



Downgrading Orchestrator Deployments in VMware ESX

This chapter contains the following sections:

- [Downgrading Guidelines and Limitations, on page 1](#)
- [Downgrading Multi-Site Orchestrator, on page 2](#)

Downgrading Guidelines and Limitations



Note This chapter describes how to downgrade Multi-Site Orchestrator that was deployed without using Cisco Application Service Engine. If you deployed the Orchestrator inside Application Service Engine, follow the downgrade instructions described in [Upgrading or Downgrading Orchestrator Deployments in Application Service Engine](#) instead.

The following list describes the guidelines and limitations for downgrading the Cisco ACI Multi-Site Orchestrator:

- If you plan to downgrade the Cisco APIC as well, you must downgrade Cisco ACI Multi-Site Orchestrator first.
- This release of Cisco ACI Multi-Site Orchestrator, can be downgraded to any Release 1.2(1) or later. If you plan to downgrade to an earlier release, you must first downgrade to a 1.2(x) release, then follow the instructions described in [Downgrading Cisco ACI Multi-Site, Release 1.2\(x\)](#) to downgrade further.
- When downgrading to a release prior to Release 2.1(1), you must remove any Cisco Cloud APIC sites you may have added to your Cisco ACI Multi-Site Orchestrator. Failing to remove the cloud sites will cause the downgrade to terminate.
- If you have configured any read-only user roles and are downgrading to a release prior to Release 2.1(2), the read-only roles will be removed from all users. This means that any user that has **only** read-only roles will have no roles assigned to them and a Power User or User Manager will need to re-assign them new read-write roles.

In addition, if you used an external authentication server to configure the read-only user roles, you must reconfigure the authentication servers and remove those read-only user roles. The read-only user roles

use a different format attribute-value (AV) string to specify read-write and read-only permissions and failing to update the configuration will cause those users to not authenticate correctly.

Additional details about external authentication servers configuration steps are described in the *Cisco ACI Multi-Site Configuration Guide*, but in short, you must update any user configuration strings from:

```
cisco-av-pair=shell:misc-roles=writeRole1|writeRole2/readRole1|readRole2
```

to:

```
cisco-av-pair=shell:misc-roles=role1,role2
```

- If you are downgrading to a release prior to Release 2.1(2), ensure that all users have the `Phone Number` field filled out. The field was required in earlier releases and any user created in Release 2.1(2) or later without a phone number provided will be unable to log into the GUI if the Orchestrator is downgraded to Release 2.1(1) or earlier. A Power User or User Manager can also update the field for any user after the downgrade.
- If you are downgrading to a release prior to Release 2.1(1), you will need to update all passwords stored by the Orchestrator, such as the passwords for all sites and authentication providers.
- Before you downgrade the Cisco ACI Multi-Site Orchestrator, remove the configuration of all features that are not supported in the release to which you are downgrading.

Downgrading Multi-Site Orchestrator

This section describes how to downgrade the Cisco ACI Multi-Site Orchestrator.

Before you begin

You must complete all the prerequisites detailed in [Downgrading Guidelines and Limitations, on page 1](#).



Note When downgrading to a release prior to Release 2.1(1), you must remove any Cisco Cloud APIC sites you may have added to your Cisco ACI Multi-Site Orchestrator. Failing to remove the cloud sites will cause the downgrade to terminate.

Step 1 Download the Cisco ACI Multi-Site Orchestrator downgrade (target) image.

- Go to the Software Download link:
<https://software.cisco.com/download/home/285968390/type>
- Click **ACI Multi-Site Software**.
- Choose the Cisco ACI Multi-Site Orchestrator release version.
- Download the *ACI Multi-Site Upgrade Image* file (`misc-<version>.tar.gz`) for the release.

Step 2 Copy the downgrade image to each node.

Copy the `misc-<version>.tar.gz` file you downloaded to the `/opt/cisco/misc/builds/` directory on each node. You can use SCP or SFTP to transfer the file.

Example:

SFTP:

```
# sftp root@<node-ip>sftp> cd /opt/cisco/msc/builds/sftp> put msc-<version>.tar.gzsftp> quit
```

Example:

SCP:

```
# scp ./msc-<version>.tar.gz root@<node-ip>:/opt/cisco/msc/builds/
```

Step 3 On each node, extract the file.

Example:

```
# cd /opt/cisco/msc/builds/# tar -xvzf msc-<version>.tar.gz
```

Step 4 On node2 and node3, load the downgrade image.

On node2 and node3 only, run the following commands, replacing:

- *<current-version>* with the currently installed Cisco ACI Multi-Site Orchestrator release, for example *msc_2.2.1c*
- *<downgrade-version>* with the target downgrade version you downloaded and extracted in previous steps, for example *msc_1.2.1h*

Example:

```
# cd /opt/cisco/msc/builds/<current-version>/downgrade/# ./downgrade.sh <downgrade-version>
```

Step 5 From node1, downgrade Cisco ACI Multi-Site Orchestrator cluster.

On node1 only, run the following commands, replacing:

- *<current-version>* with the currently installed Cisco ACI Multi-Site Orchestrator release
- *<node2-ip>* with the IP address of node2
- *<node2-password>* with the root user password for node2
- *<node3-ip>* with the IP address of node3
- *<node3-password>* with the root user password for node3
- *<downgrade-version>* with the version you are downgrading to

Note If you leave the IP and password arguments out, the script will prompt you to enter them.

Example:

```
# cd /opt/cisco/msc/builds/<current-version>/downgrade/# ./downgrade.sh -1 <node2-ip> -2
<node2-password> -3 <node3-ip> -4 <node3-password> <downgrade-version>
```

It may take several minutes for the downgrade to complete. After the downgrade is complete, you can verify that it was successful and the Cisco ACI Multi-Site Orchestrator cluster is ready for use by accessing the Orchestrator GUI.

Step 6 If necessary, update stored passwords.

Starting with Release 2.1(1), Multi-Site Orchestrator encrypts all stored passwords, such as each site's APIC passwords and the external authentication provider passwords. As a result, when downgrading to a release prior to Release 2.1(1), you must re-enter all the password after the Orchestrator downgrade is completed.

To update APIC passwords:

- a) Log in to the Orchestrator after the downgrade.
- b) From the main navigation menu, select **Sites**.

- c) For each site, edit its properties and re-enter its APIC password.

To update external authentication passwords

- a) Login into the Orchestrator after the downgrade.
 - b) From the navigation menu, select **Admin > Providers**.
 - c) For each authentication provider, edit its properties and re-enter its password.
-