Upgrading the Cisco Secure Access Control System

This chapter explains how to upgrade an ACS deployment or a standalone ACS server from 5.3/5.4 or from the latest available patch to 5.5.

Note When you upgrade from ACS 5.4 to ACS 5.5 using the "Upgrading an ACS server using the ApplicationUpgrade Bundle" method, it is mandatory to install the "**Pointed-PreUpgrade-CSCum04132-5.4.0.46.0a**" patch before you start upgrading from ACS 5.4 version. You can install this patch directly on any cumulative patch version.

Note When you upgrade from ACS 5.3 to 5.5 using the "Upgrading an ACS server using the ApplicationUpgrade Bundle" method, it is mandatory to install the following patches one by one in the order specified:

1 Install ACS 5.3 patch 8 (ACS 5.3.0.40.8) or a subsequent patch. You need to install patch 8 or a subsequent patch prior to the upgrade or the upgrade may fail.

2 Install the **"Pointed-PreUpgrade-CSCum04132-5.3.0.40**" patch over patch 8 or a subsequent patch before you start upgrading from ACS 5.3 version.

Note If you are using ACS 5.0/5.1/5.2, you must first upgrade to ACS 5.3/5.4 before upgrading to ACS 5.5. For information on upgrading from ACS 5.x to ACS 5.3, see the *Installation and Upgrade Guide for Cisco Secure Access Control System 5.3*.

Note The versions prior to ACS 5.5 does not have any security policy configuration in CLI. When you upgrade from ACS 5.3 or 5.4 to ACS 5.5, the password-policy is configured by default for CLI Admin.

Note Upgrading to ACS 5.5 may fail if any LDAP identity store is configured without groups or attributes and an AD identity store is not configured. To avoid this issue, before upgrading to ACS 5.5, either add groups or attributes to the LDAP identity store or configure an AD identity store.

This chapter describes the following scenarios:

- Upgrading an ACS Deployment from 5.4 to 5.5, page 11-3
- Upgrading an ACS Deployment from 5.3 to 5.5, page 11-12
- Upgrading an ACS Server from 5.4 to 5.5, page 11-12

  You can use any one of the following procedures:

  – Upgrading an ACS Server Using the Application Upgrade Bundle, page 11-12—For an incremental upgrade of an ACS server from 5.4 to 5.5.

  – Reimaging and Upgrading an ACS Server, page 11-14—To back up ACS 5.4 application data and restore it on ACS 5.5.
- Upgrading an ACS Server from 5.3 to 5.5, page 11-15
- Applying an ACS Patch, page 11-16
- Upgrading ACS 5.3 or 5.4 on the CSACS-1120 or CSACS-1121 to the Cisco SNS-3415 or Cisco SNS-3495, page 11-17

The upgrade process involves upgrading an ACS server, which includes the Monitoring and Report Viewer and the configuration information in the database.

Note ACS 5.5 upgrades ADE-OS 1.x to the 2.x version as a part of the application upgrade process.

During the upgrade process, ACS upgrades the ACS server to 5.5 and restores the data to the ACS 5.5 server. As part of the restore operation, ACS converts the configuration data to a 5.5-compatible format.

ACS stores the data upgrade information in the acsupgrade.log file. To view the content of this log file, download the support bundle.

For information on downloading the support bundle, see the *CLI Reference Guide for Cisco Secure Access Control System 5.5*. Also, see ADE.log, which logs the details of all operations that are performed in the ACS CLI. If you are migrating ACS from 4.*x* to 5.5, follow the migration procedure as described in the *Migration Guide for Cisco Secure Access Control System 5.5*.

You must have a repository that is configured with an FTP, Network File System (NFS), or Secure FTP (SFTP) network server (but not a TFTP repository) to perform the ACS upgrade.

To create a repository, use the **repository** command. For more details about the commands that are used in this chapter, see the *CLI Reference Guide for Cisco Secure Access Control System 5.5*.

