RADVISION®
an Avaya company

Scopia PathFinder Server

Deployment Guide

Version 8.2

For Solution 8.2 (Intel servers only)

8.2

No representation of warranties for fitness for any purpose other than what is specifically mentioned in this guide is made either by RADVISION Ltd or its agents.

RADVISION Ltd reserves the right to revise this publication and make changes without obligation to notify any person of such revisions or changes. RADVISION Ltd may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this publication, it is furnished under a license agreement included with the product as a separate document. If you are unable to locate a copy, please contact RADVISION Ltd and a copy will be provided to you.

For further information contact RADVISION or your local distributor or reseller.

Deployment Guide for Scopia PathFinder Server Version 8.2, July 23, 2013

http://www.radvision.com

Table of Contents

Chapter 1: About Scopia PathFinder

Chapter 2: Preparing the Scopia PathFinder Server Setup

Chapter 3: Setting up the Scopia PathFinder Server

Chapter 4: Performing the Initial Configuration of the Scopia PathFinder Server

Chapter 5: Scalability, High Availability and Load Balancing with Scopia PathFinder

Chapter 6: Performing Maintenance Procedures

Chapter 1 | About Scopia PathFinder

Scopia PathFinder provides a complete firewall and NAT traversal solution for H.323 deployments, enabling secure connectivity between enterprise networks and remote sites.

Scopia PathFinder is part of the Scopia Solution the components of which can be combined to fit the existing network topology and videoconferencing requirements of the organization.

Scopia PathFinder maintains the security and advantages of firewall and NAT over heterogeneous video networks and allows seamless integration with existing video endpoints and infrastructure components.

Figure 1: Scopia PathFinder Functionality on page 5 illustrates the functionality of Scopia PathFinder.

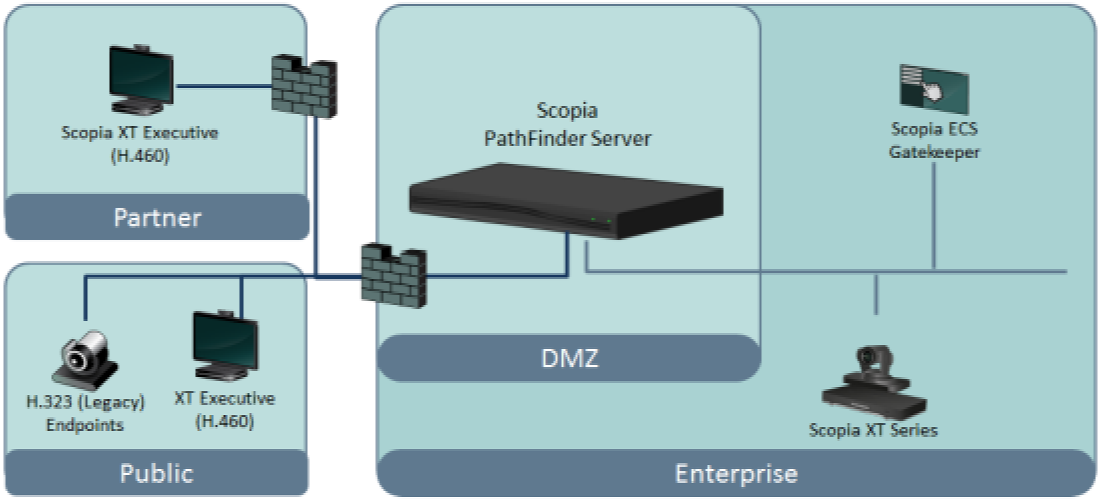


Figure 1: Scopia PathFinder Functionality

Scopia PathFinder uses the H.460 protocol. H.460 enhances the standard H.323 protocol to manage firewall/NAT traversal, employing ITU-T standards.

Endpoints which are already H.460 compliant can communicate directly with the Scopia PathFinder Server, where the endpoint acts as an H.460 client to the Scopia PathFinder Server which acts as an H.460 server.

The endpoints in a private network can communicate with the endpoints located in the public network via the Scopia PathFinder Server. Endpoints in the public network can join a conference hosted in the private network via the Scopia PathFinder Server if there is an open connection through the firewall. The Scopia ECS Gatekeeper provides standalone address resolution functionality in H.323 networks.

The Scopia PathFinder Server offers external endpoints a static address when joining conferences hosted in your organization. You can *dial1234@pathfinder.company.com* to access from outside the firewall, or you can dial *1234* directly if you are an H.460 client logged in to the Scopia PathFinder Server.

Navigation

- Main Features of Scopia PathFinder on page 5
- Technical Specifications on page 7

Main Features of Scopia PathFinder

Scopia PathFinder enables firewall and NAT traversal for secure connectivity between enterprise networks and remote sites. Scopia PathFinder has many powerful features including:

- Works with any firewall, endpoint and gatekeeper

  Scopia PathFinder solves near-end and far-end firewall issues by allowing you to maintain existing security measures with no changes to existing firewalls. All H.323 standards-based endpoints and gatekeepers are supported. Scopia PathFinder is also fully compatible with Scopia ECS Gatekeeper features: enhanced dial plan, hierarchy, conference hunting, CDR records and API for integration.

- Highly secured

  The Scopia PathFinder Server uses a hardened version of the Linux operating system which has a proven track record in secured system access.

  The Scopia PathFinder Server also provides uncompromised security by separating and restricting IP traffic between the external and internal network cards (NICs). The external NIC accepts access only from a very specific range of ports and media types, which significantly limits intrusive attempts on the system.

  Customers can restrict access of all management interfaces to a single NIC which resides either in the DMZ or in the secured zone.

  The Scopia PathFinder Server works as an application layer firewall for H.323 calls and inspects the contents of the traffic, blocking specific content, such as invalid H.323/RTP/RTCP packets. The Scopia PathFinder Server routes only validated H.323 based packets or RTCP/RTP based packets from the external NIC to the internal NIC.

- Scalable and distributed

  You can now deploy multiple Scopia PathFinder Servers for improved availability for dial in and dial out from your organization. As a result, enterprises can improve reliability or accommodate more external endpoints joining videoconferences by adding more Scopia PathFinder Servers to their deployments.

  The Scopia PathFinder Server works with an external load balancer providing unlimited scalability and solid redundancy for large deployments.

- Guest user dial-in

  The Scopia PathFinder Server supports Direct Public Access (DPA). Any public H.323 endpoint can directly call through the Scopia PathFinder Server without the need to deploy an additional Scopia PathFinder Client. Public H.323 endpoints which do not support the H.460 standard can directly call the Scopia PathFinder Server and easily and securely participate in any call or conference call inside the organization.

- URI Dialing

  With support for URI dialing Scopia PathFinder enables seamless and intuitive connectivity between enterprises, with customers and home workers. The following dialing methods are supported for both outgoing public calls and incoming public calls:

  – <Number>@<Domain> e.g. 5640@company.com

  – <Number>@<IP Address> e.g. 5640@216.2.12.310

  – <Name>@<Domain> e.g. Paul@company.com

  – <Name>@<IP Address> e.g. Paul@216.2.12.310

- Enhanced management capabilities

Scopia Management fully supports the Scopia PathFinder Server providing comprehensive maintenance tools such as user management, real-time monitoring, traps and alarms, automated log collection, and direct web access.

- Integrated web-based event log

  Use the event log for quick and effective troubleshooting

Technical Specifications

This section lists important information about the device you purchased. Refer to this information when preparing system setup and afterwards to verify that the environment still complies with these requirements.

This information lists the technical specifications of the Scopia PathFinder Server.

- System power requirements:
  - 350W, 100-240VAC input, 50/60Hz auto-switched
- Environmental requirements:
  - Operating temperature: 10°C to 35°C (50°F to 95°F)
  - Humidity: 90% non-condensing at 35°(95°F)
  - Storage and transit temperature: -40°C to 65°C (-40°F to 149°F), ambient
- Physical dimensions:
  - Size: 430mm (16.9”) width x 43mm (1.7”) height x 508mm (20”) depth
  - Weight: ~15kg (~34lbs)
  - 19-inch rack-mountable with flanges
- External interfaces:
  - Dual Gigabit NICs (rear panel)
  - 1 x DB9 serial port connector (rear panel)
  - 4 x USB 2.0 connectors (rear panel)
- Communications:
  - H.323
  - IPv4
  - Bit rate: up to 4Mbps per call
- Call capacity:
  - Up to 100 concurrent calls
  - Up to 600 registered devices
- Scalability:
  - RADWARE AppDirector 208
  - RADWARE AppDirector 1000
  - F5 BIG-IP Load Traffic Manager 1600 Series
- Firewall traversal:
  - H.460.18, H.460.19 including support for multiplexed media

  - Direct Public Access (DPA) solution for direct communication between internal endpoints in the internal network and external ones in the public network.
- Security:
  - H.235 for call privacy in all traversal modes (H.460, tunneling, DPA)

Chapter 2 | Preparing the Scopia PathFinder Server Setup

Perform the procedures in this section to prepare the site and device for installation.

Navigation

Planning Your Topology for Scopia PathFinder

Communication in the deployment comprises management, external communication traffic (unsecured), and internal communication traffic (secured). The Scopia PathFinder Server supports these communication protocols used by the system:

Table 1: Protocols supported by the Scopia PathFinder Server

Type of Network Traffic	Protocols supported by the Scopia PathFinder Server
Management	External management (TCP-XML based), HTTP, SSH, SFTP
External communication (insecure)	H.460, proprietary client-server tunneling, DNS
Internal communication (secure)	H.323

To create a secure deployment, administrators in organizations need to separate the various types of network traffic in the deployment.

The Scopia PathFinder Server houses two NIC cards. The Scopia PathFinder Server provides uncompromised security by using the two NICs for separating and restricting IP traffic in the deployment. The external NIC accepts access only from a very specific range of ports and media types, which significantly limits intrusive attempts on the system. The internal NIC is dedicated to the local traffic. We recommend configuring the second NIC to also support management traffic.

There are two recommended ways of deploying the dual-NIC Scopia PathFinder Server:

- Bypassing the enterprise firewall

  The external NIC is connected to the external network while the internal NIC resides in the enterprise LAN. The external endpoints have access to the external NIC through the firewall and the NAT. The internal NIC communicates with the components of the internal network and bypasses the firewall to the enterprise LAN. Figure 2: Deploying a Dual-NIC Scopia PathFinder Server bypassing the enterprise firewall on page 10 illustrates this type of deployment.

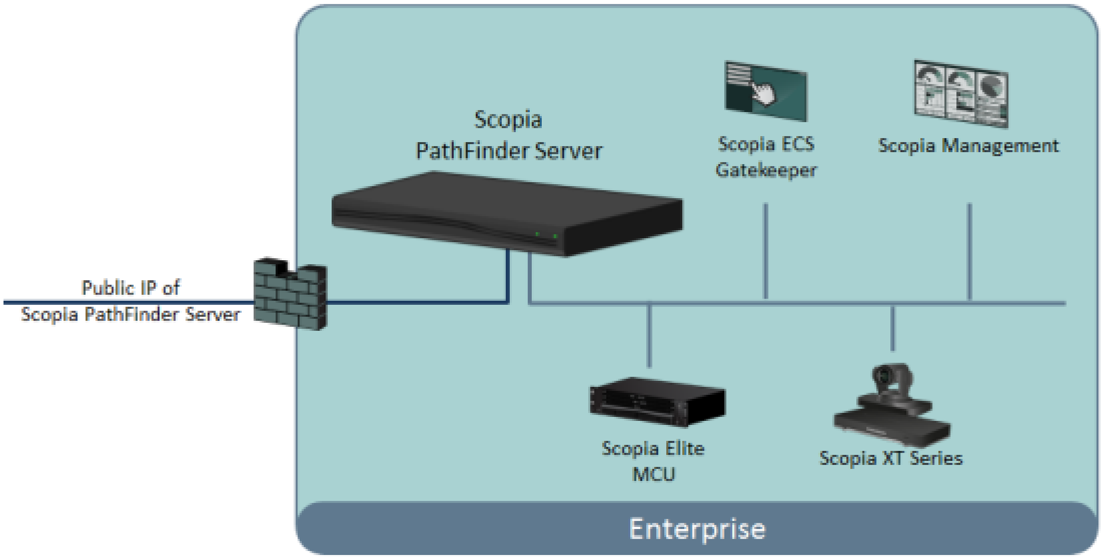


Figure 2: Deploying a Dual-NIC Scopia PathFinder Server bypassing the enterprise firewall

- Located in the DMZ

  The Scopia PathFinder Server is located in the DMZ behind the firewalls. The DMZ is divided into two subnets. The external NIC is connected to the outer DMZ and the internal NIC is connected to the inner DMZ. The subnets do not communicate between them. Figure 3: Deploying a high-security Dual-NIC Scopia PathFinder Server on page 10 illustrates this highly secure deployment.

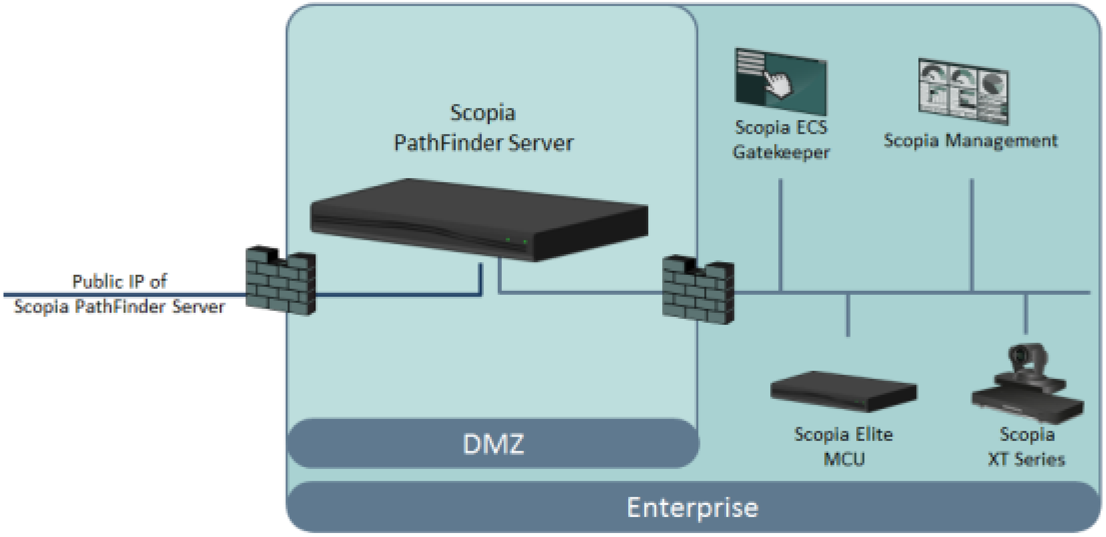


Figure 3: Deploying a high-security Dual-NIC Scopia PathFinder Server

Deploying the Scopia PathFinder Server requires configuring the unit itself as well as several other components. For information on components that are part of the Scopia Solution, see the *Scopia Solution guide*.

SCOPIA PathFinder Servers can also be clustered behind a load balancing system for scalability and high availability. See Scalability, High Availability and Load Balancing with Scopia PathFinder on page 52.

Important:

Small and medium-size enterprises that set up videoconferences within their enterprise can choose to deploy Scopia PathFinder Server with a single NIC. Contact Customer Support for information on that type of deployment.

Ports to Open on Scopia PathFinder

Scopia PathFinder is Scopia Solution’s answer to firewall traversal. The Scopia PathFinder Server is an H.460 server, typically deployed in the DMZ, while the Scopia PathFinder Client is an H.460 client, typically deployed outside the enterprise firewall with the H.323 endpoint (see Figure 4: H.323 connections to Scopia PathFinder Server on page 12).

Many recent H.323 endpoints have built-in H.460 functionality (which enables secure communication), thereby avoiding the need for a Scopia PathFinder Client. If an H.323 endpoint located in a partner company does not have H.460 capabilities, it must communicate via the Scopia PathFinder Client to access the Scopia PathFinder Server in the DMZ (see Figure 4: H.323 connections to Scopia PathFinder Server on page 12).

Important:

There must be no firewall between the H.323 endpoint (device) and the Scopia PathFinder Client.

An H.323 endpoint in the public network can also directly dial the Scopia PathFinder Server using direct port access (ports 4000-5000).

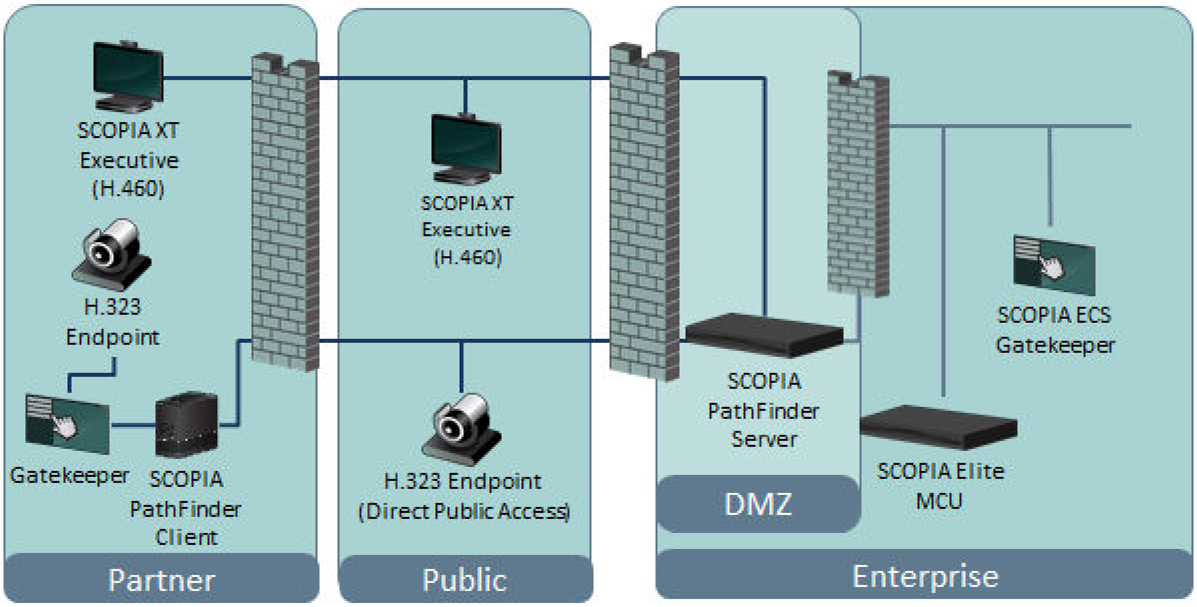


Figure 4: H.323 connections to Scopia PathFinder Server

When opening ports to and from Scopia PathFinder Server, use the following as a reference:

- If opening ports that are both to and from the Scopia PathFinder Server, see Table 2: Bidirectional Ports to Open the Scopia PathFinder Server on page 13.
- If opening ports that are both to and from the Scopia PathFinder Client, see Table 3: Bidirectional Ports to Open on the Scopia PathFinder Client on page 15.

