# NetBackup™ Access Appliance 8.5 Upgrade Guide

October 2025

VERITAS
now part of Cohesity

# Access Appliance 8.5 Upgrade Guide

Last updated: 2025-10-29

## Legal Notice



Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

http://www.veritas.com

## Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

https://www.veritas.com/support

You can manage your Veritas account information at the following URL:

https://my.veritas.com

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

| | |
|---|---|
| Worldwide (except Japan) | CustomerCare@veritas.com |
| Japan | CustomerCare_Japan@veritas.com |

## Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Veritas website.

## Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Veritas website.

## Veritas Services and Operations Readiness Tools (SORT)

Veritas Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

# Contents

Chapter 1

# Introduction

This chapter includes the following topics:



## About the Access Appliance upgrade

Access Appliance supports the following upgrade methods:

- Rolling upgrade and Parallel upgrade
  Use this method if the Access Appliance is configured and the appliance nodes are part of the Access cluster.
- Node-by-node upgrade
  Use this method if the appliance nodes are in factory state.

---

**Note:** The appliance nodes that are in **Not in Access cluster** state cannot be upgraded. You can reset a node to the default factory settings, and then upgrade the node.

---

**Table 1-1** Upgrade methods

| Upgrade method | Description |
|---|---|
| Rolling upgrade | During a rolling upgrade, each node in the Access cluster is upgraded successively without stopping the Access cluster. Rolling upgrade minimizes the service downtime.<br><br>Download the required upgrade package to one of the nodes in the cluster and upgrade the node where the upgrade package is downloaded. The upgrade process copies and installs the upgrade package to other nodes in the cluster. During the upgrade, services switch between the nodes to keep the Access Appliance online. The services are down only when the services switch between the nodes.<br><br>If upgrade fails on one of the nodes, the update is automatically rolled back on all the nodes in the cluster and the nodes are restored to their earlier version.<br><br>**Note:** Rolling upgrade is not supported for a single-node configuration. |
| Parallel upgrade | During a parallel upgrade, both nodes in the cluster are upgraded and restarted simultaneously. The cluster services are down while the nodes are restarting.<br><br>Download the required upgrade package to one of the nodes in the cluster and upgrade the node where the upgrade package is downloaded. The upgrade process copies and installs the upgrade package to other nodes in the cluster. The services are down when the nodes are restarted.<br><br>If upgrade fails on one of the nodes, the update is automatically rolled back on all the nodes in the cluster and the nodes are restored to their earlier version. |
| Node-by-node upgrade | **Warning:** Ensure that all the nodes are in factory state before you use this upgrade method.<br><br>Download the required upgrade package to each node, and then upgrade each node separately by installing the update on each of the nodes.<br><br>If the upgrade fails, the update is rolled back and the node is restored to its earlier version. |

# About the supported software versions

Table 1-2 shows the Access software versions for the recent Access Appliance releases.

**Table 1-2** Access Appliance releases and the corresponding Access software versions

| Appliance release | Access software version |
|---|---|
| 7.4.2 | 7.4.2 |

**Table 1-2** Access Appliance releases and the corresponding Access software versions *(continued)*

| Appliance release | Access software version |
|---|---|
| 7.4.3 | 8.2.0 |
| 8.0 | 8.4.0 |
| 8.1 | 8.5.0 |
| 8.2 | 8.7.0 |
| 8.3 | 8.10.0 |
| 8.4 | 8.12.0 |
| 8.5 | 8.13.0 |

# Supported upgrade paths

Access Appliance supports direct upgrade to version 8.5 from the following versions:

- 8.3.x
- 8.4

# Supported upgrade paths if continuous replication is configured

The following describes the supported upgrade paths to Access version 8.5 if continuous replication is configured on the cluster.

- Direct upgrade path
  You can upgrade directly from version 8.3.x and 8.4 to version 8.5.
- Multi-step upgrade path
  If the appliance is on an earlier version than 8.3, you must first upgrade to 8.3.x or 8.4 before you can upgrade to version 8.5.

# About the preupgrade check

The preupgrade check determines if the system is ready for an upgrade. The preupgrade check runs automatically when you start the upgrade. The preupgrade check performs tests, which identify any potential problems that might result in an upgrade failure. You must resolve the issues before you upgrade the cluster.

The following tests are performed during the preupgrade check:

- System self-test to verify the health of system and software services, such as network and system configuration.
- Certificate check to ensure that the self-signed certificate is configured correctly.
- Ensure that no previous incomplete upgrade process is ongoing.
- MongoDB check to ensure that MongoDB works as expected.
- Version check to ensure that the upgrade path is supported and the current system can be upgraded to the target version.
- The Docker daemon is configured correctly.
- Sufficient free space is available for the upgrade.
  To free up space, the `/opt/VRTSnas/core/kernel`, `/opt/VRTSnas/core/use`, and `/opt/VRTSnas/log` files are automatically compressed to `old-*.tar` files, and these tar files are archived to the `/log/VRTSnas/log` directory . The original log files are deleted to free up space.
- No other bootable devices are present that may interfere when restarting the nodes during the upgrade.
- The administrator password does not expire within seven days.
- All the cluster nodes are up and healthy with the same software version installed on all the nodes.
- CIFS server is not configured as a standalone server.
- Version check to ensure that the version of Veritas Data Deduplication is supported.

## Running the preupgrade check

Starting with version 8.0, you can run a preupgrade check independently after you download the software release update package from the Veritas website or when you upload the software release update package from a local system.

With an independent preupgrade check, you can verify if the appliance is ready for an upgrade without starting the upgrade operation.

---

**Note:** The preupgrade check runs automatically when you upgrade the appliance. Running an independent preupgrade check is optional.

---

**To run a preupgrade check independently on a software release update package:**

1. Open an SSH session and use the admin credentials to log in the appliance.

   The Veritas Appliance Shell menu is displayed.

