VMware Workspace One UEM Integration with ServiceNow

VMware Workspace ONE

vmware®

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

https://docs.vmware.com/

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

Contents

VMware Workspace ONE UEM ServiceNow Integrations

1

With the Workspace ONE UEM integrations with ServiceNow, you can resolve issues quicker and make data-driven decisions based on a wide range of data sets. This topic describes integrating Workspace ONE UEM ServiceNow CMDB and the ITSM Connector for ServiceNow to improve efficiency for helpdesk and support organizations.

Integration with ServiceNow CMDB

ServiceNow CMDB (Configuration Management Database) gives visibility into users' devices and apps for specific incidents. This visibility gives helpdesk administrators a better understanding of the incident and speeds remediation. With ServiceNow CMDB, you can store contextual information relevant to your users or assets.

Using the ServiceNow Service Graph connector for Workspace ONE UEM, you can populate the device and the application data into the ServiceNow CMDB enabling asset tracking and IT Operations Management (ITOM) Visibility. Imported device details in ServiceNow CMDB include important hardware information, user details, and management status. Application details include application name and identifiers, installation statuses, and more.

Use this data within ServiceNow to find device and app details. Helpdesk users include the details for managing tickets and reconciling deployed assets and warranty statuses with procurement.

Integration with the ITSM Connector for ServiceNow

Helpdesk and support organizations face challenges with managing and using multiple tools efficiently. The Workspace ONE UEM ITSM (IT Service Management) connector for ServiceNow helps teams manage these tools.

Before an integration, a support ticket is raised within ServiceNow when encountering an issue ion a device or by an employee. The helpdesk or the support administrator reviews the issue within ServiceNow. Then, they navigate to Workspace ONE UEM for further troubleshooting, remote support, and issue remediation. This frequent switching between multiple systems, while keeping them all in sync with the necessary troubleshooting notes and updates, is inefficient and an annoyance.

With the seamless integration within ServiceNow for Workspace ONE UEM and Workspace ONE Assist, you can simplify Support workflows and increase efficiency. Using the Workspace ONE UEM ITSM Connector for ServiceNow, the helpdesk or the support administrators can access Workspace ONE UEM and Workspace ONE Assist actions from within the ServiceNow portal without navigating to the Workspace ONE UEM console or authenticating multiple systems.

Read the following topics next:

- Integration with ServiceNow CMDB
- Integration with the ITSM Connector for ServiceNow

Integration with ServiceNow CMDB

With ServiceNow CMDB, you can simplify operations, solve issues faster, and make data driven decisions. Also, you can track assets and have ITOM Visibility with the Workspace ONE UEM and ServiceNow CMDB integration.

Before You Begin

To use this Service Graph connector, you need a subscription to a Subscription Unit based in the ITOM Visibility application or in the ITOM Discovery application. Also, you must be able to access the API settings. Create API configurations in Workspace ONE UEM at the Organization Group relevant to this setup (typically the latest parent group including all device and app data).

ServiceNow CMDB supported versions:

- Workspace ONE UEM - any version
- ServiceNow - must be at least Orlando or later

Configure ServiceNow CMDB

1 Set up the Service Graph Connector. You need the following information to complete the graph connector setup:

Form	Description
Application Registries Form	OAuth authentication credentials. You don't need these credentials when configuring Basic Authentication credentials.
HTTP(s) Connection Form	HTTP connection settings for Basic Authentication
Data Source Form	Validate data source settings
Status Values of Applications	Status of applications you want to import
Scheduled Data Import Form	Pre-populated scheduled data

Form	Description
Connection Form	Connection settings for another OAuth connection
SG-Workspace ONE UEM Create Data Source and Scheduled Import Form	Service graph data sources and scheduled data import settings for another OAuth connection

For information on setting up the Service Graph Connector, see Service Graph Connector for VMware Workspace ONE UEM.

2 Complete API integration. To complete the integration, you need the API URL for your instance that appears under **Settings > System > Advanced > API > REST API**.

3 Configure the connection for authentication.

Option 1: Configure OAuth Client. Authentication appears in the Workspace ONE UEM console under **Settings & Groups > Configurations > OAuth Client Management**.

- To add a new OAuth Client and a sufficient role for API access, such as Console, see Create an OAuth Client to Use for API Commands.
- To set up the Token URL for the OAuth for the correct region and URL, see Using UEM Functionality With a REST API.