Important:

In order for an H.323 endpoint (or other H.323 device) within the enterprise to successfully connect to the Scopia PathFinder Server in the DMZ via the enterprise firewall (see Figure 5: Contacting Scopia PathFinder Server from within the enterprise on page 13), you must do one of the following:

- Install a Scopia PathFinder Client within the enterprise
- Use H.460-enabled endpoints
- Open the internal firewall to the Scopia PathFinder Server (1024-65535, bidirectional)

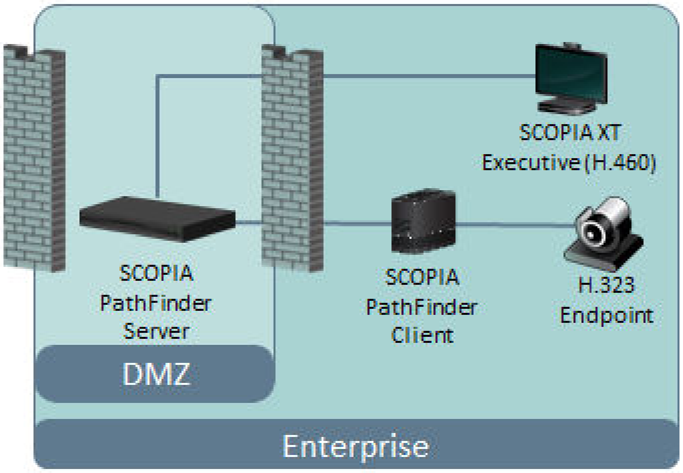


Figure 5: Contacting Scopia PathFinder Server from within the enterprise

Important:

The specific firewalls you need to open ports on depends on where your Scopia PathFinder Server, Scopia PathFinder Client, and other Scopia Solution products are deployed.

Table 2: Bidirectional Ports to Open the Scopia PathFinder Server

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
22	SSH/SFTP (TCP)	SSH client endpoint	Enables initial configuration, log download and server upgrade	Cannot initialize the server, download logs and upgrade the server	Mandatory for configuring the Scopia PathFinder Server
53	DNS (UDP)	DNS server	Enables querying the DNS for domains per call	Cannot support domain name calls and dialing by URI	Mandatory if using URI dialing
1719	UDP	H.460.18 endpoint/ H.460.18 client gatekeeper	Enables H.460.18 RAS capabilities	H.460.18 endpoints cannot register through Scopia PathFinder Server, firewall traversal function based on H.460.18 and H.460.19 cannot function.	Mandatory for H.460 endpoints To configure, see Configuring the UDP Port for RAS on the Scopia PathFinder Server on page 35
1720	TCP	Any H.323 device using Q.931 signaling in DPA mode	Enables IP call signaling	No signaling capabilities: guest users cannot dial into internal endpoints	Mandatory if in DPA mode

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
2776	TCP, UDP	H.460.18 endpoint/ H.460.18 client gatekeeper	Enables H.460.18 Call Signaling, H.460.19 Multiplex Media Channel	H.460.18 endpoints cannot register through Scopia PathFinder Server or set up logical channels. Firewall traversal function based on H.460.18 and H.460.19 cannot function.	Mandatory for H.460 endpoints
2777	TCP, UDP	H.460.18 endpoint/ H.460.18 client gatekeeper	Enables H.460.18 and H.460.19 Call Control, H.460.19 Multiplex Media Control Channel	H.460.18 endpoints cannot set up Call Control channels or logical channels. Firewall traversal function based on H.460.18 and H.460.19 cannot function.	Mandatory for H.460 endpoints
3089	TCP, UDP	Scopia PathFinder Client	Enables signaling and media traversal	If the TCP port is blocked, Scopia PathFinder Client cannot connect to Scopia PathFinder Server. Legacy H.323 endpoints behind the Scopia PathFinder Client cannot call external endpoints. If the UDP port is blocked, Scopia PathFinder Client can only traverse media via TCP.	Mandatory if using Scopia PathFinder Client
3089	TCP, UDP	Scopia PathFinder Server	Enables signaling and media connection to neighbor server	Cannot connect or traverse media to neighbor server	Mandatory if using a neighbor server
4000-5000	TCP, UDP	Any H.323 device using Q.931 signaling in DPA mode	Enables Direct Public Access (DPA) for H.323 call signaling, control and media traversal	Cannot setup/ connect DPA mode calls	Mandatory if in DPA mode To limit range, see Limiting the TCP/UDP Port Range for H.323 Direct Access Calls on the Scopia PathFinder Server on page 35

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
8080	HTTP (TCP)	Web client/ browser	Provides access to the web user interface	Cannot configure Scopia PathFinder Server	Mandatory for configuring the Scopia PathFinder application
8089	XML (TCP)	XML API Client	Enables managing Scopia PathFinder Server via XML API	The External Management System cannot get Scopia PathFinder Server status or receive traps from Scopia PathFinder Server	Optional

Table 3: Bidirectional Ports to Open on the Scopia PathFinder Client

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
3478	STUN (UDP)	STUN server	Enables an endpoint located in the remote network to send a STUN Binding Request when connecting to another endpoint in the same network	Scopia PathFinder Client cannot determine its public IP address. Smart Direct Media Connect cannot function.	Recommended

❗ **Important:**

If there is a firewall between the H.323 client and the Scopia PathFinder Client, all high ports must be opened in both directions (1024-65535). We therefore recommend no firewall between the endpoint and the Scopia PathFinder Client.

Checking Site Suitability

Prior to setting up your device, you need to verify your site suitability for:

- System power requirements
- System environmental requirements
- The device physical dimensions.

For more information, see Technical Specifications on page 7 to learn about these requirements. Ensure the site conforms to the listed requirements.

Unpacking the Device

About this task

We strongly recommend that you follow safety guidelines described in this section during unpacking.

Procedure

1. Inspect the shipping box to verify that it is not seriously damaged during shipping.
2. Place the shipping box on a horizontal surface paying attention to the This Side Up symbol on the shipping box. See Figure 6: This Side Up symbol on page 16.

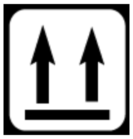
   

   Figure 6: This Side Up symbol

   ⚠ **Caution:**

   The accessories kit is situated on top of the device inside the shipping box and can be damaged if the box is placed upside down. Pay attention to the This Side Up symbol on the shipping box to handle the box correctly at all times.

   ⚠ **Caution:**

   To prevent injury and equipment damage, follow lifting guidelines described in the Safety Guide when lifting or moving the shipping box.
3. Cut the plastic straps.

   ⚠ **Caution:**

   The plastic straps are tightly stretched and can hit you when you cut them. To avoid this, make sure you do not face the side of the box secured by the straps before you cut the straps.
4. Cut the strapping tape.
5. Open the shipping box.
6. Take the accessories kit out of the shipping box.
7. Take the device out of the shipping box.
8. Carefully open the additional boxes, remove the packing material, and remove the drives and other contents.

Important:

We recommend that you keep the packaging materials in case you need to repack the device.

9. After opening the shipping box, check the shipment is complete. Compare the contents of the shipment with your packing list.

Inspecting for Damage

After you verify that all of the equipment is included, carefully examine the power supplies and cables for any damage resulting from shipping. If you suspect any damage from shipping, contact your local freight carrier for procedures on damage claims. If you observe any physical defects in the items you ordered, contact Technical Support for Return Material Authorization (RMA) form.

Important:

Before proceeding with the installation, verify that all of the ordered parts are present and in good condition. Keep a record of the parts and serial numbers. If any parts are missing or damaged, contact your sales representative.

Chapter 3 | Setting up the Scopia PathFinder Server

Mount the device onto a 19” square-hole rack. Use a shelf to support the device in the rack (Figure 7: Shelf mounted Scopia PathFinder Server on page 18).

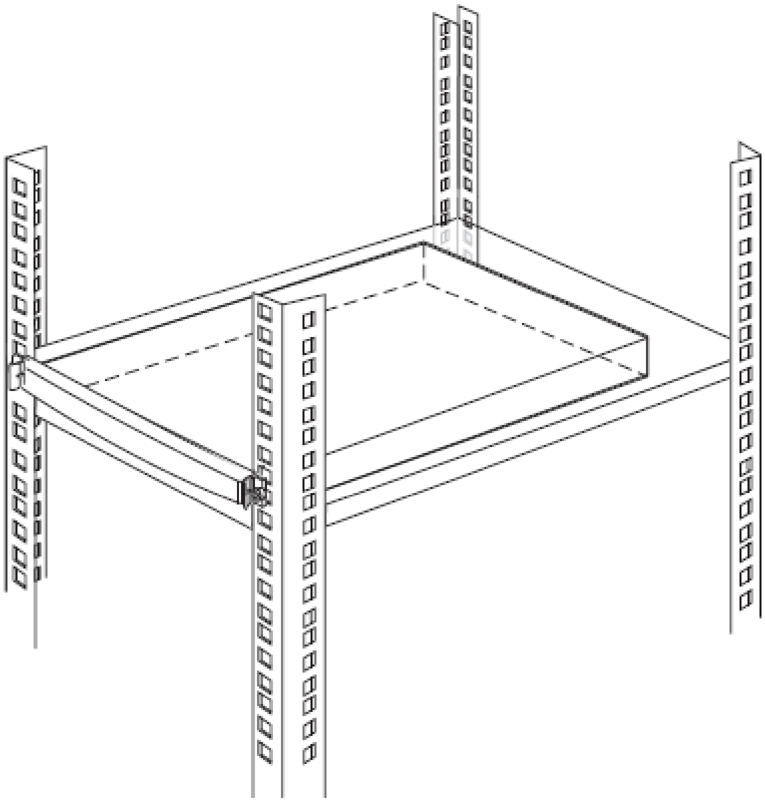


Figure 7: Shelf mounted Scopia PathFinder Server

These sections describe how to set up the device:

Navigation

- Verifying Rack Suitability on page 18
- Mounting the Scopia PathFinder Server onto the Rack Using a Shelf on page 20
- Connecting Cables to the Device on page 27
- Obtaining the License Key of the Scopia PathFinder Server on page 28
- Verifying the Scopia PathFinder Server Installation on page 29

Verifying Rack Suitability

There are some critical requirements that you must meet when choosing a rack and before mounting the device into it.

Navigation

- Choosing the Type of Rack on page 19
- Making Space for the Scopia PathFinder Server on page 19

Choosing the Type of Rack

There are many types of racks on the market. The installation instructions in this guide are intended for a 19” rack.

- Verify that the 19” rack meets the EIA-310 standards. This standard includes precise definitions of the shape of the holes, their size, the depth of the rack and other features. For more information on the EIA-310 standard, see http://electronics.ihs.com/collections/eia/index.htm
- Notice that the vertical square holes on the rack posts are not spaced equally. They form a repeating pattern of two holes close together, then one hole separate, then two holes close together and so on. See Figure 8: Hole distribution on 19” rack on page 19.

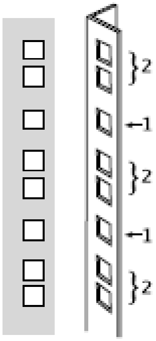


Figure 8: Hole distribution on 19” rack

Making Space for the Scopia PathFinder Server

When checking for an empty space to setup the device, be aware of its physical dimensions.

- Install the device in an open rack whenever possible. If installation in an enclosed rack is unavoidable, ensure that the rack has adequate ventilation.
- Avoid placing the device in an overly congested rack or directly next to another equipment rack. Otherwise, the heated exhaust air from other equipment can enter the inlet air vents and cause the device to overheat.
- Maintain a minimum clearance of 3 inches (7.62 cm) on the left and right of the device for the cooling air inlet and exhaust vents.
- Find a space on the rack which is at least 7 empty square holes in height on the rack posts.

  The Scopia PathFinder Server takes up 3 holes (1U) on the posts. You need at least 2 additional holes to slide the device into the rack.

  See Figure 9: Height of the Scopia PathFinder Server in the rack on page 20.

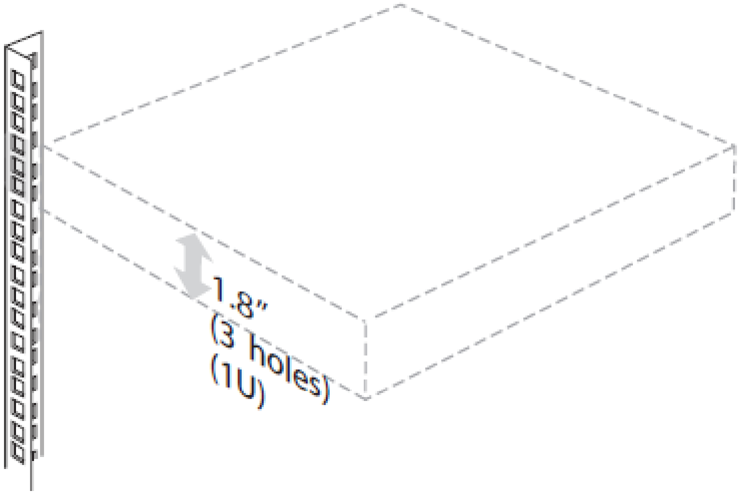


Figure 9: Height of the Scopia PathFinder Server in the rack

- To mount the Scopia PathFinder Server between two posts, the width between the inner sides of the two posts must be at least 17.7 inches (45 cm). See Figure 10: Width between inner sides of posts on page 20.

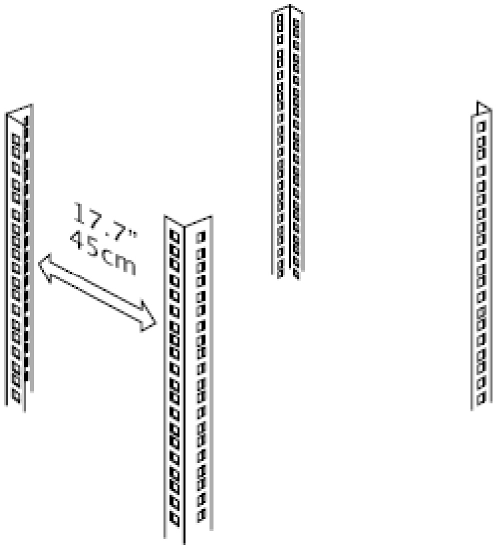


Figure 10: Width between inner sides of posts

Mounting the Scopia PathFinder Server onto the Rack Using a Shelf

This section describes how to mount the unit on to your rack:

Navigation

- Locating a Shelf in the Rack on page 21

- Checking the Accessories Required for Mounting on page 22
- Attaching Brackets to the Scopia PathFinder Server on page 23
- Marking the Location of the Device-fixing Cage Nuts on page 24
- Removing the Cage Nut Screws on page 25
- Mounting the Device-fixing Cage Nuts on page 26
- Mounting the Scopia PathFinder Server onto the Shelf on page 26

Locating a Shelf in the Rack

About this task

Before choosing a shelf that will support the device, follow this procedure.

Procedure

1. Read Verifying Rack Suitability on page 18, which contains important positioning and spacing information.
2. Prepare masking tape or a felt-tip pen to mark the location of the device-fixing cage nuts. If the holes on the rack are marked with numbers, write down the numbers on a piece of paper.
3. If you choose to mount the shelf, see the manufacturer’s guidelines for mounting a shelf.

   When looking for a location on the rack (see Locating a Shelf in the Rack on page 21):

   - Choose a shelf on a rack with at least 1.73 inches (4.4 cm) of empty space above.
   - Verify that the shelf you want to use is properly mounted and secured.
   - Verify that the shelf can support the device weight. See Technical Specifications on page 7.
   - Verify a hole is present 0.75 inches (2 cm) above the shelf (measured from the center of the hole).

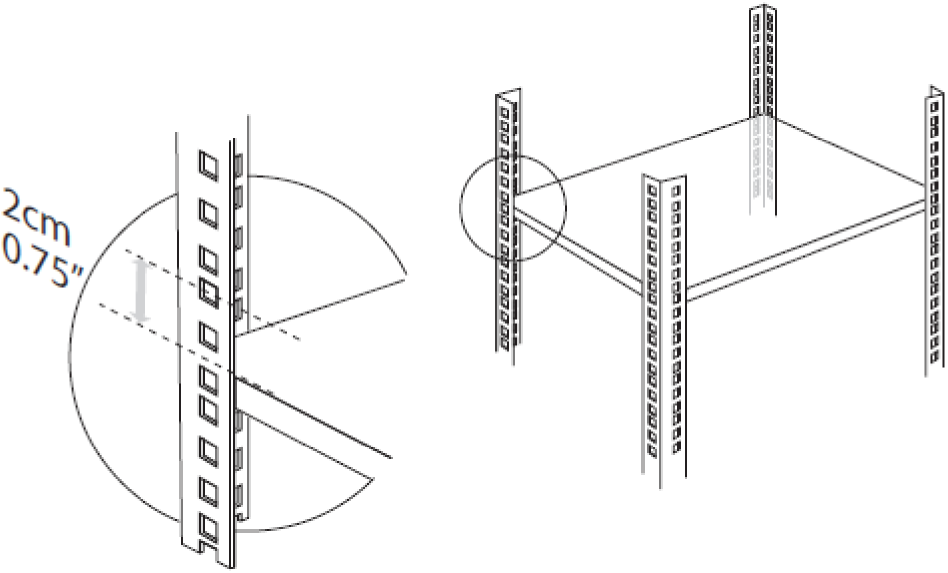


Figure 11: Checking the location of the shelf in the rack

4. Ensure the shelf is positioned horizontally in the rack.

5. Ensure the rack breaks are locked or the rack is stabilized.

Checking the Accessories Required for Mounting

Check you have the accessories necessary for mounting the device (see Figure 12: Accessories required for mounting on page 23):

- 2 mounting brackets (left and right)
- 2 cage nuts (M6) each with its hexagon socket cap screw (M6x10, DIN 7984), not included.
- 4 Phillips screws already mounted on the device.

Important:

Make sure you have a ruler, an Allen wrench (4 mm diameter), and a screwdriver (Nr. 1 tip) ready to hand before you start the setup.

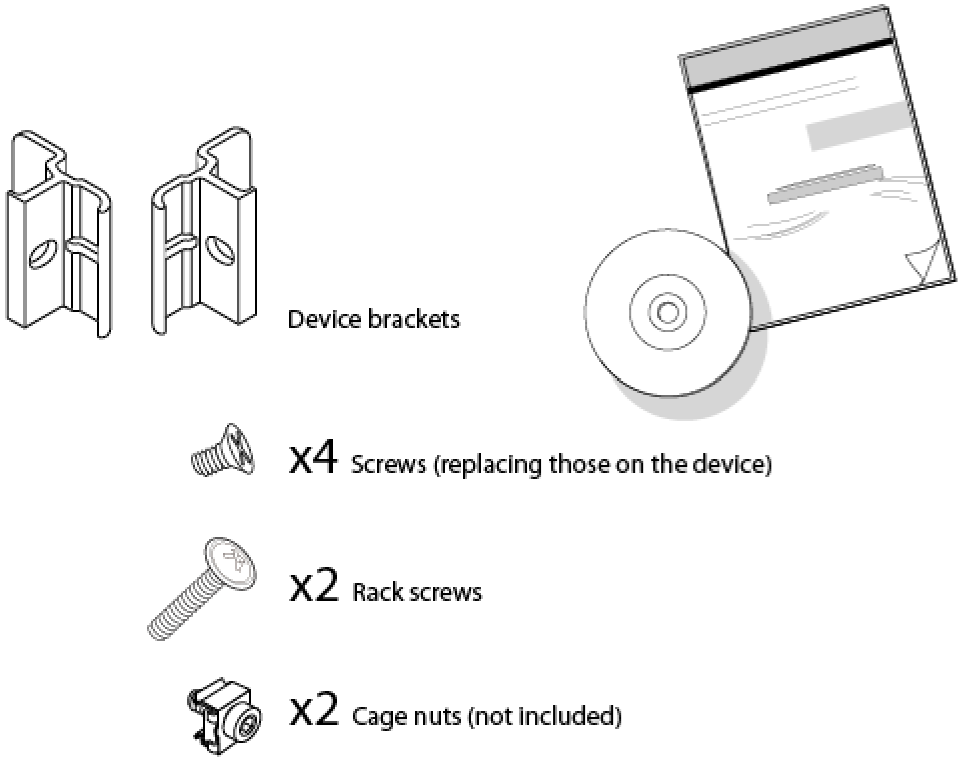

Device brackets
x4 Screws (replacing those on the device)
x2 Rack screws
x2 Cage nuts (not included)

Figure 12: Accessories required for mounting

Attaching Brackets to the Scopia PathFinder Server

About this task

The brackets serve to secure the device to the rack's front posts.

