

Cisco NAC Appliance Migration Guide - Release 4.1(8) to Release 4.7(0)

Document Number OL-21013-01 Revised: June 14, 2010

Overview

This Guide describes how to upgrade from an earlier Cisco NAC Appliance release on non-Cisco hardware to a next generation (NAC-3315/3355/3395) platform using the Cisco NAC Appliance Migration utility.



If you are planning to upgrade a Dell 1850-based CAM/CAS to release 4.1(8) prior to running the Migration utility, contact the Cisco Technical Assistance Center (TAC) for important information regarding Cisco NAC Appliance Release 4.1(x) upgrade on the Dell 1850 platform.

The Migration script upgrades NAC Appliance Software from release 4.1(8) to release 4.7(0) only, and applies ONLY to non-Cisco hardware.



Warning

Do not execute the Migration Utility on Cisco NAC-3140, NAC-3310, NAC-3350, or NAC-3390 appliances, as this will result in database corruption. If you want to upgrade to release 4.7(x) from these devices, refer to the "Upgrading to Release 4.7(x)" section in the *Release Notes for Cisco NAC Appliance* corresponding to your latest Cisco NAC Appliance release version.

If you are migrating from non-Cisco hardware, you can download the Migration utility from the Cisco NAC Appliance Software Download Site. You must first upgrade your Cisco NAC Appliance software that is running on the non-Cisco hardware to release 4.1(8).

After migrating to the Cisco NAC 3315/335/3395 Appliance with release 4.7(0), you can follow the normal procedure to upgrade the new appliance to 4.7(1) or later.



Before You Start

| | After upgrading your existing Cisco NAC Appliance release to 4.1(8), if you experience any difficulties and want to revert to the previous release, you need to perform a fresh installation on your CAMs/CAS to return to your previous software release. It is recommended to create a backup snapshot for your current software version before upgrading to release 4.1(8). |
|---|---|
| | It is imperative that you follow the migration steps in the order presented. If you deviate from the following procedures, you could lose your existing configuration and may not be able to bring your network back to operational capacity in a satisfactory time frame. |
| | |
| | Acquire new Cisco NAC Appliances to replace the Clean Access Manager(s) and all Clean Access |
| ì | Server(s) as appropriate for your existing network topology. |
|] | Server(s) as appropriate for your existing network topology. Get new Cisco NAC Appliance license files based on the eth0 MAC address of your new Clean Access Manager. For more information, follow the guidelines in <i>Cisco NAC Appliance Service</i> <i>Contract/Licensing Support</i> . |

Prepare Your Existing Appliances for Migration

| Note | |
|------|--|

Ensure that you perform all the upgrade and migration steps offline, not in the production environment. After completing the migration, you can bring up the appliances in the production network and verify connectivity.

- **Step 1** Upgrade old hardware to 4.1(8). Upgrade all CAM/CAS machines on the network according to the appropriate upgrade instructions for your existing Clean Access release in the "Upgrade" section of the *Release Notes for Cisco NAC Appliance, Version 4.1(8)*.
- **Step 2** After you upgrade your existing appliances to release 4.1(8), verify successful Clean Access Agent login/web login functionality.

Step 3 Create and save a database snapshot from your existing Clean Access Manager(s). Be sure to save copies of the snapshot file(s) on a separate machine accessible on the local network. For more information, see the "Backing Up the CAM Database" section in the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.1(8).*

