
Migrating from Cisco CAS 2.0.2

This document describes the process of migrating from Cisco Configuration Assurance Solution 2.0.2 to the equivalent OPNET solution.

This document assumes that you have all three of the following Cisco Configuration Assurance Solution (Cisco CAS) components and corresponding documentation installed:

- Cisco CAS Audit and Analysis
- Cisco Report Server
- Cisco Virtual Network Data Server

The following table describes how the Cisco CAS components correspond to the current OPNET release with a reference to the migration steps for each component.

Note—You must complete the migration steps for all three components to transition from Cisco CAS 2.0.2 to the equivalent OPNET releases.

Table IN-1 Cisco to OPNET Releases and Reference to Migration Steps

Cisco Release	OPNET Release	Component Migration Steps
Cisco CAS Audit and Analysis 2.0.2	IT Sentinel 14.5 PL1	Audit and Analysis Migration
Cisco Report Server 2.5 PL3	OPNET Report Server 2.5 PL3	Report Server Migration
Cisco CAS 2.0.2 Virtual Network Data Server	OPNET VNE Server 4.5	Virtual Network Data Server Migration
End of Table IN-1		

Audit and Analysis Migration

Migrating Cisco CAS Audit and Analysis 2.0.2 to OPNET 14.5 PL1

Step 1: Initiate Transition Program

Before uninstalling and migrating to OPNET products, you must initiate the transfer program by doing one of the following:

- Email: cisco_solutions@opnet.com
- Contact your OPNET Account Manager

Step 2: Identify Current Release Directories

- Before beginning the migration, make sure you know where your release directory (<reldir>) and administration directory (<admin_dir>) are located. If you don't know, follow [Procedure 1](#).

Procedure 1 Locating System Directories

- 1 Start Cisco Configuration Assurance Solution 2.0.
- 2 Choose Help > About This Application.
- 3 Select the Environment tab and expand the System Information node.
- 4 Note the following paths for future reference:
 - Cisco release directory
 - Admin directory (op_admin)

Note—The `cisco_cas_envdb2.0` file in the Admin directory (op_admin) subdirectory stores your preferences.

- 5 Quit.

End of Procedure 1

Step 3: Back Up Cisco CAS Audit and Analysis 2.0.2 Data

Typically, you might have stored projects and other data in one of the following “models” directories:

- Standard Model Directory—A directory created as part of the Cisco CAS installation (<reldir>/models/std. Although this is not the recommended place to store customized files, you might have saved data in this directory.
- User Home Directory—Recommended directory where user-specific administration, model, and report data is stored: op_admin, op_models, op_reports (for example, on a Windows platform, in C:\Documents and Settings\<username>).
- User Created—A directory that you create as a user and identified as a model directory using the `mod_dirs` preference.

Key Concept—When you login to the machine where Cisco CAS is installed, you have a user home directory that includes the following subdirectories: op_admin, op_models, and op_reports. These directories are separated from the installation directory for your use as a specific user.

Back up any data of the following types that you want to keep for future use.

Projects and Results

If you have any projects in the standard model directories (<reldir>/models/std) that contain analysis results or custom settings, copy the files to a separate backup directory.

Leave your op_admin, op_models, and op_reports directories as-is.

Cisco CAS Network Validation Rules and Templates

For Cisco CAS Network Validation rules and templates stored in standard model directories (for example, C:\Program Files\Cisco\CiscoCAS2.0\12.0.A\models\std\utilities\netdoctor), create a backup directory and copy them to it.

Cisco CAS Network Validation rules and templates stored outside the standard model directories can be left where they are.

Reports directory

Make a backup of the op_reports directory so that you can access the reports after migration.

Note—After migration, reports created with Cisco CAS cannot be opened from OPNET IT Sentinel. To open one of these reports, use a web browser to launch its index file from the backup directory.

Automation Tasks

If you scheduled automation tasks as a part of your Cisco CAS installation, you can also migrate their configuration if necessary. For example, you might have a Cisco CAS Network Validation audit that runs daily that you want to use.