2. Check if any upgrade packages are available on SORT server.

   ```
   system software available-patch
   ```

3. Download the software release update package:

   ```
   system software download-update update-name=update_name
   ```

4. Verify if any software release update package is downloaded:

   ```
   system software downloaded
   ```

5. Run the preupgrade check:

   ```
   start appliance preupgrade-check patch=update_name
   ```

   To check the status, run the `show appliance preupgrade-check status` command.

   ---

   **Note:** Wait for a few seconds before you check the status. If you check the status immediately after running the `preupgrade-check` command, the status of the preupgrade checks might not be available. If you check the status without running the `preupgrade-check` command, **Operation failed** error message is displayed.

   ---

For details about the commands, see the *Veritas Access Appliance Command Reference Guide*.

# Error messages displayed during the preupgrade check

The following table lists the error messages that you may come across during the preupgrade check, which runs automatically when you start the appliance upgrade:

**Table 1-3**

| Error message | Recommended action |
|---|---|
| Errors that are displayed during the system self-test. | The appliance runs a self-test to check the current status of the various appliance components. Review the checks for which the status is displayed as FAILED. Try to correct the issue and retry the operation. If the issue persists, use the `support data-collect` command to collect logs and contact Veritas Technical Support. |
| V-409-776-30019: The password for user *username* will expire in *number_of_days* days. | Change the password before upgrading the appliance.<br>Change the password using the `Admin> passwd username` command. |
| V-409-776-1111: One or more USB devices are attached to the appliance. | Remove all the attached USB mass storage devices from the appliance, and then try again. |
| V-409-776-30014: The docker daemon is not configured correctly. | Contact Veritas Technical Support and refer them to article 100051459. |
| V-409-776-30053: The password for user *username* is set to the default password. | For increased security, forced password changes are enforced to ensure that known default passwords do not exist on the system. Change the default password before upgrading the appliance.<br>Change the password using the `Admin> passwd username` command. |
| V-409-776-30054: The password for the IPMI user *username* is set to the default password. | For increased security, forced password changes are enforced to ensure that known default passwords do not exist on the system. Change the default password for the IPMI user before upgrading the appliance.<br>Change the password using the `Admin>ipmi passwd username oldpassword new_password` command. |
| V-409-776-30078: GRUB configuration file check failed. | The file `/boot/grub2/grub.cfg` was modified after system startup. Revert the changes by updating the parameters in the `grub.cfg` file as per the values that are set in `/proc/cmdline`. |

**Table 1-3** *(continued)*

| Error message | Recommended action |
|---|---|
| V-409-776-30026: One or more server certificate files are missing.<br>V-409-776-30027: The local client certificate file is not configured correctly.<br>V-409-776-30028: MongoDB is not configured with the correct certificate key file. | Contact Veritas Technical Support and refer them to article 100052338. |
| V-409-776-30029: The certificate is not valid. | Local or remote CA certificate fingerprint is not present in the Tomcat keystore. Contact Veritas Technical Support and refer them to article 100052338. |
| V-409-776-30048: A previous uncomplete upgrade process was detected. | There can be multiple reasons for this issue.<br>Collect the logs using the `support data-collect` command, and then contact Veritas Technical Support. |
| V-409-776-30025: Database service might be down for various reasons. | Collect the logs using the `support data-collect` command, and then contact Veritas Technical Support. |
| V-409-776-30052: Insufficient free space for the MongoDB database. Contact Veritas Support to delete analysisReport, componentHealthStatus, inventory, unknownEvents, and event databases and restart the MongoDB service. | Contact Veritas Technical Support to delete the analysisReport, componentHealthStatus, inventory, unknownEvents, and event databases and restart the MongoDB service. |
| V-409-776-1112: The appliance isn't 3340/3350. | The appliance model is not an Access appliance. The downloaded software release update is for an Access appliance model. |
| V-409-776-1105: The current appliance version is same as the software release update version. | View the software version running on the appliance using the `show appliance status` command. Download a newer software release update from the Veritas Download Center. |
| V-409-776-1106: This appliance has already been running with a version that is greater than the patch version. | View the software version running on the appliance using the `show appliance status` command. Download a newer software release update from the Veritas Download Center. |

**Table 1-3** *(continued)*

| Error message | Recommended action |
|---|---|
| V-409-776-1121: Version check failed. | Contact Veritas Technical Support. |
| V-409-776-1120: The space *size* is not enough. | Contact Veritas Technical Support to free up space by deleting unwanted files. |
| V-409-776-1013: Logic Volume /dev/system/config usage over 30G. | Delete unwanted files and retry the operation. |
| V-409-776-30033: Unable to resize *directoryname* during an upgrade. | The amount of space used by *directoryname* is greater than the allocated size *size*M. Free up space by deleting unwanted files from *directoryname*. |
| V-409-776-1117: The cluster is not in a valid state for upgrade. A cluster should contain at least two nodes. | Unable to retrieve the node list because of an internal error. Contact Veritas Technical Support. |
| V-409-776-1113: The cluster is not in a valid state for upgrade. One or more nodes are not in the cluster. | Both the nodes must be a part of the cluster with node status set to RUNNING. Contact Veritas Technical Support. |
| V-409-776-1114: The cluster is not in a valid state for upgrade. Appliance version is not consistent across the cluster. | The appliance version must be the same for both the nodes in the cluster. Contact Veritas Technical Support. |
| V-409-776-1115: The cluster is not in a valid state for upgrade. Access software version is not consistent across the cluster. Contact Veritas Technical Support to resolve this issue. | The Access software version must be the same for both the nodes. Contact Veritas Technical Support. |
| V-409-776-1118: Pre-upgrade network interface card (NIC) consistency check failed. There is a mismatch between the NICs installed on the cluster nodes. | The NICs on both the nodes must be of the same specifications. Contact Veritas Technical Support. |
| V-409-776-1116: The cluster is not in a valid state for upgrade. The shared Configuration partition is not properly mounted on the attached storage. | The shared configuration volume is not mounted correctly on the attached storage. Contact Veritas Technical Support. |

