CA eHealth® and CA Spectrum®

Integration and User Guide

CA eHealth Release 6.3.1 / CA Spectrum Release 9.4

CA Technologies Product References

This document may reference the following CA Technologies products:

- CA ARCserve® Replication and High Availability (CA ARCserve RHA)
- CA eHealth® AdvantEDGE View
- CA eHealth® Application Response
- CA eHealth® Business Service Console (CA eHealth BSC)
- CA eHealth® Converged Network Data Collector
- CA eHealth® Fault Manager
- CA eHealth® Live Health® Application
- CA eHealth®
- CA eHealth® Response
- CA eHealth® Service Availability
- CA eHealth® TrapEXPLODER
- CA eHealth® Voice Quality Monitor (VQM)
- CA eHealth® AIM for Apache
- CA eHealth® AIM for Microsoft Exchange
- CA eHealth® AIM for Microsoft IIS
- CA eHealth® AIM for Microsoft SQL Server
- CA eHealth® AIM for Oracle
- CA eHealth® Integration for Alcatel-Lucent 5620 NM (CA eHealth - Alcatel)
- CA eHealth® Integration for Alcatel-Lucent 5620 SAM (CA eHealth-Alcatel SAM)
- CA eHealth® Integration for Alcatel-Lucent EMS-CBGX (CA eHealth - Lucent)
- CA eHealth® Integration for BrixExfo (CA eHealth - BrixExfo)
- CA eHealth® Integration for Cisco IP Solution Center (CA eHealth - Cisco ISC)
- CA eHealth® Integration for Cisco WAN Manager (CA eHealth - Cisco WAN Manager)
- CA eHealth® Integration for HP OpenView (CA eHealth - OpenView)
- CA eHealth® Integration for HP Network Node Manager (CA eHealth - NNM)
- CA eHealth® Integration for IBM Netcool (CA eHealth - Netcool)
- CA eHealth® Integration for Nortel Preside (CA eHealth - Nortel Preside)
- CA eHealth® Integration for Nortel Shasta SCS GGSN (CA eHealth - Nortel GGSN)
- CA eHealth® Integration for Nortel Shasta SCS PDSN

- CA eHealth® Integration for Psytechnics (CA eHealth - Psytechnics)
- CA eHealth® Integration for Starent PDSN (CA eHealth - Starent PDSN)
- CA eHealth® Integration for Starent GGSN (CA eHealth - Starent GGSN)
- CA Embedded Entitlements Manager (CA EEM)
- CA eTrust® Identity and Access Management (eTrust IAM)
- CA Insight AIM for CA eHealth®
- CA Insight™ Database Performance Monitor for Distributed Databases (CA Insight DPM for Distributed Databases)
- CA Performance Center
- CA SiteMinder®
- CA Spectrum® Infrastructure Manager (CA Spectrum)
- CA Systems Performance for Infrastructure Managers (CA SystemEDGE)
- CA Network and Systems Management (CA NSM)
- Distributed eHealth

Contact CA Technologies

Contact CA Support

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

- 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

Providing Feedback About Product Documentation

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

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: CA eHealth and CA Spectrum Integration

This section contains the following topics:

Introduction

This guide describes how to set up the integration between the current releases of CA eHealth and CA Spectrum. This guide also describes how to use the features to perform tasks, run reports and synchronized discovery, and clear alarms.

Integration Overview

The CA eHealth and CA Spectrum integration helps you maintain critical service levels across complex network environments. The integration combines the automated availability and performance management of CA eHealth with the CA Spectrum network service and analysis platform.

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

The historical data and automated reporting capabilities of CA eHealth:

- Automate the tasks of calculating long-term trends, providing a baseline for network resources.
- Provide performance reports for critical network components such as backbones, server clusters, and internet links.

CA eHealth also offers proactive troubleshooting and capacity planning features.

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

- Use CA eHealth to discover devices automatically that CA Spectrum manages, eliminating the need to reenter and continually update configuration data manually.
- Access CA eHealth reports, such as At-a-Glance and Trend, directly from the CA Spectrum OneClick topology. Quick access gives you an overview of device status and in-depth historical information.
- To reduce the mean-time-to-repair for network issues, you can:
  - Manage the Live Exceptions alarms from the CA Spectrum OneClick console
  - View Alarm Detail reports
  - Clear alarms
- Access CA eHealth reports from the CA Spectrum alarms, giving you a historical context for more effective troubleshooting.
- Use CA eHealth for capacity planning, proactive troubleshooting, performance optimization, and service level management of your network components that CA Spectrum manages.

The integration of the current version of CA Spectrum with CA eHealth Release 6.0 or higher provides a cohesive view of the integration by:

- Supporting the CA eHealth High Availability (HA) and Disaster Recovery (DR) failover scenarios. In CA eHealth High Availability and Disaster Recovery failover scenarios, a secondary server takes over for a primary server when required.
- Providing a location within CA Spectrum OneClick for configuring integration options for individual CA eHealth servers.
- Creating a set of models that represents a CA eHealth server cluster and its constituent parts. The server models are accessible under the existing CA eHealth Manager tree in CA Spectrum OneClick. A standalone CA eHealth system is modeled as a cluster consisting of one CA eHealth server.

Chapter 2: Setup Information and Checklist

This section contains the following topics:

Setup Time

The setup process typically requires the following time estimates:

Task	Time Estimate
Set up the integration	1.5 to 6 hours
Verify requirements and complete the setup checklist	1 hour
Add a license	10 minutes
Run the setup program and configure alarms	30 minutes
Configure CA Spectrum global collections, run CA eHealth discovery, and map elements to models. The mapping time depends on the size of the environment, and could be longer in large environments.	15 minutes – 5 hours

System Requirements

Before you run the CA eHealth CA Spectrum integration setup program, verify that your CA eHealth and CA Spectrum systems meet the current system requirements.

The integration supports multiple releases of CA eHealth and CA Spectrum. The present version of CA Spectrum supports version 6.3.x of CA eHealth for English locales only. Although CA eHealth r6.1.1 was translated into Japanese, our testing indicated that CA Spectrum r9.3 does not support that version of CA eHealth. Later versions of CA eHealth are not localized.

Important! CA eHealth must be installed on a dedicated system. Do not install it on the same system as CA Spectrum.

Devices must *not* be in a secure domain, otherwise the integration functions improperly. Model devices in CA Spectrum to enable element-model mapping and alarm processing.

Note: For information about CA eHealth system requirements and installation, see the *CA eHealth Release Notes* and *CA eHealth Installation Guide*. For information about CA Spectrum system requirements and installation, see the *CA Spectrum Installation Guide.*

Mapping Upgrade Considerations

When upgrading CA Spectrum, any existing mappings are updated to a new format. The new format lets you run the CA eHealth report launches in CA Spectrum OneClick when multiple elements are mapped to a model. The integration OneClick server initiates the update, utilizing information in its MySQL database. To update existing mappings to the new format, it is required that the original integration OneClick server performs the upgrade. Using a new OneClick Server as the integration server results in the removal of all mappings.

Mappings for any element information that cannot be verified on the integration OneClick server are removed during the update. If a new OneClick server is configured as the integration server, all mappings are removed.

Important! The MySQL database that the CA eHealth and CA Spectrum integration uses did not exist before CA Spectrum Release 9.0. Therefore, if you are upgrading from CA Spectrum Release 8.1 or earlier, all element mappings are removed during this process. In this case, execute an initial mapping after upgrading.

During the mapping update, there can be a delay between the SpectroSERVER startup and the OneClick server startup. The update itself can also take some time. During this delay, the device models do not respond to mapping requests. All CA eHealth Live Health Application alarms are sent to the device models (based on the IP address) until the mappings have been updated.

Software Configuration

The CA eHealth and CA Spectrum integration uses four basic configurations, which are described in the following list. Multiple standalone CA eHealth systems without Distributed eHealth are unsupported.

Standalone CA eHealth System, Single (Separate) CA Spectrum Server

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

Standalone CA eHealth System, Distributed SpectroSERVER

Lets you configure CA eHealth so that you can connect with multiple SpectroSERVERs, all of which can view CA eHealth reports. However, the CA eHealth Live Health Application alarms must be sent to only one SpectroSERVER. When configuring Live Exceptions or Health reports to forward traps, specify a single SpectroSERVER to handle all traps. The CA Spectrum Main Location Server is the recommended destination.

Distributed eHealth, Distributed SpectroSERVER

Lets you use Distributed eHealth to connect multiple CA eHealth systems with multiple SpectroSERVERs. When using Distributed eHealth:

- Configure each Distributed eHealth System with discovery policies and assign each policy to a separate global collection on the CA Spectrum OneClick server.
- To forward Live Exceptions traps to a single CA Spectrum server, as described previously, configure each Distributed eHealth System.
- To forward traps to a single CA Spectrum server, configure Health reports on each CA eHealth system and the Distributed eHealth Console.
- Configure CA Spectrum so that you can:
  - Access the CA eHealth At-a-Glance and Trend reports on a single Distributed eHealth Console (front end).
  - Access the CA eHealth Performance Dashboard and Live Reports on Distributed eHealth Systems (back ends).

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

Distributed eHealth, Single CA Spectrum SpectroSERVER

Lets you configure one CA Spectrum SpectroSERVER so that you can connect with one Distributed eHealth System. When using this configuration, you must:

- Configure each Distributed eHealth System with discovery policies and assign each policy to a separate global collection on the CA Spectrum OneClick web server.
- Configure each Distributed eHealth System so that you can forward Live Exceptions traps to the CA Spectrum server.
- Configure Health reports on each CA eHealth system and the Distributed eHealth Console so that you can forward traps to the CA Spectrum server.
- Configure CA Spectrum so that you can:
  - Access the CA eHealth At-a-Glance and Trend reports on a single Distributed eHealth Console (front end).
  - Access the CA eHealth Performance Dashboard and Live Reports on Distributed eHealth Systems (back ends).

OneClick Server Roles

The CA Spectrum OneClick web server uses web services that the CA eHealth server provides to perform the integration features that are configured. All OneClick web servers need some features, such as requesting discovery policy information. A single OneClick web server can handle other features such as element mapping.

Note: The server roles do not affect CA eHealth report launching from CA Spectrum. If the CA eHealth server information is configured on a OneClick web server, clients of that server can launch CA eHealth reports regardless of server roles.

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

Disabled

This role is the default role when configuring the integration with the CA eHealth server. There is no communication with the CA eHealth server. The OneClick clients of this OneClick web server cannot configure synchronized discovery.