- Step 4 Export and save local copies of SSL certificates, private keys, and appropriate third-party Root/Intermediate certificates from your Clean Access Manager(s) and all Clean Access Servers on the network according to the "Manage CAM SSL Certificates" section of the *Cisco NAC Appliance Clean Access Manager Installation and Configuration Guide, Release 4.1(8)* and "Manage CAS SSL Certificates" section of the *Cisco NAC Appliance Clean Access Server Installation and Configuration Guide, Release 4.1(8)*, respectively.
- **Step 5** Save local copies of your FlexLM license files or perfigo.com license strings for safe keeping:
 - FlexLM license files are located in the /perfigo/control/tomcat/normal-webapps/upload/ directory on the CAM.
 - To save a local copy of your perfigo.com license string, navigate to the CAM Administration > CCA Manager > Licensing web console page and copy the entire string from the Perfigo Product License Key field.
- **Step 6** Back up additional Cisco NAC Appliance elements that fall outside of the standard CAM database snapshot function:
 - Network time servers for both CAM and CAS.
 - Network DNS servers for both CAM and CAS.
 - Network interface eth2 and eth3 configurations for both CAM and CAS, if applicable.
 - Host files for both CAM and CAS.
 - Serial port configuration settings for both CAM and CAS, if applicable.
 - SSL Authorization settings for both CAM and CAS.
 - CAM daily database backups.
 - Other CAM database snapshots.



- For CAM Backup, refer to the "Administering the CAM" chapter in the Cisco NAC Appliance -Clean Access Manager Installation and Configuration Guide, Release 4.1(8).
- For CAS Backup, refer to the "Administering the CAS" and the "Configuring the CAS Managed Network" chapters in the *Cisco NAC Appliance Clean Access Server Installation and Configuration Guide, Release 4.1(8).*

Run the Migration Utility

Note

To minimize database corruption risks and ensure that the migration process goes as quickly as possible, Cisco strongly recommends exporting and archiving Agent report files, and purging existing event logs, Agent report files, and any files used for File Distribution requirement types from the CAM database before launching the Migration utility. Cisco recommends that each file does not exceed 50 MB in size.

Step 1 Download the Migration utility nac_migration-4.7.0.tar.gz from the Cisco NAC Appliance Software Download Site.

Step 2 Copy the utility nac_migration-4.7.0.tar.gz to the /store directory of the release 4.1(8) NAC Appliance using secure copy or secure ftp as shown in Figure 1.