**Table 1-3** *(continued)*

| Error message | Recommended action |
|---|---|
| V-409-776-30114: The FIPS mode for MSDP is enabled but the FIPS configuration file is not present in the catalog file system of a WORM-enabled Veritas Data Deduplication instance. | Contact Veritas Technical Support and refer them to article 100055226. |
| V-409-776-1125: One or more disks under a volume are not in proper state. | One or more disks reported unhealthy status. Contact Veritas Technical Support. |
| V-409-776-30020: Appliance cannot be upgraded if Veritas Volume Replicator (VVR) is configured. | Contact Veritas Technical Support. |
| V-409-776-30034: Unable to start the appliance upgrade because volume recovery tasks are in progress. | Contact Veritas Technical Support. |
| V-409-776-30035: Unable to start the appliance upgrade because host-based NetBackup client is configured with Veritas Data Deduplication. | Contact Veritas Technical Support to unconfigure the host-based NetBackup client, perform an upgrade, and configure container-based NetBackup client. |
| V-409-776-30036: Unable to start the appliance upgrade because an erasure-coded volume is present in the cluster. | File systems with erasure-coded layout are deprecated in version 7.4.3 and are no longer supported. Contact Veritas Technical Support. |
| V-409-776-30038: Unable to start the appliance upgrade because an NFS-Ganesha (GNFS) server is set up for the cluster. | NFS server support for the NFS-Ganesha server (GNFS) is deprecated in version 7.4.3. Use the `NFS> server switch` command from the Access command-line interface to switch to a kernel-based NFS server. |
| V-409-776-30039: Unable to start the appliance upgrade because the appliance is not configured to use a Network Time Protocol (NTP) server or the NTP server is disabled. | At least one NTP server must be configured for the cluster. Unlike in earlier releases, configuring NTP is not optional.<br>To configure or enable the NTP server, use the `system ntp` command from the Access command-line interface. |
| V-409-776-30040: Unable to start the appliance upgrade because an FTP server is configured for the cluster. | Support for FTP is deprecated. Unconfigure the FTP server before upgrading the appliance. |

**Table 1-3** *(continued)*

| Error message | Recommended action |
|---|---|
| V-409-776-30041: Unable to start the appliance upgrade because deduplication is enabled for file systems. | Support for file system deduplication is deprecated in version 7.4.3. Disable file system deduplication before upgrading the appliance. |
| V-409-776-30044: One or more VxFS file systems are full. Unable to start the appliance upgrade because there is no free space on one or more VxFS file systems. | Contact Veritas Support and ask them to refer to article 100052630. |
| V-409-776-30079: Unable to start the appliance upgrade because replication jobs running. | Pause the replication jobs using these command-line interface commands: `Replication> continuous show` to get the list of file systems that are configured for continuous replication, `Replication> continuous status` *`fs_name`* to display the replication status, and `Replication> continuous pause` *`fs_name`* to pause any replication jobs that are running. |
| V-409-776-30086: Private network settings are not configured as expected. | Contact Veritas Support and refer them to article 100054849. |
| V-409-776-30087: Syntax validation failed for the Veritas Cluster Server (VCS) configuration file. | Contact Veritas Support and refer them to article 100054029. |
| V-409-776-30067: Failed to retrieve the node status because there was an issue with vxlogview unified log command. | Contact Veritas Technical support and refer them to article 100052760. |
| V-409-776-30089: A Veritas File Replication (VFR) job is ongoing. | Pause the job using the `Replication> episodic job pause` command. You can view the details about the job using the `Replication> episodic job show` and the `Replication> episodic job status` command. |
| V-409-776-1110: The service group check failed. | All the service groups are not online. Use the `support services autofix` command from the Access command-line interface to resolve this problem. |

**Table 1-3** *(continued)*

| Error message | Recommended action |
|---|---|
| V-409-776-30151: The CIFS service is configured in standalone mode with the security setting set to user. | The CIFS service is configured in standalone mode with the security setting set to user. The user security mode is not supported when the FIPS mode is enabled for the appliance. To resolve this issue, refer to article 100059081. |
| V-409-776-30174: One or more VDD instances are running on MSDP 16.0 or 17.1 version which is not supported or one of the VDD instances is host-based and in unconfigured state. | Upgrade all 16.0 and 17.1 containers to a higher version. If any of the VDD instances is host-based and in unconfigured state, reconfigure the VDD instance to container-based using the `dedupe reconfig` command. |
| V-409-776-30181 3005 UID is used by some other local user. | Find the username of 3005 UID using the `getent passwd 3005` command in support shell environment. Delete this user from GUI or Access Clish and then add back the user again. |
| V-409-776-30181: 3005 UID/GID is not free on the cluster. | ■ Go to the Support Shell environment. Find out the user who has occupied 3005 UID or GID or both.<br>■ To check which user has used 3005 UID:<br>**`getent passwd 3005`**<br>■ To check which user has used 3005 GID:<br>**`getent group 3005`**<br>■ If 3005 UID is occupied by a local user, and this user does not use CIFS, S3 or NFS, delete that user from GUI and add it back again.<br>After deleting the local user , if 3005 GID is still not free, contact Veritas Technical Support.<br>■ If 3005 UID is occupied by any other user contact Veritas Technical Support. |

**Table 1-3** *(continued)*

| Error message | Recommended action |
|---|---|
| V-409-776-30183: Unable to start the appliance upgrade operation because replication jobs are in running state | Stop the replication service and try again.<br>To stop the replication:<br>■ Run the `replication continuous service status` command to get the status for service.<br>■ Run the `replication continuous service stop` command to stop any replication service. |
| V-409-776-30185: Integrity validation failed for routing configuration file. | Contact Technical Support and ask them to refer to article 100075306. |

Chapter 2

# Upgrading Access Appliance

This chapter includes the following topics:



## Access Appliance upgrade overview

You can upgrade a two-node cluster or a one-node cluster configuration by using the Access Appliance UI or by using the node-level CLI. Refer to the following steps to upgrade Access Appliance:


See “Supported upgrade paths” on page 7.

