This documentation and any related computer software help programs (hereinafter referred to as the "Documentation") are for your informational purposes only and are subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be used or disclosed by you except as may be permitted in a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO THE END USER OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2008 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.
CA Product References

This document references the following CA products:

- CA eHealth® (eHealth)
- CA SPECTRUM® (SPECTRUM)
- CA eHealth® Live Health® Application (eHealth Live Health Application)
- CA Embedded Entitlements Manager (CA EEM)

Contact CA

Contact Technical Support

For your convenience, CA provides one site where you can access the information you need for your Home Office, Small Business, and Enterprise CA products. At http://ca.com/support, you can access the following:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Provide Feedback

If you have comments or questions about CA product documentation, you can send a message to techpubs@ca.com.

If you would like to provide feedback about CA product documentation, complete our short customer survey, which is also available on the CA Support website, found at http://ca.com/docs.
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Override Mappings</td>
<td>34</td>
</tr>
<tr>
<td>Authentication Options</td>
<td>35</td>
</tr>
<tr>
<td>How To Enable One-way Authentication from SPECTRUM to eHealth</td>
<td>35</td>
</tr>
<tr>
<td>Error Handling</td>
<td>38</td>
</tr>
<tr>
<td>Use Advanced Logging Troubleshooting Tool</td>
<td>39</td>
</tr>
<tr>
<td>Setup Name Synchronization</td>
<td>40</td>
</tr>
<tr>
<td>Distributed Web Services Calls</td>
<td>42</td>
</tr>
<tr>
<td>Configure Distributed Web Services Calls</td>
<td>43</td>
</tr>
<tr>
<td>Special Web Configurations</td>
<td>43</td>
</tr>
<tr>
<td>How to Set Up Access to Traffic Accountant Reports</td>
<td>44</td>
</tr>
<tr>
<td>Tomcat Logs Files</td>
<td>44</td>
</tr>
<tr>
<td>Chapter 4: SPECTRUM Usage</td>
<td>47</td>
</tr>
<tr>
<td>Tasks</td>
<td>47</td>
</tr>
<tr>
<td>Run Reports from the SPECTRUM OneClick Console</td>
<td>47</td>
</tr>
<tr>
<td>View Trend Reports</td>
<td>48</td>
</tr>
<tr>
<td>View At-a-Glance Reports</td>
<td>48</td>
</tr>
<tr>
<td>View Traffic Accountant Reports</td>
<td>49</td>
</tr>
<tr>
<td>View eHealth Reports for Alarms</td>
<td>49</td>
</tr>
<tr>
<td>View Alarm Detail Reports</td>
<td>50</td>
</tr>
<tr>
<td>Clear Alarms</td>
<td>50</td>
</tr>
<tr>
<td>Run Synchronized Discovery</td>
<td>51</td>
</tr>
<tr>
<td>Monitor eHealth Discoveries</td>
<td>51</td>
</tr>
<tr>
<td>Chapter 5: eHealth Usage</td>
<td>53</td>
</tr>
<tr>
<td>Run Reports from the eHealth Console</td>
<td>53</td>
</tr>
<tr>
<td>Launch the OneClick Console</td>
<td>54</td>
</tr>
<tr>
<td>Clear SPECTRUM Alarms</td>
<td>54</td>
</tr>
<tr>
<td>Appendix A: Legacy Utilities</td>
<td>55</td>
</tr>
<tr>
<td>Run the Setup Program</td>
<td>55</td>
</tr>
<tr>
<td>How to Configure the Integration From the Command Line</td>
<td>57</td>
</tr>
<tr>
<td>How to Configure the Integration With a SPECTRUM OneClick Server Running SSL</td>
<td>58</td>
</tr>
<tr>
<td>Index</td>
<td>61</td>
</tr>
</tbody>
</table>
Chapter 1: eHealth SPECTRUM Integration

This section contains the following topics:

Introduction (see page 7)
Integration Overview (see page 7)

Introduction

This guide describes how to set up the integration between eHealth r6.1 and SPECTRUM r9.0 and use the features to perform tasks, run reports and synchronized discovery, and clear alarms.

Integration Overview

eHealth and SPECTRUM integration helps you maintain critical service levels across complex network environments by combining eHealth’s automated availability and performance management with the SPECTRUM network service and analysis platform.

SPECTRUM manages networks, pinpoints and corrects problems, and alerts you to changes in network or device status. The system creates a model of every entity in the network, including cables, network devices, servers, and applications. SPECTRUM provides a seamless view of the enterprise network.

eHealth’s historical data and automated reporting capabilities automate the tasks of calculating long-term trends, providing a baseline for network resources, and providing performance reports for critical network components such as backbones, server clusters, and Internet links. eHealth also offers proactive troubleshooting and capacity planning features.

The eHealth and SPECTRUM integration gives you significant time and productivity benefits. The integration lets you:

- Use eHealth to automatically discover devices managed by SPECTRUM, eliminating the need to manually re-enter and continually update configuration data.
- Access eHealth reports, such as At-a-Glance and Trend, directly from the SPECTRUM OneClick topology, giving you a quick overview of device status and in-depth historical information.
- Manage Live Exceptions alarms from the SPECTRUM OneClick console, view Alarm Detail reports, and clear alarms to reduce the mean-time-to-repair for network issues.

- Access eHealth reports from SPECTRUM alarms, giving you a historical context for more effective troubleshooting.

- Use eHealth for capacity planning, proactive troubleshooting, performance optimization, and service level management of your network components managed by SPECTRUM.
Chapter 2: Setup Information and Checklist

This section contains the following topics:

Setup Time (see page 9)
System Requirements (see page 9)
Software Configuration (see page 10)
OneClick Server Roles (see page 11)
Setup Checklist (see page 12)

Setup Time

The setup process typically requires the following time estimates:

<table>
<thead>
<tr>
<th>Task</th>
<th>Time Estimate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set up the integration</td>
<td>1.5 to 6 hours</td>
</tr>
<tr>
<td>Verify requirements and complete the setup checklist</td>
<td>1 hour</td>
</tr>
<tr>
<td>Add a license</td>
<td>10 minutes</td>
</tr>
<tr>
<td>Run the setup program and configure alarms</td>
<td>30 minutes</td>
</tr>
<tr>
<td>Configure SPECTRUM Global Collections, run eHealth discovery, and map elements to models. The mapping time depends on the size of the environment, and could be longer in large environments.</td>
<td>15 minutes – 5 hours</td>
</tr>
</tbody>
</table>

System Requirements

Before you run the eHealth SPECTRUM Integration setup program, verify that your eHealth and SPECTRUM systems meet the following requirements:

- eHealth System – eHealth r6.1. This release supports Solaris, Windows, and HP-UX platforms.

  **Note:** SPECTRUM 9.0 is also backwards compatible with eHealth 6.0 SP2.

- SPECTRUM OneClick Server – SPECTRUM r9.0. This release supports Solaris, Windows, and Linux platforms.
Important! eHealth should be installed on a dedicated system. Do not install it on the same system as SPECTRUM.

The following system and environment requirements should also be considered:

- Devices should not be in a secure domain, otherwise the integration will not function properly. Devices should be modeled in SPECTRUM to enable element-model mapping and alarm processing.
- IPv6 is not supported on eHealth r6.1. Thus, element-model mappings and synchronized discovery do not support eHealth servers or eHealth elements using IPv6.

Note: For information about installing eHealth software, see the eHealth Installation Guide. For information about installing SPECTRUM software, see the SPECTRUM Installation Guide.

Software Configuration

There are three basic configurations for the eHealth and SPECTRUM integration, described in the following list. Multiple standalone eHealth systems without Distributed eHealth are not supported.

Single eHealth System, Single (Separate) SPECTRUM Server

Includes a SPECTRUM OneClick server and a SpectroSERVER, which can be separate systems. No special steps are required for this configuration.

Single eHealth System, Multiple SPECTRUM Servers

Lets you configure eHealth to monitor multiple SPECTRUM servers, all of which can view eHealth reports. However, eHealth Live Health Application alarms can only be sent to one SPECTRUM server. When configuring Live Exceptions or Health reports to forward traps, specify a single SpectroSERVER to handle all traps. The SPECTRUM Main Location Server is the recommended destination.

Distributed eHealth, Multiple SPECTRUM Servers

Lets you use Distributed eHealth to connect multiple eHealth systems with multiple SPECTRUM servers. When using Distributed eHealth:

- Configure each Distributed eHealth System with discovery policies and assign each policy to a separate Global Collection on the SPECTRUM OneClick server.
- Configure each Distributed eHealth System to forward Live Exceptions traps to the single SPECTRUM Main Location Server, as above.
• Configure Health reports on each eHealth system and the Distributed eHealth Console to forward traps to the single SPECTRUM Main Location Server.