For automation tasks stored in standard model directories (for example, C:\Program Files\Cisco\CiscoCAS2.0\12.0.A\models\std\utilities\netdoctor), create a backup directory and copy them to it.

Automation tasks stored outside the standard model directories can be left where they are.

Step 4: Uninstall Cisco CAS 2.0.2

Deregister licenses and uninstall all components of Cisco CAS 2.0.2 by following the procedures in Chapter 7 “Uninstalling Cisco CAS” of the *Installation Guide for Cisco Configuration Assurance Solution 2.0.2*.

Note—During this step:

- Do not remove the op_reports, op_models, and op_admin directories.
 - Do not remove Report Server.
-

Step 5: Obtain OPNET License(s)

After you deregister your Cisco license(s), request the equivalent OPNET license(s) by doing one of the following:

- Email: cisco_solutions@opnet.com
- Contact your OPNET Account Manager

You will need to provide your Cisco licensing information to obtain the equivalent OPNET licensing.

Step 6: Install OPNET IT Sentinel 14.0 PL3

Using the *Installation Instructions* supplied with the product:

- Install OPNET IT Sentinel 14.0 PL3 (software and models only).
- Register your licenses:
 - 1) Start OPNET IT Sentinel 14.0.
 - 2) Choose License > License Management.
 - 3) Click “Add License”.

Note—This release of IT Sentinel will be used only to perform intermediate conversions of model formats and product settings, after which you will remove it.

Note—The 14.0 license server installed with this software will automatically convert your license file to a new format. If you have other Cisco 2.0.x or OPNET 12.x (or earlier) products, they can get licenses from the 14.0 license server. 12.0 license servers will be unable to read the converted license file and should be replaced with a 14.0 license server.

Step 7: Migrate Your Cisco Product Settings

Preserve your Cisco product settings for use with OPNET IT Sentinel, as follows:

- 1) (Linux only) Edit the PATH environment variable on your computer:
 - a) Remove `Cisco CAS`.
 - b) Add `IT Sentinel`.
- 2) We recommend using a clean environment database to begin running your OPNET software. A clean file will be created automatically when you begin using your new software.

However, if you want to preserve the settings you are using with Cisco CAS, do the following:

- a) Rename the environment database (`cisco_cas_envdb2.0` in your `op_admin` directory) to `env_db12.0`.
- b) Launch IT Sentinel. The product settings (preferences) in the renamed environment database are migrated automatically.

Step 8: Convert Cisco CAS 2.0.2 Projects to OPNET 14.0 PL3 Format

Convert all custom projects you saved in Step 3. When you first open a project created in Cisco CAS 2.0.2, you will be prompted for node model conversion and model attribute conversion:

- 1) Click Yes to confirm the Node Model conversion.
- 2) Click Yes to confirm the Model Attribute conversion.
- 3) Save the project. This will confirm the changes and upgrade the project to 14.0 PL3.

Step 9: Uninstall OPNET IT Sentinel 14.0 PL3

Uninstall all components of OPNET IT Sentinel 14.0 PL3, as follows:

Windows

- 1) Log in as Administrator.
- 2) Use the Windows Add/Remove Programs utility to remove the following components:
 - OPNET Model Library 14.0
 - OPNET License Server 14.0
 - OPNET IT Sentinel 14.0

Linux

- 1) Log in as root.
- 2) Open a terminal window and execute the following commands:

```
% cd <usr_home>/14.0.A
% cd 'Uninstall_OPNET Model Library 14.0'
% ./Uninstall_OPNET_Model_Library_14.0
    (Click Uninstall, then click Done when uninstall is complete.)
% cd <usr_home>/14.0.A
% cd 'Uninstall_OPNET License Server 14.0'
% ./Uninstall_OPNET_License_Server_14.0
    (Uninstall is done in silent mode.)
% cd <usr_home>/14.0.A
% cd 'Uninstall_OPNET IT Sentinel 14.0'
% ./Uninstall_OPNET_IT_Sentinel_14.0
    (Click Done when uninstall is complete.)
```

Step 10: Install OPNET IT Sentinel 14.5 PL1

Using the *Installation Instructions* supplied with the product:

- Install OPNET IT Sentinel 14.5 PL1 (software, models, and documentation).

