	Both	pf_useserver-groupinfo	No
AD Groups			
Non Unix-enabled AD Groups	Both	pf_authgroupsad	No
Default AD Domain	Both	pf_addomain	No

Table 9: When Settings

GUI Editor Setting	Role/Shell	Policy Variable	Manage Defaults
Time Restrictions			
Restrict by day, date, time	Both	pf_enable-timerestrictions	Yes
By Time Period	Both	pf_restrictionhours	Yes
By Date	Both	pf_restrictiondates	Yes
By Day of Week	Both	pf_restrictiondow	Yes

Table 10: How Settings

GUI Editor Setting	Role/Shell	Policy Variable	Manage Defaults
Shell Settings			
PM secure shells allowed to run	Shell	pf_allowshells	Yes
Run in restricted mode	Shell	pf_restricted	Yes
Environment variables that cannot change	Shell	pf_shellreadonly	Yes
Shell execution directory	Shell	pf_shellcwd	Yes
Shell session PATH	Shell	pf_shellpath	Yes

NOTE: You can not manage the following variables using the GUI editor; you must use the text editor:

- pf_cpolicy -- the path to a customer-specific pmpolicy file included after matching the user to a profile, but before authenticating the user. If configured, add this file to the repository, and identify it using a relative path (relative to the policy directory).
- pf_realshell -- specifies the actual shell program to run, in the case of pmloginshell. **Note**: This variable is obsolete in vr 5.6.0 and only provided here only for reference to the obsolete vr 5.5.2 pmloginshell program.
- pf_forbidsubmithostsad -- Active Directory host groups where members are forbidden to submit commands.
- pf_authsubmithostsad -- Active Directory host groups where commands can be submitted.
- pf_forbidrunhostsad -- Active Directory host groups where members are forbidden to run commands.
- pf_authrunhostsad -- Active Directory host groups where commands can run.

Adding a Privilege Manager role

To create a new Privilege Manager role

1. From the **PM Policy Editor** view, click the **Add Role** button.
2. From the **Select Role Type** dialog, choose **Privilege Manager Role** and click **OK**.

   The **New Role** dialog displays and allows you to specify:
   - **General** Settings
     - General Settings
     - Authentication Settings
     - User Defined Variables
   - **What** Settings
     - Commands
   - **Where** Settings
     - Run Hosts Settings
     - Submit Hosts Settings
     - Forbidden Run Hosts Settings
     - Forbidden Submit Hosts Settings
   - **Who** Settings
     - Users Settings
     - Groups Settings
     - AD Groups Settings

- **When** Settings
    - Time Restrictions Settings

See Overriding role property defaults on page 124 for more information about specifying role-specific overrides for a specific property.

Add a Privilege Manager restricted shell role

To add or modify shell roles

1. From the **PM Policy Editor** view, click the **Add Role** button.
2. From the **Select Role Type** dialog, choose **Privilege Manager Restricted Shell Role** and click **OK**.

    The **New Role** dialog displays and allows you to specify:

    - **General** Settings
        - General Settings
        - Authentication Settings
        - User Defined Variables
    - **What** Settings
        - Shell Commands
        - Pre-authorized Commands
    - **Where** Settings
        - Run Hosts Settings
    - **Who** Settings
        - Users Settings
        - Groups Settings
        - AD Groups Settings
    - **When** Settings
        - Time Restrictions Settings
    - **How** Settings
        - Shell Settings

See Overriding role property defaults on page 124 for more information about specifying role-specific overrides for a specific property.

Adding Privilege Manager role based on an existing role

To add a new role based on an existing role

1. From the **PM Policy Editor** view, click the **Add Role** button.

2. From the **Select Role Type** dialog, choose **Use an existing role as a template for the new role**.

3. Select an existing role to use as the template and click **OK**.

   Refer to Default roles (or profiles) on page 122 for a description of the roles provided by Privilege Manager for Unix.

Saving policy files

To save a policy file

1. Click **Save** to save the policy.

   You can also click the ▣ (close) icon in the upper-right of the policy panel to close the policy. If you have made changes, you are prompted to save them.

   The policy is saved as a new version; not as the version number that you opened.

   > NOTE: If the file contains unresolved syntax errors when you click **Save**, the editor gives you an option to **Save with Errors**. One Identity recommends that you correct errors *before* saving to ensure that the policy server does not reject all commands.

   > The **Errors** pane is located across the bottom of the **Edit Policy** view and provides feedback on any errors encountered when you click the **Error Check** button. While in the text editor, error checking only checks for syntax errors; when in the GUI editor, error checking also checks that the policy is correctly configured to use profile-based (or role based) policy. Double-clicking an error message takes you to the line in question.

2. Enter a comment describing the changes and click **OK** to save the latest revision of the policy.

   The new version of the policy becomes the latest version in use by Privilege Manager.

Deleting Privilege Manager role

To delete Privilege Manager role

1. From the **PM Policy Editor** view, select a role and click **Delete Role**.

2. From the **Delete Role** dialog, click **Delete**.

3. Confirm the delete.

NOTE: Deleting a role from the policy may prevent users from running commands or completing tasks that are allowed by this role.

Changing policy version

To change the policy version

1. From the **PM Policy Editor** view, click the **Change Version** button.

   The **Change Version** dialog displays.

2. Select a version of the policy to open.

3. Enter a change commit message and click **OK**.

4. Confirm your desire to replace the existing policy currently in use by Privilege Manager for Unix.

   The policy file is saved as a new version and becomes the currently active policy.

Reviewing policy changes

The **Policy Changes** report provides the details of changes made to the policy.

To create the Policy Changes report

1. From the **PM Policy Editor** view, click the **Policy Change Report** button.

   You can also navigate to this report from the **Reporting** tab on the mangement console.

   The report opens a new **Policy Changes** tab on the **Reporting** view.

2. Select a policy group from the drop-down menu.

3. Choose one of these options:

   a. Show all changes to the policy.

   b. Show only changes for a specific pmpolicy file (not available for sudo-based policy).

   c. Show only changes for a particular version of it.

4. Open the **Export** drop-down menu and select the format you want to use for the report: **PDF** or **CSV**.

   It launches a new browser or application page and displays the report in the selected format.

NOTE: When generating multiple reports simultaneously or generating a single report that contains a large amount of data, One Identity recommends that you increase the JVM memory. See JVM memory tuning suggestions on page 214 for details.

ONE IDENTITY™

Managing role defaults

You can set global policy defaults for Privilege Manager roles and restricted shell roles. When you set a global default for a property, it applies to all roles unless you have set a specific property in an individual role to override the global policy default. See Overriding role property defaults on page 124 for more information about specifying role-specific overrides for a specific property.

To manage role defaults

1. From the **PM Policy Editor** view, click **Manage Defaults**.

   The **Role Defaults** dialog displays allowing you to specify the following settings:

   - Role **General** Settings
       - General Settings
       - Authentication Settings
       - User Defined Variables
   - Role **What** Settings
       - Pre-authorized Commands
   - Role **When** Settings
       - Time Restrictions Settings
   - Role **How** Settings
       - Shell Settings

   NOTE: Not all variables can be set as global defaults using the **Manage Defaults** button on the GUI editor; however, you can set any variable as a global default using the text editor. See Role property variables on page 125 for a list of variables.

2. For example, to set a global default for the **Enable role** property you must use the text editor.

   a. From the **PM Policy Editor** view, click the **Text Editor** button in the top-right corner.

   b. Double-click the **global_profile.conf** configuration policy name or right-click and choose **Open as text**.

   c. Add the following line to the global_profile.conf file:

   ```
   pf_enableprofile = true;
   ```

   d. Click **Save**, enter a commit description, and click **OK**.

Modifying PM policy files with the text editor

When you open a policy from a policy group that is configured to use a pmpolicy rather than a sudo policy type, the mangement console allows you to edit the policy files that pertain to that policy using either a GUI editor or a text editor, however there are certain variables that you can *only* modify by means of the text editor.

To modify policy files using the text editor

1. From the **Policy** tab, navigate to the **PM Policy Editor** view.

2. Click the **Text Editor** button in the top-right corner of the **PM Policy Editor** view.

3. From the **Open** menu, select either:

   a. **Current version** to open the latest saved version of the policy that is currently in use by the mangement console for a policy group.

   b. **Version** to open the **Open Version** dialog from which you select a policy group and a version of a policy and click **OK** to open the file.

   When you open a policy-based policy file in the text editor, the mangement console lists the policies in the policy group in the left navigation tree:

   - Under the **Configuration** folder, it lists the .conf files from the policy group and opens the default Privilege Manager policy configuration file, pm.conf.

   - Under the **Restricted Shell Roles** folder, it lists the .shellprofile files from the policy group.

   - Under the **Roles** folder, it lists the .profile files from the policy group.

   NOTES:

   - **Roles** in the mangement console's GUI editor are "profiles" in the policy.

   - You can switch back and forth between the GUI editor and the text editor. To switch back to the GUI editor once in the text editor, click the **GUI Editor** button in the top-right corner of the **PM Policy Editor** view.

4. To open a specific policy in the text editor, either double-click the policy or right-click it and choose **Open as text** from the context menu.

   When using the text editor:

   a. Boolean values are represented by check boxes in the GUI Editor.

      For example, 'pf_enableprofile = false' is represented as an unchecked check box.

   b. String values are represented by a text field with a field label in the GUI Editor.

      For example, 'pf_profiledescription= "Some Descriptive Text"' is represented as 'Description:[template]'.

   c. Arrays or lists are represented as text boxes in the GUI Editor.

      For example, 'pf_authgroups = {"admins", "dbas"}; is represented as a text box where the user can enter multiple values.

5. Click the **Add** button in the **Policy** panel to add a new policy file.

The **Add Policy File** dialog opens.

   a. Select the type of policy file you want to add.

     Choose

- **Privilege Manager Configuration File**
- **Privilege Manager Role**
- **Privilege Manager Restricted Shell Role**

   b. Enter a name for the new policy file.

     Note that the file type changes according to the type of policy file you selected.

   c. Optionally, select the **Use an existing file as a template** option.

     The list of files to choose changes according to the type of policy file you selected.

   d. When you click **OK** on the **Add Policy File** dialog, it adds the new file to the left navigation tree.

6. Click the **Save** button to save the current policy file; click **Save All** to save all modified policy files.

7. Click the **Close** button in the **Policy** panel to close all modified policy files. If you have made changes, you are prompted to save them.

   NOTE: You can also click the ▣ (close) icon in the upper-right of the text editor window to close the policy. When you close a modified policy file without saving changes, the policy name in the left-hand navigation panel is italicized. Later, you can click the **Save All** button to save any changes you have made to that policy.

8. To delete a policy, click the **Delete** button in the **Policy** panel and confirm your request.

9. To discard you changes, right-click the policy name and choose the **Revert** option from the context menu. You are prompted to confirm your request to revert the changes to the selected file.

NOTE: See Edit panel commands on page 119 for more information about editing the policy in the text editor.

Reviewing the Access and Privileges by User report

The **Access and Privileges by User** report identifies the hosts where the selected user can login, the commands that user can run on each host, as well as the "runas aliases" information for that user.

To create the Access & Privileges by User report

1. From the mangement console, navigate to **Reporting**.

2. From the **Reports** view, double-click the **Access and Privileges by User** report name.

   The report opens a new **Access & Privileges by User** tab on the **Reporting** view.

3. Choose the type of user to include in the report: a local user or Active Directory user.

4. Click **Browse** to select the user name.

5. Select the **Show detailed report** option.

6. Open the **Export** drop-down menu and select the format you want to use for the report: **PDF** or **CVS**.

   It launches a new browser or application page and displays the report in the selected format.

NOTE: When generating multiple reports simultaneously or generating a single report that contains a large amount of data, One Identity recommends that you increase the JVM memory. See JVM memory tuning suggestions on page 214 for details.

Reviewing the Access and Privileges by Host report

The **Access and Privileges by Host** report identifies all users with logon access to a host and the commands users can run on the host. To run this report you must have an active policy group; you can only include hosts that are joined to a policy group in the report.

To create the Access & Privileges by Host report

1. From the mangement console, navigate to **Reporting**.

2. From the **Reports** view, double-click the **Access and Privileges by Host** report name.

   The report opens a new **Access & Privileges by Host** tab on the **Reporting** view.

3. Browse to select the host for which you want to create the report.

4. Select the **Show detailed report** option.

5. Open the **Export** drop-down menu and select the format you want to use for the report: **PDF** or **CSV**.

   It launches a new browser or application page and displays the report in the selected format.

NOTE: When generating multiple reports simultaneously or generating a single report that contains a large amount of data, One Identity recommends that you increase the JVM memory. See JVM memory tuning suggestions on page 214 for details.

Event logs and keystroke logging

Privilege Manager enables event logging. Each time a command is run, the policy server *accepts* or *rejects* the requested command according to the rules in the policy and creates an event (audit) log. The policy server records the keystroke input and terminal output for each accepted command, creating comprehensive "keystroke logs" files. With these logs, you can perform forensic-level auditing of any command executed.

Event logs are always captured and stored on the policy servers in `/var/opt/quest/qpm4u/pmevents.db`; keystroke logs are stored at `var/opt/quest/qpm4u/iolog`.

> NOTE: You can use the `iolog_dir` and `iolog_file` policy options to reconfigure the iolog file location. For more information about the policy options, refer to the *Privilege Manager Administration Guide*.

You can view event logs or replay keystroke logs from the **Policy** tab of the mangement console if you are logged in either as the ***supervisor*** or an Active Directory account with rights to audit the policy file; that is, an account in the **Audit Sudo Policy** or **Audit PM Policy** role.

> BEST PRACTICE: As a best practice, One Identity recommends that you set up a separate policy server for archiving and viewing logs.

Enabling keystroke logging

To enable keystroke logging for sudo policy

1. From the mangement console, navigate to **Policy | Sudo Policy Editor**.

2. Open the **Open** menu and select **Current version** to open the latest saved version of the policy file that is currently in use by the mangement console. See Opening a policy file on page 119 for details.

3. Add the following line to the policy file to enable keystroke logs:

   ```
   Defaults log_output
   ```

4. Add an entry for a local user in the form **who where = (as_whom) what**. For example:

   ```
   localuser     ALL=(ALL)     ALL
   ```

   where *localuser* is a local user account name.

   > NOTES:
   > - This allows *localuser* to perform any command on any machine as any user.
   > - To set up a local user, see Adding a local user on page 64.

5. Save and close the policy.

To enable keystroke logging for pmpolicy

1. Using the GUI editor, open the role's **General** setting page.

2. Select the **Enable keystroke logging** option.

Recording keystrokes

Privilege Manager only generates a keystroke log when the policy server accepts a command and keystroke logging is enabled in the policy. When the policy server *accepts* a command, Privilege Manager records the keystrokes and stores them on the policy server. If the policy server *rejects* a command, Privilege Manager does not record keystrokes nor does it generate a log.

To generate a keystroke log

1. Log into the host on which the Privilege Manager software is installed as a non-privileged user specified in the policy.

2. At the command prompt, enter:

   ```
   sudo bash
   ```

   Enter your password.

   When you enter **sudo bash**, it opens a new shell.

3. At the new shell's command prompt, enter the following lines:

   ```
   echo "This is fun."
    echo "My keystrokes are being recorded"
    whoami
    id
   ```

   > NOTE: For a fun demonstration, type **echo"This is a mistake"** and then backspace over **a mistake** and enter **fixed**. When you replay the keystroke log you will see that it records every keystroke!

4. Enter **exit** to close the bash shell.

   It records every keystroke after you enter **sudo** until you enter **exit**.

You are now ready to replay your keystroke log from the mangement console.

Listing events and replaying keystroke logs

Keystroke logs are related to events. When you run a command, such as **sudo whoami**, the policy server either *accepts* or *rejects* the command based on the rules in the policy. When the policy server accepts the command, it creates an event and a corresponding

keystroke log. If it rejects the event, it does not create a keystroke log. In order to view a keystroke log, you must first list events.

NOTE: To record and replay keystroke logs, you must log in either as the ***supervisor*** or an Active Directory account with rights to audit the policy file; that is, an account in the **Audit Sudo Policy** or **Audit PM Policy** role.

To list events and replay keystroke logs

1. From the mangement console, navigate to **Policy | Event Logs**.

   NOTE: You can also access **Event Logs** from these context menus:

   - From the host list on the **All Hosts** view, right-click a host name and choose **Find event logs**.
   - From the console **All Local Users** tab, right-click a user name and choose **Find event logs**.
   - From a host's properties **Users** tab, right-click a user name and choose **Find event logs**.
   - From the console **Active Directory** tab, right-click an AD object name and choose **Find event logs**.

2. Select options in the search controls on the **Find Event Logs** pane, and click **Find**.

   For example, you can search for all events logged for a particular user, or all events logged on a particular host, or you can find events logged during a specific date and time.

   - In the **Policy Group** box, select a policy group name.
   - In the **Where user is** box, enter or select either a local user or Active Directory user.
   - In the **Where Host is** box, select or enter either a fully qualified host name format (**myhost.mycompany.com**) or a short name format (**myhost**), depending on how host names are resolved and the use of the short name setting in the `pm.settings` file.

     NOTE: Host names may appear in the event logs and keystroke log files in either format. To ensure you match a host name, when you specify host name search criteria, use the short host name format with an asterisk wild card (**myhost***).

   - In the **Log contains** box, enter an optional keyword to search for in the contents of all logs.

     For example, you can find events that pertain to the usage of a specific command or content of the command output.

   - In the **Log status** box, choose to list all logs reporting **Accepted** events, **Rejected** events, or both types of events.

3. Click the **Replay keystroke log** button next to a listed event to load the log for replay.

   A **Replay Log** tab displays.

4. Click the **Play** button (▶) to replay the log.

Replay log controls

▶ ▶| |◀ ■ | ▸▸▸ 1x | [████████████████████_____] | 📋 Text View
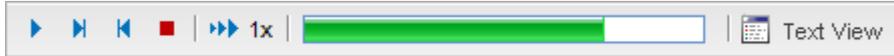
To use the replay log controls

1. Click ▶ , the **Play** button, to start or pause the log replay.

2. Click ▶| , the **Step Forward** button, to step forward through the keystrokes.

   NOTE: The **Step Forward** and **Step Backwards** buttons are not enabled while the log is replaying.

3. Click |◀ , the **Step Backwards** button, to step backwards through the keystrokes.

4. Click ■ , the **Stop** button, to stop the replay and reset the log back to the beginning.

5. Click ▸▸▸, the **Replay Speed** button, to change the speed of the replay. Clicking this button repeatedly steps through speed selections of 1 to 5 times the normal speed.

6. Click 📋 Text View , the **Text View** button, to display the entire replay log as text without replaying it.

   NOTE: To close a text view of a log, click the **Text View** button again.

Reporting

Management Console for Unix enables administrators to quickly and easily provide auditors with granular reports on Unix identity information, including the highly desirable assessment of which Active Directory user can authenticate on specific Unix systems. By consolidating the generation and viewing of reports within the console, Management Console for Unix reduces the time and effort required to create key reports that traditionally required multiple collections, data collation, and manual processes across multiple Unix systems.

The topics in this section explain how to export reports for the hosts managed through the mangement console. It also provides a description of the reports available on the **Reporting** tab.

Running reports

You can run various reports that capture key information about the Unix hosts you manage from the mangement console and the Active Directory domains joined to these hosts from the **Reports** view on the **Reporting** tab.

NOTE: The Active Directory reports are only available when you are logged on as an Active Directory account in the **Manage Hosts** role.

To run reports

1. Ensure the hosts for which you want to create reports have been recently profiled.

   Reports only generate data gathered from the clients during a *Profile* procedure. Profiling imports information about the host, including local users and groups.

   NOTE: You can configure the mangement console to profile hosts automatically.

   See Automatically profiling hosts on page 42 for details.

2. From the mangement console, click the **Reporting** tab.

3. From the **Reports** view, expand the report group names to view the available reports, if necessary.

- **Host Reports**

  Unix host information gathered during the profiling process

- **User Reports**

  Local and Active Directory user information

- **Group Reports**

  Local and Active Directory group information

- **Access & Privileges Reports**

  User access information

- **License Usage Reports**

  Product licensing information.

4. Use one of the following methods to select a report:

   - Double-click a report name in the list (such as the **Unix Host Profiles** report).

   - Right-click a report name and select **Run report**.

   - Click the report icon ⬈ next to a report.

   The selected report name opens a new tab on the **Reports** view which describes the report and provides some report parameters you can select or clear to add or exclude details on the report.

5. Optionally clear parameters to exclude information from the report.

6. To create a report, either

   a. Click **Preview** to see a sample of the report in a browser.

   b. Open the **Export** drop-down menu and select the format you want to use for the report: **PDF** or **CSV** (if available).

   NOTE:

   If the CSV report does not open, you may need to reset your internet options. See CSV or PDF reports do not open on page 198 for details.

By default, the mangement console creates reports in the application data directory:

- On Windows:

  ```
  %SystemDrive%:\ProgramData\Quest Software\Management Console for
  Unix\reports
  ```

- On Unix/Linux:

  ```
  /var/opt/quest/mcu/reports
  ```

NOTE: You may need to reconfigure your browser preferences to allow you to save the report in a specific folder.

