Linux Device Management

VMware Workspace ONE UEM 1907

vmware®

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Copyright © 2019 VMware, Inc. All rights reserved. Copyright and trademark information.

Contents

1 Workspace ONE UEM on Linux 4

Requirements for Workspace ONE UEM on Linux 4

2 Linux Enrollment 5

Enroll Your Linux Devices 5

Command-line Utilities for Workspace ONE Intelligent Hub on Linux 7

3 Linux Device Management 9

Device Dashboard 9

Device List View 11

Linux Device Details Page 12

Workspace ONE UEM on Linux

1

Use Workspace ONE UEM on your Linux devices to enroll and manage your enterprise Linux devices. The Workspace ONE UEM console gives you tools and features to manage the entire lifecycle of Linux devices.

The flexibility of the Linux operating system makes it a preferred platform for a wide range of uses, including notebooks, Raspberry Pi devices, and other IoT-capable devices. With Workspace ONE UEM, you can build on the flexibility and ubiquity of Linux devices and integrate them with your other mobile platforms in a central location for mobile device management.

This chapter includes the following topics:

- Requirements for Workspace ONE UEM on Linux

Requirements for Workspace ONE UEM on Linux

Workspace ONE UEM is compatible with all versions and configurations of Linux running on either x86_64 or ARM7 architecture. Make sure that your system meets these additional Workspace ONE UEM version and network requirements before you deploy your Linux devices.

Linux Requirements

You can enroll devices running any version and any configuration of Linux running on either x86_64 or ARM7 architecture into Workspace ONE UEM.

Workspace ONE UEM Requirements

You can enroll Linux devices in any Workspace ONE UEM version from 1903 onward.

You must deploy the Workspace ONE Intelligent Hub for Linux v1.0.

Linux Enrollment 2

You must enroll Linux devices to establish communication between the devices and Workspace ONE UEM and for devices to access internal content and features.

For Workspace ONE UEM 1903, SAML authentication for enrollment is not supported. Also, advanced and single-user staging enrollment are not supported, where an admin enrolls on behalf of a user, or enrolls and waits for a user to enter credentials.

To download the Workspace ONE UEM Agent for Linux, your organization must be whitelisted with Workspace ONE UEM. Please contact your account representative to receive access to the download file.

This chapter includes the following topics:

- Enroll Your Linux Devices
- Command-line Utilities for Workspace ONE Intelligent Hub on Linux

Enroll Your Linux Devices

To establish communication between each device and the Workspace ONE UEM console, install the Workspace ONE Intelligent Hub on your Linux devices.

You can enroll devices at the same time you install the Intellident Hub, or you can enroll devices with the ws1HubUtil after after you've installed the Intelligent Hub. In either case you can fully script the enrollment in a single command, or you can prompt the user to enter enrollment information.

Prerequisites

Gather the user name, password, organization group, and server address for the Linux device on which you're installing Workspace ONE UEM.

You can also enroll using a token. Obtain the token and use it in the `–group` argument. You will be prompted for user name and password, but you can leave these blank when enrolling with a token.

Also consult the Command-line Utilities for Workspace ONE Intelligent Hub on Linux for commands you use to follow these instructions.

Procedure

1 Download the Workspace ONE Intelligent Hub for Linux (WorkspaceOneIntelligent Hub-Linux-{Arch}-{Version}.sh) from the Workspace ONE Resource Portal. The downloaded file must correspond to the targeted processor architecture.

2 Copy the Workspace ONE Intelligent Hub client file to the file system over SSH or by using a USB drive.

3 Give Workspace ONE Intelligent Hub execute permissions.

For example:

```
$ chmod +x “/tmp/Workspace ONE Intelligent Hub–Linux–x86_64–0.0.0.1.sh"
```

4 Run the Workspace ONE Intelligent Hub client installer with root privileges.

a To install the Workspace ONE Intelligent Hub without enrolling, run the client installer without any additional arguments.

For example:

```
$ sudo “/tmp/Workspace ONE Intelligent Hub–Linux–x86_64–1.0.0.sh”
```

b To install and enroll in a single command, run the client installer with your user name, password, organization group, and server info in the command.

For example:

```
$ sudo “/tmp/Workspace ONE Intelligent Hub–Linux–x86_64–0.0.0.1.sh” ––enroll –user XYZ –
password ‘X Y Z’ –group XYZ –server
```

c To install and prompt the users for enrollment credentials, run the client installer with just the `––enroll` argument. Enter the user name, password, organization group, and server info when prompted.