| Desktop - root@192.168.137.4 - WinSCP | | | | | | | | _ 🗆 : |
|---|---------------|-------------------------------|----------------|----------------------------|------------|----------------|-----------|-------|
| Local Mark Files Commands S | ession Option | s <u>R</u> emote <u>H</u> elp | 6 1 | 🟦 📀 🔤 🏄 🔚 | - 🛛 🗘 | Ø 🔿 Default | • | · 🍯 |
| 🔄 root@192.168.137 💌 🀜 📑 🗸 📑 | | | | | | | | |
| 🥪 C: Volume_1 💽 🛛 😓 👻 🔝 | 🔯 🚮 🔯 | 🔄 te | | 🗁 store 💌 📢 | • • • | 🖻 🗖 🚮 💆 | 🖮 te | |
| \Documents and Settings\Administrator\Desktop |) | | | /store | | | | |
| ame 🔺 Ext | Size | Туре | 1 | Name 🔺 Ext | Size | Changed | Rights | Own |
| adsiedit.msc | 42,986 | Microsoft Comm | 1 | 💼 | | 11/10/2009 4:3 | rw×r-×r-× | root |
| cca_upgrade-4.1.8.tar.gz | 138,411, | WinRAR archive | | Cca_upgrade-4.1.3 | | 10/17/2007 8:4 | rw×r-×r-× | 514 |
| Cisco ASDM Launcher.Ink | 709 | Shortcut | ÷ | Cca_upgrade-4.1.3.1 | | 4/5/2008 8:00: | rw×r-×r-× | 513 |
| Client_4_0_0.zip | 548,519, | WinRAR ZIP arc | ÷., | Cca_upgrade-4.1.6 | | 8/27/2008 10:3 | rw×r-×r-× | 514 |
| en_windows_vista_x86_dvd_X12-34293.is | 1,525,62 | PART File | 1 | Cca_upgrade-4.1.8 | | 11/11/2009 6:0 | rwxr-xr-x | 514 |
| File nacguest-2.0-build-62.iso.URL | 79 | Internet Shortcut | | Ecca_upgrade-4.1.3.1.t | 126,754, | 4/5/2008 6:33: | rw-rr | root |
| FileZilla Server Interface.lnk | 1,612 | Shortcut | | Ecca_upgrade-4.1.6.tar.gz | 137,347, | 8/27/2008 9:16 | rw-rr | root |
| kerbtray.exe | 39,936 | Application | | Cca_upgrade-4.1.8.tar.gz | 138,411, | 11/10/2009 4:2 | rw-rr | root |
| kerbtray.zip | 11,909 | WinRAR ZIP arc | | Cca_upgrade-4.1.8.tar | 53,303,188 | 11/10/2009 5:0 | rw-rr | root |
| KTPASS output.txt | 576 | Text Document | | 🖬 db-4.1.6-4.1.8.sql | 0 | 11/11/2009 6:0 | rw-rr | root |
| ktpass.zip | 32,761 | WinRAR ZIP arc | | ac_migration-4.7.0.ta | 30,596 | 11/11/2009 10: | rw-rr | root |
| nac_migration-4.7.0.tar.gz | 30,596 | WinRAR archive | | - | | | | |
| Packetyzer.Ink | 660 | Shortcut | | | | | | |
| perfigo.txt | 53 | Text Document | | | | | | |
| putty.exe | 454,656 | Application | | | | | | |
| Router_Switch_Com2.ht | 22,403 | HyperTerminal File | | | | | | |
| Softerra LDAP Browser 2.6.Ink | 2,341 | Shortcut | : | | | | | |
| tftpd32.exe | 147,456 | Application | | | | | | |
| tutty.exe | 427,008 | Application | | | | | | |
| VNC Viewer 4.Ink | 603 | Shortcut | : | | | | | |
| WinRAR, Ink | 618 | Shortcut | | | | | | |
| WinSCP3.exe | 4,257,792 | Application | | | | | | |
| WinSCP3.Ink | 538 | Shortcut | | | | | | |
| | | P | Ľ | • | | | | |
| 3 of 2,115 MB in 0 of 27 | | - | _ | 0 B of 434 MB in 0 of 10 | | | | |
| 🕫 F2 Rename 📑 F4 Edit 📑 F5 Copy 📑 F | 6 Move 💣 Fi | Create Directory 💙 | < F8 | Delete 😁 F9 Properties 🥂 F | 10 Quit | | | |
| 17 574 D 21 000 D 31 1 | ο Δ | CETRU | | 0.02.10 | | | | |

Figure 1 Copying the Migration Utility to NAC Appliance

Step 3 Run the following commands in the release 4.1(8) NAC Appliance using SSH or serial console:

a. To run the migration utility, you need to stop the perfigo service by providing the **service perfigo stop** command for CAM.



For CAS, type the command as service perfigo maintenance to stop the perfigo service.

- **b.** Type cd /store to go to the /store directory.
- c. Create a directory named migration by typing the command mkdir -p migration.
- d. Move the migration utility to the migration directory by entering the command mv nac_migration-4.7.0.tar.gz migration/.
- e. Go to the migration directory by typing cd migration.
- f. Unzip the utility by entering tar -xvzf nac_migration-4.7.0.tar.gz.
- g. The tar command unzips the utility and creates a directory named nac_migration-4.7.0.

Figure 2 illustrates the above commands.