• Configure SPECTRUM to access reports on a single Distributed eHealth Console (front end).

In this configuration, the SPECTRUM OneClick server can display alarms and view reports from any eHealth system.

OneClick Server Roles

The SPECTRUM OneClick server uses web services provided by the eHealth server to perform the integration features that are configured. Some features, such as requesting discovery policy information, are needed by all OneClick servers. Other features, such as element mapping, only need to be performed by a single server.

**Note:** Server roles do not impact eHealth report launching from OneClick. If the eHealth server information is configured on a OneClick server, clients of that server can launch eHealth reports regardless of server roles.

The roles that a OneClick server can take are as follows:

**Disabled**

This is the default role if a server is not configured for integration with an eHealth server. There is no communication with the eHealth server. OneClick clients of this server will not be able to configure synchronized discovery.

**Passive**

This is the default role when configuring the integration with the eHealth server. The only communication with the eHealth server is to obtain server and discovery configuration data. If clients of this OneClick server need to configure synchronized discovery, the server must be in a Passive or Active role.

**Active**

A OneClick server in an Active role communicates with the eHealth server to obtain server and discovery configuration data, but it also is used to run the element-to-model mappings and request discoveries. Clients of an Active server can configure synchronized discovery.

In networks with only one OneClick server, the server role should be set to Active. In management networks with multiple OneClick servers, there should be one and only one OneClick server in an Active role.

If regions are being configured there should be one active server per region.
Setup Checklist

For each SPECTRUM OneClick server you want to configure, copy and complete the Setup Checklists that follow. The checklists help you to supply the information for the setup program.

<table>
<thead>
<tr>
<th>Computer</th>
<th>Information</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SPECTRUM OneClick Server:</strong></td>
<td>The Hostname or IP Address of the SPECTRUM OneClick server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Port Number on which OneClick listens for Web requests.</td>
<td><strong>Default:</strong> 80</td>
</tr>
<tr>
<td></td>
<td>The Path where OneClick is installed on the server.</td>
<td><strong>Default:</strong> spectrum</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Use the default value unless you specified another path when installing OneClick.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>User name and Password for accessing this host.</td>
<td>User name:</td>
</tr>
<tr>
<td></td>
<td>Password:</td>
<td></td>
</tr>
<tr>
<td><strong>SPECTRUM OneClick Server roles:</strong></td>
<td>The servers that will act in an active or passive role in your SPECTRUM environment. There should be one and only one server in an Active role in your SPECTRUM environment. If regions are being configured there should be one active server per region.</td>
<td></td>
</tr>
<tr>
<td><strong>SpectroSERVER:</strong></td>
<td>The Hostname of the SpectroSERVER that is configured to receive traps from eHealth.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The IP address of the SpectroSERVER that is configured to receive traps from eHealth.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Port Number on which the SpectroSERVER receives traps.</td>
<td><strong>Default:</strong> 162</td>
</tr>
<tr>
<td><strong>eHealth Server:</strong></td>
<td>The Hostname or IP Address of the eHealth server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you use Distributed eHealth, this server must be an</td>
<td></td>
</tr>
</tbody>
</table>
## Computer Information

<table>
<thead>
<tr>
<th>Computer Information</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>eHealth Distributed console.</td>
<td></td>
</tr>
</tbody>
</table>
| The Port Number on which eHealth listens for Web requests. | **Default:** 80  
**Note:** If you use Distributed eHealth, this server must be an eHealth Distributed console. |
| Password for the eHealth username "admin". | **Password:** |
| **Note:** If you use Distributed eHealth, the user must be valid on all eHealth systems. |       |
| The maximum number of traps eHealth Live Exceptions sends per second. This value is defined by the NH_TRAPS_PER_SECOND environment variable. | **Default:** 100 |
| The maximum number of traps to queue to the Live Exceptions notifier server at one time. This value is defined by the NH_TRAP_GOVERNOR_SIZE environment variable. | **Note:** This should be based on the number of alarms that are expected in a single eHealth polling cycle. Increasing the NH_TRAP_GOVERNOR_SIZE will increase the memory used in the process of notifying SPECTRUM of new/cleared alarms. However, if this size is too low some alarm notifications may not make it to SPECTRUM. | **Default:** 1000 |

For more information about eHealth environment variables, see the *eHealth Command and Environment Variables Reference Guide*. 
Chapter 3: Setup

This section contains the following topics:

- Add a License (see page 15)
- Setup Program (see page 15)
- Password for Naming and Discover Web Services (see page 16)
- Configure the eHealth Alarm Notifier (see page 16)
- Configure Health Reports (see page 17)
- Configure SPECTRUM to Recognize the eHealth Server and to Clear Alarms (see page 18)
- Alarm Configuration (see page 19)
- How to Create SPECTRUM Global Collections (see page 23)
- Synchronized Discovery (see page 24)
- Map eHealth and SPECTRUM Elements (see page 31)
- Authentication Options (see page 35)
- Setup Name Synchronization (see page 40)
- Distributed Web Services Calls (see page 42)
- How to Set Up Access to Traffic Accountant Reports (see page 44)
- Tomcat Logs Files (see page 44)

Add a License

eHealth r6.1 does not require a license to use the SPECTRUM 9.0 integration. However, if you are using an earlier release of eHealth (prior to r6.0 SP1) with an earlier release of SPECTRUM (prior to SPECTRUM 8.1), and you have a SPECTRUM license key, you can enter the license using the eHealth Console interface.

For information about how to enter license information, see the eHealth Installation Guide.

For information about integrating earlier releases of eHealth and SPECTRUM, see the corresponding eHealth SPECTRUM Integration User Guide for those releases.

Setup Program

The nhSpectrumSetup utility is being phased out. It can be used to change the SPECTRUM setup for previously scheduled and scripted discoveries using the SPECTRUM Import functionality.

Note: For information about how to run the utility, see Appendix A.
Password for Naming and Discover Web Services

When upgrading your eHealth installation, naming and discover web services using the front end must be configured with non-default admin password if the admin user password is not the default, otherwise the web service calls will fail.

You must either update the password on all computers or update the front end to another value then back to the original one.

**Note:** This does not apply to fresh installations of eHealth because password is initially the default and updating the password also updates the table where the admin password is stored for access by web services.

Configure the eHealth Alarm Notifier

If you use eHealth Live Health Application, you can configure the Live Exceptions browser to forward eHealth Live Health Application alarm traps to a SpectroSERVER.

**To configure Live Exceptions to forward traps**

1. Launch the Live Exceptions browser.
2. Select Setup, Trap Destinations.
   The Trap Destinations Manager dialog appears.
3. Click New.
4. Using the Setup Checklist, specify the following under Edit Trap Destination:
   - Hostname of the SpectroSERVER.
   - IP address of the SpectroSERVER.
   - Port number for the SpectroSERVER.
5. Click Add.
6. Confirm that the name of the SpectroSERVER appears in the Existing Trap Destinations list, and click OK.
7. Select Setup, Notifier Rules.
   The Notifier Manager dialog appears.
8. Click New.
   The Notifier Rule Editor dialog appears.
9. Do the following:
   a. Enter SPECTRUM in the Name field.
   b. Select Send Trap in the Action list.
   c. Select the SpectroSERVER you specified in Step 4 in the To NMS list.
   d. Select both Raised and Cleared under When an Alarm Is.
   e. Specify either a specific subject or All Subjects under Elements Within.
   f. Click OK.
   Your Notifier rule is saved.

Configure Health Reports

You can also configure individual Health reports to forward traps for Health exceptions to the SpectroSERVER. When the scheduled Health report runs, eHealth sends an SNMP trap to the SpectroSERVER for each element in the Exceptions section of the Health report.

Only scheduled Health reports forward exceptions. If you run a Health report on-demand, it will not forward exceptions.

To forward exceptions from Health reports
1. Launch the eHealth Console.
2. Select Reports, Customize, Health Reports.
3. Select the report from which you want to forward Health exceptions.
4. Select General from the Presentation Attributes drop-down list.
5. Select NMS IP and Port Trap Address in the Attribute table.
6. Specify the SpectroSERVER IP address and port number, separated by a colon, in the Value field. For example: 001.02.03.004:162
7. Select Exceptions from the Presentation Attributes drop-down list.
8. Select Send Exceptions SNMP Trap in the Attribute table.
9. Select Yes in the value field.
10. Click OK.
Configure SPECTRUM to Recognize the eHealth Server and to Clear Alarms

After completing the eHealth setup, you must also configure SPECTRUM to recognize the eHealth server or Distributed eHealth console.