Procedure

1. Position the device on a flat, horizontal surface. Make sure the device front panel faces toward you.
2. Unscrew the two Phillips screws on either side of the device. See Figure 13: Removing the Phillips screws on the side panel on page 24.

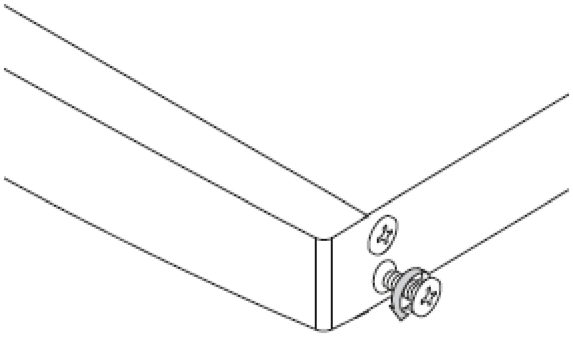


Figure 13: Removing the Phillips screws on the side panel

3. Attach the brackets on each side of the device side panel with the Phillips screws. See Figure 14: Aligning the bracket with the Scopia TIP GatewayScopia PathFinder Server front panel on page 24. Use the Phillips screws of the accessories kit, as they have the correct length and color.

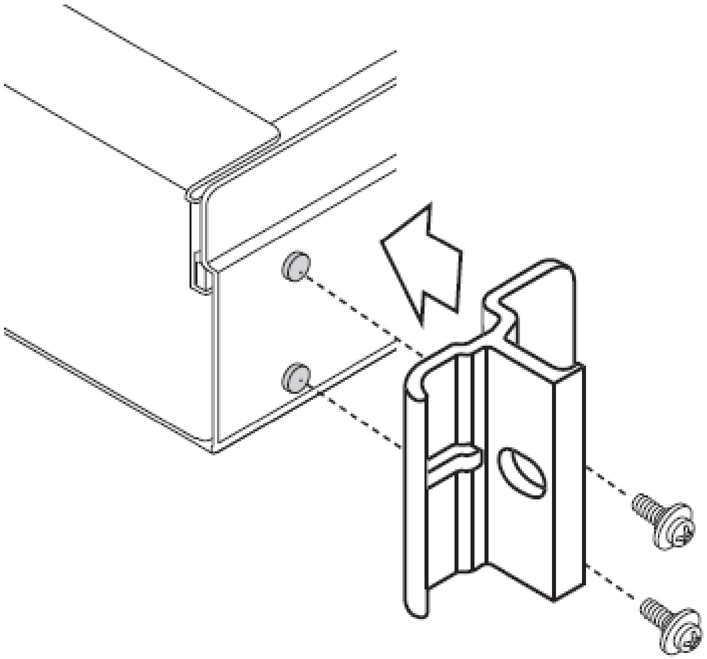


Figure 14: Aligning the bracket with the Scopia TIP GatewayScopia PathFinder Server front panel

Marking the Location of the Device-fixing Cage Nuts

About this task

There is a pair of cage nuts, one for each front-facing rack post. You need these cage nuts to fix the device brackets to the post.

Before attaching the cage nuts to the rack, mark where you plan to attach them, so you can be sure they are level and properly placed.

Procedure

1. From inside the front-facing rack post, mark the location of the device-fixing cage nut measured at 0.75 inches (2 cm) above the shelf. See Figure 15: Marking the location of the device-fixing cage nut on the rack on page 25.

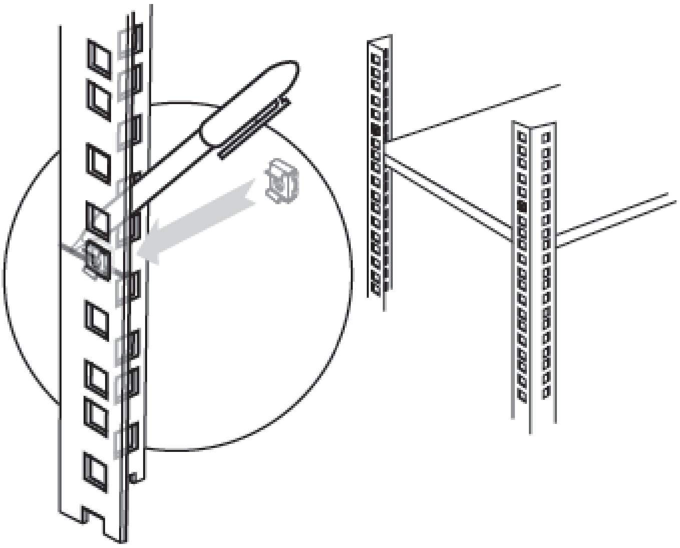


Figure 15: Marking the location of the device-fixing cage nut on the rack

2. Repeat this procedure for the other front-facing post.

Removing the Cage Nut Screws

About this task

The cage nuts are not included with this product, but are typically supplied with pre-mounted screws. Remove the screws and put them aside for later. See Figure 16: Removing the cage nut screw on page 26.

Figure 16: Removing the cage nut screw

Mounting the Device-fixing Cage Nuts

About this task

After you have marked the location of these cage nuts on the front-facing posts, you can mount them into the rack. Insert each cage nut on each of the posts where you have placed marks on the rack.

Procedure

1. Rotate the bottom cage nut so that its wings are on the top and bottom sides of the cage nut. See Figure 15: Marking the location of the device-fixing cage nut on the rack on page 25.
2. Compress the wings. From the back side of the post, insert first the wide wing, then the narrow wing into the marked square hole. Release the wings after the nut is in position.

Mounting the Scopia PathFinder Server onto the Shelf

About this task

After you have inserted the cage nuts onto the posts, you can mount the device onto the rack. Before mounting the device, read the Safety Guidelines described in the Safety Guide. Secure the device on the rack's posts to prevent it from moving around or falling.

⚠ **Caution:**

The device is heavy and we recommend that you ask someone to help you lift it.

Procedure

1. Lift the device.
2. Slide the device onto the shelf until the holes on the device's brackets align with the cage nuts you mounted previously. See Figure 17: Sliding the Scopia PathFinder Server onto the shelf on page 27.

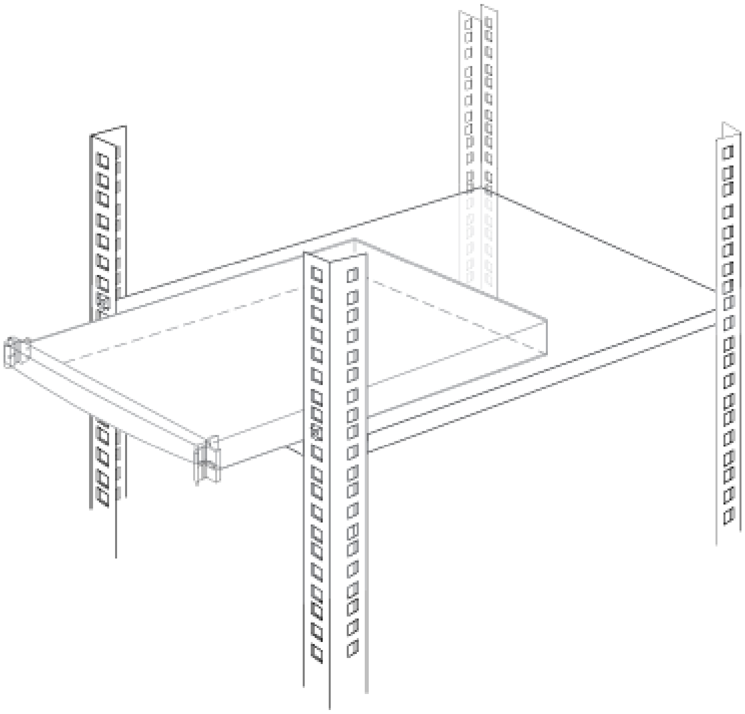


Figure 17: Sliding the Scopia PathFinder Server onto the shelf

3. Insert the two long rack screws provided with the product through the bracket holes into the cage nuts in the rack. Using the Allen wrench tighten the screws to secure the device to the front posts. See Figure 18: Securing the Scopia PathFinder Server to the rack on page 27.

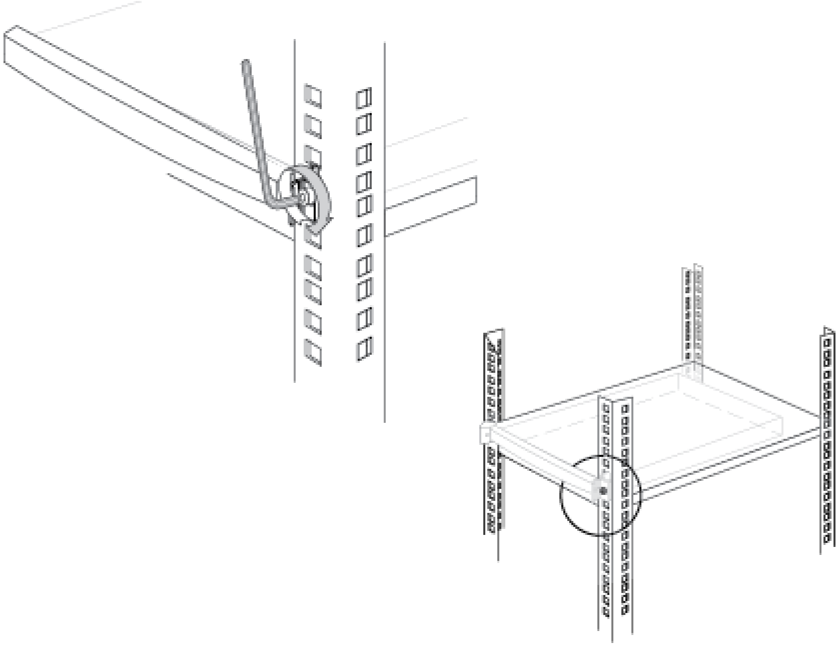


Figure 18: Securing the Scopia PathFinder Server to the rack

Connecting Cables to the Device

About this task

Follow the safety guidelines described in the Safety Guide during this procedure, and follow this procedure to connect the power, network, and serial cables supplied with the accessories kit.

Procedure

1. On the rear side of the device, connect the power cable to the AC power connector (see Figure 19: Rear panel of the device on page 28).

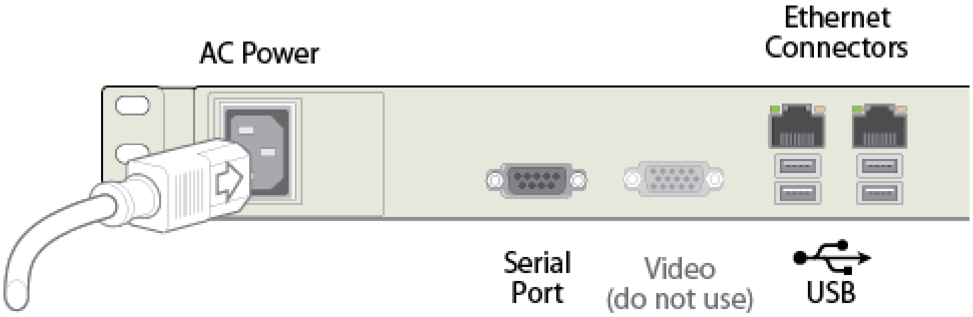


Figure 19: Rear panel of the device

2. Connect the other end of the power cable to the mains.
3. Connect a network cable to the left ethernet connector on the rear side of the device (see Figure 19: Rear panel of the device on page 28).

   Important:

   Use both ethernet connectors for dual-NIC deployments. A dual-NIC deployment raises security by using different subnets for media versus management. Use the left ethernet connector for management and the right connector for media.

4. Use a serial cable to connect a PC to the device's serial port. This connection is required for local configuration and maintenance.

   Important:

   Do not connect a screen or a keyboard to the device directly. Define the device's basic settings via the serial connection only.

Obtaining the License Key of the Scopia PathFinder Server

You need a license key for installing and operating the Scopia PathFinder Server. To obtain the license key, carefully read the instructions enclosed in the customer support letter you received when you purchased the product. Then navigate to http://licensing.radvision.com and fill in the required information.

Verifying the Scopia PathFinder Server Installation

About this task

After you installed the device and performed its initial configuration, you need to verify that it is installed and configured correctly.

Procedure

1. On the front panel, verify that the power LED is lit green.

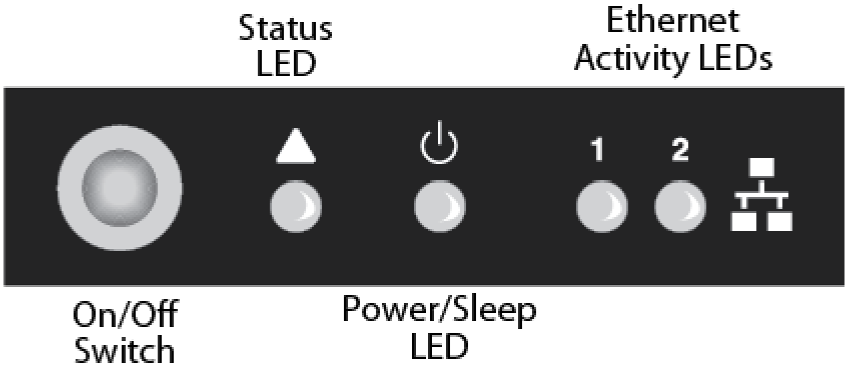


Figure 20: Locating the front panel LEDs

2. Verify that the status LED is lit green.
3. Check the network connection by verifying that the Ethernet activity LED is lit green.

Chapter 4 | Performing the Initial Configuration of the Scopia PathFinder Server

After connecting the system and powering it, perform the initial configuration of Scopia PathFinder Server as described in these sections:

Navigation

Configuring the IP Addresses of the Scopia PathFinder Server

About this task

There are two network cards (NICs) in the Scopia PathFinder Server to enable deploying it with better security and management of network traffic:

- NIC 1 (Ethernet port defined as eth0) always supports the external traffic.
- NIC 2 (Ethernet port defined as eth1) is always dedicated to the internal network traffic.

For a highly secure dual-NIC deployment we recommend to also configure the management role to eth1. This procedure describes how to configure this type of topology. Figure 21: The role of the dual-NIC Scopia PathFinder Server in a deployment on page 31 illustrates these roles.

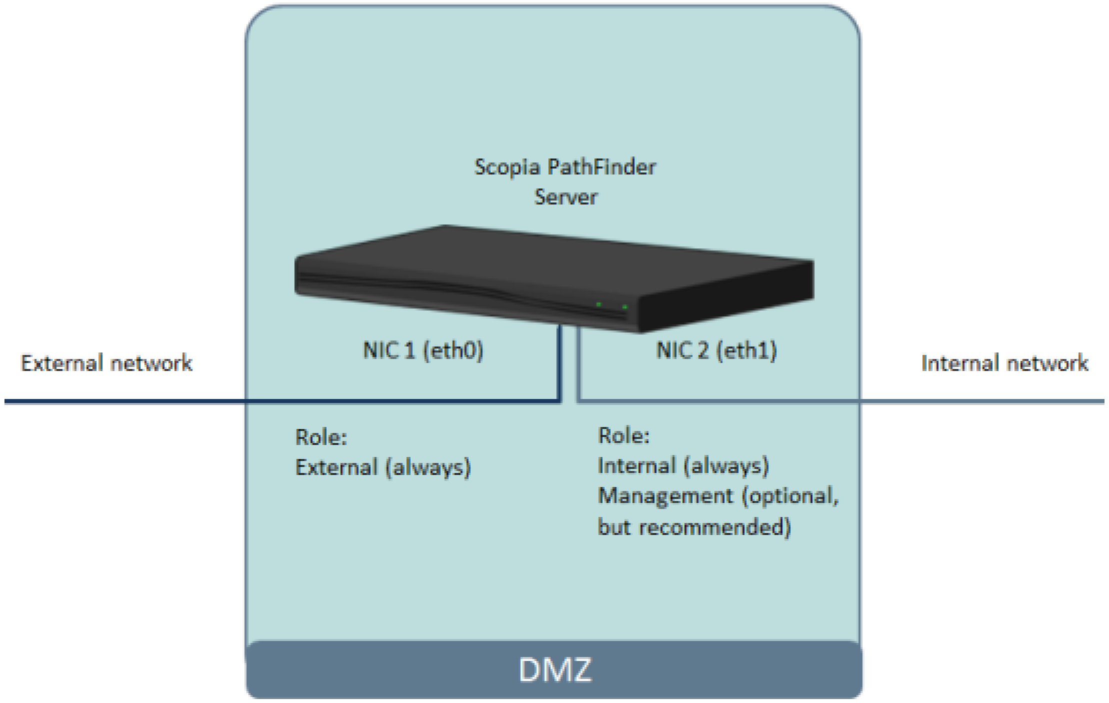


Figure 21: The role of the dual-NIC Scopia PathFinder Server in a deployment

Before you begin

Make sure you have these items:

- A PC with available serial port
- Serial cable provided with your Scopia PathFinder Server. Use the serial port on the server's rear panel to assign the new IP addresses.
- A client program to configure the administration console of your Scopia PathFinder Server using an SSH connection. We recommend using PuTTY. You can download this free application from **http://www.chiark.greenend.org.uk/~sgtatham/putty/**
- IP address of each NIC in the Scopia PathFinder Server
- Dedicated subnet mask for the Scopia PathFinder Server

  Important:

  In a dual-NIC deployment we strongly recommend connecting the NICs to two different subnets.
- IP address of the default router the Scopia PathFinder Server uses to communicate over the network
- IP address of the DNS server
- Fully Qualified Domain Name (FQDN) for the Scopia PathFinder Server

Procedure

1. Login to the administration shell menu of your Scopia PathFinder Server.

   a. Start PuTTY on your PC

   b. Select the **Serial** page in the **PuTTY Configuration** dialog box.

   c. Verify that the connection fields are setup as follows:

Field Name	Value
Serial line to connect to	**COM1**
Speed (baud)	**9600**
Data bits	**8**
Stop bits	**1**
Parity	**None**
Flow Control	**None**

d. Turn on the power to your Scopia PathFinder Server.

e. When prompted, enter a user name and password to login to Scopia PathFinder Server. The default user name and password are both **admin**.

2. Configure the NIC interfaces.

a. Once in the **Main Menu**, enter **2** to access the **Network administration menu**.

b. Enter **2** to access the **Change network configuration menu**

c. Enter **1** to configure eth0 (external NIC 1).

d. Enter the IP address of eth0 (NIC 1).

