Tools

SSH Terminal

Use the SSH Terminal screen to establish an SSH session to a router. From an SSH session, you can issue CLI commands on a router.

Establish an SSH Session to a Device

To establish an SSH session to a device:

1. In vManage, open **Tools** > **SSH Terminal**.

2. From the left pane, select the device on which to collect statistics:

   a. Select the device group to which the device belongs.

   b. If needed, sort the device list by its status, hostname, system IP, site ID, or device type.

   c. Click on the device to select it.

3. Enter the username and password to log in to the device.

You can now issue CLI commands to monitor or configure the device.

Rediscover Network

Use the Rediscover Network screen to locate new devices in the overlay network and synchronize them with the vManage NMS.

Screen Elements

- Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.

- Title bar—Includes the title of the screen, Rediscover Network.

- Rows Selected—Displays the number of rows selected from the table.

  - Rediscover button—Click to rediscover the devices in the network.

- Device Groups drop-down—Lists all configured device groups in the network.

- Search box—Includes the Search Options drop-down, for a Contains or Match string.

- Refresh icon—Click to refresh data in the device table with the most current data.

- Show Table Fields icon—Click to display or hide columns from the device table. By default, all columns are displayed.

- Table of devices in the overlay network—To re-arrange the columns, drag the column title to the desired position.

Rediscover the Network

To locate new devices in the overlay network, click the **Rediscover** button located directly beneath the title bar. Cisco vManage rediscovers every device and link and displays updated information about the network.

Synchronize Device Data

To synchronize the data on a specific device with the vManage NMS:

1. From the **Device Groups** drop-down list, select the device group to which the device belongs. The device table lists all the devices in the selected group.

2. Select the device.

3. Click **Rediscover** to confirm re-synchronization of the device data.

4. In the **Rediscover Network** window, click **Rediscover** to confirm re-synchronization of the device data.

Admin Tech: Collect System Information

Table 1: Feature History

Feature Name	Release Information	Description
Admin-tech Enhancements	Cisco IOS XE Release Amsterdam 17.2.1r Cisco SD-WAN Release 20.1.1	This feature enhances the **admin tech** file to include **show tech-support memory**, **show policy-firewall stats platform** and **show sdwan confd-log netconf-trace** commands in the admin-tech logs. The admin-tech tar file includes memory, platform, and operation details.

Use the Admin Tech to collect system status information for a device in a tar file to aid in troubleshooting and diagnostics.

1. From the device table, select the device.

2. Next, go to **More Actions** > **Admin Tech**.

3. In the **Generate admin-tech File** window, limit the contents of the Admin Tech tar file if desired:

   a. The **Include Logs** checkbox is selected by default. Deselect this checkbox to omit any log files from the compressed tar file. Log files are stored in the /var/log/directory on the local device.

   b. Select the **Include Cores** checkbox to include any core files. Core files are stored in the /var/crash directory on the local device.

   c. Select the **Include Tech** checkbox to include any files related to device processes (daemons), memory details and operations. These files are stored in the /var/tech directory on the local device.

4. Click **Generate**. A tar file is created which contains the contents of various files on the local device. This file has a name similar to `20150709-032523-admin-tech.tar.gz,` where the numeric fields are the date and time.

5. Send the `admin-tech.tar.gz` file to your Cisco SD-WAN customer support contact.

For more information on Admin Tech and tech-support commands, see request admin-tech and show tech-support.

Interface Reset Command

Use the Interface Reset command to shutdown and then restart an interface on a device in a single operation without having to modify the device's configuration.

1. From the device table, select the device.

2. Next, go to **More Actions** > **Interface Reset**.

3. In the **Interface Reset** window, select the desired interface.

4. Click **Reset**.

Template Migration

Migrate Shared Templates to Cisco IOS XE SD-WAN Templates

Overview

In Cisco IOS XE Release Amsterdam 17.2.1r with Cisco vManage 20.1.1, Cisco vManage adds support for new feature templates exclusively for Cisco IOS XE SD-WAN devices. In previous releases, when you created a template for both Cisco vEdge and Cisco IOS XE SD-WAN devices, the same template was shared for both device types. For these templates, the configuration was specified using Cisco vEdge commands and converted, if required, for Cisco IOS XE devices. Due to this, some functionality was unavailable on Cisco IOS XE SD-WAN devices.

In previous releases, there are two types of shared templates:

- Shared feature templates: If you specify a Cisco IOS XE SD-WAN device when creating a feature template, a shared feature template is created.

- Shared device templates: A device template that contains a shared feature template.

In Cisco IOS XE Release Amsterdam 17.2.1r and onwards, the feature templates have been separated for Cisco vEdge devices and Cisco IOS XE SD-WAN devices. These new feature templates exclusively for Cisco IOS XE SD-WAN devices enable support for additional features. To use these improved feature templates, Cisco vManage can migrate your older, shared feature templates to the new templates.

List of Migrated Templates

The following table lists the existing shared templates that were previously used for Cisco vEdge device and Cisco IOS XE SD-WAN device and their new corresponding templates for Cisco IOS XE SD-WAN devices available in Cisco vManage 20.1.1.

Note The AAA feature template is not supported with the new Cisco IOS XE SD-WAN device feature templates.

If your existing template contains an AAA feature template, you can replace it as follows:

- Before migration: Replace it with the AAA-Cisco template that was introduced in 19.1.

- After migration: After the migration is complete, manually create a Cisco AAA template and attach it to your device template.

