ONE IDENTITY™

One Identity Management Console for Unix 2.5.3

Release Notes

December 2020

These release notes provide information about the One Identity Management Console for Unix 2.5.3 release.

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

This release is a minor release that includes various bug and stability fixes. See Resolved issues for a list of fixes included in this release.

End of support notice

After careful consideration, One Identity has decided to cease the development of the Management Console for Unix (MCU). Therefore, the MCU will enter limited support for all versions on April 1, 2021. Support for all versions will reach end of life on Nov 1, 2021.

As One Identity retires the MCU, we are building its feature set into modern platforms starting with Software Distribution and Profiling. Customers that use the MCU to deploy Authentication Services and Safeguard for Sudo can now use our Ansible collections for those products, which can be found at Ansible Galaxy.

Resolved issues

The following is a list of issues addressed in One Identity Management Console for Unix 2.5.3.

Table 1: Resolved issues

Resolved Issue	Issue ID
Some QPM RPMs blocked on dependencies.	258804
Licensing requirements and reports are removed from MCU in this version.	258796
MCU is updated to include to Jetty 9.4.34.v20201102.	258196
MCU now supports FreeBSD.	257742
After profiling QPM version numbers occasionally contained extra strings, for example: `7.0.0.6 license`.	256007
MCU could not install QAS 5.0 on a macOS.	254695
A `vasgp` upgrade issue was reported, when upgrading from verion 4.1.x to 4.2.x with dpkg.	247576
MCU could not install software on macOS 10.15.	244986

ONE IDENTITY™

Resolved Issue	Issue ID
MCU did not recognize the new `dnsupdate` name. It should recognize both `dnsupdate` and `quest-dnsupdate`.	231187
MCU now more easily detects QPM software folders.	225043
It was not possible to activate certain policy servers in MCU due to issues caused by SSH key length. For example, to configure the default RSA key length to 1024, specify `-DQuestRSAKeyLength=1024`. Expected values are 768, 1024 and 2048. The default value is 2048.	199713
MCU showed incorrect date and time for events.	199672
The default questusr password can now be set to different lengths. An ability to choose from a configurable set of characters is added in this version. For example, to configure the default password length to 12 (minimum 9), in the `custom.cfg` file, specify `-DQuestUsrPwdLength=12` .	199669
Attempting to open a QPM4U 6.1 policy caused it to open and suddenly close. It was only possible to open the policy in text mode.	199666
MCU did not recognize newer QAS packages.	199662
Support is added for MCU for Microsoft Windows Server 2016 and 2019.	199660
After upgrading to MCU 2.5.2, the version in **Help	About** showed old version.	199658
Using MCU to upgrade to QPM 6.1 or 7.0 appeared to fail but then looked fine after re-profiling.	198960

Known issues

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

Table 2: Known issues

Known Issue	Issue ID
SSH Failure Management Console for Unix does not support Security-Enhanced Linux (SELinux).	27455
Policy Editor When multiple people are editing the same policy file, the last saved version of	27703

Known Issue	Issue ID
the policy overwrites the other's changes.	
PowerShell Cmdlets	27854
!= comparison operator is not working for "Find" filters.	
Workaround: Use PowerShell cmdlets to search for objects.	
Windows browser on same host as server	717024
Internet Explorer and Edge running on the same Windows host as the server do not connect.	
Workaround: Run Internet Explorer or Edge on other hosts, or use Chrome or Firefox.	
Help button	736930
The **?** button shows built-in 2.5.1 documentation, not 2.5.3.	
Workaround: https://support.oneidentity.com/authentication-services/technical-documents links to the current online documentation.	
Getting Started tab shows nothing	783061
After logging in the **Getting Started** tab may show none of its content.	
Workaround: Use the browser's **Refresh** button.	

System requirements

Before installing Management Console for Unix 2.5.3, ensure that your system meets the following 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.

One Identity Management Console for Unix Web Server

Table 3: System requirements

Component	Requirements
Supported Platforms	Can be installed on the following configurations:

Component	Requirements
	• 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 referred to as JRE 8, JDK 8, JRE 1.8, and JDK 1.8).
Managed Host Requirements	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* in the *One Identity Management Console for Unix Administration Guide* for information about changing the default memory allocation setting in the configuration file.