| root@CAM-1:/store/migration | |
|--|---|
| File Edit View Terminal Tabs Help | |
| [root@CAM-1 ~]# cd /store/ | |
| [root@CAM-1 store]# mkdir -p migration | |
| [root@CAM-1 store]# mv nac_migration-4.7.0.tar.gz migration/ | , |
| [root@CAM-1 store]# cd migration/ | |
| [root@CAM-1 migration]# | |
| [root@CAM-1 migration]# tar -xvzf nac_migration-4.7.0.tar.gz | : |
| nac_migration-4.7.0/ | |
| nac_migration-4.7.0/RPMS/ | |
| <pre>nac_migration-4.7.0/RPMS/nac-db-schema-4.6.1-k9.rpm</pre> | |
| <pre>nac_migration-4.7.0/RPMS/nac-db-schema-4.7.0-k9.rpm</pre> | |
| nac_migration-4.7.0/notes.html | |
| nac_migration-4.7.0/README | |
| nac_migration-4.7.0/backup.sh | |
| nac_migration-4.7.0/bin/ | |
| nac_migration-4.7.0/bin/unpack.sh | |
| nac_migration-4.7.0/bin/caslist.sh | |
| nac_migration-4.7.0/bin/restore.sh | |
| nac_migration-4.7.0/bin/camlist.sh | |
| nac_migration-4.7.0/bin/showstate.sh | |
| nac_migration-4.7.0/bin/mktar | = |
| [root@CAM-1 migration]# | |
| | |
| | |

Figure 2 Unzipping the Migration Utility

- Step 4 Type cd nac_migration-4.7.0 to go to the nac_migration-4.7.0 directory.
- **Step 5** Type the command ./backup.sh to run the migration script.
- **Step 6** The following warning message is displayed:

Warning: This migration utility will transform the current 'controlsmartdb' database into a release 4.7.0-compatible database temporarily and revert to the original database afterwards. Cisco strongly recommends you create a backup snapshot of your current configuration immediately prior to beginning the migration process to release 4.7.0 and avoid performing any significant configuration updates in your system until after the new hardware has been configured to match your existing appliances and brought online.

Is the system backup taken and ready to continue? (y/n)? [n]

Press y to confirm that you have taken the backup.

• If the uploaded file for a "File Distribution" requirement type in the CAM database exceeds 50MB, the following warning message is displayed.

Maximum file distribution size exceeds 50 MB. Aborting the upgrade and rebooting the system. Please remove such large files from the database before performing the upgrade. Exiting.

SATCING.

The upgrade process is aborted, the .ISO CD-ROM is ejected, and the appliance is rebooted.

Before attempting to perform the upgrade again, you must manually purge "File Distribution" files larger than 50MB from the database using the CAM **Device Management > Clean Access > Clean Access Agent > Requirements > Requirement List** web console page, or move the uploaded file to a network server and create a "Link Distribution" requirement to replace the oversized "File Distribution" files.



Figure 3 shows the output for a standalone CAM.

```
Figure 3
               Running the Script
               root@CAM-1:/store/migration/nac_migration-4.7.0
                                                                             . 6
×
 File Edit View Terminal Tabs Help
[root@CAM-1 nac migration-4.7.0]# ./backup.sh
Warning: This migration utility will transform the current controlsmartdb
database into a release 4.7.0-compatible database temporarily and revert to
the original database afterwards. Cisco strongly recommends you create a
backup snapshot of your current configuration immediately prior to beginning
the migration process to release 4.7.0 and avoid performing any significant
configuration updates in your system until after the new hardware has been
configured to match your existing appliances and brought online.
Is the system backup taken and ready to continue? (y/n)? [n] y
Proceeding..
Saving the database
Stopping postgresql service: [ OK ]
1456723 blocks
Starting postgresql service: [ OK ]
Start upgrading database's encoding to UTF8...
Stopping postgresql service: [ OK ]
Starting postgresql service: [
                                0K
                                    1
Upgrading the database
DELETE 25
Restoring the database
Stopping postgresql service: [ OK
                                    1
Starting postgresql service: [ OK
/ /store/migration/nac_migration-4.7.0
Running /store/migration/nac_migration-4.7.0/bin/mktar /store/migration/nac_migr
ation-4.7.0/upgrade-pre-list /store/migration/nac_migration-4.7.0/upgrade-list
11
/store/migration/nac migration-4.7.0
NAM-10.134.0.2/
NAM-10.134.0.2/unpack.sh
NAM-10.134.0.2/restore.sh
NAM-10.134.0.2/UPGRADE.tar.gz
NAM-10.134.0.2/version
NAM-10.134.0.2/showstate.sh
NAM-10.134.0.2/upgrade-list
Done. Please copy NAM-10.134.0.2.tar.gz off to the new hardware.
                                                                                    7751
[root@CAM-1 nac_migration-4.7.0]#
```