To enable SPECTRUM to access eHealth reports
1. Log in to the SPECTRUM OneClick home page as a SPECTRUM Administrator.
2. Click Administration.
   The Administration Pages menu appears.
3. Select eHealth Configuration.
   The eHealth Configuration window appears.
4. Enter the following information:

   **eHealth Server Name**
   Specifies the hostname or IP address of the eHealth server.

   **eHealth Server Port**
   Specifies the port number on which eHealth listens for Web requests.

   **eHealth Admin Password**
   Specifies the password for the user name "admin".

   **OneClick Server Role**
   Specifies what role this OneClick server will perform in the network.

   **SSL access required**
   Specifies that the eHealth server uses Secure Sockets Layer (SSL) for secure web communications when this field is set to Yes.

   **Use legacy report launching (SPECTRUM Release 8.1 and later)**
   Setting this field to no displays the drill-down report options only for those models in SPECTRUM that are mapped to eHealth elements. If you select yes, drill-down options appear for all host, router, switch, and port models. In this configuration, eHealth attempts to find the appropriate element on which to report. If eHealth cannot find an appropriate element, an error message appears when you try to drill-down to an eHealth report for that model.

5. Select Active in the Alarm Notifier for eHealth Status section to enable SPECTRUM to clear eHealth Live Health Application alarms.

   If you configure eHealth to forward alarms to SPECTRUM and configure SPECTRUM to view eHealth alarms, the alarm notifier lets you clear those alarms directly from the OneClick console.
6. (Optional) Click Test to verify that the server name, port, user name, and password result in a successful connection to the eHealth server.

7. Click Save.

**Alarm Configuration**

If you configured eHealth to forward eHealth Live Health Application alarms or Health exceptions to a SpectroSERVER, you must also configure SPECTRUM to receive the alarms.

For integration purposes, the eHealth server may be represented by either an EventAdmin or a Host_systemEDGE model type in SPECTRUM. If the eHealth server is running a SystemEDGE agent, we recommend that you use the Host_systemEDGE model type. If the eHealth server is not running a SystemEDGE agent, then you must use an EventAdmin model.

**Modeling Considerations**

The following recommendations should be considered when creating models:

- **Polling servers**—You only need one model for each polling server. Each model processes eHealth alarms for its corresponding eHealth server. In a distributed SPECTRUM environment, we recommend that the polling server model is placed on the Main Location Server (MLS) because the MLS is traditionally lightly loaded with other models. However, if you want to balance the alarm processing load across several SpectroSERVERs, each polling server can be modeled on the SpectroSERVER of your choice.

- **Distributed eHealth Console**—The Distributed eHealth Console server that is referred to in the following procedure must be modeled on each SpectroSERVER in a distributed SPECTRUM environment. If the Distributed eHealth Console is running a SystemEDGE agent, it should be modeled using a Host_systemEDGE model type on only one landscape. The Distributed eHealth Console should be modeled using the EventAdmin model type on the remaining landscapes to avoid duplication of agent management.

- **Standalone eHealth server**—You must model the standalone eHealth server on each landscape in your SPECTRUM environment. In a distributed SPECTRUM environment one of these models will be used for alarm processing. We recommend that the model on the MLS is configured for alarm processing, but any of the server models may be used. If the standalone eHealth server is running a SystemEDGE agent, it should be modeled using a Host_systemEDGE model type on only one landscape. The distributed console should be modeled using the EventAdmin model type on the remaining landscapes to avoid duplication of agent management.
The following diagram illustrates the modeling considerations:

![Diagram](image.png)

**Note:** Standalone eHealth servers should be modeled similarly to a Distributed eHealth Console.

**Configure SPECTRUM to View eHealth Alarms**

You must also configure SPECTRUM to receive the alarms if you configured eHealth to forward eHealth Live Health Application alarms or Health exceptions to a SpectroSERVER.

**To enable SPECTRUM to view eHealth alarms**

1. Select Start Console at the top of the OneClick page to launch the OneClick Console, and log in as a SPECTRUM administrator.
2. Select your SpectroSERVER, and select Universe on the Explorer tab of the OneClick Navigation panel.
3. Select Universe under the Landscape for the Main Location Server SpectroSERVER, if you are monitoring multiple SpectroSERVERs.
4. Select the Topology tab on the Contents panel. Click the Create a New Model by Type icon in the Topology tab toolbar area.
   The Select Model Type dialog appears.
5. Select the All Model Types tab. Select EventAdmin or Host_systemEDGE, and click OK.

   The Create Model of Type dialog appears.

6. Enter the name and IP address of the eHealth server or Distributed eHealth console, and click OK.

   The eHealth server is added to the topology as the selected model type.

   **Note:** For more information about creating a model in OneClick, see the *SPECTRUM Modeling Your IT Infrastructure Administrator Guide*.

7. Repeat steps 3 through 6 on each SpectroSERVER you are monitoring to create models representing the eHealth server or Distributed eHealth console. Create only one Host_systemEDGE model for the server.

8. Repeat steps 3 through 6 on the SpectroSERVER of your choice (we recommend using the Main Location Server) to create models representing each eHealth server that will be sending Live Exceptions alarms to the SpectroSERVER.

   **Note:** The remaining steps are only needed on the Main Location Server SpectroSERVER or the models representing eHealth servers that will be sending Live Exceptions alarms to the SpectroSERVER.

9. Select the server model in the OneClick Topology.

10. Select the Attributes tab in the Component Detail panel.

11. Double-click map_traps_to_this_model_using_IP_header in the left window of the Attributes panel.

    The attribute is added to the right window of the Attributes panel.

12. Double-click map_traps_to_this_model_using_IP_header in the right pane, and select Yes. Click OK.

13. Select SBG_AlertForwardingEnabled in the left window of the Attributes panel.

    The attribute is added to the right window of the Attributes panel.

14. Double-click SBG_AlertForwardingEnabled in the right window, and select Yes. Click OK.
15. Double-click traps_per_sec_storm_threshold in the left window of the Attributes panel.

The attribute is added to the right window of the Attributes panel.

16. Double-click traps_per_sec_storm_threshold in the left window of the Attributes panel, and set the value to the maximum number of traps eHealth sends per second. Click OK.

The value is saved.

**Note:** If you are using Host_systemEDGE models, you must create and assign a container for these models after you configure SPECTRUM to view alarms.

### Create and Assign a Container to a Host_systemEDGE Model

The EventAdmin model is a container model. If an eHealth alarm is generated for a device that is not monitored in SPECTRUM, an EventModel representing that device is created in the EventAdmin container. Since Host_systemEDGE models are not containers, you must create a container for these models in SPECTRUM and assign the container to the Host_systemEDGE model. The same container may be used for multiple eHealth servers represented by Host_systemEDGE models.

**To create and assign a container**

1. Select the Universe on the landscape where your alarm processing Host_systemEDGE model is defined.
2. Select the Topology tab.
3. Click the Create Model by Type icon.
4. Select LAN from the Container tab in the Select Model Type dialog. Click OK.
5. Give the model a name (such as Unmanaged eHealth Alarms), and click OK.
6. Select the new container model in the Topology view.
7. Select the Attributes tab in the Component Detail panel.
8. Double-click model_handle in the left window.

   The attribute moves to the right window of the Attributes panel. Note the model handle shown in the right window.
9. Select the Host_systemEDGE model in the topology view.
10. Select the Attributes tab in the Component Detail panel.
11. Double-click EventModelContainerHandle in the left window.
   The attribute will be moved to the right window of the Attributes panel.
12. Double-click EventModelContainerHandle in the right window.
   Change the value to the model handle noted in step 8 above.

**Migrate from an EventAdmin Model to a Host_systemEDGE Model**

Any EventModels that have been generated in the EventAdmin container must be manually copied to the new container created in the previous section.

**To manually copy models to a container**

1. Select the EventAdmin model in the SPECTRUM OneClick Explorer view.
2. Select the List tab in the Contents panel.
3. Select all EventModel models in the list.
4. Click the copy icon in the tool bar.
5. Select the new LAN container in the OneClick Explorer view.
6. Select the Topology tab.
7. Click the paste icon.
   
   **Note:** After you copy the models to the new container, you should destroy the old EventAdmin model to avoid alarm duplication.