See “Downloading the appliance software updates” on page 18.

See “Performing an upgrade pre-check” on page 24.

See “Completing pre-upgrade tasks” on page 26.

See “Performing an upgrade” on page 28.

See “Completing post-upgrade tasks” on page 32.

# Downloading the appliance software updates

You can download the software update from the Access Appliance UI or from the Access Appliance shell menu.

See "Downloading the software update using the UI" on page 18.

See "Downloading software updates using the Access Appliance shell menu" on page 19.

## Downloading the software update using the UI

You can download the software update from SORT or from the Download Center on the Veritas Support website. If you download the software update from the Veritas Support website, you must first download the software update to a Windows system that can access the Download Center and the cluster nodes and then upload the software update to one of the nodes.

See "Downloading a software update from the Veritas Support website" on page 19.

**To download the software update:**

1. Sign in to the Access Appliance UI using the following URL:

   `https://console-ip:14161`

   where *console-ip* is the management console IP address where the web interface is hosted.

2. Go to **Settings > Software management > Software update**.

3. To download the software update do one of the following:

   - If the appliance has access to SORT, click **Check online for update**.
     A notification is displayed on the top of the page. To monitor the progress, click **View details**. If a software update is available, it is downloaded and displayed under **Downloaded package files**; else no updates available on SORT is displayed when you click **View details** on the tasks page.
   - To upload a software update that was downloaded from the Veritas Support site, click **Upload**, browse to the location where the software update is downloaded, select the software update and click **Upload**.
     You can select only a single software update at a time.
     The progress of the upload operation is displayed on the page. After the upload is complete, the software update is displayed under **Downloaded package files**.

### Downloading a software update from the Veritas Support website

You can download the software update from the Veritas Support site. You require Veritas account credentials to download the file

**To download the required software update:**

1. Go to the Veritas Support website (https://www.veritas.com/support/en_US) and click **Downloads**, which redirects you to the Download Center.
2. In the Veritas Download Center, in the **Products** list, select **Appliances**, in the **Sub product** list select **Access Appliance OS**. Select the version as **8.5** and click **Explore**.
3. Expand **Base and upgrade installers**.

   Select the upgrade RPM upgrade package from this section and click **Download**. You must sign in with your Veritas account credentials to download the upgrade file.

## Downloading software updates using the Access Appliance shell menu

Appliance software updates can be downloaded by using the Access Appliance shell menu or manually through a share. Updates must be downloaded to the appliance before you start the upgrade.

### Downloading software updates directly to an Access Appliance node

Use this procedure to download a software release update to an appliance node. For a rolling upgrade or a parallel upgrade, download the package to one of the nodes in the cluster. For a node-by-node upgrade, you need to download the package to both the nodes.

For more details about the upgrade methods, See “About the Access Appliance upgrade” on page 5.

**To download software release updates directly to an appliance node, complete the following steps:**

1. If not already done so, open an SSH session and log on to the appliance as an administrator using the Access Appliance shell menu.
2. To determine if a software update is available from the Veritas Support website, enter the following command:

   ```
   system software available-patch
   ```

   The software release update that is available for installation is displayed. Note the name of the software release update package. For example, VRTSaccess-app-update-8.3-1.x86_64.rpm
3. To download the available software update, enter the following command:

   ```
   system software download-update update-name=update-name
   ```

   where update-name is the name of the software release update package. For example:`system software download-update update-name=VRTSaccess-app-update-8.3-1.x86_64.rpm`

   You can view the download progress by using the `system software download-progress` command.

   ```
   [access-8.2] node > system software download-progress

   The status of VRTSaccess-app-update-8.3-1.x86_64.rpm is
   downloading, and the progress is:

   [9%|ETA: 0:08:35]
   ```

4. To verify that the software update has downloaded successfully, enter the following command:

   ```
   system software downloaded
   ```

   The downloaded software update is validated and details such as the patch name, size, and version are displayed.

## Downloading software updates to an Access Appliance node using a client share

Use this procedure to download the software updates to an appliance node using an NFS share. You can download the software update from the Veritas Support website (https://www.veritas.com/support/en_US). You must sign in with your Veritas account credentials to download the release update.

**To download the software release update on an appliance node using an NFS client share, complete the following steps:**

1. If not already done so, open an SSH session and log on to the appliance as an administrator using the Access Appliance Shell Menu.
2. To open an NFS share, enter the following command:

   ```
   system software share open
   ```

3. Mount the appliance share directory as follows.

   For a Linux NFS share:

   ```
   mkdir -p /mount/Node_management_IP
   ```

   ```
   mount Node_management_IP:/inst/patch/appliance/available
   /mount/Node_management_IP
   ```

   where *Node_management_IP* is the IP address that is assigned to eth1 of each node.

4. Download the upgrade package and the SHA256 checksum.

   - Release update
     Download the release update by clicking Downloads on the Veritas Support website
   - SHA256 checksum
     Copy the text file that contains the SHA256 checksum. The checksum is displayed when you click the `VRTSaccess-app-update-8.3-1.x86_64.rpm` release update.