Step 11: Convert IT Sentinel 14.0 PL3 Projects to 14.5 PL1 Format

You can convert any of the custom projects you saved in Step 8 now or in the future. To convert a project, open it in OPNET IT Sentinel 14.5 PL1.

When you first open a project that was saved in 14.0 PL3 format, you might be asked if node model conversion and model attribute conversion should be performed:

- 1) Click Yes to confirm the Node Model conversion.
- 2) Click Yes to confirm the Model Attribute conversion.
- 3) Save the project. This will confirm the changes and upgrade the project to 14.5 PL1.

Additional Settings that Might Need To Be Reconfigured

- License server password (license_password preference)

-
- Report Server password (report_server_password preference)
 - Automation login settings (automation.password preference)
 - Any other OPNET-related passwords (SSL decryption, Naviscore, etc.)

Report Server Migration

Migrating from Cisco Report Server 2.5 PL3 to OPNET Report Server 2.5 PL3

The upgrade/conversion process consists of steps to export reports and settings from the Cisco installation for use in the OPNET installation. Report Server, in general, supports migration of reports, custom folders and filters from previous installations. Report Access, user account, and attribute visibility settings must be manually recreated.

Procedure 2 Migration Steps

- 1 In the existing Cisco Report Server installation, log in as admin and go to the Settings page. Note the settings for:
 - Report Access Control
 - User Account
 - Attribute Visibility
 - Searches

Note—You will need to manually restore these settings in the OPNET installation.
- 2 Install OPNET Report Server.
- 3 Log into OPNET Report Server and navigate to Settings > Migration.
- 4 Enter the path to the Cisco Report Server installation and select the checkbox for Migrate Custom Folders and Filters.
- 5 Press Verify to make sure the previous installation reports are valid.
- 6 Press Import to migrate reports.
- 7 Navigate to Settings and configure:
 - Report Access Control
 - User Account
 - Attribute Visibility
 - Searches

Note—These settings must always be configured again after an install or upgrade.

End of Procedure 2

End of Procedure 2

At this point, OPNET Report Server contains Cisco reports, user created folders/filters and is ready to receive reports from OPNET products.

Release Specific Conversion Issues

If you used the conversion process to move from a Cisco release that used Cisco Virtual Network Data Server 4.5.1, then any Cisco Virtual Network Data Server reports in the Cisco Report Server are also viewable in OPNET Report Server under the OPNET VNE Server product at both the Home page and View by Products page. No additional action is required to view the migrated Cisco reports.

If you used the conversion process to move from a Cisco release that used Cisco Virtual Network Data Server 6.0.2, the Cisco Virtual Network Data Server reports were published as Cisco Virtual Network Data Server reports and will not be visible in the Home page. They ARE visible in the View by Products page. To make these reports viewable at the Home page you need to do the following:

- 1) Add a Cisco Virtual Network Data Server folder at Home and refresh the page.
- 2) Add a Cisco Virtual Network Data Server filter.
- 3) At Home, edit sub-folders and apply the Cisco Virtual Network Data Server filter.

Contact OPNET Technical Support for assistance as needed.

Virtual Network Data Server Migration

Migrating Cisco CAS 2.0.2 Virtual Network Data Server to OPNET VNE Server 4.5 PL1

The migration process consists of manual steps to export data and settings from the Cisco installation for use in the OPNET installation. Depending upon the release you are moving to, you might be able to migrate user configuration settings (resource files) as well. The following table illustrates the supported resource migration scenarios.

Table IN-2 Resource Migration Table

Resource Migration From/To	VNES 6.0.2	VNES 6.5.1
VNDS 4.5.1	Yes	No
VNDS 6.0.2	No	Yes
End of Table IN-2		

Once you have decided what OPNET Guru or Sentinel release you will be using, the compatible OPNET VNE Server release is the one to transition to from the deployed Cisco release. If the VNDS and VNES releases are the same, you can migrate groups, device and platform info, helper files, and interface utilization, but you will need to reconfigure product settings in the OPNET VNE Server installation manually. If you are moving between upgradable releases in [Table IN-2](#), migration of everything except groups is automated.