**How to Create SPECTRUM Global Collections**

Global Collections help you organize the network elements managed by SPECTRUM into logical groups in the SPECTRUM OneClick Topology.

eHealth uses specified Global Collections as a starting point to discover network elements managed by SPECTRUM. Therefore, before running the eHealth discover process, use Global Collections to specify which network elements you want eHealth to monitor.
To create a Global Collection, follow this process:

1. Log in to the SPECTRUM OneClick Console.
2. Create one or more Global Collections containing the devices you want to monitor with eHealth.
   
   **Note:** Devices within container models will not be discovered. Device models must be at the top-level of the Global Collection to be discovered.
3. If you are using Distributed eHealth, you must create a separate Global Collection for each Distributed eHealth System, so that different eHealth systems are not polling the same device.

For more information about SPECTRUM Global Collections, see the *SPECTRUM Modeling Your IT Infrastructure Administrator Guide*.

### Synchronized Discovery

Synchronized discovery is performed one-way from SPECTRUM to eHealth and reduces the effort of having to perform discovery on both products.

You can perform synchronized discovery for the following cases:

- New discovery from a global collection of specific models (devices)
- New discovery when device models are added to a global collection.
- Rediscover when a device is reconfigured

**Note:** Synchronized discovery is not supported on remote pollers.

eHealth discovery is policy based and permits the storage and reuse of the environment under which an element was originally discovered. It also provides control over the following properties:

- **Discover Properties** – finder controls and environment variables
- **Match/Merge Properties** – determines the key components for matching and merging devices and elements
- **Configuration Properties** – includes element naming, group inclusion, element exclusion, and so on

SPECTRUM uses its near real-time fault system to push a scheduled discovery to eHealth. The global collections are used to identify the set of device models to synchronize. You create a new eHealth discovery policy and associate it with a global collection.

**Note:** Devices within container models will not be discovered. Device models must be at the top-level of the Global Collection to be discovered.
The eHealth web services are leveraged to notify eHealth of any membership changes, reconfiguration changes, or manual requests to invoke eHealth discovery for a model set.

If a GlobalCollection is configured for Synchronized Discovery, SPECTRUM monitors the device models in the GlobalCollection for the following types of changes:

- **Membership Changes** - SPECTRUM detects when new members are added to a global collection and requests an eHealth discovery if configured to do so. A device model can be a member of more than one synchronized global collection, but this is not a recommended configuration. As such, SPECTRUM raises an alarm on models in this scenario.

  **Note:** eHealth is not notified if a device is removed from a synchronized global collection.

- **Model Reconfiguration** - If SPECTRUM detects a reconfiguration of a device model, it requests an eHealth discovery if configured to do so.

You can configure and manually request eHealth discoveries from any SPECTRUM OneClick console that is configured in a Passive or Active role. When SPECTRUM makes the request to the eHealth server it will come from the OneClick server in an Active role.

Each eHealth server should execute only one discovery at a time. Therefore, when multiple discovery requests are needed, SPECTRUM queues the requests and sends one request per eHealth server at set intervals.

In a Distributed eHealth environment, any new or modified elements that are discovered using Synchronized Discovery will not be available for mapping until the Element Synchronize job executes on the Distributed Console. These new or updated elements are automatically mapped on the next Incremental Mapping after the Element Synchronize job completes. We recommend that you activate the Legacy Report Launching feature to permit users to access reporting for new elements.

**How To Set Up Synchronized Discovery**

Synchronized discovery involves the eHealth server and a SPECTRUM OneClick server in an active role. Additional SPECTRUM OneClick servers can be configured in a passive role to let clients configure and request discoveries.

To set up synchronized discovery for the first time, follow this process:

1. Configure the synchronization interval and optional name synchronization on the active SPECTRUM OneClick server.
2. Configure additional passive SPECTRUM OneClick servers.
3. Create or edit a discover policy on the eHealth server to be used in SPECTRUM.

4. Configure SPECTRUM to trigger automatic discovery requests.

5. Add the policy to a GlobalCollection on a SPECTRUM OneClick client.

6. Request a discovery. (Automatic discovery requests can also be enabled.)

**Note:** eHealth Manager privileges can be disabled to prevent SPECTRUM users from seeing eHealth information.

### Configure the Active SPECTRUM OneClick Server

The default synchronization interval is 5 minutes. However, you set the interval depending on the number of devices in your synchronized GlobalCollections. The more devices in your environment, the longer the interval needed to ensure that the discovery request queue functions smoothly.

This procedure assumes you already have eHealth set up in your environment and that you have eHealth and SPECTRUM administrative privileges.

**To configure the synchronization interval**

1. Log in to the SPECTRUM OneClick server.

2. Select the Administration tab.

   The Administration Pages list appears on the left pane.

3. Select eHealth Configuration from the Administration Pages list.

   The eHealth Configuration page appears on the right pane.

4. Select Active from the drop-down list in the One-Click Server Role field if the server is not already in an active role.

5. Click Save.

6. Scroll down to the Active Server Configuration section. Enter the interval you want in the Discovery Synchronization Interval field.

   **Note:** If you find that your discoveries do not finish before the next discovery interval starts, you must increase this interval.

7. Click Save.

   The server configuration is saved.
Configure Additional Passive SPECTRUM OneClick Servers

In order for SPECTRUM OneClick client servers to have access to eHealth information, the servers must be configured in an active or passive role. If you have multiple SPECTRUM OneClick servers, one should be active and the rest should be passive.

To configure a SPECTRUM client
1. Log in to the SPECTRUM OneClick client.
2. Select the Administration tab.
   The Administration Pages list appears on the left pane.
3. Select eHealth Configuration from the Administration Pages list.
   The eHealth Configuration page appears on the right pane.
4. Select Passive from the drop-down list in the What is This OneClick Server's Role? field if the server is not already in a passive role.
5. Click Save.
   The client configuration is saved.

Create a Discover Policy

You can create an eHealth discovery policy to add to a global collection in SPECTRUM. CA recommends that you assign only one policy per device model.

If more than one policy is assigned to a device model present in multiple GlobalCollections, an alarm will be generated in SPECTRUM. This alarm is meant as a notification of the violation of best practices and can be cleared if desired.

To create a discover policy
1. Log in to the eHealth Server using OneClick for eHealth.
   For information about how to launch OneClick for eHealth, see the *eHealth Administration Guide*.
2. Expand the Tasks and Information folder in the tree.
   Folders appear beneath it.
3. Expand the Resource Discovery folder.
   A list of services appears.
4. Click Policies.
   A list of existing policies appears in the right pane.
5. Right click on the list of policies, and select New Policy from the pop-up menu.

![Policies - admin@New Server - OneClick for eHealth by CA]

**Note:** You can also Edit, Copy or Delete a policy from this menu. The Create Discover Policy pane appears.
6. Select the options you want to create a policy. Select the Create New Elements parameter, and click Edit. The Modify Parameter "Create New Elements" section appears below the Parameters section.

7. Select Yes for the value in the Modify Parameter "Create New Elements" section, and click the OK button in that section.

8. Click OK at the top of the Create Discover Policy pane. The policy is created and appears on the list of policies.

For specific information about creating policies and using parameters, see the eHealth Administration Guide and the eHealth Command and Environment Variables Reference Guide.
Configure SPECTRUM to Trigger Automatic Discovery Requests

You can configure SPECTRUM to automatically request eHealth discoveries. Discovery requests can be automated for the following scenarios:

■ Upon initial assignment of a discovery policy to a global collection or a new device model being added to a synchronized global collection.
■ Upon completion of a device model reconfiguration when the device belongs to a synchronized global collection.

**Note:** The automated discovery settings will only apply to future policy assignments. You will need to manually request discoveries for any Global Collections that were previously assigned discovery policies.

**To configure automated discovery**

1. Start a SPECTRUM OneClick client console.
2. Select the eHealth Manager in the Explorer tab on the left pane.
3. Select the Information tab on the right pane.
4. Do one or both of the following:
   ■ For automated discovery of new global collections and device models, set the Request Discovery for Device Models Added to Global Collections to Enabled.
   ■ For automated discovery for reconfigured models, set the Request Discovery Upon Device Reconfiguration to Enabled.

Add a Policy to a Global Collection

After you create a policy in eHealth, you assign it to a global collection in SPECTRUM as part of the synchronized discovery process.

**To assign a policy to a global collection**

1. Start a SPECTRUM OneClick client console.
2. Select the global collection you want from the Explorer tab on the left pane. The contents of the collection appear on the right pane.
3. Select the Information tab and expand the eHealth Discovery Policy section. Click Assign Discovery Policy.
   
