Cisco Configuration Assurance Solution Sentinel Tutorials

Software Release 11.5

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-7554-02

Cisco Configuration Assurance Solution
Sentinel Tutorials

Copyright

Document Copyright

Title: Sentinel Tutorials
Part Number: D00203
Version: 10

Software Copyright

Product Name: IT Guru
Product Release: 11.5

Documentation Conventions

OPNET documentation uses specific formatting and typographic conventions to present the following types of information:

- Objects, examples, and system I/O
- Object hierarchies, notes, and warnings
- Computer commands
- Lists and procedures

Objects, Examples, and System I/O

- Directory paths and file names are in plain Courier typeface:

  `opnet\release\models\std\ip`

- Function names in body text are in italics:

  op_dist_outcome()

- The names of functions of interest in example code are in bolded Courier typeface:

```
/* determine the object ID of packet's creation module */
src_mod_objid = op_pk_creation_mod_get (pkptr);
```

- Variables are enclosed in angle brackets (< >):

  `<opnet_user_home>/op_admin/err_log`

Object Hierarchies, Notes, and Warnings

Menu hierarchies are indicated by right angle brackets (>); for example:

Open File > Print Setup > Properties...

Attribute hierarchies are represented by angled arrows (↘) that indicate that you must drill down to a lower level of the hierarchy:

Attribute level 1 ➘ Attribute level 2 ➘ Attribute level 3

Note—Notes are indicated by text with the word Note at the beginning of the paragraph. Notes advise you of important supplementary information.

WARNING—Warnings are indicated by text with the word WARNING at the beginning of the paragraph. Warnings advise you of vital information about an operation or system behavior.

Computer Commands

These conventions apply to Windows systems and navigation methods that use the standard graphical-user-interface (GUI) terminology such as click, drag, and dialog box.

- Key combinations appear in the form "press **<button>+x**"; this means press the **<button>** and **x** keys *at the same time* to do the operation.
- The mouse operations *left-click* (or *click*) and *right-click* indicate that you should press the left mouse button or right mouse button, respectively.

Lists and Procedures

Information is often itemized in bulleted (unordered) or numbered (ordered) lists:

- In bulleted lists, the sequence of items is not important.
- In numbered lists, the sequence of items is important.

Procedures are contained within procedure headings and footings that indicate the start and end of the procedure. Each step of a procedure is numbered to indicate the sequence in which you should do the steps. A step may be followed by a description of the results of that step; such descriptions are preceded by an arrow.

Procedure FM-1 Sample Procedure Format

1 Procedure step.

➥ Result of the procedure step.

2 Procedure step.

End of Procedure FM-1

For more information about using and maintaining OPNET documentation, see the OPNET IT Guru Documentation Guide.

Contents

About the Tutorials in This Book

The tutorials in this book are the same tutorials that are delivered on the Documentation CD that comes with the OPNET software installation package. You can access the tutorials by choosing Help > Tutorials from the main menu of your OPNET application.

The tutorials are printed here in the same format as they appear online. This ensures page-by-page equivalency with the electronic version. Consequently, any hypertext links or action buttons that help you navigate the tutorials online are not active in the printed version. However, because it is frequently referenced from many of the tutorials, App A Troubleshooting Sentinel Tutorials on page TUT-A-1 has been included in this book.

For best results, do the tutorials in the order in which they appear in the book. The tutorials are in the same order in which they appear on the menus of the electonic version.

1 IT Sentinel Quick Start

IT Sentinel Quick Start

Introduction

IT Sentinel automatically performs tasks such as network configuration import, validation, and security analyses. The tasks run unattended at scheduled times and the results are available for viewing from the Report Server.

This tutorial gives an overview of the IT Sentinel workflow. You will perform the following:

1) Configure Device Configuration Import to import configuration files from a particular directory and save the settings for use during the automated run.
2) Configure NetDoctor to run a selected set of rules to identify relevant configuration errors, and save the NetDoctor settings for use during the automated run.
3) Set up an automation task to run the actions you specify within a schedule.
4) View the reports published to the Report Server during the automation run after the task completes.

Before You Begin

This tutorial can be performed independently or as part of a suite. If you are performing this tutorial as part of a suite, complete the tutorials in this order:

1) IT Sentinel Quick Start (this tutorial)
2) Setting Up Sentinel Automation
3) NetDoctor Notification in IT Sentinel
4) Using Flow Analysis with Sentinel
5) Comparing Networks with Sentinel
6) Working with the Report Server

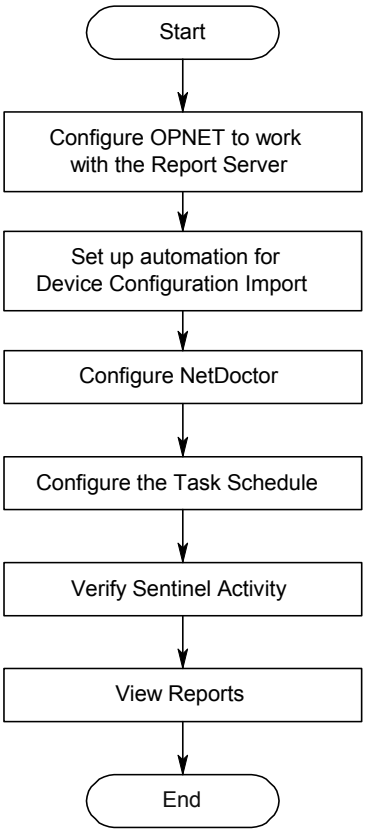
Prerequisite Tutorials

There are no prerequisite tutorials.

Tutorial Workflow

The following figure shows the workflow of the tutorial.

IT Sentinel Quick Start Tutorial Workflow



Configuring Report Server Preferences

The results of the automated task runs are published to the Report Server. Therefore, if you have not already done so, you must install and configure the Report Server. For information, see the Report Server User Guide.

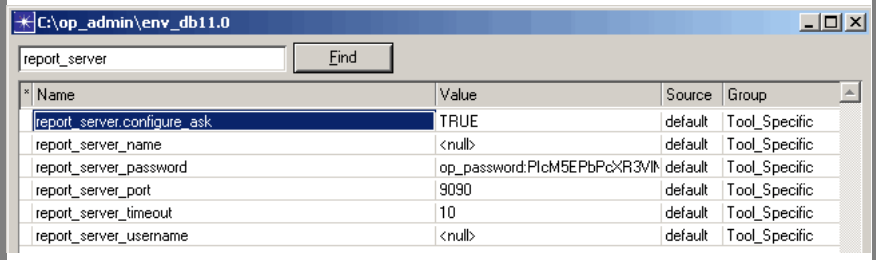
You must also ensure that the Report Server preferences are specified correctly in IT Sentinel. The IT Sentinel software prompted you the first time it was run for the name of your Report Server and the username and password that you should use when publishing reports. If you did not enter this information, or would like to verify your settings, choose **Edit > Preferences** and search for the string "**report_server**".

1. If IT Sentinel is not already running, start it.

2. Choose **Edit > Preferences** to open the **Preferences** dialog box.

3 Type **report_server** in the **Find** field and click the **Find** button.

➥ The Report Server preferences are listed in the dialog box.



4 Make sure that the computer on which the Report Server is running is listed in the value of the **report_server_name** preference, and that the correct port is listed in the value of the **report_server_port** preference.

Contact your system administrator if you are not sure about these values.

5 Also make sure that the username/password combination that is used to publish reports to the Report Server is specified correctly in the **report_server_username** and **report_server_password** preferences.

The username and password are provided by your Report Server administrator, who specifies this information in the Report Server

configuration file. For more information, see the Report Server Administration chapter of the Report Server *User Guide*.

6 Make any needed changes, and then click **OK** to close the **Preferences** dialog box.

Configuring Automation for Device Configuration Import

In this section, you configure the Device Configuration Import dialog box to import network configuration files from the correct location, and with the desired settings, for use during the automated run. Then, you save these settings to an automation settings file.

1. If IT Sentinel is not already running, start it.

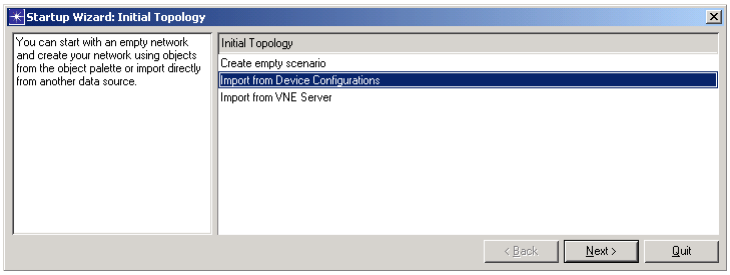
2. Select **File > New…**

3. From the pull-down menu, select **Project**, then click **OK**.

4. Enter **<your_initials>_Test** as the project name. Next, use the default name, **scenario1**, for the scenario name, then click **OK**.

   (When you save a file as part of a tutorial, it is good practice to include your initials in the file name. If multiple users perform the same tutorial, the initials ensure that each user has a unique copy and does not interfere with the work of others.)

5 The **Startup Wizard: Initial Topology** dialog box displays.



6 Select **Import from Device Configurations**, then click **Next**.

➥ The **Import Device Configurations** dialog displays.

7 Click in the first row of the table under the **Vendor** column. OPNET will create a new row for importing Cisco configuration files.

8 Click **Browse**.

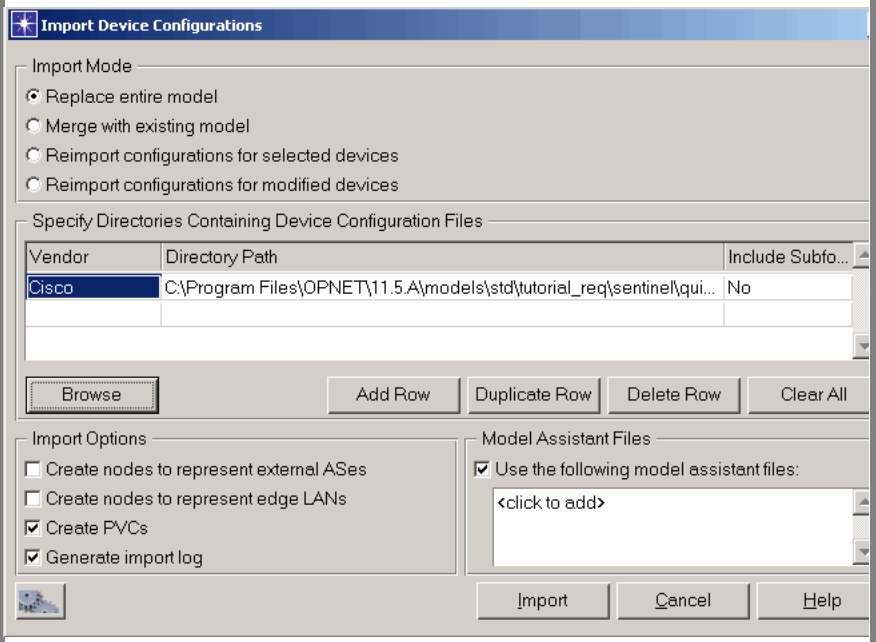
9 Choose the following directory:

<rel_dir>\models\std\tutorial_req\sentinel\quickstart_configs

<reldir> refers to the IT Sentinel release installation directory.

10 Click **OK**.

11 Select the **Generate Import Log** checkbox. This step is optional but can be helpful when troubleshooting.



12 Click the "**Save settings for automation**" button  in the bottom left corner of the dialog box.

➥ A file browser dialog box prompts you for the name of the automation settings file.

13 Select your default models directory from the directories listed on the left.

14 Type **<Initials>_DCI_Settings** in the **File name** field, and then click **Save**.

➥ Your Device Configuration Import settings are now saved.

This file will be used later when setting up the automation tasks.

15 You do not need to import device configurations at this time. (In later tutorials, you will learn how to test configurations as part of the automation workflow.) Click **Cancel** to close the **Import Device Configurations** dialog box.

➥ The blank scenario is now displayed.

Configuring NetDoctor Automation

NetDoctor identifies current or potential trouble spots in your network by applying selected rules to your network model and indicating how the network configuration deviates from the rules.

In this section, you will configure NetDoctor and save the settings for use during the automated task run.

1 Choose **NetDoctor > Configure/Run NetDoctor…,** or click the toolbar button  .

➥ The **Configure/Run NetDoctor** dialog box displays.

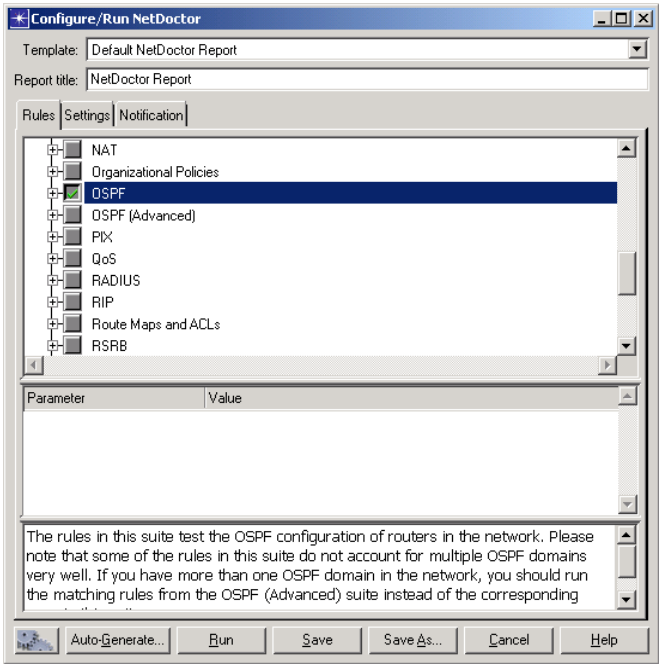
You are interested in running only the OSPF rule suite to check for OSPF-related configuration problems.

2 Select the **OSPF** tree branch in the **Rule Suites** treeview.

➥ All the OSPF rules are selected.

Make sure you do not select the tree branch **OSPF (Advanced)**.

You can click the "**+**" next to the OSPF tree branch to expand the tree and verify that all the OSPF rules are selected.



3 Click the **Settings** tab.

4 From the **Output Format** list, choose **Web Report**.

5 Make sure that the **Send report to Report Server** checkbox is checked.

6 Click on **Save As…**

➥ The **Save As** dialog box displays.

7 Select your default models directory from the directories listed on the left.

8 Enter **<Initials>_OSPF_Template** in the **File name** field, and then click on **Save**.

➥ Your OSPF-specific NetDoctor template is now saved in this file.

9 Click on the "**Save settings for automation**" button  .

➥ The **Save As** dialog box for the settings file displays.

10 Select your default models directory from the directories listed on the left.

11 Enter **<*initials*>_NetDoctor_Settings** in the **File name** field, and then click **Save**.

➥ Your NetDoctor settings are now saved in this automation task step file.

This file will be used in a later step when setting up the automation tasks.

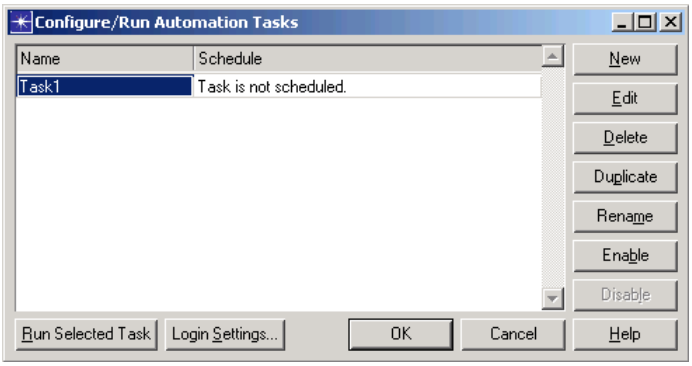
12 Click **Cancel** to close the **Configure/Run NetDoctor** dialog box, since you do not want to run NetDoctor at this time.

Configuring Automation Tasks

In the previous sections, you saved the Device Configuration Import and NetDoctor settings to use during the automated run. In this section, you will configure an automation task to use these settings and set up a schedule for running the task.

1 Open the **Configure/Run Automation Tasks** dialog box. To do this, choose **File > Automation > Configure/Run Automation Tasks,** or click the toolbar button  .

This dialog box lists the automation tasks that are currently configured. You can create, edit, or delete tasks using this dialog box.

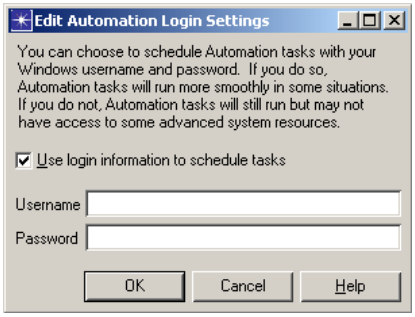


The default task, **Task1**, is selected.

2 (Optional) Configure the login settings that IT Sentinel will use to execute the automation tasks.

2.1 Click on the **Login Settings** button in the Configure/Run Automation Tasks dialog box.

2.2 Fill in the **Edit Automation Login Settings** dialog box, shown below.



2.3 Click **OK** to return to the Configure/Run Automation Tasks dialog box

3 Click in the **Name** column of the task table and then rename the task ***<initials>*_Quickstart**.

4 Click **Edit** to configure this task.

➥ The **Edit Task Details** dialog box displays.

5 In the **Task Steps** table, you can specify the number and sequence of steps that you want to include in the automation task. Click on the first row in the **Task Step Type** column and then hold down the mouse button.

➥ The available types of automation task steps display.

6 Create two steps in the following order:

- Import Topology from Device Configurations
- Generate NetDoctor Report

6.1 Select **Import Topology from Device Configurations** from the list.

6.2 Click on the first row in the column, **Automation Settings File**.

➥ The available Device Configuration Import settings files display.

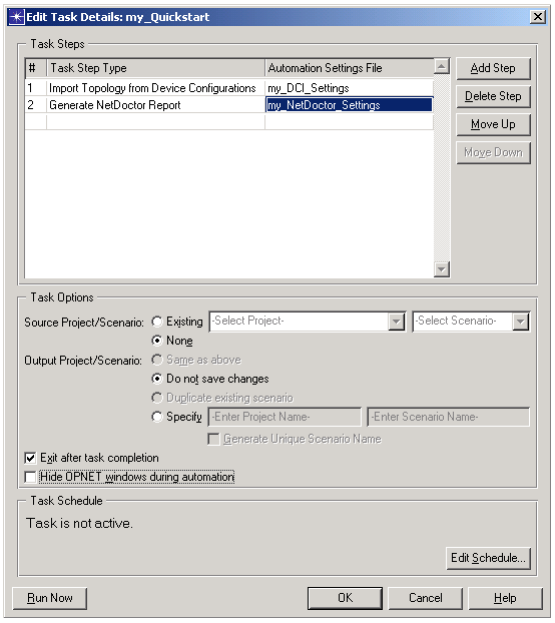
6.3 Select the **<*Initials*>_DCI_Settings** file, which you saved earlier in this tutorial.

6.4 To add the second step, click **Add Step**.

➥ Another row is added for the second task step.

6.5 Click in the **Task Step Type** column of the second row, and then select **Generate NetDoctor Report** from the list.