Procedure 3 Migration Steps

- 1 In the Cisco installation, manually export groups. Use the steps below that are appropriate for the version of VND Server and database. Group information is exported to the following files: grp_list.txt, grp_mbrs.txt, and subgrp_mbrs.txt.

Export Group Data to Files (4.5 Oracle)

- 1.1 Open a command prompt and navigate to the VND Server 4.5 installation directory. Enter the following commands:

```
vnes_grp_list_export.bat <DB account> <DB password>
```

```
vnes_grp_mbrs_export.bat <DB account> <DB password>
```

```
vnes_subgrp_mbrs_export.bat <DB account> <DB password>
```

Note—<DB account> is the account used by the VND Server 4.x installation to access the Oracle database and <DB password> is the password for that account.

➔ Files are written to the VND Server 4.5 installation directory.

Export Group Data to Files (4.5 PostgreSQL)

- 1.1 Obtain the group_export.sql file from OPNET Tech Support and copy the file to the <vnds_install>\database\postgresql directory.
- 1.2 Open a command prompt and navigate to the following directory in the VND Server 4.5 installation directory: <vnds_install>\database\postgresql. Enter the following command:

```
<DSS_bindir>\psql -U dssuser -d vnes -f group_export.sql -v 1=grp_list.txt -v  
2=grp_mbrs.txt -v 3=subgrp_mbrs.txt
```

Note—<DSS_bindir> is the bin directory for the PostgreSQL installation (for example, C:\Cisco\DSS\PostgreSQL\8.2\bin)

- 1.3 When prompted, enter the password for the dssuser account.

➤ Files are written to the following directory:
<vnds_install>\database\postgresql

Export Group Data to Files (6.x PostgreSQL or Oracle)

- 1.1 Open a command prompt and navigate to the VND Server 6.x installation directory. Enter the following command:

```
vnes.bat DB_UTIL exportGroupData
```

➤ Files are written to the VND Server 6.x installation directory.

- 2 In the Cisco installation, manually export interface utilization data using the following steps. Open a command prompt and navigate to the VND Server installation directory. Enter the following command:

```
vnes.bat EXP_UTIL
```

➤ Files are written to the following directory in the Cisco installation:
<vnds_tempdir>\trafficExport

WARNING—The export of utilization data may take a significant amount of time to complete. The amount of time required depends on the amount of interface utilization data.

- 3 In the Cisco installation, manually export the device info file.
- 4 In the Cisco installation, make note of Authentication Settings and all local user accounts and roles.
- 5 In the Cisco installation, make note of Notification settings (if used).
- 6 In the Cisco installation, verify the database password. Use the steps below that are appropriate for the database that the software is configured to use. (The default database password for Cisco installations is CisCo123.)

Verify Database Password (PostgreSQL)

- 6.1 Select Start > Programs > PostgreSQL 8.2 > Command Prompt.

6.2 In the PostgreSQL command prompt, enter the appropriate psql command to connect to the database.

6.3 When the Data Storage Server listens on the default port, enter the following command:

```
psql -U dssuser -d vnes
```

6.4 If you chose a non-default listening port for the Data Storage Server when you installed VNE Server, enter the following command:

```
psql -U dssuser -d vnes -p <port>
```

6.5 Enter the password for the dssuser account when prompted.

➔ A welcome message displays when you successfully connect to the database.

6.6 Type \q at the vnes=> prompt to quit psql.

Note—If you are unable to determine the password for the database, contact OPNET Technical Support to obtain assistance in resetting the password for the dssuser account to a known value.