It launches a new browser or application page and displays the report in the selected format.

NOTE: When generating multiple reports simultaneously or generating a single report that contains a large amount of data, One Identity recommends that you increase the JVM memory. See JVM memory tuning suggestions on page 214 for details.

Reports

The mangement console provides comprehensive reporting which includes reports that can help you plan your deployment, consolidate Unix identity, secure your hosts and troubleshoot your identity infrastructure. The following table lists the reports that are available in Management Console for Unix.

NOTE: Report availability depends on several factors:

- **User Log-on Credentials**: While some reports are available when you are logged in as *supervisor*, there are some reports that are only available when you are logged on as an Active Directory user. See Active Directory configuration on page 165 for details.

- **Roles and Permissions**: Reports are hidden if they are not applicable to the user's console role. For example, you must have an activated policy server to activate the sudo-related reports. See Console Roles and Permissions system settings on page 161 for details.

Host reports

Table 11: Host reports

Report	Description
Authentication Services Readiness	Provides a snapshot of the readiness of each host to join Active Directory. This report is best used for planning and monitoring migration projects. The basic report includes the following information:

- Total number of hosts
- Total number, percentage and names of the hosts ready to join
- Total number, percentage and names of the hosts ready to join with advisories
- Total number, percentage and names of the hosts not ready to join
- Total number of hosts not checked for AD readiness

Use the following report parameters to define details to include in the report.

ONE IDENTITY™

Report	Description
	- Joined to AD - Ready to Join AD - Ready to Join AD with Warnings - Not Ready to Join AD - Not Checked for Readiness NOTE: This report is available when you are logged on as the ***supervisor*** or an Active Directory account in the **Manage Hosts** role.
Privilege Manager Readiness	Provides a snapshot of the readiness of each host to join a policy group. The basic report includes the following information: - Total number of hosts - Total number, percentage and names of the hosts ready to join - Total number, percentage and names of the hosts not ready to join - Total number of hosts not checked for readiness Use the following report parameters to define details to include in the report. - Joined to a policy group - Ready to join a policy group - Ready to join a policy group with warnings - Not ready to join a policy group - Not checked for readiness NOTE: This report is available when you are logged on as the ***supervisor*** or an Active Directory account in the **Manage Sudo Policy** role or the **Audit Sudo Policy** role.
Unix Computers in AD	Lists all Unix computers in Active Directory in the requested scope. By default, this report is created using the default domain as the base container. Browse to search Active Directory to locate and select a different base container to begin the search. NOTE: This report is available when you are logged on as an Active Directory account in the **Manage Hosts** role.
Unix Host Profiles	Summarizes information gathered during the profiling process of each managed host. This report includes the following information: - Total number of hosts included in the report - Host Name, IP Address, OS, Hardware - Sudo version number

ONE IDENTITY™

Report	Description
	Use the following report parameters to define details to include for each host. • Authentication Services Properties • Privilege Manager Properties • Local Users • Local Groups • Host SSH Keys • Installed One Identity Software NOTE: This report is available when you are logged on as the ***supervisor*** or an Active Directory account in the **Manage Hosts** role.

User reports

Table 12: User reports

Report	Description
AD User Conflicts	Returns all users with Unix User ID numbers (UID numbers) assigned to other Unix-enabled user accounts. By default, it creates this report using the default domain as the base container. Browse to search Active Directory to locate and select a different base container to begin the search. NOTE: This report is available when you are logged on as an Active Directory account in the **Manage Hosts** role.
Local Unix User Conflicts	Identifies local user accounts that would conflict with a specified user name and UID on other hosts. You can use this report for planning user consolidation across your hosts. This report includes the following information: • Host Name, DNS Name or IP Address where a conflict would occur • User Name, UID Number, Primary GID Number, Comment (GECOS), Home Directory and Login Shell for each host where conflicts exist Use the following report parameters to define the user name and UID number that would cause a conflict with existing local user accounts: • User Name is • UID Number is NOTE: This report is available when you are logged on as the ***supervisor*** or an Active Directory account in the **Manage Hosts** role.

ONE IDENTITY™

Report	Description
Local Unix Users	Lists all users on all hosts or lists the hosts where a specific user account exists in `/etc/passwd`. This report includes the following information: • Host Name, DNS Name or IP Address where the user exists • User Name, UID Number, Primary GID Number, Comment (GECOS), Home Directory, and Login Shell for each host where the user exists If you do not define a specific user, it includes all local users on each profiled host in the report. To locate a specific user, use the following report parameters: • User Name contains • UID Number is • Primary GID Number is • Comment (GECOS) contains • Home Directory contains • Login Shell contains NOTE: When you specify multiple report parameters, it uses the AND expression; therefore, ALL of the selected parameters must be met in order to locate the user account. NOTE: This report is available when you are logged on as the **_supervisor_** or an Active Directory account in the **Manage Hosts** role.
Local Unix Users with AD Logon	Identifies the local user accounts that are required to use Active Directory credentials to log onto the Unix hosts. This report includes the following information for hosts that are joined to an Active Directory domain: • Host Name, DNS Name or IP Address of hosts where users exist that are required to log on using their AD credentials • User Name, UID Number, Primary GID Number and Comment (GECOS) of local user account • The SAM account Name of the Active Directory account that the local user account must use to log on NOTE: This report only includes hosts joined to an Active Directory domain with a Authentication Services 4._x_ agent. NOTE: This report is only available when the host has Authentication Services 4._x_ or later installed and is joined to Active Directory. You must be logged in with an Active Directory account in the **Manage Hosts** role.
Master /etc/-passwd List	Provides a consolidated list of all user accounts from all hosts, excluding any local users marked as system users. This report includes the following information:

Report	Description

- Username
- Empty password
- UID
- GID
- GECOS
- Home directory path
- Account's shell

You can consolidate the list of user accounts by matching values for accounts across multiple hosts. Accounts found with matching values are listed as a single local account. This list is best used for migrating local users to Active Directory.

Indicate how you want to match user accounts by selecting the value parameters that you want to match:

- Username
- UID
- GID
- GECOS
- Home Directory
- Shell

Optionally, you can include the host name for the accounts, as well:

- Include the host name for accounts

NOTE: If you select the **Include the host name for accounts** option, the mangement console adds a column to the `Master_etc_passwdList .csv` file to identify the host for each user account. One Identity provides the **Host** column information to help you resolve the entries in the file. However, before you import the `.cvs` file into the **Unix Account Import Wizard**, you must remove the **Host** column.

You can easily migrate local users to Active Directory by exporting the *Mater /etc/passwd List* report, then importing it into the **Unix Account Import Wizard**, accessible from the Control Center's **Tools** link. The **Unix Account Import Wizard** is a versatile tool that helps migrate Unix account information to Active Directory. It is especially well suited to small, one-shot import tasks such as importing all the local user accounts from a specific Unix host. The **Unix Account Import Wizard** can import Unix data as new user and group objects or use the data to Unix-enable existing users and groups.

NOTE: This report is available when you are logged on as the ***supervisor***

Report	Description
	or an Active Directory account in the **Manage Hosts** role.
Unix-Enabled AD Users	Lists all Active Directory users that have Unix user attributes.

NOTE:

- A User object is considered to be 'Unix-enabled' if it has values for the UID Number, Primary GID Number, Home Directory and Login Shell.
- If Login Shell is `/bin/false`, the user is considered to be disabled for Unix or Linux logon.
- Account Disabled indicates whether the Active Directory User account is enabled or disabled.

By default, it creates this report using the default domain as the base container. Browse to search Active Directory to locate and select a different base container to begin the search.

NOTE: This report is only available if you have configured the mangement console to recognize Active Directory objects (see Configuring the console to recognize Unix attributes in AD on page 101), and you are logged on as an Active Directory account in the **Manage Hosts** role.

Group reports

Table 13: Group reports

Report	Description
AD Group Conflicts	Lists all Active Directory groups with Unix Group ID (GID) numbers assigned to other Unix-enabled groups.
	By default, it creates this report using the default domain as the base container. Browse to search Active Directory to locate and select the base container to begin the search.
	NOTE: This report is available when you are logged on as an Active Directory account in the **Manage Hosts** role.
Local Unix Groups	Identifies the hosts where a specific group exists in `/etc/group`. This report includes the following information: • Host Name, DNS Name or IP Address where the group exists • Group Name, GID Number, and members for each host where the group exists If you do not specify a group, it includes all local groups on each profiled host in the report.

ONE IDENTITY™

Report	Description
	To locate a specific group, use the following report parameters:

- Group Name contains
- GID Number is
- Member contains
- Include all group members in report

NOTE: The **Member contains** field accepts multiple entries separated by a comma. Spaces are taken literally in the search. For example, entering:

- **adm, user** searches for members whose name contains 'adm' or 'user'
- **adm,user** searches for members whose name contains 'adm' or 'user'.

NOTE: When you specify multiple report parameters (for example, **Group Name contains**, **GID Number is**, and **Member contains**), it uses the AND expression; therefore, ALL of the selected parameters must be met in order to locate a group.

In addition, it includes all of the group members in the report by default, but you can clear the **Include all group members in report** option.

NOTE: This report is available when you are logged on as the *supervisor* or an Active Directory account in the **Manage Hosts** role.

Report	Description
Unix-Enabled AD Groups	Lists all Active Directory groups that have Unix group attributes.

NOTE: A Group object is considered "Unix-enabled" if it has a value for the GID Number.

By default, it creates this report using the default domain as the base container. Browse to search Active Directory to locate and select a different base container to begin the search.

NOTE: This report is only available if you have configured the mangement console to recognize Active Directory objects (see Configuring the console to recognize Unix attributes in AD on page 101), and you are logged on as an Active Directory account in the **Manage Hosts** role.

Access & Privileges reports

NOTE: The Access & Privileges reports do not report on users and groups from a NIS domain.

Table 14: Access & Privileges reports

Report	Description
Access & Privileges by Host	Identifies all users with log-on access to hosts and the commands the users can run on the hosts. This report includes the following information: • Total number of users that can log on to the host • The users that can log on to the host • The commands users can run on the host • The runas aliases for which the user can run commands on the host • The commands the runas alias can run on the host **Browse** to select a host. Optionally, select the **Show detailed report** option. NOTE: This report is available when you are logged on as the *supervisor* or as an Active Directory account in the **Manage Sudo Policy**, **Manage PM Policy**, **Audit Sudo Policy**, or **Audit PM Policy** roles. You must have an active policy group for Privilege Manager to run this report; you can only include hosts that are joined to a policy group.
Access & Privileges by User	Identifies the users with log on access to hosts, the commands that user can run on each host, and the "runas aliases" information for that user. This report includes the following information: • Total number of hosts where the user can logon • The hosts where the user can logon • The commands the user can run on each host • The runas aliases for which the user can run commands on each host • The commands the runas alias can run on each host Use the following report parameters to specify the user to include in the report: • A local user (default) • An AD user **Browse** to select a user. Optionally select the **Show detailed report** option. NOTE: This report is available when you are logged on as the *supervisor* or as an Active Directory account in the **Manage Sudo Policy**, **Manage PM Policy**, **Audit Sudo Policy**, or **Audit PM Policy** roles. You must have an active policy group for Privilege Manager to run this report; you can only include hosts that are joined to a policy group.
Commands	Provides details about the commands executed by users on hosts joined to

Report	Description
Executed	a policy group, based on their privileges and recorded as events or captured in keystroke logs by Privilege Manager. This report allows you to search for commands that have been recorded as part of events or keystroke logs for a policy group and includes the following information:

- Command name
- User who executed the command
- Date and time the command was executed
- Host where the command was executed

Use the following report parameters to define details in the report:

- Policy Group
- Command
- Host
- Log status
- Date

NOTE: You can use wildcards in the text string you enter in the **Command** box, such as * and ?.

NOTE: This report is available when you are logged on as the *supervisor* or as an Active Directory account in the **Manage Sudo Policy**, **Manage PM Policy**, **Audit Sudo Policy**, or **Audit PM Policy** roles. You must have an active policy group for Privilege Manager to run this report; you can only include hosts that are joined to a policy group.

Report	Description
Console Access and Permissions	Lists users who have access to the mangement console based on membership in a console role and the permissions assigned to that role. This report includes the following information:

- List of roles
- List of permissions assigned to each role
- List and number of members assigned to each role

NOTE: This report is available when you are logged on as the *supervisor* or an Active Directory account in the **Manage Console Access** role. However, when you access this report as *supervisor*, the mangement console requires that you authenticate to Active Directory.

Report	Description
Logon Policy for AD User	Identifies the hosts where Active Directory users have been granted log on permission. This report includes the following information for hosts joined to an Active Directory domain:

- Total number of hosts where the AD user has access
- List of hosts where the AD user has access

Report	Description
	Specify the Active Directory users to include in the report: • All AD users (default) • Select AD user **Browse** to search Active Directory to locate and select an Active Directory user. NOTE: The report might show both the Active Directory login name and local user names in the **Login Name** column for a selected AD user account because an Active Directory user account can have one or more local user accounts mapped to it. NOTE: Only hosts joined to an Active Directory domain with a Authentication Services 4.*x* agent are included in this report. NOTE: This report is available when you are logged on as an Active Directory account in the **Manage Hosts** role.
Logon Policy for Unix Host	Identifies the Active Directory users that have been explicitly granted log on permissions for one or more Unix computers. This report includes the following information for hosts joined to an Active Directory domain: • Host Name, DNS Name or IP Address of the host selected for the report • Users that have been granted permission to log on Specify the managed hosts to include in the report: • All profiled hosts (default) • Select host **Browse** to locate and select a managed host that is joined to Active Directory. NOTE: This report only includes hosts joined to an Active Directory domain with a Authentication Services 4.*x* agent. NOTE: This report is available when you are logged on as an Active Directory account in the **Manage Hosts** role.
Policy Changes	Provides details of changes made to a policy for a Privilege Manager policy group. This report includes the following information: • Name of the user that made changes to the policy • Version number for the changes • Time and date the changes were saved and actively used to enforce policy • Changes made to the policy based on version Select a policy group.

ONE IDENTITY™

Report	Description
	Select either to: • Show all changes to the policy • Show only changes for a specific pmpolicy file (not available for sudo-based policy) • Show changes to the policy for changes for one or more revisions NOTE: This report is available when you are logged on as the **supervisor** or as an Active Directory account in the **Manage Sudo Policy**, **Manage PM Policy**, **Audit Sudo Policy**, or **Audit PM Policy** roles. You must have an active policy group for Privilege Manager to run this report; you can only include hosts that are joined to a policy group.

Product Licenses Usage reports

Table 15: Product Licenses Usage reports

Report	Description
Product License Usage	Provides a summary of all licensing information. This report includes the following information for hosts managed by the console: • Product • Purchased licenses • Used licenses

One IDENTITY™

Setting preferences

You can set both *User* and console *System* preferences. *User* preferences are settings that only apply to the user that is currently logged on to the mangement console. Whereas, *System* preferences are global settings that apply to all users using the mangement console.

You access **User preferences** from the top-level **User** menu represented by the authenticated user's login name. Its menu also has options for sign in/sign out. You access **System settings** from the top-level **Settings** menu represented by the *gear* icon, . Its menu also has a link to the **Software updates** dialog where you can check for client software updates.

While you can change **User Preferences** using any log on account; to change console **System Settings** you must log onto the mangement console using the ***supervisor*** account or an Active Directory account with rights to change **System Settings**; that is, an account in the **Console Administration** role.

User preferences

These are the user preferences:

- General user preferences
- Host Credentials settings

General user preferences

Use the **General** settings to set the default domain to use as the default for all Active Directory tasks.

Setting the default domain

You can set the default domain to use as the default for Active Directory tasks; such as:

- Join Hosts to Active Directory
- Check for AD Readiness

To set the default domain

1. From the top-level **User** menu, navigate to **User preferences | General**.

2. Open the **Default Domain** drop-down menu and choose a domain.

Host Credentials settings

Use the **Host Credentials** settings to:

- Modify the saved host credentials
- Remove all saved host credentials

Modifying saved host credentials

You can modify the host credentials cached on the server. This is the information that is pre-populated into the **Log on to Host** dialog after you save the credentials for the host.

To change saved host credentials

1. From the top-level **User** menu, navigate to **User preferences | Host Credentials**.

    Hosts Credentials lists the hosts that have saved credentials.

2. To modify a particular host's credentials, select a host from the **Host Credentials** view and click **Edit credentials**.

    You can search for a particular host using the **Search for host** box.

3. On the **Saved Credentials** dialog, change the host connection settings and click **OK**.

NOTE: For more information, see Caching Unix host credentials on page 189.

Removing saved host credentials

You can remove saved host credentials from the persistent cache using the **Host Credentials** setting.

To remove saved host credentials

1. From the top-level **User** menu, navigate to **User preferences | Host Credentials**.

ONE IDENTITY™

2. To clear the credentials from one or more hosts, select the hosts and click **Clear credentials**.

   The mangement console clears the credentials for the selected hosts.

3. To clear all saved passwords for your hosts, click **Clear all credentials**.

System preferences

These are the system preferences:

- General system settings
- Console Roles and Permissions system settings
- Active Directory system settings
- Privilege Manager system settings
- Authentication Services system settings

General system settings

Use the general system settings to:

- Allow duplicate SSH host keys when adding hosts
- Set the session timeout period
- Automatically mark system users when profiling hosts the first time

Duplicate SSH Host Keys

To ensure uniqueness of hosts, by default, the mangement console prevents you from adding hosts with the same SSH host key. Since a host can have more than one resolvable DNS name and multiple IP addresses, there should only be one SSH host key returned for whichever DNS name or IP address you use to access the host. However, if you want to add hosts with the same SSH key to the mangement console, you can enable this setting. Enable (or disable) the **Duplicate SSH host keys** setting in **System settings**.

NOTE: If you enable **Duplicate SSH Host Keys**, you can profile multiple hosts that share the same public key. Once this is enabled there will be no way to validate if a host has been added more than once. You could potentially add a host multiple times under alternate IP addresses or DNS names. If this happens, duplicate users and groups would be visible, and reports will show redundant data. One Identity recommends that you NOT enable this feature to ensure that each host has a unique public key. However, it might be desirable to enable this feature if you want to add multiple hosts that are used for replication where each host shares the same public key.

To add hosts with the same SSH host key

1. Log onto the mangement console using the ***supervisor*** account or an Active Directory account with rights to change **System Settings**; that is, an account in the **Console Administration** role.

2. From the top-level **Settings** menu, navigate to the **General** settings.

3. Select the **Allow hosts with the same SSH host keys to be added to the console** option.

4. Click **OK** to save your selection and close **System Settings**.

Setting session timeout

By default, after 15 minutes of inactivity in the console, users are logged out. You can extend the session timeout to up to 4 hours.

To extend the session timeout period

1. From the top-level **Settings** menu, navigate to the **General** settings.

2. Under **Session Timeout**, select your desired timeout period and click **OK**.

Automatically marking host system users

You can enable the mangement console to mark local user accounts as "system users" when it profiles hosts.

To mark system users automatically during host profile

1. From the top-level **Settings** menu, navigate to the **General** settings.

2. Under **Host System Users**, select **Mark system users automatically when profiling**. (Set by default)

   NOTE: This setting is set by default. However, it only marks system users automatically during the initial profile.

3. Enter a UID number or range of numbers to mark.

   Use a colon (:) to signify a range of numbers; comma delimit multiple numbers or ranges. For example,

   ```
   0:499,501,555:600
   ```

   NOTE: Do not add extra spaces.

4. Enter specific account names you want to mark. For example,

   ```
   root,web*,*nobody,ma?k
   ```

   NOTE: Comma delimit multiple names; do not add extra spaces. You can use

ONE IDENTITY™

wildcards in the text string, such as * and ?.

System users are identified by the 👥 icon displayed in the user state column, indicated with the ⚠.

NOTE: You can provide both a UID range and specific user account names.

Console Information settings

Both users and remote hosts use the information on the **Console Information** settings to find and identify this mangement console on the network.

NOTE: The Control Center also uses the console information to find and identify this mangement console, as well as perform automatic profile and automatic QAS status tasks.

During the post-installation configuration steps, the console information was set on the **Identify Console** dialog of the setup wizard. You can modify these settings from **System settings | General | Console Information**.

Table 16: Console Information settings

Option	Description
Console host address	Enter the DNS name or IP address to access this mangement console. NOTE: This is a critical setting needed by the *Profile Automatically* and *Check QAS Agent Status Automatically* features; thus, it is important to use a name that other computers on the network can use to resolve to this host.
Console name	Enter the name of the computer where this mangement console was installed. The mangement console pre-populates this with the computer's DNS name, but you can modify this to identify the computer.
Contact	(Optional) Enter the user name of the contact person responsible for installing/maintaining this mangement console.
Description	(Optional) Enter a brief description to identify this mangement console on the network.