Passive

In this role, the only communication with the CA eHealth server is to obtain server and discovery configuration data. If the clients of this OneClick web server are required to configure synchronized discovery, the OneClick web server must be in a Passive or Active role.

Active

A OneClick web server in an Active role (also known as the integration server) communicates with the CA eHealth server to obtain server and discovery configuration data. The active role is also used to run the element-to-model mappings and request discoveries. Clients of an Active OneClick web server can configure synchronized discovery. An Active OneClick web server also models and monitors the status of the Distributed eHealth cluster when the CA eHealth web services are enabled.

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

If the regions are being configured, there must be one active server per region.

Setup Checklist

For each CA Spectrum OneClick server that you want to configure, copy and complete the Setup Checklists in the following table. The checklists help you to supply the information for the setup program.

Computer	Information	Value
CA Spectrum OneClick Server:	Host name or IP Address of the CA Spectrum OneClick server.	
	Port number on which OneClick listens for Web requests. **Default:** 80	
	Path where OneClick is installed on the server. **Default:** spectrum **Note:** Use the default value unless you specified another path when installing OneClick.	
	User name and Password for accessing this host.	User name: Password:
	Location of the SSL certificate file for the standalone CA eHealth system or Distributed eHealth Console.	
CA Spectrum OneClick Server roles:	The servers that will act in an active or passive role in your CA Spectrum environment. There should be one and only one server in an Active role in your CA Spectrum environment. If regions are being configured there should be one active server per region.	Active: Passive:
SpectroSERVER:	Host name of the SpectroSERVER that is configured to receive traps from CA eHealth.	
	IP address of the SpectroSERVER that is configured to receive traps from CA eHealth.	
	Port number on which the SpectroSERVER receives traps. **Default:** 162	
CA eHealth Server:	Host name or IP Address of the CA eHealth server. **Note:** If you use Distributed eHealth, this server must be a Distributed eHealth Console.	

Computer	Information	Value
	Port number on which CA eHealth listens for Web requests. **Default:** 80 **Note:** If you use Distributed eHealth, this server must be a Distributed eHealth Console.	
	Password for the CA eHealth user name "admin". **Note:** If you use Distributed eHealth, the user must be valid on all CA eHealth systems.	Password:
	The location of the SSL certificate file for the OneClick server and any Distributed eHealth Systems when configuring a Distributed eHealth cluster.	
	The maximum number of traps CA eHealth Live Exceptions sends per second. This value is defined by the NH_TRAPS_PER_SECOND environment variable. **Default:** 100	

Computer	Information	Value
	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:** Base the value on the number of alarms that are expected in a single CA eHealth polling cycle. Increasing the NH_TRAP_GOVERNOR_SIZE increases the memory used in the process of notifying CA Spectrum of new/cleared alarms. However, if this size is too low some alarm notifications may not make it to CA Spectrum. **Default:** 1000	

For more information about CA eHealth environment variables, see the *CA eHealth Command and Environment Variables Reference Guide*.

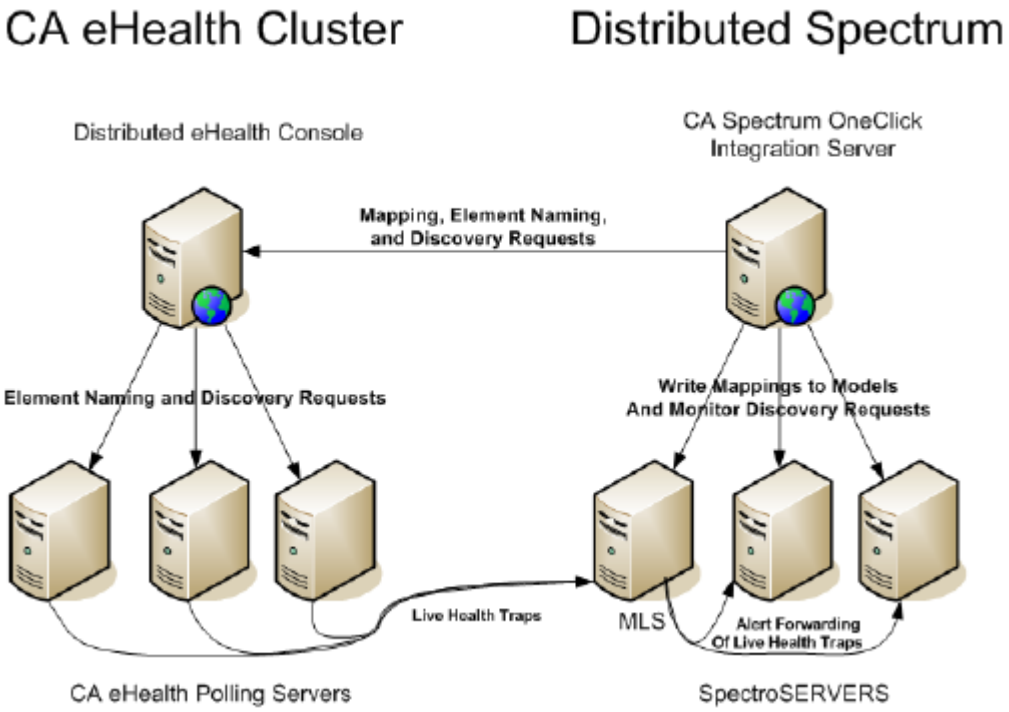
Chapter 3: Installing and Configuring the Integration

This section contains the following topics:

Communication Overview

The Spectrum OneClick integration server utilizes web services on the Distributed eHealth Console to perform mapping, element naming, and discovery operations within CA eHealth. Element naming and discoveries must be executed on the polling servers. Therefore, the Distributed eHealth Console forwards those requests to the appropriate polling server to satisfy the request. The response is returned to the Distributed eHealth Console, which then forwards the response to the OneClick server. The OneClick server rarely communicates directly with a Distributed eHealth System.

The following diagram illustrates the inter-server communication paths that are utilized in the CA eHealth and CA Spectrum integration in a sample distributed environment:



Viewing the CA eHealth Live Health Application alarms in CA Spectrum requires SNMP traps to be sent to CA Spectrum. The diagram shows the recommended trap forwarding configuration, with all Distributed eHealth Systems sending CA eHealth Live Health Application traps to the MLS. The MLS traditionally does not have many models, allowing more capacity for the CA eHealth Live Health Application trap processing. However, the CA eHealth Live Health Application traps can be sent to any SpectroSERVER you select. Setting the SBG_AlertForwarding attribute to Yes on the EventAdmin or Host_systemEDGE model representing a Distributed eHealth System server allows forwarding of the alarms to other SpectroSERVERs if the target model does not exist on the same server.

Note: If your network includes a single standalone CA eHealth system, then the CA eHealth Live Health Application traps originate from the standalone system. Web services requests from OneClick terminate at the standalone system. Multiple CA eHealth clusters or multiple standalone CA eHealth systems cannot be integrated with CA Spectrum.

To configure the communication between CA eHealth and CA Spectrum, follow these steps:

1. Configure the CA eHealth server.
2. Configure Distributed Web Services if you are planning to have CA Spectrum monitor a Distributed eHealth cluster.

3. Configure the CA Spectrum OneClick web server.
4. (Optional) Set up authentication options.

SSL Scenarios and Action Required

If you decide to secure the CA Spectrum OneClick web servers or CA eHealth servers (or both) using Secure Socket Layer (SSL), consider installing the SSL certificates. Otherwise, many aspects of the integration fail to operate while SSL is enabled. If SSL is not in use, you can skip any sections of this guide regarding SSL.

How your SSL certificate is signed or generated determines whether you configure SSL and the configuration steps needed.

Determine which scenario applies and follow the process indicated. If your certificates are:

- **Signed by a Trusted Authority** - For a certificate that is signed by a Trusted Authority, no configuration is needed. You can skip the procedures that are related to configuring SSL for CA eHealth and CA Spectrum.
- **Generated Using Your Own Certificate Authority Server** - Install the certificate for their certificate authority server and use the -trustcacerts option. You can skip the remaining procedures that are documented in this guide that are related to configuring the SSL certificates.
- **Self-signed** - Install all self-signed certificates using the procedures that are detailed in this guide for CA eHealth (see page 20) and CA Spectrum (see page 27).

Note: For more detailed information about securing the servers using SSL, see the *CA eHealth Administration Guide* and the *CA Spectrum Administrator Guide*.

How to Configure the CA eHealth Server

Configure the CA eHealth server before you can configure CA Spectrum connect to it. The configuration process for the CA eHealth server is as follows:

1. Add a license (see page 20).
2. Import the SSL certificate to CA eHealth (see page 20) if you are integrating with a CA Spectrum OneClick web server that is running SSL.
3. Run the setup program (see page 21).
4. Configure communication (see page 25) when you are integrating a Distributed eHealth environment with CA Spectrum.

Add a License

The current version of CA eHealth does not require a license to integrate with and use the current version of CA Spectrum.

Note: For information about how to enter CA eHealth license information, see the *CA eHealth Installation Guide.* For information about integrating earlier releases of CA eHealth and CA Spectrum, see the corresponding *CA eHealth CA Spectrum Integration and User Guide* for those releases.

How to Import SSL Certificates to CA eHealth When a OneClick Web Server is Running SSL

To secure the CA Spectrum OneClick web server using *self-signed* SSL certificates or a certificate from your own root Certificate Authority, import the necessary certificates to CA eHealth. You import the certificates so that the nhSpectrumSetup utility can operate correctly. The certificates are required on the standalone CA eHealth system or the Distributed eHealth Console.

More information:

SSL Scenarios and Action Required (see page 19)

Import an SSL Certificate to CA eHealth

If you are using a self-signed SSL certificate to secure the OneClick server, import it to CA eHealth. If you are using a certificate signed by your own Certificate Authority, import the internal Root Certificate to CA eHealth.

Follow these steps:

1. Place the certificate in the CA eHealth $NH_HOME/Jre directory.
2. Open a shell on the CA eHealth server.
3. Execute the following command:

   ```
   'bash'
   ```

4. Execute the following command:

   ```
   cd $NH_HOME/Jre
   ```

5. Import the certificate using the following commands:

   ```
   bin/keytool –import –keystore lib/security/cacerts –file <certificate_filename>
   -alias <certificate_alias> -trustcacerts
   ```

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.

6. Enter the following password:

   ```
   changeit
   ```

   changeit

   Specifies the default password for the keystore.

   The certificate is imported to CA eHealth.

