CA Spectrum® Infrastructure Manager

Enterprise VPN Manager User Guide

r9.4

ca®
technologies

CA Technologies Product References

This guide references CA Spectrum® Infrastructure Manager (CA Spectrum).

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

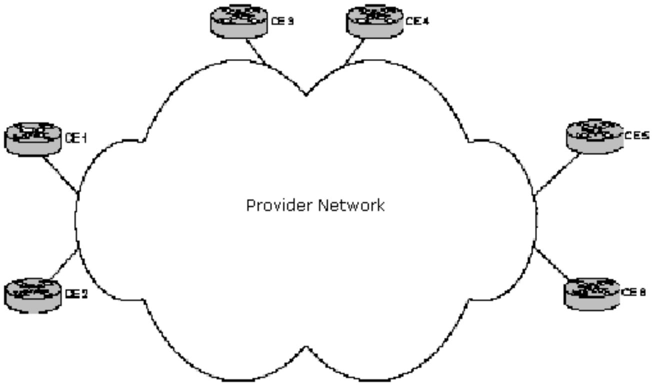
Chapter 1: Introduction

This section contains the following topics:

Enterprise VPN Manager

Enterprise VPN Manager is a CA Spectrum OneClick application that lets you discover, model, and monitor a provider-provisioned VPN. Your enterprise network ends at your customer edge (CE) devices. When lack access to performance statistics from provider core (P) or provider edge (PE) routers, you can infer service health by monitoring the behavior at the edges of the provider network, where enterprise CE devices exist.

The following illustration shows a typical provider-provisioned VPN from an enterprise customer perspective:



Model the links and devices (the CE routers) connected to a service provider using the Enterprise VPN Manager discovery, manual modeling, or import functionality. The Enterprise VPN Manager component then continuously monitors health and the service that is delivered by a service provider. The Provider_Cloud model represents the service that is provided to you by a service provider. The Outage events are processed and rolled-up into the health of the service provider which is reflected on the Provider_Cloud model. The Outage events are detected by actively polling CE routers for an availability and by polling the status of interfaces on CE routers which are connected to a service provider. Enterprise VPN Manager supports Layer 3 Multiprotocol Label Switching (MPLS) VPN networks for discovery, modeling, and monitoring. In addition, it can also model (manually or by importing the information) and monitor Layer 2 Virtual Private LAN Service (VPLS).

In addition to active polling, Enterprise VPN Manager supports Service Assurance (SA) Ping tests. Set up these tests to monitor service delivery and compliance with response time service-level agreements (SLAs). Ping tests offer the strongest option for service monitoring because they measure end-to-end response time.

Note: All elements that are connected to a given service provider must be modeled on a single SpectroSERVER.

Access Enterprise VPN Manager

You can access the Enterprise VPN Manager in the OneClick Navigation panel. Expand the appropriate landscape in the Explorer tab and select Enterprise VPN Manager.

Model information is displayed in the Contents and Component Detail panels.

Chapter 2: Discovery and Modeling

This section contains the following topics:

Provider_Cloud Model

The Provider_Cloud model represents the service that is offered to you by a service provider. Enterprise VPN Manager offers several methods to model network entities and services, such as Discovery, import, and manual modeling functionality to accommodate the unique needs of your enterprise.

Existing Device Models

If the CE devices with BGP4_App modeled in CA Spectrum, you can run Enterprise VPN Discovery to detect their connections to the service provider. Otherwise, you can delete and remodel the devices or run Application Reconfiguration on those devices. Once the necessary application models are present, you can run Enterprise VPN Discovery.

Add Autonomous System Numbers (ASNs) to the CA Spectrum Database

By default, CA Spectrum includes over two thousand officially registered Service Provider ASNs. You can add additional Service Provider ASNs to the CA Spectrum database with the Model Type Editor by modifying the ASNamesList attribute of the EntVpnManager model type.

Note: For more information about editing model type attributes, see the *Model Type Editor User Guide.*

Enterprise VPN Discovery Prerequisites

Model the physical components of your network, before using the Enterprise VPN Manager Discovery functionality.

Note: For information about modeling your network, see the *Modeling and Managing Your IT Infrastructure Administrator Guide* and the *Modeling Gateway Toolkit Guide.*

At minimum, verify that your CE routers are modeled in CA Spectrum.

On CE routers, verify that BGP peering to the service provider is properly configured. If your devices do not support BGP peering, Enterprise VPN Manager supports import from a CSV text file that is based on Autonomous System Numbers (ASN) and manual modeling.

More information:

Import Peer/Provider Information (see page 15)
Create a Service Provider Model (see page 17)

Access Enterprise VPN Discovery Configuration

The Enterprise VPN Discovery subview contains discovery controls and configuration.

Follow these steps:

1. Expand the appropriate landscape in the Explorer tab of the Navigation panel. Select Enterprise VPN Manager.

   Information and configuration appear in the Information tab of the Contents panel.

2. Expand the Configuration subview, and then expand the Enterprise VPN Discovery subview.

   The Enterprise VPN Manager Discovery options display:

   - Run Discovery
   - Import Config File
   - Provider Name Filter Type
   - Provider Name Filter
   - Discover On Activation
   - Create On Trap
   - Enable Background Discovery

- Background Discovery Interval (minutes)
- ASN Mapping

More information:

Enable Background Discovery (see page 12)
Configure Automatic Discovery on Model Activation (see page 11)
Configure the Background Discovery Interval (see page 13)
Run an On-Demand Enterprise VPN Discovery (see page 13)
Map Multiple Autonomous System Numbers to a Single Provider (see page 31)
Filter Service Provider Names During Discovery (see page 14)
Configure Enterprise VPN Manager for a bgpEstablished Trap (see page 12)

Configure Automatic Discovery on Model Activation

You can configure Enterprise VPN Manager to discover provider networks and CE interfaces automatically using the Discover On Activation option. When Discover On Activation is enabled, an Enterprise VPN Discovery is initiated each time CA Spectrum activates a device model. This process occurs on initial device model creation or on a SpectroSERVER restart. Determine whether this processing load (during these times) is appropriate in your environment. If not, disable this attribute.