Option 2: Configure Basic Authentication in Workspace ONE UEM.

a Create and use a Workspace ONE UEM Administrator account for Service Graph with API permissions.

b Select the organization group for connecting to third-party services.

c To generate an API key, go to **Groups & Settings > All Settings > System > Advanced > API > Rest API**. Workspace ONE Intelligence uses the API key to connect to any third-party service.

Integration with the ITSM Connector for ServiceNow

Improve your daily operations for IT management with the Workspace ONE ITSM Connector for ServiceNow. With the ITSM Connector for ServiceNow, helpdesk and support organizations face can access Workspace ONE UEM and Workspace ONE Assist actions from within the ServiceNow portal.

Before You Begin

To configure this connector, you must be able to access the API settings and create API configurations in Workspace ONE UEM at the Organization Group relevant to this setup (typically the latest parent group including all device and application data).

ITSM for ServiceNow supported versions:

- ServiceNow - Quebec or later
- Workspace ONE UEM - 2107 or later

- Workspace ONE Assist - 21.03 or later

Determine your authentication connection. Before configuring the connection in the application, create an OAuth 2.0 client on Workspace ONE UEM or a new dedicated account. Create a role with the required security rights.

For information on the following, see:

- Roles with required security rights: Access-based New User Roles under Assigning Roles
- Creating new role: Create a Role That Can Use REST APIs
- Creating an OAuth Client: Create an OAuth Client to Use for API Commands (Saas)
- Basic Auth account: Admin Accounts

Install the Workspace ONE ITSM Connector for ServiceNow

With the Workspace ONE ITSM Connector for ServiceNow, Workspace ONE UEM device actions can only performed on Workspace ONE UEM enrolled devices. While it is not mandatory, consider installing the Service Graph connector for VMware Workspace ONE UEM prior to installing the ITSM connector. The Service Graph connector ensures that all Workspace ONE UEM devices and their details are available in ServiceNow. For more information, see Integration with ServiceNow CMDB.

Note If the Service Graph connector is not installed, then ensure the device or the configuration item's operating system information that is used in the ServiceNow database matches the following operating system values.

- Android: The operating system value must contain "android".
- iOS device or configuration item: The operating system value must contain "iOS".
- macOS device or configuration item: The operating system value must contain "mac".
- Linux machines or configuration item: The operating system value must contain "Linux".
- Windows desktops or configuration item: The operating system value must contain "windows".

To access Workspace ONE UEM and Workspace ONE Assist functionality from the ServiceNow Incidents page, download and install the VMware Workspace ONE ITSM Connector from the ServiceNow Store.

1 Log in to your ServiceNow instance as an administrator.

2 Install the VMware Workspace ONE ITSM Connector plugin from the plugins directory.

3 Continue through the Guided Setup for the connector.

Configure the Workspace ONE ITSM Connector for ServiceNow

To set up the ITSM connector, you must have the necessary credentials. Search for and select the VMware Workspace ONE ITSM Connector.

To configure the ITSM connector, follow the guided setup. The following are the core configuration actions:

- Configure the connection - Connects your ServiceNow instance to Workspace ONE UEM.
- Configure the actions - Configures the actions available to the ITSM agents.
- Configure the application defaults - Sets the defaults for the application behavior.
- Assign Roles - Assigns VMware Workspace ONE ITSM Connector roles to Groups and Users.

Configure the Connection

The Workspace ONE ITSM Connector supports authentication to Workspace ONE UEM through an OAuth 2.0 client or a Basic Auth and tenant key. OAuth 2.0 is industry standard protocol for secure authentication and authorization for REST API calls.

Option 1: Configure OAuth Details

Use this option in the ServiceNow guided setup if you are using OAuth 2.0. All details for configuration are for the Workspace ONE UEM API. To complete configuration, select and update the following details:

1 Go to the **Configure OAuth Host details** tab and select **Configure**.

2 Update the **Host** text box with the hostname for the Workspace ONE UEM API.

3 Select the **Active** check box.

A warning message might display if you are switching from Basic Auth.

All the other details on this page are preconfigured and should not be modified.

4 Go to the **Configure OAuth Client details** tab and select **Configure** .

5 Enter the OAuth Client details the **Client ID**.

6 Update the **Client Secret**.

7 Update the **Token URL**.

All the other details on this page are preconfigured and should not be modified.

Option 2: Configure Basic Auth Details

Use this section in the ServiceNow guided setup if you are using Basic Auth Details. All details for configuration are for the Workspace ONE UEM API. To complete configuration, select and update the following details.