Run the Setup Program

The nhSpectrumSetup utility provides the launch for the OneClick link on the Live Health tab of the CA eHealth web user interface. The setup program prompts you for the information that you recorded on the setup checklist.

Note: If you are using SSL with OneClick, the SSL certificate must be installed (see page 20) before you run nhSpectrumSetup.

Follow these steps:

1. Log in to the CA eHealth system as the CA eHealth administrator.
2. Open a terminal window and change to the CA 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 CA Spectrum Import Setup dialog appears.

4. Enter the following information:
   - Hostname or the IP address of the CA Spectrum OneClick web server
   - Port number for OneClick web server web requests
   - Path where the CA Spectrum OneClick web server is installed
   - Set the Https field to Yes or No
   - Username that is used to log in to the OneClick web server
   - Password for the specified user name

5. Click OK.

   CA eHealth verifies your settings and displays a message notifying you that the settings are valid. The validation process can take a few seconds.

6. Restart CA eHealth.

   The setup is complete.

Change the CA eHealth Server Port

When the CA eHealth web server port is changed, modify the NH_HTTP_PORT environment variable. Any Live Health alarms that were raised in Spectrum before the port number was changed launches to the old port number. Use landscape overrides (or the CA eHealth Server model settings in the current release) to override the port number for the server.

To change the server port, follow this process:

1. Set the NH_HTTP_PORT environment variable.
2. Change the CA eHealth server port.
3. Restart the CA eHealth server.

Run the Setup Program From the Command Prompt

You can run the nhSpectrumSetup command from the command line to configure the CA eHealth CA Spectrum integration.

Follow these steps:

1. Log in to the CA eHealth system as the CA 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. The command has the following format:

   - On Windows:

     ```
     nhSpectrumSetup [-h] [-list] [-host name] [-port number] [-path path] [-https true|false ] [-user name] [-password] [-debug]
     ```

   - On UNIX:

     ```
     ./bin/nhSpectrumSetup [-h] [-list] [-host name] [-port number] [-path path] [-https true|false ] [-user name] [-password] [-debug]
     ```

-h

Displays help for this command.

-list

Lists the current setup parameters.

- host *name*

Specifies the host name or IP address of the CA Spectrum OneClick web server.

- port *number*

Specifies the port number for the CA Spectrum OneClick server web requests.

Default: 80

- path *path*

Specifies the path where CA Spectrum is installed.

Default: spectrum

Note: Use the default value unless you specified another path when installing CA Spectrum.

- https true|false

Specifies whether the CA Spectrum OneClick web server is accessed using SSL.

- user *name*

Specifies the username that is used to log in to the CA Spectrum OneClick web 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, type the password. The program then reads the password.

-debug

Enables the debug mode which provides details when there is a failure when validating the configuration.

Distributed eHealth Communication

All CA eHealth web servers in the cluster must be configured to use the same web protocol (HTTP/S) and port.

Configure the Password for Distributed eHealth Communication

The only CA eHealth user with web service access is the 'admin' user. The admin user must have the same password on all cluster systems. Distributed eHealth relies on the reportCenterAdminPassword parameter for distributed authentication. To set this password, use the nhRptCtrConfig command.

Note: For more information about using the nhRptCtrConfig command, see the *CA eHealth Installation Guide*.

Configure the Protocol and Port for Distributed eHealth Communication

Distributed eHealth communication relies on the webServicesProtocolAndPort parameter to properly forward distributed requests from the Distributed eHealth Console to the Distributed eHealth System servers.

To set the parameter, run the nhParameter command.

Note: Configure this setting even if the value is the default of http:80.

This command uses the following syntax:

```
> 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

  ```
  nhParameter -set webServicesProtocolAndPort https
  ```

- Set to https and nondefault port 444

  ```
  nhParameter -set webServicesProtocolAndPort https:444
  ```

- Set to http and nondefault port 81

  ```
  nhParameter -set webServicesProtocolAndPort http:81
  ```

- Revert to default, http:80

  ```
  nhParameter -delete webServicesProtocolAndPort
  ```

Verify the parameter setting

To verify the setting for the webServicesProtocolAndPort parameter, use the following command:

```
nhParameter –get webServicesProtocolAndPort
```

Configure Distributed eHealth Communication if SSL is in Use

If you are using Secure Sockets Layer (SSL) in a Distributed eHealth cluster, also secure the communication between the Distributed eHealth Console and the Distributed eHealth Systems. If you secure your servers using self-signed certificates or certificates from your own Certificate Authority, import those certificates (see page 20) into the Distributed eHealth Console.

More information:

SSL Scenarios and Action Required (see page 19)

Configure the Live Exceptions Alarm Notifier

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

Note: For more information about configuring Live Exceptions, see the CA eHealth online help.

Follow these steps:

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 information under Edit Trap Destination:

   - Hostname of the SpectroSERVER.
   - IP address of the SpectroSERVER.
   - Port number for the SpectroSERVER.

   Note: If you are utilizing the Trap Director feature in CA Spectrum, you can enter the Trap Director SpectroSERVER at this step. You must still configure a model to process the Live Exceptions traps in CA Spectrum, but with Trap Director that model does not need to reside on the target 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. Perform the following steps:

   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.

   The Notifier rule is saved.

Configure Health Reports

You can also configure the individual Health reports to forward traps for Health exceptions to the SpectroSERVER. When the scheduled Health report runs, CA 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 an on demand Health report, exceptions are not forwarded.

Follow these steps:

1. Launch the OneClickEH console.
2. Select Tasks and Information, Report Management, Report Templates, and the Health tab.
3. Select the report from which you want to forward Health exceptions. Right-click, and select Edit Report Template.
4. Select General from the Show drop-down list under Presentation Attributes.
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.

   Example: 001.02.03.004:162

7. Click OK.
8. Select Exceptions from the Show drop-down list under Presentation Attributes.
9. Select Send Exceptions SNMP Trap in the Attribute table.

10. Select Yes in the Value field.
11. Click OK.

How to Configure the Spectrum OneClick Server

After you configure the communication with the CA eHealth server, configure the CA Spectrum OneClick web server to complete the integration.

Follow this process on the CA Spectrum web server:

1. Import the SSL certificate to OneClick when you are using a CA eHealth server that is running SSL.
2. Designate the Active CA Spectrum OneClick web server and configure it to connect with the CA eHealth server.
3. Set the name synchronization interval.
4. Map the CA eHealth and the CA Spectrum elements.
5. To manage CA eHealth alarms, configure CA Spectrum.
6. Configure any additional passive CA Spectrum OneClick web servers.
7. To access CA eHealth reports, configure CA Spectrum. Optionally, you can also configure the Active CA Spectrum web server to clear any CA eHealth Live Health Application alarms.
8. Set up synchronized discovery.
9. (Optional) Customize report launches.
10. (Optional) Enable authentication options.

How to Import SSL Certificates When a CA eHealth Server is Running SSL

Import the necessary certificates to CA Spectrum if you want to secure the CA eHealth servers using *self-signed* SSL certificates or certificates that are signed by your own root Certificate Authority. If you are using a certificate that is signed by a trusted Certificate Authority no action is required. If you are configuring the integration with a Distributed eHealth cluster, all servers in the cluster must use the same web protocol and port.

You import (see page 28) the SSL certificate for the CA eHealth front-end or standalone CA eHealth server on any OneClick web server that is configured as Active or Passive.

More information:

SSL Scenarios and Action Required (see page 19)

Import an SSL Certificate to CA Spectrum

When you want to secure the CA eHealth server using SSL with self-signed certificates or a certificate signed by your own Certificate Authority, import the necessary certificates to CA Spectrum so that the integration works correctly.

Follow these steps:

1. Place the certificate in the *$SPECROOT*/Java/jre directory on the OneClick server.
2. Open a shell on the OneClick web server.
3. Execute the following command:

   `'bash'`
4. Execute the following command:

   `cd $SPECROOT/Java`
5. Import the certificate using the following commands:

   `bin/keytool –import –keystore $SPECROOT/custom/keystore/cacerts –file <certificate_filename> -alias <certificate_alias> -trustcacerts`

   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.
6. Enter the following password:

   `changeit`

   changeit

   Specifies the default password for the keystore.
7. Restart the CA Spectrum OneClick web server for the certificates to take effect.

   The SSL certificates are imported.

Configure CA Spectrum to Integrate with the CA eHealth Server

After completing the CA eHealth setup, configure CA Spectrum to recognize the CA eHealth server or Distributed eHealth Console.

Follow these steps:

1. Log in to the CA Spectrum OneClick home page as a CA 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 CA eHealth server. When CA eHealth is configured for SSL or the one-way CA Spectrum to CA eHealth single sign-on authentication option, use the fully qualified domain name (FQDN).

   eHealth Server Port

   Specifies the port number on which CA eHealth listens for web requests.

   Note: If SSL access is required the default value for eHealth Server Port is 443.

   eHealth Admin Password

   Specifies the password for the user name "admin".

   OneClick Server Role

   Specifies what role this OneClick server performs in the network.

   SSL access required

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

   Note: If the CA eHealth server has a self-signed certificate or a certificate signed by your own Certificate Authority installed, install the certificate for the CA eHealth server in the CA Spectrum JRE.

   Unmapped model report launching

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

5. (Active Server Only) Select Active for the eHealth Alarm Notification Status to enable CA Spectrum to clear any CA eHealth Live Health Application alarms.

   If you configure CA eHealth to forward alarms to CA Spectrum and configure CA Spectrum to view CA eHealth alarms, the alarm notifier lets you clear those alarms directly from the OneClick console on the active CA Spectrum server.

6. (Optional) To verify that the server name, port, user name, and password result in a successful connection to the CA eHealth server, click Test.

7. Click Save.

eHealth Manager Hierarchy in CA Spectrum

When the current version of CA Spectrum is integrated with CA eHealth (Release 6.0 or later), the CA eHealth server topology is added to the eHealth Manager hierarchy in CA Spectrum OneClick. The topology is automatically added by the OneClick server that is configured in the Active role.

The new models in this hierarchy are:

eHealth Cluster

Organizes the servers in the cluster. A standalone CA eHealth System is considered a cluster of one server in CA Spectrum.

EhealthServer models

When CA Spectrum is integrated with CA eHealth (Release 6.1 and higher), these models organize the CA eHealth discovery policy models for the server. The web server settings available on these models are used to configure URLs for the report launches to each server.

Note: These models do not replace the EventAdmin or Host_systemEDGE models that are required for CA eHealth alarm processing.

Name Synchronization

Name synchronization lets CA eHealth elements take CA 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, CA Spectrum requests that the device element is named based on the device model name. The element is named according to the CA eHealth naming rules. CA eHealth applies whatever logic and restrictions necessary to make the synchronized name fit within the CA eHealth scheme. All elements that are related to the device element are renamed using the device model name.

Note: Name synchronization requires that a Router, Switch, or System element be present. Names for standalone elements, such as LANWAN, CPU, and Disk are not synchronized.

This feature can be used in the following circumstances:

Name Synchronization with Standalone CA eHealth

CA Spectrum makes the naming request to the standalone CA eHealth server. The synchronized name is 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. CA 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 is not 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 that are seen on alarm reports do not match the names for At-A-Glance and Trend reports.

Note: To configure this feature in Distributed eHealth properly, see the Distributed eHealth Communication section.

Name Updates

During an incremental mapping update, the element names are updated for all elements that are 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 CA Spectrum
- A new LANWAN element is added in CA eHealth

The CA eHealth element name is stored in a CA Spectrum attribute (EH_Report_Element_Name_List) for all mapped models. If EH_Report_Element_Name_List attribute is used with the element naming feature and the element naming feature causes the name to change in CA eHealth, the original element name is stored in CA Spectrum until the next incremental mapping, which reflects the new name.

When using element or model name synchronization, two mappings are required for the EH_Report_Element_Name_List Spectrum attribute to update if the CA Spectrum model names are changed. The first mapping sets the element name and the second mapping updates the CA Spectrum attribute.

Synchronized Discovery

Synchronized discovery is performed one way from CA Spectrum to CA 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.

CA eHealth discovery is policy-based and permits the storage and reuse of the environment under which an element was originally discovered. CA eHealth discovery 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

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

Note: Devices within container models are not discovered. The device models must be at the top level of the Global Collection to be discovered.

The CA eHealth web services are leveraged to notify CA eHealth of any membership changes, reconfiguration changes, or manual requests to invoke CA eHealth discovery for a model set.

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

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

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

- **Model Reconfiguration** - When CA Spectrum detects a reconfiguration of a device model, CA Spectrum requests a CA eHealth discovery.

  Note: CA Spectrum must be configured to request a CA eHealth discovery.

Note: As a best practice, frequently follow the links that are provided in the discovery request events and monitor the events for any conflicts. Resolve any conflicts that exist and then perform a rediscovery.

You can configure and manually request CA eHealth discoveries from any CA Spectrum OneClick console that is configured in a Passive or Active role. When CA Spectrum makes the request to the CA eHealth server, the request comes from the OneClick server in an Active role.

Important! If you set up the CA Spectrum and CA eHealth integration to have CA Spectrum initiate discoveries in CA eHealth, the community string that is specified on the device in CA Spectrum is used in CA eHealth for the discovery. If the community string you use is a read-only string, not all of the elements of the device may be discovered. To ensure all of the elements of the device are discovered, use a read/write community string.

Each CA eHealth server executes only one discovery at a time. Therefore, when multiple discovery requests are needed, CA Spectrum queues the requests. CA Spectrum then sends one request per CA eHealth server at set intervals.

In a Distributed CA eHealth environment, any new or modified elements that are discovered using Synchronized Discovery are not 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 Unmapped Model Report Launching feature to permit users to access reporting for new elements.

How to Create Global Collections

Global collections help you organize the network elements that CA Spectrum manages into logical groups in the CA Spectrum OneClick Topology.