Follow these steps:

1. Expand the Enterprise VPN Discovery subview as described in Access Enterprise VPN Discovery Configurations (see page 10).

   Enterprise VPN Discovery options appear.

2. Click set next to Discover On Activation. Select Yes to enable. The option is disabled by default.

   Discover On Activation is set. The value that you selected is displayed next to Discover On Activation.

More information:

Access Enterprise VPN Discovery Configuration (see page 10)

Configure Enterprise VPN Manager for a bgpEstablished Trap

Several devices that are configured with BGP4_App send a bgpEstablished trap when they establish a connection (a new peering session). You can configure Enterprise VPN Manager to discover provider networks and CE interfaces automatically in response to a bgpEstablished trap. When Create On Trap is enabled, an Enterprise VPN Discovery is initiated each time a bgpEstablished trap is received.

The Create On Trap option offers an alternative to Background discovery. Determine whether this Discovery option is appropriate in your environment. If this behavior is not desired, disable this attribute.

Follow these steps:

1. Expand the Enterprise VPN Discovery subview as described in Access Enterprise VPN Discovery Configurations (see page 10).

   Enterprise VPN Discovery options appear.

2. Click set next to Create On Trap and select Yes.

   Enterprise VPN Manager runs Discovery when it receives a bgpEstablished trap.

More information:

Access Enterprise VPN Discovery Configuration (see page 10)

Enable Background Discovery

You can configure Enterprise VPN Manager to discover provider networks and CE interfaces automatically using the Background Discovery option. When Enable Background Discovery is enabled, an Enterprise VPN Discovery is initiated based on the Background Discovery Interval. This process lets you determine the frequency of Discovery in your network. Determine whether this processing load (during these times) is appropriate in your environment.

Follow these steps:

1. Expand the Enterprise VPN Discovery subview as described in Access Enterprise VPN Discovery Configurations (see page 10).

   Enterprise VPN Discovery options appear.

2. Click set next to Enable Background Discovery and select Yes.

   Background Discovery is enabled and recurs according to the frequency that you set in the Background Discovery Interval.

Configure the Background Discovery Interval

If you enable background Discovery, you can configure the frequency for background Discovery. Enable Background Discovery must be set to Yes to enable the value for the Background Discovery Interval parameter.

Follow these steps:

1. Expand the Enterprise VPN Discovery subview as described in Access Enterprise VPN Discovery Configurations.

   Enterprise VPN Discovery options appear.

2. Click set next to Background Discovery Interval.
3. Enter a value (in minutes).

   The Background Discovery interval is set.

More information:

Access Enterprise VPN Discovery Configuration (see page 10)
Enable Background Discovery (see page 12)

Run an On-Demand Enterprise VPN Discovery

Enterprise VPN Discovery is the simplest method of modeling your network. Meet the prerequisites, before running an on-demand Enterprise VPN Discovery.

Follow these steps:

1. Expand the Enterprise VPN Discovery subview (see page 10).

   Enterprise VPN Discovery options appear.

2. Click Run.

   The Enterprise VPN Discovery runs, and Discovery status is displayed in the window next to the Run button.

More information:

Enterprise VPN Discovery Prerequisites (see page 10)
Access Enterprise VPN Discovery Configuration (see page 10)

Run Enterprise VPN Discovery on Selected Models

You can configure the Enterprise VPN Network Services Discovery from the OneClick views that display models.

Follow these steps:

1. Select the models.
2. Click Tools, Utilities, Network Services Discoveries, Enterprise VPN Discovery.

   The Discovery process is initiated. You can check the status in the Configuration subview.

Configuring Enterprise VPN Discovery During Modeling

CA Spectrum lets you configure Network Services Discoveries, including Enterprise VPN Discovery, during modeling. As a part of modeling configuration, you can specify the network service discoveries to run with the modeling process.

Note: For more information, see the *Modeling and Managing Your IT Infrastructure Administrator Guide*.

Filter Service Provider Names During Discovery

The Enterprise VPN Manager lets you filter the Service Provider names during Discovery run.

Follow these steps:

1. Select Enterprise VPN Manager in the Explorer tab.
2. Select the Information tab in the Contents panel.

   The configuration options for Enterprise VPN Manager display.

3. Expand the Enterprise VPN Discovery subview.

   The Discovery options are available, including these options:

   Provider Name Filter Type

   Determines whether the Provider names in the 'Provider Name Filter' field are included or excluded from modeling. Select from the following options:

   - Exclusive
   - Inclusive

   Provider Name Filter

   Lists the Service Provider names to be included or excluded when the Enterprise VPN Discovery is run. This field is used together with the 'Provider Name Filter Type' field.

   Note: Add Service Provider names to the Provider Name Filter field to filter and save them. If the Provider Name Filter Type is Inclusive and the Provider Name Filter is empty, all Provider Names are discovered.

More information:

Access Enterprise VPN Discovery Configuration (see page 10)

Import Peer/Provider Information

Enterprise VPN Manager enables you to import service provider information from MPLS and VPLS VPNs to create Provider_Cloud models. If BGP peering is not used to communicate with your provider, import lets you associate your Provider_Cloud models with sites. The import file must be in a comma-separated value (CSV) formatted file. You can create a CSV file with a text editor or can export it from another application. Know the service provider ASN and the IP Address for MPLS VPNs or the Interface Model Name for VPLS VPNs of your CE Interfaces.