   The Assign Discovery Policy window appears.

4. Select an eHealth machine from the Available eHealth Machines list, and the discovery policy you want from the Available Discovery Policies list. Click Apply.
   
   The policy is applied to the global collection.

   For information about initiating a synchronized discovery, see Run Synchronized Discovery.

### Map eHealth and SPECTRUM Elements

SPECTRUM/eHealth mapping matches eHealth elements such as routers and systems to corresponding models in SPECTRUM. By mapping a one-to-one relationship, SPECTRUM can provide eHealth reporting options for the model in OneClick. It also allows LAN/WAN alarms to appear on the appropriate port model in SPECTRUM (alarms from unmapped LAN/WAN elements are disposed on the device model instead).

**Note:** Mapping activities are performed by the active OneClick server.

The following mapping methods are available:

- Initial mapping lets you map models and elements for the first time. You can also use initial mapping when you add a new Distributed eHealth System to a cluster.

- Incremental mapping lets you update your existing mappings after you add new or remove elements from an eHealth system, or new models in SPECTRUM.
Map eHealth and SPECTRUM Elements

- Map by IP address maps a specific IP address on the specified eHealth system to the models in SPECTRUM.
- Update landscape overrides applies the changes that you have made to the mapping-overrides.xml file. For more information, see Override Mappings.

An initial mapping process (and incremental if many element and model changes have occurred) can take a long time. This phase of the setup can take several hours to complete, depending upon the size of your environment.

Create Initial Mapping

After you create your global collections and discover the models in eHealth, you typically run an initial mapping to map the SPECTRUM models and eHealth elements.

**To perform an initial SPECTRUM eHealth mapping**
1. Log in to the SPECTRUM OneClick home page on the active OneClick server.
2. Select Administration at the top of the page.
   The Administration Pages menu appears.
3. Select eHealth Configuration.
   The eHealth Configuration window appears.
4. Scroll down to the eHealth mapping utilities section, and click Use eHealth Topology.
   OneClick loads the topology information for the eHealth system specified in the eHealth Configuration section.
5. Click Run Initial Mapping.

Maintain Mappings

SPECTRUM automatically maintains eHealth mapping through an incremental mapping process. This process ensures that new eHealth elements and SPECTRUM models are mapped on an ongoing basis.

The frequency of incremental mapping is determined by the eHealth Mapping Update Frequency field on the eHealth Configuration page. By default, incremental mapping is run every 720 minutes (12 hours).

You can also manually run incremental mapping by clicking the Run Incremental Mapping button.
Incremental mappings can only be run after you complete an initial mapping.

**Note:** The incremental mapping process requires that the OneClick server and eHealth server or Distributed eHealth console clocks be synchronized. It is recommended that these servers be synchronized by a time server. Failure to do so can cause model or element changes to be missed.

**Map by IP Address**

You can map models and elements on a one-by-one basis to determine how or even whether the mapping can be resolved.

**To map by an IP address**

1. Log in to the SPECTRUM OneClick home page.
2. Select Administration at the top of the page.
   
   The Administration Pages menu appears.
3. Select eHealth Configuration.
   
   The eHealth Configuration window appears.
4. Scroll down to the eHealth mapping utilities section.
5. Click Use eHealth Topology, if that button is present.
   
   OneClick loads the topology information for the eHealth system specified in the eHealth Configuration section.
6. Enter an IP address in the text box.
7. Click Map By IP.

**Clear Mappings**

After you map SPECTRUM models and eHealth mappings, you can clear the mappings. This lets you remove any existing mappings and start again with either a new initial mapping session or manual mappings.

**To clear the SPECTRUM mappings**

1. Log in to the SPECTRUM OneClick home page.
2. Select Administration at the top of the page.
   
   The Administration Pages menu appears.
3. Select eHealth Configuration.
   
   The eHealth Configuration window appears.
4. Scroll down to the eHealth mapping utilities section.
5. Click Clear Map.

Override Mappings

With SPECTRUM, you can control the mapping process with manual overrides. This can be useful for situations in which a mapping cannot be determined programatically, or if you want to use a different mapping other than the default. For example, if multiple ports on a device cannot be mapped because their values are not unique, but you know the correct mapping to use, you can manually specify those mappings in an XML file.

Also, in large environments it is considered a best practice to use a different eHealth console for each SPECTRUM landscape. The current eHealth integration uses the same eHealth IP address for every mapping. You can use the overrides to point models on each landscape to a different eHealth console using IP addresses or host names.

**To override SPECTRUM eHealth mappings**

1. Log in to the SPECTRUM server as the SPECTRUM administrator.
2. Open a command prompt window and change to the following directory:
   \$SPECROOT\tomcat\webapps\spectrum\WEB-INF\ehlth\config
3. Copy the mapping-overrides.xml file to the \$SPECROOT\custom\ehlth\config directory.
4. Change to the \$SPECROOT\custom\ehlth\config directory.
5. Review the mapping-overrides.xml file for more information about types of overrides and examples of override settings.
6. Edit the mapping-overrides.xml file to add your override settings, and save the file.

The next time that you map models to elements, the mapping process checks for and uses applicable overrides in the mapping-overrides.xml file.

If you create landscape overrides in the mapping-overrides.xml file, you must update the landscape overrides using the eHealth Configuration window of the OneClick Web console. Click the Update Landscape Overrides button to update the OneClick server with the configured overrides.

Any new OneClick clients will use the new settings. Any open OneClick clients should be closed and re-opened to update to the latest settings.
Mapping overrides (element-to-model) are added only after any of the mapping activities are executed. Mappings are not updated with the landscape overrides. However, you can easily force your manual mappings to be executed by choosing a device IP and running Map By IP. This updates all manual mappings.

**Authentication Options**

eHealth offers the following integration options for authentication:

- SPECTRUM to eHealth one-way single authentication support
- eHealth SAML support
- eHealth RADIUS support

All three methods let you use SPECTRUM, however only the SPECTRUM to eHealth one-way single authentication option lets you drill down from SPECTRUM OneClick to the eHealth web user interface without providing additional credentials. The RADIUS and SAML options prompt you for credentials everytime you drill down from SPECTRUM to eHealth.

**Note:** For more information about eHealth support for RADIUS and SAML authentication, see the *eHealth Installation Guide*.

**How To Enable One-way Authentication from SPECTRUM to eHealth**

The limited SPECTRUM to eHealth single authentication option provides one-way drill-down from SPECTRUM to eHealth using CA EEM. This integration lets you use SPECTRUM OneClick to access the eHealth web user interface without being challenged for a user login. This authentication option is not bi-directional.

**Note:** CA EEM offers support for several types of authentication, including LDAP.

User name synchronization across eHealth, CA EEM and SPECTRUM must be maintained.

To enable a SPECTRUM user to take advantage of this feature, the following process must occur:

1. If the user does not already have an eHealth web user account, the administrator must establish one for the user.
2. To help ensure that the user can access all features available through the eHealth web user interface, the administrator must enable those privileges by configuring the SPECTRUM user’s web user account appropriately.
3. The user must have three identical user accounts (with the same user name) for the CA EEM server, eHealth Apache web server, and SPECTRUM user database server.
4. The SPECTRUM administrator for the system must install CA EEM software and follow the installation procedures in the CA EEM documentation. CA EEM must be installed on a separate, standalone server system.
   
   **Note:** If you want to use LDAP authentication with the integration, you must configure the CA EEM server accordingly. For more information, see the CA EEM documentation.

5. The eHealth administrator for the system must run the nhWebSso command line utility to enable the SPECTRUM eHealth system to use one-way drill-down authentication.

### Install CA EEM Software

CA Embedded Entitlements Manager (CA EEM) is a CA proprietary software product that enables a limited one-way single authentication drill-down option from SPECTRUM OneClick to the eHealth web user interface.

CA EEM is the new name for eTrust IAM. eTrust IAM will be rebranded throughout the documentation in a future release, but the current documentation reflects the eTrust IAM name.

**Note:** For information about the required version of CA EEM and download information, see the *eHealth Release Notes*. For information about configuring eHealth and SPECTRUM to use SSO with CA SiteMinder, contact CA Services.
Run the nhWebSso Command Line Utility

The SPECTRUM to eHealth one-way single authentication support and the eHealth SAML support use the nhWebSso utility to enable or disable the authentication option on an eHealth Apache server.

This command has the following format and should be executed on your eHealth server:

```
nhWebSso [-h][ -rev] [ -hostname hostName [ -idleTimeout idleTimeout] [ -disableFallback]] -disable
```

- `-h`
  (Optional) Displays this command usage.