CA eHealth uses specified global collections as a starting point to discover network elements that CA Spectrum manages. Therefore, before running the CA eHealth discover process, use global collections to specify which network elements that you want CA eHealth to monitor.

To create a global collection, follow this process:

1. Log in to the CA Spectrum OneClick Console.
2. Create one or more global collections containing the devices that you want to monitor with CA eHealth.

   Note: Devices within container models are not discovered. To discover the device models, the device models must be at the top level of the global collection.
3. (Distributed eHealth) Create a separate global collection for each Distributed eHealth System so that different CA eHealth systems are not polling the same device.

For more information about CA Spectrum global collections, see the *CA Spectrum Modeling and Managing Your IT Infrastructure Administrator Guide*.

How To Set Up Synchronized Discovery

Synchronized discovery involves the CA eHealth server and a CA Spectrum OneClick web server in an active role. More CA Spectrum OneClick web 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 CA Spectrum OneClick web server.
2. Configure more passive CA Spectrum OneClick web servers.
3. Create or edit a discover policy on the CA eHealth server to be used in CA Spectrum.
4. Configure CA Spectrum to trigger automatic discovery requests.
5. Configure the community string on the CA Spectrum devices that you want to discover in CA eHealth.

   Note: When you set up the CA Spectrum and CA eHealth integration to have CA Spectrum initiate discoveries in CA eHealth, the community string specified on the device in CA Spectrum is used in CA eHealth for the discovery. If the community string you use is a read-only string, not all of the elements of the device may be discovered. To ensure all of the elements of the device are discovered, use a read/write community string.

   For administrators, there is an attribute in CA Spectrum, *CommunityNameForSNMPSet*s that if populated, is used as the community string for synchronized discovery instead of the general *Community_Name* attribute. The *Community_Name* attribute may be visible to most OneClick users, while the *CommunityNameForSNMPSets* attribute is typically hidden. This setting lets you expose the read-only string for users, but CA Spectrum can share the read-write community string with CA eHealth for discovery.
6. Add the policy to a global collection on a CA Spectrum OneClick client.
7. Request a discovery. (Automatic discovery requests can also be enabled.)

Note: The eHealth Manager privileges can be disabled to prevent CA Spectrum users from seeing CA eHealth information.

Configure the Active CA Spectrum OneClick Server

To have CA Spectrum request CA eHealth discoveries, configure one active CA Spectrum OneClick server and set the synchronization interval.

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 an interval is necessary to ensure that the discovery request queue functions smoothly.

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

Follow these steps:

1. Log in to the CA 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 that you want in the Discovery Synchronization Interval field.

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

   The server configuration is saved.

Configure Additional Passive CA Spectrum OneClick Servers

To have the OneClick clients on a CA Spectrum server access CA eHealth information, configure the servers in an active or passive role. If you have multiple CA Spectrum OneClick web servers, one server must be active and the remaining servers must be passive.

The passive servers are only required when you use synchronized discovery and web server alarming features.

Follow these steps:

1. Log in to the Active CA Spectrum OneClick web server.
2. Open the OneClick home page in a browser, and click the Administration tab.

   The Administration Pages appear.
3. Click eHealth configuration.

   The eHealth configuration page appears on the right pane.
4. Select Passive from the drop-down list in the OneClick web server 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 a CA eHealth discovery policy to add to a global collection in CA Spectrum. We recommend 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 is generated in CA Spectrum. This alarm is meant as a notification of the violation of best practices and can be cleared if desired.

Follow these steps:

1. Log in to OneClick for eHealth (OneClickEH).

   For information about how to launch OneClickEH, see the *CA eHealth Administration Guide*.

2. Expand the Tasks and Information folder in the tree.

   Folders appear beneath it.

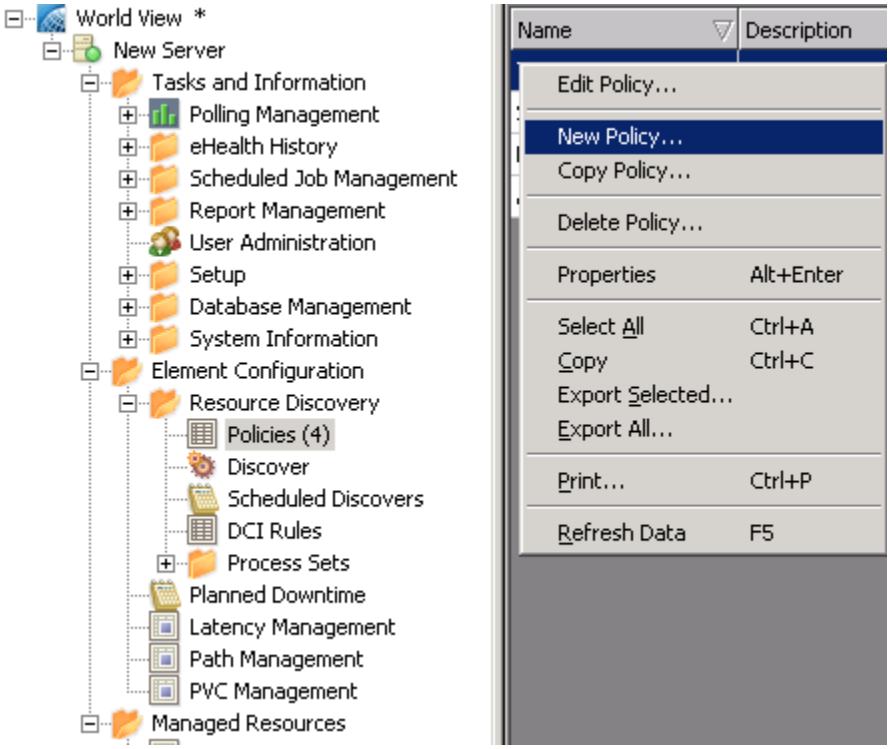
3. Expand the Resource Discovery folder.

   A list of services appears.

4. Click Policies.

   A list of existing policies appears in the right pane.

5. Right-click the list of policies, and select New Policy from the pop-up menu.



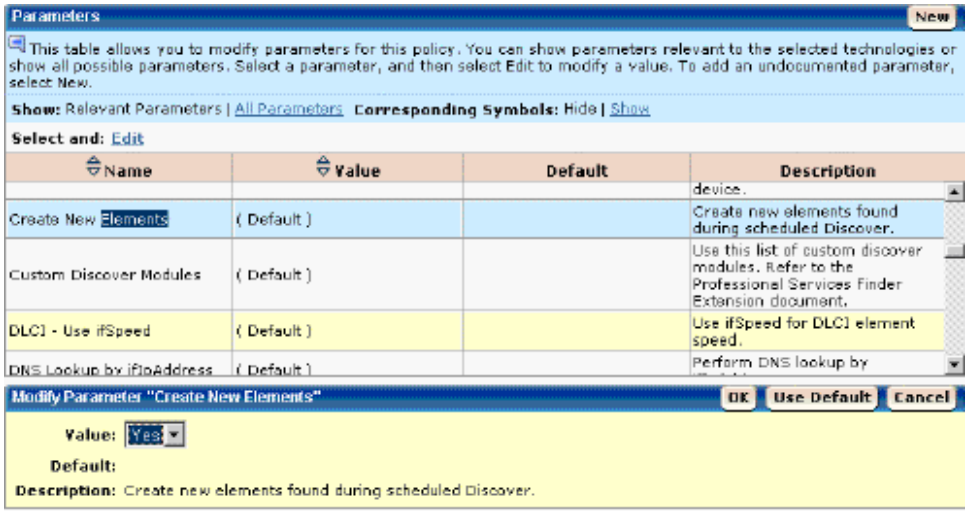
Note: You can also Edit, Copy, or Delete a policy from this menu.

The Create Discover Policy pane appears.

6. Select the options that 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 *CA eHealth Administration Guide* and the *CA eHealth Command and Environment Variables Reference Guide*.

Configure CA Spectrum to Trigger Automatic Discovery Requests

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

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

Note: The automated discovery settings only apply to future policy assignments. Manually request discoveries for any global collections that were previously assigned discovery policies.

Follow these steps:

1. Start a CA Spectrum OneClick client console.
2. Select the eHealth Manager in the Explorer tab in the Navigation pane.
3. Select the Information tab on the right pane.
4. Do one or both of the following actions:
   - 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

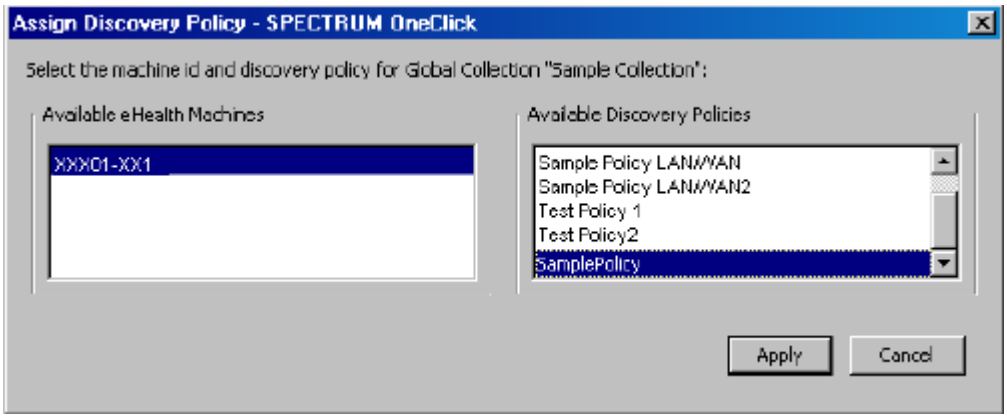
After you create a policy in CA eHealth, you assign it to a global collection in CA Spectrum as part of the synchronized discovery process.

Follow these steps:

1. Start a CA Spectrum OneClick client console.
2. Select the global collection that you want from the Explorer tab on the Navigation pane.

   The contents of the global collection appear on the Contents pane.
3. Click the Information tab in the Component Detail pane and expand the eHealth Discovery Policy section. Click Assign Discovery Policy.

   The Assign Discovery Policy dialog appears.
4. Select a CA eHealth system 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.

More information:

Run Synchronized Discovery (see page 62)

Mapping Elements

The CA Spectrum and CA eHealth mapping matches CA eHealth elements such as routers, systems, LAN/WANs and virtual elements to corresponding models in CA Spectrum. Mappings permit CA Spectrum to provide CA eHealth reporting options for the model in OneClick. Mapping also permits CA eHealth alarms for mapped elements to appear on the appropriate models in CA Spectrum. Alarms from unmapped elements are disposed on the device model instead.

Note: The Active OneClick web server performs the mapping activities.

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 CA eHealth System to a cluster.
- Incremental mapping lets you update your existing mappings after you add or remove elements from a CA eHealth system, or new models in CA Spectrum.
- Map by IP address maps a specific IP address on the specified CA eHealth system to the models in CA Spectrum.
- Update landscape overrides apply the changes that you have made to the mapping-overrides.xml file.

Mapping support includes the following virtual elements and models if *both* CA eHealth and CA Spectrum are monitoring one or more of these virtual elements:

- VMware
- Solaris Zones
- Microsoft Hyper-V
- IBM LPAR

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.

Note: If your CA eHealth and CA Spectrum environments were previously integrated and mapped, any existing virtual technology elements and models are mapped on the next incremental mapping.

Create Initial Mapping

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

Follow these steps:

1. Log in to the CA 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 page appears.
4. Scroll down to the CA eHealth mapping utilities section, and click Use eHealth Topology.

   OneClick loads the topology information for the CA eHealth system that is specified in the eHealth configuration section.
5. Click Run Initial Mapping.

Maintain Mappings

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

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

You can also manually run an incremental mapping by clicking the Run Incremental Mapping button.

You can only run an incremental mapping after you complete an initial mapping.

Note: The incremental mapping process requires that the OneClick web server and CA eHealth server or Distributed eHealth Console clocks be synchronized. We recommend that you synchronize these servers using 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.

Follow these steps:

1. Log in to the Active CA Spectrum OneClick web server.
2. Open the OneClick home page in a browser, and click the Administration tab.

   The Administration Pages menu appears.
3. Select eHealth configuration.

   The eHealth configuration page appears.
4. Scroll down to the eHealth mapping utilities section.
5. Click Use eHealth Topology, if that button is available.

   OneClick loads the topology information for the CA eHealth system that is specified in the eHealth configuration section.
6. Enter an IP address in the text box.

   Note: The IP address must match the IP address value of a CA eHealth element.
7. Click Map By IP.

   The IP address is used to map the model.

Clear Mappings

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

Follow these steps:

1. Log in to the Active CA Spectrum OneClick web server.
2. Open the OneClick home page in a browser, and click the Administration tab.

   The Administration Pages menu appears.
3. Select eHealth configuration.

   The eHealth configuration page appears.
4. Scroll down to the eHealth mapping utilities section.
5. Click Clear Map.

   The CA Spectrum mappings are cleared.

Override Mappings

With CA Spectrum, you can control the mapping process with manual overrides. Overrides are useful for situations in which a mapping cannot be determined programmatically. Overrides are also useful when you want to use a different mapping other than the default mapping. For example, if multiple ports on a device cannot be mapped because their values are not unique and 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 Distributed eHealth Console for each CA Spectrum landscape. The current CA eHealth integration uses the same Distributed eHealth Console for the At-a-Glance and the Trend reports. To point the report launches for models on each landscape to a different Distributed eHealth Console using IP addresses or host names, use the overrides.

Follow these steps:

1. Log in to the Active CA Spectrum OneClick web server as the CA 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. To add your override settings, edit the mapping-overrides.xml file and then save the file.

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

If you create landscape overrides in the mapping-overrides.xml file, update the landscape overrides using the eHealth configuration page of the OneClick Administration web pages. To update the OneClick server with the configured overrides, click the Update Landscape Overrides button.

Any new OneClick clients use the new settings. To update to the latest settings, close any open OneClick clients and then reopen the clients.

The 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 execute by choosing a device IP and running Map By IP, which updates all manual mappings.

Alarm Configuration

If you configured CA eHealth to forward Live Exceptions alarms or Health exceptions to a SpectroSERVER, configure CA Spectrum to receive the alarms.

For integration purposes, you can use an EventAdmin or a Host_systemEDGE model type in CA Spectrum to represent the CA eHealth server. If the CA eHealth server is running a SystemEDGE agent, we recommend that you use the Host_systemEDGE model type. If the CA eHealth server is not running a SystemEDGE agent, use an EventAdmin model.

Modeling Requirements for Alarm Processing