5. Run the following command to compute the checksum of the rpm file:

   ```
   sha256sum VRTSaccess-app-update-8.3-1.x86_64.rpm
   ```

   Verify that the SHA256 checksum matches the checksum that you downloaded from the Veritas Support website.

6. Copy this release update to the mounted share.

   **Note:** To avoid any issues, ensure that you do not run commands on the appliance nodes when you copy the update.

7. Unmount the shared directory after copying the update.

8 Close the NFS share by using the command:

```
system software share close
```

9 List the downloaded files by using the command:

```
system software downloaded
```

The downloaded update is validated and details such as the patch name, size, and version are displayed.

## Downloading software updates to an Access Appliance node using SCP

Use this procedure to copy the software updates to the `/inst/patch/appliance/available` directory on the Access Appliance from a Linux or a Windows system using the Secure copy protocol (SCP).

To copy a software update from a Windows system, you must install OpenSSH on Windows. For details about installing OpenSSH, See "Installing OpenSSH" on page 23.

**To download the software update:**

1 Download the software update from the Veritas Download Center to a Windows or a Linux system. Ensure that the system is in the same network as the Access Appliance.

- Go to the Veritas Support website and click **Downloads**.
- In the Veritas Download Center, in the **Products** list, select **Appliances**, in the **Sub product** list select **Access Appliance OS**. Select the version and click **Explore**.
- Expand **Base and installers**.

2 From the Access Appliance node-level CLI run the following commands:

```
support elevate
```

```
# cd /inst/patch/appliance/available
```

3 Copy the RPM file using the following command:

For Linux:

```
# scp username@linuxserver:/full-path-to-accessappliance-patch.rpm
```

where *username* is the admin user for the Linux server.

For Windows:

```
scp username@domain-or-ip-of-windows-machine:
full-path-to-accessappliance-patch-on-windows-machine
/inst/patch/appliance/available
```

where *username* is the admin user for the Windows server.

For example, if the RPM was downloaded to the Downloads directory on Windows by user administrator:

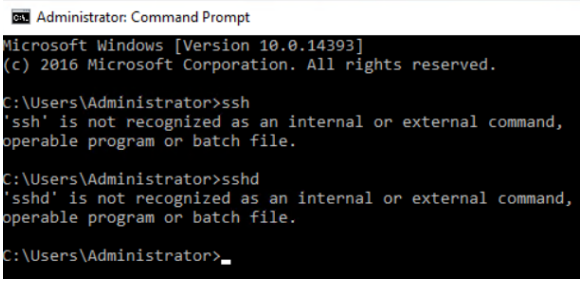
```
aa01:/inst/patch/appliance/available # scp
administrator@xx.yy.zz.aa:/Downloads/VRTSaccess-app-update-8.3-1.x86_64.rpm
 .
```

4 Log in to the Access Appliance node-level CLI and run the `system software downloaded` command to view details such as the patch name, size, and the version.

### Installing OpenSSH

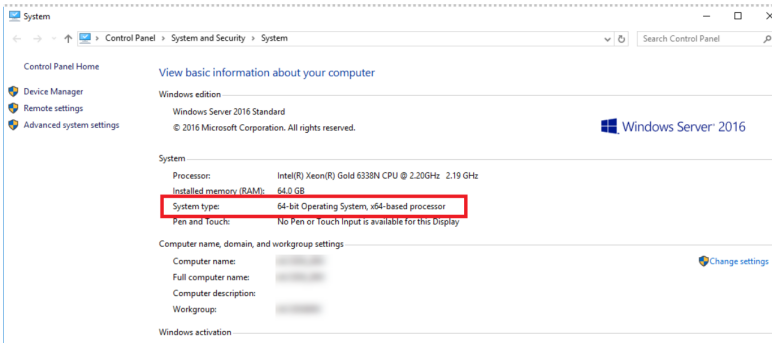
Use the following procedure to install OpenSSH on a Windows system.

Before you begin, check if OpenSSH is already installed on the Windows system. Open command prompt and run the `ssh` command. If OpenSSH is already installed, the command usage is displayed. If you see a message that says the `ssh` command is not recognized, OpenSSH is not installed and you need to follow the steps described below to install it.

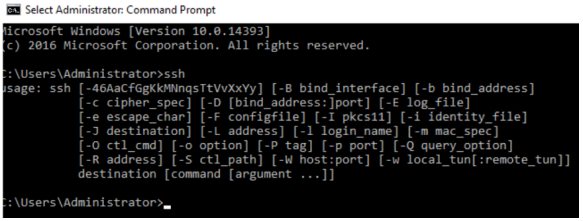


**To install and configure OpenSSH on a Windows:**

1. Get OpenSSH from the GIT hub repository. Navigate to GitHub (https://github.com/PowerShell/Win32-OpenSSH/releases) and select the required version of OpenSSH package that is compatible with your Windows type.




2. Download and install the package on your system.
3. Validate if OpenSSH package is installed by running the `ssh` command from the command prompt.




You can now download the Access Appliance software update on a Windows machine.

See “Downloading software updates to an Access Appliance node using SCP” on page 22.

For more details about OpenSSH, refer to the Microsoft documentation.

# Performing an upgrade pre-check

The pre-upgrade check determines if the system is ready for an upgrade. The pre-upgrade check runs automatically when you start the upgrade. The pre-upgrade

check performs tests, which identify any potential problems that might result in an upgrade failure. You must resolve the issues before you upgrade the cluster.

---

**Note:** Veritas recommends that you perform a pre-check one week in advance to ensure that you have sufficient time to fix any issues that are discovered during the pre-check. Additionally, run the pre-check again a day prior to the planned upgrade. The pre-check takes approximately 10 minutes to complete and does not require a scheduled downtime.

---

You can perform the pre-check using the Access Appliance UI or from the Appliance Shell Menu.

See "Running an upgrade pre-check using the UI" on page 25.