Verify Database Password (Oracle)

6.1 Open a command prompt.

6.2 Navigate to the VND Server installation directory.

6.3 Verify that you can login into Oracle using the VND Server database user account.

For a local Oracle database installation enter the following command:

```
sqlplus <user name>/<password>
```

For example, if the VND Server database user name and password are vnes and pwd respectively, enter:

```
sqlplus vnes/pwd
```

For a remote Oracle database enter the following command:

```
sqlplus <user name>/<password>@<DB TNS Service Name>
```

For example, if the VND Server database user name and password are vnds and pwd respectively, and the Database TNS Service Name is o92avnds, enter:

```
sqlplus vnds/pwd@o92avnds
```

6.4 Type quit at the SQL> prompt to exit.

6.5 An Oracle banner, and a “Connected To:” message appears when you successfully connect to the database.

Note—If you are unable to log in using the VND Server user account, consult Oracle documentation and/or contact Oracle Technical Support to obtain assistance in resetting the password for the VND Server user account to a known value.

-
- 7 Deregister your Cisco VND Server license by following the *Uninstalling License Server* procedures in Chapter 14 of the *Installation Guide for Cisco Configuration Assurance Solution 2.0.2*.

Note—Make sure you have a valid OPNET VNE Server license available before proceeding to the next step. If you need assistance, do one of the following:

- Email: cisco_solutions@opnet.com
- Contact your OPNET Account Manager

- 8 Install the OPNET VNE Server software release that you wish to use following the steps in the associated *OPNET VNE Server Installation Guide*.
- 9 Depending upon the specific Cisco and OPNET releases that you are moving between, work through one of Scenario 1 or 2. Scenario 1 supports automated migration of settings and data. Scenario 2 is a manual migration workflow.

Scenario 1 – automated migration:

- 9.1 If you are moving between releases supporting resource migration as listed in [Table IN-2](#):

-VNDS 4.5.1 to VNES 6.0.2

-VNDS 6.0.2 to VNES 6.5.1

the installer will provide a panel asking if you wish to migrate settings. Selecting “yes” will migrate:

-resource file settings

-device info

-helper files

-interface utilization (choose “no” – already exported in step 2)

- 9.2 Select “yes” when asked if you wish to migrate settings and complete installation. Select “no” for exporting interface utilization – this was already done in step 2.

For Scenario 1, continue with step 9.

Scenario 2 – manual migration:

- 9.1 If you are moving from the Cisco release to the same OPNET release (4.5.1 to 4.5.1 or 6.0.2 to 6.0.2) or skipping a release (4.5.1 to 6.5.1) then you must migrate manually:

-groups

-device info

-helper files

When done migrating the above items, you will need to manually reconfigure product settings using the VNE Server Mgmt Web.

For Scenario 2, continue with step 8.

-
- 10 Copy device info and text helper files from one installation to the other by opening a command window, navigating to the VNE Server installation directory and entering the following command:

```
vnes.bat FILE_MIG <Cisco install path> <OPNET install path>
```

- 11 Run CLEANALLDBSILENT by opening a command window, navigating to the VNE Server installation directory and entering the following command:

```
vnes.bat CLEANALLDBSILENT
```

- 12 Manually import device info file.
- 13 Configure the ASCII Generic Data Import adapter to import the group data exported from the Cisco installation. Ensure that the inputFile property for groupCreate, addNodeToGroup, and subGroupCreate corresponds to the appropriate files exported from Cisco VND Server (grp_list.txt, grp_mbrs.txt, and subgrp_mbrs.txt, respectively).
- 14 Configure Generic Interface Utilization Import to import the utilization data exported from the Cisco installation. Ensure that the path property points to the exported utilization files in <vnds_tempdir>\trafficExport (or location to which you copied exported utilization files).
- 15 Create local user accounts and configure Authentication.
- 16 Manually configure Notifications (if used).
- 17 If you were not able to perform the automated Scenario1 migration in step 7, then use the Mgmt Web to manually reconfigure the VNE Server product settings (resource files) at this time. This consists of the Adapter Schedule and any adapters and services that you use.
- 18 Refer to the Release Notes for the VNE Server version you are using and do any post-installation upgrade cleanup recommended in the Migration of Product Configuration section.

End of Procedure 3

Final Operation

At this point, you are now finished migrating from a Cisco Virtual Network Data Server installation to an OPNET VNE Server installation. Next steps are to start the product and build a network model, import any groups you have using Ascii Generic Data Import and import any interface utilization data you have using Generic Interface Utilization Import.