Publishing console to Active Directory

A Service Connection Point (SCP) enables a service to publish service-specific data in Active Directory which can then be used by network clients to locate, connect, and authenticate to an instance of the service. Management Console for Unix can create and register an SCP with Active Directory so that client applications (such as Control Center) can locate and browse to instances of the mangement console running on the network.

To publish an SCP with Active Directory, enable the setting in **Console Information** settings. When you enable this setting, Management Console for Unix creates an SCP as a child of the Active Directory computer object of the computer where Management Console

for Unix server is running. Once created, the SCP contains the keywords and service binding information that allows clients to browse to the initial screen of the mangement console. That is, a client application searches the Global Catalog (GC) for the SCP containing the Management Console for Unix keywords and then uses the service URL to browse to the mangement console. Please keep in mind, that the ServiceConnectionPoint object will appear in the GC based on the replication policy (usually every 5 minutes); therefore, the client application (such as, Control Center) may not find it immediately after the SCP is published to Active Directory.

NOTE: You can only register an SCP if the mangement console is installed on a computer that is joined to Active Directory.

To publish the mangement console to Active Directory

1. Log onto the mangement console using the **supervisor** account or an Active Directory account with rights to change **System Settings**; that is, an account in the **Console Administration** role.

2. From the top-level **Settings** menu, navigate to **System settings | General | Console Information**.

   The Management Console for Unix service uses the information displayed on this dialog to create and register the SCP with Active Directory.

3. Under **Publish console to Active Directory**, select the **Register a Service Connection Point with Active Directory** option to publish the mangement console to Active Directory.

NOTE: If the **Register a Service Connection Point with Active Directory** option is disabled, see Cannot create a service connection point on page 197.

Changing supervisor account password

You can change your *supervisor* account password in **System settings** when you are logged in as **supervisor**.

To change supervisor account password

1. Log onto the mangement console using the **supervisor** account.

2. From the top-level **Settings** menu, navigate to **System settings | General | Change Password**.

3. Enter your current **supervisor** account password and the new password.

4. Click **OK** to save your changes and close **System Settings**.

NOTE: If you have forgotten the current *supervisor* account see Reset the supervisor password on page 206 for more information on resetting your supervisor password.

Setting custom privilege elevation commands

You can specify up to three custom privilege elevation commands to use when performing tasks on hosts that require elevated privileges.

To set custom privilege elevation commands

1. From the top-level **Settings** menu, navigate to **System Settings | General | Custom Privilege Elevation**.

2. In the **Custom Elevation** box, enter the elevation command and any optional parameters required by the command. For example:

   ```
   /opt/quest/bin/pmrun
   ```

   > NOTE: Enter the full path to the command if the command is not in the system's path.

3. Optionally, select the **Use single quotes for command arguments** option if the command requires arguments in quotes.

   For example, the sudo command does not require arguments in quotes, like this:

   ```
   # sudo echo bob
   ```

   Whereas the su command does require arguments in quotes, like this:

   ```
   # su root -c "echo bob"
   ```

4. To specify another user instead of *root* when performing tasks on hosts that require elevated privileges, replace *root* with "%s" as in:

   ```
   # su %s -c "echo bob"
   ```

   Enter "%s" to specify a user name other than *root* to use elevated credentials. In the **Log On To Host** dialog, when you select the **Use elevated credentials** option, you can replace *root* with another account in the **User name** field.

5. Optionally, click **Test** to validate that the command works.

   On the **Test Privileged Elevation Command** dialog,

   a. Enter or select a host where the command exists.

   b. Enter user credentials and click **Test**.

      A message displays to explain whether the test was successful or not.

6. Click **OK** to save the changes.

When a test for a command completes successfully, it becomes available on the **Log On To Host** dialog. (Search for **Log On To Host** in the online help for details.)

Console Roles and Permissions system settings

What a user sees in the mangement console is based on the rules that pertain to the console role the user is assigned. A user can only access and perform tasks specified for his roles. The default **supervisor** account is a member of all roles, however, that account is blocked from performing Active Directory tasks because the **supervisor** does not have Active Directory credentials.

NOTE: While all console roles, except **supervisor**, have permission to view the **Active Directory** tab, to perform certain Active Directory tasks, such as Unix-enabling an Active Directory user or group, the AD user assigned to the role must have the appropriate rights in Active Directory.

To access and perform tasks within the mangement console, assign users to one or more of the following console roles:

NOTE: All roles run reports. See Reports on page 143 for more information about the reports that are available for each role.

Table 17: Console roles and permissions

Role	Description	Default Permissions	Available UI
Manage Hosts	Members can add, view, and manage hosts, as well as run reports.	• View hosts • Manage hosts	• **Hosts** tab • **All Local Users** tab • **Active Directory** tab • **Reporting** tab
Manage Sudo Policy	Members can view and edit the sudoers policy file, run reports, and access a read-only view of all hosts.	• View hosts • Edit Sudoers Policy	• **Hosts** tab (view hosts only) • **Policy | Sudo Policy Editor** view • **Policy | Event Logs** view • **Policy | Replay Log** view • **Active Directory** tab • **Reports** tab to access the **Access and Privileges** and **Policy**

Role	Description	Default Permissions	Available UI
			Changes reports
Audit Sudo Policy	Members can audit sudo policy through reports, replay keystroke logs, and access a read-only view of all hosts.	• View hosts (read-only) • View and replay keystroke logs	• **Hosts** tab (view hosts only) • **Policy | PM Policy Editor** view • **Policy | Event Logs** view • **Policy | Replay Log** view • **Active Directory** tab • **Reports** tab to access the **Access and Privileges** and **Policy Changes** reports

Console Administration	Members can modify console **System Settings** and access a read-only view of all hosts.	• View hosts (read-only)
		• Manage console System Settings
			• **Hosts** tab (view hosts only)
			• **Active Directory** tab
			• **Settings | System settings** view
			  • **General** settings
			  • **Console Information** settings
			  • **Privilege Manager** settings
			  • **Active Directory** settings
			  • **Licenses** settings

Manage Console Access	Members can add and remove members of console roles, run	• View hosts (read-only)	• **Hosts** tab (view hosts only) • **Active Directory**

One **IDENTITY**™

Role	Description	Default Permissions	Available UI
	reports, and access a read-only view of all hosts.	• Set console permissions (Roles and Permissions)	tab • **Reports** tab to access only the **Console Access and Permissions** report • **Settings | System settings** view • **Console Roles and Permissions** settings
Manage PM Policy	Members can view and edit the Privilege Manager policy, run reports, and access a read-only view of all hosts.	• View hosts • Edit PM Policy	• **Hosts** tab (view hosts only) • **Policy | Edit Policy** view • **Policy | Event Logs** view • **Active Directory** tab • **Reports** tab to access the **Access and Privileges** and **Policy Changes** reports
Audit PM Policy	Members can audit Privilege Manager policy through reports, replay keystroke logs, and access a read-only view of all hosts.	• View hosts (read-only) • View and replay keystroke logs	• **Hosts** tab (view hosts only) • **Policy | Event Logs** view • **Policy | Replay Log** view • **Active Directory** tab • **Reports** tab to access the **Access and Privileges** and **Policy Changes** reports

Role	Description	Default Permissions	Available UI
Reporting	Members can run and view all reports and access a read-only view of all hosts.	• View hosts (read-only) • View and produce any report	• **Hosts** tab (view hosts only) • **Active Directory** tab • **Reports** tab to access reports

NOTE: Management Console for Unix does not allow you to add domain-local Active Directory groups to roles; you can only add security-enabled global and universal groups.

Adding (or Removing) role members

NOTE: This task requires that you are logged in as the **_supervisor_** or an Active Directory account with rights to add or remove members of console roles; that is, an account in the **Manage Console Access** role.

To add additional Active Directory members or groups to a role

1. From the top-level **Settings** menu, navigate to **System settings | Console Roles and Permissions**.

2. Select a role and click **Members**

   NOTE: If you are logged in as **_supervisor_**, the mangement console requires that you authenticate to Active Directory in order to select Active Directory users or groups to add members to a role.

3. On the **Role Members** dialog, click **Add**.

4. On the **Select AD Object** dialog, use the search controls to find and select Active Directory users or groups.

5. Select one or more objects from the list and click **OK**.

   The mangement console adds the selected objects to the list.

6. Click **OK** to save your selections.

7. Click **OK** on the **Console Roles and Permissions** dialog to close **System Settings** and return to the mangement console.

Reviewing the Console Access and Privileges report

The **Console Access and Permissions** report lists users who have access to the mangement console based on membership in a role and the permissions assigned to the

role.

To create the Console Access & Privileges report

1. From the mangement console, navigate to **Reporting**.

2. From the **Reports** view, double-click the **Console Access and Permissions** report name.

   The report opens a new **Console Access and Permissions** tab on the **Reports** view.

3. Open the **Export** drop-down menu and select the format you want to use for the report: **PDF** or **CSV**.

   NOTE: If you are logged in as ***supervisor***, the mangement console requires that you authenticate to Active Directory in order to view the settings for **Active Directory**.

   It launches a new browser or application page and displays the report in the selected format.

   NOTE: When generating multiple reports simultaneously or generating a single report that contains a large amount of data, One Identity recommends that you increase the JVM memory. See JVM memory tuning suggestions on page 214 for details.

Active Directory system settings

Use the **Active Directory** settings to configure the console for Active Directory, specify which sites, domains, domain controllers, and global catalogs the mangement console may access, and to define the default domain you want the console to use when authenticating a user account.

NOTE: If you are logged in as ***supervisor***, the mangement console requires that you authenticate to Active Directory in order to view the settings for **Active Directory**.

Active Directory configuration

To configure the mangement console for Active Directory

1. From the top-level **Settings** menu, navigate to **System settings | Active Directory**.
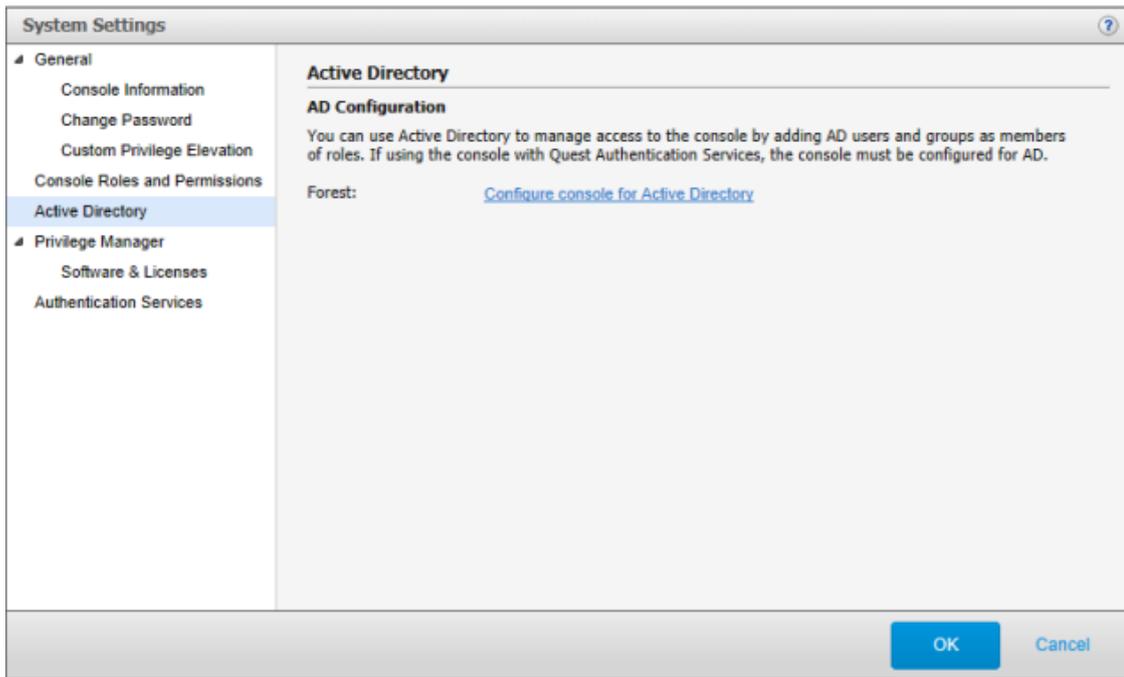
2. On the **AD Configuration** dialog, click the **Configure console for Active Directory** link next to **Forest**.

    > NOTE:
    >
    > If a domain name is displayed instead of the link, the mangement console is already configured for Active Directory. To limit how the console accesses Active Directory, refer to Configuring advanced settings on page 167 for information about limited the sites, domains, domain controllers, or global catalogs you want the console to contact.

3. On the **Configure console for Active Directory Logon** dialog,

    a. Enter a domain in the forest.

    b. Enter the Active Directory credentials.

        The wizard uses these credentials to configure the mangement console for use with Active Directory.

    c. Click **Connect to Active Directory**.

    d. When you see the message that indicates your console connected to Active Directory successfully, click **Next**.

4. On the **Set up console access by role** dialog, click **Add** to specify the Active Directory users and groups that you want to have access to the features available in Management Console for Unix.

    The **Select Users and Groups** dialog opens:

    a. Use the search controls to find and select Active Directory users or groups. Select one or more objects from the list and click **OK**.

The mangement console adds the selected object(s) to the list on the **Set up console access by role** dialog.

By default the mangement console assigns users to **All Roles**, which gives those accounts permissions to access and perform all tasks within the console. See Console Roles and Permissions system settings on page 161 for more information.

> NOTE: During the initial set up, you can only assign one role per user. Use **System Settings** to add additional roles to a user. See Adding (or Removing) role members on page 164 for details.

    b. Click in the **All Roles** cell to activate the drop-down menu from which you can choose a role for the user account.

    c. Click **Finish** to save your selections and return to **System Settings**.

5. Click **OK** to close **System Settings** and return to the mangement console.

The additional features are now unlocked; however, you must be logged on as an Active Directory user to perform **Active Directory** tasks.

6. Navigate to the **User** menu in the upper right-hand region of the screen and click **Sign out**. Then sign back on using an Active Directory account that has been granted access to the mangement console (that is, an account that was added to the list on the **Set up console access by role** dialog).

Configuring advanced settings

By default, the mangement console contacts Active Directory through any site, domain, domain controller, or global catalog that is available. To limit how the console contacts Active Directory, click **Advanced Settings** and specify which sites, domains, domain controllers, or global catalogs you want the console to contact.

To configure advanced Active Directory settings

1. Log into the mangement console with the ***supervisor*** account or an Active Directory account rights to change **System Settings**; that is, an account in the **Console Administration** role.

2. From the top-level **Settings** menu, navigate to **System settings | Active Directory** and click the **Advanced Settings** button.

> NOTE: If the **Advanced Settings** button is not enabled, you must first configure the console for Active Directory. See Active Directory configuration on page 165 for details.

> If the Active Directory configuration has become invalid (for example, the console is restricted to a domain that no longer exists), refer to Unable to configure Active Directory on page 194 for information about temporarily setting the domain and site settings until you can reset the configuration from the **Advanced Settings** dialog.

3. On the **Active Directory Credentials** dialog, enter credentials to log into Active

Directory and click **OK**.

The **Active Directory Forest Configuration** dialog opens which allows you to configure which sites, domains, domain controllers, or global catalogs you want the mangement console to contact for all Active Directory related tasks.

4. Choose either the **Sites** or the **Domains** option.

   The **Sites** option allows you to select and deselect only sites. The **Domains** option allows you to select or deselect individual domain controllers.

5. Expand the tree view and select which site, domain, domain controller, or global catalog node you want the console to contact for all Active Directory related tasks.

6. Click **Verify configuration**. (Note: You must test before you can save the change.).

7. Click **OK** to return to **System Settings**.

To remove a console access restriction in Advanced Settings

1. Expand the tree view and deselect site, domain, domain controller, or global catalog node.

2. Click **Verify configuration**. (Note: You must test before you can save the change.).

3. Click **OK** to save the change and return to **System Settings**.

Setting the default logon domain

The mangement console uses the default log-on domain to authenticate the user name you use when logging onto the console.

To set the default log-on domain

1. Log into the mangement console with the *supervisor* account or an Active Directory account with rights to change **System Settings**; that is, an account in the **Console Administration** role.

2. From the top-level **Settings** menu, navigate to **System settings | Active Directory** and click the **Advanced Settings** button.

3. On the **Active Directory Credentials** dialog, enter a user name and password to authenticate to Active Directory.

   The **Active Directory Forest Configuration** dialog displays.

4. Next to **Default logon Domain** (at the bottom of the dialog), choose the default domain to use when logging onto the console.

   This allows you to log onto the mangement console using a simple name instead of "user@domain".

5. Click **Verify configuration**. (Note: You must test before you can save the change.).

6. Click **OK** to return to **System Settings**.

Privilege Manager system settings

You can configure the mangement console to communicate with one or more Privilege Manager policy groups which allows you to centrally manage security policy, remotely configure the Privilege Manager hosts, and view keystroke logs generated by the policy. The **Privilege Manager** settings in **System Settings** allows you to activate previously configured service accounts on policy servers. This enables you to view and edit the policy, view keystroke logs, and run policy reports.

Use the **Privilege Manager** settings to configure the service account and activate the policy groups that you want to use for checking policy and keystroke logging.

Before you can use the Privilege Manager features, you must install and configure a Privilege Manager primary policy server. See Installing the Privilege Manager packages on page 109 for details.

Configuring a service account

Configuring a service account activates the policy group and allows the console to access both pmpolicy or sudoers policy files, view events and keystroke logs for a policy group.
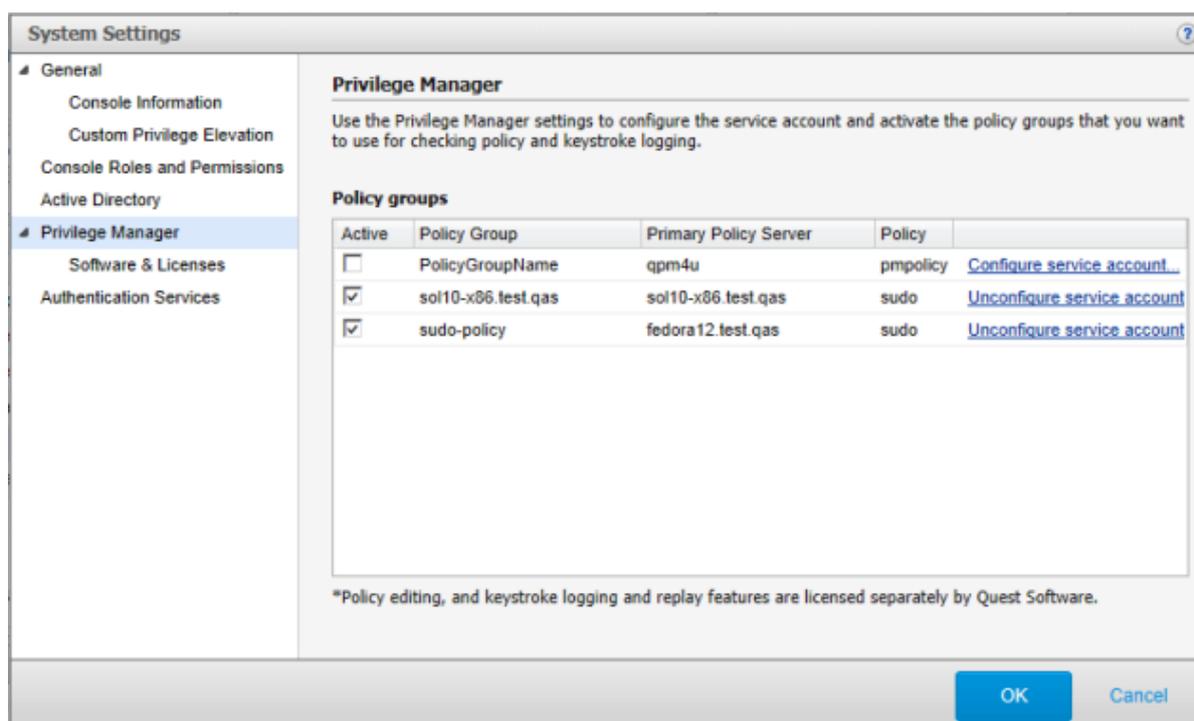
To configure service account

1. Log in as *supervisor* or an Active Directory account with rights to change **System Settings**; that is, an account in the **Console Administration** role.

2. From the top-level **Settings** menu, navigate to **System settings | Privilege**

Manager.

3. Click **Configure service account** next to the primary policy server listed.

   NOTE: If your policy group is not listed, make sure you have added and profiled the host where Privilege Manager software is installed as the primary policy server to the mangement console; then re-profile the host.

4. On the **Configure Service Account** dialog, enter credentials to log onto the primary policy server and click **OK**.

   NOTE: This task requires elevated credentials.

5. Verify that the **Active** box is checked and click **OK**.

When you configure the service account, the mangement console,

1. Creates "questusr", (the user service account), if it does not already exist, and a corresponding "questgrp" group on the host.

   NOTE: The *questusr* account is a user service account used by Management Console for Unix to manage Privilege Manager policy and search event logs. It is a non-privileged account (that is, it does not require root-level permissions) used by the console to gather information about existing policy servers and commit policy changes. *questgrp* is the primary group (gid) for *questusr*.