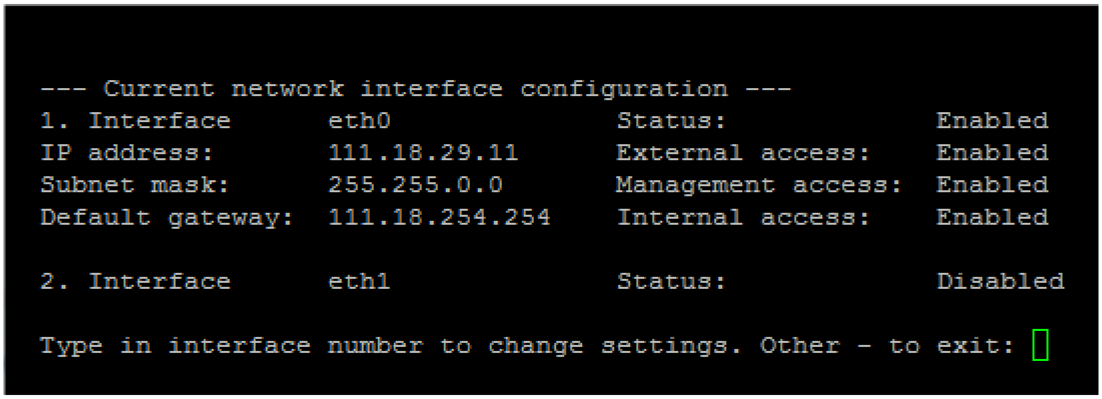
e. Enter the IP address of the subnet mask to which eth0 belongs.

f. Enter the IP address of the default gateway.

The window displays the new settings. The **External access**, **Management access**, and **Internal access** fields are automatically enabled.

External access is enabled so that the NIC can communicate with the external network. Traffic on the NIC typically comprises H.460, tunneling, DNS query traffic, and H.323.

Management access and internal access are automatically disabled after you enable these fields in eth1 (NIC 2).



```
--- Current network interface configuration ---
1. Interface       eth0              Status:             Enabled
IP address:        111.18.29.11      External access:    Enabled
Subnet mask:       255.255.0.0       Management access:  Enabled
Default gateway:   111.18.254.254    Internal access:    Enabled

2. Interface       eth1              Status:             Disabled

Type in interface number to change settings. Other - to exit:
```

Figure 22: Configuring NIC 0 (external NIC)

g. Enter **2** to configure eth1 (internal NIC 2).

h. Enter **y** in the **Interface status** to enable eth1.

i. Enter the IP address of eth1 (NIC 2).

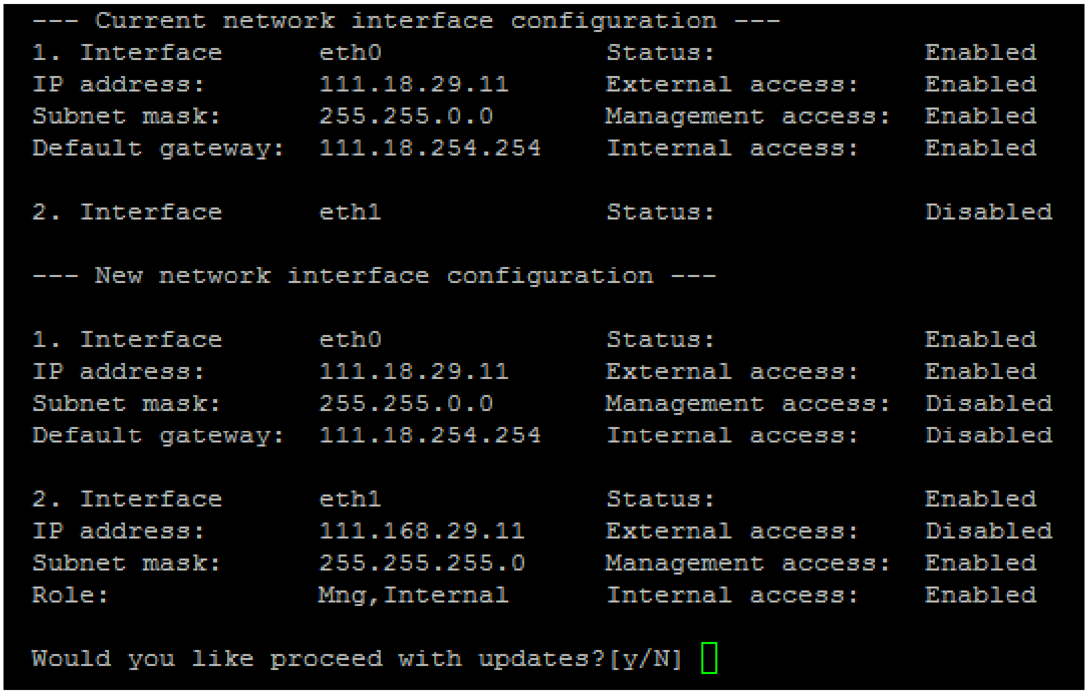
j. Enter the IP address of the subnet mask to which eth1 belongs.

k. Enter **y** to enable the **Management role** of eth1.

l. Enter **y** to enable the **Internal role** of eth1.

Field	Description
Internal access	Enable this field so that the NIC can handle standard H.323 traffic in the internal network.
Management access	Enable this field for the NIC's handling of management traffic such as: • HTTP, required for accessing the web user interface of Scopia PathFinder Server • SSH, required for accessing the shell administration menu of Scopia PathFinder Server • SFTP, for uploading or downloading resources of Scopia PathFinder Server • XML over TCP, required for third-party management interface.

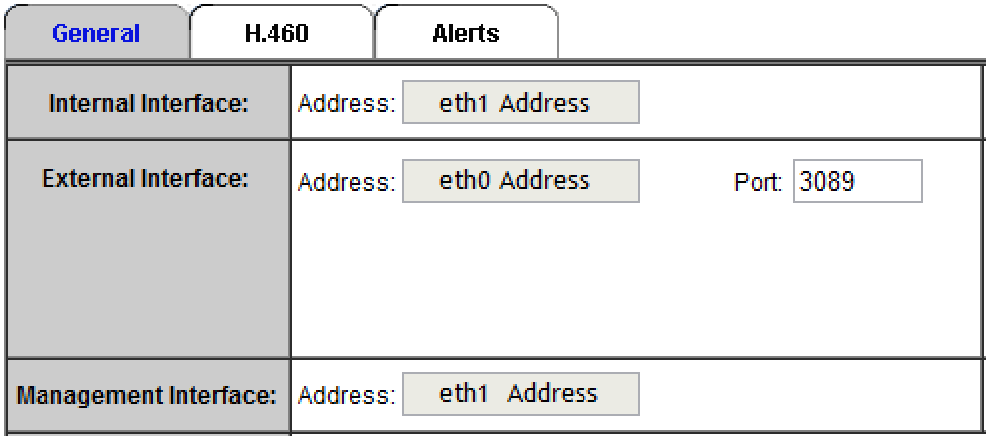
The system automatically disables the external role of eth1. The window displays the NIC configuration as illustrated in Figure 23: The network interface configuration screen (Intel server) on page 33.



```
--- Current network interface configuration ---
1. Interface      eth0                  Status:             Enabled
IP address:       111.18.29.11          External access:    Enabled
Subnet mask:      255.255.0.0           Management access:  Enabled
Default gateway:  111.18.254.254        Internal access:    Enabled

2. Interface      eth1                  Status:             Disabled

--- New network interface configuration ---

1. Interface      eth0                  Status:             Enabled
IP address:       111.18.29.11          External access:    Enabled
Subnet mask:      255.255.0.0           Management access:  Disabled
Default gateway:  111.18.254.254        Internal access:    Disabled

2. Interface      eth1                  Status:             Enabled
IP address:       111.168.29.11         External access:    Disabled
Subnet mask:      255.255.255.0         Management access:  Enabled
Role:             Mng,Internal          Internal access:    Enabled

Would you like proceed with updates?[y/N]
```

Figure 23: The network interface configuration screen (Intel server)

The configuration automatically sets the IP addresses of the NICs in the web interface of the Scopia PathFinder Server. To view this page, login to the web interface and navigate to **Settings > General** (Figure 24: The page displaying the NIC IP addresses in the Settings tab on page 34).



Internal Interface:	Address: eth1 Address	
External Interface:	Address: eth0 Address	Port: 3089
Management Interface:	Address: eth1 Address	

Figure 24: The page displaying the NIC IP addresses in the Settings tab

3. Configure the DNS server as your enterprise DNS server.

   a. In the **Network administration** menu enter **3** to access the DNS configuration menu.

   b. Enter **A** to add a DNS server.

   c. Enter the IP address of the new server.

4. Configure the new FQDN.

   a. In the **Network administration menu**, enter **4** to access the FQDN configuration menu.

   b. Enter the FQDN of the Scopia PathFinder Server. The system displays the host name and domain name, as well as the new FQDN of the Scopia PathFinder Server.

5. Add a static route to define call paths so that they are redirected from the Scopia PathFinder Server to Scopia ECS Gatekeeper and internal endpoints on other subnets.

   A static route is required if the internal network has many subnets. For example:

   - If the internal NIC is in network 168.168.1.10, and all internal endpoints and the Scopia ECS Gatekeeper are also located in network 192.168.1.0, there is no need for a static route.
   - If the internal network has many subnets (such as 168.168.2.0, 172.16.0.0), you need to configure the static route so that the Scopia PathFinder Server can communicate with devices inside subnets other than 168.168.1.0.

   a. In the **Network administration** menu enter **6** to access the static route configuration menu.

   b. Enter **A** to add a new static route.

   c. Enter the routing rule in this format:

   <host_ip|network_ip/prefix> via <gateway>>

6. Close the SSH session.

Configuring Ports on the Scopia PathFinder Server

This section provides instructions of how to configure the following ports and port ranges on the Scopia PathFinder Server:

Navigation

- Configuring the UDP Port for RAS on the Scopia PathFinder Server on page 35
- Limiting the TCP/UDP Port Range for H.323 Direct Access Calls on the Scopia PathFinder Server on page 35

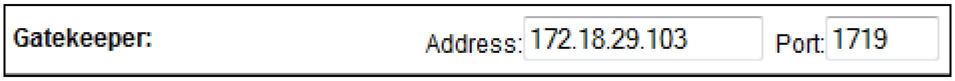
Configuring the UDP Port for RAS on the Scopia PathFinder Server

About this task

The Scopia PathFinder Server has designated port 1719 for RAS (communication with the gatekeeper). You can configure a different port for RAS (if, for example, port 1719 is busy).

Procedure

1. Access the Scopia PathFinder Server Administrator web interface.
2. Log in to the Scopia PathFinder web user interface.
3. Select **Settings > General**.
4. Locate the Gatekeeper area (see Figure 25: Gatekeeper Settings on page 35).



Gatekeeper: Address: 172.18.29.103 Port: 1719

Figure 25: Gatekeeper Settings

5. Modify the port range in the **Port** field.
6. Select **Save**.

Limiting the TCP/UDP Port Range for H.323 Direct Access Calls on the Scopia PathFinder Server

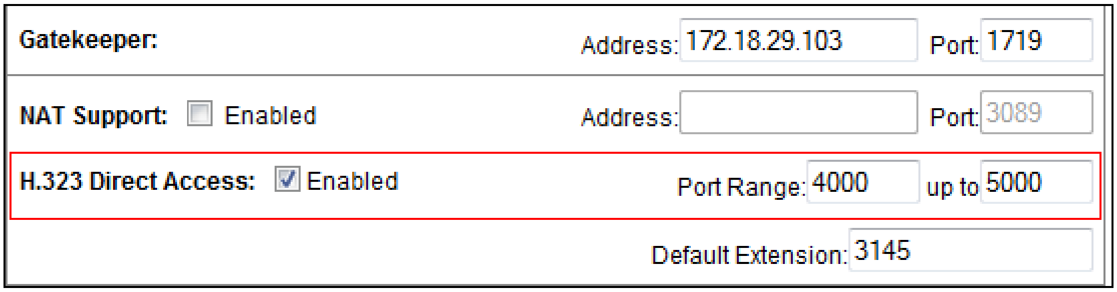
About this task

The Scopia PathFinder Server has designated ports 4000-5000 for H.323 Direct Public Access (DPA), which allows non-H.460 public endpoints to call internal endpoints without being registered to the Scopia PathFinder Server. To provide additional security for your firewall, you can limit this range.

To calculate approximately how many ports the Scopia PathFinder Server uses, multiply the number of simultaneous DPA calls by 10. The multiplication factor is lower for audio-only calls and higher for calls with dual video. We recommend using 10 as an approximation.

Procedure

1. Access the Scopia PathFinder Server Administrator web interface.
2. Select **Settings > General**.
3. Enable H.323 Direct Access by selecting the checkbox next to **H.323 Direct Access** (Figure 26: H.323 Direct Access Settings on page 36).



Gatekeeper: Address: 172.18.29.103 Port: 1719

NAT Support: □ Enabled Address: Port: 3089

H.323 Direct Access: ☑ Enabled Port Range: 4000 up to 5000

Default Extension: 3145

Figure 26: H.323 Direct Access Settings

4. Modify the port range in the **Port Range** fields.
5. Select **Save**.

Integrating the Scopia PathFinder Server with Other Scopia Solution Components

Your Scopia PathFinder Server is part of the Scopia Solution and must be integrated with other components:

Navigation

- Integrating the Scopia PathFinder Server with Scopia ECS Gatekeeper on page 36
- Integrating the Scopia PathFinder Server with NAT on page 37

Integrating the Scopia PathFinder Server with Scopia ECS Gatekeeper

About this task

The Scopia ECS Gatekeeper provides address resolution functionality in H.323 networks and also manages video traffic over IP networks. To allow endpoints from the external network to communicate with endpoints in the internal network, you need to configure the IP address of ECS in the Scopia

PathFinder Server. Endpoints participating in calls can be legacy H.323 and H.460 compliant. Calls can be dialed using IP addresses, URI dialing, and E.164 dialing.

URI dialing requires resolving a destination like name@company.com or number@company.com into the IP of an endpoint. This is performed by the gatekeeper. When the URI address refers to a destination in another network, it requires the Scopia PathFinder Server and the Scopia ECS Gatekeeper to work together.

Important:

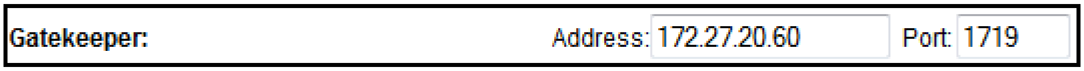
In the settings of the gatekeeper, add the IP address of the Scopia PathFinder Server at port 1719 as the gatekeeper's neighbor, as described in Enabling URI Dialing to External Endpoints on page 43.

Before you begin

Verify you have the IP address of the Scopia ECS Gatekeeper.

Procedure

1. Access the Scopia PathFinder Server Administrator web interface.
2. Select the **Settings** tab.
3. In the **General** tab navigate to the **Gatekeeper Address** field. See Figure 27: Integrating the Scopia PathFinder Server with Scopia ECS Gatekeeper on page 37.



Gatekeeper: Address: 172.27.20.60 Port: 1719

Figure 27: Integrating the Scopia PathFinder Server with Scopia ECS Gatekeeper

4. Enter the IP address of the Scopia ECS Gatekeeper.
5. If required, change the port number which is set to **1719** by default.

Integrating the Scopia PathFinder Server with NAT

About this task

Enable this functionality if the external NIC of the Scopia PathFinder Server uses a private IP address to communicate with endpoints outside the organization.

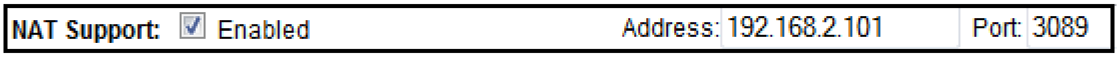
Do not enable NAT support if the server's external NIC communicates with the Internet by using a public IP address.

Before you begin

Verify you have the NAT IP address.

Procedure

1. Access the Scopia PathFinder Server Administrator web interface.
2. Select **Settings > General > NAT Support**.



NAT Support: ☑ Enabled Address: 192.168.2.101 Port: 3089

Figure 28: Configuring NAT support

3. Configure the **NAT** settings as follows:

Table 4: Configuring NAT support

Field	Description
NAT Support	Enable **NAT Support** if the external NIC of the Scopia PathFinder Server uses a private IP address to communicate with endpoints outside the organization. If deploying the PathFinder with a load balancer, you must enable **NAT Support**. For more information, see Configuring Scopia PathFinder Servers for the Load Balancer on page 59.
Address	Enter the public IP address of the NAT device in the **Address** field. **Important:** In the firewall/NAT device, verify that the NAT address is mapped to the private IP address of the Scopia PathFinder Server's external NIC.
Port	If required, change the Scopia PathFinder Client port number which is set to **3089** by default.

Configuring Port Access for H.460 Endpoints

About this task

The Scopia PathFinder Server acts as an H.460 server, enabling H.460 endpoints (which are H.460 clients) to register with the Scopia PathFinder Server.

It supports NAT/firewall traversal for endpoints compliant with the H.460.18/19 standard approved by ITU-T. H.460 is an extension of H.323 to enable endpoints to connect via a firewall, from outside the enterprise to an endpoint inside the enterprise via a Scopia PathFinder Server with NAT address.

For example, in Figure 29: H.460 endpoints register with Scopia PathFinder Server on page 39, an external H.460 endpoint in the internet can dial the E.164 number of an endpoint within the enterprise. The H.460 endpoint sends the call request to the Scopia PathFinder Server using destination port 1719.

The Scopia PathFinder Server then routes this request to the ECS. Once the endpoint gets its registration request accepted through port 1719, it opens two connections to the Scopia PathFinder Server using port 2776 (call signaling) and 2777 (call control) and the Scopia PathFinder Server in turn routes these requests to the ECS.