For example:

```
$ sudo “/tmp/Workspace ONE Intelligent Hub–Linux–x86_64–0.0.0.1.sh” ––enroll
```

5 If you did not enroll during the installation, enroll after the installation using the **ws1HubUtil**. Choose to send enrollment details in one command or separately.

a To automate the enrollment for the end user, run the **ws1HubUtil** and include the enrollment arguments in order.

For example:

```
$ sudo /opt/Workspace ONE Intelligent Hub/bin/ws1HubUtil –enroll –user XYZ –password XYZ –
group XYZ –server https://www.host.com
```

b To prompt the users for enrollment credentials when they enroll, run the **ws1HubUtil** without additional arguments.

Command-line Utilities for Workspace ONE Intelligent Hub on Linux

Use these command-line utilities to expedite your deployment of the Workspace ONE Intelligence Hub on your Linux devices.

Table 2-1. Supported Command-line Arguments for the Client Installer

Command-line argument	Value	Description	Comments
-enroll	N/A	Continue with registration and enrollment after installation.	If not supplied, must run ws1HubUtil.
-user	Enrollment user string	User credentials generated from the console.	Applicable if **-enroll** is used. If no command-line argument is entered, you are prompted to enter the details .
-password	Password string	Credentials generated from the console.	Applicable if **-enroll** is used. If no command-line argument is entered, you are prompted to enter the details .
-group	Organization group string	Organization groupID to which the device must enroll.	Applicable if **-enroll** is used. If no command-line argument is entered, you are prompted to enter the details .
-server	Server string	Console URL to which device has to enroll.	Applicable if **-enroll** is used. If no command-line argument is entered, you are prompted to enter the details .
-path	Directory path	Installation path for the client.	
-keep-logs	N/A	Preserve the client logs after uninstall.	

Table 2-2. Supported Command-line Arguments for the Agent Utility

Command-line argument	Description	Comments
stop	Stops the client processes.	
start	Runs the client processes.	
restart	Restarts the client processes.	
unenroll	Unenrolls the device from console.	Might prompt the client to unenroll based on the response received from the console.
uninstall	Uninstalls the client	

Table 2-3. Supported Command-line Arguments for the ws1HubUtil Utility

Command-line argument	Value	Description	Comments
-enroll	n/a	Continue with enrollment.	Applicable if **-enroll** is used. If no command-line argument is entered, you are prompted to enter the details .
-user	Enrollment user string	User credentials generated from console.	Applicable if **-enroll** is used. If no command-line argument is entered, you are prompted to enter the details .
-password	Password string	Credentials generated from console.	Applicable if **-enroll** is used. If no command-line argument is entered, you are prompted to enter the details .
-group	Organization group string	Organization groupID to which device must enroll.	Applicable if **-enroll** is used. If no command-line argument is entered, you are prompted to enter the details .
-server	Server string	Console URL to which device must enroll.	Might prompt the client to unenroll based on the response received from the console.
-unenroll	n/a	Unenrolls the device from the console.	
-beacon	n/a	Sends beacon to Console.	
-uninstall	n/a	Uninstalls the client.	
-stopService	n/a	Stops the client processes.	
-startService	n/a	Runs the client processes.	
-restartservicee	n/a	Restarts the client processes.	

Linux Device Management

3

After your devices are enrolled and configured, manage the devices using the Workspace ONE UEM console. The management tools and functions enable you to keep an eye on your devices and remotely perform administrative functions.

You can manage all your devices from the UEM console. However, the reporting details and available actions for enrolled devices may vary based on your deployment type and device fleet.

The Dashboard is a searchable, customizable view that you can use to filter and find specific devices. This feature makes it easier to perform administrative functions on a particular set of devices.

The Device List View displays all the devices currently enrolled in your Workspace ONE UEM environment and their status.

The Device Details page provides device-specific information such as profiles, apps, Workspace ONE Intelligent Hub version and which version of any applicable OEM service currently installed on the device. You can also perform remote actions on the device from the Device Details page that are platform-specific.