Devices and interfaces must be modeled in CA Spectrum before importing a CSV-formatted text file.

The following parameters are supported for a line entry in an import file:

ProviderASN,SiteIfIdentifier,ProviderName,Region,SiteName,SitePriority

ProviderASN

Specifies the Autonomous System Number of the provider. Required parameter.

SiteIfIdentifier

Specifies the IP Address for MPLS VPNs or the Interface Model Name of the site interface for VPLS VPNs. SiteIfIdentifier is required.

ProviderName

Specifies the Name of the service provider.

Region

Lets you define Alarm Domains. This option is helpful when users have regional responsibility. The following values are available:

- Unavailable = Unavailable
- Arin = United States and Canada
- Lacnic = Latin America
- Ripe = EMEA
- Afrinic = Africa
- Apnic = Asia Pacific

SiteName

Specifies the name of the Provider_Cloud model.

SitePriority

Specifies an integer from 1 to N where 1 represents the primary connection and 2 through N represent backup connections.

The following text is an example of a CSV import file:

```
1234,138.42.14.143,ProvName,Lacnic,SiteName,3
```

Follow these steps:

1. Expand the Enterprise VPN Discovery subview as described in Access Enterprise VPN Discovery Configurations.

   The Enterprise VPN Discovery options display.

2. Click Import.

   The Import File dialog opens.

3. Locate your import file and click Open.

   Your peer or provider information is imported.

More information:

Access Enterprise VPN Discovery Configuration (see page 10)

Create a Service Provider Model

Enterprise VPN Manager lets you manually model the connections to a service from your provider. Manual modeling is an alternative method of modeling devices that do not support the BGP4_App MIB, which is required to run Enterprise VPN Discovery. Manually modeling the connections to your service provider requires significant time and maintenance.

Note: For more information about manual modeling, see the *Modeling and Managing Your IT Infrastructure Administrator Guide*.

Follow these steps:

1. In the OneClick Universe Topology tab, click in the Topology toolbar.

   The Select Model Type dialog opens.

2. In the All Model Types tab, select Provider_Cloud and click OK.

   The Create Model of Type dialog opens.

3. Fill in the appropriate information that is requested in the dialog and click OK.

   This model represents the network of the provider.

4. Create models of your CE devices.
5. Select a CE model in the Topology view.
6. Select the Interfaces tab of the Component Detail panel.
7. Locate the interface that is connected to the provider.
8. Right-click the interface and select Start Connection.
9. Return to the Universe Topology view.
10. Right-click the Provider_Cloud model and select Connect with <interfaceName>.

    This operation associates the interface of CE router with the provider. Repeat for each CE interface that must be manually connected to the provider.

Chapter 3: Service Monitoring Configuration

This section contains the following topics:

Overview

Enterprise VPN Manager can gather information about your provider network by pinging or polling. Ping tests offer the strongest measurement of service health because they measure end to end, while a port polling is focused on a single resource (a device or interface). However, the Ping tests have resource requirements that can affect on your network and equipment. Specifically, the Ping tests require the following additional resources:

- Processing time in CA Spectrum
- Network bandwidth to set up the tests
- Processing time in the CE routers
- Network bandwidth to execute the tests

Despite the resource requirements of Ping tests, they provide a valuable addition to your management capabilities. We recommend enabling the Ping tests.

Note: An SNMP read or write community name is required to provision SNMP polling.

Polling Configuration

Polling for port status serves as an alternative to Ping testing. Polling does not create as much of a network strain as Ping testing. SNMP secure information is not required to enable polling.

Port Polling

Enterprise VPN Manager uses the port status of the connected interfaces to update the status of the Provider_Cloud model. If port polling is disabled, the status is not updated. We recommend leaving port polling enabled (the default).

Note: Port polling includes all BGP sessions (active and inactive).

Follow these steps:

1. Locate the appropriate Enterprise VPN Manager model.
2. In the Contents panel, select the Information tab.
3. Expand the Configuration subview.
4. Expand the Management Configuration subview.
5. Locate Enable Port Polling, click set, and select Yes.

   Port Polling is now enabled.

Peer Session Polling

You can configure Enterprise VPN Manager to poll the status of peer sessions. When Peer Session Polling is enabled, Enterprise VPN Manager looks for changes to PeerState. The total number of operative and inoperative BGP peering sessions is used to compute the percentage of peering failures. This metric is evaluated when Enterprise VPN Manager determines the Provider_Cloud status.

Note: For more information about enabling alarms on failed peering sessions, see *Modeling and Managing Your IT Infrastructure Administrator Guide*.

Follow these steps:

1. Locate the appropriate Enterprise VPN Manager model.
2. In the Contents panel, select the Information tab.
3. Expand the Configuration subview.
4. Expand the Management Configuration subview.
5. Locate Enable Peer Session Polling and click set.
6. Select Yes to enable peer session polling.

More information:

Provider_Cloud Condition (see page 28)

Ping Test Requirements

Verify that the following requirements are met to enable Ping tests:

- Devices must support Cisco RTTMON MIB or RFC2925.
- Devices must be modeled with a read/write community name.

Configure at least one site with one of the following options:

- Ping from Site.
- Ping to/from Site.

Configure at least one (other) site with one of the following options:

- Ping to Site.
- Ping to/from Site.
- Ping Test Interval, Ping Test Timeout, and Response Time Threshold, set to appropriate values.
- The 'Enable Ping Tests' parameter must be enabled on each Provider_Cloud model that participates in the ping test.
- The 'Enable Ping Tests' parameter must be enabled on the Enterprise VPN Manager model.