See "Running a pre-check from the appliance shell menu" on page 26.

# Running an upgrade pre-check using the UI

The upgrade pre-check determines if the system is ready for an upgrade. Run the pre-check at the beginning of an upgrade to check for any potential problems that might result in an upgrade failure. If the pre-check fails, the upgrade cannot proceed. You must resolve the issues before you upgrade the cluster.

---

**Note:** Veritas recommends that you perform a pre-check one week in advance to ensure that you have sufficient time to fix any issues that are discovered during the pre-check. Additionally, run the pre-check again a day prior to the planned upgrade.

---

**To run a pre-check:**

1. Sign in to the Access Appliance UI using the following URL, if not already done so:

   `https://console-ip:14161`

   where *console-ip* is the management console IP address where the web interface is hosted.

2. Navigate to **Settings > Software management > Software** update.

   The downloaded software update is displayed under **Downloaded package files**. To view the details about the software update click the package name.

3 For the software update, click the Actions menu (vertical ellipsis) from the right side of the row in the UI and click **Start pre-check**.

4 When you are prompted for confirmation, click **Start pre-check**.

A notification is displayed on the top of the page. To monitor the progress of the pre-check operation, click **View details**. The pre-check takes approximately 10 minutes to complete. If the pre-check completes successfully, a notification about the pre-check completing successfully is displayed on the top of the page. If any issues are detected during the pre-check, an error notification is displayed on the top of the page. You can click **View details** on the **View all activities** pane to see the error details. The pre-check continues with the rest of the checks and shows all the issues that are encountered during the pre-check.

See "Upgrading Access Appliance using the UI" on page 28.

## Running a pre-check from the appliance shell menu

Use the following procedure to run the pre-check from the appliance shell menu:

**To run a pre-upgrade check:**

1 Open an SSH session and use the admin credentials to log in the appliance.

The Veritas Appliance Shell menu is displayed.

2 To run the pre-upgrade check run the following command:

```
start appliance preupgrade-check patch=update_name
```

where *update-name* is the name of the software update that you want to install.

3 Monitor the pre-upgrade check and ensure that all the pre-upgrade checks pass successfully. To check the status, run the `show appliance preupgrade-check status` command.

---

**Note:** Wait for a few seconds before you check the status. If you check the status immediately after running the `preupgrade-check` command, the status of the preupgrade checks might not be available. If you check the status without running the `preupgrade-check` command, **Operation failed** error message is displayed.

---

# Completing pre-upgrade tasks

Ensure that you complete the following tasks before you begin with the upgrade:

# Performing manual preupgrade tasks

Before upgrading to version 8.5, perform the following steps to check the status of the appliance and to ensure that the appliance is ready for an upgrade:

1. Open an SSH session and log on to the appliance node as an administrator using the Access Appliance Shell menu.
2. Check the appliance version and the Access software verison to ensure the upgrade path is supported:

   ```
   show appliance status
   ```

3. Verify the health of the hardware components of the appliance node:

   ```
   system self-test hardware
   ```

   Ensure that the test completes with the **Node does not have any errors** message.
4. Verify the status of components such as the Access service, the S3 service, and the installed RPM packages:

   ```
   system self-test software
   ```

   Ensure that the test completes with **PASS** status.
5. Check all open sessions and terminate all sessions except the upgrade session:
6. Verify that no USB drive or other bootable devices are attached to appliance.
7. Ensure that the password for the maintenance account and any appliance administrator users does not expire within seven days. If the password expires for any of these users, change the password before you start the upgrade.
8. Ensure that the default password is not used for the maintenance account and the administrator and sysadmin users. If the default password is used for any of the users, change the password before you start the upgrade.
9. Ensure that an NTP server is configured for the cluster.
10. Disable the objectaccess server if a bucket is not created:

    From the Access command-line interface, run the `Objectaccess>server disable` command.

# Performing preupgrade tasks when replication is configured

If continuous replication is configured and replication jobs are running on the file systems, complete the following steps:

1. Check that status of the replication service:

   ```
   Replication> continuous service status
   ```

2. If the status is RUNNING, stop the replication service:

   ```
   Replication> continuous service stop
   ```

3. Upgrade the secondary site.
4. Upgrade the primary site.
5. Start the replication service:

   ```
   Replication> continuous service start
   ```

If episodic replication is configured and replication jobs are running on the file systems, complete the following steps:

1. Check the status of configured jobs:

   ```
   replication episodic job status job_name
   ```

2. For all the replication jobs that are running, pause the jobs:

   ```
   replication episodic job pause job_name
   ```

3. Upgrade the target cluster.
4. Upgrade the source cluster.
5. Resume the replication jobs that were paused before the upgrade:

   ```
   replication episodic job resume job_name
   ```

# Performing an upgrade

You can install the software update from the Access Appliance UI or from the Appliance Shell Menu.

See “Performing an upgrade from the appliance shell menu ” on page 29.

## Upgrading Access Appliance using the UI

Use the following procedure to upgrade a two-node or a one-node cluster configuration using the UI.

**To upgrade the appliance:**

1. Sign in to the Access Appliance UI using the following URL, if not already done so:

   `https://console-ip:14161`

   where *console-ip* is the management console IP address where the web interface is hosted.

2. Navigate to **Settings > Software management > Software** update.

   The downloaded software update is displayed under **Downloaded package files**. To view the details about the software update click the package name.

3. For the software update, click the Actions menu (vertical ellipsis) from the right side of the row in the UI click **Start upgrade**.

4. Review the displayed details and click **Next**.

5. To upgrade a two-node cluster, do the following:

   - Choose the method for upgrading the cluster. Click **Parallel** to upgrade both the nodes in parallel. Click **Rolling** to upgrade each node successively.
   - Choose if you want to upgrade the Veritas Data Deduplication server.
   - Click **Upgrade**.