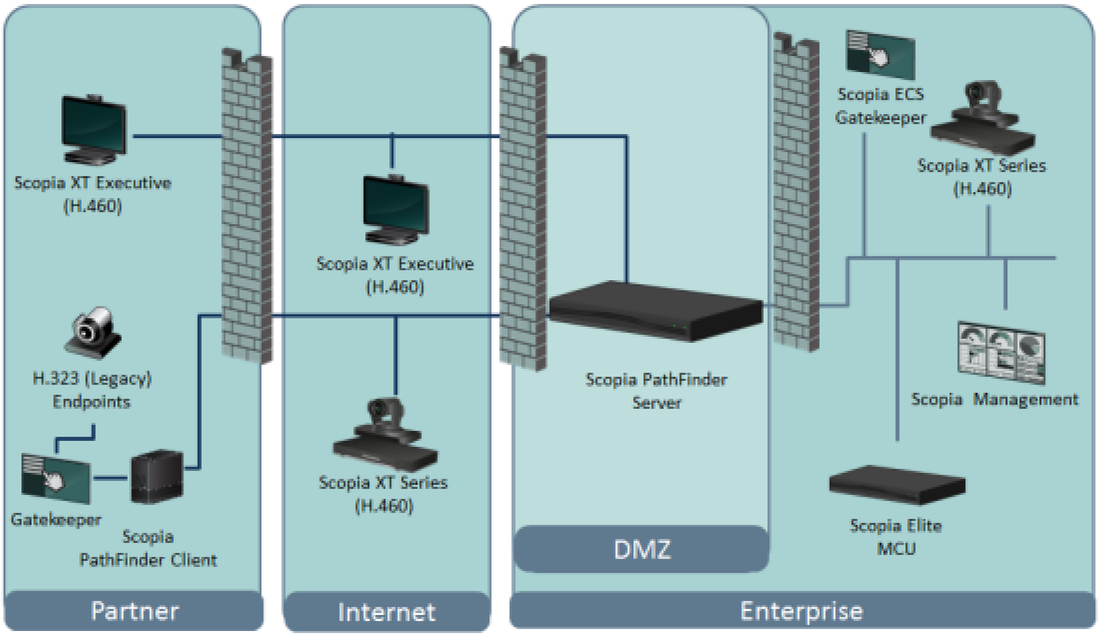


Figure 29: H.460 endpoints register with Scopia PathFinder Server

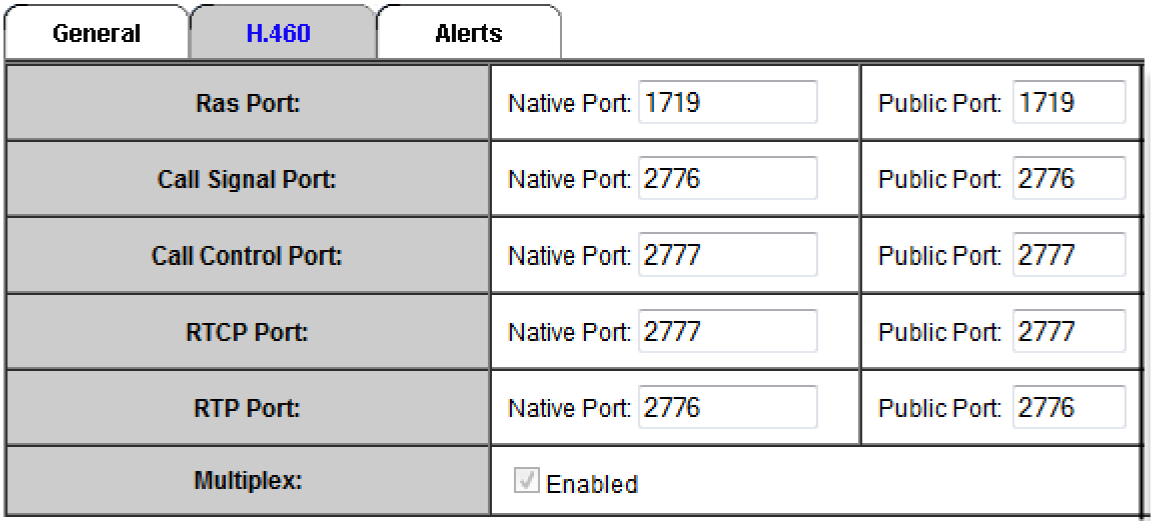
For more information on the firewall's port configuration see Ports to Open on Scopia PathFinder on page 11. The Scopia PathFinder Server ports are configured by default to support these calls. Follow this procedure to change the default configuration.

Procedure

1. Access the Scopia PathFinder Server Administrator web interface.
2. Select **Settings > H.460**. The window displays the default port values for H.460 endpoint port access.

   Carefully read this information before changing the default values:

   - If you leave these fields blank, the system does not change the port's origin value.
   - As these ports are unique, you cannot define more than one of these to the same port.
   - Both the native port and the public port face the external network. Native ports are those used on the Scopia PathFinder Server. Public ports are ports opened on the NAT/firewall. Public ports must match those configured on your external firewall/NAT.
   - It is not recommended to change the default value of the Ras port's public port to avoid changing the port value in all endpoints you use with your deployment.



Ras Port:	Native Port: 1719	Public Port: 1719
Call Signal Port:	Native Port: 2776	Public Port: 2776
Call Control Port:	Native Port: 2777	Public Port: 2777
RTCP Port:	Native Port: 2777	Public Port: 2777
RTP Port:	Native Port: 2776	Public Port: 2776
Multiplex:	☑ Enabled	

Figure 30: Configuring Scopia PathFinder Server for H.460 endpoint access

Field	Description
Ras Port	RAS (Registration, Admission, Status) is required for communication between the remote endpoint and the Scopia PathFinder Server. It allows the endpoint to request admission of the call.
Call Signal Port	Used for call setup, call proceeding, alerts, connection, call release upon completion.
Call Control Port	Provides control service to the multimedia session that has been established.
RTCP Port	Real-time Transmission Control Protocol provides statistics on the quality of the multimedia session in place.
RTP Port	Real-Time Transport Protocol port carries the media flow.
Multiplex	When enabled, reduces the number of required ports by sending media and control communications over RTP/RTCP via UDP ports 2776 and 2777. The **Multiplex** option is automatically enabled when you enable NAT support (see Integrating the Scopia PathFinder Server with NAT on page 37).

Enabling Endpoints in the Organization to Call External Endpoints

Internal endpoints call external endpoints using their IP or URI address. If the external endpoint is registered to the Scopia ECS Gatekeeper, it can also dial the endpoint's E.164 number. Since external endpoints are typically not registered to the gatekeeper, this requires the gatekeeper to work with the PathFinder Server to complete the call.

A gatekeeper routes audio and video H.323 calls by resolving dial strings (H.323 alias or URI) into the IP address of an endpoint, and handles the initial connection of calls.The Scopia ECS Gatekeeper provides address resolution functionality in H.323 networks and also manages video traffic over IP networks. When the destination address is located in another network, the gatekeeper forwards the request to the Scopia PathFinder Server to complete the call and resolve the destination.

You must configure both the Scopia PathFinder Server and the Scopia ECS Gatekeeper to support IP and URI dialing, as described in the following topics:

Navigation

- Configuring Access for H.323 Legacy Endpoints on page 41
- URI Dialing Functionality on page 42
- Enabling URI Dialing to External Endpoints on page 43
- Enabling IP Dialing to External Endpoints on page 47

Configuring Access for H.323 Legacy Endpoints

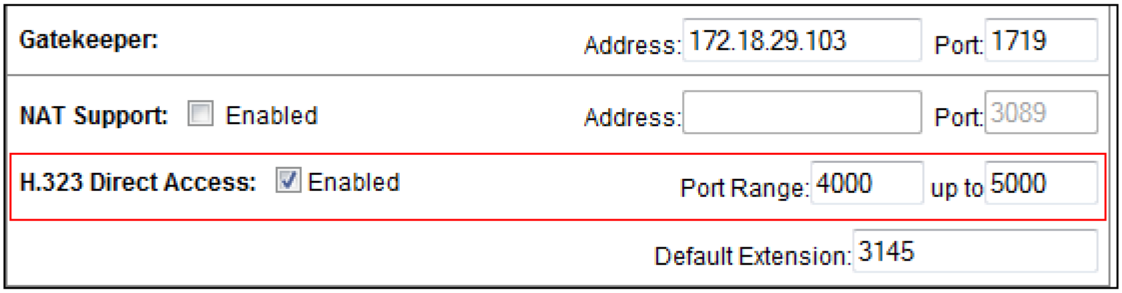
About this task

Direct Public Access enables opening a direct dial line to the Scopia PathFinder Server to call external H.323 legacy endpoints.

To set up this connection, you need to configure the Scopia PathFinder Server to accept H.323 calls and forward them. You also need to configure the Scopia ECS Gatekeeper to one or more Scopia PathFinder Servers to facilitate the routing of these calls. For more information on configuring the Scopia ECS Gatekeeper, see the *User Guide for Scopia ECS Gatekeeper*.

Procedure

1. Access the Scopia PathFinder Server Administrator web interface.
2. Select **Settings > General**.
3. Configure the following settings for Direct Public Access:



Gatekeeper: Address: 172.18.29.103 Port: 1719

NAT Support: □ Enabled Address: Port: 3089

H.323 Direct Access: ☑ Enabled Port Range: 4000 up to 5000

Default Extension: 3145

Figure 31: Configuring Access for H.323 Legacy Endpoints

Table 5: Configuring Access for H.323 Legacy Endpoints

Field	Description
H.323 Direct Access	Enable **H.323 Direct Access** to open a direct dial line to the Scopia PathFinder Server for H.323 endpoints that do not support the secure H.460 protocol.
Port Range	Define the range of ports used for direct H.323 calls in the field. ❗ **Important:** If the external NIC of the Scopia PathFinder Server is located behind a firewall, this range of port must also be opened in the firewall, as well as port 1720 for H.323 signaling.
Default Extension	Enter the default extension that you usually configure to the MCU IVR (Interactive Voice Response). Scopia PathFinder Server redirects a call to the default extension when the endpoint dials only the server's IP address without any extension.

4. Select **Save**.

URI Dialing Functionality

The Scopia Solution fully supports URI dialing, a dial format for contacting endpoints outside your organization.

URI is an address format used to locate a device on a network. An endpoint's URI consists of the endpoint's name or number, followed by the domain name of the server to which the endpoint is registered, such as the organization's Scopia PathFinder Server. For example, *<endpoint name>@<server_domain_name>*.

All Scopia Solution endpoints work transparently with URI dials, including the Scopia XT Series and Scopia Desktop Clients. You can also perform URI dials from the conference control of Scopia Management.

URI dialing is compatible with Scopia PathFinder and other third party firewall traversal systems. Dialing an endpoint from one organization to another requires first traversing your own firewall with Scopia PathFinder, out through the internet, and then into the firewall of the recipient’s organization using their firewall traversal system (Figure 32: URI dialing between two enterprises using Scopia PathFinder on page 43).

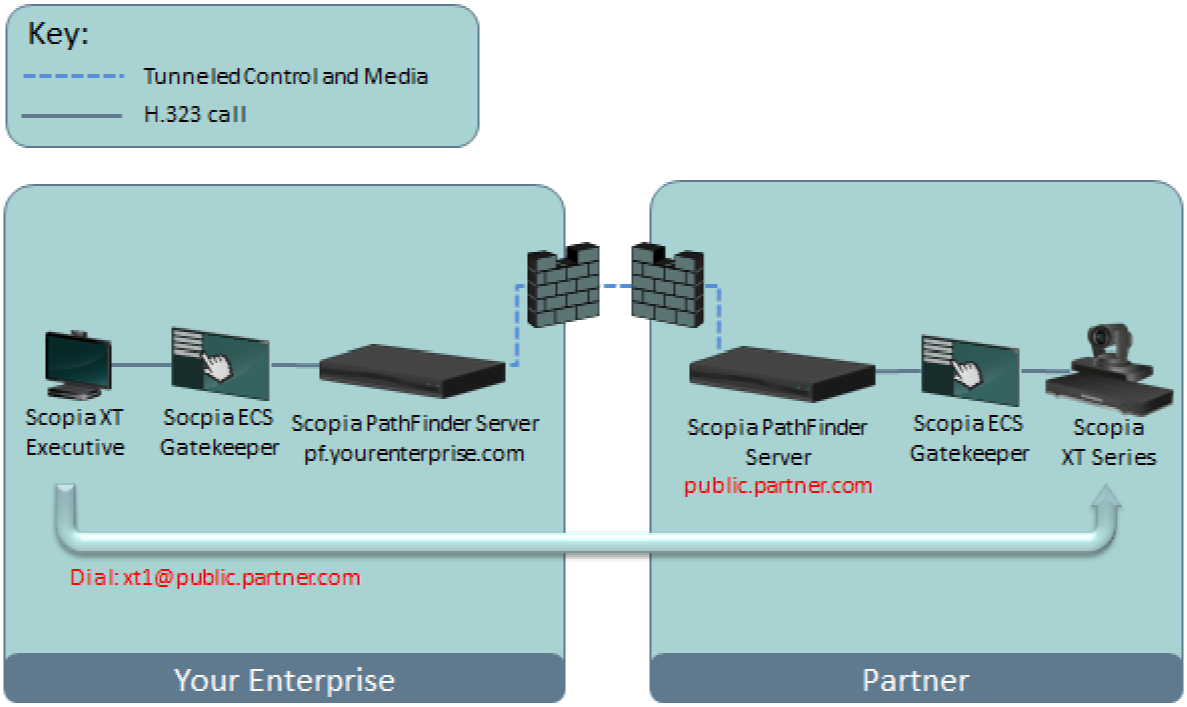


Figure 32: URI dialing between two enterprises using Scopia PathFinder

To access an endpoint in the other company, the URI's domain name is the second company's firewall traversal system, like the name of their Scopia PathFinder Server, or the organization's domain name. For example, in Figure 32: URI dialing between two enterprises using Scopia PathFinder on page 43, dialing to the partner company requires knowing the following:

- The name or number of the endpoint, in this example *xt1*
- The domain name of the PathFinder Server of that company, *public.partner.com* in this example, or the organization's domain name, *partner.com*.

Important:

As with regular web domain names, the name of the Scopia PathFinder Server resolves to an IP address via standard DNS lookup if it has been allocated a global DNS name. If the server's IP address does not have a DNS name, the URI dial should directly specify the server's IP address instead. For example, the URI *xt1@123.456.789.1* specifies the alias followed by the server's IP address.

To set up this connection, you need to configure the Scopia PathFinder Server to accept H.323 calls and forward them. You also need to configure the Scopia ECS Gatekeeper to define one or more Scopia PathFinder Servers as ECS's neighbor, to facilitate the routing of these calls.

Enabling URI Dialing to External Endpoints

About this task

A gatekeeper routes audio and video H.323 calls by resolving dial strings (H.323 alias or URI) into the IP address of an endpoint, and handles the initial connection of calls.The Scopia ECS Gatekeeper provides address resolution functionality in H.323 networks and also manages video traffic over IP networks.

You can call endpoints using their IP address, URI, or E.164 number. This procedure describes how to set the gatekeeper to forward URI calls from internal endpoints to external endpoints in another enterprise, via the Scopia PathFinder Server. Since external endpoints are not registered to the gatekeeper, this requires the gatekeeper to work with the PathFinder Server to complete the call.

URI is an address format used to locate a device on a network. An endpoint's URI consists of the endpoint's name or number, followed by the domain name of the server to which the endpoint is registered, such as the organization's Scopia PathFinder Server. For example, <*endpoint name*>@<*server_domain_name*>.

When the URI address refers to a destination in another network, the gatekeeper forwards the request to the Scopia PathFinder Server to complete the call and resolve the destination (Figure 33: URI dialing between two enterprises using Scopia PathFinder on page 44).

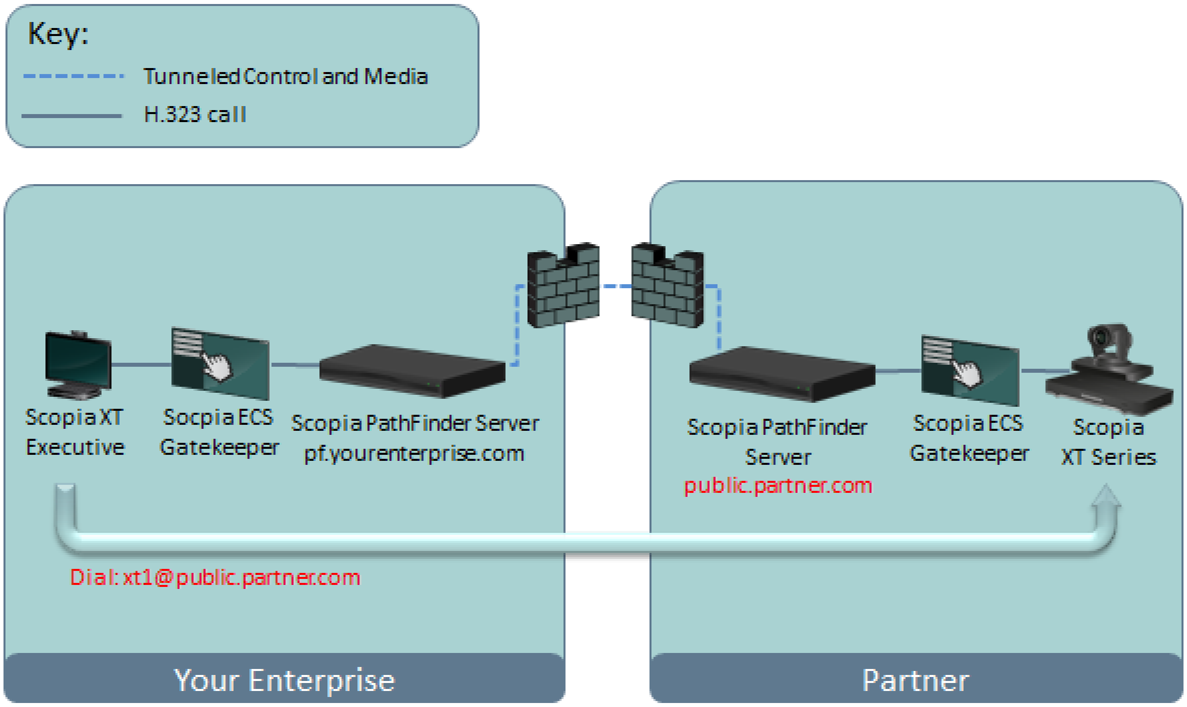


Figure 33: URI dialing between two enterprises using Scopia PathFinder

Endpoints participating in calls can be legacy H.323 and H.460 compliant.

You can also configure the gatekeeper to forward IP calls to the PathFinder Server, as described in Enabling IP Dialing to External Endpoints on page 47. For deployments with multiple PathFinder Servers, including several servers acting as one server behind a load balancer, perform this procedure for each server. For more information about configuring multiple PathFinder Servers behind a load balancer, see Scalability, High Availability and Load Balancing with Scopia PathFinder on page 52.

Before you begin

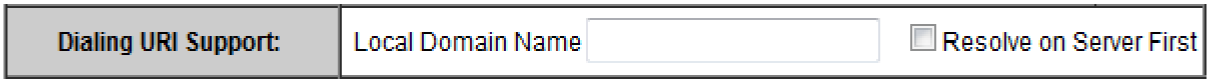
- Enable Direct Public access on the PathFinder Server, as described in Configuring Access for H.323 Legacy Endpoints on page 41. This allows internal endpoints to call external legacy H.323 endpoints that do not support H.460.

  If you are configuring multiple PathFinder Servers, with or without a load balancer, do this for each PathFinder Server.
- To allow endpoints from the external network to communicate with endpoints in the internal network, you need to configure the IP address of ECS in the Scopia PathFinder Server, as described in Integrating the Scopia PathFinder Server with Scopia ECS Gatekeeper on page 36.
- Verify you have the IP address of the Scopia PathFinder Server NIC connected to the internal network.

  If you are configuring multiple PathFinder Servers, with or without a load balancer, do this for each PathFinder Server.

Procedure

1. Access the Scopia PathFinder Server Administrator web interface.
2. Navigate to **Settings > General > Dialing URI Support**.



Dialing URI Support: Local Domain Name □ Resolve on Server First

Figure 34: Configuring URI dialing support

3. Configure the Scopia PathFinder Server to handle the domain name or IP address included in the URI dialing of inbound or outbound calls, as described below.