6.6 Click on the second row in the **Automation Settings File** column, and then select **<*Initials*>_NetDoctor_Settings** from the list.



7 Select the **None** option for the **Source Project/Scenario** task option, and **Do not save changes** for the **Output Project/Scenario** task option.

➥ When the task runs, a new (blank) project and scenario will be used. After the automation run, the project will not be saved.

8 Verify that the **Exit after task completion** checkbox is selected.

This specifies that IT Sentinel should exit after the automation run.

9 Verify that the **Hide OPNET windows during automation** checkbox is not selected.

Typically, you would leave this option selected since you normally run Sentinel in an automated and unattended mode; therefore, you do not want its windows appearing on the screen.

However, for purposes of running this tutorial and knowing when Sentinel finishes, you will turn this option off.

You have now specified the steps that will be executed as part of this automation task and the task options. Next, you will schedule the task to run daily at a specified time.

If you are not logged in as an administrator, you must configure your username and password prior to scheduling tasks.

1. Click the **Edit Schedule…** button.

   ➥ The **Edit Task Schedule** dialog box displays.

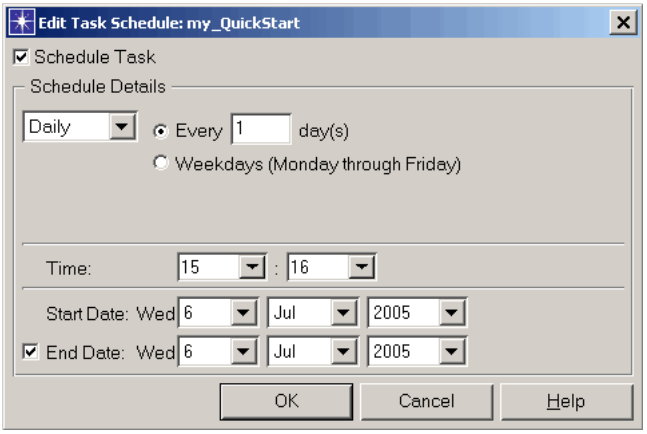
2. Make sure the **Schedule Task** checkbox is selected.

3. Select **Daily** in the **Schedule Details** pop-up menu, and then select **Every 1 day** for the frequency at which the task will run.

4. Specify the time at which the task will run by selecting the hour and minutes in the **Time** pop-up menus.

   Specify the time to be **2 minutes** from the current time. For example, if the current time is 2:15 pm (14:15), select 14:17 in the **Time** pop-up menus.

5 Specify the **Start Date** to be the current date.



6 Select the **End Date** checkbox and specify the end date to be the current date. This will ensure that your tutorial automation task will run today only. If this checkbox is cleared, the task will run every day indefinitely.

7 Click **OK** to close the **Edit Task Schedule** dialog box.

8 Click **OK** to close the **Edit Task Details** dialog box.

9 Click **OK** in the **Configure/Run Automation Tasks** dialog box.

The configured automation tasks are now scheduled and the **Configure/Run Automation Tasks** dialog box closes.

The automation task is scheduled to run 2 minutes from now.

10 Select **File > Exit**, and choose not to save the project when prompted.

➥ In a few minutes, Sentinel will run and execute your scheduled automation task.

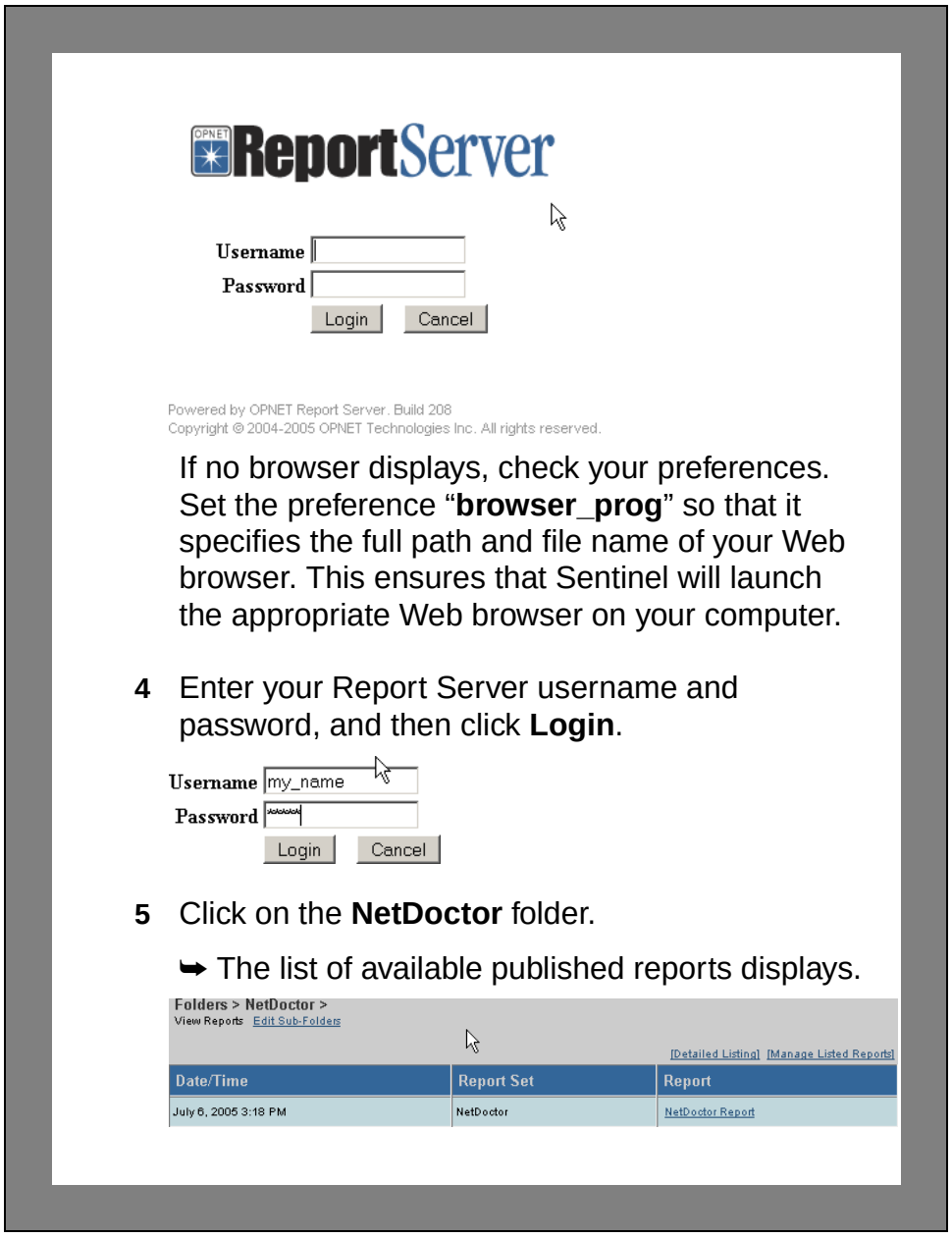
11 Wait for the automation task to finish.

Viewing Reports in the Report Server

When the automation task executes at the specified time, the network device configurations are imported into a temporary project and the selected NetDoctor rules are applied. The results of the NetDoctor run are saved in a Web report and published to the Report Server.

In this section, you will view the published NetDoctor report in the Report Server.

1. Wait a few minutes after the automation task has ended to ensure the report has been published.
2. Start IT Sentinel.
3. Select **Automation > Web – Open Report Server Home**.
   ➥ A browser window displays the Report Server home page.



If no browser displays, check your preferences. Set the preference "**browser_prog**" so that it specifies the full path and file name of your Web browser. This ensures that Sentinel will launch the appropriate Web browser on your computer.

4 Enter your Report Server username and password, and then click **Login**.

5 Click on the **NetDoctor** folder.

➥ The list of available published reports displays.

6 Find the NetDoctor report with a date/time that corresponds to your scheduled automation run, and then click on the report name.

➥ The NetDoctor report displays in a new browser window.

7 View the Web report.

The Executive Summary report shows that there are several OSPF errors.

Summary

With IT Sentinel, you can automatically perform network configuration import, validation, and reporting.

In this tutorial, you learned how to:

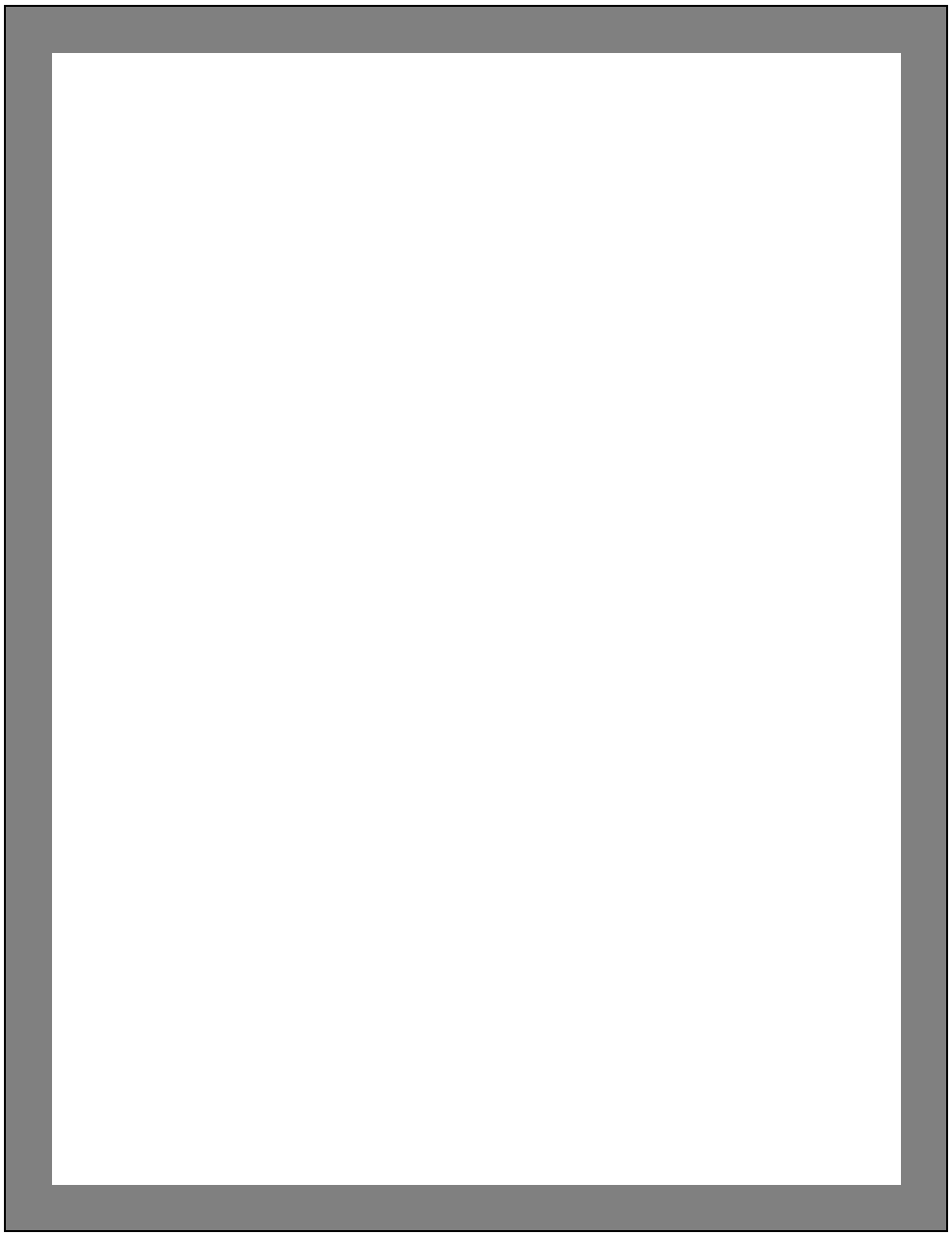
- Configure automation for Device Configuration Import
- Configure automation for NetDoctor
- Schedule and run automation tasks
- Set preferences for the Report Server and view reports from the Report Server

If you have any problems, use the **Automation > Open Automation Log Manager** menu to view the automation logs. The logs will tell you if there was a configuration problem.

What's Next?

Other tutorials are available on the following topics:

- Setting Up Sentinel Automation
- NetDoctor Notification in IT Sentinel
- Using Flow Analysis with Sentinel
- Comparing Networks with Sentinel
- Working with the Report Server



2 Setting Up Sentinel Automation

Setting Up Sentinel Automation

Introduction

IT Sentinel provides the capability to perform tasks such as network configuration import, validation, and security analyses automatically. The tasks run unattended at scheduled times, and the task results are available for viewing from the Report Server.

This tutorial shows how you can use IT Sentinel to do the following:

- Configure, modify, and automate Device Configuration Imports
- Configure, verify, refine, and automate NetDoctor analyses
- Create and schedule an automation task
- Execute and verify an automation task

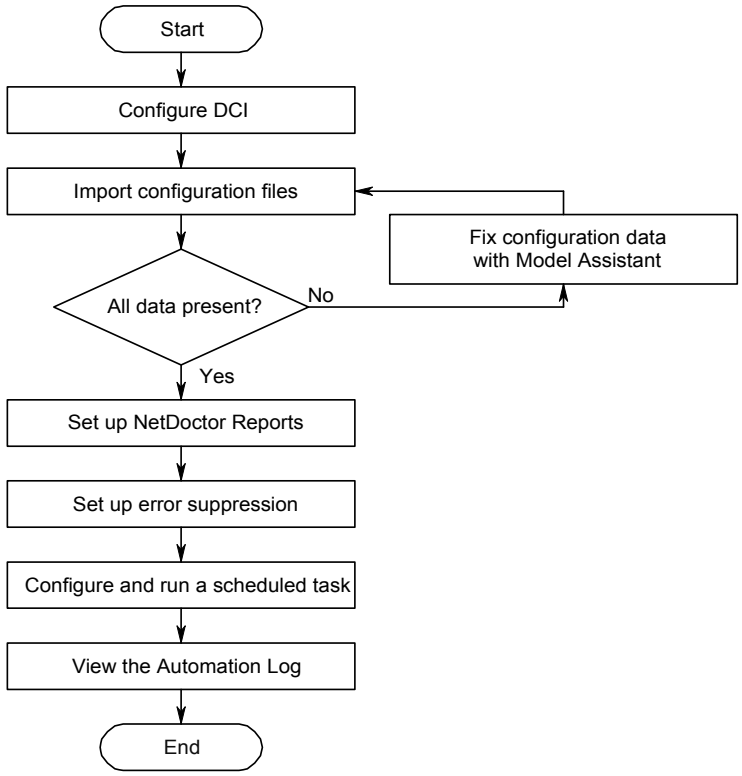
Prerequisite Tutorials

To learn the topics presented in this tutorial effectively, complete the IT Sentinel Quick Start tutorial before you do this tutorial.

Workflow

The following figure shows the workflow of this tutorial.

Workflow for Setting Up IT Sentinel Automation



Tutorial Objective

Middletown Bell provides local phone service and Internet access to one million homes and businesses. Your department is responsible for monitoring the state of the network and repairing any system outages. You would like to be more proactive in detecting and fixing potential problems before they cause problems for your customers. As part of this effort, you will use IT Sentinel to routinely import your network to test the configuration.

First, you will configure an automation task that will run each night. Then you will test the task to verify that it works as expected. To accomplish this

1) Create an automation file to import your device configuration files
2) Use the Import Assistant to solve problems related to the import
3) Configure NetDoctor to do configuration checks
4) Schedule an automation task to run the network configuration tests

Configuring the Network Import

Given that you want to automate a network checkup each night, you must first configure IT Sentinel to import your current network configuration. Once the configuration has been imported, an automated NetDoctor process can validate it.

To create an automation file that stores information about your network import, do the following:

1. Choose **File > New…**
2. Select **Project** from the pull-down menu, and click **OK**.
3. Accept the default project name, then click **OK**.
4. Click **Quit** to exit the Startup Wizard.
5. Choose **Topology > Import Topology > From Device Configurations…**

   ➥ The **Import Device Configurations** dialog box appears.

   You will be importing Cisco router configurations to produce an up-to-date topology. Before setting this up as an automated task, you need to do the import manually. This validates the import.

5.1 Click in the first row of the table under the **Vendor** column. OPNET will create a new row for importing Cisco configuration files.

5.2 Click **Browse**.

5.3 For this lesson, there is a set of ready-made router configuration files. Choose the directory **<reldir>\models\std\tutorial_req\module\configs\with_areas_broken** and click **OK** (**Select** on UNIX platforms).

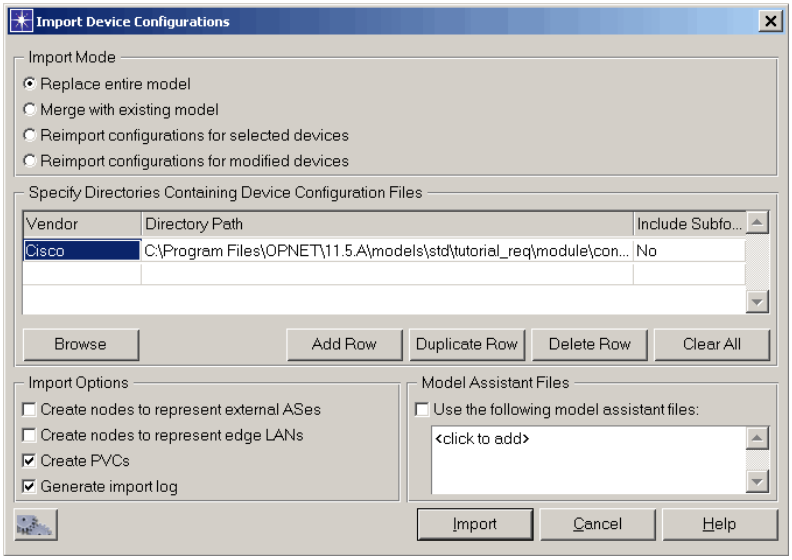
➥ The file browser closes and the **Cisco** row of the **Import Device Configurations** dialog box shows the correct directory path.

5.4 Make sure that the **Create PVCs** checkbox is selected.

5.5 Select the **Generate Import Log** checkbox. This step is optional but can be helpful when troubleshooting.

5.6 If any files are listed under **Model Assistant Files**, remove them by clicking on each file and selecting **NONE**, or you can save time by unchecking the **Use the following model assistant files** check box.

5.7 The completed dialog box should look similar to the figure below:



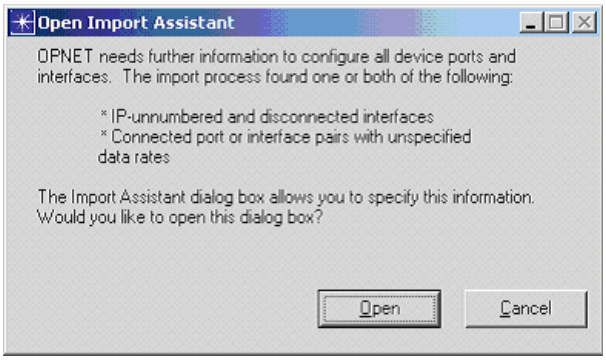
5.8 Click **Import**.

➥ IT Sentinel finds the configuration files and imports them.