- `-hostname hostName`
  (Required if `-disable` is not specified.) Specifies the fully qualified hostname of a CA EEM backend server.

- `-idleTimeout idleTimeout`
  (Optional) The idle timeout (in minutes) before the user is rechallenged for authentication when accessing eHealth from an external application.

  **Default:** 10 minutes

- `-disableFallback`
  (Optional) Specifies that single authentication fallback is disabled.

- `-disable`
  Disables single authentication if specified.

**Example: Enable Support**

```
nhWebSso -hostname hostName -idleTimeout 10 -disableFallback
```

**Example: Disable Support**

```
nhWebSso -disable
```
Error Handling

Login failure can occur with SPECTRUM eHealth One-way SSO, eHealth RADIUS, and eHealth SAML support due to the following misconfiguration or network issues:

- The authentication server is down or not reachable due to network breakdown. When this happens, the Apache server falls back to the standard eHealth authentication mechanism.

- The web user is not recognized (for example, a user account does not exist in the SAML server user directory) or is not authenticated by the authentication server. In this case, the Apache server falls back to the standard eHealth authentication mechanism.

- The web user exists in the authentication server but has an invalid password. When this happens, the Apache server falls back to the standard eHealth authentication mechanism.

- The web user exists in the CA EEM, RADIUS or SAML user directory and authenticates on the corresponding server, but does not have a valid eHealth account. In this case, the user is denied access and is redirected to an error page.

Fallback is a configurable option that can be turned off by an administrator. A user is denied access when fallback is disabled.

The default eHealth administrator account 'admin' is available to fall back to the standard eHealth authentication, regardless of the previously mentioned errors.
Use Advanced Logging Troubleshooting Tool

In the eHealth Management area of the Administration page, you can access the Advanced Logging option, which provides you with tools for troubleshooting and debugging the eHealth web software. This feature is available to eHealth web administrators only. Web users cannot access it.

**Note:** Use advanced logging solely as a troubleshooting tool and only under the direction of Technical Support. These log files can consume a significant amount of disk space. Do not enable them on a regular basis.

If you enable advanced logging, eHealth stores the files by default in the /ehealth/web/output/users/username directory.

**Creating Technical Support Information**

If you experience any problems or errors while using the eHealth products and features, Support may direct you to create a troubleshooting Zip file. You must be logged in as the eHealth web administrator to create these files.

To create a troubleshooting Zip file

1. Log in as the eHealth web administrator.
2. Click the Administration tab on the Web interface navigation bar.
3. In the left frame, click eHealth Management and then click Advanced Logging.
4. On the Advanced Logging page, click Create Technical Support Information.
5. Under Areas to Include, select one or more areas as instructed by your Technical Support Engineer.
6. If your eHealth system is a member of a Distributed eHealth cluster, in the Cluster Members field, do one of the following:
   - Select Host to specify the cluster member for which you want to collect troubleshooting information. The default is the local cluster member.
   - Select Cluster to collect the same information from all cluster members except the local member.
   - Select All to collect the same information from all cluster members.
7. In the File Directory field, specify the directory in which to create the Zip file. The default is /ehealth/tmp.
8. In the Call Ticket Number field, specify the number of the call ticket for your problem report. If specified, the number is used in the Zip file name for identification purposes. If you do not have a call ticket associated with this problem, leave the field blank.
9. Click Create File.
The Troubleshooting Tool

When there is a problem in a specific area, Support typically requests certain files that can help to diagnose the problem. To assist with the file collection, this tool collects copies of files from various subdirectories of the eHealth installation. It creates a Zip file named diagnostics_callTicketNumber_date_time.zip in the specified File Directory location. Email or FTP the Zip file to Support to assist with the process of troubleshooting the problem that you have reported.

Note: Depending upon the options that you select, the troubleshooting Zip file could be very large. Typical Zip files can range in size from 50 KB to 150 MB. If you have had Advanced Logging enabled for a long time, the Zip file may be several Gigabytes in size.

After Support confirms that they have received the file, delete the Zip file from your File Directory location to free up disk space. Certain types of problems may require you to enable advanced logging features prior to creating the troubleshooting Zip file. The web server advanced logging features are on the Advanced Logging page of the eHealth Web interface. To enable advanced logging for eHealth system processes, you must use OneClickEH. Your Support engineer will assist you when advanced logging is necessary.

Errors and Troubleshooting

eHealth gathers as many of the troubleshooting files as possible into the Zip file. For each troubleshooting option, the tool searches for each file and then checks for available space in the File Directory location. If it cannot find a specific file, or if File Directory does not have enough free space to hold a file, the tool omits that file and proceeds to the next one. The Zip file contains a log file that lists the files that were included, as well as those files that were omitted.

Setup Name Synchronization

Name synchronization lets eHealth elements take SPECTRUM names whenever possible. The name synchronization is done when a Synchronized Discovery request is executed or when an element is mapped to a model.
Name synchronization uses the following process:

1. A Router or System element is mapped to a similar model, or a new element or model is found and mapped

2. If enabled, SPECTRUM requests that the device element be named based on the device model name. The element is named according to the eHealth naming rules. eHealth applies whatever logic and restrictions it needs to in order to make the synchronized name fit within the eHealth scheme. All elements related to the device element are renamed using the device model name.

**Note:** Name Synchronization requires a Router, Switch, or System element to be present. Names for stand-alone LANWAN, CPU, Disk, etc. elements will not be synchronized.

This feature can be used in the following circumstances:

**Name Synchronization with Stand-Alone eHealth**

SPECTRUM makes the naming request to the stand-alone eHealth server. The synchronized name should be immediately updated and available for all reporting.

**Name Synchronization in Distributed eHealth**

Elements and their names must be changed on the Distributed eHealth system to which they belong. SPECTRUM makes the naming request to the Distributed eHealth console and ensures that the request is passed to the appropriate distributed system. The synchronized name will not be seen at the Distributed eHealth console level until the element configuration data is updated at the designated interval. Until this update occurs, the element names seen on alarm reports will not match those for At-A-Glance and Trend reports.

**Note:** You must use the same administrative name and password on each machine in the cluster.
Name Updates

During an incremental mapping update, the element names will be updated for all elements related to a device element in the following scenarios:

- The device model name changes
- A new port model is added to the device model in SPECTRUM
- A new LANWAN element is added in eHealth

The eHealth element name is stored in a SPECTRUM attribute (EH_Element_Name) for all mapped device and port models. You can read or write over this attribute value, but it will be overwritten by automated mappings. If this is used in combination with the element naming feature and the element naming causes the name to change, the original name will be stored in SPECTRUM until the next incremental mapping which will reflect the new name.

When using element or model name synchronization, two mappings are required for the EH_Element_Name Spectrum attribute to update if SPECTRUM model names are changed. The first mapping will set the element name and the second mapping will update the SPECTRUM attribute.

Distributed Web Services Calls

SPECTRUM can use eHealth web services on the eHealth front end system as the single point of entry to eHealth in a cluster. This minimizes the system and network configuration for SPECTRUM with eHealth. SPECTRUM calls the eHealth web services, such as discovery and element naming and performs configuration actions on the appropriate back ends. The web service forwards these requests from the front end system to the back end system, and provides status information and results.

SPECTRUM permits web service access to the admin user only. For inter-cluster front end to back end communication use, the admin user gets the password from the NH_PARAMETER table for parameter "reportCenterAdminPassword" using the same java method used by Report Center (\top\java\dev\src\com\concord\lib\jdbcLib\Parameter.java).

Note: The admin user must have same password on all cluster systems.

All Back End web servers must be configured to use the same web protocol (HTTP/S) port. This is so the front end knows how to communicate to the back end.
Configure Distributed Web Services Calls

On the front end (Distributed Console) used by SPECTRUM, eHealth can be configured to contain a new NH_PARAMETER table entry, webServicesProtocolAndPort. This sets the protocol and port that all back ends are configured with, and is used by the front end web services to communicate with the back ends.

Run the nhParameter command to set this parameter when the back ends are configured to use other than the default of http:80.