More information:

Configure Ping Tests (see page 22)
Configure Ping Source and Destination (see page 22)
Enable or Disable Ping Tests (see page 24)

Ping Test Scalability

The scalability of Ping tests must be considered in large environments where fully meshed testing is performed. Performance testing has shown that full mesh testing beyond 50 sites greatly increases network traffic. Enterprise VPN Ping tests are therefore disabled by default. The number of Ping tests (and the resource requirements) can be efficiently managed by organizing your Ping tests.

We recommend selecting a relatively small number of important sites to perform Ping testing. When the number of sites (or remote offices) exceeds 50, let larger regional offices test back to corporate headquarters or test among themselves. For example, in an enterprise environment that consists of several regional offices and a corporate headquarters, configure your corporate headquarters as Ping to Site and your larger regional offices as Ping from Site to reduce the network load.

More information:

Configure Ping Source and Destination (see page 22)

Configure Ping Tests

Configure Ping Tests in Enterprise VPN Manager.

Follow these steps:

1. Access Enterprise VPN Manager.
2. Select the List tab in the Content panel and select the Provider_Cloud model.
3. Select the Information tab in the Component Detail panel and expand the Ping Test Configuration subview.

   The following Ping test configurations are available:

   Ping Test Interval (sec)

   Determines ping test frequency. Raise the value to reduce network traffic.

   Default: 1200 seconds

   Note: Lower values for the Ping Test Interval attribute can cause a severe performance impact.

   Ping Test Timeout (sec)

   Sets the timeout value before an event is generated for Ping tests. An event is generated if the ping response is not received before the timeout.

   Default: 5 seconds

   Response Time Threshold (ms)

   Sets the event threshold for the response time of a successful Ping test.

   Default: 250 milliseconds

Configure Ping Source and Destination

Remote sites typically communicate more efficiently with a central location than with each other. You can select the interfaces that send and receive a ping. By default, interfaces are set to Ping from Site. Therefore, no testing occurs until at least one interface is set to either Ping to Site or Ping to/from Site.

The following settings are available:

Ping Disabled

Indicates that ping is not enabled for this interface.

Ping from Site

Indicates that this interface can only originate a ping.

Ping to Site

Indicates that this interface can only receive a ping.

Ping to/from Site

Indicates that this interface can originate and receive a ping.

Follow these steps:

1. Select the appropriate Provider_Cloud model to change all relevant interfaces or select an individual Interface model to make an individual change.
2. Open the Attribute Editor.
3. Click Add next to the User Defined folder.

   The Attribute Selector dialog opens.
4. In the left panel of the Attribute Selector, select the Port folder.
5. In the right panel of the Attribute Selector, locate and select the PingTestEnable attribute and click OK.

   PingTestEnable is now displayed in the right panel of the Attribute Editor.
6. Select the appropriate value in the PingTestEnable list.

   Click OK.

Note: For more information on the Attribute Editor, see *Modeling and Managing Your IT Infrastructure Administrator Guide*.

Collapse BiDirectional Ping

Collapsing the BiDirectional pings reduces network traffic by eliminating potentially redundant ping tests. If one site can receive responses from another, the network between them functions properly. Therefore no test is sent in the opposite direction if BiDirectional tests are collapsed. By default, Collapse BiDirectional Ping is enabled.

Follow these steps:

1. Locate the appropriate Enterprise VPN Manager model.
2. In the Contents panel, select the Information tab.

3. Expand the Configuration subview.
4. Set the value of Collapse BiDirectional Ping to Yes.

Enable or Disable Ping Tests

Ping tests involve additional resource requirements on your network and equipment. As result, these tests are disabled by default. Ping tests are not conducted until:

- Ping source and destination for all Interfaces participate in the ping is configured
- Enable Ping Tests is set to Yes for each Provider_Cloud participating in the Ping test
- Enable Ping Tests is set to Yes on the Enterprise VPN Manager model

To enable or disable ping tests on the Enterprise VPN Manager model

1. Locate the appropriate Enterprise VPN Manager model.
2. In the Contents panel, select the Information tab.
3. Expand the Configuration subview.
4. Expand the Ping subview.
5. Set the value of Enable Ping Tests to Yes to enable ping testing. The default value is No.

To enable or disable ping tests on a Provider_Cloud model

1. Locate the appropriate Enterprise VPN Manager model.
2. In the Contents panel, select the List tab.
3. Select the appropriate Provider_Cloud model.
4. In the Component Detail panel, select the Information tab.
5. Expand the Ping Test Configuration subview.
6. Set the value of Enable Ping Tests to Yes to enable ping testing. The default value is No.

More information:

Ping Test Requirements (see page 21)

Chapter 4: Manage Provider VPN Services

This section contains the following topics:

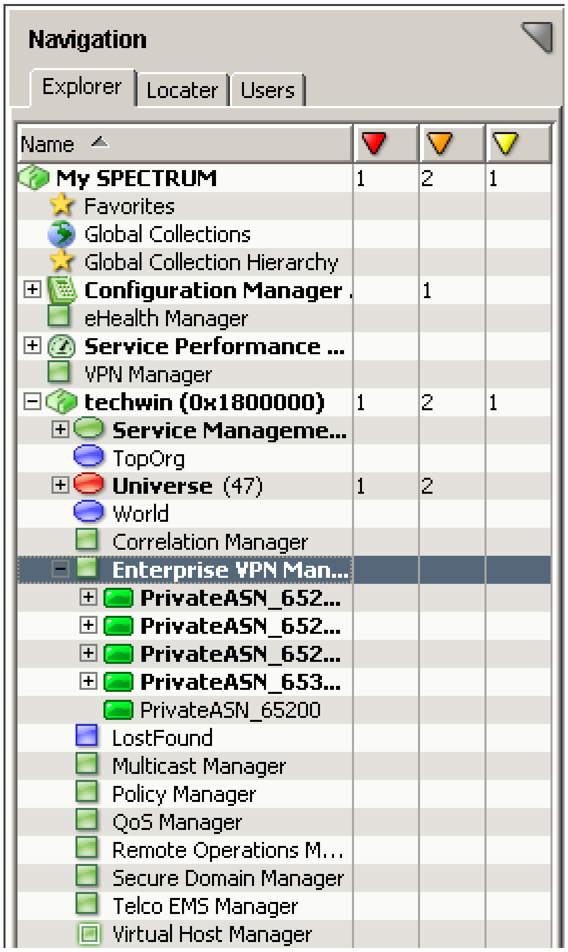
Enterprise VPN Manager Services

Enterprise VPN Manager enables you to continuously monitor the services that are provided to you by your service provider. You can see events and alarms pertaining to the health of various sites and the overall health of your provider. Enterprise VPN Manager lets you monitor the service across the three hierarchal levels (Enterprise VPN Manager model, Provider_Cloud model, and the individual interface/site models) of your provider network.

Enterprise VPN Manager Navigation

The OneClick Navigation panel displays a hierarchal view of your network. The Enterprise VPN Manager model exists within a particular landscape.

Expand the Enterprise VPN Manager model to see your providers and the sites that are connected to your providers, as shown in the following image:



Name	▼	▼	▼
My SPECTRUM	1	2	1
Favorites			
Global Collections			
Global Collection Hierarchy			
Configuration Manager .		1	
eHealth Manager			
Service Performance ...			
VPN Manager			
techwin (0x1800000)	1	2	1
Service Manageme...			
TopOrg			
Universe (47)	1	2	
World			
Correlation Manager			
Enterprise VPN Man...			
PrivateASN_652...			
PrivateASN_652...			
PrivateASN_652...			
PrivateASN_653...			
PrivateASN_65200			
LostFound			
Multicast Manager			
Policy Manager			
QoS Manager			
Remote Operations M...			
Secure Domain Manager			
Telco EMS Manager			
Virtual Host Manager			

Conduct an Enterprise VPN Search

You can access Enterprise VPN searches through the Locater tab. The Enterprise VPN search results, which appear in the Contents tab, help you access views that present management, performance, and configuration information. The Component Detail panel displays information about the device that is selected in the Contents panel. The following Enterprise VPN searches are available:

- All CE Devices by Provider
- All CE Interfaces by Provider
- All Enterprise VPN Managers
- All Providers

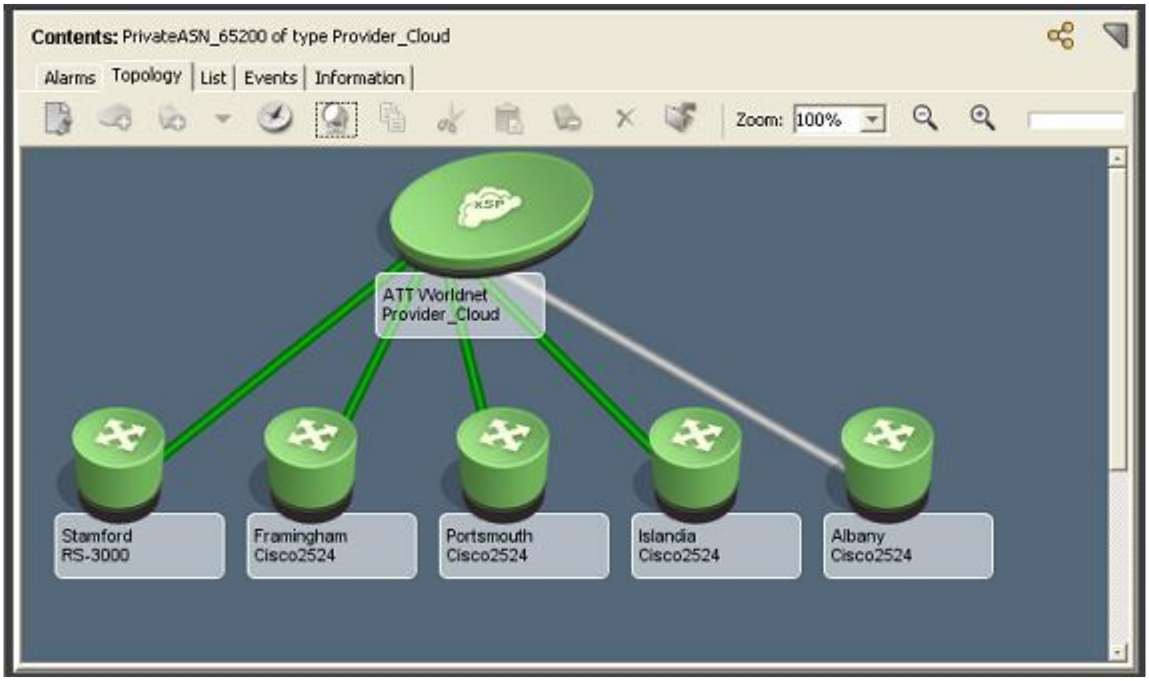
View Provider_Cloud Topology

The Provider Topology view displays the CE devices that are connected to a Provider_Cloud model. Selecting the Provider_Cloud or an interface model icon displays model information in the Component Detail panel.

Follow these steps:

1. Select the appropriate landscape from the Explorer tab in the OneClick Navigation panel.
2. Expand the Enterprise VPN Manager subview.
3. Select the appropriate Provider_Cloud model.
4. Select the Topology tab in the Contents panel.