While importing the files, IT Sentinel checks your model directories for node models that match the devices you are importing. If

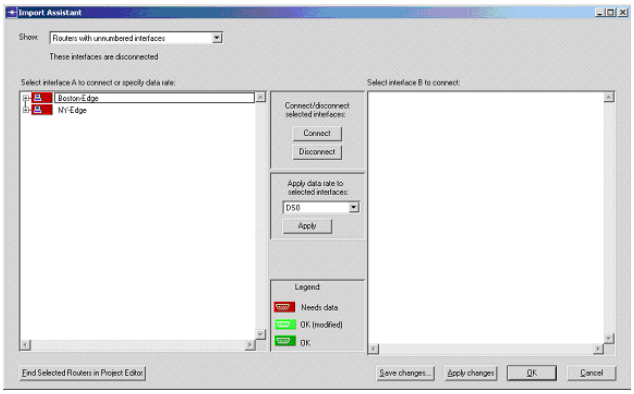
IT Sentinel does not find a matching node model for a device, it creates one during import.

➥ The **Open Import Assistant** dialog box opens. This happens when IT Sentinel cannot find some of the information it needs from the configuration files being imported.



5.9 Click **Open**.

➥ The **Import Assistant** dialog box displays.



Correcting the Configuration Import with the Import Assistant

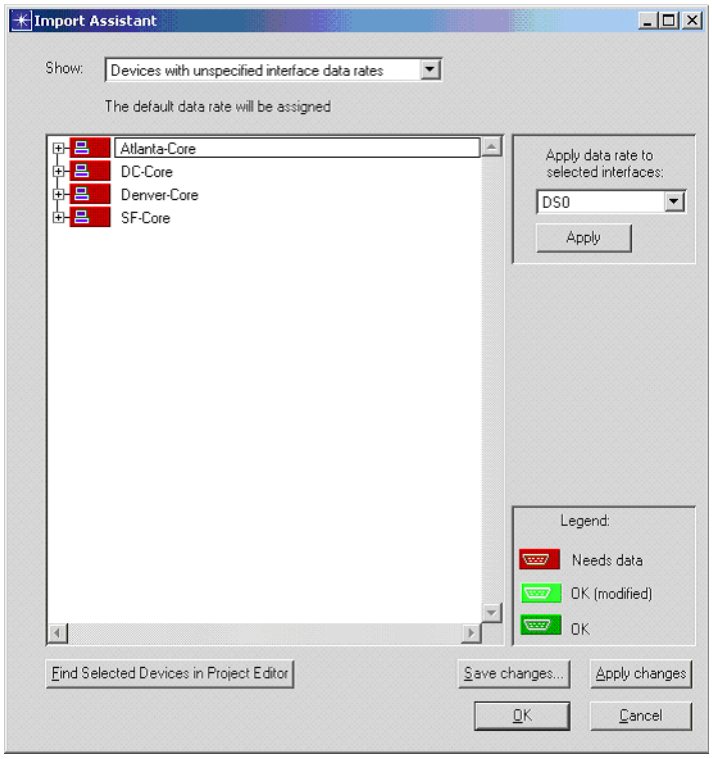
The Import Assistant lets you specify information that is required to build a correct network model. The information is saved in a model assistant file named **<project-name>-<scenario-name>.ma** and can be applied automatically when you import the router configuration again. You will follow this workflow when using the Import Assistant:

- Examine the dialog box to understand the information presented
- Correct problems with unnumbered interfaces
- Correct problems with data rates
- Verify that all routers are connected correctly

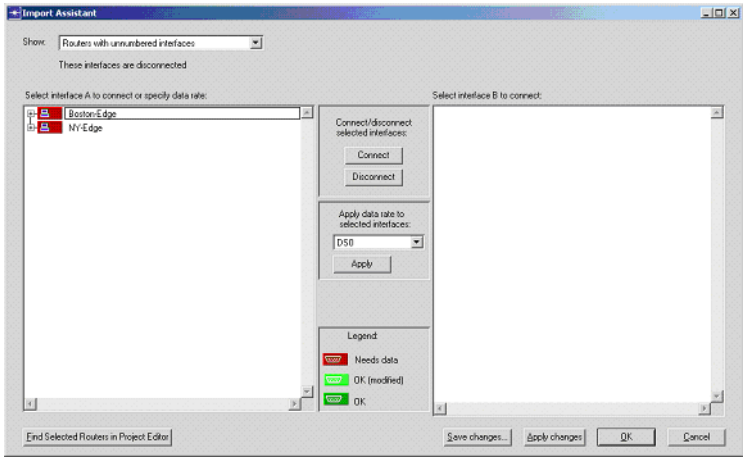
1 The **Show** drop-down list controls which routers appear in the pane below it.

1.1 Select the **Devices with unspecified interface data rates** option and notice that four routers (Atlanta-Core, DC-Core, Denver-Core, and SF-Core) are listed. This means that IT Sentinel did not find interface data rates in the router configuration import

file for at least one interface on each of these routers. You must supply the information for these four routers.



1.2 Select the **Routers with unnumbered interfaces** option and notice that the Boston-Edge and NY-Edge routers are shown in red. You must supply information about those two routers.



Correcting Problems with Unnumbered Interfaces

When IT Sentinel imports a router configuration file, it determines how a router is connected by analyzing the IP addresses of the router interfaces. If an interface does not have an IP address, IT Sentinel cannot determine where the interface should be connected and leaves it unconnected. As the system administrator, you can provide this information to IT Sentinel.

Follow these steps to supply the missing information.

1. Verify that the **Show** drop-down list shows **Routers with unnumbered interfaces**.

2. Expand the Boston-Edge router.

   ➥ Observe the router ports.

   Notice the phrase **<unconnected>** in the **Connected to** column for the Serial0/1 port.

3. Expand the Serial0/1 port, and click on **(<IP unnumbered>)**.

   ➥ The NY-Edge router appears in the **Select interface B to connect:** pane.

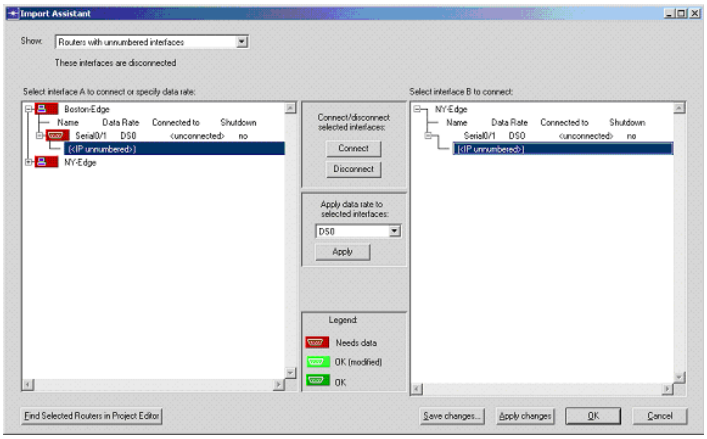
NY-Edge also has an unconnected interface, so IT Sentinel is suggesting that the two unconnected interfaces could be connected to each other.

This tutorial presents the simple case of two disconnected interfaces. In a production network, you might have multiple disconnected interfaces (all would be listed in the **interface B** pane), and you might have to examine the router configurations to determine the correct connections.

4 Select the IP address for NY-Edge (**<IP unnumbered>**).

4.1 In the **interface B** pane, expand NY-Edge.

4.2 Select the IP address (**<IP unnumbered>**) for port Serial0/1 of NY-Edge.



5 Click the **Connect** button.

➥ Both routers with disconnected interfaces are now connected. The router icons change from red to light green.

Correcting Problems with Unspecified Data Rates

When IT Sentinel imports a router configuration file, it determines the interface data rate by obtaining the rate from the file or by inferring the rate from the interface technology specified in the file. For example, an ATM interface is assumed to have an OC3 data rate.

When IT Sentinel infers the data rate this way, the routers that might need to be corrected are listed in the Import Assistant dialog box. This allows you to change the data rate if the inferred rate is incorrect.

In this tutorial, you will change the rate for one interface and confirm the inferred rate for the other three interfaces. You will then save the import assistant file with this information.

1. In the **Show** drop-down list, select **Devices with unspecified interface data rates**.

2. Expand all the routers.

   ➥ The router interfaces appear.

   Notice that each interface has a data rate of SONET/OC3.

3 Change the data rate to SONET/OC1 for the Atlanta-Core interface.

3.1 Expand the Atlanta-Core interface (ATM0/0) to see its IP address.

3.2 Select the interface. You can select either the name or the IP address.

3.3 In the **Apply data rate to selected interfaces** drop-down list, select **SONET/OC1** and click **Apply.**

➥ The new rate is applied to the interface and the router icon becomes light green. The light green indicates that you modified the router configuration.

4 Confirm the SONET/OC3 data rate for the DC-Core interface.

4.1 In the **Apply data rate to selected interfaces** drop-down list, reset the data rate to **SONET/OC3**.

4.2 Select the DC-Core interface (ATM1/0).

4.3 Click **Apply**.

➥ The router icon becomes light green.

5 Confirm the SONET/OC3 data rate and click **Apply** for the Denver-Core interface and the SF-Core interface.

6 Click on **Apply Changes**.

Verifying Other Configuration Details

Follow these steps.

1 Select **All devices** from the **Show** drop-down list and verify that all router icons are green.

➥ Some router icons appear light green, if you modified their configurations.

2 Click **Save changes...**

3 Change the name of the file to **<initials>_daily_model_assistant**, then click **OK.**

4 Click **OK** in the **Import Assistant** dialog box.

➥ The **Import Assistant** dialog box closes.

5 Observe the information in the **Import Summary (Concise)** dialog box. This report provides brief information about the import that was just run including any modifications performed with the **Import Assistant.**

6 Close the **Import Summary (Concise)** dialog by clicking **Close**, or click on **View Details** to see a full text report.

➥ The **Import Summary** dialog box closes.

Now the network topology is complete. IT Sentinel has chosen router and link models and configured model attributes according to the information in the router configuration files.

Testing the New Import

You have already manually imported the topology and created a model assistant file that includes information needed to ensure a smooth import. In this section you see how to specify the model assistant (**.ma**) file you created.

1. Choose **Topology > Import Topology > From Device Configurations...**

   ➥ The **Import Device Configurations** dialog box appears.

2. Check the **Use the following model assistant files** checkbox, and then click on **<click to add>** in the **Model Assistant Files** pane.

   ➥ A file list displays.

   Notice that the model assistant file you just saved appears in the list.

3. Select the file **<initials>_daily_model_assistant.**

4. Click **Import**.

   Notice that IT Sentinel imports the topology without assistance from you.

Saving the Import Settings for Automation

Now that you have tested your import settings manually, you can be confident that the import will work correctly when it is done as part of an automation task.

To save the settings for use in an automation task, do the following:

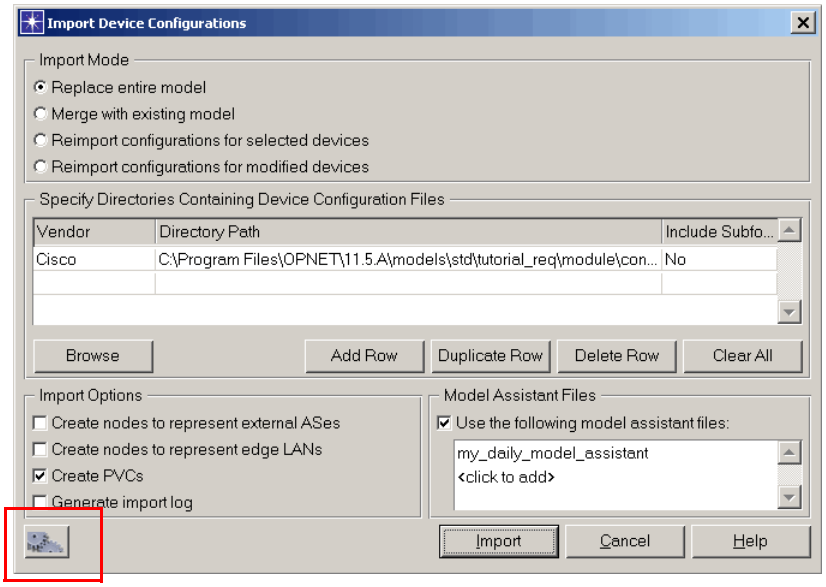
1. Choose **Topology > Import Topology > From Device Configurations…**

   ➥ The **Import Device Configurations** dialog box appears.

2. Uncheck the **Generate Import Log** box.

3. IT Sentinel saved the settings from the previous import. You want your automated task to use these settings regardless of any imports that have been done before. To do this, you must save your settings to an automation (**.af**) file, as follows:

3.1 Click the automation save button. This is the button with a picture of a gear box.



3.2 At the prompt, name your automation file **<initials>_daily_dci_import** (use a name that describes the purpose of the file).

3.3 Make sure your default models directory is selected in the Model directory panel on the left, then click **Save** to save the file.

3.4 Click **Cancel** to close the **Import Device Configurations** dialog box.

Configuring NetDoctor

Your automation task will have two parts: importing the topology and validating the topology by running a suite of NetDoctor rules. In previous steps, you configured the import part of your task. Now, you will configure NetDoctor to run the rules that interest you.

1 Choose **NetDoctor > Configure/Run NetDoctor…**

➥ The **Configure/Run NetDoctor** dialog box opens.

2 You want to begin with a blank template, so verify that the **Template** is set to **Default NetDoctor Report**.

3 In the network you are studying, you are interested primarily in verifying that the IP and OSPF settings are correct.

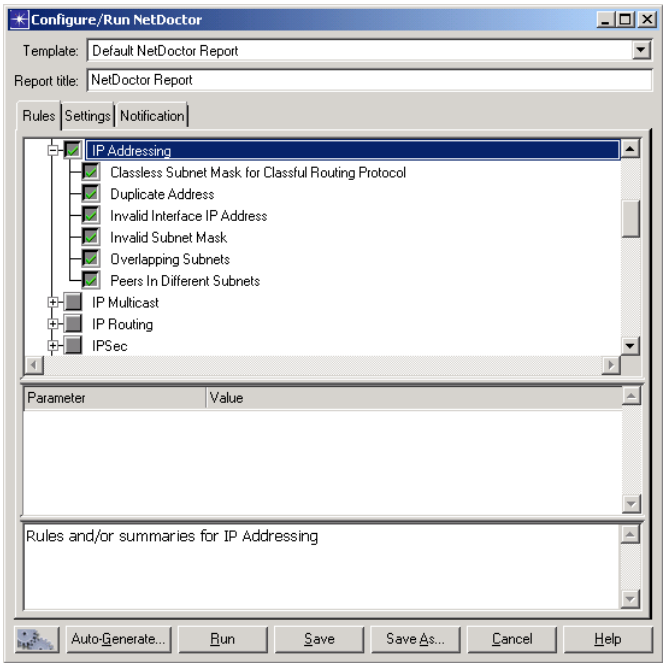
3.1 Scroll down to the **IP Addressing** rule suite. This is a collection of rules that test common errors related to IP address configurations.

3.2 Expand the **IP Addressing** rule suite, which contains several rules.

After inspecting the rules, you decide to include all of them in your study. Click on **IP Addressing** to select the entire rule suite.

3.3 Make sure there is a green checkmark next to **IP Addressing.**

If there is a green dot or no mark at all, click on **IP Addressing** again to select it. The green checkmark means that all the rules in the suite are selected.



3.4 Scroll down to the **IP Routing** rule suite.

3.5 Expand the **IP Routing** suite, then click on **IP Routing** to select all the rules in that rule suite.

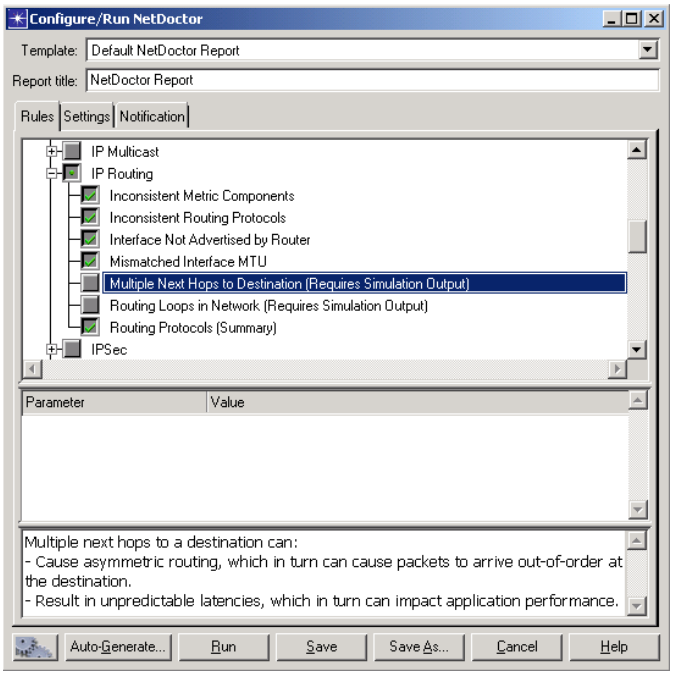
3.6 Note that two options (**Multiple Next Hops to Destination** and **Routing Loops in Network**) require output from Flow Analysis. You will not be running Flow Analysis in this tutorial.

Click on **Multiple Next Hops to Destination** to turn off that rule.

➥ The green checkmark next to **IP Routing** changes to a green dot.

This shows that some, but not all the rules in the suite are selected.

3.7 Click on **Routing Loops in Network** to turn off that rule.



3.8 Scroll down to the **OSPF** rule suite.

3.9 Click on **OSPF** to enable all the rules in that suite.

➥ A green checkmark appears next to **OSPF**.

4 The report title—as it will appear in your report and on the report server—is at the top of the dialog box.

To help you distinguish between reports, you should give your new NetDoctor report a meaningful title.

Replace the default title with **IP and OSPF Configuration**.

5 Now that you have configured your report template, you need to save it.

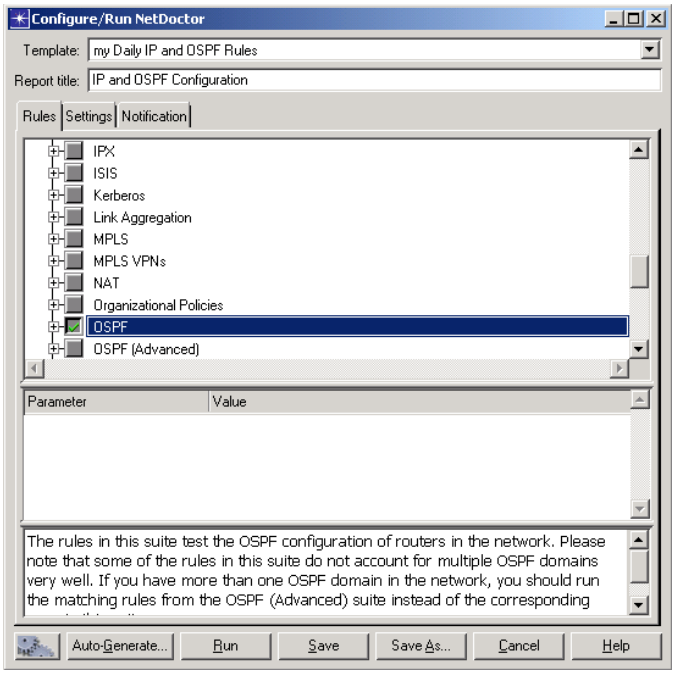
5.1 Click **Save As…**

5.2 When prompted, enter **<initials> Daily IP and OSPF Rules** for the file name.

5.3 Verify that your default models directory is selected in the left pane, then click **Save**.

➥ The report template is saved.