When upgrading to the current version of CA Spectrum, be aware that the modeling required to support the CA eHealth and CA Spectrum integration has changed. Any EventAdmin representing a Distributed eHealth Console or standalone CA eHealth system with element-to-model mappings receives alarm 0x5420000. You can destroy any of these models except for the standalone CA eHealth server model on the SpectroSERVER receiving the Live Exceptions alarms. You can clear alarm 0x5420000 on that standalone CA eHealth server model.

The following models are required for CA eHealth alarm processing in CA Spectrum:

- **Distributed eHealth System -** You need one model for each Distributed eHealth System that forwards alarms to CA Spectrum. Each model processes CA eHealth alarms for its corresponding CA eHealth server. In a Distributed SpectroSERVER (DSS) environment, we recommend that this 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, you can model each Distributed eHealth System on the SpectroSERVER of your choice. If the Distributed eHealth System is running a SystemEDGE agent, model it using a Host_systemEDGE model type.

  Note: Modeling the Distributed eHealth Console to satisfy the CA eHealth CA Spectrum integration is not required.

- **Standalone CA eHealth Server** - If the server forwards alarms to CA Spectrum, you need one model to represent the standalone CA eHealth server. In a DSS environment, we recommend that the model is placed on the MLS, but you can use any SpectroSERVER. If the standalone CA eHealth system is running a SystemEDGE agent, model the standalone server using a Host_systemEDGE model type.

Configure CA Spectrum to View CA eHealth Alarms

If you configured CA eHealth to forward alarms to a SpectroSERVER, configure CA Spectrum to receive the alarms.

Note: With Trap Director enabled, Live Exceptions can forward traps to the Trap Director SpectroSERVER. Trap Director locates the models that you configure in the following steps when they reside on other SpectroSERVERs.

Follow these steps:

1. To launch the OneClick Console, select Start Console at the top of the OneClick page, and log in as a CA 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 CA eHealth server or Distributed eHealth Console, and change the Manager Name value to **eHealth**. Click OK.

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

   Note: For more information about creating a model in OneClick, see the *CA Spectrum Modeling and Managing Your IT Infrastructure Administrator Guide*.
7. Select the EventAdmin or Host_systemEDGE model in the OneClick Topology.
8. Select the Attributes tab in the Component Detail panel.
9. 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.
10. Double-click map_traps_to_this_ model_using_ IP_header in the right pane, and select Yes. Click OK.
11. Select SBG_AlertForwardingEnabled in the left window of the Attributes panel.

    The attribute is added to the right window of the Attributes panel.
12. Double-click SBG_AlertForwardingEnabled in the right window, and select Yes. Click OK.

13. 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.

14. 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 CA eHealth sends per second. Click OK.

    The value is saved.

15. Repeat steps 3 through 14 on the SpectroSERVER of your choice. We recommend using the Main Location Server to create models representing each CA eHealth server that is sending the Live Exceptions alarms to the SpectroSERVER.

    Note: If you are using any Host_systemEDGE models, create and assign a container for these models after you configure CA Spectrum to view alarms.

Create and Assign a Container to a Host_systemEDGE Model

The EventAdmin model is also a container model. An EventModel representing a device is created in the EventAdmin container when a CA eHealth alarm is generated for that device, and the device is not monitored in CA Spectrum. Because the Host_systemEDGE models are not containers, create a container for these models in CA Spectrum and assign the container to the Host_systemEDGE model. You can use the same container for multiple CA eHealth servers that are represented using the Host_systemEDGE models.

Follow these steps:

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. Provide a name for the model (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 is moved to the right window of the Attributes panel.

12. Double-click EventModelContainerHandle in the right window.

    Change the value to the model handle that you noted previously in step 8.

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.

Follow these steps:

1. Select the EventAdmin model in the Navigation pane of the CA Spectrum OneClick Explorer tab.
2. Select the List tab in the Contents pane.
3. Select all EventModel models in the list.
4. Click the copy icon in the toolbar.
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, we recommend that you destroy the old EventAdmin model to avoid an alarm duplication.

   The models are copied to the container.

Customize Report Launches

The launch definitions for mapped elements are stored in a generic, flexible XML file that you can customize. The XML comments and an XSD file are provided to help you change the XML file if necessary.

By default, a report launch is available for all element types and the launch also targets the Distributed eHealth Console in a Distributed eHealth cluster. You can add one or more tns:elementType XML elements to the tns:report XML element to establish the element types for which the report launch is available. Adding a target=”poller” attribute to the tns:report XML element causes the report launch to target the Distributed eHealth System that is home to the mapped element.

Several substitution variables are available for use in the URL of the report launch. Not all of the substitution variables that the default report launches are used, but they can be useful in building custom report launches. The available substitution variables are:

- {baseURL}
- {machineID}
- {elementID}
- {elementName}

The {machineID}, {elementID}, and {elementName} substitution variables can be used to insert the corresponding values into the URL based on the selected mapped element. The {baseURL} substitutes the protocol://server:port value that is based on the mapped element, the target attribute value from the tns:report element, and any override settings.

Regarding the report launches, the order of precedence of the override settings is as follows:

1. The landscape overrides.
2. The settings on the corresponding EhealthServer model in the eHealth Manager tree.
3. The protocol and port settings and the CA eHealth system name that appear on the eHealth Configuration Administration web page.

Example:

A report launch is defined with target=”poller” and the mapped element exists on the poller named mercury. Mercury is configured for HTTP on port 443. No landscape overrides are in place. To satisfy the SSL requirements, the Access Protocol, Server Port, and Server Host Name settings on the EhealthServer model have been set to https, 443, and mercury.acme.com respectively.

The {baseURL} is replaced with https://mercury.ca.com:443 in the URL when launching the report.

Note: For more information about how to construct URLs for CA eHealth reporting, see the CA eHealth online help.

Customize a Report Launch

You can customize the launch names to reflect the element names.

Follow these steps:

1. Copy the eHealthReports.xsd and eHealthReports.xml files from the $SPECROOT/tomcat/webapps/spectrum/WEB-INF/ehlth/config directory to the $SPECROOT/custom/ehlth/config directory.
2. Open the $SPECROOT/custom/ehlth/config/eHealthReports.xml file and make any of the following changes:
   - To add a report launch, add a tns:report entry similar to the existing launches, and specify elementTypes and url. If there are no elementTypes listed, then the launch is present for all element types.
   - To define the target server, specify either **poller** or **console** for the target attribute of tns:report.
   - To define the minimum CA eHealth version for each launch, specify the version using the minimumVersion attribute.
3. Save the changes.

Authentication Options

CA eHealth offers the following integration options for authentication:

- CA Spectrum to CA eHealth one-way single authentication support
- CA eHealth SAML support
- CA eHealth RADIUS support

All three methods let you use CA Spectrum. However, only the CA Spectrum to CA eHealth one-way single authentication option lets you drill down from CA Spectrum OneClick to the CA eHealth web user interface without providing extra credentials. The RADIUS and SAML options prompt you for credentials every time you drill down from CA Spectrum to CA eHealth.

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

How to Enable One-way Authentication from CA Spectrum to CA eHealth

The CA Spectrum to CA eHealth single authentication option provides one-way drill-down from CA Spectrum to CA eHealth through Embedded Entitlements Manager. This integration lets you use CA Spectrum to access the CA eHealth web user interface without being challenged for a user login. This authentication option is not bi-directional.

Note: Embedded Entitlements Manager offers support for several types of authentication, including LDAP. The Embedded Entitlements Manager integration for CA eHealth and CA Spectrum is limited to one-way single sign-on from CA Spectrum to CA eHealth. Though Embedded Entitlements Manager supports more authentication types, any implementation beyond single authentication is considered a customization, and coverage is not included as part of standard CA support. Contact CA Services for more information about custom implementations, including the LDAP option.

The user name synchronization across CA eHealth, Embedded Entitlements Manager, and CA Spectrum must be maintained.

Note: Although OneClick for CA eHealth user names and web user interface user names are case-sensitive, Embedded Entitlements Manager treats user names as case-insensitive for validation purposes.

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

1. If the user does not already have a CA eHealth web user account, the administrator must establish one for the user.
    a. Log in to the CA eHealth OneClick Portal (http://<EHEALTH_CONSOLE>/OneClickEH) and click Launch OneClick for eHealth.
    b. In the left pane, select Tasks and Information, User Administration.
    c. Right-click User Administration and select New User.
    d. Specify a User account and password, and appropriate access permissions that includes CA eHealth OneClick access.
2. To ensure that all features are accessible through the CA eHealth web user interface, the administrator must enable those privileges by configuring the web user account of the CA Spectrum user appropriately.
3. The user must have three identical user accounts (with the same user name) for the Embedded Entitlements Manager server, CA eHealth Apache Web server, and CA Spectrum user database server.

4. The CA Spectrum administrator for the system must install Embedded Entitlements Manager software and must follow the installation procedures in the Embedded Entitlements Manager documentation. Embedded Entitlements Manager must be installed on a separate, standalone server system.

   Note: If you want to use the LDAP authentication with the integration, configure the Embedded Entitlements Manager server accordingly. For more information, see the Embedded Entitlements Manager documentation.

5. The CA eHealth administrator for the system must run the nhWebSso command-line utility to enable the CA Spectrum - CA eHealth system to use the one-way drill-down authentication. Run this utility on both the CA eHealth back-end polling server and the CA eHealth reporting front-end server. You run this utility on both servers because the Alarm Detail Reports are run against the back-end polling server that manages the element being reported.

CA EEM Software

CA EEM is a proprietary software product that enables a limited one-way single authentication drill-down option from CA Spectrum to the CA eHealth web user interface.

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

Run the nhWebSso Command-Line Utility

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

This command has the following format and must be executed on your CA 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) Specifies the idle timeout (in minutes) before the user is rechallenged for authentication when accessing CA eHealth from an external application.

Default: 10 minutes

-disableFallback

(Optional) Specifies that single authentication fallback is disabled.

-disable

Disables single authentication when specified.

Example: Enable Support

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

Example: Disable Support