   The Provider Topology resembles the following example:


Contents: PrivateASN_65200 of type Provider_Cloud

More information:

Access Enterprise VPN Manager (see page 8)

View Events and Alarms

Events and Alarms that are generated on a selected Provider_Cloud model display in the Events tab and Alarms tab of the OneClick Contents panel.

Note: For more information about the Contents panel, see the *Operator Guide*.

Execute OnDemand Ping Test

Enterprise VPN Manager lets you provision an OnDemand Ping test between two sites. The OnDemand Ping tests are a good way to troubleshoot connectivity between two sites without the resource requirements that are necessary to provision background Ping tests in a large environment.

Follow these steps:

1. Activate the Topology view for the appropriate Provider_Cloud model.
2. Click Select OnDemand Ping Start Point from the right-click menu of the interface model icon from which you would like to initiate the Ping test.
3. Right-click the interface model icon that is the destination of Ping test, and select Ping Test From <source_model_name>. This process starts the on-demand Ping test.

   The results of the Ping test appear in a dialog after the Ping test completes.

Note: You can execute an on-demand Ping test using interface models in the Navigation panel.

More information:

View Provider_Cloud Topology (see page 27)

Provider_Cloud Condition

Enterprise VPN Manager provides information about the status or condition of a Provider_Cloud model. The following types of information contribute to status reporting:

- Status of the interfaces that are connected to the Provider_Cloud
- Results of the automated service assurance tests (Ping and Response Time)

Important! To enable calculation of the VPN Manager Provider_Cloud condition, verify that the Live Pipes field is enabled. VPN status is not properly updated when Disabling Live Pipes are disabled.

The total number of operative and inoperative BGP peering sessions is used to compute the percent of peering failures. The percent of peering failures is evaluated when Enterprise VPN Manager determines the Provider_Cloud status.

Note: For more information on BGP peering sessions, see *Modeling and Managing Your IT Infrastructure Administrator Guide.*

The default thresholds are available in the Information tab of the Provider_Cloud model. The thresholds and their default value are:

- Critical Alarm Threshold % - 5%
- Major Alarm Threshold % - 3%
- Minor Alarm Threshold % - 1%

Provider_Cloud Roll-Up Condition

The aggregate condition of the interfaces contributes to the roll-up condition of the Provider_Cloud. For example, if 100 interfaces (or sites) are connected to a provider and 4 of those interfaces are unreachable by CA Spectrum, the condition is calculated as follows:

4 of 100 interfaces (4 percent) are unreachable.

This provider has a condition of Major Alarm because the 4 percent outage is above the default Major Alarm Failure threshold of 3 percent.

More information:

Provider_Cloud Condition (see page 28)

Service Assurance Test

Automated service assurance tests provide the best indication of provider health. These tests assure not only that the interface and the BGP peering session is operating but that the endpoints are able to pass traffic. An additional test verifies that the traffic passing through the network of the provider can reach the endpoint within the time thresholds that are specified in the service agreement.

Hide Symptomatic Alarms

Hiding symptomatic alarms reduces the number of alarms that are presented to you. You can configure Enterprise VPN Manager to generate a single alarm when a percentage of your interfaces that are connected to a service provider lose connectivity. When a significant number of sites are experiencing simultaneous problems, the provider is typically the root cause. The Minor Alarm Threshold is a point where Enterprise VPN Manager suppresses multiple site alarms and it instead generates an alarm on the Provider_Cloud model.

For example, you model a network with ten CE devices that are connected to a Provider_Cloud model. The alarm thresholds have the following settings:

- Critical Alarm Threshold %: 35
- Major Alarm Threshold %: 25
- Minor Alarm Threshold %: 15

Note: These settings are usually high and are not recommended for operational use.

When one CE device (10 percent of the devices that are connected to the service provider) becomes unreachable by CA Spectrum, a red alarm is raised on the device model and the status of the Provider_Cloud model remains green. The status of the Provider_Cloud model remains green because 10 percent falls below the 15 percent Minor Alarm Threshold. When a second CE device (20 percent) becomes unreachable, the Minor Alarm Threshold is violated. The status of the Provider_Cloud model is Minor Alarm and the alarms on the device models are hidden. The status of the two unreachable devices remains critical, but no Contact Lost alarms appear in the alarm log.

Follow these steps:

1. Locate the appropriate Enterprise VPN Manager model.
2. In the Contents panel, select the List tab.
3. Select the appropriate Provider_Cloud model.
4. In the Component Detail panel, select the Information tab.
5. Expand the Configuration Information subview.
6. Specify the following thresholds:

   Critical Alarm Threshold (%)

   Specifies the threshold for hiding Critical alarms.

   Default: 5

Major Alarm Threshold (%)

Specifies the threshold for hiding Major alarms.

Default: 3

Minor Alarm Threshold (%)

Specifies the threshold for hiding Minor alarms.