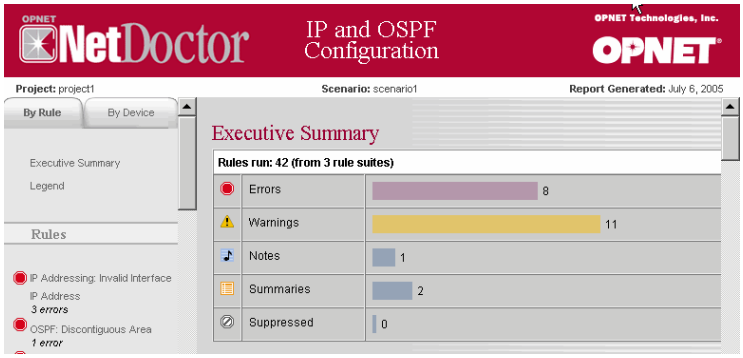
The dialog box should now look similar to the one below.



6 To test your NetDoctor template, click **Run**.

➥ IT Sentinel runs each of the rules you specified in your template.

7 After the rules complete, the report appears in a web browser.



8 From the **Executive Summary**, you can see that NetDoctor found several errors and warnings. The legend on the left shows the errors and warnings generated by multiple rules.

Refining the NetDoctor Results

When you review your NetDoctor report, you may find errors or warnings that are not of interest to you.

For example, NetDoctor may warn you about a configuration error of which you are already aware but that you do not plan to fix immediately. If you do not want this error to appear in each report, you can choose to turn off the rule that reports the error. However, this means that the rule will be skipped for all devices. If you want to turn off rule results for specific devices only, you can use a suppression file to list all the error messages you want omitted from your report.

In the left pane, you see that NetDoctor reported three invalid IP addresses. You suspect that these errors are not important to your network's operation.

1. To view the specific error messages, click on **IP Addressing: Invalid Interface IP Address.**

   ➥ The specific rule report appears.

2. The three errors apply to Ethernet interfaces on three routers: DC-Edge, Denver-Edge, and Seattle-Edge. You know that these three routers are no longer connected to Ethernet links.

Because these errors are not important, you want to suppress them in future NetDoctor reports.

2.1 Close the web browser.

2.2 In IT Sentinel, choose **NetDoctor > Suppress Messages…**

➥ The **Edit Suppressions** dialog box will open.

2.3 Verify that **<initials> Daily IP and OSPF Rules** is the selected report.

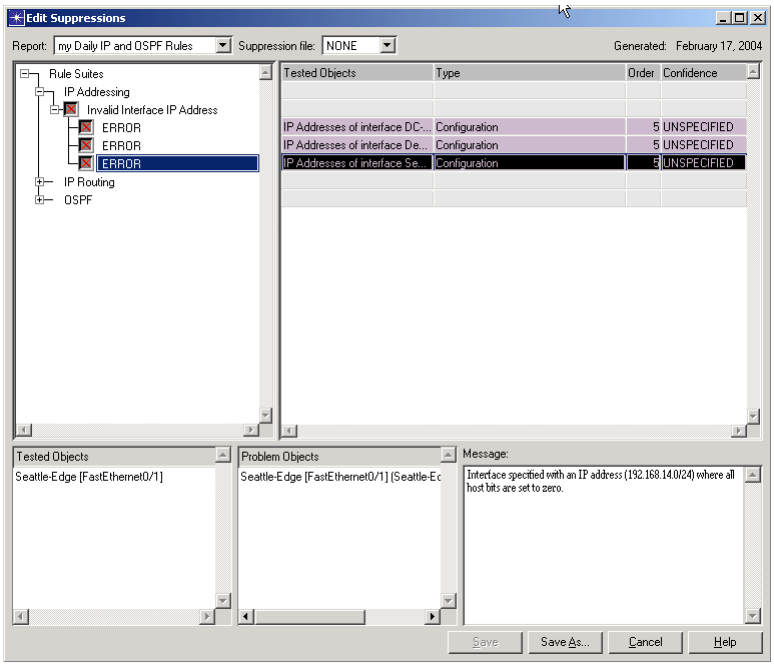
This is the report template you want to use when selecting rules to suppress.

2.4 The errors you would like to suppress are generated by the **Invalid IP Address** rule. Expand **Rule Suites > IP Addressing > Invalid Interface IP Address.**

➥ There are three errors listed. These are the three that you want to suppress.

2.5 Select all the errors under **Invalid Interface Address.**

➥ A red 'X' appears next to each error.



2.6 To save this information to a suppression file, click **Save As…**

2.7 When prompted, enter **<initials>_ip_addressing** for the file name and click **Save**.

2.8 Click **Close** to close the dialog box.

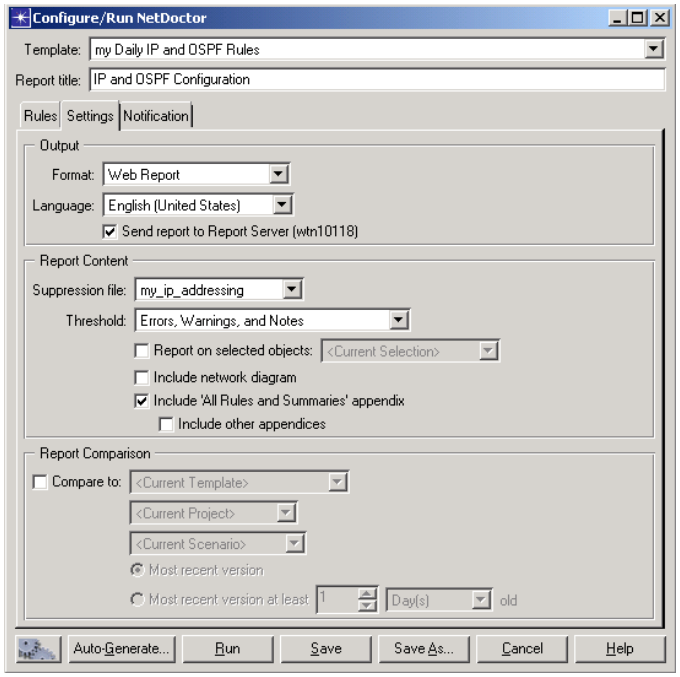
3 Now that you have a suppression file, you must modify your template to use the file.

3.1 Choose
NetDoctor > Configure/Run NetDoctor…

4 Verify that **<initials> Daily IP and OSPF Rules** is the selected template in the template field.

4.1 Click on the **Settings** tab.

4.2 Click on the **Suppression file** pull-down menu and select **<initials>_ip_addressing**.

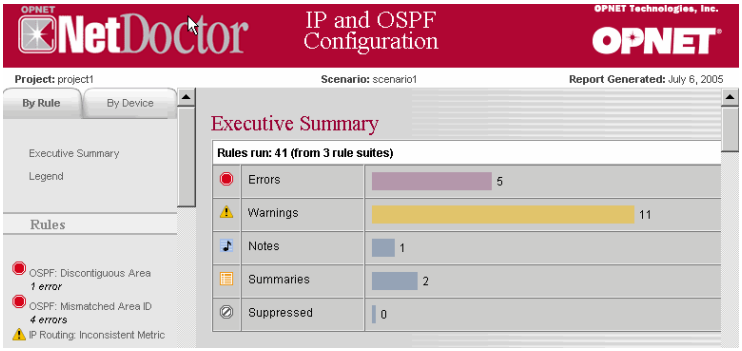


4.3 Click **Save** to save the changes to your template.

5 To verify that this template generates the report you want, click **Run** to test the changes.

6 When the report appears, note that the IP addressing errors no longer appear in the legend.

The **Executive Summary** now shows that three errors are suppressed; the other errors appear as before.



7 Close the web browser.

Now that you have configured and verified a NetDoctor analysis run, you want to save its settings to an “automation task step” file. This file enables you to use this analysis in an automated run.

1 Select
NetDoctor > Configure/Run NetDoctor...

2 Make sure that
<initials> Daily IP and OSPF Rules is the selected template in the top pull-down menu.

3 Click on the **Save current settings for automation** button. 

4 At the prompt, name your automation file **<initials>_Daily_IP_and_OSPF_Rules**.

5 Make sure that your default models directory is selected in the **Model directories** treeview, then click **Save** to save the file.

6 Click **Cancel** in the **Configure/Run NetDoctor** dialog box, since you will not be running NetDoctor at this time.

7 Choose **File > Close** to close the project. When asked if you want to save the project, choose **Don't Save**.

Creating the Automated Task

In the previous steps, you created automation files that contain the configuration information for your topology import and NetDoctor rules. Now, you want to run configuration validation tests automatically every night.

To accomplish this, you must create an automation task. The **Configure/Run Automation Tasks** dialog box is used to manage tasks. Each task is a sequence of automation steps like “Import Topology from Device Configurations.” The tasks can be scheduled to run at any time during the day. You would like to create a task to import your topology and run NetDoctor.

1. In the system window, choose **Automation > Configure/Run Automation Tasks**.

2. The **Configure/Run Automation Tasks** dialog box displays. If the default task, **Task1**, is listed, select it. Otherwise, click **New** to create a new task.

3. Click **Rename** and rename your task **Daily IP and OSPF Validation**.

4 Click **Edit**.

➥ The **Edit Task Details** dialog box opens.

5 Each task consists of a series of steps. Each step defines an operation that IT Sentinel should run. Your task will consist of two steps: importing your topology and running NetDoctor.

5.1 Click in the first row under **Task Step Type,** and select **Import Topology from Device Configurations** from the pop-up menu.

5.2 You must now specify an automation file that contains settings for importing from device configuration files. Click in the first row under **Automation Settings File.**

➥ A list of all automation files that contain information about importing from device configuration files appears.

5.3 Choose **<initials>_daily_dci_import**.

This is the automation file you created at the beginning of this tutorial. IT Sentinel will use these settings when importing your topology.

5.4 To add a new step to run NetDoctor, click **Add Step**.

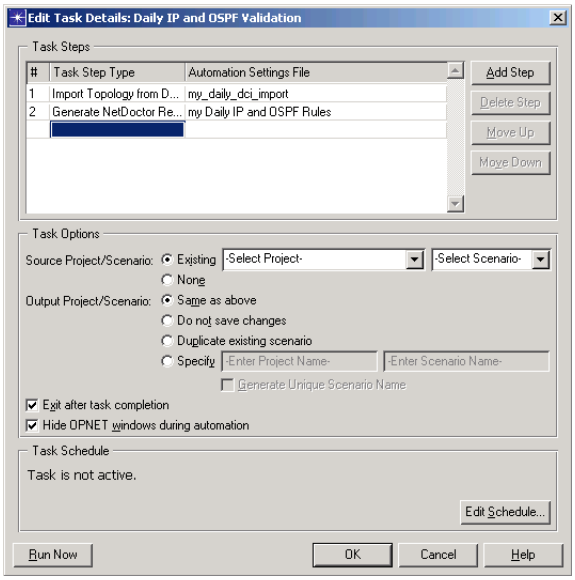
➥ A new row appears below the selected row.

5.5 Click on ***None*** and select **Generate NetDoctor Report**.

5.6 Click in the second row under **Automation Settings File** column.

5.7 Choose **<initials>_Daily_IP_and_OSPF_Rules**. This is the automation file associated with

the NetDoctor template you created earlier. Your dialog box should look similar to the one below.



When IT Sentinel runs your task, it opens an existing project or creates a new one according to the settings you specified in **Source Project/Scenario**.

When importing a topology, you generally want to begin with a new project and scenario.

5.8 Click the **None** radio button to specify that IT Sentinel should start with a new project.

6 After IT Sentinel runs through the steps, you can choose to save the output. You will use this project for later tutorials, so you should save the new project.

6.1 Click the **Specify** radio button under **Output Project/Scenario**.

6.2 Replace **–Enter Project Name–** with **<initials>_daily_config_validation** to name the new project you save.

6.3 Replace **–Enter Scenario Name–** with **ip_and_ospf_network** to name the new scenario.

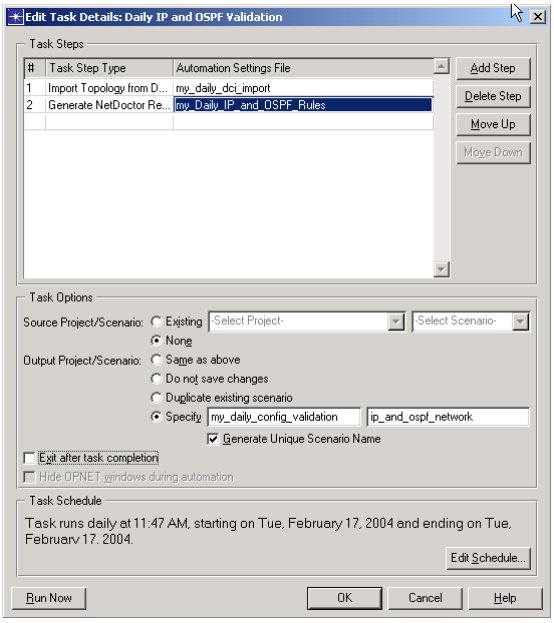
6.4 If you want to see the history of your network or run Object/Attribute Difference reports to understand how your network has changed, make sure to generate a unique scenario name. IT Sentinel will use the scenario name you provide and append the date and time of the automated task to the name.

Select the **Generate unique scenario name** checkbox.

7 IT Sentinel gives you the option to exit the application after the automation task finishes. When running an automated task in a production environment, you may choose to exit after the task completes so that you do not take up system resources and licenses longer than necessary. However, when you are designing an automated task, it is helpful if IT Sentinel stays open upon task completion. This allows you to make any modifications to your task without having to restart the software.

Uncheck the **Exit after task completion** checkbox.

8 Your dialog box should look similar to the one below:



9 When you deploy the automated task, you need to schedule it to run on a regular basis. In this initial testing phase, you do not want to schedule a test run for some time in the future. Clicking the **Run Now** button closes IT Sentinel and runs the automated task immediately.

9.1 Click **Run Now**.

9.2 When prompted, click **OK** to exit.

➥ IT Sentinel restarts in automated mode and begins your automated task. If prompted, choose not to save any existing projects.

If you are running Sentinel as a user that is not an Administrator, you will be unable to run tasks without first specifying a valid username and password in the Login Settings. To do this, click OK to exit the Edit Task Details dialog box, click on the Login Settings button, and enter a valid username and password. You can then choose to Run Selected Task.

Verifying the Automation Task

After you create an automation task, make sure you test it at least once to verify that it works as expected. This includes watching the run to verify that all the task steps are executed and reviewing the automation log for any errors.

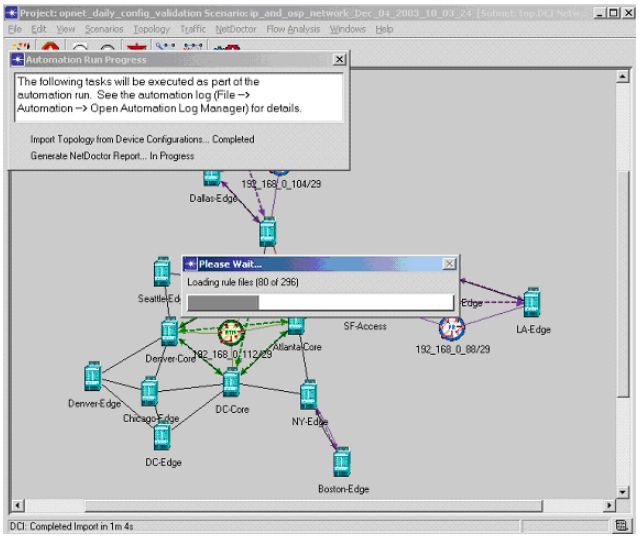
1. As IT Sentinel runs through the automation task, you should see a progress indicator dialog box. This dialog box lists all the steps that are executed as part of the task and indicate which step is in progress.

   You should see the two steps you configured:

   - Import Topology from Device Configurations
   - Generate NetDoctor Report

   You will also see IT Sentinel execute these steps.

The Project Editor will appear as if someone is going through each of the automation task steps manually.



2 After the task finishes, IT Sentinel keeps the Project Editor open and reverts to manual-mode. You can now examine the network model and view the NetDoctor reports to verify they are as expected.

3 If IT Sentinel encounters an error while executing an automation task, it writes the error to the task's automation log. This log also contains helpful information such as when steps began

and whether their output was sent to the Report Server. If there is any problem with an automation task, the first place to look for information is in the log. The last step in validating your automation task is verifying that the automation log does not contain any unexpected messages.

3.1 Choose **File > Automation > Open Automation Log Manager**.

➥ The **Automation Log Manager** appears.

The **Automation Log Manager** lets you view or delete any of the logs created while executing automation tasks.

3.2 Click on the column heading labeled **Date** until it has a down-facing arrow.

➥ This sorts the logs based on the date and time they were created.

The log from your most recent task should now be at the top.

3.3 Click on the first entry to select the most recent log.

3.4 Click **Open**.

➥ The **Log Browser** appears.

The log lists any messages that were generated during your automation task.

3.5 To view a message, click in the **Message** column. You can then read the full text.

3.6 To view the log based on task step, expand the **Category** item in the treeview on the left. A list of all of the operations that created entries in the log appears.

3.7 Click on the **Generate NetDoctor Report** item to show only the messages generated by NetDoctor.

Now that you have created and tested your automation task, you can schedule your task to run unattended. Before deploying automation, make sure you change your task to exit IT Sentinel after your task completes, and set the task schedule.

IT Sentinel will run your task automatically and output its results to the Report Server, from which the published reports can be retrieved and viewed.