Upgrade Paths

You can use the following upgrade paths to upgrade the ACS server from 5.x versions to ACS 5.5:

- **Path 1:** ACS 5.4 to ACS 5.5. To upgrade from ACS 5.4 to 5.5, see Upgrading an ACS Server from 5.4 to 5.5, page 11-12.
- **Path 2:** ACS 5.3 to ACS 5.5. To upgrade from ACS 5.3 to 5.5, see Upgrading an ACS Server from 5.3 to 5.5, page 11-15.
- **Path 3:** ACS 5.0/5.1/5.2 to ACS 5.3/5.4 to ACS 5.5. To upgrade from 5.0/5.1/5.2 to ACS 5.3, see the *Installation and Upgrade Guide for Cisco Secure Access Control System 5.3*. To upgrade from 5.0/5.1/5.2 to ACS 5.4**,** see the *Installation and Upgrade Guide for Cisco Secure Access Control System 5.3*.

Note When you upgrade from ACS 5.3 to ACS 5.5, you must install patch 8 or a subsequent patch before you start upgrading to ACS 5.5.

Note If you want to upgrade the ACS installed on a virtual machine to ACS 5.5, the virtual machine disk size should be greater than or equal to 500 GB.

Upgrading an ACS Deployment from 5.4 to 5.5

Note When you upgrade from ACS 5.4 to ACS 5.5, it is mandatory to install the pointed patch before you start upgrading from ACS 5.4 version. The name of the patch file is **Pointed-PreUpgrade-CSCum04132-5-4-0-46-0a.tar.gpg**. You can install this pointed patch directly on FCS candidate build or on top of any cumulative patch version.

Follow the procedure that is described in this section to upgrade an ACS 5.4 deployment to ACS 5.5. The deployment upgrade process consists of the following phases:

- Upgrading the Log Collector Server, page 11-3
- Upgrading the Secondary Servers, page 11-6
- Upgrading the Primary Server, page 11-8

Note ACS does not support interoperability between ACS 5.4 and ACS 5.5 deployments.

Usually, in a deployment scenario where multiple ACS instances are involved, the primary ACS instance functions as a master database for the configuration data, and one of the secondary ACS instances stores the Monitoring and Report data. You can also use the primary instance to store the Monitoring and Report data.

Initially, you need to upgrade the log collector server to ACS 5.5 and use this server as a common log collector between the ACS 5.4 and 5.5 deployments, until the 5.5 upgrade for all servers is complete.

There are some exceptions to this usual setup, which you can handle as described below:

If the ACS 5.4 primary server also functions as a log collector in your 5.4 deployment, you should promote any one of the secondary servers as the primary server in the deployment before upgrading the existing primary server. See Promoting a Secondary Server to Primary, page 11-10.

Note Before upgrading any secondary server, must deregister it from the primary server.

Upgrading the Log Collector Server

To upgrade a log collector server to ACS 5.5, complete the following steps:

Step 1 Choose any secondary server to become a log collector:

a. From the primary ACS server, choose **System Administration > Configuration > Log Configuration > Log Collector**.

The Log Collector page is displayed.

b. From the **Select Log Collector Server** drop-down list, choose the new secondary instance to be the log collector, and click **Set Log Collector**.

The ACS services of the new secondary log collector are restarted.

Step 2 Enter the **show application status acs** command in EXEC mode to check whether all process are up and running successfully, and press **Enter.**

The console displays:

```
Process 'database'                running
Process 'management'              running
Process 'runtime'                 running
Process 'ntpd'                    running
Process 'adclient'                running
Process 'view-database'           running
Process 'view-jobmanager'         running
Process 'view-alertmanager'       running
Process 'view-collector'          running
Process 'view-logprocessor'       running
```

You can now see that all processes are up and running.

Step 3 Deregister the old log collector server from the deployment, and delete it from the ACS 5.4 primary server so that it is now a standalone server:

a. From the web interface of the ACS 5.4 primary server, choose **System Administration > Operations > Distributed System Management**.

The Distributed System Management page appears.

b. From the Secondary Instances table, check the check box next to the secondary instance that you want to deregister.

c. Click **Deregister**.

The system displays the following message:

```
This operation will deregister the selected ACS Instance from the Primary Instance.

Do you wish to continue?
```

d. Click **OK**.