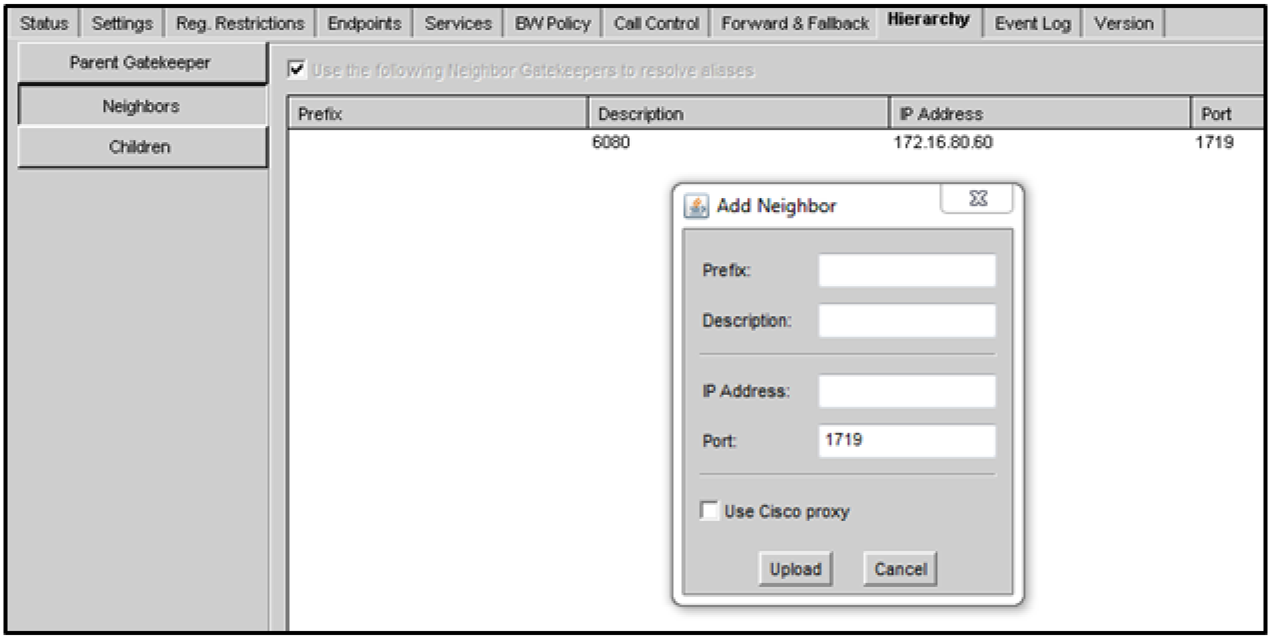
Table 6: Configuring URI support

Field	Description
Local Domain Name	Enter the domain name of the organization in which the Scopia PathFinder Server is physically located. This configuration enables the server to optimize the handling of calls when used with **Resolve on Server First**, described below.
Resolve on Server First	Select to strip the domain name/IP address from the dialed string before transferring the relevant message to its destination. **Important:** We recommend enabling this setting to optimize the handling of call transfer. Do not select this option if your organization has a policy of transferring a message to its destination by using the complete endpoint's dial string (for example, 1234@5.6.7.8) instead of its alias (1234 in this example).

4. Access the Scopia ECS Gatekeeper web interface.

If you are using Scopia Management's built-in gatekeeper, log in to the administrator portal of Scopia Management and access the link from the gatekeeper's page (for more information on accessing Scopia Management, see *Administrator Guide for Scopia Management*).

5. Select **Hierarchy > Neighbors**.



☑ Use the following Neighbor Gatekeepers to resolve aliases

Prefix	Description	IP Address	Port
	6080	172.16.80.60	1719

Prefix:

Description:

IP Address:

Port: 1719

☐ Use Cisco proxy

Figure 35: Configuring a Neighboring PathFinder Server for outgoing URI calls

6. Configure the PathFinder Server as a neighboring server to the Scopia ECS Gatekeeper to facilitate outgoing URI dialing, as described below.

   This is required since the external endpoint is not registered to the gatekeeper, and therefore it cannot resolve the address of the external endpoint. When an internal endpoint calls an external endpoint using its URI address, the gatekeeper sends the request to all devices configured as its neighbor, which may include other gatekeepers and PathFinder Servers, to check which one can resolve the address.

Table 7: Configuring a Neighboring Scopia PathFinder Server for outgoing URI calls

Field	Description
Add	Select to add the Scopia PathFinder Server.
Prefix	Leave this field empty since URI dialing does not route calls to zones using dial prefixes. URI dialing routes calls using the domain name in the URI string, which is resolved to any zone worldwide.
Description	Enter the name of your Scopia PathFinder Server.
IP Address	Enter the IP address of your Scopia PathFinder Server. This is the IP address of the internal NIC connected to the internal network.
Port	The default port value, **1719**, is mandatory for URI dialing.

7. Select **Upload**.
8. If your deployment includes multiple PathFinder Servers, including several servers acting as one server behind a load balancer, repeat the steps above for each PathFinder Server.

Enabling IP Dialing to External Endpoints

About this task

You can call endpoints using their IP address, URI, or E.164 number. This procedure describes how to set the gatekeeper to forward IP calls from internal endpoints to public endpoints, via the Scopia PathFinder Server. Since external endpoints are not registered to the gatekeeper, this requires the gatekeeper to work with the PathFinder Server to complete the call (Figure 37: IP call to an external endpoint on page 47).

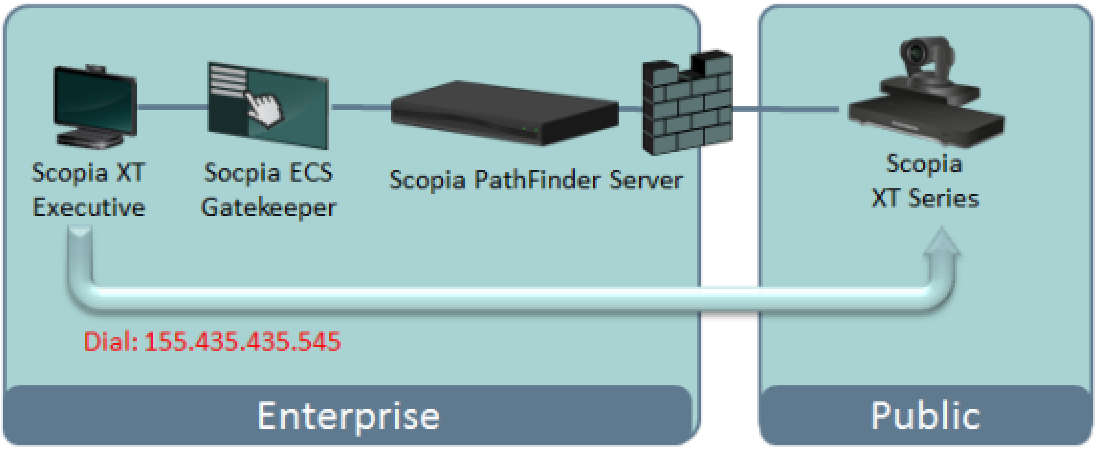


Figure 37: IP call to an external endpoint

You can also configure the gatekeeper to forward URI calls to the PathFinder Server, as described in Enabling Endpoints in the Organization to Call External Endpoints on page 40. For deployments with multiple PathFinder Servers, including several servers acting as one server behind a load balancer, perform this procedure for each server. For more information about configuring multiple PathFinder Servers behind a load balancer, see Scalability, High Availability and Load Balancing with Scopia PathFinder on page 52.

Before you begin

- Verify you have the IP address of the Scopia PathFinder Server NIC connected to the internal network.

  If you are configuring multiple PathFinder Servers, with or without a load balancer, do this for each PathFinder Server.
- Enable Direct Public access on the PathFinder Server, as described in Configuring Access for H.323 Legacy Endpoints on page 41. This allows internal endpoints to call external legacy H.323 endpoints that do not support H.460.

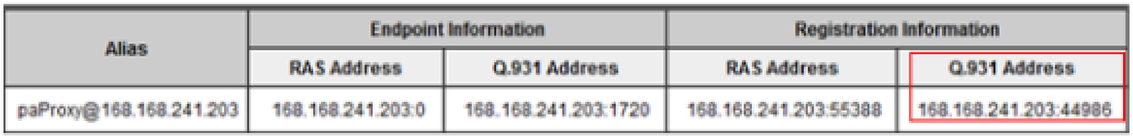
If you are configuring multiple PathFinder Servers, with or without a load balancer, do this for each PathFinder Server.

- Verify you have the Direct Public Access address of the PathFinder Server:

  If you are configuring multiple PathFinder Servers, with or without a load balancer, do this for each PathFinder Server.

  1. From the PathFinder Server web interface, select **Client Status > Client Name** that has the format *paProxy@<IP address>*. The PathFinder Server automatically created this proxy address when you enabled Direct Public Access.
  2. Note the address (IP address and port) under **Q.931 Address > Registration Information** (see Figure 36: Registration information required for configuring the ECS on page 48).

     You need this registration information to configure IP dialing.



Alias	Endpoint Information		Registration Information	
	RAS Address	Q.931 Address	RAS Address	Q.931 Address
paProxy@168.168.241.203	168.168.241.203:0	168.168.241.203:1720	168.168.241.203:55388	168.168.241.203:44986

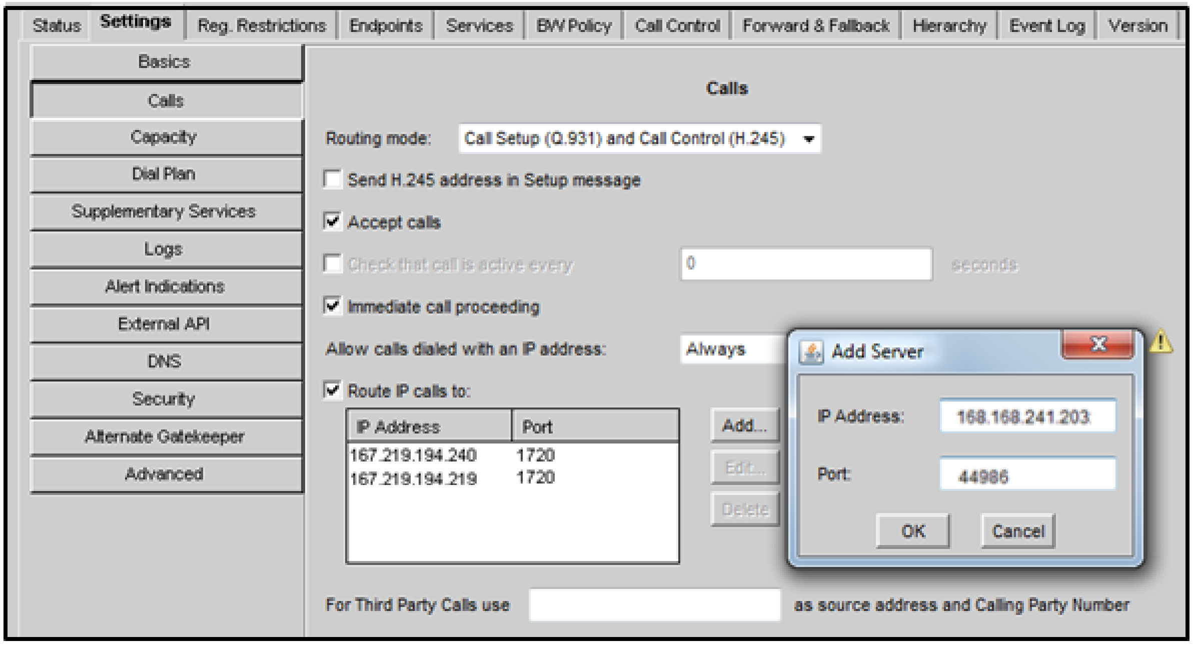
Figure 36: Registration information required for configuring the ECS

Procedure

1. Access the Scopia ECS Gatekeeper web interface.

   If you are using Scopia Management's built-in gatekeeper, log in to the administrator portal of Scopia Management and access the link from the gatekeeper's page (for more information on accessing Scopia Management, see *Administrator Guide for Scopia Management*).

2. Select **Settings > Calls**.



Calls

Routing mode: Call Setup (Q.931) and Call Control (H.245)

☐ Send H.245 address in Setup message

☑ Accept calls

☐ Check that call is active every 0 seconds

☑ Immediate call proceeding

Allow calls dialed with an IP address: Always

☑ Route IP calls to:

IP Address	Port
167.219.194.240	1720
167.219.194.219	1720

Add Server

IP Address: 168.168.241.203

Port: 44986

For Third Party Calls use as source address and Calling Party Number

Figure 38: Configuring IP dialing in the Scopia ECS Gatekeeper

3. Configure IP dialing as follows:

Table 8: Enabling IP Dialing

Field	Description
Route IP calls to	Select this option to enable routing IP calls to the PathFinder Server.
Add	Select to add the PathFinder Server to the list of servers. The gatekeeper routes IP calls to the PathFinder Server(s) in the list.
IP Address	Enter the IP address and port of the PathFinder Server that it automatically created when you enabled H.323 Direct Access. For more information, see Configuring Access for H.323 Legacy Endpoints on page 41. You need to add the PathFinder Server's IP address to instruct the gatekeeper where to forward all IP calls when the destination IP address is not registered to the gatekeeper.
Port	

4. Select **OK**.

5. Select **Upload.**

6. If your deployment includes multiple PathFinder Servers, including several servers acting as one server behind a load balancer:

   a. Repeat the steps above for each PathFinder Server.

   b. Verify you have the correct redundancy policy set up between the gatekeeper and each PathFinder Server.

   The ECS has its own load balancing method to work with multiple PathFinder Servers for outgoing calls from internal endpoints to external endpoints (Figure 39: Forwarding traffic to the PathFinder Server on page 50). By default, it is configured to the **Scalability** policy, enabling it to send requests to each PathFinder Server in the cluster, in a round robin manner.

   Alternatively, you can set the ECS to work with the **Priority** policy, where the ECS can route the call to the first PathFinder Server in the list and continue to the next one only if a failure occurred. Contact Customer Support to configure this setting.

   Important:

   This is separate from the redundancy policy you configured for the load balancer, which instructs it how to direct incoming traffic from the external network to the internal network (Figure 39: Forwarding traffic to the PathFinder Server on page 50). For more information about setting up the load balancer, see Scalability, High Availability and Load Balancing with Scopia PathFinder on page 52.

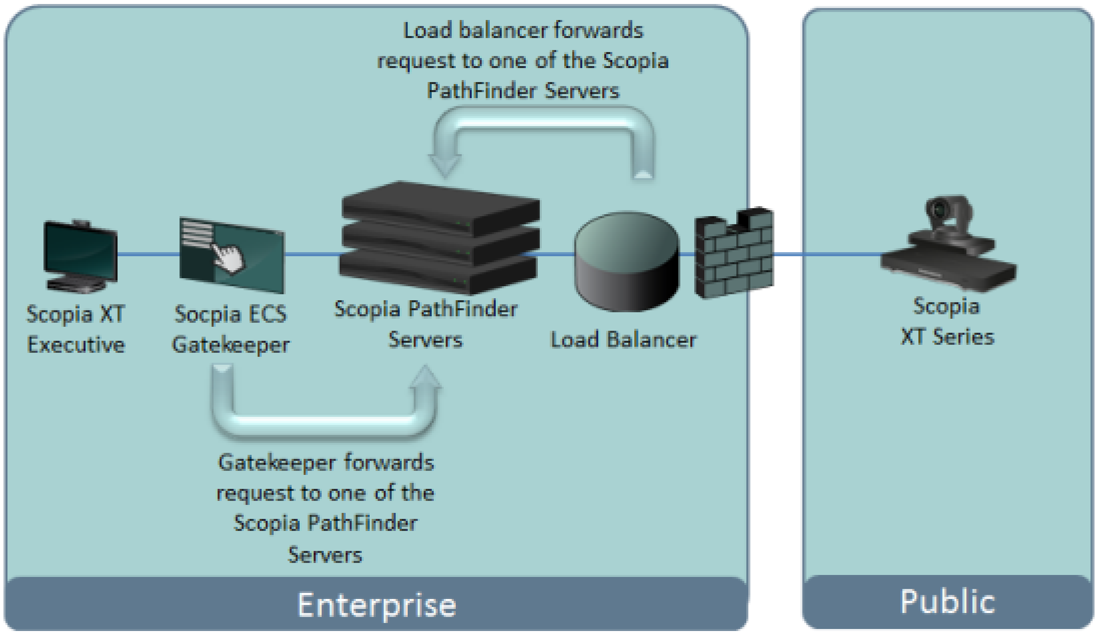

Load balancer forwards request to one of the Scopia PathFinder Servers
Scopia XT Executive
Socpia ECS Gatekeeper
Scopia PathFinder Servers
Load Balancer
Scopia XT Series
Gatekeeper forwards request to one of the Scopia PathFinder Servers
Enterprise
Public

Figure 39: Forwarding traffic to the PathFinder Server

Configuring Priority of Audio or Video

About this task

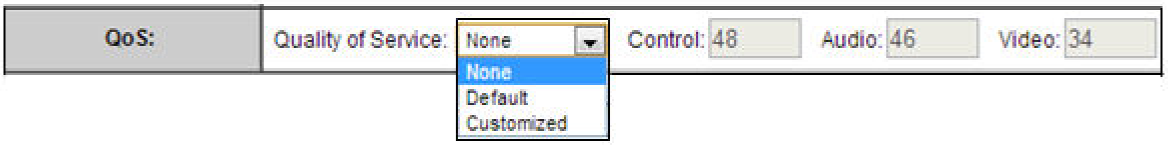
Quality of Service helps solve network performance issues by assigning relative priorities to the following packets:

- **Audio**, which is one of the media sent during a call. For example, by assigning high priority to audio under poor network conditions with high packet loss, you determine that audio is the most important element of the videoconference to be maintained at the expense of better video quality. Audio is transmitted via the RTP and RTCP protocols in H.323 calls.
- **Video**, which includes shared data stream like a presentation, also known as dual video. Far end camera control (FECC) is another example of information carried on the data stream. Video is transmitted via the RTP and RTCP protocols in H.323 calls.
- **Control**, which includes signaling and media control.
  - Signaling, also known as call control, sets up, manages and ends a connection or call. These messages include the authorization to make the call, checking bandwidth, resolving endpoint addresses, and routing the call through different servers. Signaling is transmitted via the H.225.0/Q.931 and H.225.0/RAS protocols in H.323 calls. Signaling occurs before the control aspect of call setup.
  - Control, or media control, sets up and manages the media of a call (its audio, video and data). Control messages include checking compatibility between endpoints, negotiating video and audio codecs, and other parameters like resolution, bitrate and frame rate. Control is communicated via H.245 in H.323 endpoints. Control occurs within the framework of an established call, after signaling.

Follow this procedure to determine the relative priorities for audio, video, and control transmitted via the Scopia PathFinder Server.

Procedure

1. Access the Scopia PathFinder Server Administrator web interface.
2. Select the **Settings > General > QoS** tab.
3. In the **General** tab navigate to **QoS**.



QoS: Quality of Service: None Control: 48 Audio: 46 Video: 34

Figure 40: Configuring QoS in the Scopia PathFinder Server

4. Select the **Quality of Service** level according to your network requirements.

Important:

During low-bandwidth conditions, Scopia Management uses these priority settings to adjust the quality of the meeting.