Summary

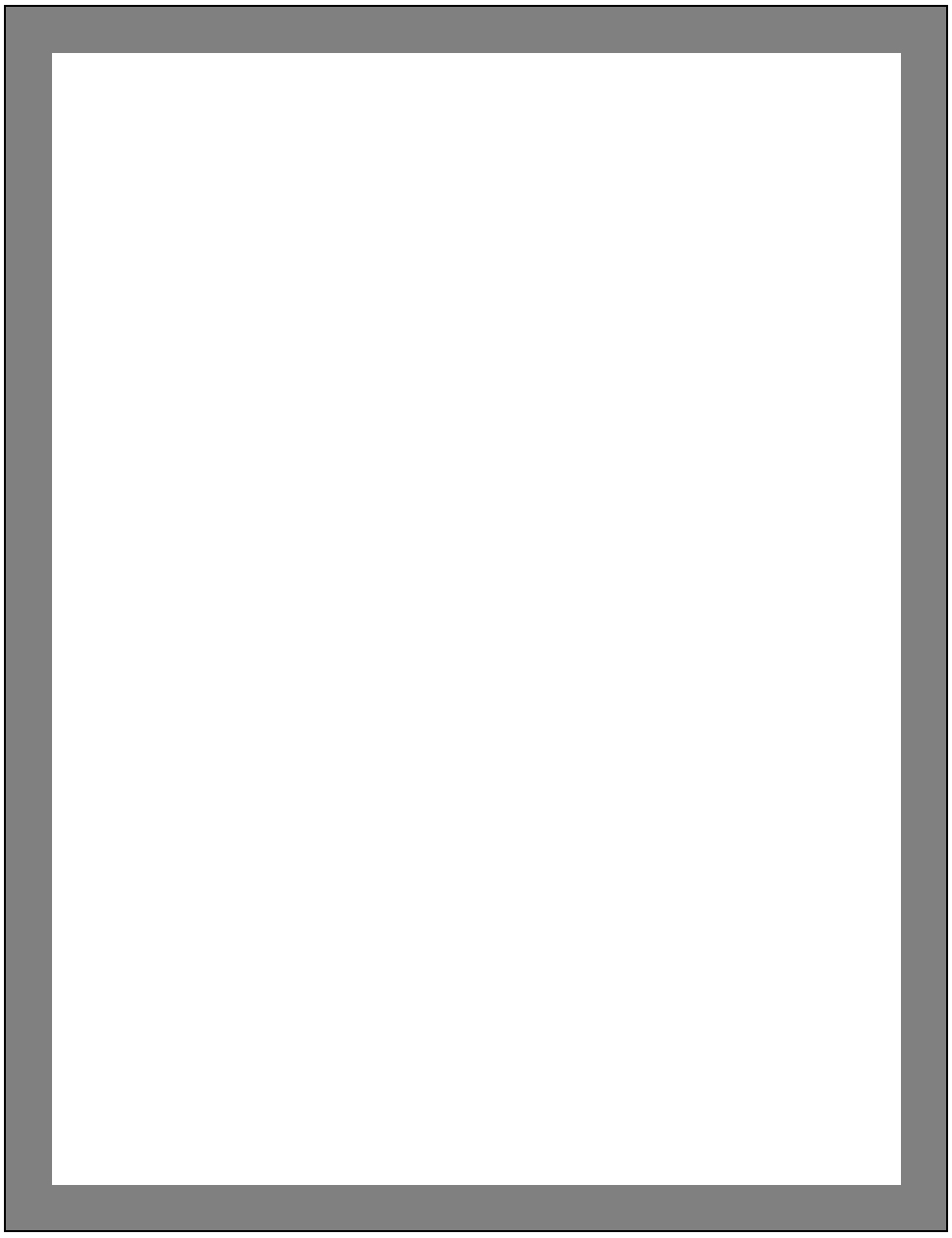
In this tutorial, you learned how to:

- Configure, correct, and automate Device Configuration Imports
- Configure, verify, refine, and automate NetDoctor analyses
- Create and schedule an automation task
- Execute and verify an automation task by looking in the Automation Log

What's Next?

Other tutorials are available on the following topics:

- NetDoctor Notification in IT Sentinel
- Using Flow Analysis with Sentinel
- Comparing Networks with Sentinel
- Working with the Report Server



3 NetDoctor Notification in IT Sentinel

NetDoctor Notification in IT Sentinel

Introduction

In the previous tutorial, you created an automation task that routinely imports your up-to-date network topology, then uses NetDoctor to detect configuration problems.

During deployment, you would like to be notified as soon as NetDoctor detects an error. The Notification feature of NetDoctor can be used to send you e-mail about potential network problems. E-mail notification messages can be sent to a standard e-mail account or to a pager.

In this lesson, you will learn how to configure NetDoctor Notification.

Before You Begin

To do this tutorial, you need to know the following:

- General knowledge
  - Your email account settings
  - The name of your mail server
  - The email address of your mail server
- OPNET-specific knowledge: You need to know how to configure NetDoctor automations (see the IT Sentinel Quick Start and Setting Up Sentinel Automation tutorials).

Prerequisite Tutorials

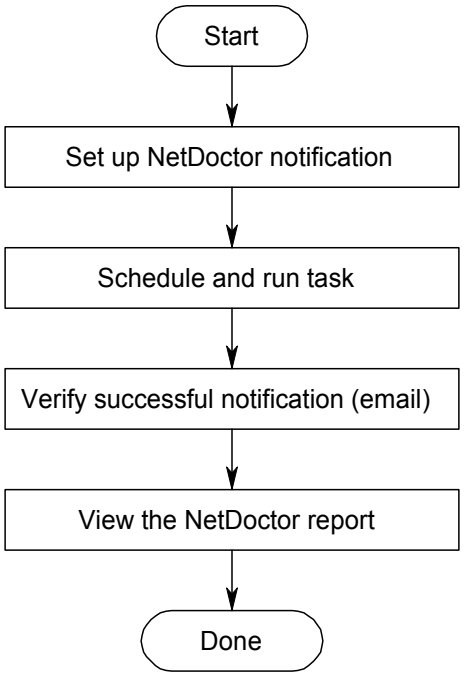
To learn the topics presented in this tutorial effectively, complete the following tutorials before you do this tutorial:

- IT Sentinel Quick Start
- Setting Up Sentinel Automation

Workflow

The following figure shows the workflow for configuring NetDoctor to generate an email notification when NetDoctor detects errors or warnings.

Workflow for Using NetDoctor Notification



Configuring NetDoctor Notification

1. Start IT Sentinel, if it is not running already.

2. Open the project that you created in the previous tutorial: **<initials>_daily_config_validation**.

3. Choose **NetDoctor > Configure/Run NetDoctor...**

   ➥ The **Configure/Run NetDoctor** dialog box opens.

4. Click on the **Template** pull-down menu and select **<initials> Daily IP and OSPF Rules**. This is the NetDoctor template you created in the previous lesson.

5. Click on the **Notification** tab.

   The **Notification** tab contains controls for configuring how IT Sentinel should notify you of the configuration issues it detects.

6. Make sure that the **Plug-in** pull-down menu is set to **“E-mail”**.

7. Make sure the **Enabled** checkbox is selected. This activates the e-mail notification feature.

8 Before you can receive notifications, you must configure NetDoctor Notification according to your needs:

8.1 Enter your mail server in the **SMTP Server** setting.

The **SMTP Server** setting directs IT Sentinel to the correct mail server to use when sending the e-mail notifications.

8.2 Put your e-mail address in the **Send To** field.

The **Send To** field is a comma-separated list of addresses that will receive the notifications.

8.3 Put your e-mail address in the **From** field.

The **From** address is the sender of the notifications. It is generally a good idea to use the address of the person or group responsible for the automation task.

8.4 Leave the **Reply-To** field the same as the **From** field.

The **Reply-To** address directs responses to e-mail notifications to the designated e-mail address. This field should contain the e-mail address of the person who is responsible for handling inquiries about the task. If it is the same as **From**, the **Reply-To** field is not added to the outgoing e-mail.

8.5 Enter **[Daily NetDoctor Results]** for the **E-mail Subject Prefix**.

All NetDoctor Notification messages have a subject line that contains the **E-mail Subject Prefix** and the name of the rule (or rule summary) that triggered the message. You should use an **E-mail Subject Prefix** that is specific to your report so that you can filter the various messages easily.

8.6 Enter **[Daily NDR]** for the **Pager Prefix.**

The **Pager Prefix** is similar to the **E-mail Subject Prefix**. If you opt to send your messages in the “pager” format, IT Sentinel uses the **Pager Prefix** to construct the subject of the message. The **Pager Prefix** is usually much shorter than the **E-mail Subject Prefix** to allow for the limited display size of most pagers.

8.7 Set the **Threshold** to **Errors**.

The **Threshold** allows you to specify the types of messages for which NetDoctor should send notifications. The **Threshold** setting can be configured to send messages of interest from the NetDoctor run: “Errors”, “Errors and Warnings”, “Errors, Warnings and Notes”, or “Errors, Warnings, Notes, and Passed”. Depending on your policies, you can modify the **Threshold** to meet your needs.

8.8 Change the **Notifications** to **Per Rule and Summary** so that you receive all possible messages.

The **Notifications** setting allows you to restrict or unrestrict the amount of message traffic you receive during a NetDoctor run. You can choose to receive a separate message for each rule that is triggered or one message that summarizes the results.

8.9 Leave **Messages Included** set to **New Messages Only**.

The **Messages Included** setting is another way to limit the number of messages you receive, if you enabled **Report Comparison** on the **Settings** tab. If you specify that you would like to receive **New Messages Only**. IT Sentinel will only send messages that do not appear in the report against which the current report is compared. **All Messages** means that you want to receive all notifications regardless of whether they are unique to the current report.

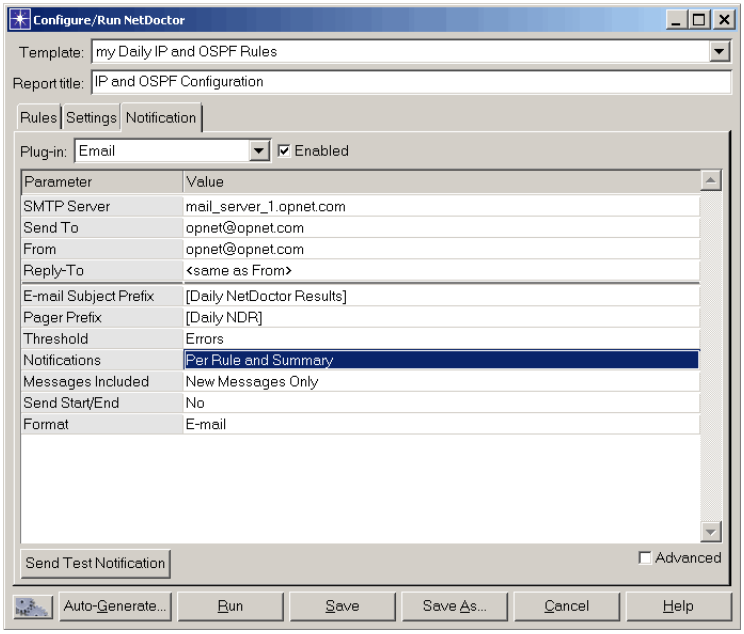
8.10 Set **Send Start/End** to **No**.

If you wish, NetDoctor can send separate messages immediately before the NetDoctor run begins and after the end of the NetDoctor run. For this lesson, you do not need to enable this feature.

8.11 Set the **Format** to **E-mail**.

NetDoctor can send messages in either an **E-mail** or **Pager** format. The pager format is more concise for a pager's limited display size.

8.12 Your dialog box should appear similar to the following figure, but with your own mail server and address settings.



When you set up notification for the first time, it is a good idea to send a test notification. This does not test the NetDoctor rules themselves. Instead, it sends a test message to verify that your **SMTP Server** and **Send To** settings are correct.

9 Click **Send Test Notification**, and click **OK** on the T**est Notification Sent Successfully** box.

➥ A test message with a list of notification preferences and their settings is sent.

Make sure you receive the test notification before you save your settings to a template.

- If a message window appears when you try to send the notification, check the information you typed into the **SMTP Server** and **Send To** fields.
- If you do not see a message window and do not receive the expected notification, check with your e-mail administrator.

10 After you configure notification, click **Save** to save the settings in your template, then **Cancel** to close the dialog box.

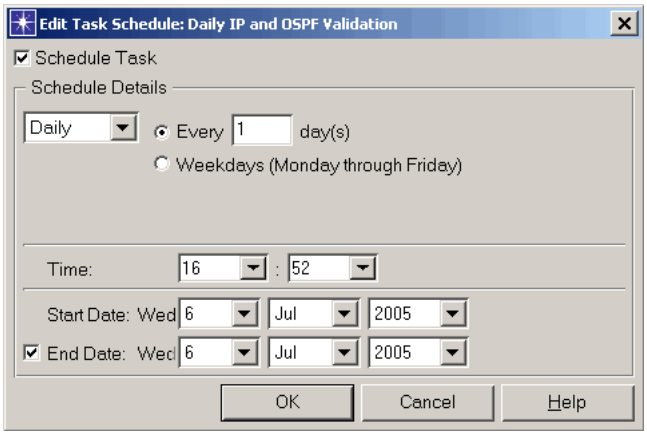
Scheduling the Automation Task

Now that you have configured NetDoctor to send notifications, you can get messages about the state of your network when your automation task runs.

1. Choose **File > Automation > Configure/Run Automation Tasks**.
2. Select the **Daily IP and OSPF Validation** task, and click **Edit**.
3. In the **Edit Task Details** dialog box, click **Edit Schedule…**

   ➥ The **Edit Task Schedule** dialog box opens.
4. Click in the **Schedule Task** checkbox to select it.
5. Verify that the schedule is set to run **Daily** and occur every **1** day.
6. Verify that **Start Date** is set to today's date.
7. Click in the **End Date** checkbox to select it, then set it to today's date.

8 Change the **Time** to 2 minutes from now. Your dialog box should look similar to the one below.



9 Click **OK**.

10 Click **OK** to close the **Edit Task Details** dialog box.

11 Click **OK** to close the Configure/Run Automation Tasks dialog box.

12 Choose **File > Exit** to quit IT Sentinel.

If prompted, choose not to save changes. Your automation task should run in about a minute.

Examining the Notification Messages

After the automation task completes, you will receive multiple messages. These messages will list the specific errors that NetDoctor found. To see the details of the errors, click on the **Report Server** link found in any of the messages, and open the report that corresponds to your task.

Summary

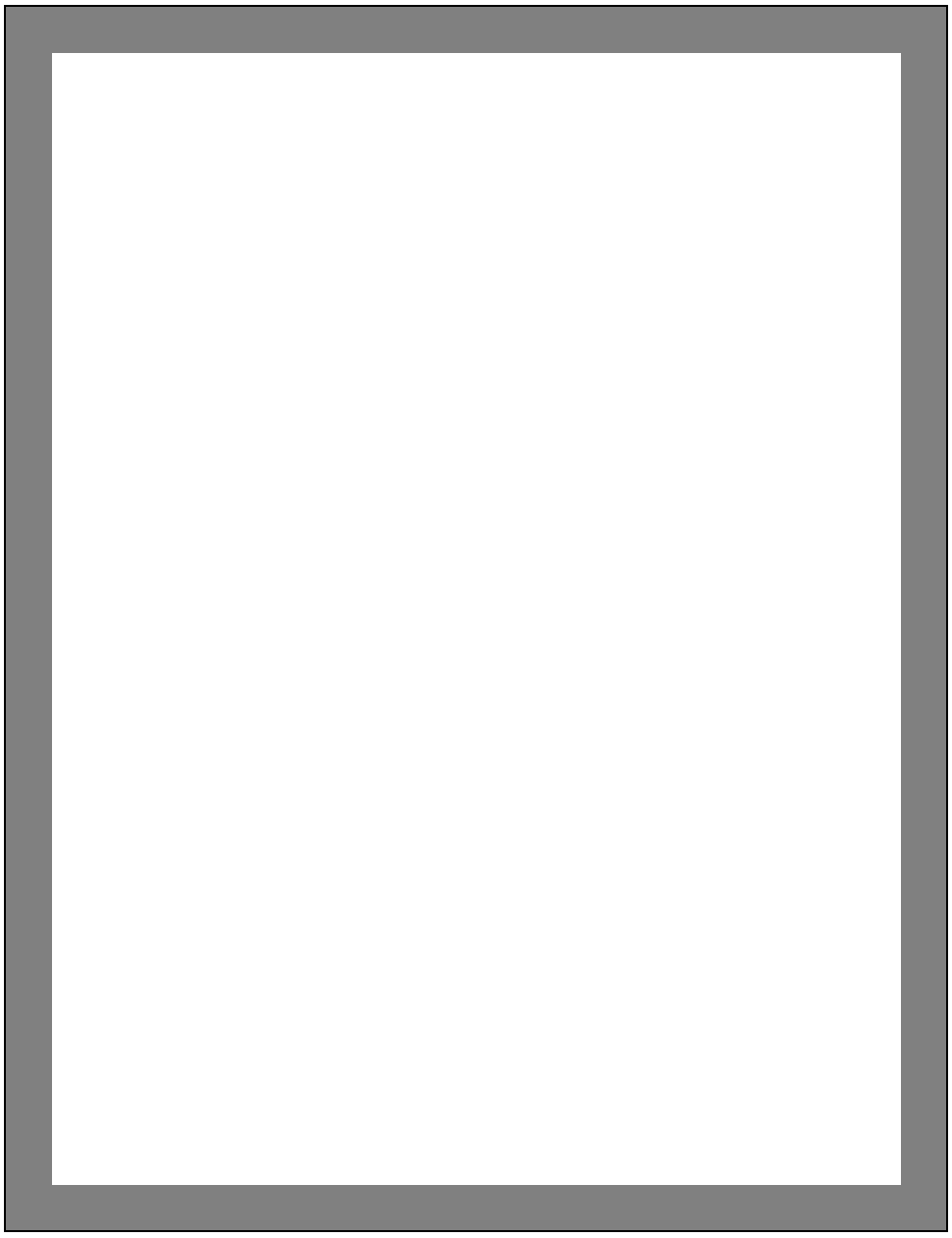
Lessons learned

- You learned the basic workflow for configuring the NetDoctor notification process
- You learned how to configure NetDoctor to generate automatic email notifications
- You learned how to schedule the automation task

What's Next?

Other tutorials are available on the following topics:

- Using Flow Analysis with Sentinel
- Comparing Networks with Sentinel
- Working with the Report Server



4 Using Flow Analysis with Sentinel

Using Flow Analysis with Sentinel

Introduction

In the Setting Up Sentinel Automation tutorial, you created an automation task that routinely imports the up-to-date network topology and uses NetDoctor to detect any configuration problems.

Flow Analysis can also be used as part of an automation task—separately or with NetDoctor—to diagnose configuration problems like routing loops and multiple next hops to a destination.

In this lesson, you will learn how to configure Flow Analysis automation and feed the results into NetDoctor.

Prerequisite Tutorials

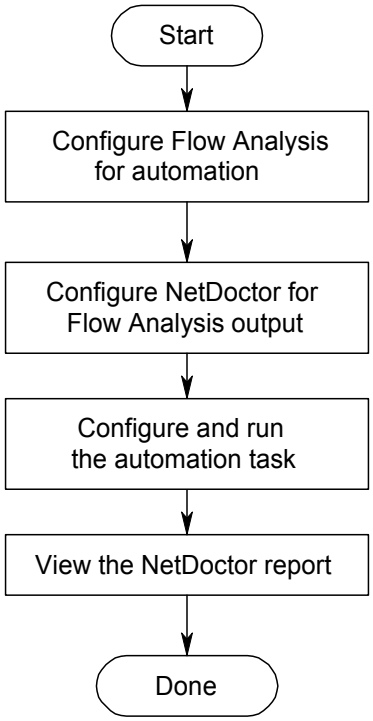
To learn the topics presented in this tutorial effectively, complete the following tutorials before you do this tutorial:

- IT Sentinel Quick Start
- Setting Up Sentinel Automation
- NetDoctor Notification in IT Sentinel

Workflow

The following figure shows the workflow for incorporating Flow Analysis information in an automated NetDoctor analysis.