The secondary instance (old log collector) services are restarted.

e. Log in to the ACS 5.4 primary server.

f. Choose **System Administration > Operations > Distributed System Management**.

g. From the Secondary Instances table, check the check box next to the deregistered secondary instance that you want to delete.

h. Click **Delete**.

The following message appears:

```
Are you sure you want to delete the selected item/items?
```

i. Click **OK**.

The Secondary Instances table on the Distributed System Management page appears without the deleted secondary instance.

Step 4 Back up the log collector data:

From the ACS CLI, enter the following **backup** command in EXEC mode to perform a backup and place the backup in a remote repository:

backup *backup-file-name* **repository** *repository-name*

Note When you back up your data, if the data size exceeds the allowed disk quota of ACS, a warning message is displayed in the CLI, and an alarm is triggered in ACS Monitoring and Reports.

Step 5 Upgrade the old ACS log collector:

Perform the procedure in Upgrading an ACS Server from 5.4 to 5.5, page 11-12.

When all the process are up and running on the log collector server, you need to view the Monitoring and Report Viewer; choose **Monitoring Configuration > System Operations > Data Upgrade Status** to confirm if the upgrade is successful**.** The Data Upgrade Status page appears with the status of the Monitoring and Report Viewer data upgrade.

When the database upgrade completes, ACS displays the following message:

```
Upgrade completed successfully.
```

Now the old log collector is upgraded to 5.5 and functions as the ACS 5.5 standalone primary server, as well as a log collector. For more information, see Upgrading the ACS Monitoring and Report Viewer, page 11-11.

Step 6 Define the 5.5 log collector as a remote log target for the 5.4 deployment.

a. Choose **System Administration > Configuration > Log Configuration > Remote Log Targets**.

The Remote Log Targets page appears.

b. Click **Create**.

The Create page appears.

c. Enter the values for the following fields:

- Name—The name of the remote log target. Maximum length is 32 characters.
- Description—(Optional) A description of the remote log target. Maximum description length is 1024 characters.
- Type—The type of remote log target. Syslog is the only option.
- IP Address—IP address of the remote log target, in the format *x.x.x.x*. Specify the IP address of the 5.5 log collector server.
- Use Advanced Syslog Options—Click to enable advanced syslog options, which include port number, facility code, and maximum length.
- Port—The port number of the remote log target that is used as the communication channel between the ACS and the remote log target (default is 514). Enter **20514** for the port number.
- Facility Code—(Optional) Choose an option from the Facility Code drop-down list.
- Maximum Length—The maximum length of the remote log target messages. Valid options are from 200 to 1024.

d. Click **Submit**.

The remote log target configuration is saved. The Remote Log Targets page appears with the new remote log target configuration.

Now, the authentication details from the 5.4 deployment are logged in both the 5.4 and 5.5 log collector servers.

Step 7 On the 5.4 primary server, configure the appropriate logging categories for the remote log target:

a. Choose **System Administration > Configuration > Log Configuration > Logging Categories > Global**.

The Logging Categories page appears; from here, you can view the logging categories.

b. Click the name of the logging category that you want to configure, or click the radio button next to the name of the logging category that you want to configure, and click **Edit**.

c. In the **General** tab, complete the following fields:

- Log Severity—Use the drop-down list to choose the severity level. Valid options are FATAL, ERROR, WARN, INFO, and DEBUG.
- Log to Local Target—Check to enable logging to the local target.
- Local Target is Critical—Check the check box to make this local target the critical target. Usable for accounting and for AAA audit (passed authentication) logging category types only.

d. Click the **Remote Syslog Target** tab and choose **Remote Targets** to view the logs.

e. Click **Submit**.

The Logging Categories page appears, with your configured logging category. Proceed with Upgrading the Secondary Servers, page 11-6.

Upgrading the Secondary Servers

Use this procedure to upgrade each ACS 5.4 secondary server in your deployment to ACS 5.5:

Tip To ensure that you preserve the local certificates of the secondary server, you should promote each secondary server to the primary role and then perform the ACS 5.5 upgrade. See Upgrading the PKI Data and Certificates, page 11-9.