1 Go to the **Configure Basic Auth Host** tab and select **Configure**.

2 Update the **Host** text box with the hostname for the Workspace ONE UEM API.

3 Select the **Active** check box.

A warning message might display if you are switching from OAuth.

All the other details on this page are preconfigured and should not be modified.

4 Go to the **Configure Basic Credentials** tab and select **Configure**.

5 Update the **User Name** and the **Password** text boxes with credentials of the Basic Auth account you created.

6 Select **Update**.

All the other details on this page are preconfigured and should not be modified.

7 Go to the **Configure Tenant Code** tab and select **Configure**.

8 Update the **Value** text box with the Tenant Code for the Workspace ONE UEM API. The Tenant Code for your instance appears in your Workspace ONE UEMinstance under **Settings > System > Advanced > API > REST API > AirWatchAPI** .

9 Select **Update**.

Validate Connection Details

After configuring the OAuth or the Basic Auth details, validate the connection. This section is read-only and shows the previously configured key values.

When using OAuth 2.0, select **Verify OAuth Token**. A message appears confirming that a token can be retrieved. If an error is reported, then verify and fix the credentials. Repeat until it succeeds.

When using OAuth 2.0 or Basic Auth, select **Test Connection**. The connection to Workspace ONE UEM is verified. The version of the Workspace ONE UEMplatform appears. If there is an error code and error message, then the connection failed. If necessary, verify and update credentials.

Mark each tab as complete before configuring the actions.

Configure Service Desk

Configure all the actions available to the Service Desk Administrator. By default, all actions are available. Edit to remove actions that you do not need.

Configure Actions

Configure all the actions available to the Workspace ONE UEM Administrator. By default, all actions are available.

Complete the following to remove actions that you do not need:

1 Search for and select the VMware Workspace ONE ITSM Connector.

2 Click **Setup**.

3 Select **Configure Service Desk**.

4 Click **Configure Actions**.

5 Click **Configure**.

6 Select the actions that are not needed and remove them.

7 Click **Save**.

Assign Roles

After configuring actions, you must assign roles. To assign roles, complete the following:

1 Go to the **Assign roles to User Groups** or **Assign roles to User** tab and select **Configure**.

2 Select the User or User Group.

3 Go to the **Role** tab and select **Edit** to add the required roles.

4 Select **Save**.

The Workspace ONE ITSM Connector application has preconfigured roles.

The WS1UEMStandard and WS1UEMAdvanced roles control what actions are available to the ServiceNow ITSM agents. With the WS1UEMConsoleViewer role, you can access the Workspace ONE UEM console from the Incident form if you need further investigation or actions.

There are also enhanced roles which add flexibility. With enhanced roles, individual actions can be assigned to users and groups. While the WS1UEMStandard and the WS1UEMAdvanced roles provide the default set of actions, each action has its own associated role that can be managed individually.

The following are the available actions and roles:

Action	Role
WS1UEMStandard	x_vmw_ws1uem.ws1uemstandard
WS1UEMAdvanced	x_vmw_ws1uem.ws1uemadvanced
WS1UEMConsoleViewer	x_vmw_ws1uem.ws1consoleviewer
Change Passcode	x_vmw_ws1uem.ws1uemchangepasscode
Lock Device	x_vmw_ws1uem.ws1uemlockdevice
Remote Assist	x_vmw_ws1uem.ws1uemremoteassist
Request Device Log	x_vmw_ws1uem.ws1uemdevicelogs
Send Message	x_vmw_ws1uem.ws1uemsendmessage
Soft Reset	x_vmw_ws1uem.ws1uemsoftreset
Sync Device	x_vmw_ws1uem.ws1uemsyncdevice
Find Device	x_vmw_ws1uem.ws1uemfinddevice
View Encryption Recovery Key	x_vmw_ws1uem.ws1uemviewencryptionkeys
Add Device	x_vmw_ws1uem.ws1uemadddevice
Device Wipe	x_vmw_ws1uem.ws1uemdevicewipe
Enterprise Wipe	x_vmw_ws1uem.ws1uementerprisewipe

Action	Role
Application Install	x_vmw_ws1uem.ws1uemapplicationinstall
Profile Install	x_vmw_ws1uem.ws1uemprofileinstall

The following represents actions that are available for WS1UEMStandard and WS1UEMAdvanced.