2. Adds *questusr* to the *pmpolicy* and *pmlog* Privilege Manager configuration groups, and as an implicit member of *questgrp*.

   NOTE: *questusr*, *pmpolicy*, and *pmclient* are all non-privileged service accounts (that is, they do not require root-level permissions). The *pmpolicy* and *pmclient* users are used to sync the security policy on policy servers and on Sudo Plugin hosts (offline policy cache), respectively.

   The *pmlog* and *pmpolicy* groups are used to control access to log files and the security policy, respectively.

3. Adds the policy group SSH key to *questusr*'s authorized_keys, /var/opt/quest/home/questusr/.ssh/authorized_keys.

4. Verifies the user service account can login to the host.

   NOTE: If you receive an error message saying you could not log in with the user service account, refer to Service account login fails on page 208 to troubleshooting this issue.

If *questusr* is inadvertently deleted from the console,

1. Re-profile the host.

2. Unconfigure the service account. See Unconfiguring a service account on page 171 for details.

3. Reconfigure the service account.

Unconfiguring a service account

Unconfiguring a service account deactivates the policy group in the mangement console and disables console access to the policy file and keystroke logs on the primary policy server.

To unconfigure service account

1. Log in as **supervisor** or an Active Directory account with rights to change **System Settings**; that is, an account in the **Console Administration** role.

2. From the top-level **Settings** menu, navigate to **System settings | Privilege Manager**.

3. Click **Unconfigure service account** next to the primary policy server listed.

4. On the **Unconfigure Service Account** dialog, enter credentials to log onto the primary policy server and click **OK**.

   NOTE: This task requires elevated credentials.

5. Verify that the **Active** box is not checked.

NOTE: When you unconfigure a service account, the mangement console,

1. leaves the "questusr" and the corresponding "questgrp" account on the host.

2. removes *questusr* from the *pmpolicy* and *pmlog* groups.

3. leaves *questusr* as an implicit member of *questgrp*.

4. removes the policy group SSH key from *questusr*'s authorized_keys, `/var/opt/quest/home/questusr/.ssh/authorized_keys`.

Activating policy groups

To centrally manage a policy, view events, or reply keystroke logs for a policy group, you must activate it.

NOTE: You can only activate an inactive policy group if it has been previously configured. See Configuring a service account on page 169 for details.

To activate policy groups

1. Log in as **supervisor** or an Active Directory account with rights to change **System Settings**; that is, as an Active Directory account in the **Console Administration** role.

2. From the top-level **Settings** menu, navigate to **System settings | Privilege Manager**.

3. Select the **Active** box next to the policy groups you wish to activate and click **OK** to save the change and return to the mangement console.

   NOTE: If your policy group is not listed, make sure you have added and profiled the host where Privilege Manager software is installed as the primary policy server to

the mangement console; then re-profile the host.

Deactivating policy groups

You cannot remove policy groups directly from **Privilege Manager** system settings.
However, if you decide you no longer want to manage the policy file, view events or replay
keystroke logs for a particular policy group, you can deactivate it. Deactivating the policy
group does not unconfigure the service account; it simply disables console access to the
policy and keystroke logs on the primary policy server. See Unconfiguring a service
account on page 171 for details about unconfiguring the Service Account.

To deactivate policy groups

1. Log in as *supervisor* or an Active Directory account with rights to change **System
   Settings**; that is, as an Active Directory account in the **Console Administration**
   role.

2. From the top-level **Settings** menu, navigate to **System settings | Privilege
   Manager**.

3. Deselect the **Active** box to deactivate the policy group and click **OK** to save the
   change and return to the mangement console.

Software & Licenses settings

Use the **Software & Licenses** settings to:

- Set the Privilege Manager software location on the server.
- Check for Privilege Manager licenses.

NOTE: Centralized policy management and keystroke logging are licensed separately.

Setting the Privilege Manager software path

When you install from the product ISO, the setup wizard copies available software
packages to a default location on the local computer.

The default directories are:

- On Windows platforms: `%SystemDrive%:\Program Files\Quest Software\Management
  Console for Unix\software\qpm\default`
- On Unix and Linux platforms: `/opt/quest/mcu/software/qpm/default`

NOTE: If you install Management Console for Unix from the Privilege Manager for Unix
ISO, the "default" directory is replaced with the product version number.

If you plan to install Privilege Manager software onto your hosts from the console, you
must ensure the path to the packages is correctly set in **System Settings**.

To ensure the path to the Privilege Manager software packages is correctly set

1. Make note of where your Privilege Manager software packages are located.
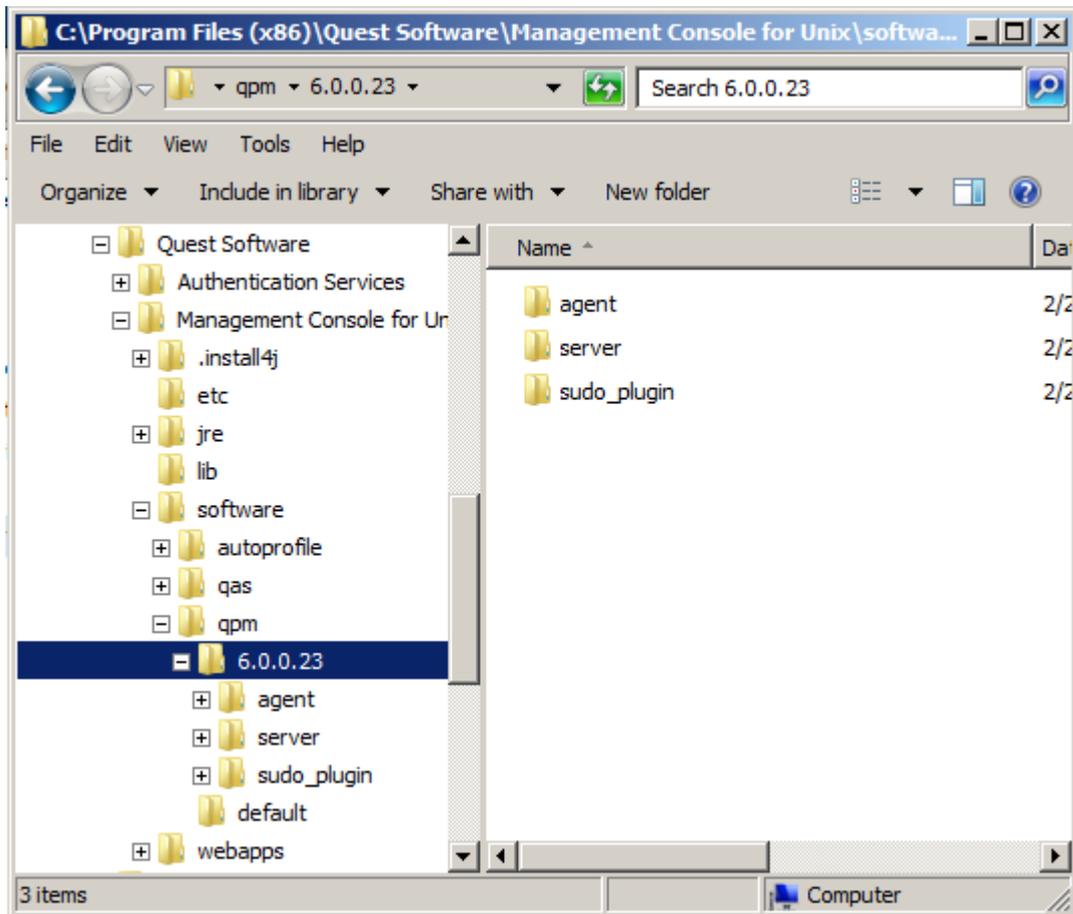
2. Log into the mangement console with the ***supervisor*** account or an Active Directory account with rights to change **System Settings**; that is, an account in the **Console Administration** role. See Console Roles and Permissions system settings on page 161 for details.

3. From the top-level **Settings** menu, navigate to **System settings | Privilege Manager | Software & Licenses**.
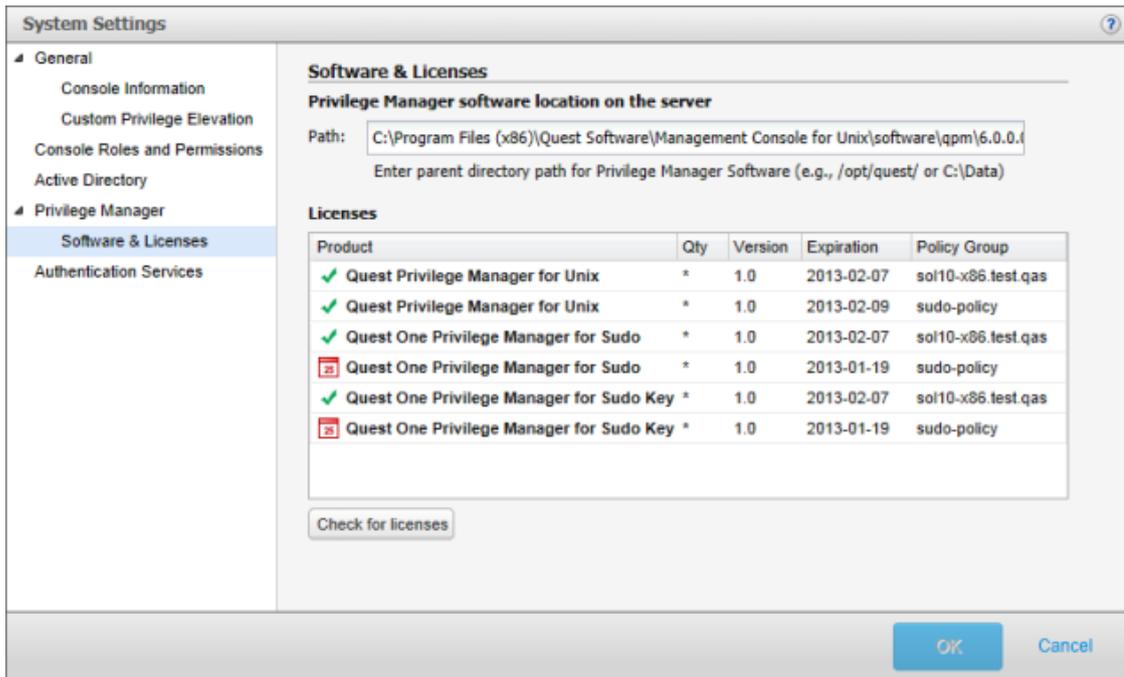
4. In the **Path** box, enter the path to where the Privilege Manager software packages are located on the server and click **OK**.

NOTES:

- The path to the software packages must point to the folder containing the `agent`, `server`, and `sudo_plugin` directories. It is typically the version number of Privilege Manager for Unix.

- When running Management Console for Unix on Windows, the location of the Privilege Manager software packages must be accessible to the mangement console service which runs as 'NT AUTHORITY\NetworkService.

Checking for Privilege Manager licenses

You cannot add Privilege Manager licenses to the primary server by means of the mangement console. You must install the One Identity license files using the `pmlicense` command. See the *Privilege Manager for Unix Administration Guide* for details.

NOTE: You must have a Privilege Manager Policy Server configured in order to update licensing.

To refresh Privilege Manager license information in the console

1. Log onto the mangement console using the *supervisor* account or an Active Directory account with rights to change **System Settings**; that is, an account in the **Console Administration** role.

2. From the top-level **Settings** menu, navigate to **System settings | Privilege Manager | Software and Licenses**.

3. Click **Check for licenses**.

4. Click **OK** to save the **System Settings** and return to the mangement console.

NOTE: The mangement console automatically updates the license information each time you login.

Privilege Manager license alerts

While the mangement console always allows you to add Unix hosts and manage local users and groups without a license, One Identity provides a free 30-day unlimited-use trial license that allows you to manage any number of hosts with Privilege Manager for Unix and Privilege Manager for Sudo. After the evaluation period expires, you will receive a "License" alert if you continue to use the Privilege Manager products after the expiration date, and a "Usage" alert if you exceed the number of hosts allowed. It may take up to 60 minutes for the primary policy server to update the license information. The console will report the correct information next time you log into the console, update licenses from **System Settings**, run the Product License Usage report, or when you configure a service account for a policy group.

License Alerts

When the policy server license expires, you will receive an alert on the console.

Usage Alerts

When you exceed the number of hosts allows by your current product license, you will receive an alert on the console.

After the free 30-day unlimited-use trial license expires:

- Privilege Manager for Unix does not allow you to manage any Privilege Manager Agents without an alert.
- Privilege Manager for Sudo allows you to manage up to 10 Sudo Plugin hosts without an alert.

Authentication Services system settings

Use the **Authentication Services System Settings** to change the Authentication Services path to the Authentication Services software packages, validate the Authentication Services licenses, and configure the mangement console to use the Windows 2003 R2 schema.
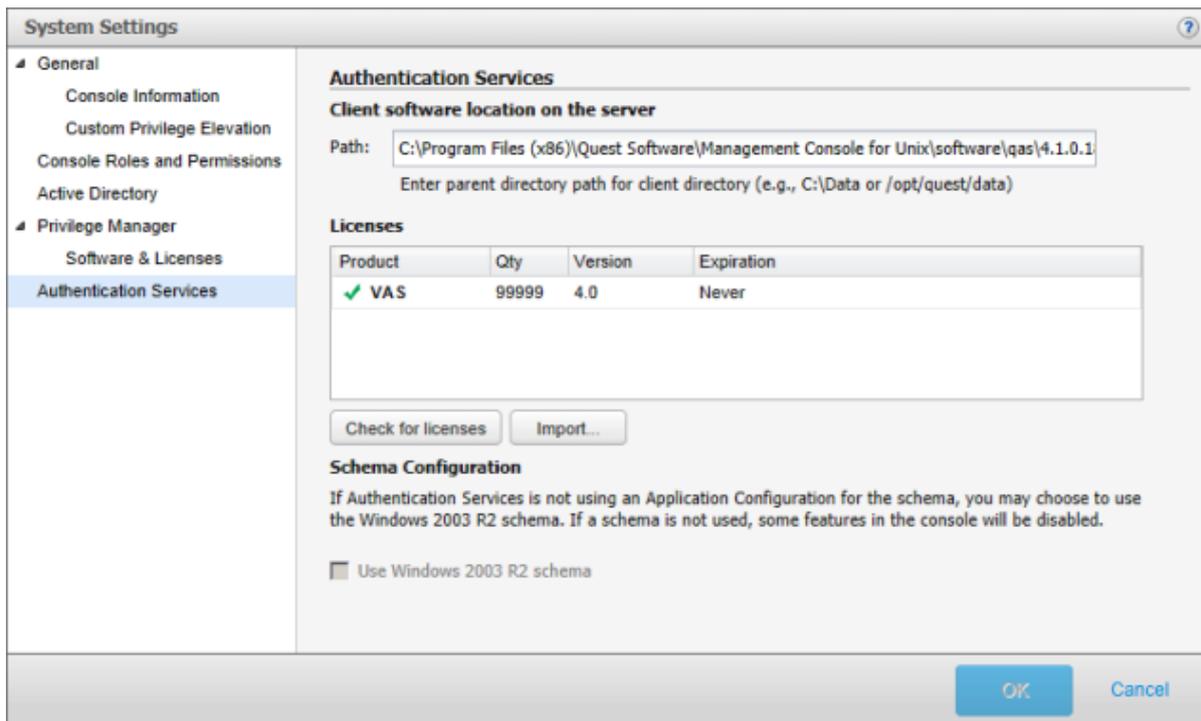
The **Authentication Services** settings lists the Authentication Services product licenses found during the installation/configuration process.

Setting the Authentication Services software path

When you install from the product ISO, the setup wizard copies available software packages to a default location on the local computer.

The default directories are:

- On Windows platforms: `%SystemDrive%:\Program Files\Quest Software\Management Console for Unix\software\qas\default`

- On Unix and Linux platforms: `/opt/quest/mcu/software/qpm/default`

NOTE: If you install Management Console for Unix from the Authentication Services ISO, the "default" directory is replaced with the Authentication Services version number.

If you plan to install Authentication Services software onto your hosts from the console, you must ensure the path to the packages is correctly set in **System Settings**.

To ensure the path to the Authentication Services software packages is correctly set

1. Make note of where your Authentication Services software packages are located.
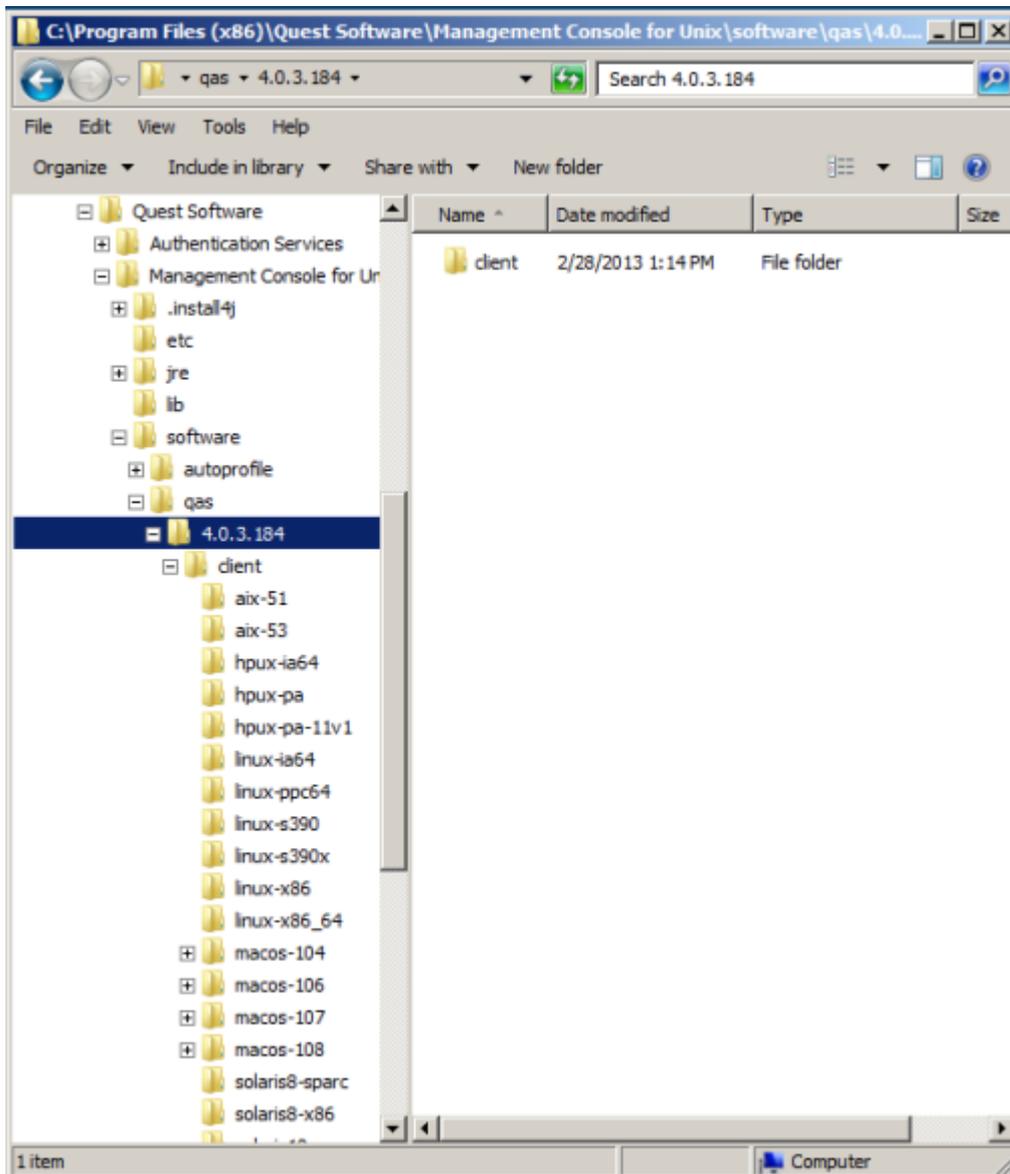
2. Log onto the mangement console using the ***supervisor*** account or an Active Directory account with rights to change **System Settings**; that is, an account in the **Console Administration** role. See Console Roles and Permissions system settings on page 161 for details.