Product licensing

Use of this software is governed by the Software Transaction Agreement found at www.oneidentity.com/legal/sta.aspx. This software does not require an activation or license key to operate.

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.

macOS

- Previous releases of Management Console for Unix supported installations on macOS, but the 2.5.2 release has discontinued this support, both for upgrades and for fresh installations.
- However, the 2.5.2 release still supports the use of macOS in other roles, such as profiling, installation of One Identity Authentication Services, and as a browser client.

Java

- For the server:
  - Previous releases required Java 6, and the 32-bit installer for Windows included a Java 6 implementation (JRE 1.6.0_35).
  - This release requires Java 8, and none of the installers include a Java implementation. A Java 8 implementation must be installed before any 2.5.2 installer can be executed, either for an upgrade or for a fresh installation.
- For the client:
  - Previous releases used Java Applet functionality to provide some parts of the user interface, so they expected a Java installation and browser plug-in on the client.
  - This release does not use Java Applet functionality, so it no longer needs nor uses client-side Java.

SSH Applet

- Previous releases included an SSH client implemented as a Java Applet, but this release does not.

- Unix, Linux, and Mac systems generally provide an ssh client already.
- For Windows, a good option is PuTTY, available from the master site at https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html or from the mirror sites listed on https://www.chiark.greenend.org.uk/~sgtatham/putty/mirrors.html.

Customized configurations

This release uses Jetty 9.4.* on Java 8, whereas the 2.5.1 and previous releases used Jetty 7.* on Java 6. The new Jetty and Java combine to provide much better HTTPS security (particularly newer TLS ciphersuites and newer versions of the TLS protocol) by default, without requiring security-related SSL/TLS customizations that had been recommended for previous releases.

If you are upgrading from a previous release and had customized its configuration, please note the following:

- If you customized the `jetty.xml` file:
    - Management Console for Unix 2.5.2 will **not** use any of the `jetty.xml` customizations from the previous release. The new Jetty release uses a newer, more maintainable modular configuration system that avoids modifying its `jetty.xml` file.
    - When the installer detects that you are upgrading and have customized the `jetty.xml` file, it will ask whether to continue or to cancel the installation.
    - If you choose to continue, the customized `jetty.xml` file will be preserved as `jetty.xml.bak` so that you can review it (and compare it with a `jetty.xml.baseline` file that has no customizations) after the installation completes. This allows you to determine whether the previous customizations are unnecessary for 2.5.2 or whether they are still relevant and should be applied manually to the new configuration.
    - In general, previous `jetty.xml` customizations of the SSL/TLS protocol versions or ciphersuites will no longer be needed, but `jetty.xml` customizations for other reasons may still be pertinent to the upgraded Jetty release.
- If you customized the `jetty.keystorePath` system property (in the `custom.cfg` file):
    - Previous releases specified the keystore location as an absolute pathname, and the `jetty.keystorePath` system property could specify any directory name and filename. By contrast, the Jetty 9.4 configuration design expects the keystore location to be a relative pathname, resolved against the new `jetty-base` directory tree, with a default of `etc/keystore`.
    - The upgrade installer does not attempt to convert old absolute keystore pathnames to new relative keystore pathnames — instead it relocates (moves and renames) the keystore from the location specified by `jetty.keystorePath` to the new default location, and then comments out the `jetty.keystorePath` setting in the `custom.cfg` file to indicate that it is no longer used.
        - If the upgrade installer sees that `jetty.keystorePath` has not been customized (that is, it specifies the default keystore path for the previous release, such as `/var/opt/quest/mcu/resources/keystore` on Unix/Linux) then the keystore is relocated from its old default location to the new

default location.

- If the upgrade installer finds that `jetty.keystorePath` has been customized, then by default it will still relocate the keystore to the new default location, but it provides an "opt-out" check box on the installer screen that displays the TCP ports. This check box is selected by default but may be explicitly cleared to indicate that the keystore should not be relocated.

  NOTE: If this check box is cleared then the upgrade installation will proceed without relocating the keystore, and the resulting configuration will not start successfully until the keystore configuration has been manually adjusted.

After an upgrade:

After an upgrade from any version of the management console, it is important to re-profile all hosts.

More resources

Additional information is available from the following:

- Online product documentation: https://support.oneidentity.com/authentication-services/technical-documents
- One Identity Privileged Account Management forum: https://www.quest.com/community/one-identity/unix-access-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

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