```
nhWebSso -disable
```

Error Handling

Login failure can occur with CA Spectrum CA eHealth One-way SSO, CA eHealth RADIUS, and CA eHealth SAML support because of the following misconfiguration or network issues:

- The authentication server is down or not reachable because of a network breakdown. In this case, the Apache server falls back to the standard CA eHealth authentication mechanism.
- The web user is not recognized or is not authenticated by the authentication server. For example, a user account does not exist in the SAML server user directory. In this case, the Apache server falls back to the standard CA eHealth authentication mechanism.
- The web user exists in the authentication server but has an invalid password. In this case, the Apache server falls back to the standard CA 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 CA eHealth account. In this case, the user is denied access and is redirected to an error page.

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

The default CA eHealth administrator account 'admin' is available to fall back to the standard CA eHealth authentication, regardless of the previously mentioned errors.

Use Advanced Logging Troubleshooting Tool

You can access the Advanced Logging option, which provides you with tools for troubleshooting and debugging the CA eHealth web software. This feature is available to CA eHealth web administrators only. Web users cannot access it.

Note: Use the 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 regularly enable them.

If you enable advanced logging, CA 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 CA eHealth products and features, Support can direct you to create a troubleshooting ZIP file. You must be logged in as the CA eHealth web administrator to create these files.

To create a troubleshooting ZIP file:

1. Log in as the CA eHealth web administrator.
2. Click the Administration tab on the CA eHealth web user interface navigation bar.
3. Click eHealth Management in the left pane, and click Advanced Logging.
4. Click Create Technical Support Information on the Advanced Logging page.
5. Locate Areas to Include and select one or more areas as instructed by your Technical Support Engineer.
6. Do one of the following actions if your CA eHealth system is a member of a Distributed eHealth cluster, in the Cluster Members field:
   - 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. Locate the File Directory field and specify the directory in which to create the ZIP file. The default is */ehealth*/tmp.

8. Locate the Call Ticket Number field and 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. Leave this field empty if you do not have a call ticket that is associated with this problem.

9. Click Create File.

   The troubleshooting ZIP file is created.

The Troubleshooting Tool

Support typically requests certain files to help to diagnose a problem that is in a specific area. To assist with the file collection, this tool collects copies of files from various subdirectories of the CA eHealth installation. The tool 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 can be large. Typically, the 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 can 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. Some problems can require you to enable advanced logging features before creating the troubleshooting ZIP file. The web server advanced logging features are on the Advanced Logging page of the CA eHealth web user interface. To enable advanced logging for the CA eHealth system processes, use OneClick for eHealth (OneClickEH). Your Support engineer can assist you when advanced logging is necessary.

Errors and Troubleshooting

CA 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 verifies the available space in the File Directory location. When the tool cannot find a specific file, or the File Directory does not have enough free space to hold a file, the tool omits that file and proceeds to the next file. The ZIP file contains a log file that describes the files included and files that were omitted.

Tomcat Logs Files

Tomcat server logs contain debugging information for CA Spectrum, CA eHealth, and synchronized discovery. This debugging information can be helpful to troubleshoot the situation if discoveries are failing.

The following logging information is available:

eHealth Mapping Detailed Logging

Provides detailed logs about the element mapping. The logs include the raw information that ALL of the CA eHealth web services send to CA Spectrum (including the discovery web service). These logs can be verbose. Only enable these logs if Information logging does not provide enough data to assess the issue accurately.

eHealth Mapping Information

Provides an 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 wrong. This log setting only supports Min/Max settings at the bottom of the page to control the Info/Debug level logging.

Accessing the log information depends on which server is experiencing problems. For example, you are logged in to the OneClick client and have problems accessing the web services to assign the discovery policy to the GlobalCollection. Then you log in to the OneClick client server and turn on the logging for synchronized discovery. Running the discoveries on CA eHealth sends alarms on the Discovery Policy or Manager Model. When this problem occurs, log in to the active server and turn on the logging feature.

The logging pages are on the Administration link of the OneClick web page. To find the settings, click the Debugging link in the horizontal gray bar, and click the Web Server Debug Page (Runtime) link on the left gray bar. The CA 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 gray bar.

How to Disable the Integration

To disable the integration, follow this process:

1. Launch the OneClick webpage.
2. Select Administration, and select eHealth Configuration from the left pane.
3. Click the Clear Map button.
4. Stop the Spectrum Tomcat server.
5. Remove the $SPECROOT/custom/ehlth/config/ehealth-config.xml file.
6. Start the Spectrum Tomcat server.
7. Open a OneClick client, and select the Locater tab.

8. Open the eHealth, Discovery Policies folder, and execute the All Discovery Policies Present in Spectrum search.
9. Delete all policy models returned.
10. Open the eHealth, Cluster Modeling folder, and execute the eHealth Server Models search.
11. Delete all server models returned.
12. Execute the eHealth Cluster Models search.
13. Delete all cluster models returned.
14. Open a bash shell on the previously active OneClick server, and execute the following command:

    ```
    cd  $SPECROOT/mysql/bin
    ./mysql –u root –p root password
    ```

15. Execute the following commands:

    ```
    drop database eh_integ;
    ```

    ```
    create database eh_integ;
    ```

    ```
    exit
    ```

    The integration is now disabled on the previously active OneClick server.
16. Execute steps 1-6 on any passive OneClick servers.

Chapter 4: CA Spectrum Usage

This section contains the following topics:

Tasks

With the CA eHealth CA Spectrum integration, you can perform the following tasks directly from the CA Spectrum OneClick console:

- Generate the CA eHealth At-a-Glance and Trend reports for elements in the OneClick Topology.
- Generate the At-a-Glance and Trend reports for mapped elements.
- View Alarm Detail reports for CA eHealth Live Health Application alarms.
- Clear the CA eHealth Live Health Application alarms.
- Request CA eHealth discoveries for devices in CA Spectrum.
- Monitor requested CA eHealth discoveries.
- Locate mapped or unmapped models in CA Spectrum OneClick.

Reports from the CA Spectrum OneClick Console

You can generate the following CA eHealth report types from the CA Spectrum OneClick console from any models that have been mapped to CA eHealth elements:

- At-a-Glance reports
- Trend reports (dependent on the element type)
- Live reports
- Performance Dashboard

The current integration supports reporting when:

- Multiple elements are mapped to a single model
- The CA eHealth Reports menu item is available when you right-click on a model in OneClick

If the CA Spectrum model is not mapped to a CA eHealth element, drill-down reports are unavailable from the Topology view.

In previous releases, the integration feature let you generate CA 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 CA eHealth element, the drill-down displayed an error. You can restore this report drill-down capability for unmapped models using the Unmapped model report launching field on the OneClick CA eHealth Configuration page.

Launch Reports from the CA eHealth Reports Dialog

You can launch one or more CA eHealth report types from the CA eHealth Reports dialog in CA Spectrum.

Follow these steps:

1. Drill down to a mapped model in the OneClick tree or topology.
2. Right-click, and select eHealth Reports from the pop-up menu.

   The eHealth Reports dialog opens.
3. Deselect the Close dialog after launching checkbox if you want to launch multiple reports.
4. Select one element in the Mapped Elements list.
5. Select one or more reports in the Available Reports list.
6. Double-click an entry in the Available Reports list or click Launch.

   The reports are generated.
7. Click Close.

   The eHealth Reports dialog closes.

View Trend Reports for Unmapped Models

You can view a CA eHealth Trend report when using the Unmapped model report launching option. CA 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.

Follow these steps:

1. Select the icon in your Topology in the CA 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 CA eHealth Trend Type Report, where Type is a resource such as System, Router, or LAN/WAN.
3. Select the CA eHealth Trend Type Report (Unmapped) menu option if you are using the unmapped model reporting option.
4. Select the Trend variable that you want to display.

   A new browser window opens.
5. Enter your CA 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 for Unmapped Models

You can view a CA eHealth At-a-Glance report when using the Unmapped model report launching option. The CA eHealth At-a-Glance reports provide detailed information for all critical performance parameters through a series of charts. These charts show the trends for the following important variables:

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

Follow these steps:

1. Select the icon in your Topology in the CA 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 CA eHealth At-a-Glance Type Report, where Type is a resource such as System or Router.

   A browser window opens.
3. Select the menu option CA eHealth At-a-Glance Type Report (Unmapped) if you are using the unmapped model reporting option.
4. Enter your CA eHealth web user name and password.

   A status window appears displaying progress as the report generates, then the report appears.

View CA eHealth Reports for Alarms

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

Follow these steps:

1. Right-click the appropriate row in the alarm list, and select one of the following reports:
   - CA eHealth At-a-Glance Type Report
   - CA eHealth Trend Type Report

   A new browser window opens.
2. Enter your CA eHealth web user name and password.

   A status window appears displaying progress as the report generates, and then the report appears.

View Alarm Detail Reports

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

Time

Specifies the time that 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.

Follow these steps:

1. Right-click the row in the alarm list, and select Alarm Detail Report (CA eHealth).

   A new browser window opens.

2. Enter your CA 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 a CA eHealth Live Health Application alarm from CA Spectrum when the problem has been fixed, or you have determined it is not a real problem.

Note: Verify that you have enabled the eHealth alarm notification status option first.

To clear an alarm from CA Spectrum, right-click the appropriate row in the alarm list, and select Clear Alarm. The alarm is cleared in both CA Spectrum and the CA eHealth Live Exceptions Browser.

Note: The alarms that are cleared in this manner will not be removed from an open CA eHealth Live Exceptions Browser until the next polling cycle (every 5 minutes by default).

Run Synchronized Discovery

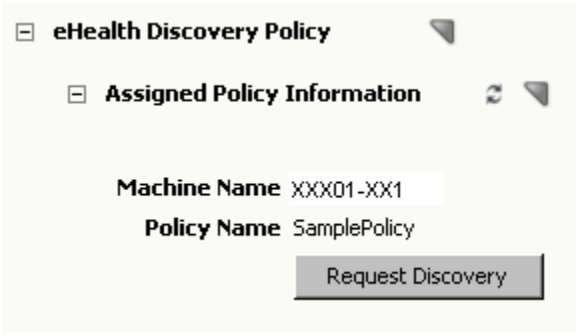
You can manually request discovery of a global collection, or have CA Spectrum automatically request CA eHealth discoveries. A manual request is processed according to the queue rules and typically is not executed immediately.

Important! When the CA Spectrum and CA eHealth integration is set up so that Spectrum initiates discoveries in CA eHealth, the community string that is specified on the device in CA Spectrum is used in CA eHealth for the discovery. If this community string is a read-only string, not all of the elements of the device are discovered in CA eHealth. Therefore, verify that you use a read/write string in CA Spectrum.

Follow these steps:

1. Start a CA Spectrum OneClick client console.
2. Select a global collection from the Explorer tab in the Navigation pane.

   The contents of the global collection appear in the Collection pane.
3. Select the Information tab. Expand the CA eHealth Discovery Policy section on the Information tab, and click Request Discovery.



   The discovery request is queued.

Monitor CA eHealth Discoveries

When the discoveries are requested and 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.

Follow these steps:

1. Start the CA Spectrum OneClick client console.
2. Expand the eHealth Manager tree in the Explorer Tab.
3. Expand the eHealth Cluster node.
4. Expand the corresponding CA eHealth server node.

5. Select the policy of interest.
6. To view the discovery events, select the Events tab.

   The discovery events for all discovery policies for the selected server are displayed.

Locate Mapped or Unmapped Models

To find models when you have the models in CA Spectrum mapped to elements in CA eHealth, use the Locater searches in OneClick. You can also locate models that have not been mapped.

Follow these steps:

1. Start the CA Spectrum OneClick client console.
2. Open the Locater Tab.
3. Expand the eHealth folder.
4. Expand the Mapped Models or Unmapped Models.
5. Execute the search of interest.