Workflow for Automating Flow Analysis



Configuring Flow Analysis

The process used to configure Flow Analysis for automation is similar to the process used to configure Device Configuration Import.

1. Open the project from the Setting Up Sentinel Automation tutorial: **<initials>_daily_config_validation**

2. Choose the **Flow Analysis > Configure/Run Flow Analysis**... menu item.

   ➥ The **Configure/Run Flow Analysis** dialog box appears.

3. Flow Analysis has many reports to choose from.

   3.1 Click the **Select Reports…** button.

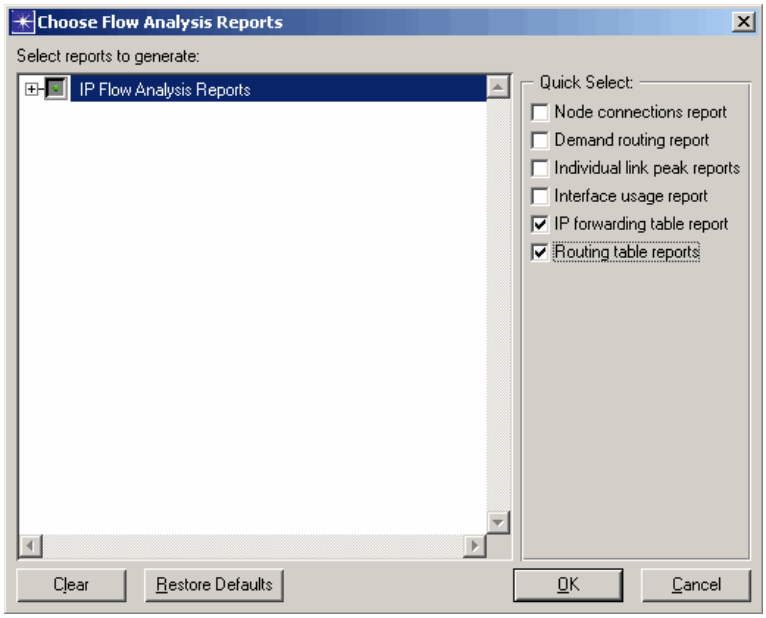
   ➥ The **Choose Flow Analysis Reports** dialog box appears.

   3.2 Clear the selection by clicking on **IP Flow Analysis Reports** in the treeview.

   ➥ The green dot indicating that reports are selected disappears.

3.3 In the **Quick Select** pane on the right side of the dialog box, make sure the following checkboxes are selected:

- **IP forwarding table report**
- **Routing table reports**



3.4 Click **OK** to save the changes.

➥ The **Configure/Run Flow Analysis** dialog box is active again.

4 After Flow Analysis is configured, you must save the settings to an automation file as follows:

4.1 Click the **Save Automation Settings** button  to save the Flow Analysis settings for automation.

4.2 Enter the following file name: **<initials>_flan_routing_table_reports** then click **Save**.

4.3 Click **Cancel** to close the **Configure/Run Flow Analysis** dialog box.

Configuring NetDoctor

Now that you have saved an automation file for running Flow Analysis, you need to revisit the NetDoctor template. In the Setting Up Sentinel Automation tutorial, you omitted certain rules that relied on simulation input. Now that you will be running Flow Analysis, you can take advantage of these rules.

1. Choose the **NetDoctor > Configure/Run NetDoctor...** menu item.

2. Click on the **Template** pull-down menu and select the **<initials> Daily IP and OSPF Rules** template you created in the Setting Up Sentinel Automation tutorial.

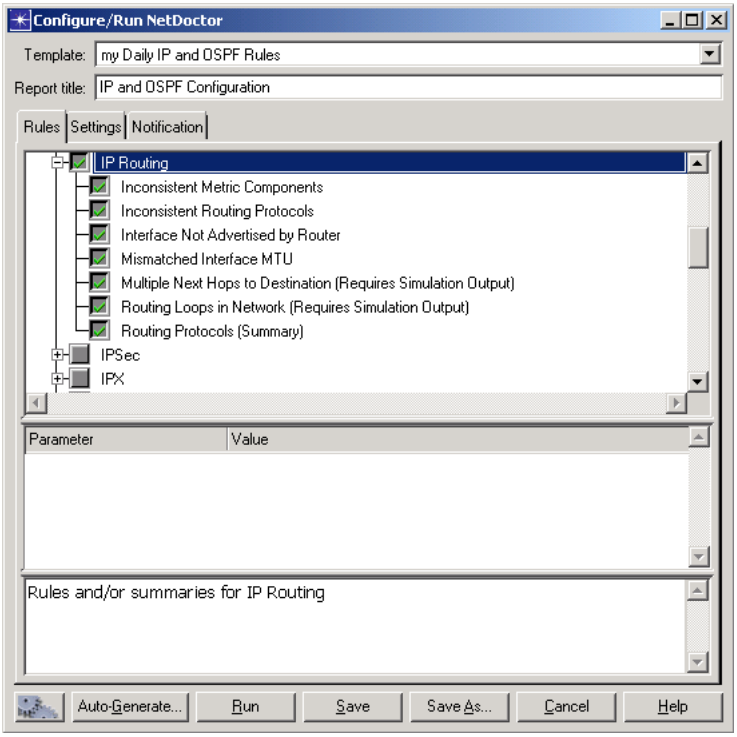
3. Expand the **IP Routing** rule suite.

4. The **Multiple Next Hops to Destination** and **Routing Loops in Network** rules detect configuration problems that are not apparent from the device configuration data but that cause network performance degradation. These rules rely on simulation output. Flow Analysis will provide these results.

   4.1 Click on **Multiple Next Hops to Destination** to select it.

4.2 Click on **Routing Loops in Network** to select it.

➥ The green dot next to **IP Routing** changes to a green check mark to indicate that all rules in the suite are selected.



4.3 Click **Save** to save the changes you made to the template.

4.4 Click **Cancel** to close the dialog box.

Configuring the Automation Task

Now that the settings have been saved, you need to add Flow Analysis to the automation task.

1. Choose **File > Automation > Configure/Run Automation Tasks**.

2. Click on the **Daily IP and OSPF Validation** task that you created in the Setting Up Sentinel Automation tutorial.

3. Click **Edit** to edit the task.

4. You need to add a Flow Analysis step to the task. Because NetDoctor relies on the output of Flow Analysis, make sure that the Flow Analysis step is before NetDoctor.

   4.1 Click **Add Step** to add a new row.

   4.2 Click ***None*** and select **Run Flow Analysis** in the new row.

   4.3 Click on the **Automation Settings File** column for the **Run Flow Analysis** row. Select the file that you created earlier:

   <initials>_flan_routing_table_reports

4.4 Click **Move Up/Move Down** if necessary to move the **Run Flow Analysis** entry before NetDoctor, but after the topology import.

This ensures that Flow Analysis and NetDoctor are run in the correct sequence so that the output of Flow Analysis is available to NetDoctor for its run.

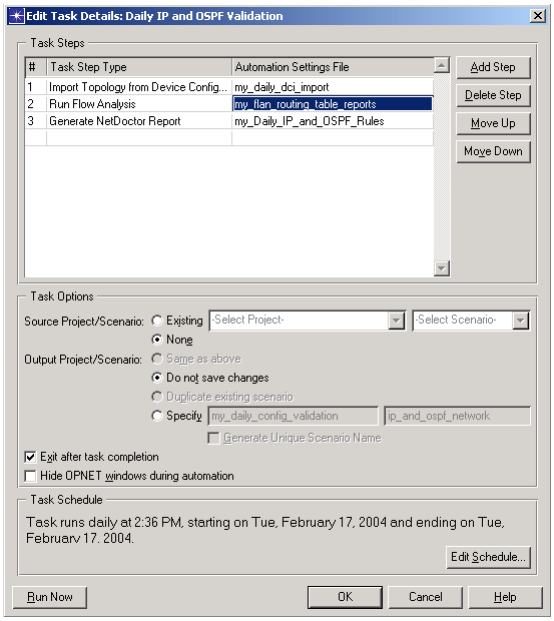
5 Unless you want to keep a historical record of the network state and its analysis, you do not need to keep the project you used during the automation run. To prevent the project from being saved to disk, select the **Do not save changes** radio button.

6 You can now test the new automation task.

6.1 Make sure that **Exit after task completion** is selected.

6.2 Make sure **Hide all windows during automation** is *not* selected. This lets you see the progress of the task as it runs.

The dialog box should look like this.



7 Click **Run Now**.

8 When prompted, click **OK** to begin the automation task and exit IT Sentinel.

If prompted to save the current scenario, do NOT save it.

➥ IT Sentinel runs the automation task, and exits when the task finishes.

You can now view the reports that were created during the automation run.

Normally, the automation task is scheduled to run unattended—usually at night. Therefore, the next steps in the tutorial would be done the next morning, long after IT Sentinel has finished its work.

Viewing Reports

By default, all reports generated during an automation task are sent to the Report Server.

The Report Server is a central repository that allows you to view the output of the analyses without having to run IT Sentinel. You must have an account—set up by the Report Server administrator—before you can access reports on the Report Server.

1 Start IT Sentinel.

2 Choose **Automation > Web – Open Report Server Home**.

➥ The main page of the Report Server appears in a browser window.

3 Enter your username and password, then click **Login.**

➥ The Report Server home page appears.

4 Reports are sorted into folders based on the report types.

4.1 Click on the NetDoctor folder. The most recent report is at the top.

4.2 Click on the **IP and OSPF Configuration** link.

➥ The NetDoctor report appears.

The IP Routing notes show that NetDoctor found some cases of routing tables that contain multiple next hops to a destination. This analysis relies on output from Flow Analysis.

4.3 Close the NetDoctor report.

4.4 Click on the Flow Analysis folder. Again, the most recent report is at the top.

4.5 Click on the **Daily_IP_and_OSPF_Validation_Automation-Automation** link.

➥ The Flow Analysis Report appears.

4.6 Close the Flow Analysis report.

Summary

In this tutorial you learned how to use Flow Analysis to augment the data NetDoctor draws from when running its rules.

In the next tutorial, you will learn how to generate Object/Attribute Difference reports automatically to track changes in the network.

What's Next?

Other tutorials are available on the following topics:

- Comparing Networks with Sentinel
- Working with the Report Server

5 Comparing Networks with Sentinel

Comparing Networks with Sentinel

Introduction

A key component to diagnosing problems in your network is understanding how that network has changed over time. IT Sentinel Object/Attribute Difference reports show the differences between two topologies of the same network.

In this tutorial, you will learn how to use IT Sentinel automation to generate Object/Attribute Difference reports and find changes in your network. After you finish this tutorial, you will know how to generate object/attribute difference reports as part of an automation task.

Prerequisite Tutorials

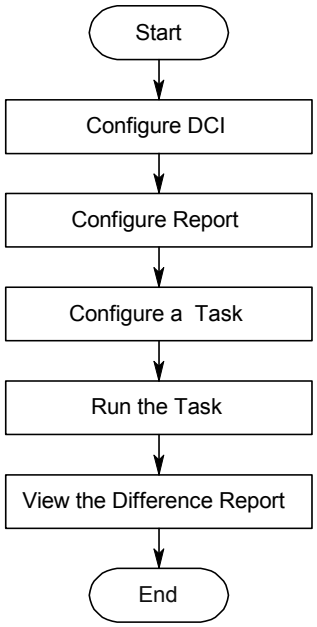
To effectively learn the topics presented in this tutorial, complete the following tutorials first:

- IT Sentinel Quick Start
- Setting Up Sentinel Automation
- NetDoctor Notification in IT Sentinel
- Using Flow Analysis with Sentinel

Workflow

The following figure shows the workflow for creating automated Object/Attribute Difference reports from successive network imports.

Workflow for Automating Object/Attribute Difference Reports



Importing a New Topology

In previous tutorials, you imported a set of configuration files for a network with mismatched OSPF areas. In this tutorial, you will create an automation file to import a set of configuration files in which the OSPF problems have been corrected.

1. Open the project **<initials>_daily_config_validation**.
2. Select **Topology > Import Topology > From Device Configurations**.
   ➥ The Import Device Configurations dialog box opens.
3. Click in the first row of the table under the **Vendor** column.
4. Select **Cisco** from the drop-down list if it is not already selected.
5. Click **Browse.**

6 Choose the directory ***<reldir>*\models\std\tutorial_req\module\configs\baseline** and click **OK** (**Select** on UNIX platforms).

➥ The file browser closes and **Cisco** row of the **Import Device Configurations** dialog box shows the correct directory path.

7 Make sure that the **Create PVCs** checkbox is selected.

8 Under **Specify Model Assistant Files**, make sure that **<initials>_daily_model_assistant** is listed, and the **Use the following model assistant files** checkbox is checked.

9 Click on the **Save settings for automation** button  and perform the following:

9.1 Enter **<initials>_repaired_dci_import** for the file name.

9.2 Click **Save**.

10 Click **Cancel** to close the **Import Device Configurations** dialog box.

Configuring the Object/Attribute Difference Report

Object/Attribute Difference reports are the result of comparing two scenarios. In automation, the first scenario is always the active scenario used in the automation task. The second scenario is specified in the automation file. You will now create an automation file to compare against a scenario created in a previous tutorial.

1. Select **Scenarios > Object/Attribute Difference Report > Generate Report…**

2. Specify the project and scenario to compare against.

   You can choose a scenario by name or specify a base name and time parameter. If you choose to specify a base name and time, IT Sentinel uses the timestamp in the scenario name to find the scenario.

   2.1 Set the project to **<initials>_daily_config_validation**.

   2.2 Select the **Specified project, and the scenario with given base name that was created** checkbox.

You can choose to specify a time range. For example, if you want to compare against a scenario you created last week, compare it against the scenario created seven days ago. You can also choose to compare against the most recent scenario. For this exercise, use the latter option.

2.3 Click on the **Most recently** radio button.

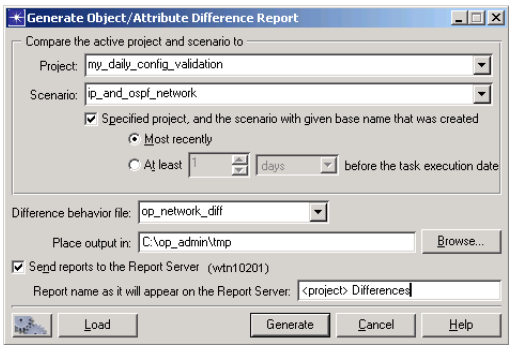
3 Make sure **Send reports to the Report Server** is enabled.

This stores your reports on your OPNET Report Server.

4 In the report name field, enter **<project> Differences**.

Give your report a name that describes what it contains. The Report Name field allows for any text and accepts two variables: **<project>** and **<scenario>**. In the report name, the string **<project>** will be replaced with the name of the

automation project. The variable **<scenario>** will be replaced with the name of the automation scenario.



5 Save the current settings to an automation file.

5.1 Click the “save settings for automation” button. 

5.2 Enter **<initials>_most_recent_differences** for the automation file name.

5.3 Click **Save**.

6 Click **Cancel** to close the **Generate Object/Attribute Difference** dialog box.

Configuring the Automation Task

After saving your automation files, you can create an automation task to import your new configuration files and generate an Object/Attribute Difference report to show the changes. This report will be sent to the Report Server for viewing later.

1. Select **File > Automation > Configure/Run Automation Tasks**.
2. Click **New** to create a new task.
3. Click **Rename** and enter **Daily Differences** for the task name.
4. Click **Edit** to edit the new task.
5. Click on ***None*** and select **Import Topology from Device Configurations**.
6. Click in the cell under **Automation Settings File** and select **<initials>_repaired_dci_import**.
7. Click in the cell below **Import Topology from Device Configurations** and select **Generate Object/Attribute Difference Report**.

8 Click in the cell to the right of **Generate Object/Attribute Difference Report** and select **<intials>_most_recent_differences**.

9 Click the **None** radio button next to **Source/Project scenario**.

Because you are importing a new topology, there is no reason to use an existing scenario when starting IT Sentinel.

10 You want to store your new scenario in the same project as the previous tutorials.

10.1 Under **Output Project/Scenario**, click the **Specify** radio button.

10.2 Enter **<initials>_daily_config_validation** in the project field.

10.3 Enter **ip_and_ospf_network** in the scenario field.

If you choose to generate a unique scenario name, IT Sentinel appends a timestamp to the name you specified in the Scenario field. IT Sentinel uses this timestamp to locate the correct scenario to generate an

Object/Attribute Difference report. You may want to use this topology again for other difference reports.

10.4 Make sure **Generate Unique Scenario Name** is selected.

11 Make sure **Hide OPNET windows during automation** is not checked so you can see your automation as it runs.

12 Click **Run Now** to run the automation task now.

Viewing the Report

Now that you have generated an Object/Attribute Difference report, you can access the Report Server to view it.

1. Restart IT Sentinel.
2. Choose **Automation > Web – Open Report Server Home**.

   ➥ A Web browser displays the home page of your Report Server.
3. Enter your username and password.
4. Click **Login.**
5. Click the **View by Products** link at the top of the page and click the **All Reports** link for your corresponding product.
6. The top entry should be for **<initials>_daily_config_validation-Differences**

   This is the report you just created.

7 Click on the link to view the report.

➥ The report displays and indicates that there are several differences between the new network and the previous network.

8 Click on **Nodes with differences** to jump to that section of the report.

➥ The results indicate that changes to the **OSPF Parameters.Interface Information.Area ID** attribute were found.

Summary

In this tutorial, you learned how to generate a Object/Attribute Difference report as part of an automated task. This enables you to see how your network has changed over time.

What's Next?

Other tutorials are available on the following topics:

Working with the Report Server

6 Working with the Report Server

Working with the Report Server

Introduction

With IT Sentinel, you can use several different search methods to search for reports published to the Report Server.

This tutorial shows how you can

- View reports by application
- Search for reports
- Create and use sub-folders
- Create and use filters

Prerequisite Tutorials

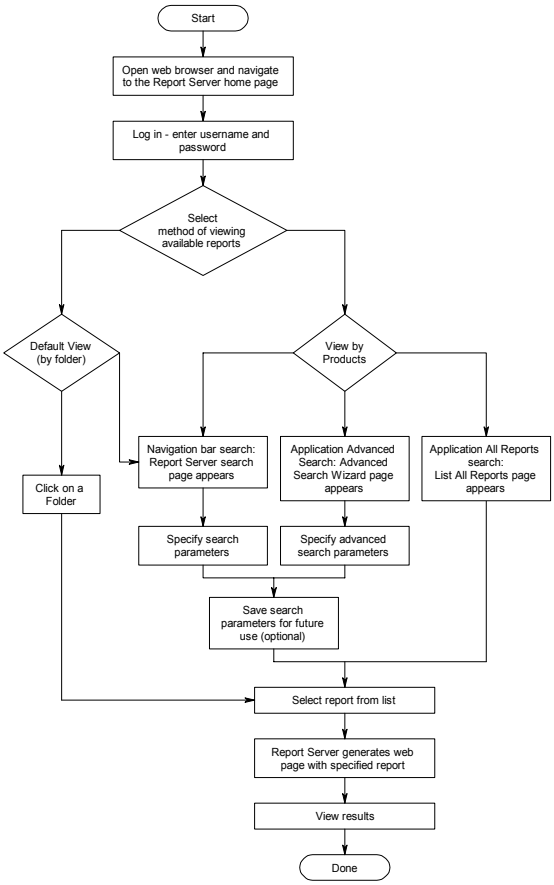
To understand the topics presented in this tutorial, complete the tutorials listed below before attempting this one:

- IT Sentinel Quick Start
- Setting Up Sentinel Automation
- NetDoctor Notification in IT Sentinel
- Comparing Networks with Sentinel
- Using Flow Analysis with Sentinel

Workflow

The following figure shows the workflow for a report search

Report Server Workflow



Viewing Reports By Application

In previous tutorials, you used automated tasks to generate reports. These reports were sent to the OPNET Report Server for future viewing.