Default: 1

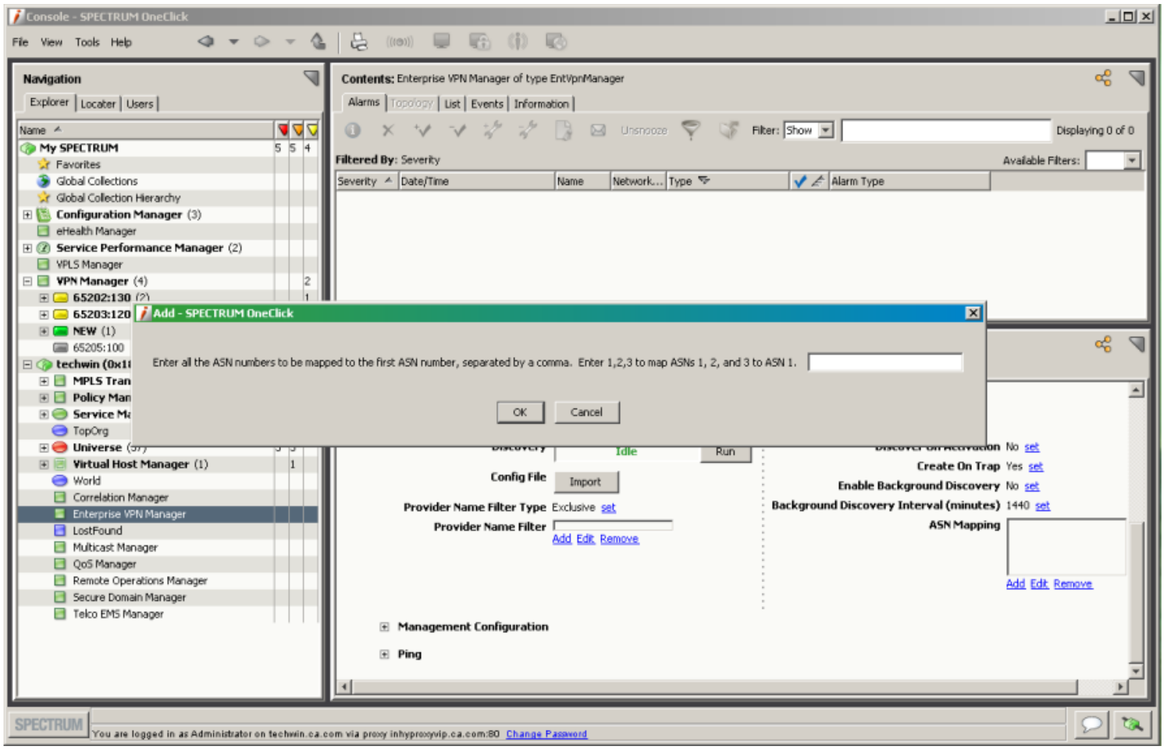
7. Select the Impact tab.
8. Expand the Symptoms subview.

   You can view the affected device sites.

Map Multiple Autonomous System Numbers to a Single Provider

The CA Spectrum MultipleASNLists attribute is now a list rather than a text string. This list lets you easily map multiple Autonomous System Numbers (ASNs) to a single provider.

This option is available when you select Configuration from the Enterprise VPN Manager and then edit the ASN Mapping field. CA Spectrum displays a List Renderer that lets you easily add, edit, or remove each list of ASNs that are mapped to the first ASN in the list, as shown in the following image:



Enter all the ASN numbers to be mapped to the first ASN number, separated by a comma. Enter 1,2,3 to map ASNs 1, 2, and 3 to ASN 1.

Discovery: Idle
Config File
Provider Name Filter Type: Exclusive
Provider Name Filter
Discover On Activation: No
Create On Trap: Yes
Enable Background Discovery: No
Background Discovery Interval (minutes): 1440
ASN Mapping

You are logged in as Administrator on techwin.ca.com via proxy inhyproxyvip.ca.com:80

Appendix A: Enterprise VPN Manager Events

This section contains the following topics:

Enterprise VPN Manager Events

Enterprise VPN Manager events enhance management of provider based services. Most of these events mirror the roll-up and service assurance methods of provider status calculation.

Roll-Up Method

The events in the roll-up method approach reflect the health of the service provider, infrastructure, which is modeled using the Provider_Cloud model type. The supported events are listed in the following table:

Event	Event ID	Description
InitialEvent	0x5180400	Provider is Initial
MinorEvent	0x5180401	Provider is Minor (% sites down)
MajorEvent	0x5180402	Provider is Major (% sites down)
CriticalEvent	0x5180403	Provider is Critical (% sites down)
GoodEvent	0x5180404	Provider is Good (all sites up)
MinorAlarmEvent	0x5180405	Provider Minor Alarm (% sites down)
MajorAlarmEvent	0x5180406	Provider Major Alarm (% sites down)
CriticalAlarmEvent	0x5180407	Provider Critical Alarm (% sites down)

Service Assurance Method

Multiple events are generated using the condition calculation method. They can be classified in several ways:

Scope

- Single test between a Pair of Sites
- Tests from a Site to all its Destinations
- Tests from all Sites to all their Destinations connected to the Provider

Test Type

- Connectivity (Did the Ping Succeed)
- Response Time (Did the Ping Succeed within the threshold)

Test Phase

- Test Model Creation
- Test Setup
- Ping Test Operation
- Response Time Threshold

Test Phases

Events occur at each phase of test creation, setup, or execution. The results that are reported attempt to determine the most likely root cause. Events that are caused by other events are typically excluded. An example of this result is shown in the following test phases:

1. Test Model Creation
2. Test Setup
3. Ping Test Operation
4. Response Time Threshold

Each successive test phase builds on the previous one. For example, if the Test Model cannot be created, none of the other phases are attempted. Therefore, you see a Test Creation Event (SingleTestCreateFailed) instead of multiple Ping Failure and Response Time Failure events (and alarms). The same is true for the Ping Test Operation and Response Time Threshold phases. If the Ping connectivity test fails (the timeout is 5 seconds), a Response Time failure is not reported. The default value for critical Response Time threshold is 250 milliseconds. Conversely, the Ping test can succeed but the Response Time threshold fails. The event sequence shows the following events:

Event	Event ID
SinglePingTestGood	0x5180604
SingleRTThreshFailed	0x5180607

Assume that you manage 100 sites and have modified the Ping values of minor, major, and critical thresholds to 5, 10 and 20 percent respectively. Next assume that 21 percent of the Ping tests from a site fail. A critical alarm is raised because it exceeds the value of the critical alarm threshold. There are 79 tests that have succeeded. Of these remaining successful ping tests, there are nine Response Time threshold violations. The calculation is done using 9 of 79 tests leading to a failure rate of 11 percent; this percentage is a major alarm status because it exceeds the major alarm threshold. The event sequence that is displayed in this case is as follows:

Event	Event ID
SiteTotalPingTestsCritical	0x5180621
SiteTotalRTThreshMajor	0x5180624

The example demonstrates how the success of each succeeding phase depends on the results of the previous phase. An event sequence can have the following events:

Event	Event ID
SiteTotalPingTestsGood	0x5180618
SiteTotalRTThreshCritical	0x5180625

More information:

Service Assurance Method (see page 34)

Single Test Between Sites

The following events are generated for a single site-to-site test.