3. From the top-level **Settings** menu, navigate to **System settings | Authentication Services**.
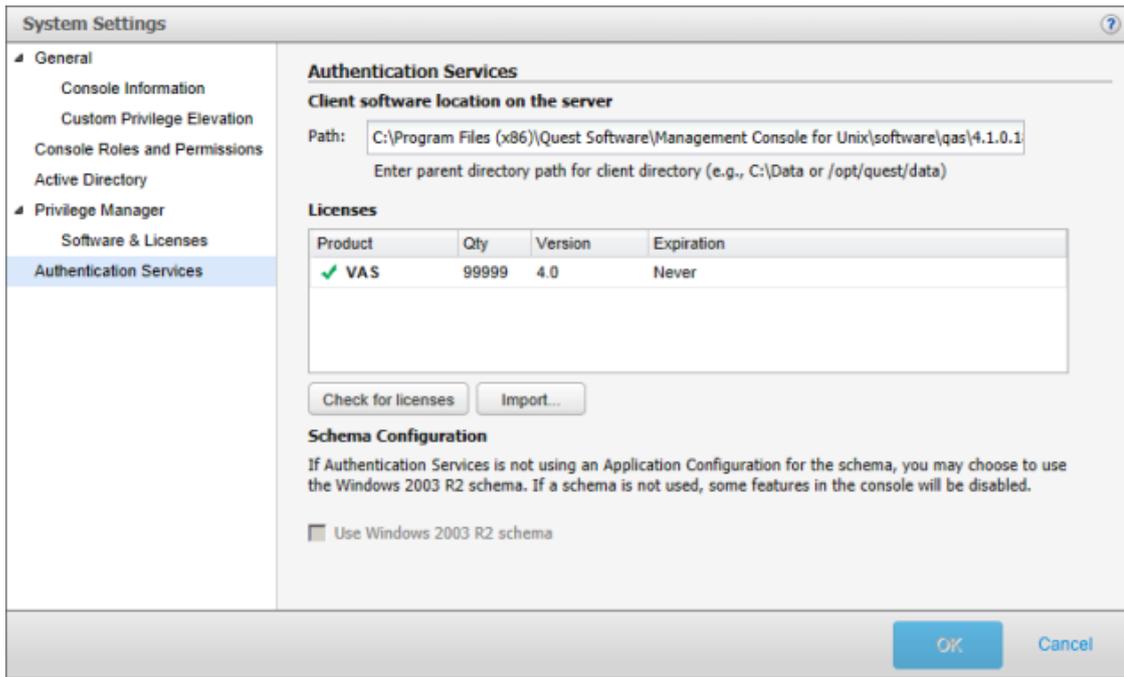
4. In the **Path** box, enter the path where the Authentication Services software packages are located on the server.

5. Click **OK** to save your selection and close **System Settings**.

Authentication Services license alerts

While the mangement console always allows you to add Unix hosts and manage local users and groups without a license, One Identity provides a free 30-day unlimited-use trial license that allows you to manage any number of hosts with Authentication Services 4.*x*.

License Alerts

After your license expires you will receive a "license" alert if you continue to use the product after the expiration date. The alert is triggered when you log into the console or update licenses from **System Settings**.

Usage Alerts

You will receive a "usage" alert if you exceed the number of hosts allowed by your current product license.

Checking for Authentication Services licenses

To refresh Authentication Services license information in the console

1. Log onto the mangement console using the **supervisor** account or an Active Directory account with rights to change **System Settings**; that is, an account in the **Console Administration** role.

2. From the top-level **Settings** menu, navigate to **System settings | Authentication Services**.

3. Click **Check for licenses**.

    NOTE: If the mangement console is not configured for Active Directory that option is disabled.

4. Click **OK** to save the **System Settings** and return to the mangement console.

Importing Authentication Services licenses

NOTE: The Import Authentication Services Licenses feature does not upload the license to the Authentication Services license application container in Active Directory; it only imports it to the console server for use by Management Console for Unix.

To import a Authentication Services license

1. Log onto the mangement console using the **supervisor** account or an Active Directory account with rights to change **System Settings**; that is, an account in the **Console Administration** role.

2. From the top-level **Settings** menu, navigate to **System settings | Authentication Services**.

3. Click **Import**.

4. Browse for the license file and click **OK**.

Configuring Windows 2003 R2 schema

If you are running Authentication Services without a Authentication Services application configuration in your forest and your domain supports Windows 2003 R2, you can enable Management Console for Unix to use the Windows 2003 R2 schema. However, please note, some functionality provided by the Authentication Services application configuration will be unavailable.

To configure Windows 2003 R2 schema

1. From the top-level **Settings** menu, navigate to **System settings | Authentication Services**.

2. Select the **Use Windows 2003 R2 schema** option.

ONE IDENTITY™

Security

Management Console for Unix provides different levels of security to protect sensitive information stored on the server and in the Unix systems that you wish to manage. Management Console for Unix protection focuses on the following areas:

- Management Console for Unix server and console
- Active Directory
- Managed Unix hosts
- The database

This section outlines the security features used by Management Console for Unix for each of these areas of protection.

Management Console for Unix server and console

Access to the Management Console for Unix server is controlled by the **supervisor** account when using the core version; or with Active Directory credentials when the mangement console is configured for Active Directory. When you enable Active Directory log on, you can configure access to the mangement console to allow individual users or members of Active Directory groups to access the mangement console. See Console Roles and Permissions system settings on page 161 for details on how to enable access for users and groups.

NOTE: Since Active Directory supports nested groups, a user may be granted access even if they are not a direct member of the nominated group, but are a member of one or more child groups. Care should be taken when using nested groups to ensure that access is not accidentally granted to the wrong users.

When authenticating with Active Directory credentials, you may

- Use Windows Integrated Authentication for single sign-on. See Authenticating Active Directory users using Windows Integrated Authentication on page 181.

  -OR-

- Log on with your Active Directory credentials at the log on screen. See Configure an IE web browser for SSO on page 212.

Authenticating the supervisor user

When a user logs on as '**supervisor**', the password is hashed on the client with a known salt and compared with the stored value in the Management Console for Unix database. The plain text password is never stored on the server. The password encryption is irreversible. As a result, if the **supervisor** password is lost it cannot be recovered, but may be reset by a user with logon access to the machine where the Management Console for Unix server is running. See Reset the supervisor password on page 206 for details.

Authenticating Active Directory users using Windows Integrated Authentication

Windows Integrated Authentication (WIA) allows a user to securely reuse their desktop credentials to log onto the mangement console when using a browser that supports WIA. Using WIA requires that the console server is installed and running on a Windows machine that is joined to the forest which you have chosen to manage, or is installed and running on a Unix machine that is running Authentication Services and is joined to the forest which you have chosen to manage. The client browser must also be joined to the same forest.

Authenticating Active Directory users using a username and password

When authenticating Active Directory users using a username and password, the credentials are used to obtain a Kerberos Ticket Granting Ticket (TGT) from Active Directory. If the Management Console for Unix server is running on a machine that is joined to a domain in a managed Active Directory forest (either on Windows or using Authentication Services on Unix or Linux), a Kerberos service ticket is also obtained for the host account. This second step is necessary to ensure that the TGT has not been falsified and to map any Domain Local Groups to the server's domain.

If the server has not been joined, or is joined to a different forest than the one being managed, an attacker could subvert the logon security by spoofing fake responses from Active Directory (for example, by hijacking DNS to point to a rogue Active Directory service). This is because the security guarantees of the Kerberos protocol require proof of a shared key between Active Directory and the server, before it can be proven that a given TGT is valid; and this proof requires obtaining a service ticket encrypted in the server's key.

NOTE: While you can run the Management Console for Unix server on a computer that is

not joined to the forest, **One Identity recommends that you run the Management Console for Unix server on a machine joined to the Active Directory forest you are managing to ensure that Active Directory users can be securely authenticated**

Installing a production certificate

SSL/TLS encryption of HTTP traffic between the server and web browser, and integrity checking of data received from the Management Console for Unix server is required to ensure that:

- The web browser application is using code and data coming from a trusted source
- Information about the Unix hosts managed by Management Console for Unix is not exposed in clear text on a network
- Authentication information, such as Active Directory passwords and Unix logon and root passwords, are kept secure

For this reason, Management Console for Unix is configured to require all connections to the browser be secured with the SSL/TLS protocol. See Disabling SSL/TLS encryption on page 185.

When installed, Management Console for Unix will initially be configured with a newly generated self-signed certificate. Because the authenticity of this certificate cannot be verified, your browser will usually display a warning message whenever you launch the mangement console. To rectify this situation, you can install a custom key pair for SSL/TLS.

Generating a custom SSL/TLS certificate and key pair for Management Console for Unix

You can obtain a trusted certificate from a third-party Certificate Authority. Each authority has its own instructions, but all require you to generate a Certificate Signing Request (CSR). See Exporting Data using the -certreq command for details about generating a CSR using the PKCS#10 format.

Optionally you can use a tool (such as, keytool or OpenSSL) to manually generate the public/private key pair and the certificate you need. You can also obtain a certificate and key pair from your Enterprise Certificate Authority.

NOTE: See Generating Keys and Certificates with OpenSSL for details about using OpenSSL to generate a certificate.

To install a custom SSL/TLS certificate and key pair using keytool

NOTE: See keytool - Key and Certificate Management Tool for more information about using keytool.

ONE IDENTITY™

1. Generate a private key in the keystore file using the `keytool` command:

```
keytool -genkeypair -storetype JKS -alias <aliasName> -keyalg RSA
-keysize 2048 -validity <numberOfDaysForCertificateToBeValid>
-keystore <keystoreName>
```

NOTE: See step 3 below for the final `keystoreName` value.

   a. Enter the keystore password and provide the other specifications it asks for (or click enter to accept the default). When it asks, "what is your first and last name?" enter the Management Console for Unix server's resolvable host name, such as

```
computer.test.com
```

   NOTE: Optionally, you can include this option in the above keytool command:

```
-dname "CN=<hostName>"
```

   where < hostName> is the Management Console for Unix server's resolvable host name.

   If the host name does not match the Management Console for Unix server's resolvable host name, your browser might indicate a security problem with the certificate that states the presented certificate was issued for a different web site's address.

   b. Verify the newly created keystore file:

```
keytool -list -v -keystore <keystoreName>
```

   Enter the keystore password when prompted.

   c. Export the certificate from the keystore:

```
keytool -export -alias <aliasName> -keystore <keystoreName> -rfc -file
<certificateName>.cer
```

   Enter the keystore password when prompted.

2. Stop the Management Console for Unix service.

   See Start/stop/restart Management Console for Unix service on page 215 for details.

3. Jetty and the Management Console for Unix expect the keystore file to be in a standard location:

   - On Windows platforms: `%SystemDrive%:\ProgramData\Quest Software\Management Console for Unix\jetty-base\etc\keystore`

   - One Unix/Linux platforms: `/var/opt/quest/mcu/jetty-base/etc/keystore`

If the keystore file from Step 1 is not already in this location, copy or move it to this location and ensure it has read permissions that will allow the Management Console for Unix service to read it.

4. Open the `custom.cfg` file for editing.

   See Setting custom configuration settings on page 208 for general information about customizing configuration settings for the mangement console.

5. Modify the following Jetty Settings:

```
-Djetty.sslContext.keyStorePassword=<password>
-Djetty.sslContext.keyManagerPassword=<password>
-Djetty.sslContext.trustStorePassword=<password>
```

where <password> is your plain text password or, if obfuscated (as explained below), is something similar to:

```
OBF:1tvp1saj1y7z1sar1tvd
```

NOTE: Optionally you can obfuscate your SSL keystore password so it is not stored in plain text by running the following command from your installation directory:

- On Windows platforms:

  `%SystemDrive%:\Program Files\Quest Software\Management Console for Unix\gen_secure_password.exe [<username>] <password>`

- On Unix and Linux platforms:

  `/opt/quest/mcu/gen_secure_password [<username>] <password>`

The output of gen_secure_password.exe lists

- your password in plain text

- an "MD5:" checksum

- an encrypted version of the password using UnixCrypt (if a user name was supplied.)

- the obfuscated password pre-pended with "OBF:"

Jetty only supports obfuscation (OBF) of SSL keystore passwords; the others can be ignored.

6. Save the `custom.cfg` file.

7. Start the Management Console for Unix service.

For more information, see the Jetty documentation at: Configuring SSL/TLS.

Importing certificate to trusted domains on Windows

To import certificates to trusted domains on Windows platforms

1. Copy the certificate to the Windows computer on which the mangement console is running.

2. Double-click the certificate to open the certificate details.

3. On the **General** tab, click the **Install Certificate** and click **Next**.

   The certificate import wizard starts.

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

5. Select **Trusted Root Certification Authorities** and click **OK**.

6. Click **Next**.

7. Click **Finish**.

8. Click **OK** when a message says the import was successful.

NOTE: You can also import certificates into a trusted domain by means of your browser.

Importing certificate to trusted domains on Unix or Linux

To import certificates to trusted domains on Unix or Linux platforms

1. As `root`, run the following commands:

```
cp server.crt /etc/ssl/certs
cp server.key /etc/ssl/private
```

Disabling SSL/TLS encryption

SSL is enabled by default. A self-signed certificate is installed but you should replace it with a valid certificate for your organization. While not recommended, it is possible to disable SSL/TLS encryption entirely.

To disable SSL/TLS encryption

1. Add the following line to the `custom.cfg` file:

```
-Dssl.enabled=false
```

One **IDENTITY**™

NOTE: All HTTPS traffic will be redirected to the HTTP port.

2. Update any browser bookmarks to specify the HTTP port number.

Customizing HTTP and SSL/TLS ports

To customize HTTP and SSL/TLS ports

1. Add the following lines to the `custom.cfg` file:

   ```
   -Dmcu.port.https=<port>
   -Dmcu.port.http=<port>
   ```

   where <port> is any port number not already in use on the machine hosting the server and *-Dmcu.port.https* is for SSL ports and *-Dmcu.port.http* is for non-SSL port.

   NOTE: The Command Line utilities and Web Services do not work unless you connect with the non-secure (http) port which allows the utility to discover the secure port.

   For more information about the Command Line utilities and Web Services, refer to these links:

   - Command line utilities on page 222
   - Web services on page 233

   See Setting custom configuration settings on page 208 for general information about customizing configuration settings for the mangement console.

Changing allowed ciphers

The cipher suites used by Jetty SSL are provided by the JVM. See Java Cryptography Architecture Oracle Providers Documentation.

The ciphers are used in preference order. If a vulnerability is discovered in a cipher (or if it is considered too weak to use), it is possible to include or exclude it in the Jetty configuration without the need to update the JVM.

For more information, see Disabling/Enabling Specific Cipher Suites. The `jetty.server.dumpAfterStart` property, described at the end of that topic is a useful aid for diagnosing Jetty configuration in general and SSL/TLS configuration in particular.

Active Directory

NOTE: When you are logged on as an Active Directory user, you can access information

about Active Directory users, groups and computers. See Active Directory configuration on page 165 for details.

This information is protected by using your credentials to securely connect to Active Directory using the GSS/SASL security layer for the LDAP protocol. Only the information that is visible to the Active Directory account to which you are logged on is available. While some of this information may be cached on the server, it is only available to the user that originally requested it, ensuring that the access control rules for Active Directory objects are honored by the Management Console for Unix server.

The mangement console may request Active Directory credentials when you perform tasks, such as the **Check for AD Readiness** or when you configure the Active Directory settings for a host. In this case, the credentials are not stored on the server, but are only used for the selected task.

Managed Unix hosts

Secure access to the managed Unix hosts is performed using the SSH protocol. Management Console for Unix uses SSH internally to profile hosts, manage users and groups, and run **Readiness Check Results** reports.

While the SSH protocol encrypts traffic and can use passwords to authenticate users, it uses public key cryptography to authenticate the server. If the server is not correctly authenticated, it is possible for an attacker to act as a 'man-in-the-middle' and obtain the user's logon and root passwords for a host. For this reason, it is important to understand how the options to manage SSH host keys affect the security of your Management Console for Unix installation.

Managing SSH host keys

Management Console for Unix uses SSH as the network protocol to provide secure remote access and administration of Unix hosts. It maintains a list of valid SSH host keys used to authenticate the connections.

The mangement console allows you to directly import these keys, using one of the following methods:

- By using the **Import SSH Host Keys** button to upload a new public SSH key for a selected host.

  When you use this command you are prompted to accept the new fingerprint for the selected host.

- By supplying an OpenSSH `known_hosts` file when using the **Import** option on the **Add Hosts** dialog.

  The `known_hostfile` contains the host addresses and public key data for known server hosts.

NOTE: See Known_hosts file format on page 188 for more information about the

supported `known_hosts` file format.

Alternatively, when profiling a host, new SSH keys are automatically accepted for the selected host by default. However, you can clear the **Automatically accept SSH keys** option on the **Profile Hosts** dialog if you want to be prompted to validate the host's SSH key if a key is not already cached for the selected host. If you clear this option, you must accept a host's fingerprint in order to proceed with the profiling process.

NOTE: While the **Automatically accept SSH keys** option is enabled by default, clearing this option disables it for subsequent profiles for this user. Regardless of whether the **Automatically accept SSH keys** option is selected or not, when a modified key is encountered, the profile task will prompt you to accept the new changed keys.

You can view the SSH fingerprint and algorithm used to access a host on the **Details** tab of a host's properties.

NOTE: While the Management Console for Unix server automatically accepts SSH host keys by default, to avoid potential "man-in-the-middle" attacks, One Identity recommends that you either disable this option so that you can manually review and accept the key fingerprints, or directly import the keys by using one of the methods described above. This ensures that your SSH connection is secured to a trusted host before supplying your log on or root credentials.

Known_hosts file format

When importing a *known_hosts* file, the mangement console expects the file to be in a particular file format. The rules for a *known_hosts* file are:

- It must contain lines of text consisting of a host's IP address, SSH algorithm, and SSH host key; each field separated by a space. The format is: `address algorithm publicKey`
- It must only contain one host entry per line.
- It does not support Hashed host names.
- It does not support multiple host names per entry.

The default location for a *known_hosts* file is: `${user.home}/.ssh/known_hosts`

Handling changes to SSH host keys

If an SSH host key is different than what is expected, the mangement console might indicate that the host is experiencing a "man-in-the-middle" attack. More commonly however, it simply indicates that the SSH host key has changed. When profiling, if the mangement console finds a SSH host key that is different than the one that is already cached on the server, it prompts you to accept the changed key.

For other actions, such as adding or deleting a user, a changed host key always results in an error. If you encounter an error, you must update the new SSH key before you can

ONE IDENTITY™

complete the action. See Managing SSH host keys on page 187 for information about updating the host's SSH Key cached in the mangement console database.

> NOTE: Management Console for Unix caches SSH connections to improve performance when multiple actions need to be performed against a host. Because of this, you might see unexpected behavior. For example, if you profile a host and accept its public key, the mangement console stores the host's public key and caches the SSH connection for a short period of time. If you perform another host action, such as profiling, it uses the cached connection if it is available. You are not prompted to accept a new key while re-using the previously verified and trusted SSH connections obtained from the cache. Once the connection is flushed from the cache, any subsequent host action will identify a new public key and the console will prompt you to accept the new SSH host key.

Detecting multiple hosts with the same key

By default, Management Console for Unix prevents you from adding hosts with the same SSH host key to the mangement console. This is to ensure uniqueness of hosts since a host can have more than one resolvable DNS name and multiple IP addresses. There should only be one SSH host key returned for whichever DNS name or IP address you use to access the host. However, if you want to enable the mangement console to add hosts that share the same SSH key, enable the **Duplicate SSH Host Keys** setting in **System Settings**. See Duplicate SSH Host Keys on page 156 for details.

> NOTE: When you enable the **Duplicate SSH Host Keys** option, it is possible to add the same host more than once, each with a unique name. In this case the reported data will be duplicated for that host.

Caching Unix host credentials

Management Console for Unix caches both standard and elevated credentials:

- **Session caching**: User names and passwords are cached for the duration of the browser session (that is, until the session expires upon log out or you close your browser page). The mangement console uses the cached credentials any time during the current session. That is, if persistent credentials are not already cached, the user name and password fields will be blank the first time it needs credentials to complete a task on the host during a browser session. Once entered, it caches these fields and reuses them during the current session; therefore, these fields are pre-populated for subsequent tasks with the previously entered credentials.

- **Persistent caching**: When you select the option to save your credentials on the server, the mangement console encrypts the user name and password and stores the encryption key on the Management Console for Unix server. When persistent credentials are available, the mangement console uses them any time you access the service. That is, saved user names and passwords persist across browser sessions, and when needed, it pre-populates these fields the first and subsequent times it needs them to complete a task on a host.

You can remove the persistent credentials from the cache. See Removing saved host credentials on page 155. Once removed, the mangement console uses the session-cached credentials.

> NOTE: The option to create persistent credentials is available through several actions such as **Profile Host** where you can select the **Save my credentials on the server** option. If you are profiling multiple hosts and select the **Enter different credentials for each selected host** option, you can select the **Save** option for individual hosts or click the **Save all credentials** button to save credentials for all hosts.
>
> See Modifying saved host credentials on page 155 for more information about managing Unix host credentials.

Security of credential caching

When using persistent caching, the mangement console encrypts host credentials, as follows:

1. It generates a salt or retrieves it from the Java KeyStore, a storage facility for cryptographic keys and certificates, if it has previously been stored in the keystore.

2. It uses the salt to generate a unique 128-bit encryption key for the authenticated user. The key generation algorithm is the PBKDF2 algorithm using HMAC with SHA1. This algorithm is designed to prevent brute force attacks on the password by ensuring that the same passwords will result in different keys and by increasing the work factor by iterating many times over the key generation function.

3. It uses the generated key to encrypt the credentials (including user name, password, and any elevation credentials) using the AES algorithm in CBC mode. It then uses Message Authentication Code (MAC) using the HMAC with SHA-256 algorithm to verify the integrity of the saved data.