Field	Description
None	Select this setting when the network has sufficient bandwidth for each stream (audio, video, and media control) and does not require any prioritization of the different streams.
Default	Select this setting to use the following default priority values for each stream: • **48** for the media **Control** stream. This highest priority ensures that calls are set up properly even if it means that other calls ongoing may reduce their video or audio during a call setup. All TCP connections use the QoS value set in this field. • **46** for the **Audio** stream. This priority ensures that audio is always given precedence over video. This audio applies to multiple video channels (e.g., sound stream for endpoint microphones and presentations). • **34** for the **Video** stream. The lowest default priority is given to video image quality. It applies to endpoint camera images and also covers data streams like far end camera control.
Customized	Enter your own relative priorities as a number from **0-255** to represent the relative priority of **Audio**, **Video**, and **Control**.

Chapter 5 | Scalability, High Availability and Load Balancing with Scopia PathFinder

Scopia PathFinder Servers provide firewall traversal and NAT solution services to both H.460-compliant and non-H.460 endpoints. You can provide both scalability and high availability for your PathFinder Servers by deploying multiple PathFinder Servers behind a load balancer. High availability is a state where you ensure better service and less downtime by deploying additional servers. Scalability describes the ability to increase the capacity of a network device by adding another identical device (one or more) to your existing deployment.

A load balanced group of PathFinder Servers, also known as a cluster, act as a single virtual server. A load balancer can distribute traffic among the servers in the cluster, so that if one PathFinder Server has too many incoming calls at a given time, for example, another PathFinder Server can take up the load of managing incoming calls in a round-robin manner. Other load balancing methods can be configured for the load balancer, according to your deployment's requirements. Likewise, if one server fails, the remaining servers can continue working, providing high availability of the deployment.

Figure 41: Load balancing PathFinder Server in the enterprise's DMZ on page 52 illustrates a typical deployment of multiple PathFinder Servers with a load balancer.

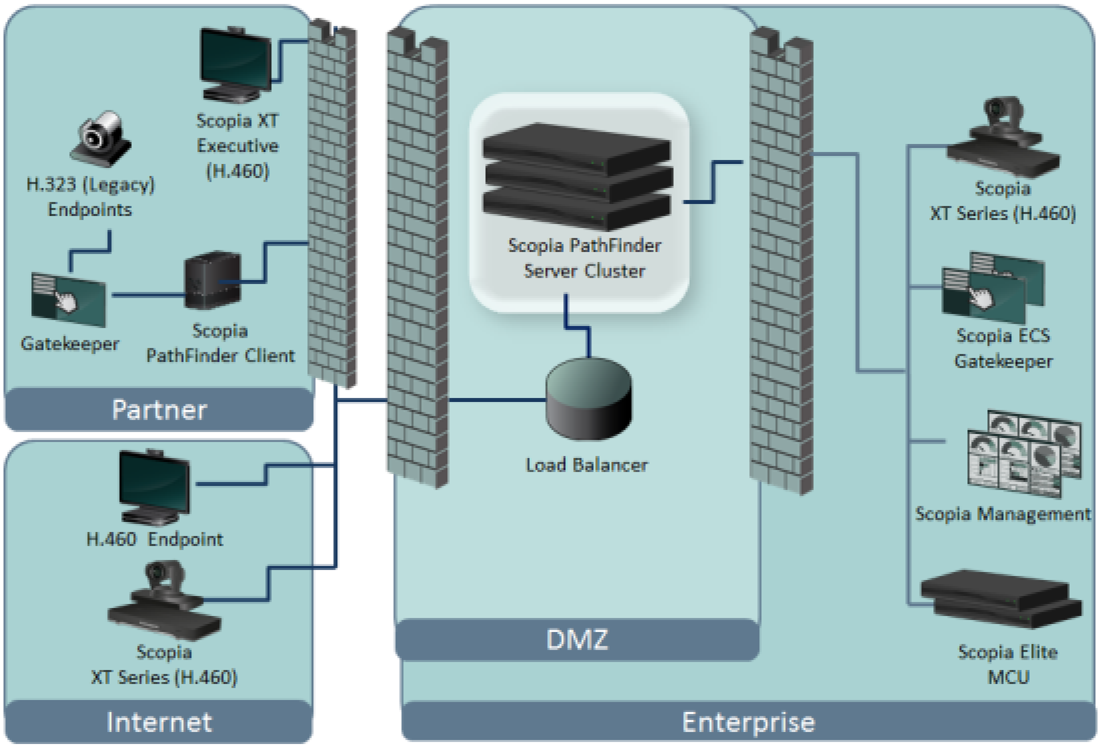


Figure 41: Load balancing PathFinder Server in the enterprise's DMZ

Load balancing multiple PathFinder Servers is also often required for service provider deployments, where the large capacity can serve multiple enterprises within one deployment. This topology is similar to the one illustrated in Figure 41: Load balancing PathFinder Server in the enterprise's DMZ on page 52.

In each case, the deployment requires the following components:

- Scopia PathFinder Servers

  The servers are configured as a cluster that has a virtual IP address for routing calls inbound to the local network. We recommend connecting both network interface cards (NIC) of each PathFinder Server:

  - The first NIC connects to a DMZ switch along with the load balancer
  - The second NIC connects to the company’s internal network

  For more information about a dual NIC configuration, see Configuring the IP Addresses of the Scopia PathFinder Server on page 30. PathFinder Servers with one NIC can also be part of the cluster.

- A load balancer

  A load balancer groups together a set (or cluster) of servers to give them a single IP address, known as a virtual IP address. It distributes client service requests amongst a group of servers. It distributes loads according to different criteria such as bandwidth, CPU usage, or cyclic (round robin). Load balancers are also known as application delivery controllers (ADC).

  The following load balancers are certified for the current version of PathFinder Server:

  - Radware AppDirector
  - F5 BIG-IP Load Traffic Manager (LTM)

  PathFinder Server redundancy can also be managed using other third-party load balancers.

- A gatekeeper

  A gatekeeper routes audio and video H.323 calls by resolving dial strings (H.323 alias or URI) into the IP address of an endpoint, and handles the initial connection of calls. Gatekeepers also implement the dial plan of an organization by routing H.323 calls depending on their dial prefixes. Scopia Management includes a built-in Scopia Gatekeeper, while ECS is a standalone gatekeeper.

- H.323 endpoints

  Your deployment can include H.323 endpoints that are H.460 compliant or H.323 (legacy) endpoints which do not support H.460. Both types of endpoints can reside either in the enterprise (secured network) or in the Internet. Endpoints that want to register to the Scopia PathFinder Server do so via the cluster’s virtual IP address or register to the Scopia PathFinder Client if they are not H.460-compliant. The Scopia PathFinder Client registers to the PathFinder Server via the cluster’s virtual IP address.

For information on the components that are part of the Scopia Solution, see the *Scopia Solution Guide*.

Navigation

- Workflow to Configure Scopia PathFinder Server for Redundancy on page 53
- Configuring Radware Load Balancer for Scopia PathFinder Servers on page 54
- Configuring the F5 BIG-IP LTM for Scopia PathFinder Servers on page 56
- Configuring Scopia PathFinder Servers for the Load Balancer on page 59

Workflow to Configure Scopia PathFinder Server for Redundancy

About this task

To configure the main components required for Scopia PathFinder redundancy, perform the tasks as they are listed in the workflow below.

The following load balancers are certified for the current version of PathFinder Server:

- Radware AppDirector
- F5 BIG-IP Load Traffic Manager (LTM)

PathFinder Server redundancy can also be managed using other third-party load balancers.

Procedure

1. Install and configure one of the PathFinder Servers, as described in:
   - Preparing the Scopia PathFinder Server Setup on page 9
   - Setting up the Scopia PathFinder Server on page 18
   - Performing the Initial Configuration of the Scopia PathFinder Server on page 30
2. Test the deployment's operability to verify that the Scopia Solution functions with a single PathFinder Server.

   You can now deploy multiple servers behind a load balancer by going through the tasks listed below.
3. Configure your load balancer to work with PathFinder Server, as follows:
   - If configuring the Radware AppDirector, see Configuring Radware Load Balancer for Scopia PathFinder Servers on page 54.
   - If configuring the F5 BIG-IP LTM, see Configuring the F5 BIG-IP LTM for Scopia PathFinder Servers on page 56.
4. Configure the PathFinder Server to work with the load balancer, as described in Configuring Scopia PathFinder Servers for the Load Balancer on page 59.
5. For each PathFinder Server in the cluster, perform the necessary configurations described in Performing the Initial Configuration of the Scopia PathFinder Server on page 30.

   Important:

   All Scopia PathFinder Servers in the cluster must be configured identically, apart from their native IP addresses. For more information about configuring the IP address, see Configuring the IP Addresses of the Scopia PathFinder Server on page 30.

Configuring Radware Load Balancer for Scopia PathFinder Servers

About this task

The procedure in this topic describes the initial settings required for the Radware AppDirector to function with the Scopia PathFinder deployment. For the detailed configuration of the load balancer, see Radware's AppDirector documentation.

Radware AppDirector is one of the load balancers that was certified for this release of the Scopia PathFinder deployment. To configure the F5 BIG-IP Load Traffic Manager, see Configuring the F5 BIG-IP LTM for Scopia PathFinder Servers on page 56.

See Scalability, High Availability and Load Balancing with Scopia PathFinder on page 52 for an overview of scalability and load balancing with Scopia PathFinders.

Before you begin

❗ **Important:**

This procedure should only be performed by certified Radware implementation specialists. This section focuses only on the settings which may be different from a standard Radware implementation. For more information on standard Radware deployments, see the Radware documentation.

Verify that you have all the IP addresses of the Scopia PathFinder Servers, required to configure the load balancer.

Procedure

1. Log in to the AppDirector user interface.

2. Create a server farm for Scopia PathFinder Servers in the load balancer, as described in the AppDirector documentation. A farm is the term used by AppDirector to refer to a cluster of servers.

   The settings described below are specific to Scopia PathFinder Server and may differ from a typical AppDirector deployment:

   Table 9: Virtual farm settings specific to Scopia PathFinder Server

Field	Description
Farm Name	Enter the name of the server farm.
Aging Time	Indicates the number of seconds before the connection between a source IP to the server is timed out (disconnected). The source IP refers to either the endpoint or the Scopia PathFinder Client, depending on whether the endpoint is connecting directly or via the Scopia PathFinder Client. Set the aging time to a high value (for example, 90000). Within that period of time, AppDirector routes the reconnecting client to that specific server.

Field	Description
Dispatch Method	Select the method the load balancer uses for distributing traffic between servers in this farm. We recommend one of the following: • **Round Robin**: Directs each endpoint service request to another Scopia PathFinder Server, in turn. • **Least Amount of Traffic**: Directs endpoint service requests to the Scopia PathFinder Server with the least amount of traffic.
Sessions Mode	Select **EntryPerSession** to ensure the load balancer continues to route packets from the same client to the same Scopia PathFinder Server throughout the duration of the videoconference.

3. Configure a virtual IP address for the farm, as described in the AppDirector documentation.

   This is the address the load balancer uses to forward endpoint service requests to the Scopia PathFinder Servers grouped in the farm.

4. Configure the Layer 4 rules (or policies) the load balancer uses to manage traffic, as described in the AppDirector documentation.

   AppDirector uses the Layer 4 protocol and the request’s destination port to select the required farm. TCP (Transmission Control protocol) and UDP (User Datagram Protocol) are part of the Layer 4 protocol. AppDirector manages the virtual IP addresses using Layer 4 policies.

   The settings described below are specific to Scopia PathFinder Server and may differ from a typical AppDirector deployment:

   - Use the same farm name as above
   - Set **L4 Protocol** to **Any**. This ensures the farm supports any IP protocol, including TCP and UDP.

5. Add each Scopia PathFinder Server to the farm as described in the AppDirector documentation.

   The settings described below are specific to Scopia PathFinder Server and may differ from a typical AppDirector deployment:

   - Enter the server's details, such as the IP address
   - Verify that **Client NAT** is set to **Disabled**.

6. To ensure communication is possible with the Scopia PathFinders, add the farm's virtual IP address and service port to the organization's firewalls.

7. Continue with Configuring Scopia PathFinder Servers for the Load Balancer on page 59 to configure the Scopia PathFinder Servers to function with a load balancer.

Configuring the F5 BIG-IP LTM for Scopia PathFinder Servers

About this task

The procedure in this topic describes the settings required for the F5 BIG-IP Load Traffic Manager (LTM) to function with the Scopia PathFinder deployment. For the detailed configuration of the load balancer, see the F5's documentation.

The F5 BIG-IP LTM is one of the load balancers that was certified for this release of the Scopia PathFinder deployment. To configure the Radware AppDirector, see Configuring Radware Load Balancer for Scopia PathFinder Servers on page 54.

Before you begin

Important:

This procedure should only be performed by certified F5 BIG-IP LTM implementation specialists. This section focuses only on the settings which may be different from a standard implementation, and does not elaborate on specific F5 terminology necessary to understand when deploying the load balancer. For more information on standard F5 BIG-IP LTM deployments, see the F5 documentation.

Verify that you have all the IP addresses of the Scopia PathFinder Servers and the F5 (including its default gateway, also known as its router). This is required to configure the load balancer.

Procedure

1. Access the F5 web interface.
2. Set up a virtual LAN (VLAN) for all Scopia PathFinder Servers, as described in the F5 documentation.

   A VLAN is similar to a physical LAN, but is used to group devices based on specific attributes rather than a common location. Any data packets passing in and out of the VLAN must be done via the F5's router (also known as the default gateway).
3. Add a **Self IP** for the VLAN you created, as described in the F5 documentation.

   This IP address represents the range of IP addresses of the servers in the cluster. The load balancer uses this IP address to determine which VLAN to forward the request.
4. Add a **Node** for each Scopia PathFinder Server and the default gateway, as described in the F5 documentation.

   The VLAN consists of nodes, where each node is a physical server.
5. Add a pool that contains all Scopia PathFinder Servers in your deployment, as described in the F5 documentation. A pool is the term used by F5 to refer to a cluster of servers.

   Configure the Scopia PathFinder Server pool settings, as described in the F5 documentation.

   The settings described below are specific to Scopia PathFinder Server and may differ from a typical F5 deployment:

Table 10: Pool settings specific to Scopia PathFinder Server

Field	Description
Configuration	From the list, select **Advanced**.
Name	Enter a name to identify this as the PathFinder Server cluster, such as PathFinder_Pool.
Health Monitors	Select the **gateway_icmp** health monitor. **gateway_icmp** is a pre-configured health monitor available by default on the F5. Health monitors check devices to verify that they are running, at specified intervals. For more information, see the F5 documentation.
Load Balancing Method	From the list, select the method the load balancer uses for distributing traffic between servers in this pool. The default method is **Round Robin**, which directs each endpoint service request to another Scopia PathFinder Server, in turn.
Node List	Select this option. A list of the Scopia PathFinder Servers you added as nodes appears.
Service Port	Enter **0** to indicate that this field should not be used. The Scopia PathFinder Server's service port is configured on the firewall.
New Members	Add each Scopia PathFinder Server.

6. Add a pool that contains the default gateway, as described in the F5 documentation.

   The pool may include more than one gateway, depending on your network setup.

   The settings described below are specific to Scopia PathFinder Server and may differ from a typical F5 deployment:

Table 11: Gateway pool settings specific to Scopia PathFinder Server

Field	Description
Configuration	From the list, select **Advanced**.
Name	Enter a name to identify this as the gateway cluster, such as Gateway_Pool.
Health Monitors	Select the **gateway_icmp** health monitor. **gateway_icmp** is a pre-configured health monitor available by default on the F5. Health monitors check devices to verify that they are running, at specified intervals. For more information, see the F5 documentation.
New Address	Select this option and enter the IP address of the F5's default gateway (router).
Service Port	Enter **0** to indicate that this field should not be used. The Scopia PathFinder Server's service port is configured on the firewall.
New Members	Add the F5's default gateway as a member to this pool.

7. (Optional) After configuring the pools, we recommend verifying that the servers are running by checking the list of members in each pool, as described in the F5 documentation.

8. Set up the default gateway as the router for the Scopia PathFinder Server pool, as described in the F5 documentation.

9. Add a virtual server, which includes all Scopia PathFinder Servers in your deployment, as described in the F5 documentation.

10. Configure the virtual server, as described in the F5 documentation.

    The settings described below are specific to Scopia PathFinder Server and may differ from a typical F5 deployment:

    Table 12: Virtual server settings specific to Scopia PathFinder Server

Field	Description
Default Pool	From the list, select the Scopia PathFinder Server pool you created.
Default Persistence Profile	From the list, select **source_address**. This instructs the load balancer to send all session requests from the same source IP to the same Scopia PathFinder Server.

11. Configure static network address translation (SNAT) to translate the source IP from an actual Scopia PathFinder Server to a virtual public IP, as described in the F5 documentation. This is used to convert a request to the virtual cluster IP into the real IP of one of the servers in the cluster.

    The settings described below are specific to Scopia PathFinder Server and may differ from a typical F5 deployment:

    Table 13: SNAT settings specific to Scopia PathFinder Server

Field	Description
Name	Enter a name to identify this as the NAT for the Scopia PathFinder Server cluster, such as Scopia PathFinder_SNAT.
Translation	Select **IP address** from the list and enter the IP address of the Scopia PathFinder virtual server you just created.
Origin	Select **Address List** from the list.
Type	Select **Host**.
Address	Add the IP addresses of the Scopia PathFinder Servers in the pool.

12. To ensure communication is possible with the Scopia PathFinders, add the IP address and service port of the Scopia PathFinder virtual server to the organization's firewalls.

13. Continue with Configuring Scopia PathFinder Servers for the Load Balancer on page 59 to configure the Scopia PathFinder Servers to function with a load balancer.

Configuring Scopia PathFinder Servers for the Load Balancer

About this task

This procedure describes how to configure the Scopia PathFinder Servers in the cluster to function with the load balancer.

Important:

All Scopia PathFinder Servers in the cluster must be configured identically, apart from their native IP addresses.

The following load balancers are certified for the current version of PathFinder Server:

- Radware AppDirector
- F5 BIG-IP Load Traffic Manager (LTM)

PathFinder Server redundancy can also be managed using other third-party load balancers.

For more information, see:

- Scalability, High Availability and Load Balancing with Scopia PathFinder on page 52 for an overview of scalability and load balancing with Scopia PathFinder Servers.

  Important:

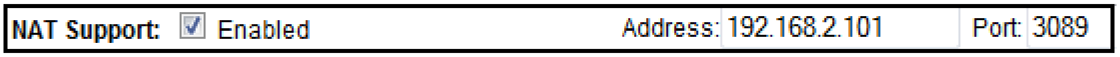
  The load balancer maps the traffic based on the source IP address. All endpoint requests that originate from the same IP address are always mapped to the same Scopia PathFinder Server.
- The load balancer's documentation.

Before you begin

Verify the default gateway of each Scopia PathFinder Server is set to the native IP address of the load balancer. For more information on setting the device's default gateway, see Configuring the IP Addresses of the Scopia PathFinder Server on page 30.