This tutorial walks you through some commonly used Report Server features. A variety of applications might send reports to your Report Server. For example, IT Guru, SP Guru, and IT Sentinel might all publish reports.

To view reports organized according to the OPNET application, follow these steps.

1. Launch a Web browser such as Firefox, Opera, or Internet Explorer.

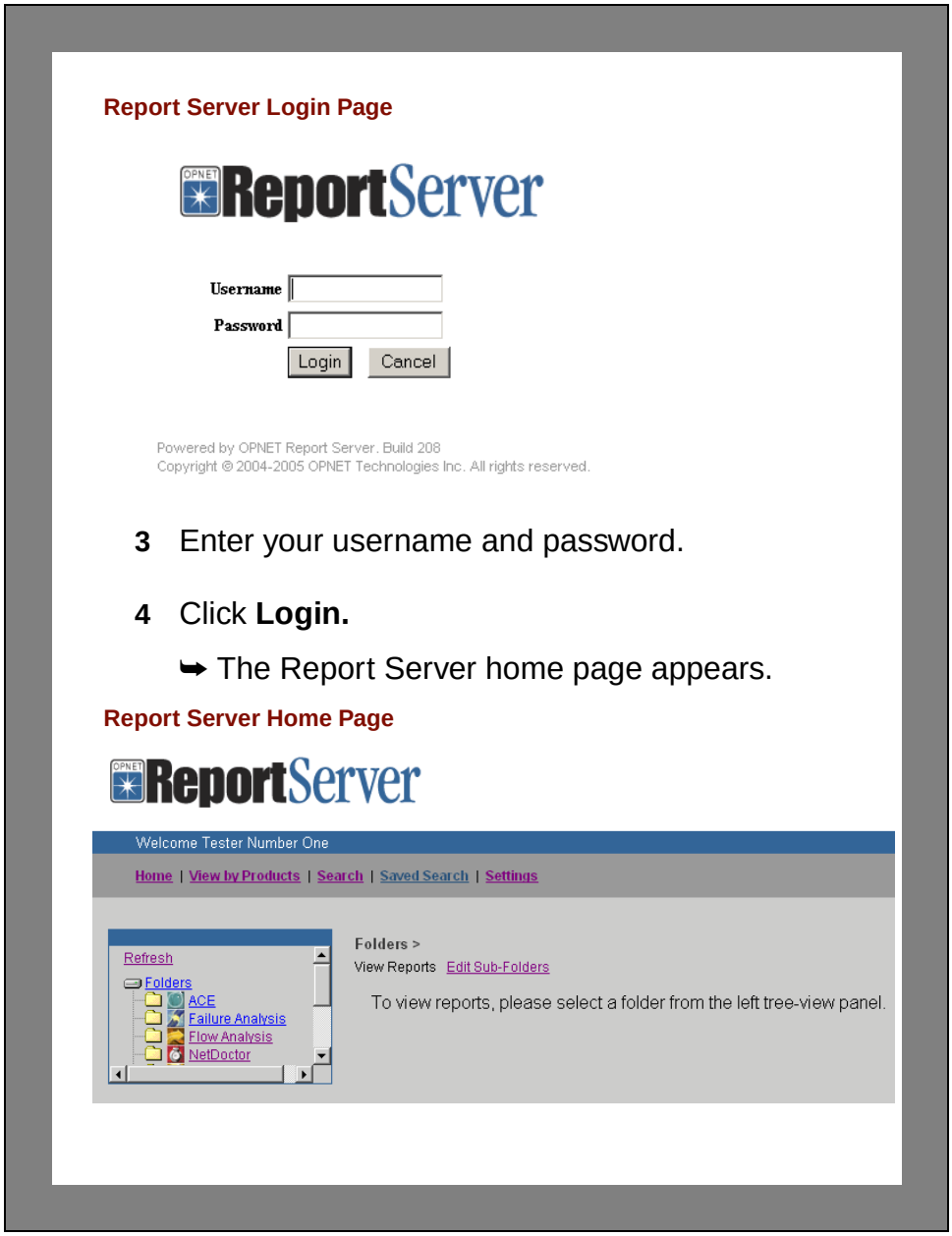
2. Enter the following URL,

```
http://<report server>:<port>/rs
```

   where <report server> is the machine hostname running your Report Server and <port> is the port on which the Report Server is running. The default port is 9090.

   ➥ A Web browser displays with the login page of your Report Server.

Report Server Login Page



3 Enter your username and password.

4 Click **Login.**

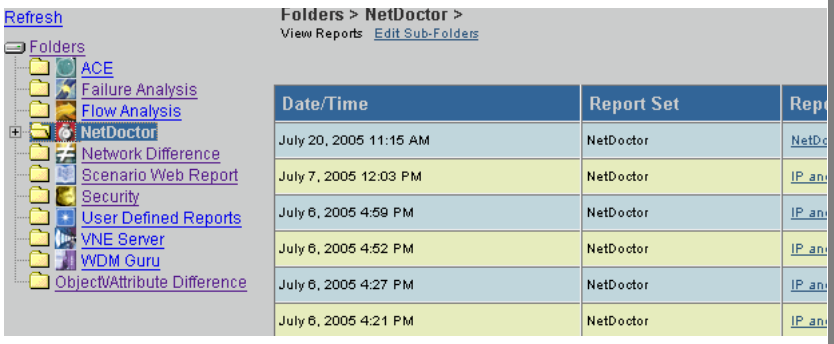
➥ The Report Server home page appears.

Report Server Home Page

5 Click on the **NetDoctor** folder.

➥ This takes you to a list of all NetDoctor reports published to the Report Server.

NetDoctor Reports in the NetDoctor Folder



- The **Date/Time** column lists when the reports were published.
- The **Report Set** column contains the type of reports. For example, NetDoctor reports are listed as “NetDoctor.”
- The **Report** column shows the names of the reports.

6 Click on the first “IP and OSPF Configuration” link.

➥ This launches a report browser window that shows a NetDoctor report.

7 Close the browser window in which you are viewing the NetDoctor Report.

➥ You are returned to the Report Server page.

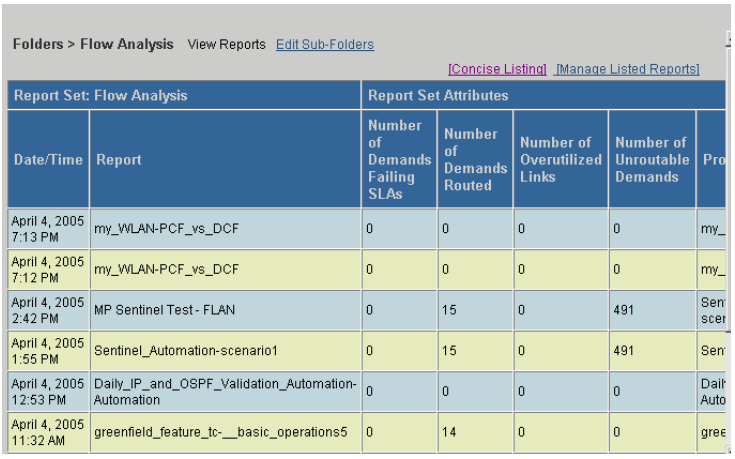
8 Click on the **Flow Analysis** folder.

➥ The list of Flow Analysis reports now appears in the browser window.

9 Click on **Detailed Listing** at the top of the reports list.

➥ A detailed list of the previously displayed reports is shown. Use the scroll bars to examine all fields of the detailed listing.

Detailed Reports Listing



Folders > Flow Analysis View Reports Edit Sub-Folders

[Concise Listing] [Manage Listed Reports]

Report Set: Flow Analysis		Report Set Attributes				
Date/Time	Report	Number of Demands Failing SLAs	Number of Demands Routed	Number of Overutilized Links	Number of Unroutable Demands	Pro
April 4, 2005 7:13 PM	my_WLAN-PCF_vs_DCF	0	0	0	0	my_
April 4, 2005 7:12 PM	my_WLAN-PCF_vs_DCF	0	0	0	0	my_
April 4, 2005 2:42 PM	MP Sentinel Test - FLAN	0	15	0	491	Sen scer
April 4, 2005 1:55 PM	Sentinel_Automation-scenario1	0	15	0	491	Sen
April 4, 2005 12:53 PM	Daily_IP_and_OSPF_Validation_Automation-Automation	0	0	0	0	Dail Auto
April 4, 2005 11:32 AM	greenfield_feature_tc-__basic_operations5	0	14	0	0	gree

10 To return to the previous view, click **Concise Listing** at the top of the reports list.

Unless you are an administrator, you cannot use the **Manage Listed Reports** option. This feature is covered in the Using the Report Server guide.

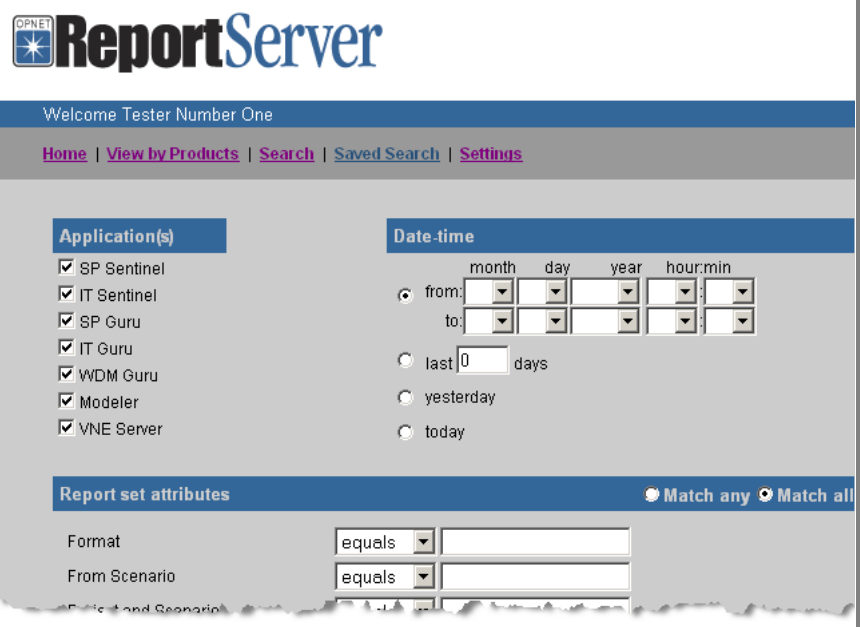
Filtering Reports by Date and Time

To filter reports based on date and time, follow these steps.

1 Click on **Search** in the navigation bar.

➥ The Report Server search page displays.

Report Server Search Page



2 Under **Application(s)**, clear all checkboxes except IT Sentinel to search the reports generated by IT Sentinel.

3 Select the **Last** field, and then specify **1** as the number of days for which you would like to see reports.

4 Scroll to the bottom of the screen.

5 In the **Save search as** text box, enter “One Day Search.”

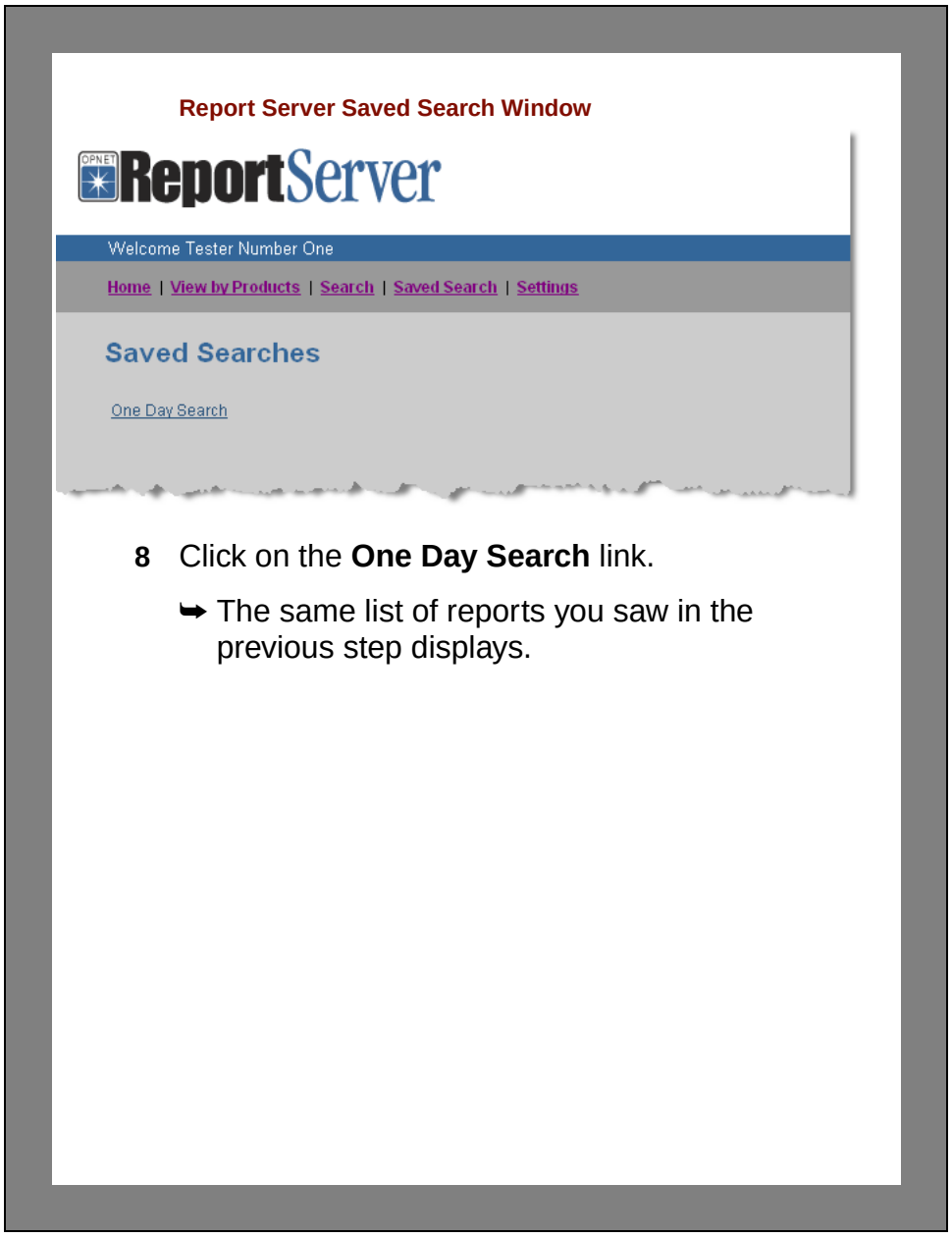
➥ The parameters of this search will be saved so that you can perform the same search later with a single click.

6 Click **Search**.

➥ A list of all of the reports created within your specified time range displays.

7 Click on the **Saved Search** link at the top of the page.

➥ This takes you to a list of all your saved searches.



8 Click on the **One Day Search** link.

➥ The same list of reports you saw in the previous step displays.

Working with Sub-Folders

Sub-folders allow you to organize your reports with more granularity. For example, you can organize your NetDoctor reports by date of creation, hostname on which they were generated, or by number of errors or warnings recorded in each report. For this tutorial, you will create a sub-folder that will contain NetDoctor reports with multiple errors.

1. Click on the **Home** link.

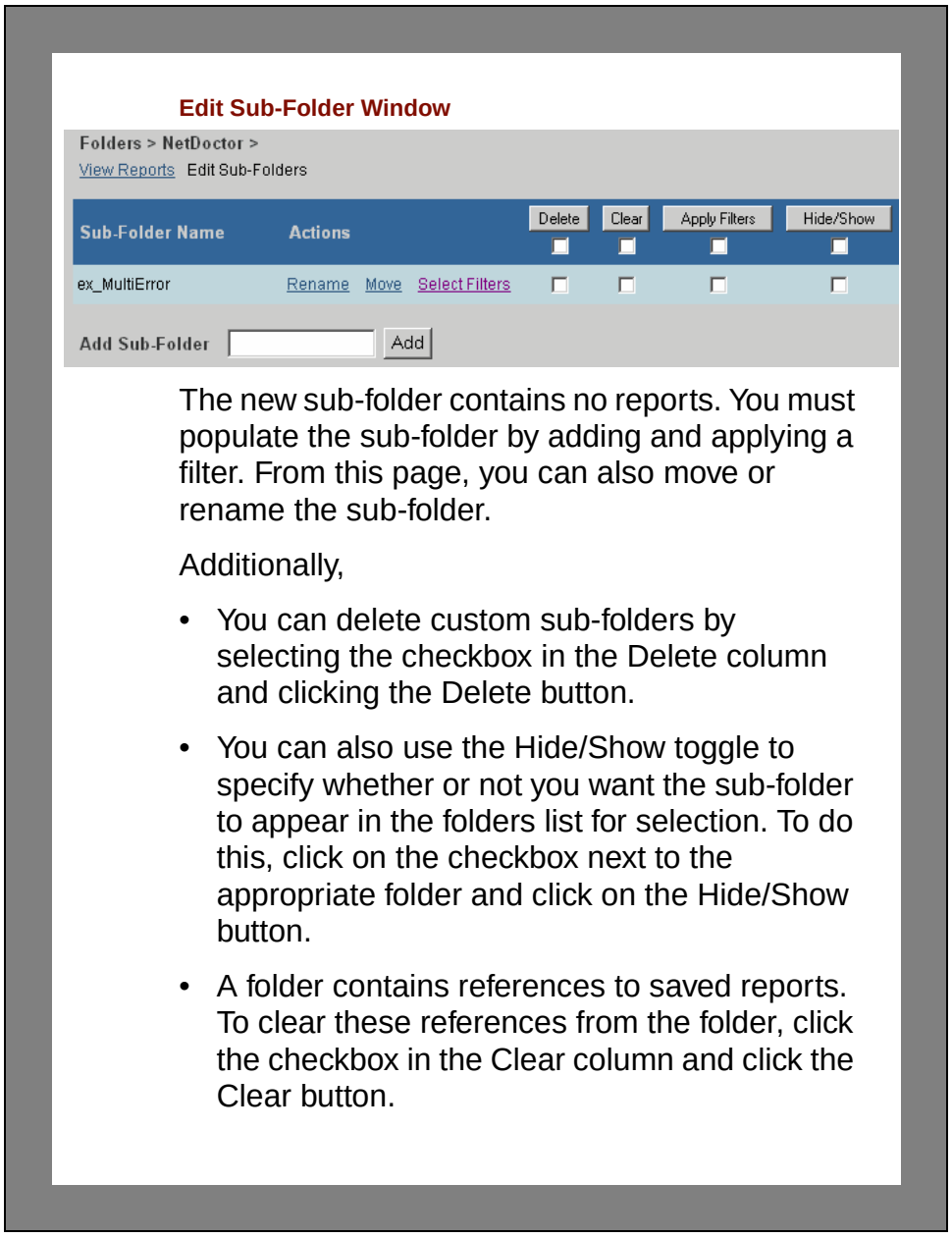
2. Click on the **NetDoctor** folder.