   To upgrade a single node cluster, choose if you want to upgrade the Veritas Data Deduplication server and click **Upgrade**.

   The progress details for the upgrade operation are displayed on the **Software management** page. The upgrade takes approximately 2 hours. The **Upgrade completed successfully** message is displayed after a successful upgrade. The **Current version** on the **Software update** tab is updated and the status of the software update package changes to **Installed**.

See "Running an upgrade pre-check using the UI" on page 25.

## Performing an upgrade from the appliance shell menu

You can view the log files for the upgrade process at the following location:

`/log/upgrade/upgrade_8.3.log`

---

**Warning:** Do not restart any of the nodes manually while the upgrade is in progress.

---

**To install the downloaded software release update, complete the following steps:**

1. Connect to the Intelligent Platform Management Interface (IPMI) console of the node where you downloaded the software update package.

   **Note:** Veritas recommends that you log in using the Access Appliance shell menu from the IPMI console instead of an SSH session. The IPMI console is also known as the Veritas Remote Management Console. For details about how to access and use the Veritas Remote Management Console, refer to the *Veritas Access Appliance Initial Configuration and Administration Guide*.

2. Log in to the Access Appliance shell menu.
3. To install the software release update, run the following command:

   ```
   system software install-update update-name=
   ```

   where *update-name* is the name of the software release update that you want to install.

   A summary of the upgrade changes is displayed and you are prompted for confirmation. Review the details and type **yes** to continue.
4. When the following message is displayed and you are promoted for confirmation, type **yes** to continue:

   ```
   This software update requires a reboot of the appliance after the
   installation process completes. Do you want to continue? (yes/no)
   ```

5. For a two-node configuration, specify if you want to perform a rolling upgrade or a parallel upgrade:

   ```
   You can upgrade the cluster by performing a parallel or a rolling
    upgrade. In a parallel upgrade, cluster services are not
   available after the cluster nodes are rebooted. The cluster
   services are available after the upgrade completes successfully.
    In a rolling upgrade, each node in the cluster is upgraded
   successively and restarted without shutting down the cluster. The
    services are not available for a very limited period.

   Enter the upgrade method to use when installing the software
   update [parallel, rolling](rolling)
   ```

**6** Specify if you want to upgrade the Veritas Data Deduplication version:

```
Do you want to upgrade Veritas Data Deduplication to the latest
version? [yes, no] (no) yes
```

**7** To check the upgrade status, run the following command:

```
system software upgrade-status
```

The details about the completed tasks and the completion status are displayed.

---

**Note:** After restarting run the `system software upgrade-status` command to check the upgrade status.

---

If the upgrade fails at any point in time, error messages and the details about possible solutions are displayed and a rollback operation is initiated automatically.

After the rollback is completed successfully, the **Completed the rollback successfully** message is displayed.

If the software update is installed successfully, the following message is displayed:

Upgrade completed successfully.

The following example shows the displayed details:

```
[access-8.3] nbapp914 > system software upgrade-status

The target version is: 8.3
Current upgrade status: COMPLETED. The upgrade is 100% completed.
Latest operations:
 -[2023-01-17 19:01:58] [INFO] Running selftest.
 -[2023-01-17 19:02:47] [INFO] V-409-777-30046: Running upgrade
cleanup...
 -[2023-01-17 19:03:23] [INFO] V-409-777-1517: Upgrade completed
 successfully.
```

To ensure that the appliance was upgraded successfully, run the `show appliance status` command and verify the Access version and the appliance version.

**8** After upgrading the appliance, if the Access GUI becomes unresponsive complete the following steps:

- Determine the node that hosts the ManagementConsole service by using the following commands:

```
[access-8.3] nbapp914 >support elevate
<!-- Maintenance Mode --!>
maintenance's password:
aaapp914>hagrp -state ManagementConsole
```

- In an elevated maintenance prompt from the determined node, run the following command:

  ```
  # /opt/VRTSnas/pysnas/bin/isaconfig
  ```

# Completing post-upgrade tasks

Ensure that you complete the following tasks after the upgrade is completed successfully.

## Renewing internal certificate

From version 8.1, Access Appliance supports a single certificate for all services such as GUI and Object Access. The Appliance CA creates the internal certificate. The Access Appliance web server and S3 server use this certificate for a secure client-server communication. The internal certificate is renewed automatically when you upgrade to 8.5 from an earlier version.

If you use an internal certificate and upgrade to 8.5, you must upload the renewed internal certificate to the client trust store for a secure client-server communication. You can download the renewed internal certificate from the GUI by navigating to **Settings > Security management > Certificates > Download root certificate**.

## Downloading and installing the required EEBs

You are required to download and install the EEBs that are available on the Veritas Support website.

See “Downloading EEBs” on page 35.

See “Downloading EEBs” on page 35.

## Increasing the Veritas Data Deduplication storage to 2.4 PiB

Starting with version 8.1, you can configure up to 2.4 PiB of storage for the Veritas Data Deduplication server. You can configure two instances of Veritas Data Deduplication with 1.2 PiB storage each for a total of 2.4 PiB of storage. If you plan to increase the storage, ensure that the appliance has sufficient system memory.

You require 0.5 GB of system memory for every 1 TB of storage when you configure the Veritas Data Deduplication server. If you want to configure 1.2 PiB storage, you require 768 GB of system memory as additional system memory kit can be purchased in 386 GB increments. If there is insufficient system memory, the Veritas Data Deduplication configuration fails. Ensure that you install additional system memory as per your requirements before you configure additional storage for the Veritas Data Deduplication server.

If you don't plan to provision storage for Veritas Data Deduplication, you don't require any additional system memory.