For information about how VMware handles information collected through Workspace ONE UEM, such as analytics, see https://www.vmware.com/help/privacy.html

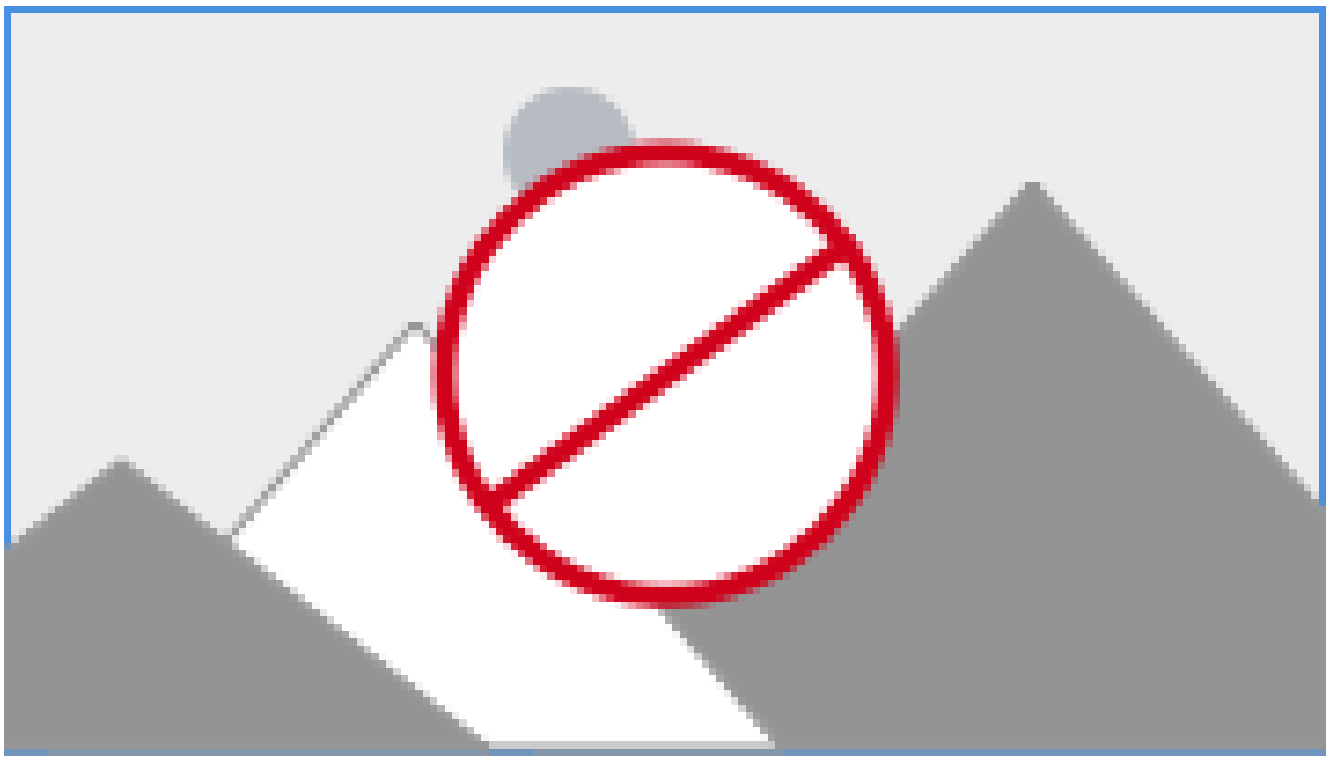
This chapter includes the following topics:

- Device Dashboard
- Device List View
- Linux Device Details Page

Device Dashboard

As devices are enrolled, you can manage them from the **Device Dashboard**.

The **Device Dashboard** provides a high-level view of your entire fleet and allows you to act on individual devices quickly.



You can view graphical representations of relevant device information for your fleet, such as device ownership type, compliance statistics, and platform and OS breakdowns. You can access each set of devices in the presented categories by selecting any of the available data views from the **Device Dashboard**.

From the **List View**, you can take administrative action: send messages, lock devices, delete devices, and change groups associated with the device.

- **Security** – View the top causes of security issues in your device fleet. Selecting any of the doughnut charts displays a filtered **Device List** view comprised of devices affected by the selected security issue. If supported by the platform, you can configure a compliance policy to act on these devices.
  - **Compromised** – The number and percentage of compromised devices (jailbroken or rooted) in your deployment.
  - **No Passcode** – The number and percentage of devices without a passcode configured for security.
  - **No Encryption** – The number and percentage of devices that are not encrypted for security. This reported figure excludes Android SD Card encryption. Only those Android devices lacking disc encryption are reported in the donut graph.