Restore the Backup Snapshot

| Step 1 | Copy the snapshot file created in the /store/migration/nac_migration-4.7.0 directory of the |
|--------|---|
| | Release 4.1(8) CAM/CAS to the /store directory of Release 4.7(0) NAC Appliance. |

- **Step 2** To restore the snapshot, run the following commands in the 4.7(0) NAC Appliance using SSH or serial console.
 - **a.** To restore the snapshot, you need to stop the perfigo service by providing the **service perfigo stop** command.



For CAS, type the command as service perfigo maintenance to stop the perfigo service.

- **b**. Type cd /store to go to the /store directory.
- c. Create a directory named migration by typing the command mkdir -p migration.

- d. Move the snapshot to the migration directory by entering the command mv <SNAPSHOT_NAME.tar.gz> migration/.
- e. Go to the migration directory by typing cd migration/.
- f. Enter the command tar -xvzf <SNAPSHOT_NAME.tar.gz>.
- g. The tar command unzips the snapshot and creates a directory with the snapshot name.

Figure 4 illustrates the above commands for a standalone CAM snapshot.



- **Step 3** Type cd <snapshot_name> to go to the snapshot directory.
- **Step 4** Type the command ./restore.sh to restore the snapshot.
- **Step 5** The following warning message is displayed:

Warning: Please ensure that your Cisco NAC Appliance configuration has not changed significantly since beginning the hardware migration process from release 4.1.8 to release 4.7.0. Significant configuration updates performed during the migration process will be lost. The current settings on this appliance will now be changed so that they match the migration snapshot of the old appliance.

Continue with the migration? (y/n)? [n]

Press y to continue.

Step 6 When prompted, enter the master secret twice as shown in Figure 5.



The master secret in Release 4.7(x) is different from the shared secret used in 4.1(x). For more information, refer to "Verify/Change Current Master Secret on CAM/CAS" section in *Cisco NAC Appliance Hardware Installation Guide, Release 4.7.*



If your master secret is lost or becomes corrupted, use the procedure in "Recover From Corrupted Master Secret" section in *Cisco NAC Appliance Hardware Installation Guide, Release 4.7.*





Step 7 Once the restore is completed, the message "Restore done" is displayed as shown in Figure 6.

Figure 6 Restore completed

```
The master secret is used to encrypt sensitive data.
Remember to configure all HA pairs with the same secret.
Please enter the master secret:
Please confirm the master secret:
Restore done.
[root@nacmanager NAM-10.134.0.2]#
```

- **Step 8** Reboot the system by typing /sbin/reboot.
- **Step 9** Repeat the migration steps for all the CASs in the network.
- **Step 10** Bring up the new appliances on the network.
- Step 11 Access the CAM web console and install a valid FlexLM license file for the Clean Access Manager as described in the "Access the CAM Web Console" section of the Cisco NAC Appliance Hardware Installation Guide, Release 4.7.
- **Step 12** In the CAM web console, navigate to **Administration > CCA Manager > Licensing** to install any additional FlexLM license files for your Clean Access Servers, as described in the "Add Additional Licenses" section of the *Cisco NAC Appliance Hardware Installation Guide, Release 4.7.*
- Step 13 Verify connectivity by performing web login and/or Agent login from a client machine on the access network.

SSL Certificates Following Migration

Cisco NAC Appliance Release 4.7(x) no longer contains the "www.perfigo.com" Certificate Authority in the .ISO or upgrade image. Administrators requiring the "www.perfigo.com" CA in the network must manually import the CA from a local machine following installation or upgrade to Release 4.7(x).