This command uses the following syntax:

```bash
> nhParameter -set webServicesProtocolAndPort http|https[:port]
```

**Values:** http:80, https:443, http:81

**Defaults:** http:80, https:443

**Examples:**

- Set to https, and default https port, 443
  ```bash
  nhParameter -set webServicesProtocolAndPort https
  ```

- Set to https and non-default port 444
  ```bash
  nhParameter -set webServicesProtocolAndPort https:444
  ```

- Set to http and non-default port 81
  ```bash
  nhParameter -set webServicesProtocolAndPort http:81
  ```

- Revert to default, http:80
  ```bash
  nhParameter -delete webServicesProtocolAndPort
  ```

**Querying from the Database**

```sql
SQL> select setting_value from nh_parameter

setting_name
    'webServicesProtocolAndPort';

setting_value
    https:444
```

**Special Web Configurations**

For SSL on the back ends, follow the SSL configuration instructions to provide the certificate to the Web Service java application on the front end. For more information, see the SSL documentation.
For SSL on the front end, SPECTRUM needs to be configured with the certificate.

**How to Set Up Access to Traffic Accountant Reports**

You can access eHealth Traffic Accountant reports from SPECTRUM, however it is not a direct integration. The eHealth server is an intermediary between Traffic Accountant and SPECTRUM.

To make Traffic Accountant report accessible from SPECTRUM, follow this process:

2. Discover NetFlow-enabled LAN/WAN elements on an eHealth statistics server (either backend or standalone).
   
   **Note:** For procedures for steps 1 and 2, see the *eHealth Traffic Accountant Guide*.

3. Integrate an eHealth statistics server with a SPECTRUM server (standalone or frontend if in a cluster; SPECTRUM cannot integrate with a backend server).
4. [Configure the eHealth Alarm Notifier](#) (see page 16).
5. [Configure SPECTRUM to view eHealth alarms](#) (see page 20).
6. [Map eHealth and SPECTRUM elements](#) (see page 31).

**Tomcat Logs Files**

Tomcat server logs contain debugging information for SPECTRUM, eHealth, and synchronized discovery. For example, this can be helpful if discoveries are failing and you need to troubleshoot the situation.
The following logging information is available:

**eHealth Mapping Detailed Logging**

Provides detailed logs about the element mapping, including the raw information that ALL of the eHealth web services send to SPECTRUM (including the discovery web service). These logs can be verbose and should only be enabled if Information logging does not provide enough data to accurately assess the issue.

**eHealth Mapping Information**

Provides informative set of logs, when this setting is turned on, for tracking the work that the element mapping does.

**eHealth Synchronized Discovery Logging**

Provides more information about the activities surrounding synchronized discovery. If you are experiencing problems or alarms with synchronized discovery, you can turn this setting on to see what is going wrong. Only this log setting supports Min/Max settings at the bottom of the page to control Info/Debug level logging.

Accessing log information depends on which server is experiencing problems. For example, if you are logged into the client and see problems accessing the web services to assign the discovery policy to the GlobalCollection, then you log in to the client OneClick server and turn on the logging for synchronized discovery. If the problem is occurring when attempting to run the discoveries on eHealth, you will likely see alarms on the Discovery Policy or Manager Model. If this occurs, log in to the active server and turn on the logging there.

The logging pages are located on the Administration link of the OneClick web page. Click the Debugging link in the horizontal grey bar, and click the Web Server Debug Page (Runtime) link on the left grey bar to find the settings. The eHealth logging is at the bottom of the page. You can also view the logs by clicking the Web Server Log link on the left grey bar.
Chapter 4: SPECTRUM Usage

This section contains the following topics:

Tasks (see page 47)  
Run Reports from the SPECTRUM OneClick Console (see page 47)  
View eHealth Reports for Alarms (see page 49)  
View Alarm Detail Reports (see page 50)  
Clear Alarms (see page 50)  
Run Synchronized Discovery (see page 51)  
Monitor eHealth Discoveries (see page 51)

Tasks

With eHealth SPECTRUM Integration, you can perform the following tasks directly from the SPECTRUM OneClick console:

- Generate eHealth At-a-Glance and Trend reports for elements in the OneClick Topology.
- Generate At-a-Glance and Trend reports for alarms.
- View Alarm Detail reports for eHealth Live Health Application alarms.
- Clear eHealth Live Health Application alarms.

Run Reports from the SPECTRUM OneClick Console

You can generate eHealth At-a-Glance and Trend reports from the SPECTRUM OneClick console for any models that have been mapped to eHealth elements.

If the SPECTRUM model is not mapped to an eHealth element, drill-down reports are not available from the Topology view.

In previous releases, the integration feature let you generate eHealth At-a-Glance and Trend reports for any router, switch, LAN/WAN interface, or system represented in the OneClick Topology. However, if there was no corresponding eHealth element, the drill-down displayed an error. You can restore this legacy report drill-down capability for unmapped elements using the Legacy Report Launching field on the OneClick eHealth Configuration page.
View Trend Reports

eHealth Trend reports display the performance of an element or a group of elements based on specific variables. You use these reports to identify the cause of unsatisfactory health ratings on specified elements. These reports display information for the previous 24 hours.

To generate a Trend report
1. Select the icon in your Topology in the SPECTRUM OneClick console that represents the interface, router, switch, or system for which you want to generate a report.
2. Right-click the icon, then select eHealth Trend Type Report, where Type is a resource such as System, Router, LAN/WAN, and so on.
3. Select the menu option is eHealth Trend Type Report (Legacy) if you are using the legacy reporting option.
4. Select the Trend variable that you want to display.
   A new browser window opens.
5. Enter your eHealth Web user name and password.
   A status window appears displaying progress as the report generates, then the report appears.

View At-a-Glance Reports

eHealth At-a-Glance reports provide detailed information for all critical performance parameters through a series of charts. These charts show the trends for important variables such as the following:

- CPU utilization
- Buffer management
- Total throughput
- Disk faults
- Disk input and output

To generate an At-a-Glance report
1. Select the icon in your Topology in the SPECTRUM OneClick console that represents the interface, router, switch, or system for which you want to generate a report.
2. Right-click the icon, and select eHealth At-a-Glance Type Report, where Type is a resource such as System, Router, and so on.
   A browser window opens.
3. Select the menu option eHealth At-a-Glance Type Report (Legacy) if you are using the legacy reporting option.

4. Enter your eHealth Web user name and password.
   A status window appears displaying progress as the report generates, then the report appears.

**View Traffic Accountant Reports**

eHealth Traffic Accountant reports display traffic data that help you analyze, plan, and troubleshoot operations in your network. These reports display information for the previous 24 hours.

**Note:** You must [set up access to Traffic Accountant reports](#) (see page 44) before you can view them.

You can access Traffic Accountant reports from the SPECTRUM Topology or SPECTRUM OneClick Alarms view. To generate a report, right-click on an alarm or an icon in your topology and select Traffic Report from the menu.

**View eHealth Reports for Alarms**

When you see an alarm in the OneClick alarm list, you can generate eHealth At-a-Glance and Trend reports to view historical data about the element generating the alarm.

**To generate reports from the OneClick alarm list**

1. Right-click the appropriate row in the alarm list, then select one of the following:
   - eHealth At-a-Glance Type Report
   - eHealth Trend Type Report
   A new browser window opens.

2. Enter your eHealth Web user name and password.
   A status window appears displaying progress as the report generates, then the report appears.
View Alarm Detail Reports

When you see a Live Exceptions alarm in the OneClick alarm list, you can view an Alarm Detail report for the alarm, in addition to the At-a-Glance and Trend reports. The alarm detail report provides in-depth information about the alarm, including:

**Time**
- Specifies the time the problem started, and the duration the alarm has been active.

**Elements**
- Specifies the name of the element that has the alarm, its technology type, IP address, and the total number of traps it has generated.

**Alarm Type**
- Indicates the condition that generated the alarm, and the severity level of the alarm.

You can use this information to troubleshoot the cause of a problem.

**To view Alarm Detail reports**

1. Right-click the row in the alarm list, and select Alarm Detail Report (eHealth).
   - A new browser window opens.
2. Enter your eHealth Web user name and password.
   - A status window appears on the screen and displays the progress as the report generates. After several seconds, the Alarm Detail report appears in the browser.

Clear Alarms

You can clear an eHealth Live Health Application alarm from the OneClick console when the problem has been fixed, or you have determined it is not a real problem.

To clear an alarm from the OneClick console, right-click the appropriate row in the alarm list, and select Clear Alarm. The alarm is cleared in both SPECTRUM and the eHealth Live Exceptions Browser.
Run Synchronized Discovery

You can manually request a global collection be discovered or have SPECTRUM automatically request eHealth discoveries. A manual request is processed according to the queue rules and likely will not be executed immediately.

**To run a discovery manually**

1. Start a SPECTRUM OneClick client console.
2. Select a global collection from the Explorer tab on the left pane.
   The contents of the collection appear on the right pane.
3. Select the Information tab. Expand the eHealth Discovery Policy section on the Information tab, and click Request Discovery.