Before upgrading a secondary ACS server, ensure that the server is active and that it is not in local mode.

To verify the status from the web interface of the secondary server, choose **System Administration > Operations > Local Operations**.

Step 1 Verify if the secondary server is a log collector. If so, change the log collector server to any other secondary server; otherwise, proceed to Step 2.

a. From the ACS 5.4 primary server, **System Administration > Configuration > Log Configuration > Log Collector**.

ACS displays the current log collector server.

b. From the Select Log Collector drop-down list, choose a different server to configure as a log collector.

c. Click **Set Log Collector**.

Step 2 Deregister the secondary server from the 5.4 deployment and delete it from the ACS 5.4 primary server, so that it now becomes a standalone server:

a. Choose **System Administration > Operations > Distributed System Management**.

The Distributed System Management page appears.

b. From the Secondary Instances table, check the check box next to the secondary instance that you want to deregister.

c. Click **Deregister**.

The system displays the following message:

```
This operation will deregister the selected ACS Instance from the Primary Instance.

Do you wish to continue?
```

d. Click **OK**.

The ACS machine restarts.

e. Log in to the ACS 5.4 primary server.

f. Choose **System Administration > Operations > Distributed System Management**.

g. From the Secondary Instances table, check the check box next to the secondary instance that you want to delete.

h. Click **Delete**.

The following message appears:

```
Are you sure you want to delete the selected item/items?
```

i. Click **OK**.

The Secondary Instances table on the Distributed System Management page appears without the deleted secondary instance.

Step 3 Back up the secondary server data.

From the ACS CLI, issue the following **backup** command in EXEC mode to perform a backup and place the backup in a repository:

backup *backup-name* **repository** *repository-name*

Note When you back up your data, if the data size exceeds the allowed disk quota of ACS, a warning message is displayed in the CLI, and an alarm is triggered in ACS Monitoring and Reports.

Step 4 Upgrade the ACS server to 5.5. See Upgrading an ACS Server from 5.4 to 5.5, page 11-12.

Step 5 Register the secondary server to the ACS 5.5 primary server.

a. Choose **System Administration > Operations > Local Operations > Deployment Operations**.

The Deployment Operations page appears.

b. Complete the following mandatory fields under the Registration dialog box:

- Primary Instance—The hostname of the 5.5 primary server with which you wish to register the secondary instance.
- Admin Username—Username of an administrator account.

- Admin Password—The password for the administrator account.
- Hardware Replacement—Check to enable the existing ACS instance to re-register with the primary instance and get a copy of the configuration that is already present in the primary instance.
- Recovery Keyword—Specify the same hostname that was used in the 5.4 deployment to ensure that you associate this secondary server with the Monitoring and Report data that was collected earlier.

  After you submit this information, this instance connects to the primary instance. The primary instance finds the associated ACS instance records based on the keyword and marks each record as registered.

c. Click **Register to Primary**.

The system displays the following message:

```
This operation will register this ACS Instance as a secondary to the specified Primary
Instance. ACS will be restarted. You will be required to login again. Do you wish to
continue?
```

d. Click **OK**.

ACS restarts automatically. Wait for some time to ensure that all processes are up and running successfully.

Note When you register a secondary instance to a primary instance, you can use any account that is created on the primary instance. The credentials that you create on the primary instance are replicated to the secondary instance.

After the registration is complete, ACS performs a full synchronization and sends the ACS 5.5 configuration data to the 5.5 secondary server.

Step 6 Import local and outstanding Certificate Signing Requests (CSRs).

See the Importing Server Certificates and Associating Certificates to Protocols section and the Generating Self-Signed Certificates section of the *User Guide for Cisco Secure Access Control System 5.5*.

Proceed with Upgrading the Primary Server, page 11-8.

Upgrade the ACS 5.4 primary server to ACS 5.5 once all the secondary servers are upgraded to ACS 5.5. When there is no secondary server that is registered with the primary server, the primary server itself acts as a log collector.

Upgrading the Primary Server

To upgrade the primary server from a 5.4 to 5.5 deployment:

Step 1 Ensure that the primary server is a standalone server:

a. Select **System Administration > Operations > Distributed System Management**.