  Ownership – View the total number of devices in each ownership category. Selecting any of the bar graph segments displays a filtered **Device List** view comprised of devices affected by the selected ownership type.

- **Last Seen Overview/Breakdown** – View the number and percentage of devices that have recently communicated with the MDM server. For example, if several devices have not been seen in over 30 days, select the corresponding bar graph to display only those devices. You can then select all these filtered devices and send them a message requesting that they check in.
- **Platforms** – View the total number of devices in each device platform category. Selecting any of the graphs displays a filtered **Device List** view comprised of devices under the selected platform.
- **Enrollment** – View the total number of devices in each enrollment category. Selecting any of the graphs displays a filtered **Device List** view comprised of devices with the selected enrollment status.
- **Operating System Breakdown** – View devices in your fleet based on operating system. There are separate charts for Apple iOS, Android, Windows Phone, and Windows Rugged. Selecting any of the graphs displays a filtered **Device List** view comprised of devices running the selected OS version.

Device List View

Use the UEM console's Device List View to see a full listing of all devices in the currently selected organization group.

For information about a specific device, see the Device Details Page.

The **Last Seen** column displays an indicator showing the number of minutes elapsed since the device has checked-in. The indicator is red or green, depending on the number of minutes defined in **Device Inactivity Timeout (min)**. This indicator can be set by navigating to **Groups & Settings > All Settings > Devices & Users > General > Advanced**.

Select a device in the **General Info** column at any time to open the details page for that device.

Sort by columns and configure information filters to review device activity based on specific information. For example, sort by the **Compliance Status** column to view only devices that are currently out-of-compliance and target only those devices. Search all devices for a friendly name or user name to isolate one device or user.

Customize Device List View Layout

Display the full listing of visible columns in the **Device List** view by selecting the **Layout** button and select the **Custom** option. This view enables you to display or hide Device List columns per your preferences.

There is also an option to apply your customized column view to all administrators at or below the current organization group (OG). For instance, you can hide 'Asset Number' from the **Device List** views of the current OG and of all the OGs underneath.

Once all your customizations are complete, select the **Accept** button to save your column preferences and apply this new column view. You can return to the **Layout** button settings at any time to tweak your column display preferences.

Search in Device List View

You can search for a single device for quick access to its information and take remote action on the device.

To run a search, navigate to **Devices > List View**, select the **Search List** bar and enter a user name, device friendly name, or other device-identifying element. This action initiates a search across all devices, using your search parameter, within the current organization group and all child groups.

Linux Device Details Page

Use the Device Details page of the Workspace ONE UEM console to access user and device actions for your enrolled Linux devices.

Device Details

You can access Device Details by selecting a device's **Friendly Name** from the **Device List View**, using one of the Dashboards, or with any of the search tools.

From the Device Details page, you can access device information broken into different menu tabs. Each menu tab contains related device information, which may vary depending on your Workspace ONE UEM deployment.

- **Summary** - View general statistics such as enrollment status, compliance, last seen, GPS availability, platform/model/OS, organization group, serial number, power status, storage capacity, physical memory, and virtual memory.
- **User** - Access details about the user of a device and the status of the other devices enrolled to this user.
- **Notes** - View and add notes regarding the device. For example, note the shipping status or if the device is in repair and out of commission.
- **Troubleshooting** - View Event Log and Commands logging information.
- **Status History** - View history of device in relation to enrollment status.

Remote Actions

The **More Actions** drop-down on the Device Details page lets you perform remote actions over the air to the selected device. The actions available vary depending on factors such as the device platform, Workspace ONE UEM console settings, and enrollment status.

- **Assign Tags** – Assign a customizable tag to a device, which can be used to identify a special device in your fleet.
- **Change Organization Group** – Change the device's home organization group to another pre-existing OG. Includes an option to select a static or dynamic OG.
- **Edit Device** – Edit device information such as Friendly Name, Asset Number, Device Ownership and Device Category.

- **Enterprise Wipe** – Enterprise Wipe a device to unenroll and remove all managed enterprise resources including applications and profiles. This action cannot be undone and re-enrollment will be required for Workspace ONE UEM to manage this device again. Includes options to prevent future re-enrollment and a Note Description field for you to add any noteworthy details about the action.
  - Enterprise Wipe is not supported for cloud domain-joined devices.
- **Delete Device** – Delete and unenroll a device from the UEM console. This action performs an Enterprise Wipe and removes the device from the UEM console.