   ![eHealth Discovery Policy](image)

   The discovery request is queued.

Monitor eHealth Discoveries

When discoveries are requested, executed events are generated on the corresponding discovery policy models. When the discovery is executed, a link to the discovery log is included in the event.

**To view discovery events**

1. Start SPECTRUM OneClick client console.
2. Expand the eHealth Manager tree in the Explorer Tab.
3. Expand the Discovery Policies folder.
4. Select the policy of interest.
5. Select the Events tab to view the discovery events.

   **Note:** By selecting the Discovery Policies folder and the Events tab, you can see the discovery events for all discovery policies.
Chapter 5: eHealth Usage

This section contains the following topics:

Run Reports from the eHealth Console (see page 53)

Run Reports from the eHealth Console

From the eHealth console, you can run additional types of reports on all of your elements, including the elements that you monitor with SPECTRUM.

Depending on which eHealth applications you use, you can run the following reports from eHealth:

- **At-a-Glance**
  Shows key performance indicators for a specific element to aid in troubleshooting.

- **Top N**
  Shows which elements are the highest or lowest performers for key indicators.

- **Trend**
  Shows historical performance for multiple variables or multiple elements.

- **Health**
  Provides current and historical data to identify problems proactively, and plan resources.

- **MyHealth**
  Provides custom, multi-chart views of specific, user specified data.

- **What-If**
  Shows the effect of changes in capacity and demand to help in capacity planning.

- **Service Level**
  Shows and analyzes service level information for a complete business unit.

You can use the eHealth console or Web interface to generate reports for a specific time period. You can also schedule eHealth reports to run automatically at specified times.

For more information about eHealth reports and how to run them, see the eHealth Web Help.
Launch the OneClick Console

You can launch the SPECTRUM OneClick console directly from eHealth to access SPECTRUM's fault management, root cause analysis, and other network management features.

To launch the OneClick Console from eHealth
1. Log in to eHealth Web console.
2. Select the Live Health tab.
3. Click Launch OneClick.
   The SPECTRUM OneClick console opens.
4. Log in to the OneClick console using your SPECTRUM user name and password.

Clear SPECTRUM Alarms

You can clear Live Exceptions alarms present in SPECTRUM from the Live Exceptions Browser in eHealth.

To clear an alarm in a Live Exceptions Browser
1. Select a row in the Event Table that represents an alarm that you want to clear.
2. Right-click the row, and select Clear Alarm.
   A message appears to confirm clearing the alarm.
3. Click Yes.
   The alarm is cleared in both the Live Exceptions Browser and in SPECTRUM.
Appendix A: Legacy Utilities

The utilities listed in this appendix are used only if you have previously scheduled a scripted discovery to be executed using discovery information collected from SPECTRUM.

This section contains the following topics:

Run the Setup Program (see page 55)
How to Configure the Integration From the Command Line (see page 57)
How to Configure the Integration With a SPECTRUM OneClick Server Running SSL (see page 58)

Run the Setup Program

The setup program prompts you for the information that you recorded on the setup checklist.

To run the setup program

1. Log in to the eHealth system as the eHealth administrator.
2. Open a terminal window and change to the eHealth directory by entering the following command, where eHealth is the full pathname:
   
   ```
   cd ehealth
   ```
3. Run the setup program by entering the following command:
   
   On Windows:
   
   ```
   nhSpectrumSetup
   ```
   
   On UNIX:
   
   ```
   .bin/nhSpectrumSetup
   ```
   
   The SPECTRUM Import Setup dialog appears.
4. Enter the following information:
   
   - Hostname or IP address of the SPECTRUM OneClick server
   - Port number for OneClick server Web requests
   - Path where OneClick is installed on the server
   - Username used to log in to the OneClick server
   - Password for the specified user name
5. Click OK.
   eHealth verifies your settings and displays a message notifying you if they are valid. The validation process may take a few seconds.

6. Restart the eHealth Console.
   The setup is complete.
How to Configure the Integration From the Command Line

The nhSpectrumSetup command configures the eHealth SPECTRUM Integration, which lets you import configuration information about the network devices that you manage with SPECTRUM.

This command does not have any arguments. To use it, enter nhSpectrumSetup at the command line, and specify the requested parameters.

**Note:** The nhSpectrumSetup command may take a few seconds to run if you enter the arguments on the command line, depending on the computer you are using.

When the discovery request is sent to the eHealth server from the OneClick server, the community string from the configured attribute is used. If you elected to use the CommunityNameForSNMPSets attribute, but some of the devices in the discovery set do not have a value in that attribute, the discovery request reverts to the standard community_name attribute.

In releases prior to eHealth r6.1 and SPECTRUM r9.0, if you have configured nhSpectrumSetup and attempt to run a discovery using Spectrum import, the list of devices to discover includes the community string from the configured Spectrum attribute.

The following command line arguments are for internal use only. These arguments allow you to set the SPECTRUM import parameters directly, without bringing up the GUI. Most users will run the command without arguments, and use the GUI to specify these parameters. However, if you want to setup multiple eHealth systems, you can create a script that sets these values on each box.

This command has the following format:

```
nhSpectrumSetup [-h] [-list] [-host name] [-port number] [-path path] [-user name] [-password]
```

- `-h` Displays help for this command.
- `-list` Lists the current setup parameters.
- `-host name` Specifies the hostname or IP address of the SPECTRUM OneClick server.
- `-port number` Specifies the port number for SPECTRUM OneClick server Web requests.
  **Default:** 80
- `-path path` Specifies the path in which SPECTRUM OneClick is installed on the server.
How to Configure the Integration With a SPECTRUM OneClick Server Running SSL

Default: spectrum.

Note: Use the default value unless you specified another path when installing SPECTRUM OneClick.

- **user name**
  Specifies the username used to log in to the SPECTRUM OneClick server.

- **password**
  Specifies the password for the selected user name.
  
  Note: The password value is not supplied as an argument. After you enter the command, you must type the password. The password is then read by the program.

- **https true/false**
  Specifies whether the SPECTRUM OneClick server is accessed using SSL.

How to Configure the Integration With a SPECTRUM OneClick Server Running SSL

This section describes how to configure the legacy discovery utilities if you have also chosen to secure the SPECTRUM OneClick server using SSL. To configure the utility, follow this process:

1. Obtain copies of all certificates required to contact the SPECTRUM OneClick server including the root and intermediate certificates.
2. Place these certificates in the $NH_HOME/Jre directory.
3. Open a command shell on the eHealth server.
4. Execute the following command:
   ```bash```
5. Execute the following command:
   ```bash```
6. Install each certificate starting with the Root certificate using the following commands:
   ```bash```
7. Enter the following password:

   changeit

   **changeit**

   Specifies the default password for the keystore.

   **Note:** Each certificate needs its own alias, if any of the certificates are already installed, you can answer no to the query regarding importing the certificate.

8. Configure the utilities to use https and port 443 by executing the following command:

   `nhSpectrumSetup --https true --port 443`
Index

A
alarms
  alarm notifier • 16
  clear • 50, 54
  configuration • 19
  reports • 49, 50
  view • 21

C
command line, configuration from • 57
configuration
  eHealth alarm notifier • 16
  Health reports • 17
  legacy utilities • 55
  options • 10
  SPECTRUM • 21, 24
containers • 23

D
discovery
  monitoring • 51
  process • 26
distributed web services calls • 43, 44

E
eHealth alarm notifier • 16

H
Health reports • 17

L
legacy configuration utilities • 55
licenses, adding • 15
log files • 45

M
mapping
  clearing • 34
  creating • 33
  maintaining • 33
  override • 35
  overview • 32
models
  considerations • 20

N
name synchronization • 27, 41

O
OneClick consoles
  launching • 54
  reports • 53
OneClick, server roles • 11
  overview • 7

P
policies • 28, 31

R
reports
  At-a-Glance • 48
  for alarms • 49, 50
  Health • 17
  running • 47, 53
  Trend • 48
  viewing • 48

S
setup
  configure Health reports • 17
  eHealth alarm notifier • 16
  global collections • 24
  licenses • 15
  software configuration • 10
  SPECTRUM • 21
  system requirements • 9
  time • 9
SPECTRUM OneClick configuration • 58
synchronized discovery
  add policy to global collection • 31
  configuration • 27, 28
  creating policy • 28
  overview • 25
  process • 26
  running • 51
  system requirements • 9
SystemEDGE agents
  alarm configuration • 19

migrating to Host_systemEDGE • 24
containers • 23
migrating to Host_systemEDGE model • 24