The Distributed System Management page appears.

b. Check if there are secondary servers listed in the Secondary Instances table. If there are any secondary servers, upgrade those servers before upgrading the 5.4 primary server. See Upgrading the Secondary Servers, page 11-6.

Step 2 Upgrade the ACS server to 5.5. See Upgrading an ACS Server from 5.4 to 5.5, page 11-12.

Step 3 Register the newly upgraded 5.5 server with the existing primary ACS 5.5 server:

a. Choose **System Administration > Operations > Local Operations > Deployment Operations**.

The Deployment Operations page appears.

b. Complete the following mandatory fields under the Registration dialog box:

- Primary Instance—The hostname of the primary server with which you wish to register the secondary instance.
- Admin Username—Username of an administrator account.
- Admin Password—The password for the administrator account.
- Hardware Replacement—Check to enable the existing ACS instance to re-register with the primary instance and get a copy of the configuration that is already present in the primary instance.
- Recovery Keyword—Specify the same hostname that was used in the 5.4 deployment to ensure that you associate this server with the Monitoring and Report data that was collected earlier.

  After you submit this information, this instance connects to the primary instance. The primary instance finds the associated ACS instance records based on the keyword and marks each record as registered.

c. Click **Register to Primary**.

The system displays the following message:

```
This operation will register this ACS Instance as a secondary to the specified Primary
Instance. ACS will be restarted. You will be required to login again. Do you wish to
continue?
```

d. Click **OK**.

ACS will restart automatically. Wait for some time to ensure that all processes are up and running successfully.

Note When you register a secondary to a primary instance, you can use any account that is created on the primary instance. The credentials that you create on the primary instance are replicated to the secondary instance.

Promote this instance as the ACS 5.5 primary server again. See Promoting a Secondary Server to Primary, page 11-10.

Now the ACS 5.4 deployment is completely upgraded to ACS 5.5.

Upgrading the PKI Data and Certificates

When you upgrade from ACS 5.4 to ACS 5.5 using application upgrade method, ACS restores the Public Key Infrastructure (PKI), the local certificates, and outstanding CSRs.

Reimaging and upgrade method allows you to back up ACS 5.4 instance data and retrieve it in ACS 5.5. If you use reimaging and upgrade method, the PKI, local certificates, and outstanding CSRs in ACS 5.5 instance are erased and the data that is retrieved from ACS 5.4 instance will be stored in ACS 5.5 instance.

Promoting a Secondary Server to Primary

Step 1 From the web interface of the primary server, choose **System Administration > Operations > Distributed System Management**.

The Distributed System Management page appears.

Step 2 In the Secondary Instances table, check the check box next to the secondary server that you want to promote to primary.

Step 3 Click **Promote**.

The system displays the following message:

```
This operation will promote the selected ACS Instance to become the new Primary Instance.
As a consequence, the current Primary Instance will be demoted to a Secondary.

Do you wish to continue?
```

Step 4 Click **OK**.

The system promotes the choosen secondary server to primary and moves it to the Primary Instances table. The existing primary server is automatically moved to the Secondary Instances table.

When the registration completes, ACS performs a full synchronization and sends the ACS 5.5 configuration data to the newly promoted primary server.

Upgrading the ACS Monitoring and Report Viewer

ACS invokes the upgrade of the Monitoring and Report Viewer as a subtask during upgrade.

The maximum disk space that is available for the ACS Monitoring and Report Viewer is 150 GB.

This section contains:

To check the status of the database upgrade, in the Monitoring and Report Viewer, choose **Monitoring Configuration > System Operations > Data Upgrade Status**.

The Data Upgrade Status page appears, indicating the status of the Monitoring and Report Viewer data upgrade.

When the database upgrade completes, ACS displays the following message:

```
Upgrade completed successfully.
```

Restoring the Monitoring and Report Viewer Data After Upgrade

When you restore the backup data after upgrading to 5.5, ACS automatically synchronizes the changes with the database and reports, if any changes are found.

The report data is available only for the period during which you create a backup and not for the period when you restore the data. For example, if you back up the data in June and restore it in August, the report data that is available is the data for June and not for August. To get the latest report data, you need to run the reports again.