Database security

The Management Console for Unix server communicates with a database on port 9001 over the loopback interface. The password used is randomly generated at install time. One Identity recommends that you configure a local firewall to exclude remote access to this port. For information on how to change the default port on which the database runs, see Database port number is already in use on page 198.

Summary of security recommendations

One Identity recommends that you implement the following to secure the data used by Management Console for Unix:

- When authenticating Active Directory users for access to Management Console for Unix make sure that the server is installed on a machine that is joined to the Active Directory forest you wish to manage.

- Install an SSL/TLS key pair and certificate that is signed by a Certification Authority that will be trusted by all users' browsers.

- Directly import SSH host keys using a *known_hosts* file, or the **Import SSH Host Key** toolbar command; or manually verify the fingerprints by disabling the **Automatically accept SSH keys** option when profiling.

- Configure a local firewall to restrict remote access to the database port (Default port is 9001).

Troubleshooting tips

To help you troubleshoot, One Identity recommends the following resolutions to some of the common problems you might encounter as you deploy and use Management Console for Unix.

NOTE: Simply re-profiling a host can resolve issues caused when the host is out of sync with the server.

Auto profiling issues

The following topics may help you resolve some problems related to Auto Profiling.

- Auto profiling takes a long time
- Auto profiling returns an error

Auto profiling takes a long time

If auto-profiling multiple hosts does not complete within a reasonable amount of time and the host is configured for multiple consoles, make sure each console address is valid and available.

To validate the console addresses

1. On the unresponsive host, open the `<Service Account Home Dir>/.quest_ autoprofile/notify.rc` configuration file.

2. Remove the entry for the unresponsive server.

NOTE: If the host continues to be unresponsive, here are some other things you can try:

- Verify the network connection.

- Verify the console address is correct in **Settings | System Settings | General | Console information**.

If this has changed, re-configure the host for auto-profile.

- Check the firewall settings. Make sure the non-SSL port is not blocked for incoming traffic on the host that has the Management Console for Unix software installation.

  The default is 9080.

  Note: If you have customized your HTTP or SSL/TLS ports, see Customizing HTTP and SSL/TLS ports on page 186 for more information.

There could be any number of things that would prevent the host from communicating with the console.

Auto profiling returns an error

If you receive an error when auto-profiling a host after a recent upgrade from 1.0.x, verify the console host address in **System Settings**.

To validate the console host address

1. From the **Settings** menu, navigate to **System Settings | General | Console Information**.

2. Verify that the host address in the **Console host address** box is the Fully Qualified Domain Name address.

   The host address in the **Console host address** box on the **Console Information** settings may have been entered as a simple address in version 1.0. To perform some tasks in version 2.x without error, such as auto-profiling, the **Console host address** must be a Fully Qualified Domain Name.

NOTE: Setting up automatic profiling on a host with Security-Enhanced Linux (SELinux) enabled will fail due to the enhanced security-related restrictions on the system. Please contact Technical Support at https://support.oneidentity.com/ for instructions on how to either work-around the issues or disable SELinux.

Active Directory issues

The following topics may help you resolve some problems related to Active Directory.

- Active Directory connectivity issues
- Unable to configure Active Directory
- Active Directory is disabled
- Active Directory tasks are disabled

Active Directory connectivity issues

Certain environmental changes cause Active Directory connectivity issues.

To verify you are communicating with Active Directory

1. If the DNS server changes, restart the server because the Java Naming and Directory Interface (JNDI) caches information about the Active Directory domain for which that the host is configured at server start up.

2. If the Active Directory servers change, restart the servers due to SRV record caching in ActiveDirectoryInfoManager.

3. Verify that time is synchronized between the Management Console for Unix server and the Active Directory domain.

   Kerberos requires that the Management Console for Unix server and Active Directory domain controller clocks are within five minutes of each other.

Unable to configure Active Directory

You specify the Active Directory configuration (that is, the set of domains, sites, and servers that you want the mangement console to contact) from **System Settings | Active Directory | Advanced Settings**. To access the **Advanced Settings** dialog, you must provide Active Directory credentials; then, once the console verifies the configuration, it saves the settings to the database.

There may be an occasion when the Active Directory configuration becomes invalid. Perhaps you set the AD configuration to specifically restrict login to a specific domain. Then later, you receive a network error saying the Active Directory credentials you provided to perform an action have been revoked because that domain no longer exists. If the Active Directory configuration becomes invalid for any reason, you will not be able to access the **Advanced Setting** dialog to change the AD configuration.

This topic explains how to temporarily set the `ad.config.domain` or `ad.config.site` system properties in the `custom.cfg` file to specify a temporary configuration to use until you can reset the AD configuration from **System Settings | Active Directory | Advanced Settings**.

- `ad.config.domain` system property contains the name of a single Active Directory domain. When specified, the mangement console will only contact Active Directory servers in this domain.

  | NOTE: Do not configure the console for a domain outside of the current forest.

- `ad.config.site` system property contains the name of a single Active Directory site. When specified, the mangement console will only contact Active Directory servers in this site.

| NOTE: Do not attempt to change the domain you are joined to with this method. You can only change the configuration within the same domain.

To reset Active Directory domain or site settings

1. Stop the Management Console for Unix service.

   See Start/stop/restart Management Console for Unix service on page 215 for details.

2. Locate the `custom.cfg` file.

   See Setting custom configuration settings on page 208 for more information about customizing configuration settings for the mangement console.

3. Add one of the following properties:

   ```
   -Dad.config.domain=<domain>
   ```

   -OR-

   ```
   -Dad.config.site=<site>
   ```

   NOTE: Only specify the `ad.config.domain` or the `ad.config.site` system property. If you specify both, the console will ignore the `ad.system.domain` setting.

4. Save the `custom.cfg` file.

5. Restart the Management Console for Unix service.

6. Navigate to **System Settings | Active Directory | Advanced Settings** to specify which sites, domains, domain controllers, or global catalogs you want the console to contact.

   See Configuring advanced settings on page 167 for details.

7. Stop the Management Console for Unix service.

8. Locate the `custom.cfg` file.

9. Remove the temporary properties you added in Step #3. Either:

   ```
   ad.config.domain=<domain>
   ```

   -OR-

   ```
   ad.config.site=<site>
   ```

10. Save the `custom.cfg` file.

11. Restart the Management Console for Unix service.

Active Directory is disabled

Kerberos is a time-sensitive protocol and requires that the clocks on the Management Console for Unix server and your Active Directory domain controllers are synchronized within five minutes. If the Management Console for Unix server gets out of sync with the Active Directory domain controller, Active Directory will be disabled temporarily and you will be instructed to check your Active Directory settings.

During the post install process, if you see an error such as "Can't find domain controller for <domain>", verify that the Management Console for Unix server and Active Directory domain controller clocks are synchronized.

Active Directory tasks are disabled

If you are logged on as an Active Directory account in the **Manage Hosts** role and the host is joined to Active Directory, but are not able to perform the Active Directory tasks, ensure that you have sufficient permission in Active Directory to perform the task.

NOTE: Read-Only domain controllers do not allow modifications. If you are still unable to perform Active Directory tasks, verify if any read-only domain controllers exist in the configured forest.

Auditing and compliance

Each action performed by the mangement console on a remote host is logged to the local syslog file. The syslog messages show you who performed the action, when, and the output (standard error, standard out).

Syslog reports any action that changes on the host, for example:

- Add, delete, modify user or group account information
- Add user to (or remove user from) users.allow
- Configure Privilege Manager policy server
- Enable (or disable) Auto Profile, SSH Key login, Auto Authentication Services agent status
- Install software
- Join to (or unjoin from) Active Directory or Privilege Manager policy group
- Map user to (or unmap user from) Active Directory

NOTE: The messages are logged in the local syslog file. Local host logs messages to local audit log files based on your host configuration.

Cannot create a service connection point

To create an SCP for Management Console for Unix

- While the mangement console does not need to be configured for Active Directory, Management Console for Unix must be installed on a computer that is joined to an Active Directory domain.

- The computer object must have access to create child objects under its own computer object.

    NOTE: The ability for SELF to create and delete child objects is allowed by default, so you should not have problems creating Service Connection Points (SCPs) unless the Discretionary Access Control List (DACL) has been changed to deny the *Create all child objects* permission.

- If the console is installed on a Windows host, SSPI must be enabled.

If you cannot create an SCP, check whether the computer where Management Console for Unix is installed is joined to the Active Directory domain.

- If the computer is NOT joined to the domain, then the **Register a Service Connection Point with Active Directory** option on the **Console Information** settings is disabled.

    NOTE: When Management Console for Unix is installed on a Unix or Linux computer, it might be possible that the Management Console for Unix server does not have access to the keytab file. When Management Console for Unix cannot read the keytab file, it acts as if it is installed on a Unix computer that is not joined to the domain.

- If the computer is joined to the domain and the creation of the SCP fails, the most likely cause is that the computer Discretionary Access Control List (DACL) '*Create all child objects*' was denied for SELF. Using the Active Directory Users and Computers (ADUC) tool, you can check and modify these permissions on the **Security** tab of the computer's properties. Consult the Microsoft documentation for information about using ADUC.

Check QAS agent status commands not available

The "Check QAS" commands are only available for hosts that have the Authentication Services 4.0.3.78 (or later) Agent software installed. If your version of Authentication Services is not using the 4.0.3.78 version of the `vas_status.sh` script, the mangement console will not report QAS agent status. Furthermore, if you customize the `vas_status.sh` script, ensure the output for customized tests are in CSV format so that the mangement console will correctly report the results.

CSV or PDF reports do not open

If you are having trouble opening CVS or PDF reports, here are some suggestions:

- Make sure your browser does not have a pop-up blocker enabled for the site. PDF and CSV files are opened as a window pop-up and require you to disable any browser pop ups before the report will open.
- If you are running Management Console for Unix on Internet Explorer, you may need to adjust your IE settings, as explained below:

To adjust your IE settings

1. From the **Tools** menu, select **Internet Options**.
2. On the **Advanced** tab, scroll to **Security** section.
3. Clear the **Do not save encrypted pages to disk** option.
4. Apply the changes.
5. Close and reopen your browser.
6. Try downloading that file again.

Or, you may need to reset your **Download** options.

To modify the Download Internet options

1. From your Internet Explorer browser, navigate to **Tools | Internet Options** and click the **Security** tab.
2. In the **Security Settings** dialog, click the **Custom level** button, scroll down to **Downloads**, and ensure that the **Automatic prompting for file downloads** and **File download** settings are set to **Enable**.

   NOTE: If you hold down the **Ctrl** key after you open the **Export** drop-down menu and select **PDF**, it allows the download to happen even if you have the **Automatic prompting for file downloads** setting disabled.

Database port number is already in use

The database server binds to port 9001. If you see an error in the log file stating that port 9001 is already in use, change the database default port number.

To change the database port number

1. Locate the `jdbc.properties` file.

   If it does not exist, create this text file and save it in the application data directory:

- On Windows:

  ```
  %SystemDrive%:\ProgramData\Quest Software\Management Console for
  Unix\resources
  ```

- On Unix/Linux:

  ```
  /var/opt/quest/mcu/resources
  ```

2. Open the `jdbc.properties` file with a text editor and enter the following line:

   ```
   hsql.server.port=n
   ```

   where: *n* is an unused port on the host where the console is running.

Elevation is not working

If you run a task using elevation and that user does not have rights to perform that action, you will get an error. The error message will tell you what command that user account is unable to run. Verify the elevation password is correct and that the user has been granted permission to run that command. Edit the policy file and give that user permission to run that command.

You can generate an Access & Privilege report to gather more information. See Access & Privileges reports on page 149 for details.

Hosts do not display

If you are expecting to find a host that the mangement console is not listing, perhaps your filters are incorrectly set.

The drop-down menus for the **Host state**, **Authentication Services State**, **Joined to Domain**, and **Status** columns allow you to filter the items displayed by various criteria.

- Use the **Host state** column drop-down menu to filter the hosts by "profiled" state.
- Use the **Authentication Services state** column drop-down menu to filter the hosts by "QAS agent status" state.
- Use the **Joined to Domain** column drop-down menu to filter the hosts by "joined" or "ready" state.
- Use the **Status** column drop-down menu to filter the hosts by "joined" or "ready" state.

NOTE: When you set a filter for one of these columns, the mangement console italicizes and bolds the column heading.

When you select a filter, the console only displays the hosts that match the criteria you set. It is important to understand that when you set multiple filters, the console only displays the hosts that meet all of the criteria you have selected.

If you want the mangement console to temporarily ignore the filter options for a column, clear the **Filters** option box in the drop-down menu. Then, re-select the **Filters** option, to re-enable those filter settings.

If filters are set, the console enables the **Clear column filters** task bar button.

To clear host filters

1. To clear a particular filter setting, open the column drop-down menu, navigate to **Filters**, and deselect the individual options.

2. To clear all filters set on any column, click the **Clear column filters** button in the **View** pane of the task bar.

Import file lists fakepath

Issue: The word "fakepath" displays in a file path rather than the actual file path. You may see this when, using Internet Explorer, you attempt to import hosts to the mangement console from a file and it displays `C:\fakepath<filename>` in the **File** box on the **Import hosts from file** dialog. This is a browser-specific issue where "fakepath" indicates that the site was not trusted.

NOTE: The import works whether it displays "fakepath" or not. That is, if you click **OK** when it displays `C:\fakepath<filename>` in the **File** box, the mangement console populates the list of hosts into the **Add Hosts** dialog from the file.

Resolution: Open the browser's Internet options and add the site to your trusted sites collection. When you add the site in question to the "Trusted sites" list in **Internet Security Properties** it will return the file path.

Information does not display in the console

If you are expecting to see information for a host that the mangement console is not showing, perhaps you have not selected to view those columns.

Use the **Columns** menu in the **View** panel of the task bar to display information related to either Privilege Manager or Authentication Services in the mangement console.

To display the One Identity product-related information

1. Open the **Columns** menu and choose either **Privilege Manager** or **Authentication Services** or both.

By choosing **Privilege Manager**, the Privilege Manager-related columns display in the mangement console; that is, the **Installed**, **Version** and **Status** columns. By choosing **Authentication Services**, the Authentication Services-related columns display in the mangement console; that is, the Authentication Services state column, represented with the ⚠ icon, the **Version**, and **Joined to Domain** columns.

NOTE: All columns show by default. Once you have opened (or closed) a column group, the mangement console remembers the setting from session to session. However, if you reinstall Management Console for Unix, it reverts back to the default of showing all columns.

License information in report is not accurate

The `pmloadcheck` daemon runs on each configured policy server to verify its status. It controls load balancing and failover for connections made from the host to the configured policy servers, and, on secondary servers, it sends license data to the primary server.

The **Product License Usage** report is only accurate up to the last synchronization interval which by default runs every 60 minutes.

NOTE: The **Product License Usage** report does not include trial license information.

Out of memory error

If you see `java.lang.OutOfMemoryError` in the logs then may need to adjust your JVM memory allocation. See JVM memory tuning suggestions on page 214 for details.

Post install configuration fails on Unix or Linux

If you installed Management Console for Unix on a Unix or Linux computer that has Authentication Services installed and is joined to an Active Directory domain and encountered the following error message when running the post installation configuration of the mangement console: "`Can't find domain controller for <domain>`", verify your installation configuration.

To verify the installation configuration

1. Verify that DNS is valid and that the server can connect to the domain.

2. Verify that you are configured for a domain in the same forest to which you are joined.

   NOTE: If the computer is not joined to a domain, you could have configured the mangement console for any domain reachable by DNS.

3. If you have Authentication Services installed, verify that the `host.keytab` file is valid by running the following command without error:

   ```
   /opt/quest/bin/vastool -u host/ -k <path_to_keytab> info id
   ```

   NOTE: Typically, the `host.keytab` file is located at: `/etc/opt/quest/vas/host.keytab`.

4. If you recently joined or rejoined and there are multiple domain controllers in the domain, wait for the computer object to be replicated to all domain controllers in the forest.

5. Verify that the clocks for the Management Console for Unix server and the Active Directory domain controller are synchronized.

   Kerberos requires that the Management Console for Unix server and Active Directory domain controller clocks are within five minutes of each other.

Privilege Manager feature issues

Management Console for Unix integrates with Privilege Manager, including the ability to centrally manage policy. The following topics may help you resolve some of the common problems you might encounter.

- Join to policy group failed
- Join to policy group option is not available
- Preflight fails because the policy server port is unavailable
- Policy Change report reports newlines

Join to policy group failed

When you join a remote Sudo Plugin host to a policy group you are required to enter a password in the **Joined password** box. The join password is the password for the `pmpolicy` user that was set when the `qpm-server` was configured. See Configuring the primary policy server on page 109 for details.

If the join operation does not recognize the `pmpolicy` user password, you will receive an error message with the following snippet:

```
Enter password for pmpolicy@<host>:
      [FAIL]
      - Failed to copy file using ssh.

      - Error: Failed to add the host to the list of known hosts
      (/var/opt/quest/qpm4u/pmpolicy/.ssh/known_hosts).
      Permission denied, please try again.
      Permission denied, please try again.
      Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).

      ** Failed to setup the required ssh access.
      ** The pmpolicy password is required to copy a file to the primary
      ** policy server.
      ** To complete this configuration, please rerun this command and
      ** provide the correct password.
```

Run the join operation again entering a correct password.

Join to policy group option is not available

If you run the **Check Client for Policy Readiness** with no errors and the console indicates that the host is "Ready to join" a policy group, yet the **Join to Policy Group** option is not available, this topic will help you troubleshoot the issue.

To join a host to a policy group, the host must meet all of the following conditions:

- When using a sudo policy type, to join a policy group, the selected hosts must have Sudo 1.8.1 (or higher), the Sudo Plugin software installed, and be added and profiled to the mangement console.

- When using pmpolicy type, the host must have the PM Agent software installed on it. See Installing Privilege Manager agent or plugin software on page 116.

- A service account must be configured on the primary policy server. See Configuring a service account on page 169).

- A policy group must be active. See Activating policy groups on page 171.

- If you select multiple hosts to join, they must be of the same type (sudo or pmpolicy). However, when selecting multiple primary servers, the *Join* option will be disabled because each primary server belongs to a different policy group.

Once you meet these conditions, you can run the **Join to Policy Group** option from the **Prepare** panel of the **All Hosts** view. See Joining the host to a policy group on page 111 for details.

Preflight fails because the policy server port is unavailable

If you have the `qpm-server` installed and you run **Check Client for Policy Readiness** from the mangement console and it tells you the policy server port is unavailable, check the port to see if another program is using that port.

Policy Change report reports newlines

The **Policy Change Report** reports newlines as a change in policy. All policy files have newlines at the end by default. If you open a policy in the GUI editor without newlines, it adds a newline to the end of each policy file. The **Policy Change Report** then reports this action as a change to the policy.

Profile task never completes

If the host remains in a profiling state, it is likely that SSH is improperly configured on that host. Verify that you can SSH to the host manually.

If the host does not reset its profiled state to either **Profiled** or **Not Profiled** within a reasonable time, restart the Management Console for Unix service (`mcu_service`) to reset its profile state. See the Start/stop/restart Management Console for Unix service on page 215 for details.

questusr account was deleted

The *questusr* account is the user service account, a non-privileged account created when you configure a service account from the mangement console. This account is used by the console to gather information about existing policy server in a read-only fashion.

NOTE: The *questusr* account does not require root-level permissions, and, the mangement console does not use *questusr* account to make changes to any configuration files.

To recreate the questusr account

1. Re-profile the host.

2. Unconfigure the service account.

   See Unconfiguring a service account on page 171 for details.

3. Configure the service account again.

   See Activating policy groups on page 171 for details.

Readiness check failed

If you run a readiness check and in the **Task Progress** windows you see an error message that says, "`Failed to find software at: ....`", verify that the path to the software is correctly set in **System Settings**. See Setting the Privilege Manager software path on page 172 or Setting Authentication Services software path on page 82 for details.)

NOTE: The path to the software packages must point to the directory containing the preflight file.

Recovering from a failed upgrade

By default, Quest Identity Manager for Unix version 1.0.*x* was installed at:

- On Windows 32-bit platforms:

  `%SystemDrive%:\Program Files\Quest Software\Identity Manager for Unix`

- On Windows 64-bit platforms:

  `%SystemDrive%:\Program Files (x86)\Quest Software\Identity Manager for Unix`

- On Unix/Linux platforms:

  `/opt/quest/imu`

When upgrading from version 1.0.*x*, by default, One Identity Management Console for Unix is installed at:

- On Windows platforms:

  `%SystemDrive%:\Program Files\Quest Software\Management Console for Unix`

- On Unix/Linux platforms:

  `/opt/quest/mcu`

When you install One Identity Management Console for Unix 2.*x*, it detects if Quest Identity Manager for Unix version 1.0.*x* is already installed.

If for some reason the upgrade procedure fails, make note of the step in the upgrade procedure where the failure occurred.