Action	WS1UEMStandard	WS1UEMAdvanced
Change Passcode	Yes	Yes
Lock Device	Yes	Yes
Remote Assist	Yes	Yes
Request Device Log	Yes	Yes
Send Message	Yes	Yes
Soft Reset	Yes	Yes
Sync Device	Yes	Yes
Find Device	Yes	Yes
View Encryption Recovery Key	Yes	Yes
Add Device	Yes	Yes
Device Wipe	No	Yes
Enterprise Wipe	No	Yes
Application Install	Yes	Yes
Profile Install	Yes	Yes

For descriptions of each action, see Device Actions.

Access-based New User Roles

Access-based roles for a new user in Workspace ONE UEM. For a new Workspace ONE UEM user, give the user the following permissions for a proper connection between the ITSM connector and Workspace ONE:

Category	Edit	Read
API > REST > Devices > REST API MDM Devices	Yes	No
API > REST >Devices > REST API Devices Write	Yes	No
API > REST >Devices > REST API Devices Execute	Yes	No

Category	Edit	Read
API > REST >Devices > REST API Devices Advanced	Yes	No
API > REST >Devices > REST API Devices Read	No	Yes
Assist	Yes	No
Device Management > Device Details > Messaging > Device Send Message	Yes	No
Device Management > Device Details > Messaging > Device Send Message	Yes	No
Device Management > Device Details > Messaging > Device Send Message Push Notification	Yes	No
Device Management > Device Details > Lock > Remote Device Lock	Yes	No
Device Management > Device Details > Enterprise Wipe > Device Remote mdm	Yes	No
Device Management > Device Details > Enterprise Wipe > Enterprise Reset	Yes	No
Device Management > Device Details > Device Wipe > Device Wipe	Yes	No
Device Management > Device Details > Passcode	Yes	No
Device Management > Device Details > Request Check-in	Yes	No
Device Management > Device Details > Remote Control	Yes	No
Device Management > Device Details > Remote View - Device Details	Yes	No
API > REST > Users > REST API Users Read	No	Yes

Configure Self-Service Catalog

The Self-Service Catalog gives employees the ability to resolve issues and perform common actions.

To use self-service actions, complete the following VMware Workspace ONE tasks.

Configure Catalog Category

All the self-service actions are available and active in the VMware Workspace ONE category.

Note Adding the VMware Workspace ONE category is not necessary to use self-service actions. You can add self-service actions to other categories on the home page. If you want to add self-service actions to another category, then skip this section and go to the Configure Catalog Items section.

To add the VMware Workspace ONE category:

1 Click **Configure**.

2 On the Service Catalog home page, click **+**.

3 Select the VMware Workspace ONE category.

4 Click **Add Here**.

Configure Catalog Items

To configure self-service actions and assign the actions to categories, complete the following:

1 Click **Configure**.

2 Select **Active**.

3 On the Accessibility tab, search for and select the Category.

4 Click **Update**.

Assign Roles

After configuring Catalog Items, you must assign roles. Assign VMware Workspace ONE ITSM Connector self-service roles to Groups and Users. To assign roles, complete the following:

1 Go to the Assign Roles tab, the User Groups tab, or the Assign Roles to User tab and select **Configure**.

2 Select the User or the User Group.

3 On the Role tab, click **Edit** to add the required roles.

4 Click **Save**.

The following are the available self-service actions and roles:

Action	Role
All Actions	** x_vmw_ws1uem.WS1CatalogAdvanced
Add Device	x_vmw_ws1uem.ws1catalogadddevice
Change Passcode	x_vmw_ws1uem.ws1catalogchangedevicepasscode
Find Device	x_vmw_ws1uem.ws1catalogfinddevice
Lock Device	x_vmw_ws1uem.ws1cataloglockdevice

Action	Role
Sync Device	x_vmw_ws1uem.ws1catalogsyncdevice
View Encryption Recovery Key	x_vmw_ws1uem.ws1catalogviewencryptionkey

Configure the Application Defaults

Configure the following Workspace ONE UEM default settings:

- Workspace ONE UEM Note - For more audit capabilities, configure this setting to add a note to a device in Workspace ONE UEM after every successful action is performed. This note details the time, action, and the ServiceNow user that performed the action.
- Workspace ONE UEM Email Validation Check - For all Workspace ONE UEM actions triggered within an incident, the ITSM Connector validates that the email address of the caller is the same as the email address retrieved from the device in Workspace ONE UEM.
- Exception List for Email Validation - An exception list of the email addresses where the email validation check is not carried out. Individual emails can be added, or a semicolon separated list can be used for multiple entries.