22

In order to establish the initial secure communication channel between a CAM and CAS, you must import the root certificate from each appliance into the other appliance's trusted store so that the CAM can trust the CAS's certificate and vice-versa.

Migrate to NAC HA Systems

While migrating to HA Systems, you need to migrate each system in the HA setup. Follow the migration steps in each system to the corresponding system in 4.7(0). When you stop the perfigo service in HA setup, stop the service in the secondary system and then in the primary system.

- In the Secondary CAM, type service perfigo stop.
- In the Primary CAM, type service perfigo stop.
- In the Secondary CAS, type service perfigo maintenance.
- In the Primary CAS, type service perfigo maintenance.

After stopping the perfigo service, perform the migration steps provided for the standalone system. While bringing up the systems, bring up the primary system first and then bring up the secondary system.

After Migration



This section is intended for customers who previously implemented HA link-detect capabilities on their release 4.1(8) CAMs/CASs. If you want to enable the link-detect feature for your release 4.7(0) HA CAM/CAS deployment for the first time, see the "Configuring High Availability" chapter of the *Cisco* NAC Appliance Hardware Installation Guide, Release 4.7.

The CAS HA **Untrusted-side Link-detect** feature has been disabled by the migration tool kit during the restore process on the new platform, to avoid a possible packet looping issue in L2 virtual gateway deployment mode with the same IP address for both trusted and untrusted interfaces. Since it is impossible to correctly detect the deployment mode using only the CAS's configuration, link-detect on the untrusted side is disabled regardless of operational mode. To re-enable this feature, perform the following steps:

Step 1 Complete the migration process for the entire NAC setup. All CAMs and CASs should have been migrated successfully and the CAM should be able to manage all the CASs. The CAS HA pair should work with the primary CAS being in the Active node and the secondary CAS being in the Standby node.

Step 2 Log in to the primary CAS web console and navigate to **Administration > Network Settings > Failover**.

- a. Enter the target IP address in the Untrusted-side Link-detect IP Address field.
- b. Enter the new secondary peer's MAC addresses in the [Secondary] Peer MAC address fields.



The peer MAC address is used to filter out/block packet from looping between the two HA nodes' trusted and untrusted interfaces.

c. Click Update.

Log in to the secondary CAS web console and navigate to Administration > Network Settings > Step 3 Failover. Enter the target IP address in the Untrusted-side Link-detect IP Address field. a. b. Enter the new primary peer's MAC addresses in the [Primary] Peer MAC address fields only. Note Do not change/modify the [Primary] Peer Serial No. field. c. Click Update. Log in to the CAM web console and navigate to **Device Management > CCA Servers > List of Servers**. Step 4 Click the Manage icon next to the CAS that was just updated. Step 5 A warning message "SSKEY on server doesn't match the value in database" is displayed. Click Reset **SSKEY** to reset the key on CAS. Step 6 Repeat the above steps for all the CASs that have the **Untrusted-side Link-detect** disabled.

More Information

For more information on upgrading the earlier releases to Release 4.7(x) or later, refer to the "Upgrading to Release 4.7(x)" section in the *Release Notes for Cisco NAC Appliance* corresponding to your latest Cisco NAC Appliance release version.

For important information on interim releases 4.5(x) and 4.6(1), be sure to examine the new features and enhancements sections of the following documents:

- *Release Notes for Cisco NAC Appliance, Version 4.5(1)*
- *Release Notes for Cisco NAC Appliance, Version 4.6(1)*

For more information on using your new Cisco NAC appliances with 4.7(x), refer to the following documents:

- Cisco NAC Appliance Hardware Installation Guide, Release 4.7
- Cisco NAC Appliance Clean Access Manager Configuration Guide, Release 4.7(2)
- Cisco NAC Appliance Clean Access Server Configuration Guide, Release 4.7(2)

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2009 Cisco Systems, Inc. All rights reserved.