Shared Feature Template	Shared Template Type	New Cisco IOS XE SD-WAN Device Feature Template	New Cisco IOS XE SD-WAN Device Feature Template Type
Banner	banner	Cisco Banner	cisco_banner
BFD	bfd-vedge	Cisco BFD	cisco_bfd
BGP	bgp	Cisco BGP	cisco_bgp

Shared Feature Template	Shared Template Type	New Cisco IOS XE SD-WAN Device Feature Template	New Cisco IOS XE SD-WAN Device Feature Template Type
DHCP Server	dhcp-server	Cisco DHCP Server	cisco_dhcp_server
Logging	logging	Cisco Logging	cisco_logging
NTP	ntp	Cisco NTP	cisco_ntp
OMP	omp-vedge	Cisco OMP	cisco_omp
OSPF	ospf	Cisco OSPF	cisco_ospf
Security	security-vedge	Cisco Security	cisco_security
SNMP	snmp	Cisco SNMP	cisco_snmp
System	system-vedge	Cisco System	cisco_system
VPN Interface GRE	vpn-vedge-interface-gre	Cisco VPN Interface GRE	cisco_vpn_interface_gre
VPN Interface IPsec	vpn-vedge-interface-ipsec	Cisco VPN Interface IPsec	cisco_vpn_interface_ipsec
VPN Interface Ethernet	vpn-vedge-interface	Cisco VPN Interface Ethernet	cisco_vpn_interface
VPN	vpn-vedge	Cisco VPN	cisco_vpn

Migrate Shared Templates

You can continue using the older shared templates, however the shared templates may not have access to the latest features. We recommend migrating existing templates to enable access to the latest features. For example, if you were using the VPN interface ethernet shared template, the template will continue to work. However, unless you migrate to the new feature templates, you will not be able to access newer features such as NAT DIA as this feature is only available in the new template.

You can migrate shared templates in one of the following ways:

- Using the migration script.

- Using the Cisco vManage Migration Tool (beta).

Migrate Shared Templates Using the Migration Script

Prerequisites

- Ensure that you have upgraded to Cisco vManage 20.1.1.

- MacOS running 10.15.3 or higher.

- Python 2.7. You can verify your installation of Python by running the following in Terminal:

```
python -c "import sys;assert sys.version_info>(2,7)" && echo "Python 2.7 is installed"
```

If `Python 2.7 is installed`" is not displayed, you must download and install the latest 2.x version of Python from https://www.python.org/downloads/.

- Ensure that the following Python packages are installed: os, json, argparse, requests, pathlibs, subprocess, sys, datetime, and random.

  Note that some of these packages are pre-installed with Python.

Set Up the Script

1. Navigate to the Cisco vManage 20.1.1 downloads page.

2. Download the `vManage Offline Template Migration Tool` to your machine.

3. Unzip the `vmanage_template_migration.zip` to a directory such as `/home/admin`. This creates a directory called `/home/admin/migration`.

4. Navigate to the directory

   ```
   cd /home/admin/migration
   ```

Run the Script

The script has the following syntax:

```
python templatemigrations.py -ip vmanage_IP -port vmanage_PORT -fv from_vmanage_VERSION -tv to_vmanage_VERSION [-prefix template_name_PREFIX]
```

You can specify the following parameters:

Argument	Description
ip	The IP address of Cisco vManage
port	The TCP port to access Cisco vManage. This is typically 9912 or 8443.
fv	From Version. The version of Cisco vManage before you upgraded.
tv	To Version. The version of Cisco vManage that you are currently running
prefix	(Optional) The name that is prefixed to the name of all migrated templates. By default, the prefix is `cisco_`

Example

```
python templatemigrations.py -ip 10.34.52.12 -port 9912 -fv 19.2 -tv 20.1 -prefix updated_
```

In this example, Cisco vManage is accessible from the URL https://10.34.52.12:9912. Cisco vManage was also upgraded from 19.2 to 20.1. Finally, the name of all migrated templates are prefixed with `updated_`. For example, if your old BGP template was called `Common_BGP_Template`, after migration, the template will be called `updated_Common_BGP_Template`

After you execute the script, it does the following:

1. Prompts you for your username and password.

2. Verifies that the versions of Cisco vManage are supported.

3. Verifies if the following are in the correct directories: session.py, migration.py, Input/supported_cedge_templates.json, and Input/JSONInputs.json.

4. Checks for authorization and authenticates.

5. Verifies if the device and/or feature template names are supported by the template naming convention. This also checks if the prefix will conflict with other template names in Cisco vmanage and if the names meet the template naming requirements – such as the maximum of 128 characters, unsupported symbols, and so on.

6. Acquires the device templates and associated feature templates. The feature templates and device templates are saved to the `Data/feature` and `Data/master` directories respectively.

7. Identifies the feature templates that must be migrated.

8. Migrates the identified feature templates using the `migration.py` script.

9. Saves the migrated templates in the directory specified by the user. The new device templates are created with the prefix appended. The new device template will also have the new feature templates associated with them.

10. Uploads all migrated device templates and feature templates to Cisco vManage. After upload, you must manually attach the devices to the migrated templates.

Migrate Shared Templates Using the Cisco vManage Migration Tool (Beta)

To migrate an existing, shared template to use the new feature templates, using Cisco vManage, do the following:

1. Navigate to **Tools** > **Template Migration (Beta)**

2. Click **Migrate All Templates**.

3. Enter a prefix for the new migrated templates. For example `Migrated_`. All migrated templates will be prefixed with this identifier.

4. Click **OK** to migrate the templates.

5. Once the migration begins, you can track the status of the migration by clicking the **Tasks** button in the top-right side of the interface.

6. Once the migration is complete, you must manually attach the migrated templates to your devices as follows:

   a. For each of the migrated templates, click the **More Actions** button on the right-side of the templates table.

   b. Click **Attach Devices to Migrated Template**.