3. Click on **Edit Sub-Folders**.

4. Enter the name of a sub-folder you wish to create in the NetDoctor reports list.

   4.1 Type **<initials>_MultiError** in the **Add Sub-Folder** box. Use your initials to make this sub-folder unique, to distinguish it from folders created by other users who may have run this tutorial.

   4.2 Click the **Add** button.



The new sub-folder contains no reports. You must populate the sub-folder by adding and applying a filter. From this page, you can also move or rename the sub-folder.

Additionally,

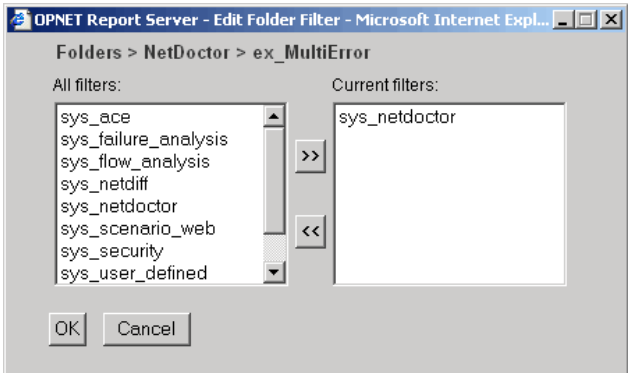
- You can delete custom sub-folders by selecting the checkbox in the Delete column and clicking the Delete button.
- You can also use the Hide/Show toggle to specify whether or not you want the sub-folder to appear in the folders list for selection. To do this, click on the checkbox next to the appropriate folder and click on the Hide/Show button.
- A folder contains references to saved reports. To clear these references from the folder, click the checkbox in the Clear column and click the Clear button.

5 Add a filter to the sub-folder.

5.1 Click on the **Select Filters** link.

➥ A dialog box displays. All available filters are listed on the left. Currently applied filters for this sub-folder are listed on the right.

Edit Folder Filter Dialog Box



5.2 Select **sys_netdoctor** from the **All Filters** window, and click the **>>** button to move it into the **Current Filters** window.

➥ Selecting the sys_netdoctor filter selects all of the reports with the report set equal to NetDoctor. You can use any of the sys_* filters to include every report from a given report set.

5.3 Click **OK**.

➥ You are returned to the Edit Sub-Folders page.

6 Click the checkbox under the **Apply Filters** column for the **<initials>_MultiError** sub-folder.

7 Apply the filter to the sub-folder.

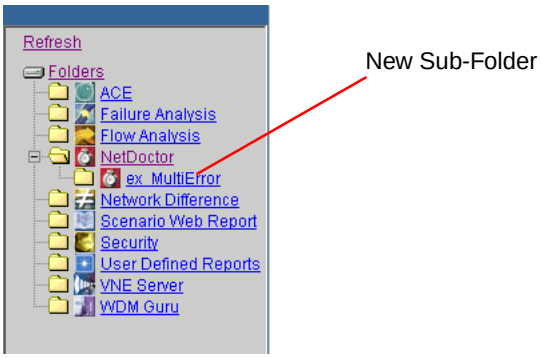
7.1 Click the **Apply Filters** button.

7.2 Click **OK** when asked to confirm that you want to apply filters.

8 Click **Refresh** in the Browse Reports navigational frame.

➥ The NetDoctor reports folder now has a **+** to the left of the icon, indicating that there are sub-folders under the main folder.

New Sub-Folder in Browse Reports List



9 Click the **+** and observe that your new sub-folder is listed.

10 Click on the **<initials>_MultiError** sub-folder.

➥ Since you applied the same filter that is applied to the top level NetDoctor folder, notice that you see the same reports list as in the NetDoctor folder.

Create a New Filter

Creating a new filter is not difficult to do and gives you the greatest amount of control over the reports in your sub-folders. In this section, you will create a filter and apply it to a sub-folder.

You are looking for major problems in the network and specifically want to see NetDoctor reports with more than 5 errors. To do this, you must specify report attributes in a filter for the selected criteria. You then apply the filter to a sub-folder to get the desired results.

Perform the following steps to create and apply the filter:

1 Click on **Settings** in the top menu.

➥ **Filter Definition** opens as the default Settings choice.

2 Create the new filter.

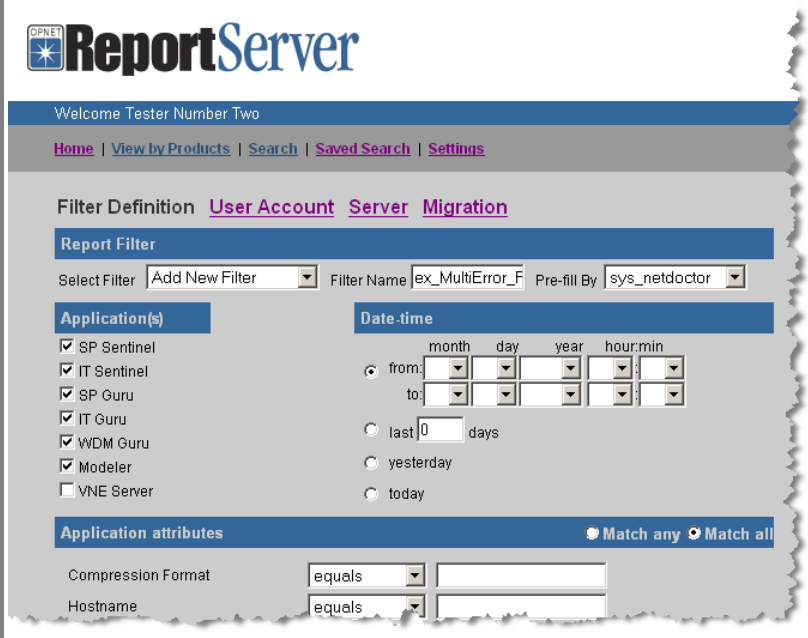
2.1 Select **Add New Filter** in the Select Filter drop-down menu.

2.2 Type **<initials>_MultiError_Filter** as the Filter Name. Enter your initials to distinguish this filter from other similar filters.

2.3 Select **sys_netdoctor** from the Pre-fill by drop-down menu.

➥ These settings let you add a new filter by starting from the baseline settings of an existing filter.

Report Filter Definition

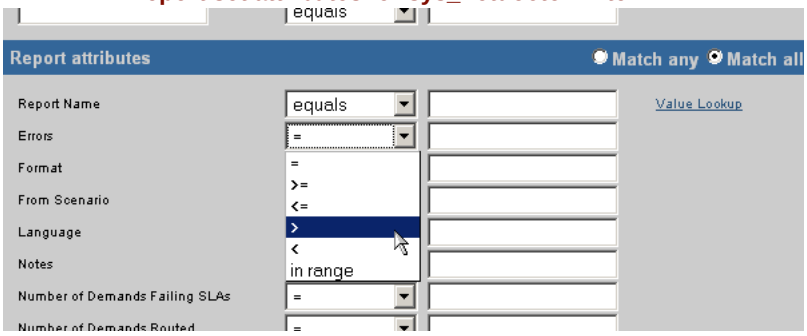


3 Create additional attributes.

3.1 Scroll down to the **Report Attributes** section.

3.2 Click on the drop-down conditions menu next to **Errors**.

Report set attributes for sys_netdoctor Filter

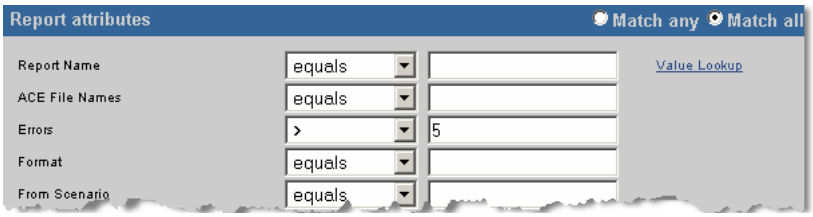


3.3 Choose the **>** sign to indicate you want to match conditions greater than the value you specify.

3.4 Specify **5** as the match value.

Be sure that the radio button for **Match all** is still selected.

Match Errors Greater Than Value



4 Save the new filter by scrolling to the bottom of the page and clicking the **Save** button.

➥ You can now use your filter to provide you with only NetDoctor reports with more than 5 errors.

5 Clear report references from the **<initials>_MultiError** sub-folder.

Before applying a new filter, you must Clear any report references already contained in the sub-folder. Regardless of any new filters applied, the sub-folder contains references to old reports unless you use the Clear function.

5.1 Click on the **Home** link.

5.2 Click on the **NetDoctor** folder.

5.3 Click on **Edit Sub-Folders**.

5.4 Click on the checkbox in the **Clear** column next to the **<initials>_MultiError** sub-folder, and click on the **Clear** button.

➥ The Clear function removes all report references from the **<initials>_MultiError** sub-folder.

5.5 Click **OK** to confirm that you want to clear reports from the **<initials>_MultiError** folder.

6 Apply the new filter to your **<initials>_MultiError** sub-folder.

6.1 Click on **Select Filters** next to the **<initials>_MultiError** sub-folder.

6.2 Click on **sys_netdoctor** in the Current Filters window and click the **<<** button to remove it from the Current Filters column.

6.3 Locate your new filter, **<initials>_MultiError_Filter**, in the All Filters window. Click on the **>>** button to move it to the Current Filters column.

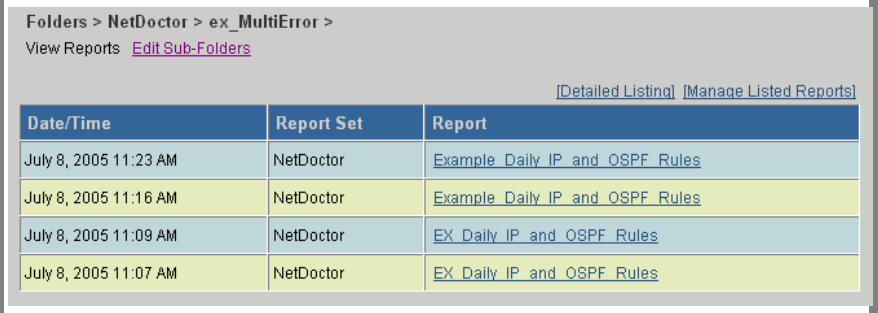
6.4 Click **OK**.

6.5 Click on the checkbox in the **Apply Filters** column next to the **<initials>_MultiError** sub-folder, and click the **Apply Filters** button.

7 Click on the **<initials>_MultiError** sub-folder link in the Folders window.

➥ Observe that your reports are all NetDoctor reports with more than 5 errors.

New Filter Applied to <initials>_MultiError Sub-Folder


Folders > NetDoctor > ex_MultiError >

View Reports Edit Sub-Folders

[Detailed Listing] [Manage Listed Reports]

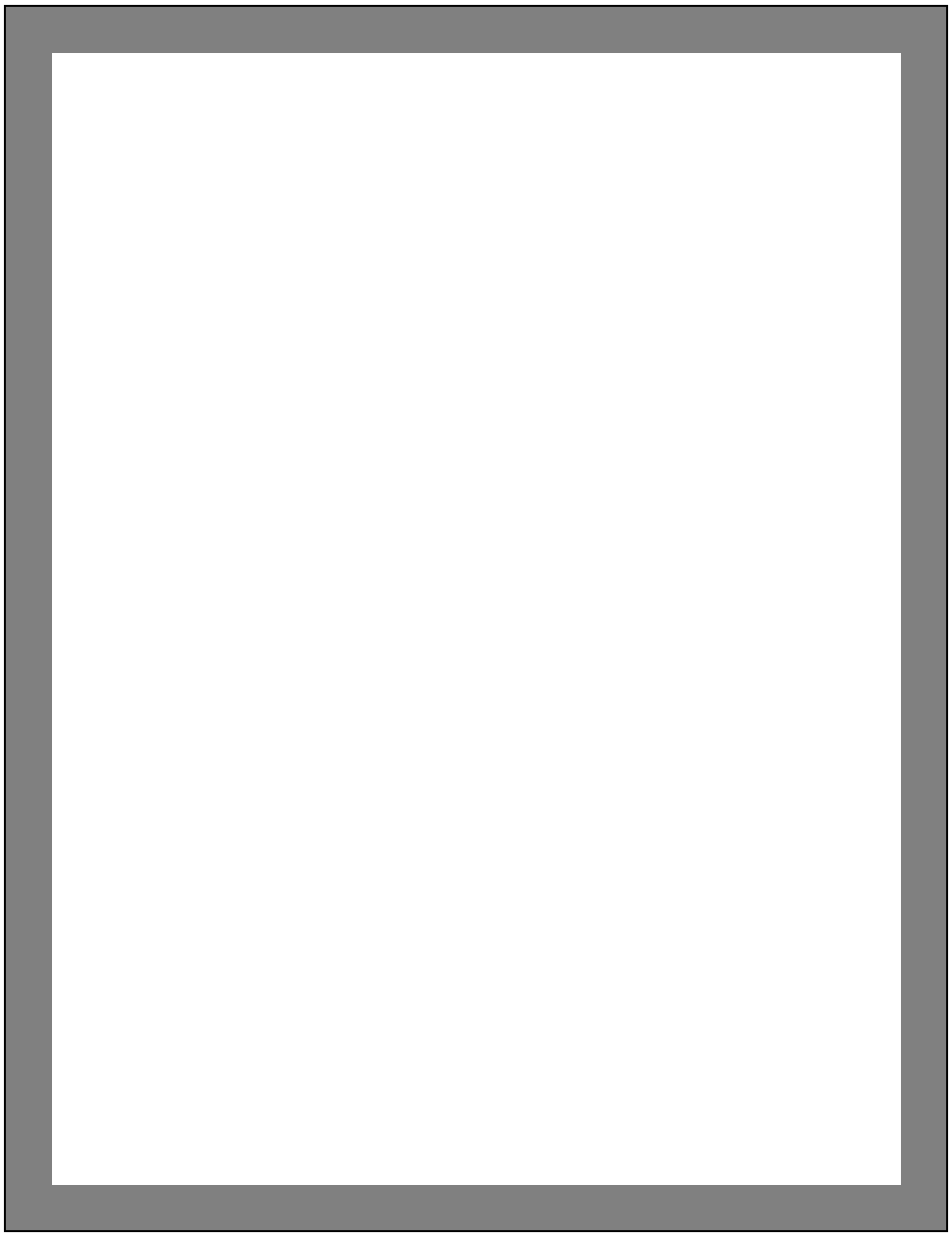
Date/Time	Report Set	Report
July 8, 2005 11:23 AM	NetDoctor	Example_Daily_IP_and_OSPF_Rules
July 8, 2005 11:16 AM	NetDoctor	Example_Daily_IP_and_OSPF_Rules
July 8, 2005 11:09 AM	NetDoctor	EX_Daily_IP_and_OSPF_Rules
July 8, 2005 11:07 AM	NetDoctor	EX_Daily_IP_and_OSPF_Rules

The listing of reports shown is based on completing all prerequisite Sentinel tutorials prior to this tutorial.

Summary

In this tutorial, you learned how to perform the following actions:

- Log on to the Report Server
- View reports by folder and sub-folder
- View reports by time and date
- Use the search page
- Work with folders and sub-folders
- Work with filters



App A Troubleshooting Sentinel Tutorials

Troubleshooting Sentinel Tutorials

Introduction

This document contains information that can help you correct common problems.

- The OPNET Installation Directory
- The tutorial_req Files
- Saving Tutorial Files
- Additional Help

The OPNET Installation Directory

To complete the tutorials, you must install the Sentinel standard models, which include the required tutorial models. The standard models are normally installed when you install the Standard Model Library.

Sentinel standard models apply to common protocols and vendor devices. The standard models are in the subdirectories under the OPNET release directory (<**reldir**>):

<reldir**>\models\std\<protocol_name>**

<reldir> describes the directory that contains the current Sentinel software.

You can find your **<reldir>** by doing the following:

1. In the main menu, select **Help > About This Application**.
2. In the **About** Sentinel dialog box, click on the **Environment** tab, then expand the **System Information** section.
3. Under **System Information**, find the **OPNET release directory**.

For example, the **<reldir>** for a default installation of this release of Sentinel on Windows is

C:\Program Files\OPNET\11.5.A

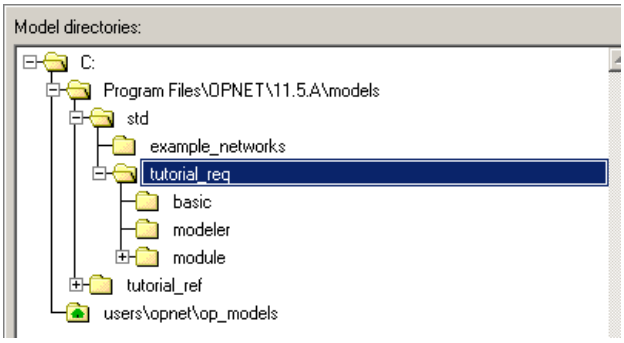
The tutorials use the Windows convention of the backslash character (\) as the separator in directory pathnames.

The tutorial_req Files

When you do a tutorial, you are asked to open specific tutorial model files. These model files are *required* to do the tutorial; they are located in the **<reldir>\models\std\tutorial_req** directory or its subdirectories.

When you are asked to open supplied model files, make sure you navigate the directory structure in OPNET's open file browser (in the left pane) to the **tutorial_req** directory.

Navigating to the tutorial_req Directory

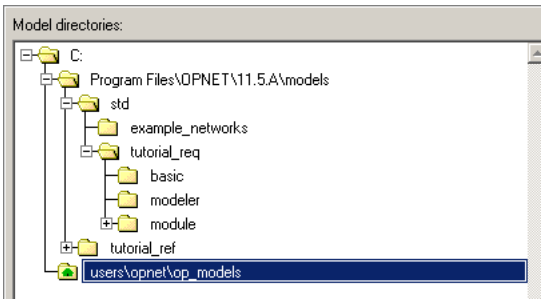


Saving Tutorial Files

In several tutorials, you will be asked to open an OPNET model file and save it with a unique prefix, such as your initials (<your_initials>). This way, several users can create and complete their own copy of the same tutorial without interfering with each others' work.

When you save a new model file, or use the **Save As...** command to save an edited model file with your initials, remember to navigate to your OPNET default model directory (normally **<home>\op_models**) to save your files.

Navigating to the op_models Directory



If you do not navigate to your default model directory (normally **<home>\op_models**) when you do a **Save As...** operation, the file is automatically saved in the current model directory.

Additional Help

If an analysis does not complete, the problem might be with the installation.

1. Read the installation instructions on the CD case.
2. Check the website for recent updates to the tutorials, models, and product installation instructions (**www.opnet.com/support**).
3. Check the FAQ section of the OPNET website (**www.opnet.com/support**).