Here are the steps it takes:

1. Stops the old IMU service.
2. Disables the autostart flag.
3. Installs version 2.*x*
4. Migrates the data from the IMU database to the MCU database.
5. Starts the new MCU service.
6. Uninstalls IMU 1.0.*x* (if you selected this option)

If a failure occurs during the upgrade procedure that prevents the upgrade from completing successfully and you have not opted to uninstall the database, the original database will be intact.

To recover from a failed upgrade

1. Copy the backup of the application database to the Quest Identity Manager for Unix version 1.0.*x* data directory.
2. Uninstall Management Console for Unix.

   See Installing and uninstalling the console on Windows on page 26 for instructions.
3. Reinstall the IMU version 1.0.*x*.

   See the *Quest Identity Manager for Unix 1.0.x Administrator's Guide* for instructions.

Reports are slow

The console may appear to "stick" in the data collection phase while generating reports.

To troubleshoot this issue, consider these possible reasons:

- You are reporting on a large dataset.
- You have a slow connection with Active Directory.
- Your network connection is slow.
- The JVM memory size is too small. See JVM memory tuning suggestions on page 214 for details.

Reset the supervisor password

The ***supervisor*** is the only account that has rights to change the ***supervisor*** account password in **System Settings**.

You entered the password for the ***supervisor*** account when you initially configured Management Console for Unix. See Set Supervisor Password dialog on page 32 for details.

The easiest way to change the ***supervisor*** password, is to log into the console as the ***supervisor***, navigate to **System Settings | General | Change Password** and modify it there. If you have forgotten the current ***supervisor*** account, you can reset the ***supervisor*** password by making changes to the configuration file. However, you must have administrator rights on the computer to access the file.

To reset the supervisor password

1. Locate the `custom.cfg` file.

   See Setting custom configuration settings on page 208 for more information about customizing configuration settings for the mangement console.

2. Add the following line to the end of the file:

   ```
   -Dforce.supervisor.password.reset=new_password
   ```

   where *new_password* is the new password.

3. Save the `custom.cfg` file.

4. Restart the Management Console for Unix service.

5. Log onto the mangement console as ***supervisor*** and provide the new password.

6. Remove the line added in Step 2 from the `custom.cfg` file and save the configuration file.

NOTE: If you leave the `-Dforce.supervisor.password.reset` parameter in the `custom.cfg` file, the mangement console will reset the specified password each time you start the service.

Running on a Windows 2008 R2 domain controller

When running Management Console for Unix on a Windows 2008 R2 Domain Controller, you must change your User Account Control Settings.

To change your User Account Control Settings

1. From the **Start** menu, navigate to **Control Panel | User Account | User Accounts | Change User Account Control settings**.

2. On the **User Account Control Settings** dialog, adjust the notification level to **Never notify** and click **OK**.

Service account login fails

There could be several reasons why you might receive an error message saying you could not log in with the user service account:

- Account does not exist
- Account has been disabled
- Account has invalid gid or login shell
- SSH server is not running
- SSH keys are not configured properly
- SSH server is not configured to allow login by means of SSH key
- SElinux may be disallowing access to SSH server files needed for SSH key authentication

To troubleshoot your login failure,

- Check your SSH server configuration to verify that public key authentication is enabled. (Refer to your SSH server configuration instructions for details.)
- Test SSH key authentication with another user.
- Reconfigure or disable SELinux.

NOTE: Configuring a service account on a host with Security-Enhanced Linux (SELinux) enabled might fail due to the enhanced security-related restrictions on the system. Contact Technical Support at https://support.oneidentity.com/ for instructions on how to either reconfigure or disable SELinux.

Setting custom configuration settings

When you start the Management Console for Unix service, it reads Java Virtual Machine (JVM) system properties from a configuration file.

You can set custom configuration settings by adding system properties, one per line, to the `custom.cfg` file, in the form:

```
-Dproperty=value.
```

The `custom.cfg` file is in the application data directory:

- On Windows:

```
%SystemDrive%:\ProgramData\Quest Software\Management Console for
Unix\resources
```

- On Unix/Linux:

  ```
  /var/opt/quest/mcu/resources
  ```

Here are some general tips for adding system properties to the `custom.cfg` file:

- All system property declarations must be on its own line:

  ```
  -Xms512m
   -Xmx512m
  ```

- Do not enter multiple entries on a single line like this:

  ```
  -Xms512m  -Xmx512m
  ```

- A line preceded by a # character specifies a commented line and will be ignored.
- The system property declarations are case sensitive. Be sure to enter lines to the `custom.cfg` file carefully.
- Restart the console service to enable the system property declarations.

The following topics give you details about setting custom system properties:

- To customize the heartbeat interval for auto-tasks, see Customize auto-task settings on page 209.
- To enable and generate debug logs, see Enable debug logging on page 210.
- To tune JVM memory settings, see JVM memory tuning suggestions on page 214.
- To disable SSL/TLS Authentication, see Disabling SSL/TLS encryption on page 185.
- To solve single sign-on issues, see Single Sign-on (SSO) issues on page 211.

Customize auto-task settings

Management Console for Unix uses a heartbeat to verify that the:

- host system is still properly configured to send updates
- current QAS status is accurate

You can customize the heartbeat interval for the automatic QAS Status update. However, if you change the heartbeat interval you must reconfigure automatic QAS agent status for all hosts previously configured.

To customize heartbeat interval

1. Locate the `custom.cfg` file.

   See Setting custom configuration settings on page 208 for more information about customizing configuration settings for the mangement console.

2. Add the following property:

```
-Dmcu.QasStatusHeartbeatsPerDay=n
```

where *n* is the number of times per day. (The default is 6 times a day.)

Valid values are: 1,2,3,4,6,8,12, and 24 times a day.

The actual time of day that heartbeats are sent vary from host to host.

3. Save the `custom.cfg` file.
4. Restart the Management Console for Unix service.

Enable debug logging

Technical Support may request that you enable and generate some debug logs for troubleshooting purposes.

To enable the debug logging

1. Stop the Management Console for Unix service

   See Start/stop/restart Management Console for Unix service on page 215 for details.

2. Open the `custom.cfg` file for editing.

   See Setting custom configuration settings on page 208 for general information about customizing configuration settings for the mangement console.

3. Add these system properties to the `custom.cfg` file:

```
-Dlog4j.configuration=log4j-debug.xml
```

   AND

```
-Djcsi.kerberos.debug=true
```

4. Save the `custom.cfg` file.
5. Start the Management Console for Unix service.

   By default, the debug logs are saved in the application data directory at:

   - On Windows platforms:

```
%SystemDrive%:\ProgramData\Quest Software\Management Console for
Unix\logs
```

   - On Unix/Linux platforms:

```
/var/opt/quest/mcu
```

Single Sign-on (SSO) issues

Management Console for Unix uses the host computer's Active Directory credentials to publish its address to the Control Center, perform single sign-on, and to validate a user's log on. On a Microsoft Windows server, the host computer's credentials are available by means of the Windows SSPI, but this limits Management Console for Unix to managing hosts in the same forest to which the Windows server is joined.

If you wish to use Management Console for Unix to manage a foreign domain or forest from a Windows server, then you must disable SSPI. See Disable SSPI for Single Sign-on on page 213. However disabling SSPI will disable single sign-on capabilities.

> NOTE: To perform single sign-on, you must
>
> - Configure Management Console for Unix for Active Directory.
> - Join your Management Console for Unix server to an Active Directory domain.
>
>   If your Management Console for Unix server is on a Linux platform, you must have Authentication Services installed to join Active Directory.
> - Join the client host (where the browser is located) to the Active Directory domain.
> - Login to the browser host using an Active Directory account.

On a Unix server, Management Console for Unix looks for the host computer's credentials by searching for a Kerberos keytab file in the following default locations:

- /etc/opt/quest/vas/HTTP.keytab
- /etc/opt/quest/vas/host.keytab

To override the default location, set the `console.keytab` system property in the `custom.cfg` configuration file, as follows:

```
-Dconsole.keytab=<PropertyValue>
```

See Setting custom configuration settings on page 208 for more information about overriding the default configuration settings.

If Management Console for Unix cannot find host computer credentials, it will run without host credentials by relying on a correctly configured DNS to find foreign domain controllers. This means that Management Console for Unix will be unable to publish its address to the Control Center, perform single sign-on, or fully validate passwords used when logging on.

Configure a Firefox web browser for SSO

In order for SSO to work on Mozilla Firefox on the host where Management Console for Unix is installed, and from a remote browser, you must configure the web browser to use Windows Integrated Authentication to automatically authenticate to the web browser.

To configure a Firefox web browser for SSO

1. Enter **about:config** in the URL address field of your web browser.

2. Enter **negotiate** in the filter search box.

3. Locate and configure the following Firefox preferences:

   ```
   network.negotiate-auth.delegation-uris = https://
   network.negotiate-auth.trusted-uris = https://
   ```

4. Save your changes and restart the browser for the changes to take effect.

Configure an IE web browser for SSO

In order for SSO to work on Windows Internet Explorer on the host where Management Console for Unix is installed, and from a remote browser, you must specify the sites in the Internet Security properties.

To configure an IE web browser for SSO

1. From Windows Internet Explorer, navigate to **Tools | Internet Options**.

2. On the **Security** tab, select the **Local Intranet** zone and click **Sites**.

3. From the **Local Intranet** dialog, click **Advanced**.

4. Add websites to this zone and click **Close**.

5. Save your changes and restart the browser for the changes to take effect.

Disable Single Sign-on (SPNEGO/HTTP negotiation)

If system credentials are available, Management Console for Unix attempts single sign-on by default. However, if you are experiencing problems, you can disable single sign-on.

To disable single sign-on

1. Locate the custom.cfg file.

   See Setting custom configuration settings on page 208 for general information about customizing configuration settings for the mangement console.

2. Add the following system property to the custom.cfg file to completely disable single sign-on:

   ```
   -Dconsole.login.sso.disable=true
   ```

   To disable single sign-on using the WinSSPI:

```
-Dconsole.login.sso.sspi-only=true
```

3. Save the `custom.cfg` file.

4. Restart the Management Console for Unix service.

   See Start/stop/restart Management Console for Unix service on page 215 for details.

Disable SSPI for Single Sign-on

If you are experiencing (non-SSO) login difficulties on a Windows server and the log file indicates that SSPI is unable to find the domain, you can disable SSPI and "fall back" to the JCSI provider. To do this you must add a system property to the `custom.cfg` configuration file.

NOTE: The drawback of using JCSI on a Windows server is that some integration features (such as, SCP, SSO, and trusted KDC) are unavailable.

Security Support Provider Interface (SSPI) is used to provide web single sign-on on Windows but limits logins and administration to domains within the same forest as the Windows host. If you are hosting the console on a Windows server joined to a forest different than the one it is administering, then you should disable SSPI. A pure-Java Kerberos implementation will be used instead, but it will not be able to do single-sign-on on Windows.

To disable SSPI

1. Open the `custom.cfg` file for editing.

   See Setting custom configuration settings on page 208 for general information about customizing configuration settings for the mangement console.

2. Add the following properties to the `custom.cfg` file to disable SSPI:

   ```
   -Dconsole.sspi.disable=true
   ```

   Or, if your problem is only with TGT validation, add this line:

   ```
   -Dconsole.sspi.disable-self-test=true
   ```

3. Save the `custom.cfg` file.

4. Restart the Management Console for Unix service.

   See Start/stop/restart Management Console for Unix service on page 215 for details.

Enable SSO for remote browser clients

In order for remote browser clients to log onto the mangement console using SSO, Management Console for Unix requires that the web browser 'delegate' the user's

credentials to the server. Therefore, you must enable the Management Console for Unix server for delegation.

To enable the Management Console for Unix server for delegation

1. Open Active Directory Users and Computers.

2. Navigate to the container in the domain on which the computer where Management Console for Unix is running resides.

   For example, if the console is installed on a domain controller, navigate to **<DomainName> | Domain controllers** and find the computer object.

3. In the details pane, right-click the computer object and click **Properties**.

4. Open the **Delegation** tab, select **Trust this computer for delegation to any service (Kerberos only)** and click **OK** to save your selection and close the properties.

NOTE: In Active Directory, computer objects have a property that gets set when you select **Trust this computer for delegation to any service (Kerberos only)**. SSO will not work if delegation is not enabled on the server.

For the delegation changes to take effect in Active Directory, you may need to reboot the client.

JVM memory tuning suggestions

Previous releases of the Management Console for Unix used Java 6 and tended to require manual tuning of the JVM memory settings. Java 8 reduces the need for this because, by default it automatically chooses its initial and maximum heap sizes as fractions of the host's memory size. The resulting maximum heap size can be displayed by running this command:

java -XshowSettings:vm -version

However, there may still be scenarios for which manual tuning is desirable. If you are experiencing performance degradation due to heavy demand from web service calls, simultaneous report generation, multiple browser connection querying, and so forth, One Identity recommends that you increase the JVM memory.

To tune JVM memory

1. Open the custom.cfg file for editing.

   See Setting custom configuration settings on page 208 for general information about customizing configuration settings for the mangement console.

2. Set the initial or start memory size using the -Xms variable and the maximum memory size using the -Xmx variable. For example:

   ```
   -Xms512m
   ```

-AND-

```
-Xmx512m
```

where "512m" specifies 512MB of memory or "1g" specifies 1GB of memory.

NOTE: 1024MB is the default memory requirement.

One Identity recommendations:

- For each 1,000 application database records (hosts, uses, groups, group memberships), increase the JVM memory by 20MB to support 1 to 3 simultaneous web browser connections.
- For each 1,000 records, increase the memory by 30MB to support 3 to 5 simultaneous web browser connections.
- Do not allocate more memory than you have; the console will fail to load.

These suggested specifications depend on your reporting demands. If you create more than two or three reports simultaneously, increase the memory specification.

For further information on specific settings refer to `<install_directory>/jvmargs.cfg`

These values are used for the JVM heap which reserves memory for the server and its database. Increasing the amount of memory available can improve performance, but increasing it too much can have a detrimental effect in the form of longer pauses for full garbage collection runs. Setting `-Xms` and `-Xmx` to the same value increases predictability by removing the most important sizing decision from the virtual machine. On the other hand, the virtual machine cannot compensate if you make a poor choice. Be sure to increase the memory as you increase the number of processors, since allocation can be parallelized. JVM heaps greater than 1.5 Gbytes require a 64-bit JVM. Anything more than that will cause the service to not start.

Numbers can include 'm' or 'M' for megabytes, 'k' or 'K' for kilobytes, and 'g' or 'G' for gigabytes. For example, 32k is the same as 32768. Unless you have problems with pauses, try granting as much memory as possible.

For further reading on garbage collection tuning refer to https://docs.oracle.com/javase/8/docs/technotes/guides/vm/gctuning/.

3. Save the `custom.cfg` file.
4. Restart the Management Console for Unix service.

   See Start/stop/restart Management Console for Unix service on page 215 for details about restarting the Management Console for Unix Service.

Start/stop/restart Management Console for Unix service

Depending on the platform you are using, use the corresponding procedure to start, stop, or restart the Management Console for Unix service (`mcu_service`).

ONE IDENTITY™

Linux or Solaris machines

***To stop, start, or restart the Management Console for Unix service (mcu_
service) on a Linux/Solaris machine***

1. Log onto the machine as root user.

2. At the root prompt, enter one of the following commands:

   To stop and restart the service automatically:

   ```
   /etc/init.d/mcu_service restart
   ```

   To stop the service and unload it:

   ```
   /etc/init.d/mcu_service stop
   ```

   To load the service and start it:

   ```
   /etc/init.d/mcu_service start
   ```

HP Unix (HPUX) machine

***To stop, start, or restart the Management Console for Unix service (mcu_
service) on an HP Unix machine***

1. Log onto the machine as root user.

2. At the root prompt, enter one of the following commands:

   To stop and restart the service automatically, enter:

   ```
   /sbin/init.d/mcu_service restart
   ```

   To stop the service and unload it, enter:

   ```
   /sbin/init.d/mcu_service stop
   ```

   To load the service and start it, enter:

   ```
   /sbin/init.d/mcu_service start
   ```

Windows machine

To stop, start, or restart the Management Console for Unix service (mcu_service) on a Windows machine

1. If you installed the **Start** menu items, navigate to **Start | Programs | Quest Software | Management Console for Unix** to either stop the service or start the service.

   This is handy on Windows 7+ because you can use the <windows_key> to search for it quickly.

2. Otherwise, you can log onto the machine as *root* user.

3. Navigate to **Start | Programs | Administrative Tools | Services** to open the **Services** dialog.

4. Locate and select the One Identity Management Console for Unix jetty service in the list.

   Use the **Start**, **Stop**, or **Restart** commands from the **Action** menu or right-click context menu.

Toolbar buttons are not enabled

You use the toolbar buttons across the top of the **All Hosts** view to perform individual tasks against one or more managed host systems. If the toolbar buttons are not active, it might be due to

- Host state
- User account role and permissions
- View settings

Host State

If you select multiple hosts, they all must be in the same state (added, profiled, or joined) to perform the desired task. If they are not all in the same state, the toolbar button for that task will be disabled.

For example, if you select all hosts, but one or more of them are not profiled, the **Install Software** toolbar button will not be available for the whole group. If you deselect the hosts that are not profiled, the **Install Software** toolbar button becomes active. Also, if one of the selected hosts is currently being profiled by auto-profile, the web services, or by another console user, the **Profile** button will be disabled. You can either wait for the profile task to complete, or deselect the host to activate the **Profile** button.

User Account Role and Permissions

Another reason for a disabled toolbar button might be your user account role. You may only have read-only access to the view and are not allowed to perform the desired task. For example, if your user account is not in the *Manage Hosts* role, then you cannot make changes to hosts.

View Settings

Other tasks, such as **Clear column filters** have nothing to do with host state or user roles. That toolbar button is only enabled if you have column filters set. If there are no column filters set, then the option to **Clear column filters** is disabled. When one or more filters are set, then the option is enabled.

UID or GID conflicts

Management Console for Unix does not automatically pick up changes to the host made externally to the console unless you configure the host for auto-profiling.

For example, when you install Privilege Manager software on a remote host, it creates a new user and group named *pmclient*, assigning a UID and GID accordingly. If you do not profile the host after installing the Privilege Manager packages, the mangement console will not recognize the new user name and group name. If you attempt to configure that host for auto-profiling or automatic QAS status updates without profiling, you might encounter a UID conflict, such as this:
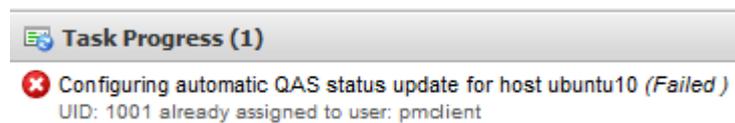
Or, if you attempt to add a new local group to that host without profiling, you might encounter a GID error like this:
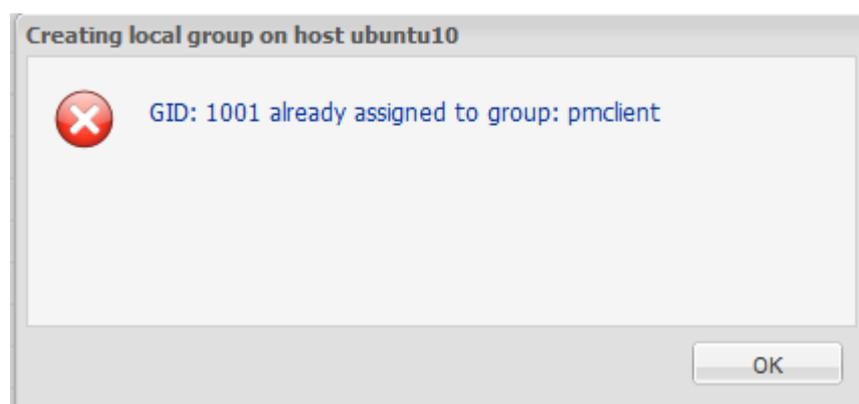
If you encounter a UID or GID conflict, profile the host and try the action again before you troubleshoot the problem further.

> NOTES:

- As a best practice, configure newly added hosts for auto-profiling before you perform any other actions so that the mangement console dynamically updates user and group information. See Automatically profiling hosts on page 42 for details.

- If Authentication Services is installed you may also get these errors because of UID/GID conflicts with Active Directory accounts. In this case, because the mangement console does not check for Active Directory conflicts, you will have to manually create the user with a different ID.

System maintenance

It is important to safeguard your data. One Identity recommends that you maintain copies of the most important files so you're always prepared for the worst.

This appendix provides general information and guidelines for maintaining or backing up your data.

Backup procedure

It is necessary to perform a backup when the service is not running. You can use normal backup methods, such as archiving the files in a compressed bundle.

To backup the Management Console for Unix program files

1. Shutdown the service.

2. Copy the application data directory to a backup location.

   By default, the application data directory is:

   - On Windows:

     ```
     %SystemDrive%:\ProgramData\Quest Software\Management Console for Unix
     ```

   - On Unix/Linux:

     ```
     /var/opt/quest/mcu
     ```

3. Restart the service.

   NOTE: For more information on stopping and restarting the service, see Start/stop/restart Management Console for Unix service on page 215.

Restore procedure

It is necessary to restore your files when the service is not running.