The models that meet the criteria are displayed. If you are viewing mapped models, click the Show mappings hyperlink to view the element mappings. You can also execute CA eHealth reports from the Mapped Models search results panel.

Using the eHealth Map Maintenance Page

You can perform various maintenance tasks on the CA Spectrum/CA eHealth mappings. Use the eHealth map maintenance section on the CA eHealth Configuration administration page on the CA Spectrum OneClick server to perform this maintenance.

Three types of mappings are available: initial mappings, incremental mappings, and map by IP. The CA Spectrum/CA eHealth mappings attempt to match CA eHealth elements that are related to routers and systems to corresponding models in CA Spectrum.

Note: Follow these steps if the eHealth map maintenance section is not visible:

1. Verify that the OneClick server role is set to Active.
2. To verify that the web services are responding, click the Test button.
3. Click Save.

Using the options that are provided, you can administer the following maintenance tasks:

Use eHealth Topology

Specifies to accept the eHealth server configuration reported by the eHealth web service, which is displayed in the table. When you select this option, the eHealth server configuration that was reported becomes the current eHealth topology from the OneClick configuration.

Note: If the eHealth server topology configured in OneClick is invalid, the mapping process does not function. If any of the following conditions are true, the topology is considered invalid:

- The IP address of the server is not found in the topology list.
- You are unable to look up the IP address of the server using name resolution.
- The configured server is not a standalone or front-end server.

Refresh eHealth Topology (button)

Specifies to refresh the current eHealth topology on the configured server.

Clear Map

Specifies to remove all CA eHealth/CA Spectrum mappings that are related to the integration on the configured server.

Run Initial Mapping

Specifies to run a full mapping and update the CA eHealth topology in the OneClick configuration. You can also use this option if you have added new servers to your CA eHealth cluster, which caused the migration of many elements from an existing server to a new server.

Run Incremental Mapping

Specifies to run an incremental mapping immediately, rather than waiting for the timed incremental update to run. This option is useful if you have deleted elements or added new elements or models to your CA eHealth or OneClick servers after the last successful initial or incremental mapping was started. You can also use this option when you add a server to the CA eHealth topology, and the new server contains entirely new elements.

Note: You cannot run an incremental mapping until an initial mapping has been completed.

eHealth Mapping Update Frequency

Lets you schedule a periodic incremental mapping. The periodic mapping is scheduled every 720 minutes (12 hours) by default. If you want to alter this setting you can, but click the Save button for your changes to take effect. The time that is listed in the eHealth Mapping Update Frequency box is from the time of the last mapping. The timer does not reset when you save a new value. To stop updates, enter zero.

Synchronize job interval

Lets you define the interval between scheduled synchronized jobs. Make sure that the interval you enter matches the scheduled Synchronize job interval on the CA eHealth distributed console.

Map By IP

Specifies to force a mapping of the device with the specified IP address against CA eHealth on the configured server. This option can be used for testing purposes. If a device is not mapping in a way that you expect, enable logging and can run a Map By IP on the problematic device. Running a Map By IP helps to determine why the mappings are not behaving the way that you expect them to behave. You specify the IP address in the field next to the Map By IP button.

Update Landscape Overrides

Specifies to update modified landscape overrides on the CA Spectrum OneClick server without restarting the server. Only new clients receive these updated settings. Restart any existing OneClick clients so that the new settings can take effect.

Chapter 5: CA eHealth Usage

This section contains the following topics:

Run Reports from the OneClickEH Console

From the OneClickEH console, you can run more types of reports on all of your elements, including the elements that you monitor with CA Spectrum.

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

At-a-Glance

Shows key performance indicators for a specific element that aids 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, multichart 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 OneClickEH console or web user interface to generate reports for a specific time period. You can also schedule CA eHealth reports to run automatically at specified times.

For more information about CA eHealth reports and how to run them, see the CA eHealth online help.

Launch the CA Spectrum OneClick Console

Launch the CA Spectrum OneClick console directly from CA eHealth to access CA Spectrum fault management, root cause analysis, and other network management features.

Follow these steps:

1. Log in to the CA eHealth web user interface.
2. Select the Live Health tab.
3. Click Launch OneClick.

   The CA Spectrum OneClick console opens.
4. Log in to the CA Spectrum OneClick console using your CA Spectrum user name and password.

Clear CA Spectrum Alarms

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

Follow these steps:

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 CA Spectrum.

Appendix A: Troubleshooting

This section contains the following topics:

Device Reconfigurations Result in Excessive CA eHealth Discoveries

Symptom:

Some device types have applications or functionality that trigger reconfigurations on every CA Spectrum polling cycle. If synchronized discovery is configured to request CA eHealth discoveries upon device reconfiguration, CA Spectrum forwards requests to CA eHealth for these devices on every discovery interval.

Solution:

Adjust the Discovery Synchronization Interval on the Active OneClick web server to 35 minutes or more.

Watch for CA Spectrum alarm 0x10050 "AN EXCESSIVE RATE OF DEVICE INTERFACE RECONFIGURATIONS" on devices in your environment.

Note: For more information about how to address the alarms, see the *CA Spectrum Modeling and Managing Your IT Infrastructure Administrator Guide*.

Once the device models have been properly configured for reconfiguration triggers, readjust the Discovery Synchronization Interval on the Active OneClick web server to its original setting.

Mapping Failure

Symptom:

The initial mapping for the CA eHealth integration fails with a NullPtrException error in the webserver log file. This failure happens when the mapping takes too long.

Solution:

If you experience an out of memory problem while running the CA eHealth initial mapping, we recommend that you increase the size of the web server memory. If you are running report manager on the same system, we recommend that you increase the memory size before you start the initial mapping.

Appendix B: Working with Overlapping Address Space (OAS) Environments

This section contains the following topics:

OAS Deployment Options and Supported Functions

When working with OAS environments, implement unique element naming and avoid the use of IP addresses as names. Using IP addresses as names can cause confusion when using centralized reporting from a distributed console.

The following information describes the deployment options for OAS environments using both CA eHealth and CA Spectrum:

Scenario 1 **– Single SpectroSERVER/CA eHealth**

A single CA eHealth system and a single CA Spectrum SpectroSERVER system.

Scenario 2 **– Distributed SpectroSERVER/CA eHealth**

A main location CA Spectrum server and distributed CA eHealth server reside on a central management LAN. A distributed CA eHealth system and a distributed SpectroSERVER reside on each remote site/LAN.

Scenario 3 **– Distributed SpectroSERVER/CA eHealth and Remote Poller**

A main location CA Spectrum server, a distributed CA eHealth server, and a distributed CA eHealth system reside on a central management LAN. A CA eHealth Remote Poller system and a distributed SpectroSERVER reside on each remote site/LAN.

Scenario 4 **– Distributed SpectroSERVER/CA eHealth, Remote Poller, and CA Spectrum Secure Domain Connector**

A main location CA Spectrum server, a Distributed CA eHealth server, and distributed CA eHealth system on a central management LAN. A CA eHealth Remote Poller system and a Spectrum Secure Domain system reside on each remote site/LAN.

Scenario 5 **– Distributed SpectroSERVER/CA eHealth, distributed CA eHealth, and CA Spectrum Secure Domain Connector**

A main location CA Spectrum server and a distributed CA eHealth server reside on a central management LAN. A distributed CA eHealth system and a Spectrum Secure Domain system reside on each remote site/LAN.

Function	1	2	3	4	5
Synchronized element and model naming	Yes	Yes	Yes	No[2]	No[2]
Synchronized discovery	Yes	Yes	Yes[1]	No[2]	No[2]
Drill down from CA Spectrum to CA eHealth reports	Yes	Yes	No	No[2]	No[2]
Live Health applications	Yes	Yes	Yes	No[2]	No[2]
CA Spectrum global applications supported	Yes	Yes	Yes	No	No
Architecture supported by CA Technologies	Yes	Yes	Yes[1]	Yes[2]	Yes[2]

Notes:

1. While it is possible to configure this function, CA Technologies does not support synchronized discovery on remote poller systems.
2. Devices must not be in a secure domain. Otherwise, the integration does not function properly. Model the devices in CA Spectrum to enable element-model mapping and alarm processing.

Recommendations for Deployment Options

The following common scenarios describe the possible deployment architectures:

Scenario One – OAS, SNMP allowed

Managed Service Provider (MSP) with multiple customers with overlapping IP Address Space (OAS). The management LAN is separate from the customer networks, and SNMP traffic is allowed through the firewall.

Scenario Two – OAS, SNMP blocked

MSP with multiple customers with overlapping IP Address Space (OAS). The management LAN is separate from customer networks, but SNMP traffic is *not* allowed through the firewall.

Scenario Three – SNMP blocked

The management LAN is separate from monitored networks using the firewall with SNMP blocked. The IP Address Space does not overlap.

Recommended Deployments

Architecture / Scenario	1 – OAS, SNMP Allowed	2 – OAS, SNMP Blocked	3 – SNMP Blocked
Scenario 1 – Single SpectroSERVER/CA eHealth	No, unless NAT is implemented, and sizing allows it.	No	No
Scenario 2 – Distributed SpectroSERVER/CA eHealth	Yes	Yes	Yes
Scenario 3 – Distributed SpectroSERVER/CA eHealth and Remote Poller	Integration may not be fully supported.	Integration may not be fully supported.	Integration may not be fully supported.
Scenario 4 – Distributed SpectroSERVER/CA eHealth, Remote Poller, and CA Spectrum Secure Domain Connector	No	No	No
Scenario 5 – Distributed SpectroSERVER/CA eHealth, distributed CA eHealth, and CA Spectrum Secure Domain Connector	No	No	No

Note: Where Network Address Translation (NAT) is deployed, SNMP v1 traps require deployment of a Trap Relay (TrapExploder) to convert the agent IP Address to an associated NAT address. SNMPv2c and v3 traps are not affected.

Deployment of NetQoS ReporterAnalyzer

To allow consolidated reporting in CA Performance Center (NPC), synchronize CA eHealth and NetQoS. In a distributed CA eHealth environment, synchronization between CA eHealth and NPC means that the distributed eHealth server is added as an NPC data source.

In a standalone or nondistributed CA eHealth environment, each CA eHealth server is also added as an NPC data source.

The synchronization between CA eHealth and NPC uses both the host name and IP address to match devices. In this way, NPC can support OAS. However, integration works only if Harvesters and CA eHealth systems both connect with the same IP address.

In a deployment where OAS exists and NAT is not an option, deploy NetQoS Harvesters on each remote site with the distributed CA eHealth systems. Harvester uses SNMP to poll the target interface to get speed and description, so you may need to deploy the Harvester on the customer site in some scenarios.

The following table represents the recommended deployments for NetQoS ReporterAnalyzer:

Architecture / Scenario	1 – OAS, SNMP Allowed	2 – OAS, SNMP Blocked	3 – SNMP Blocked
1 – Central NPC, Flow Mgr, Data Store, and Harvester	No, unless NAT is implemented.	No	No
2 – Central NPC, Flow Mgr, and Data Store. Harvester resides on the customer site.	Yes	Yes	Yes

Deployment Guidelines

The following guidelines maximize the integration benefits:

1. In an OAS environment with separate and overlapping domains:
   - The recommended deployment is CA eHealth, CA Performance Center, and CA Spectrum on a central management LAN behind a layer of Network Address Translation (NAT).

     Deploying centrally in this way offers the following benefits:

     - Full integration between components
     - Cost-effective scaling
     - Simplest and lowest cost deployment of High Availability, Disaster Recovery, or both

- In a NAT environment, avoid splitting collection engines between the central management LAN and remote domains. The split creates an undesirable mix of local devices and NAT addresses in the same implementation.
- Where NAT is not an option, or SNMP is blocked, then the deployment preference is:
  - Distributed eHealth, CA Performance Center with Flow Mgr and Data store, and CA Spectrum main location server on a central management LAN.
  - Distributed eHealth, NetQoS ReporterAnalyzer Harvester, and Distributed SpectroSERVER within each remote domain.

2. Deploy CA eHealth Remote Pollers only as an alternative to full Distributed eHealth servers where the disk space is an issue, and you do *not* require a fully supported integration to CA Spectrum and CA Performance Center.
3. Deploy CA Spectrum Secure Domain Connectors only when the CA eHealth integration and CA Spectrum Global Apps are *not* required (NCM, eVPN/VPN, and so forth), we recommend a CA Spectrum distributed SpectroSERVER.

Index

T

U