Upgrading the Database

After the 5.5 upgrade, if you restore a backup that was made prior to the upgrade, ACS displays the database version as **AVPair:DBVersion=5.5** and maintains the schema version as 5.5 in the av_system_settings table. When the database process restarts, ACS checks the ACS version and the database version if they are out-of-date and performs a schema and data upgrade.

Upgrading the Reports

After you upgrade to 5.5, if you restore a backup that was made before the upgrade, ACS checks whether the reports tag displays “View 5.5.” Then, when the web process starts, ACS performs the necessary updates.

Note When you click Switch Database, the logs that are generated after performing Step 7 (upgrading the database schema to version 5.2) of the log collector server upgrade are lost. ACS retains only the logs that are generated before you perform Step 7.

Upgrading an ACS Deployment from 5.3 to 5.5

Note When you upgrade from ACS 5.3 to ACS 5.5 using the “Reimaging and Upgrading an ACS Server method, you must install patch 8 or a subsequent patch before you start upgrading to ACS 5.5.

Note When you upgrade from ACS 5.3 to 5.5 using the "Upgrading an ACS server using the ApplicationUpgrade Bundle" method, it is mandatory to install the following patches one by one in the order specified:

1 Install ACS 5.3 patch 8 (ACS 5.3.0.40.8) or a subsequent patch. You need to install patch 8 or a subsequent patch prior to the upgrade or the upgrade may fail.

2 Install the "**Pointed-PreUpgrade-CSCum04132-5.3.0.40**" patch over patch 8 or a subsequent patch before you start upgrading from ACS 5.3 version.

After installing the specified patch, follow the same procedure that was described in Upgrading an ACS Deployment from 5.4 to 5.5, page 11-3.

Upgrading an ACS Server from 5.4 to 5.5

The following are the two ways in which you can upgrade an ACS server from 5.4 to 5.5. You can use either one of these upgrade methods:

- Upgrading an ACS Server Using the Application Upgrade Bundle, page 11-12
- Reimaging and Upgrading an ACS Server, page 11-14

Note When you upgrade from ACS 5.4 to ACS 5.5 using the "Upgrading an ACS server using the ApplicationUpgrade Bundle" method, it is mandatory to install the "**Pointed-PreUpgrade-CSCum04132-5.4.0.46.0a**" patch before you start upgrading from ACS 5.4 version. You can install this patch directly on any cumulative patch version.

Upgrading an ACS Server Using the Application Upgrade Bundle

To upgrade an ACS server from 5.4 to 5.5:

Step 1 Place the ACS 5.5 application upgrade bundle (ACS_5.5.tar.gz) in a remote repository.

To configure the repository, follow the procedure that is given in the *CLI Reference Guide for Cisco Access Control System 5.5*.

Step 2 Enter the following application upgrade command in EXEC mode.

application upgrade ACS_5.5.tar.gz *repository-name*

ACS displays the following confirmation message:

```
Save the current ADE-OS running configuration? (yes/no) [yes] ?
```

```
It is strongly recommended to take full backup before upgrade. Do you want to take a
backup now ? (yes/no) [yes] ?
```

Note The backup file created at this stage is saved in the same remote repository that you would have created to store the application upgrade bundle.

Note When you upgrade ACS from an older version to version 5.5, if the upgrade bundle size exceeds the allowed disk quota, a warning message is displayed in the CLI, and an alarm is triggered in ACS Monitoring and Reports.

Step 3 Enter **yes**.

When the ACS upgrade is complete, the following message appears:

```
% CARS Install application required post install reboot...

The system is going down for reboot NOW!

Application upgrade successful
```

While ACS upgrades the ACS 5.4 configuration data, it also converts the ACS 5.4 Monitoring and Report Viewer data to the 5.5 format.

Step 4 To monitor the status of the data upgrade, from the Monitoring and Report Viewer, choose **Monitoring Configuration > System Operations > Data Upgrade Status**.

The Data Upgrade Status page appears, indicating the status of the Monitoring and Report Viewer data upgrade.