To restore the Management Console for Unix program files

1. Shutdown the service.

2. Replace the application data directory files with the ones you previously backed up.

   By default, the application data directory is:

   - On Windows:

     ```
     %SystemDrive%:\ProgramData\Quest Software\Management Console for Unix
     ```

   - On Unix/Linux:

     ```
     /var/opt/quest/mcu
     ```

3. Once you have replaced the files, restart the service.

   NOTE: For more information on stopping and restarting the service, see Start/stop/restart Management Console for Unix service on page 215.

Command line utilities

Management Console for Unix provides Unix command line utilities and Windows Powershell cmdlets that enable you to script common local Unix user and group management tasks. For example, you can write a script to reset a local Unix user's password across multiple Unix systems.

MCU PowerShell cmdlets and Unix CLI commands

PowerShell modules provide a "scriptable" interface to many mangement console tasks. Using Management Console for Unix PowerShell commands, you can manage group membership, change user passwords, or connect to the Management Console for Unix Web service.

Management Console for Unix provides the following PowerShell cmdlets and Unix CLI commands, grouped according to service:

Table 18: PowerShell cmdlets and Unix CLI commands

PowerShell cmdlet	Unix CLI command	Description
Administrative Services		
Connect-QmcuService	connect-qmcuservice	Connect to the Management Console for Unix Web Service specified by DNS name or IP address.
Disconnect-QmcuService	disconnect-qmcuservice	Disconnects from the Management Console for Unix Web Service.
Get-QmcuConnection	get-qmcuconnection	Lists the computer connection information.
Remove-QmcuCom-puterCredential	remove-qmcucom-putercredential	Removes specified host credentials from the mangement console

PowerShell cmdlet	Unix CLI command	Description
		cache.
Set-QmcuCom-puterCredential	set-qmcucom-putercredential	Caches specified host credentials on the management console.
Computer Services		
Find-QmcuComputer	find-qmcucomputer	Finds hosts managed by the console matching a specified search criteria.
Find-QmcuGroup	find-qmcugroup	Finds local group information matching specified search criteria.
Find-QmcuUser	find-qmcuuser	Finds local user information matching specified search criteria.
Get-QmcuComputer	get-qmcucomputer	Lists hosts managed by the mangement console.
Get-QmcuGroup	get-qmcugroup	Lists local group information for the specified host.
Get-QmcuUser	get-qmcuuser	Lists local user information for the specified host.
New-QmcuComputer	new-qmcucomputer	Adds a host to the mangement console.
New-QmcuGroup	new-qmcugroup	Creates a new local group on the specified host.
New-QmcuUser	new-qmcuuser	Creates a new local user on the specified host.
Remove-QmcuComputer	remove-qmcucomputer	Removes a host from the mangement console.
Remove-QmcuGroup	remove-qmcugroup	Removes a local group from the specified host.
Remove-QmcuUser	remove-qmcuuser	Removes a local user from the specified host.
Update-QmcuComputer	update-qmcucomputer	Updates a specified host's profile.
Group Services		
Add-QmcuGroupMember	add-qmcugroupmember	Adds local users to the specified local group.
Get-QmcuGroupMember	get-qmcugroupmember	Lists all local users in a specified group.

PowerShell cmdlet	Unix CLI command	Description
Remove-QmcuGroupMember	remove-qmcugroup-member	Removes specified local users from specified local group.
User Services		
Add-QmcuGroupMembership	add-qmcugroup-membership	Adds the specified local user to the specified groups.
Get-QmcuGroupMembership	get-qmcugroup-membership	Lists all local groups of which the specified local user is a member.
Remove-QmcuGroupMembership	remove-qmcugroup-membership	Removes the specified local user from the specified groups.
Set-QmcuUserPassword	set-qmcuuserpassword	Sets the password for the specified local user.
Functions		
Get-QmcuBanner		Displays the MCU powershell console "Welcome" banner which gives basic instructions for viewing the Management Shell cmdlets.
Import-QmcuModule		Updates the Powershell module path and imports the MCU module.

MCU PowerShell cmdlets

Installing MCU PowerShell cmdlets

If the **MCU Powershell console** option is not available from the **Start** menu, under **Programs | Quest Software | Management Console for Unix**, then run the setup wizard, as follows:

To install the Management Console for Unix Powershell console

1. From the root of the distribution media, navigate to **console | client | windows**.
2. Double-click the "Quest_MCU_Powershell_cmdlets" `.msi` file to start the setup wizard.

   NOTE: For information about the `QmcuWebserviceExamples.zip` file also contained in this directory, see Web services examples on page 235.
3. At the **Welcome** dialog, click **Next**.
4. Accept the license agreement and click **Next**.
5. At **Ready to Install** dialog, click **Install**.

ONE IDENTITY™

6. At **Completed** dialog, click **Finish**.

7. To access a customized PowerShell console, from the **Start** menu, navigate to **All Programs | Quest Software | Management Console for Unix** and click **MCU Powershell console**.

To uninstall the MCU Powershell console

1. From the **Start** menu, navigate to **Control Panel | Programs | Programs and Features | Uninstall a program**.

2. Right-click **Management Console for Unix Powershell Cmdlets** and choose **Uninstall**.

3. Click **Yes**, to confirm the action.

Viewing MCU PowerShell cmdlet help information

To view Management Console for Unix Powershell cmdlet help

1. To list all Management Console for Unix PowerShell cmdlets in alphabetical order, from the Powershell prompt, enter

   ```
   Get-Command *Qmcu*
   ```

   where ***** is a wildcard.

2. To view information about a specific PowerShell cmdlet, enter

   ```
   Get-Help <CmdletName>
   ```

   -OR-

   ```
   <CmdletName> -?
   ```

   This displays the Syntax, Description, Related Links, and Remarks for the command.

3. To see examples for the cmdlet, enter

   ```
   get-help <CmdletName> -examples
   ```

4. For more information about the cmdlet, enter

   ```
   get-help <CmdletName> -detailed
   ```

5. For technical information about the cmdlet, enter

   ```
   get-help <CmdletName> -full
   ```

Unix CLI commands

Installing Unix CLI packages

To install Unix CLI packages

1. Log into your client computer and open a root shell.
2. Mount the distribution media.
3. From the root of the distribution media, navigate to **console | client**.
4. Run the appropriate command:

Table 19: Unix CLI packages

Platform	Install
Linux x86 - RPM	# rpm -ihv /<mount>/client/linux-x86/mcu-cli-<version>.x86.rpm
Linux x86 - DEB	# dpkg -i /<mount>/client/linux-x86/mcu-cli-<version>.x86.deb
Linux x86_64 - RPM	# rpm -ihv /<mount>/client/linux-x86_64//mcu-cli-<version>.x86_64.rpm
Linux x86_64 - DEB	# dpkg -i /<mount>/client/linux-x86_64/mcu-cli_<version>_amd64.deb
Solaris 10 x86	# pkgadd -d /<mount>/client/solaris8-x86/mcu-cli-<version>-i386.pkg

Uninstalling Unix CLI packages

To uninstall Unix CLI packages

1. Log in and open a root shell.
2. Run the following commands to remove the packages:

Table 20: Unix CLI packages: Uninstall commands

Package	Command
RPM	# rpm -e mcu-cli
DEB	# dpkg -r mcu-cli
Solaris	# pkgrm mcu-cli

Upgrading the Unix CLI packages

To upgrade the Unix CLI packages

1. Log in and open a root shell.
2. Mount the installation DVD and run the appropriate command:

   Table 21: Unix CLI packages

Platform	Install
Linux x86 - RPM	# rpm -Uvh /<mount>/client/linux-x86/mcu-cli-<version>.x86.rpm
Linux x86 - DEB	# dpkg -i /<mount>/client/linux-x86/mcu-cli_<version>_amd64.deb
Linux x86_64 - RPM	# rpm -Uvh /<mount>/client/linux-x86_64//mcu-cli-<version>.x86_64.rpm
Linux x86_64 - DEB	# dpkg -i /<mount>/client/linux-x86_64/mcu-cli_<version>_amd64.deb
Solaris 10 x86	# pkgadd -d /<mount>/client/solaris8-x86/mcu-cli-<version>-i386.pkg

Mac CLI commands

Installing Mac CLI packages

To install Mac CLI packages from the command line

1. Mount the dmg:

   ```
   hdiutil attach <media>/client/mac-<version>/mcu-cli-<version>.dmg
   ```

2. Copy the files to the application directory:

   ```
   sudo cp –r /Volumes/mcu-cli/mcu-cli /Applications/
   ```

3. Unmount the dmg:

   ```
   hdiutil detach /Volumes/mcu-cli
   ```

To uninstall the Mac CLI packages

1. Remove the `mcu-cli` folder:

   ```
   sudo rm –r /Applications/mcu-cli
   ```

Installing Mac CLI packages using the GUI

To install Mac CLI packages from graphical user interface

1. From the root of the distribution media, navigate to **console | client**.
2. Select either the **mac-105** or **mac-106** folder, depending on your operating system.
3. Double-click `mcu-cli-<version>.dmg` to mount the disk image file.
4. Drag the *mcu-cli* icon to the **Applications** folder.

   NOTE: Commands need to be in the path to run them.

To uninstall the Mac disk image file (dmg)

1. Drag the *mcu-cli* icon from the **Applications** folder to the Trash.

Examples of using command line utilities

The following are some examples of using the Management Console for Unix Powershell cmdlets and the Unix CLI command utilities.

- Connect to the console
- Add host to the console
- Create local group across all managed hosts
- Add a local user to a group on each managed host
- Add localuser to a group on all Linux machines
- Get a user on a specific computer
- Find a UID on a computer
- Remove all credentials stored in the console for a specific host
- Set a local user's password
- View a group's membership

Connect to the console

To connect to the mangement console
Powershell:

```
Connect-QmcuService -Server  test.example.com
```

Unix CLI:

```
connect-qmcuservice -s  test.example.com
```

Add host to the console

To add a new computer to the mangement console
Powershell:

```
New-QmcuComputer -ComputerName test.example.com
```

Unix CLI:

```
new-qmcucomputer -c test.example.com
```

You can also pipe commands together to accomplish a set of tasks.

To add, profile, and cache a computer's credentials, pipe these commands together:
Powershell:

```
New-QmcuComputer -ComputerName test.example.com | Set-QmcuComputerCredential |
Update-QmcuComputer
Login
SSH to computer: test.example.com
User: root
Password for user root: *******
```

Unix CLI:

```
new-qmcucomputer -c test.example.com | set-qmcucomputercredential | update-
qmcucomputer
Specify credentials to log in to test.example.com:
Username: root
Password: *******
```

- `New-QmcuComputer` adds the computer to the console.
- `Set-QmcuComputerCredential` caches the computers credentials.
- `Update-QmcuComputer` updates the computers profile.

The mangement console prompts you for the user name and password when it sets the credentials.

Create local group across all managed hosts

To create a new group named "admins" on all "Linux" computers
Powershell:

```
Find-QmcuComputer -Filter "OperatingSystemName=Linux" | New-QmcuGroup -Groupname
admins
```

Unix CLI:

```
find-qmcucomputer -f "OperatingSystemName=Linux" | new-qmcugroup -C –n admins
```

Add a local user to a group on each managed host

To add local users fred, joe, and bob to the admins group on each managed host
Powershell:

```
Find-QmcuGroup -Filter "Name=admins" | Add-QmcuGroupMember -Member fred,joe,bob
```

Unix CLI:

```
find-qmcugroup -f "Name=admins" | add-qmcugroupmember -m fred joe bob
```

Add localuser to a group on all Linux machines

To add localuser to a group on all Linux machines
Powershell:

```
Find-QmcuComputer -Filter "OperatingSystemName=Linux*" | Add-QmcuGroupMember -
GroupName admins -Member localuser
```

Unix CLI:

```
find-qmcucomputer -f "OperatingSystemName=Linux*" | add-qmcugroupmember -n admins
-m localuser
```

Get a user on a specific computer

Get a user on a specific computer
Powershell:

```
Get-QmcuUser -Username fred –ComputerName test.example.com
```

Unix CLI:

```
get-qmcuuser -n fred –c test.example.com
```

Find a UID on a computer

***To find all users on computer test.example.com that have a UID greater than
1000 and print the results in a tabular format***
Powershell:

```
Get-QmcuComputer -ComputerName test.example.com | Find-QmcuUser -Filter "UID>1000" |
Format-Table
```

Unix CLI:

```
get-qmcucomputer -c test.example.com | find-qmcuuser  -f "UID>1000" | format-table
```

Remove all credentials stored in the console for a specific host

***To remove all credentials stored in the mangement console for the
test.example.com***
Powershell:

```
Get-QmcuComputer -ComputerName test.example.com | Remove-QmcuComputerCredential
```

Unix CLI:

```
get-qmcucomputer -c test.example.com | remove-qmcucomputercredential
```

Set a local user's password

To set local user bob's password on test.example.com
Powershell:

```
Get-QmcuComputer -ComputerName test.example.com | Set-QmcuUserPassword -Username bob
```

Unix CLI:

```
get-qmcucomputer -c test.example.com | set-qmcuuserpassword -n bob
```

View a group's membership

To view what users are a member of a group
Powershell:

```
Get-QmcuComputer  -ComputerName  test.example.com  |  Get-QmcuGroupMember  -Groupname
localgroup
```

Unix CLI:

```
get-qmcucomputer -c test.example.com | get-qmcugroupmember -n localgroup
```

Web services

Management Console for Unix's Web Services interface allows you to integrate the Management Console for Unix database with other solutions that provide management or administrative capabilities, such as HR systems. For example, you can use these development tools to enable One Identity Access Manager to make web service calls containing an Active Directory user identifier to
retrieve information from the mangement console database about the local Unix accounts for this user.

This appendix documents how to access and authenticate to the Management Console for Unix Web Services interface.

NOTE: Web Service calls will fail with a `ProtocolException ((412) Precondition Failed)` error if you have not completed the mangement console post-installation configuration. See Setting up Management Console for Unix on page 30 for details.

Accessing the web services

To access the Management Console for Unix web services

1. Open an Internet Explorer web browser window and navigate to:

   ```
   https://<localhost>:9443/webservices
   ```

   where <localhost> is the name or IP address of the host on which the mangement console is installed.

   The Web Services interface displays a list of available SOAP services and provides links to the Computers, Credentials, Groups, and Users WSDLs.

2. Click a WSDL link to open the associated usage documentation.

Web services

Management Console for Unix provides the following Web services:

NOTE: Your "endpoint address" value as shown in the table below will be relevant to your installation. For example, replace <localhost:9443> with the name or IP address, and port of the host on which your mangement console is installed.

Table 22: Web services

Web Service	Description
ComputersService	
• AddNewGroup • RemoveGroup • GetRemoveGroupStatus • GetQasProfile • GetRemoveUserStatus • GetAddNewGroupStatus • GetNextAvailableUID • Get • GetAddNewUserStatus • GetByName • NOOP • GetAll • RemoveUser • GetGroups • GetProfileStatus • Remove • AddNewUser • Find • GetNextAvailableGID • GetUsers • Add • Profile	**Endpoint address**: https://<localhost:9443>/webservices/Computers/2010/08 **WSDL**: {http://webservices.mcu.quest.com/Computers/2010/08/} ComputersService **Target namespace**: http://webservices.mcu.quest.com/Computers/2010/08/
CredentialsService	
• NOOP • HasCached • RemoveCached • Cache	**Endpoint address**: https://<localhost:9443>/webservices/Credentials/2010/08 **WSDL**: {http://webservices.mcu.quest.com/Credentials/2010/08/} CredentialsService

Web Service	Description
	Target namespace: http://webservices.mcu.quest.com/Credentials/2010/08/

GroupsService

- AddMembers - GetUpdateStatus - GetRemoveMembersStatus - RemoveMembers - NOOP - Update - GetMembers - Find - GetAddMembersStatus	**Endpoint address**: https://<localhost:9443>/webservices/Groups/2010/08 **WSDL**: {http://webservices.mcu.quest.com/Groups/2010/08/} GroupsService **Target namespace**: http://webservices.mcu.quest.com/Groups/2010/08/

UsersService

- SetPassword - GetGroups - Find - NOOP - RemoveGroups - GetRemoveGroupsStatus - Update - GetAddGroupsStatus - AddGroups - GetSetPasswordStatus - GetUpdateStatus	**Endpoint address**: https://<localhost:9443>/webservices/Users/2010/08 **WSDL**: {http://webservices.mcu.quest.com/Users/2010/08/} UsersService **Target namespace**: http://webservices.mcu.quest.com/Users/2010/08/

Web services examples

To help you learn how to access the Management Console for Unix WebService api using Web service calls, One Identity has included eight code sample projects in the product. From the installation media, navigate to /console/client/windows/QmcuWebserviceExamples.zip directory and extract the contents of the QmcuWebserviceExamples.zip file.

The `Readme.txt` file describes each of the example projects and discusses a few important points that will help you use the WebService calls.

Database maintenance

Management Console for Unix uses a HSQLDB (Hyper Structured Query Language Database) to store its data such as information about the hosts, settings, users, groups, and so forth. This appendix provides general database information and guidelines for maintaining this database.

Database location and files

Database location

Management Console for Unix database files are located in the following locations:

- On Unix/Linux: `/var/opt/quest/mcu/db`
- On Windows: `%SystemDrive%:\ProgramData\Quest Software\Management Console for Unix\db`

Database files

The data for each database consists of multiple files located in the same directory. All the database files start with the same name as defined by the value in the `jdbc.url` key. For Management Console for Unix, the database consists of the following files by default:

Table 23: Database files

File	Description
console.lck	This file is used to determine if the database is in use. If `console.lck` exists, the server is currently running. This file is deleted once the database is properly shutdown. DO NOT BACKUP THIS FILE.
console.log	This file contains the extra SQL statements that have modified the console database since the last checkpoint (something like the 'Redo-log' or 'Transaction-log', but just text.) For a normal shutdown this file is deleted once the database has completely shutdown.

File	Description
console.properties	This file contains general settings about the database including the console.properties entry 'modified'. If [modified=yes], the database is either running or was not closed correctly (because the close algorithm sets 'modified' to 'no' at the end).
console.script	This file contains the SQL statements that make up the database up to the last checkpoint.

Database backup procedure

It is best to perform a backup when the HSQLDB is not running. use normal backup methods, such as archiving the files in a compressed bundle.

To backup a database

1. Shutdown the HSQLDB server. See Start/stop/restart Management Console for Unix service on page 215 for details about starting and starting the Management Console for Unix Service.

2. Copy the following files to a backup location: console.properties and console.script.

3. Once the HSQLDB server is stopped, replace the files in the database directory with the ones you previously backed up. See Database location and files.

4. Once you have replaced the files, start the HSQLDB server.

NOTE: If a backup immediately follows a checkpoint, then the console.log file can also be excluded, reducing the significant files to console.properties and console.script.

You can backup the files while the HSQLDB server is running, but make sure that a shutdown or checkpoint is NOT performed during the backup. If you perform a backup while the server is running, you will need to backup the console.log file, as well. This file will be deleted once the server is shutdown.

Database states

Use the following information to determine if the database was shutdown successfully.

State after shutting down the HSQLDB server:

- The console.script file contains the information in the database, excluding data for text tables.

- The console.properties file contains the entry [modified=no].

- There is no console.log file.

Aborted database state (may happen by sudden power outage, Ctrl+C in Windows)

- The `console.properties` file still contains the entry [`modified=yes`].

- The `console.script` file contains a snapshot of the database at the last checkpoint and is *OK*.

- The `console.log` file contains all the information to restore all the changes since the snapshot. As a result of abnormal termination, this file may be partially corrupt.

One IDENTITY™

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales and other inquiries, such as licensing, support, and renewals, visit https://www.oneidentity.com/company/contact-us.aspx.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product

Index

ONE IDENTITY™

L

launch

mangement console 29

licenses

alerts 175, 178

system settings 174, 179

updating 32

local groups

add 59

add AD user 97

add local user 60

delete 62

modify properties 60

remove AD user 97

search for 59

Local Unix Groups report 148

display 62

Local Unix User Conflicts report 145

Local Unix Users report 145

display 69

Local Unix Users with AD Logon
report 145

local users

add 64

add to local group 60

change password 67

delete 69

map to Active Directory users 98

modify properties 66

modify properties for multiple
users 66

remove 61

search for 65

view users required to logon using AD
account 100

log file

location 137, 210

login

accepted credentials formats 33

with AD password 100, 104

login shell field

modify for multiple users 66

Logon Policy for AD User report 149

Logon Policy for Unix Host report 149

loopback interface 190

M

Mac disk image file

installing 227-228

uninstalling 227-228

manage

local users and groups 99

SSH host keys 187

managing a foreign domain or forest
from a Windows server 211

mangement console

add hosts 39

database maintenance 237-238

install 25

launch 29

security 180

service

start 216-217

stop 216-217

system overview 19

system requirements 22

Unix install and uninstall 28

upgrade from free version 71

Windows install 27

Windows install and uninstall 26

One IDENTITY™

One Identity™

One **IDENTITY**™

ONE IDENTITY™