When enabled, the Predictive and Sampling (PS) cache feature provides support for Veritas Data Deduplication pools up to 2.478 PiB (approximately) of storage. If you have upgraded to Access Appliance 8.4 from an earlier version, the previously configured Veritas Data Deduplication instances continue to use the Finger Print (FP) cache mechanism. In order to leverage the 2.478 PiB storage, the type of cache mechanism of the Veritas Data Deduplication container instance should be converted to PS cache, Veritas strongly recommends that the operation be performed under the supervision of Veritas Technical Support.

For more details, see the *Veritas Access Appliance Solutions Guide for NetBackup Guide*.

Chapter 3

# Installing EEBs using the UI

This chapter includes the following topics:



## About Access Appliance EEBs

An Emergency Engineering Binary (EEB) includes fixes that are not a part of the ISO that is installed on the appliance. These fixes are made available as EEBs on the Veritas Support site and you are required to download and install the EEBs from the Veritas Support website.

You can install EEBs using the Access Appliance UI or by using the REST APIs.

To install an EEB using the Access Appliance UI, refer to the following topics:

See “Downloading EEBs” on page 35.

See “Installing EEBs” on page 35.

To roll back an EEB, refer to the following topic:

See “Rolling back EEBs” on page 36.

To delete an EEB, refer to the following topic:

See “Removing EEBs” on page 37.

To manage EEBs using REST APIs, see the API documentation on SORT.

# Downloading EEBs

Ensure that you perform the following procedure from a system that can access the Download Center on the Veritas Support website and the Access Appliance nodes.

**To download an EEB:**

1. Go to the Veritas Support website (https://www.veritas.com/support/en_US) and click **Downloads**, which redirects you to the Download Center.
2. In the Veritas Download Center, in the **Products** list, select **Appliances**, in the**Sub product** list select **Access Appliance OS**. Select the version as 8.5 and click **Explore**.
3. Expand **Updates**.

   This section displays the EEBs that are available for download. Download the EEBs from the **Updates** section. You must sign in with your Veritas account credentials to download an EEB.

See "Installing EEBs" on page 35.

# Installing EEBs

You can install Emergency Engineering Binaries (EEBs) from the GUI using the rolling or the parallel method. In the rolling method, EEBs are installed on each node successively. In the parallel method, EEBs are installed on all the nodes in parallel. Depending on the type of EEB that you choose to install, you have the following installation options:

- Data EEBs: You can use only the rolling method to install the EEBs.
- Non-data EEBs: You can use the rolling or the parallel method to install the EEBs.
- Both data and non-data EEBs: You can use only the rolling method to install the EEBs.

---

**Note:** If disaster recovery is configured, you must upload and install the EEBs separately on both the sites.

---

**To install an EEB:**

1. Sign in to the Access Appliance UI using the following URL:

   `https://console-ip:14161`

   where *console-ip* is the management console IP address where the web interface is hosted

2. Go to **Settings > Software management > EEBs**.

   EEBs that are already uploaded on the node are displayed on the **EEBs** tab.

3. To upload an EEB:

   - If there are no EEBs on the node, click **Choose EEBs**, browse to the system where you had previously downloaded the EEBs, select the EEBs that you want to upload, and then click **Upload file**.
   - If there are EEBs present on the node but the EEB that you want to install is not in the displayed list, click **Add**. In the **Upload EEBs** screen, click **Choose EEBs**, browse to the system where you had previously downloaded the EEBs, select the EEBs that you want to upload, and then click **Add**. The EEBs are uploaded to the `inst/patch/appliance/available` location on the node and are shown with **Available** status on the **EEBs** tab. You can upload multiple EEBs simultaneously. EEBs are uploaded to one of the nodes.

4. On the **EEBs** tab, select the EEBs that you want to install and click **Install**.

   If only data EEBs are selected, you can perform only the rolling installation. If non-data EEBs are selected, when prompted, choose whether you want to use the rolling or the parallel option. If both data and non-data EEBs are selected, you can perform only a rolling installation. Click **Install**

   A notification about the EEB installation is displayed on top of the page. To monitor the progress, click **View details**. After the EEB is installed, the status of the EEB changes from **Available** to **Installed**.

See “Rolling back EEBs” on page 36.

See “Removing EEBs” on page 37.

# Rolling back EEBs

You can roll back an EEB that is installed on the nodes.

**To roll back an EEB:**

1. Sign in to the Access Appliance UI using the following URL:

   `https://console-ip:14161`

   where *console-ip* is the management console IP address where the web interface is hosted.

2. In the left navigation pane click **Settings > Software management > EEBs**.

3. Select the EEB that you want to roll back and from the Actions menu (vertical ellipsis) from the right side of the row in the UI, click **Rollback**.

4. If only data EEBs are selected, you can perform only the rolling installation. If non-data EEBs are selected, when prompted, choose whether you want to use the rolling or the parallel option. Click **Rollback**.

   A notification is displayed on top of the page. To monitor the progress, click **View details**. The status changes from **Installed** to **Available**.

# Removing EEBs

When you remove an EEB, the EEB RPM file is deleted from the `inst/patch/appliance/available` location. If you remove an EEB that is installed on the node, only the RPM file is deleted from the `inst/patch/appliance/available` directory and you can still view the installed EEB on the **EEBs** tab with an **Installed** status shown in the UI. If you remove an installed EEB and then roll it back, the RPM file is deleted and the EEB is rolled back and no longer displayed in the UI. To install the EEB again, you need to first upload the EEB and then install it.

**To remove an EEB:**

1. Sign in to the Access Appliance UI using the following URL:

   `https://console-ip:14161`

   where *console-ip* is the management console IP address where the web interface is hosted.

2. In the left navigation pane click **Settings > Software management > EEBs**.

3. Select the EEB that you want to delete and click **Remove**.

   A notification is displayed on top of the page. To monitor the progress, click **View details**.