When the database upgrade completes, ACS displays the following message:

```
Upgrade completed successfully.
```

Step 5 Click **OK**.

Step 6 Enter the **show application version acs** command to check whether the ACS version was upgraded successfully.

The following message is displayed:

```
Cisco ACS VERSION INFORMATION
-----------------------------
Version : 5.5.0.46.0a
Internal Build ID : B.221
```

Step 7 Enter the **show application status acs** command in EXEC mode to check whether all processes are up and running successfully, and press **Enter.**

The console displays:

```
ACS role: PRIMARY
Process 'database'                running
Process 'management'              running
Process 'runtime'                 running
Process 'ntpd'                    running
Process 'adclient'                running
Process 'view-database'           running
Process 'view-jobmanager'         running
```

```
Process 'view-alertmanager'          running
Process 'view-collector'             running
Process 'view-logprocessor'          running
```

Now you can see that all processes are up and running and that ACS is successfully upgraded to version 5.5.

Reimaging and Upgrading an ACS Server

This section explains how to upgrade ACS 5.4 to 5.5 by backing up the ACS 5.4 data and restoring it on a reimaged ACS 5.5 server. You must have physical access to the ACS appliance to perform this upgrade procedure.

To perform a reimage and upgrade to ACS 5.5:

Step 1 Back up the ACS data from the ACS 5.4 server.

Step 2 Enter the following **backup** command in EXEC mode to perform a backup and place the backup in a repository.

backup *backup-name* **repository** *repository-name*

Note When you back up your data, if the data size exceeds the allowed disk quota, a warning message is displayed in the CLI, and an alarm is triggered in ACS Monitoring and Reports.

Note Ensure that you use a remote repository for the ACS 5.4 data backup. Otherwise, you might lose the backed-up data after you install 5.5.

Step 3 Use the ACS 5.5 recovery DVD to install ACS 5.5. See Reimaging the ACS Server, page 5-7.

This reimages the ACS server to a fresh ACS 5.5 server that does not have any configuration data.

Step 4 Configure a repository in the fresh ACS 5.5 server to restore the backed-up data.

Step 5 Restore the data that was previously backed up in Step 2 to the ACS 5.5 server.

Enter the **restore** command in EXEC mode to restore the backup:

restore *filename* **repository** *repository-name*

Note When you restore the backed-up data, if the data size exceeds the allowed disk quota, a warning message is displayed in the CLI, and an alarm is triggered in ACS Monitoring and Reports.

Note If you restore the ADE-OS backup in a different hardware, you must change the IP address of the ACS machine to bring it to the running state.

While restoring the data, using the 5.4 backup file, this command restores the ACS 5.4 configuration data. It also converts and upgrades the ACS 5.4 Monitoring and Report Viewer data to the 5.5 format.

If the backed-up data size exceeds the allowed disk quota of ACS, a warning message is displayed in the CLI, and an alarm is displayed in ACS Monitoring and Reports.

Step 6 To monitor the status of the data upgrade, from the Monitoring and Report Viewer, choose **Monitoring Configuration > System Operations > Data Upgrade Status**.

The Data Upgrade Status page appears, indicating the upgrade status of the Monitoring and Report Viewer data.

When the database upgrade completes, the following message is displayed.

```
Upgrade completed successfully.
```

Step 7 Click **OK**.

Note If the scheduled backup is already configured in ACS 5.4 or previous releases, you must enter the Encryption Password in the Backup ACS Configuration Data page after successful upgrade to ACS 5.5.

Warning **The ACS restore does not update PKI on EAP or management interface. HTTPS uses a self-signed certificate, even if the database has a CA signed certificate only.**
The work-around for this is:
1. Create a temporary self-signed certificate and assign EAP or management interface to it.
2. Re-assign EAP or management interface to the CA signed certificate.
3. Delete the self-signed certificate.

Note If the backup data is huge in size, the extraction process might take a minimum of 1 hour to many hours to complete.

Note Restore the backup file in the same ACS server, to avoid IP conflict issues.

Upgrading an ACS Server from 5.3 to 5.5

To upgrade your ACS 5.3 server to ACS 5.5, follow the same procedure that was described in Upgrading an ACS Server from 5.4 to 5.5, page 11-12.