Using the Workspace ONE ITSM Connector for ServiceNow

The VMware Workspace ONE ITSM Connector for ServiceNow provides the ability to perform Workspace ONE UEM and Assist actions from within ServiceNow. This topic covers using the ITSM Connector for ServiceNow.

Workspace ONE UEM Actions for Service Desk Adminstrators

The Workspace ONE UEM tab displays on the Incident page when the WS1UEMStandard or the WS1UEMAdvanced role is assigned to the administrator. The Workspace ONE UEM tab provides administrators with device action selections, a device details overview, agent details, and additional details such as profiles, applications, and certificates.

The Workspace ONE UEM Action drop-down menu displays on the Workspace ONE UEM tab for the support administrator. The support administrator can perform an action from the drop-down menu on the configuration item (CI) or device assigned to the incident. To perform Workspace ONE UEM actions on the device, enroll the configuration item or device assigned within Workspace ONE UEM.

Note Actions are only successful if the attached device corresponds to a device in Workspace ONE UEM. This match is verified by serial number, along with an email address validation of the caller against the assigned user in Workspace ONE UEM.

The Workspace ONE Action tab and actions are enabled if the Incident status is In Progress, and a caller and a configuration item are assigned to the incident. The Action tab and actions are disabled for other Incident statuses.

The Notes tab in ServiceNow Incidents records all successful actions performed on the device when audit capability is configured during the guided setup. The note details the time, action, and the ServiceNow user that performed the action.

A Workspace ONE UEM Console button appears on the Incidents page if the Workspace ONE ConsoleViewer role is configured. When the support administrator opens the console, they can navigate to advanced troubleshooting. If the configuration item is not associated with the Incident, or the Device is not available within ServiceNow, then the support administrator can use the Workspace ONE UEM button to log in to the Workspace ONE UEM console and perform further troubleshooting.

For an action to be successful, the serial number of the configuration item in ServiceNow must match the device serial number of the device in Workspace ONE UEM.

Available Actions for Service Desk Administrators

The following Workspace ONE UEM device actions are available in the ServiceNow Incidents portal for Service Desk Administrators. Some actions might be platform specific. The actions are available for those device platforms only.

- Add Device - Add or enroll a device in the Workspace ONE UEM console.
- Application Management - View details of all assigned and installed profiles and install managed applications on the CI.
- Certificate Management - Displays all assigned certificates on the CI and their expiration dates.
- Find Device - Send a message to the applicable Workspace ONE UEM application together with an audible sound designed to help the user locate a misplaced device.
- Change Passcode - Replace any existing device passcode used to access the selected device with a new passcode.
- Device Wipe - Send a command to clear the device of all data and the operating system.

  Note This action returns the device to factory default settings. You cannot undo this action.

- Enterprise Wipe - Send a command to remove all managed enterprise resources including applications and profiles.

  Note This action removes all corporate data from the device. You cannot undo this action.

- Lock Device - Send a command to lock the selected device. The devices cannot be used until it is unlocked.
- Profile Management - View details of all assigned and installed profiles and install new profiles on the CI.
- Remote Assist - Remotely connect to enrolled device to view and control its screen, manage files, and run commands in real-time.

- Request Logs - Request for the selected device to send its logs to the Workspace ONE UEM console.
- Send Message - Workspace ONE UEM console the user of the selected device.
- Soft Reset - Restart a device remotely, reproducing the effect of powering it off and on again.
- Sync Device - Sync the selected device to the Workspace ONE UEM console.
- View Encryption Recovery Key - Send a message to receive the encryption recovery key.

For more information, see Device Actions.

Workspace ONE UEM Actions for Employees

Employees are able to resolve frequently occurring issues on their devices using the Service Catalog. Perform self-service actions in the VMware Workspace ONE category or any other category in the Service Catalog based on the employee's configuration.

Available Actions for Employees

The following Workspace ONE UEM device actions are on the VMware Workspace ONE tab in Self-Service.

- Add Device - Send an email to the user with information for how to enroll their device.
- Change Device Passcode - Replace any existing device passcode used to access the selected device with a new passcode.
- Find Device - Send a text message to the device along with an alert tone to help the user locate the missing device.
- Lock Device - Lock the selected device. The device cannot be used until it is unlocked.
- Sync Device - Sync the selected device to the Workspace ONE UEM console, aligning its Last Seen status.
- View Encryption Recovery Key - Send a message to receive the encryption recovery key.