One Identity Management Console for Unix 2.5.1

Release Notes

October 2017

These release notes provide information about the One Identity Management Console for Unix release.

NOTE: This version of the One Identity Management Console for Unix release notes have been rebranded for One Identity.

About this release

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 management console:

- Local Unix user and group management
- Active Directory integration
- Privilege Manager integration
- Remote agent deployment

- Role-Based Access Control
- Reporting
- Securing Local Unix accounts with Active Directory authentication
- Web services

New features

The following is a list of the new feature introduced in One Identity Management Console for Unix.

Version 2.5.1 new features

There are no new features for the current release. See Resolved issues for the list of issues addressed and enhancements implemented in this release.

Version 2.5.0 new features

The following is a list of the new features in One Identity Management Console for Unix 2.5.0:

- **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
  - Support for Tectia SSH
- **New features for One Identity Privilege Manager for Sudo**
  - Support for Mac OS X
- **One Identity 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 features**
  - Reset or change passwords for multiple local accounts across multiple hosts
  - Modify certain user properties across multiple hosts
  - Context-sensitive help
  - New control role for access to all reports
  - Product License Usage report

Resolved issues

The following is a list of issues addressed and enhancements implemented in One Identity Management Console for Unix 2.5.1.

Table 1: 2.5.1 resolved issues and enhancements

Resolved Issue	Issue ID
When you install Authentication Services 4.0.3 on Solaris 10 (SPARC - 32/64 bit), the Solaris 10 SPARC packages are installed.	28050
Orphaned_kerberos SRV record no longer causes AD auth to fail.	28056
The Access and Privileges by User report now reports privileges for users who received privileges from Unix-enabled group.	28088
You can now specify where you want to install the management console.	28111
You can specify the database port during install; but you can not modify the database port on upgrade.	28152
Auto-profile on AIX with existing cron.deny file correctly creates a cron.allow file.	28168
Can now upgrade Privilege Manager for Unix 5.6 to 6.0 via the management console.	28203 28204
Workstation-only licenses now register count in the management console.	28384
Access and Privilege reports display all users/hosts in the details list.	28388
Fixed issue when saving policy on Firefox.	28389

The following is a list of issues addressed and enhancements implemented since the Management Console for Unix 2.5.0 release.

Table 2: 2.5.0 resolved issues and enhancements

Resolved Issue	Issue ID
Console now tracks report task ids and cancels any that have not finished when application closes or you navigate away.	26374
Enabling auto-profile on a box without a cron.allow no longer blocks all users from using cron.	26455
Console now properly displays names in group membership when QAS lowercase-names is set to true.	26458
Error message improved to indicate what the real failure was.	26784
Profile now works when /tmp directory is mounted with the noexec flag.	26861
Console now allows you to join to Active Directory using SU elevation.	26964
Local groups report no longer makes unnecessary queries to Active Directory.	26986
When reporting QAS Access Control rules, we now correctly handle OUs.	27047
Tasks requiring service accounts (such as auto-profile) create cron.allow if it does not exist. Now is created with root as the owner.	27049
Auto-profile now uses custom port specified.	27267
Console now displays VMware ESX #.# on Host list and Host properties.	27377
Console now allows quotes in the password.	27418
Console now installs software successfully with /bin/rpm permissions set to 700.	27430
Console now allows passwords with spaces.	27494

Known issues

The following is a list of issues known to exist at the time of release.

There are no issues known to exist at the time of the One Identity Management Console for Unix 2.5.1 release.

Table 3: Version 2.5.0 known issues

Known Issue	Issue ID
PowerShell Cmdlets != comparison operator is not working for "Find" filters. **Workaround**: Use PowerShell cmdlets to search for objects.	27854

Known Issue	Issue ID
Policy Editor When multiple people are editing the same policy file, the last saved version of the policy overwrites the other's changes.	27703
Java Plugin Compatibility Running Firefox with the JVM Plugin may produce security issues when loading applets. Because of the frequent updating of Firefox and Java Plugin, the editor applet and/or midterm SSH applet might not work. Make sure you are using the latest versions of both Firefox and Java Plugin on the client you use to access the console.	27871
SSH Failure Management Console for Unix does not support Security-Enhanced Linux (SELinux).	27455

System requirements

One Identity Management Console for Unix consists of two main components: a web server and a client (or management console). Before installing Management Console for Unix 2.5.1, ensure that your system meets the following minimum hardware and software requirements for your platform.