Note When you upgrade from ACS 5.3 to 5.5 using the “Upgrading an ACS server using the ApplicationUpgrade Bundle” method, it is mandatory to install the following patches one by one in the order specified:

1 Install ACS 5.3 patch 8 (ACS 5.3.0.40.8) or a subsequent patch. You need to install patch 8 or a subsequent patch prior to the upgrade or the upgrade may fail.

2 Install the **“Pointed-PreUpgrade-CSCum04132-5.3.0.40**” patch over patch 8 or a subsequent patch before you start upgrading from ACS 5.3 version.

Applying an ACS Patch

You can download the ACS 5.5 cumulative patches from the following location:

http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm

To download and apply the patches:

Step 1 Log in to Cisco.com and navigate to **Security > Access Control and Policy > Policy and Access Management > Cisco Secure Access Control System > Cisco Secure Access Control System 5.5**.

Step 2 Download the patch.

Step 3 Install the ACS 5.5 cumulative patch by running the following **acs patch** command in EXEC mode. To install the ACS patch:

acs patch install *patch-name* **repository** *repository-name*

ACS displays the following confirmation message:

```
Save the Current ADE-OS running configuration? (yes/no) [yes] ? yes
```

Note When you upgrade ACS from an older version to version 5.5, if the upgrade bundle size exceeds the allowed disk quota, a warning message is displayed in the CLI, and an alarm is triggered in ACS Monitoring and Reports.

Step 4 Enter **yes**.

ACS displays the following message:

```
Generating configuration...
Saved the ADE-OS running configuration to startup successfully
Getting bundle to local machine...
  md5: aa45b77465147028301622e4c590cb84
  sha256: 3b7f30d572433c2ad0c4733a1d1fb55cceb62dc1419b03b1b7ca354feb8bbcfa
% Please confirm above crypto hash with what is posted on download site.
% Continue? Y/N [Y]?
```

Step 5 The ACS 5.5 patch install displays the md5 and sha256 checksum. Compare it with the value displayed on Cisco.com at the download site. Do one of the following:

- Enter **Y** if the crypto hashes match. If you enter Y, ACS proceeds with the installation steps.

  ```
  % Installing an ACS patch requires a restart of ACS services.
  Would you like to continue? yes/no
  ```

- Enter **N** if the crypto hashes do not match. If you enter N, ACS stops the installation process.

Step 6 Enter **yes**.

The ACS version is upgraded to the applied patch. Check whether all services are running properly using the **show application status acs** command in ACS CLI EXEC mode.

Step 7 Enter the **show application version acs** command in EXEC mode to check if the patch is installed properly. ACS displays the following message:

```
acs/admin# show application version acs
```

```
CISCO ACS VERSION INFORMATION
-----------------------------
Version: 5.5.0.46.1
Internal Build ID: B.225
Patches:
5-5-0-46-1
acs/admin #
```

Note During patch installation, if the patch size exceeds the allowed disk quota, a warning message is displayed in the ACS CLI, and an alarm is displayed in the ACS Monitoring and Reports page.

Upgrading ACS 5.3 or 5.4 on the CSACS-1120 or CSACS-1121 to the Cisco SNS-3415 or Cisco SNS-3495

If you have ACS 5.3 or 5.4 installed on the CSACS-1120 or CSACS-1121 appliance and would like to upgrade to the Cisco SNS-3415 or Cisco SNS-3495, perform the following steps:

Step 1 Back up your existing ACS 5.3 or 5.4 setup.

Step 2 Install ACS in a Cisco SNS-3415 or Cisco SNS-3495 appliance with ACS 5.5 installed on it.

Step 3 Restore the ACS 5.3 or 5.4 backup taken in Step 1.

Note The **application upgrade** command is not applicable if you want to move to ACS 5.5 on a Cisco SNS-3415 or Cisco SNS-3495 appliance. You must install ACS 5.5 on the Cisco SNS-3415 or Cisco SNS-3495 appliance and restore the backup obtained from your CSACS-1120 or CSACS-1121 appliance.