Event	Event ID	Description
SingleTestCreateGood	0x5180600	Individual test created successfully
SingleTestCreateFailed	0x5180601	Individual test creation failed
SingleTestSetupGood	0x5180602	Individual test setup succeeded
SingleTestSetupFailed	0x5180603	Individual test setup failed
SinglePingTestGood	0x5180604	Individual ping test succeeded
SinglePingTestFailed	0x5180605	Individual ping test failed
SingleRTThreshGood	0x5180606	Individual RT test succeeded
SingleRTThreshFailed	0x5180607	Individual RT test failed

The following tests are part of each event cycle:

- Ping Connectivity
- Ping Response Time

A Ping cycle can pass the Ping Connectivity test but can fail the Response Time test when the ping response returns outside the specified response time window. In this case, the user sees SinglePingTestGood event followed by a SingleRTThreshFailed event.

Summary from One Site to All its Destinations

The following events are generated for a test from a single site to all of its destinations.

Event	Event ID	Description
SiteTotalCreatesGood	0x5180610	All of the site-to-site test that were created are good
SiteTotalCreatesMajor	0x5180612	Major % of site-to-site tests that were created failed
SiteTotalSetupsGood	0x5180614	All of the site-to-site test setups are good
SiteTotalSetupsMajor	0x5180616	Major % of site-to-site test setups failed
SiteTotalPingTestsGood	0x5180618	All of the site-to-site pings are good
SiteTotalPingTestsMinor	0x5180619	Minor % of site-to-site pings failed
SiteTotalPingTestsMajor	0x5180620	Major % of site-to-site pings failed

Event	Event ID	Description
SiteTotalPingTestsCritical	0x5180621	Critical % of site-to-site pings failed
SiteTotalRTThreshGood	0x5180622	All of the site-to-site RT thresholds are good
SiteTotalRTThreshMinor	0x5180623	Minor % of site-to-site RT thresholds violated
SiteTotalRTThreshMajor	0x5180624	Major % of site-to-site RT thresholds violated
SiteTotalRTThreshCritical	0x5180625	Critical % of site-to-site RT thresholds violated

Summary for All Sites to All Destinations in Provider

The following events are generated for tests from all sites to all destinations in a provider.

Event	Event ID	Description
TotalTestCreatesGood	0x5180700	All Ping tests for provider were created successfully
TotalTestCreatesMinor	0x5180701	Minor % of tests that were created for provider failed
TotalTestCreatesMajor	0x5180702	Major % of tests that were created for provider failed
TotalTestCreatesCritical	0x5180703	Critical % of tests that were created for provider failed
TotalTestSetupsGood	0x5180704	All Ping tests for provider setup ran successfully
TotalTestSetupsMinor	0x5180705	Minor % of test setups for provider failed
TotalTestSetupsMajor	0x5180706	Major % of test setups for provider failed
TotalTestSetupsCritical	0x5180707	Critical % of test setups for provider failed
TotalPingTestsGood	0x5180708	All Ping tests for provider executed successfully
TotalPingTestsMinor	0x5180709	Minor % of Ping tests for provider failed
TotalPingTestsMajor	0x5180710	Major % of Ping tests for provider failed
TotalPingTestsCritical	0x5180711	Critical % of Ping tests for provider failed
TotalRTThreshGood	0x5180712	All RT tests for provider executed successfully
TotalRTThreshMinor	0x5180713	Minor % of RT Threshold for provider violated
TotalRTThreshMajor	0x5180714	Major % of RT Threshold for provider violated
TotalRTThreshCritical	0x5180715	Critical % of RT Threshold for provider violated
DevTestCreatesGood	0x5180800	All RT tests for provider executed successfully

Event	Event ID	Description
DevTestCreatesMinor	0x5180801	Minor % of tests created for provider failed
DevTestCreatesMajor	0x5180802	Major % of test created for provider failed
DevTestCreatesCritical	0x5180803	Critical % of tests created for provider failed
DevTestSetupsGood	0x5180804	All Ping tests for provider setup successfully
DevTestSetupsMinor	0x5180805	Minor % of test setups for provider failed
DevTestSetupsMajor	0x5180806	Major % of test setups for provider failed
DevTestSetupsCritical	0x5180807	Critical % of test setups for provider failed
DevPingTestsGood	0x5180808	All Ping tests for provider executed successfully
DevPingTestsMinor	0x5180809	Minor % of Ping tests for provider failed
DevPingTestsMajor	0x5180810	Major % of Ping tests for provider failed
DevPingTestsCritical	0x5180811	Critical % of Ping tests for provider failed
DevRTThreshGood	0x5180812	All RT tests for provider executed successfully
DevRTThreshMinor	0x5180813	Minor % of RT Threshold for provider violated
DevRTThreshMajor	0x5180814	Major % of RT Threshold for provider violated
DevRTThreshCritical	0x5180815	Critical % of RT Threshold for provider violated

Index