One Identity Management Console for Unix Web Server

Table 4: Web Server requirements

Requirement	Details
Supported Windows Platforms	Can be installed on 32-bit or 64-bit editions of the following configurations: • Windows XP SP2 (or later) • Windows Vista • Windows 7 • Windows 8 • Windows Server 2003 SP1 (or later) • Windows Server 2008

Requirement	Details
	• Windows Server 2008 R2 • Windows Server 2012 NOTE: When running One Identity Management Console for Unix on Windows 2008 R2, functioning as a domain controller, the process must be elevated. As a best practice, One Identity does not recommend that you install or run the Windows components on Active Directory domain controllers. The recommended configuration is to install them on an administrative workstation. NOTE: The performance of some Active Directory searches may be better on: • 64-bit: Windows 2003 64-bit (and above) • 32-bit: Windows 2003 SP1 + hotfix* or Windows 2003 SP2 (and above). * Click Microsoft Support to read a Microsoft article entitled, "A hotfix is available that improves the performance of programs that query Active Directory for group memberships in Windows Server 2003". To apply this hotfix, you must have Windows Server 2003 Service Pack 1 (SP1) installed. NOTE: The 64-bit versions of Windows Server 2003 already include the fixes and features that are included in Windows Server 2003 SP1. If the computer is running a 64-bit version of Windows Server 2003, you do not have to install SP1.
Server requirements	The Management Console for Unix server requires Sun Java Runtime Environment (JRE) version 1.6. Installation of the server on a Windows operating system includes a download of 32-bit version of the 1.6 JRE for server use; Linux and Mac servers can run a 64-bit version of the 1.6 JRE. A separate Java browser plugin may be required for the web browser. For more information, see Supported web browsers. NOTE: Management Console for Unix: • is not supported on AIX • does not support Java 1.7
Managed host requirements	Click here to review a list of Unix, Linux, and Mac platforms that support Authentication Services.

Requirement	Details
	Click here to review a list of Unix and Linux platforms that support Privilege Manager for Unix. Click here 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 above) and Tectia SSH 5.0 (and above) 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 requirements	1024 MB NOTE: See *JVM Memory Tuning Suggestions* in the console online help for information about changing the default memory allocation setting in the configuration file.
Supported web browsers	While the Management Console for Unix server requires Sun JRE version 1.6; to use specific features, such as the SSH to Host feature or the Policy Editors, you must install the Sun Java browser plugin version 1.6 (or above). You can install both the Sun JRE and Java browser plugin on the same machine. For example, if you are running the browser on the machine where the server resides, you may install both the Sun JRE 1.6 and the Java browser plugin 1.7. The management console officially supports the following web browsers: • Microsoft Internet Explorer, 7, 8, 9, and 10 • Mozilla Firefox 3 (and above) NOTE: Java applets will not run in Firefox 18 with older Java versions (prior to 1.7). See *Java Applet Failures* in the console online help or more information. • Apple Safari 4 (Mac only: Windows not supported) NOTE: One Identity recommends that you: • Do no open two sessions of the management console in the same browser. • Set your screen resolution to a minimum of 1024 x 768 for the best results.

Product licensing

This product does not require licensing.

Upgrade and installation instructions

The process for upgrading One Identity 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 management console and automatically upgrades the components.

Please see the *One Identity Management Console for Unix Administration Guide* for detailed installation and configuration instructions.

NOTE: When installing both One Identity Management Console for Unix AND One Identity Authentication Services, there is no requirement as to which product must be installed first.

Upgrade Notes:

- Before you begin the upgrade procedure:
  - Delete your browser cache (Temporary Internet Files and Cookies).
  - Close One Identity Management Console for Unix and make a backup of your database.
- After an upgrade from any version of the management console, it is important to re-profile all hosts.
- If you are upgrading from Quest Identity Manager for Unix 1.0 to One Identity Management Console for Unix 2.x, be aware of the following:
  - Passwords cached by the supervisor account or Active Directory users with console access were not migrated during the upgrade process due to change 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.
  - Existing Active Directory users and groups granted access to the management console are added to the Manage Hosts role, giving them access to the features they had before the upgrade.

More resources

Additional information is available from the following:

- Online product documentation: Authentication Services - Technical Documentation
- One Identity Privileged Account Management forum: https://www.quest.com/community/products/one-identity/f/privileged-account-management

Globalization

This section contains information about installing and operating this product in non-English configurations, such as those needed by customers outside of North America. This section does not replace the materials about supported platforms and configurations found elsewhere in the product documentation.

This release is Unicode-enabled and supports any character set. In this release, all product components should be configured to use the same or compatible character encodings and should be installed to use the same locale and regional options. This release is targeted to support operations in the following regions: North America, Western Europe and Latin America, Central and Eastern Europe, Far-East Asia, Japan.

This release has the following known capabilities or limitations: One Identity Authentication Services has been tested with double-byte configured locales on the Linux platform. All of the client side components operate successfully with double-byte characters in all Unix attributes

There is no localization of either the client or Windows user interface.

About us

Contacting us

For sales or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

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
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Management Console for Unix Release Notes
Updated - October 2017
Version - 2.5.1