Procedure

1. Access the Scopia PathFinder Server Administrator web interface.
2. Select **Settings > General > NAT Support**.



NAT Support: ☑ Enabled Address: 192.168.2.101 Port: 3089

Figure 42: Configuring NAT support

3. Configure NAT support for each Scopia PathFinder Server in the cluster, as follows:

Table 14: Configuring NAT support

Field	Description
NAT Support	Enable **NAT Support** to use the virtual IP address (VIP) of the cluster when communicating with external endpoints, instead of the IP address of this PathFinder Server. This is mandatory when deploying PathFinder Server with a load balancer.
Address	Enter the VIP of the PathFinder Server's cluster, as follows: • If you have a single NIC configuration, or a dual NIC configuration with the external NIC secured behind a firewall, enter the public IP address with NAT translation to the cluster's VIP. • If you have a dual NIC configuration with the external NIC directly in the public network, set the NAT address to the VIP of the cluster and deploy your load balancer in the public network. **Important:** In the firewall/NAT device, verify that the NAT address is mapped to the private VIP address of the PathFinder Server cluster's external NIC.
Port	If required, change the Scopia PathFinder Client port number which is set to **3089** by default.

4. Select **Save**.
5. For each Scopia PathFinder Server in the cluster, perform the necessary configurations described in Performing the Initial Configuration of the Scopia PathFinder Server on page 30.

Important:

All Scopia PathFinder Servers in the cluster must be configured identically, apart from their native IP addresses. For more information about configuring the IP address, see Configuring the IP Addresses of the Scopia PathFinder Server on page 30.

Chapter 6 | Performing Maintenance Procedures

This section details to the ongoing administrator tasks required to maintain your video network:

Navigation

Managing Logs

Logs are important for troubleshooting. This section describes the log managing provided in the Scopia PathFinder Server:

Navigation

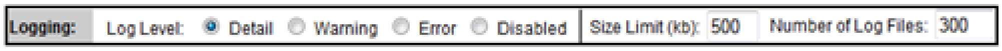
Configuring the Alert Level and Size of Logs

About this task

Log files contain important information for troubleshooting the system. You can set the level of alerts in the Scopia PathFinder Server. You can also define the size and number of log files kept on the hard disk of the Scopia PathFinder Server for further troubleshooting.

Procedure

1. Access the Scopia PathFinder Server Administrator web interface.
2. Select the **Settings** tab.
3. Navigate to the **Logging** area of the **General** tab (Figure 43: Configuring the logs on page 63).



Logging: Log Level: ● Detail ○ Warning ○ Error ○ Disabled Size Limit (kb): 500 Number of Log Files: 300

Figure 43: Configuring the logs

4. Select the log level required for this Scopia PathFinder Server.

Field Name	Description
Detail	Saves call details, warnings, and critical system errors to the log file.
Warning	Saves warnings issued by the system and critical system errors to the log file.
Error	Saves critical system errors only to the log file.
Disabled	Disables the Scopia PathFinder Server logging.

5. Select the log file size in the **Size Limit** field. The size of an individual log file is configured to 500KB by default. The maximum size of an individual log file is 10000KB.
6. Define how many log files are created in the **Number of Log Files** field. By default the maximum number of log files that are kept on the Scopia PathFinder Server is 300. The maximum number of log files is 1000. When the maximum number is reached and a new log file is created, it replaces the oldest log file.

Retrieving Application and Operating System Logs

About this task

When reporting a problem to customer support, they may ask you to retrieve and send logs from the Scopia PathFinder Server. This procedure describes how to download the Customer Support Package, which is a zipped file of bundled logs and configuration files that you can send to customer support.

The Customer Support Package collects the following information:

- Scopia PathFinder Server application and operating system configurations
- Scopia PathFinder Server application and operating system logs
- Operating system run time information (including CPU usage, memory usage, and networking status)
- Scopia PathFinder Server application run time information (including memory status and other details).

You can retrieve the Customer Support Package from Scopia PathFinder Server, or via Scopia Management as detailed in *Administrator Guide for Scopia Management*.

Alternatively, you can retrieve the Scopia PathFinder Server application and operating system configurations from the Scopia PathFinder administration console as explained in Backing Up the Configuration Settings on page 72.

Important:

You cannot restore from a Customer Support Package; you can only restore from a backup.

You can set the level of detail in the logs of the Scopia PathFinder Server and define the size and number of log files kept on the server's hard disk. For more information, see Configuring the Alert Level and Size of Logs on page 62.

Before you begin

You could need a software tool to perform this procedure. We recommend WinSCP, a Secure FTP client, to save the file(s) to the desired location. You can download this application from *http://winscp.net/eng/download.php*

Procedure

1. Access the Scopia PathFinder Server Administrator web interface.
2. Select **General > Customer Support** (Figure 44: Accessing the screen for generating the Customer Support Package on page 64).

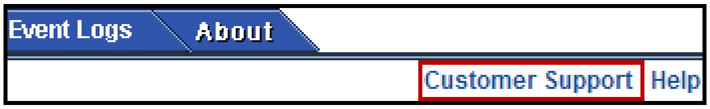
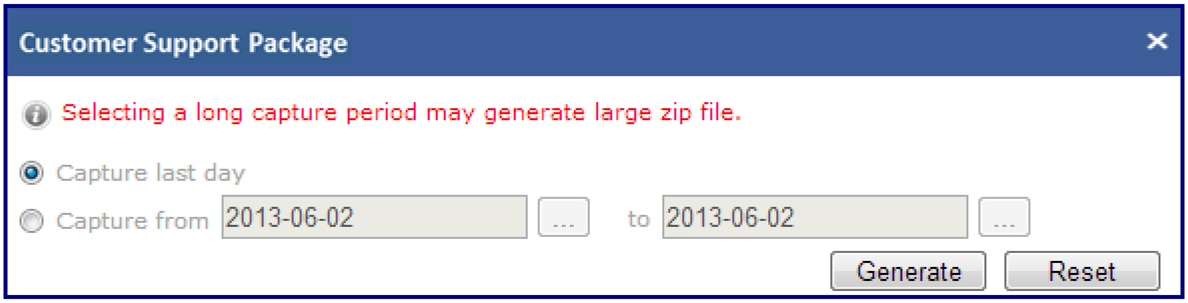


Figure 44: Accessing the screen for generating the Customer Support Package

3. To collect today's log, select **Capture last day**.


Customer Support Package

Selecting a long capture period may generate large zip file.

● Capture last day

○ Capture from 2013-06-02 ... to 2013-06-02 ...

Figure 45: Selecting the log file

4. To select log files collected during a period of time:
   a. Select **Capture from... to** (Figure 45: Selecting the log file on page 64).
   b. Select, hold and scroll through the year and month lists for the required date (Figure 46: Choosing the log file dates on page 65).

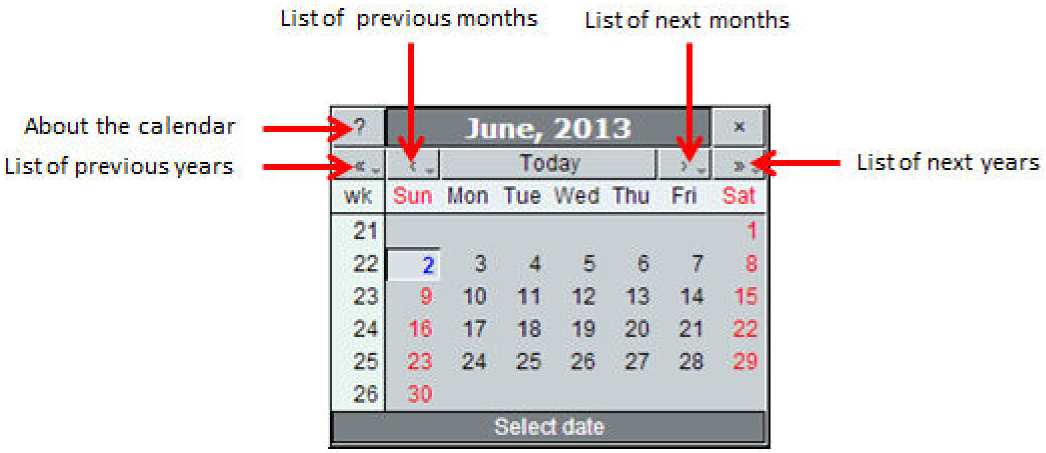


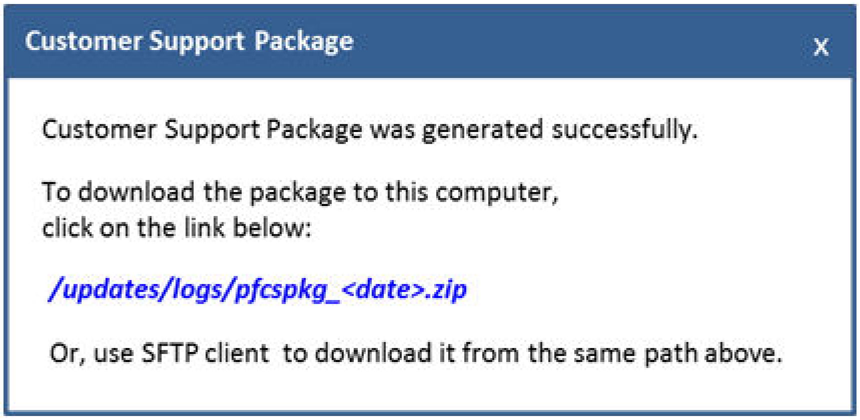
Figure 46: Choosing the log file dates

c. Select the relevant day in the calendar.

d. If necessary, select **Reset** to change dates.

5. Select **Generate**.

6. (Optional) To download the package from the Scopia PathFinder Server to your PC using the HTTP connection, select **/updates/logs/pfcspkg_<date>.zip** (Figure 47: Retrieving the Customer Support Package on page 65).



Customer Support Package

Customer Support Package was generated successfully.

To download the package to this computer,
click on the link below:

/updates/logs/pfcspkg_<date>.zip

Or, use SFTP client to download it from the same path above.

Figure 47: Retrieving the Customer Support Package

7. (Optional) To download the package from the Scopia PathFinder Server to your PC using WinSCP, run the application and perform the steps below to transfer the file.

8. Configure the connection to your Scopia PathFinder Server in the **WinSCP Login** dialog box, as follows:

Table 15: Configuring WinSCP settings

Field	Description
Host name	Enter the IP address of the Scopia PathFinder Server.
User name	Enter the username to access Scopia PathFinder Server. This is always **uadmin**.

Field	Description
Password	Enter the password. The default is **admin**. If you modified the default password, enter the new value here.
File protocol	Select **SFTP** to enable the SSH File Transfer Protocol capability.

9. Select **Login**.

10. Drag the log file from the */updates/logs* folder to the relevant folder on your computer The Scopia PathFinder Server names logs as *pfcspkg_<selected_dates>.zip* by default.

11. Close WinSCP and confirm ending the session to save the changes.

Viewing Scopia PathFinder Information

About this task

Use this feature to find useful information about the system. This information is also required when you contact Customer Support.

Procedure

1. Access the Scopia PathFinder Server Administrator web interface.

2. Select the **About** tab. The screen displays system information.

Table 16: Viewing Information on Scopia PathFinder

Field Name	Description
Version Number	Displays the version number of the Scopia PathFinder Server.
MAC Address	Displays the MAC address of the Scopia PathFinder Server.
Expiration Date	Displays the date on which your current license expires. For demonstration versions only.
Max. Connected Endpoints	Displays the maximum allowed number of connected endpoints, as determined by your license.
Max. Concurrent Calls	Displays the maximum allowed number of concurrent calls, as determined by your license.

Capturing Network Traces for Troubleshooting

About this task

This section describes how to track and capture packet traffic on the Scopia PathFinder Server, using the built-in TCPDUMP packet analyzer (*http://www.tcpdump.org/*).

You can retrieve the network captures as files and use them to troubleshoot problems.

Before you begin

- Verify you have the IP address of the Scopia PathFinder Server.
- You need software tools to perform this procedure. We recommend using these freeware applications:
  - PuTTY, an SSH client, to connect to the Scopia PathFinder Server administration console to perform the procedure in this section. You can download this application from *http://www.chiark.greenend.org.uk/~sgtatham/putty/*
  - WinSCP, a Secure FTP client, to save the file(s) to the desired location. You can download this application from *http://winscp.net/eng/download.php*

Procedure

1. Run PuTTY to connect to the Scopia PathFinder Server.

2. Configure the connection to the Scopia PathFinder Server in the **Session** tab of the **PuTTY Configuration** dialog box, as follows:

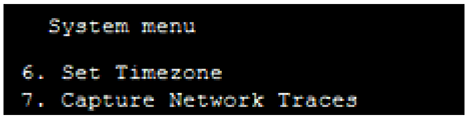
Table 17: Configuring the PuTTY session

Field	Description
Host Name (or IP address)	Enter the IP address of the Scopia PathFinder Server.
SSH	Verify the Secure Shell protocol is enabled.

3. Create a network trace file with PuTTy as follows:

   a. Enter **4** in the **Main menu** to access the **System Menu**.

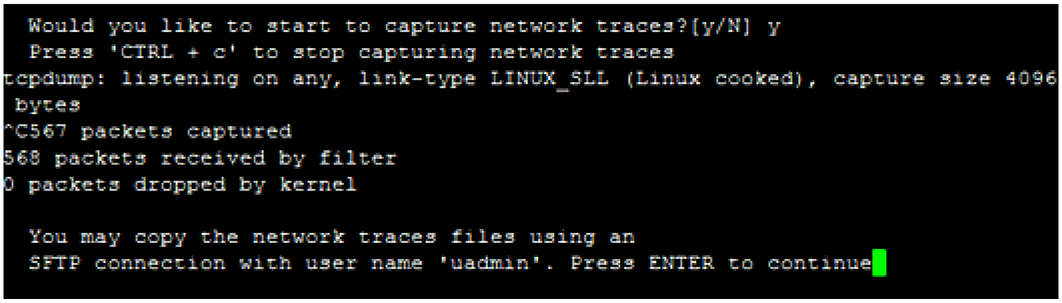
   b. Enter **7** to capture network traces (Figure 48: Capturing network traces on page 67).



```
  System menu

6. Set Timezone
7. Capture Network Traces
```

Figure 48: Capturing network traces

   c. Enter **Y** to confirm starting to capture the network traces (Figure 49: Creating the network capture files on page 68).



```
  Would you like to start to capture network traces?[y/N] y
  Press 'CTRL + c' to stop capturing network traces
tcpdump: listening on any, link-type LINUX_SLL (Linux cooked), capture size 4096
 bytes
^C567 packets captured
568 packets received by filter
0 packets dropped by kernel

  You may copy the network traces files using an
  SFTP connection with user name 'uadmin'. Press ENTER to continue
```

Figure 49: Creating the network capture files

The Scopia PathFinder Server starts the trace, which you can end by pressing **Ctrl-C**. It creates a single or multiple *.pcap* files, depending on the duration of the capture. It also generates a *.tgz* file which compresses all these *.pcap* files to a single package (Figure 50: Downloading the network capture files to your computer on page 69). As each file is dated and time stamped, you can download and review only the files which captured issues you are interested in troubleshooting.

d. Press **Enter** to return to the **Main Menu**.

e. Press **Q** to exit the session.

4. Run WinSCP to transfer the file.

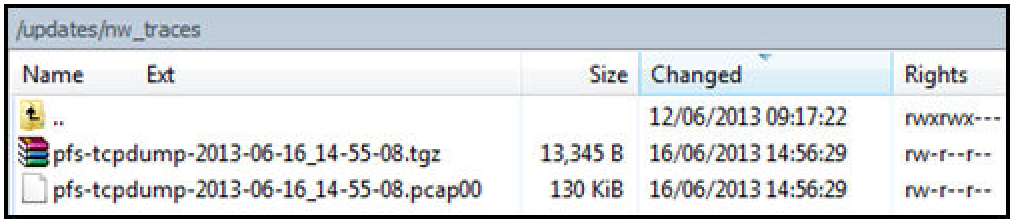
5. Configure the connection to your Scopia PathFinder Server in the **WinSCP Login** dialog box, as follows:

Table 18: Configuring WinSCP settings

Field	Description
Host name	Enter the IP address of the Scopia PathFinder Server.
User name	Enter the username to access Scopia PathFinder Server. This is always **uadmin**.
Password	Enter the password. The default is **admin**. If you modified the default password, enter the new value here.
File protocol	Select **SFTP** to enable the SSH File Transfer Protocol capability.

6. Select **Login**.

7. Drag the relevant network capture file from the */updates/nw_traces* folder to the relevant folder on your computer (Figure 50: Downloading the network capture files to your computer on page 69).



/updates/nw_traces

Name	Ext	Size	Changed	Rights
..			12/06/2013 09:17:22	rwxrwx---
pfs-tcpdump-2013-06-16_14-55-08.tgz		13,345 B	16/06/2013 14:56:29	rw-r--r--
pfs-tcpdump-2013-06-16_14-55-08.pcap00		130 KiB	16/06/2013 14:56:29	rw-r--r--

Figure 50: Downloading the network capture files to your computer

8. Close WinSCP and confirm ending the session to save the changes.

Updating, Backing Up and Restoring the Scopia PathFinder Server

You should back up your application and system configuration files on a regular basis. It is general practice to back up the latest configuration before performing maintenance procedures such as an upgrade.

Depending on your support contract, you can update the Scopia PathFinder Server application to:

- The next major version.

  Updating a major version requires a new license.

  This kind of update changes one of the first two digits in a version number. For example, updating from version 7.7 to version 8.2 requires a new license.

- An incremental version.

  Updating an incremental version does not require a new license.

  This kind of update changes the third, fourth and fifth digits in the version number. For example, updating from 8.2.0.0.29 to 8.2.0.0.34 does not require a new license.

The update procedure may vary depending on the release number and the size of the jump from the current installation to the new release.

Important:

You can restore the operating system of the Scopia PathFinder Server to any version of the server as long as you use the Intel server's backup packages.

For details about updating, backing up, restoring the Scopia PathFinder Server application and its operating system, see the following topics:

Navigation

- Upgrading the Scopia PathFinder Server on page 69
- Backing Up the Configuration Settings on page 72
- Restoring the Configuration Settings on page 73

Upgrading the Scopia PathFinder Server

About this task

If Customer Support sends you an upgrade of the Scopia PathFinder Server application or operating system, you need to upgrade your system to the latest software version for the best performance and enhanced features. This procedure describes how to upgrade the Scopia PathFinder Server and covers both the upgrading of system components and of the Scopia PathFinder Server application from version 7.7.x to version 8.2.x.

❗ **Important:**

Use the same procedure to roll back to a previous version. For information on rolling back to a Scopia PathFinder Server application version prior to 7.7.x, contact Customer Support.

Before you begin

- Verify you have the IP address of the Scopia PathFinder Server.
- Download the upgrade file to your computer.
- If required, make sure you have the license key at hand.
- You need software tools to perform this procedure. We recommend using these freeware applications:
  - WinSCP, a Secure FTP client, to save the file(s) to the desired location. You can download this application from *http://winscp.net/eng/download.php*
  - PuTTY, an SSH client, to connect to the Scopia PathFinder Server administration console to perform the procedure in this section. You can download this application from *http://www.chiark.greenend.org.uk/~sgtatham/putty/*
- Make sure no active calls are running on the Scopia PathFinder Server, as the upgrade disconnects these calls.
- Back up the configuration files of both the Scopia PathFinder Server and the operating system before performing this procedure, as described in Backing Up the Configuration Settings on page 72.

Procedure

1. Run WinSCP to transfer the file.
2. Configure the connection to your Scopia PathFinder Server in the **WinSCP Login** dialog box, as follows:

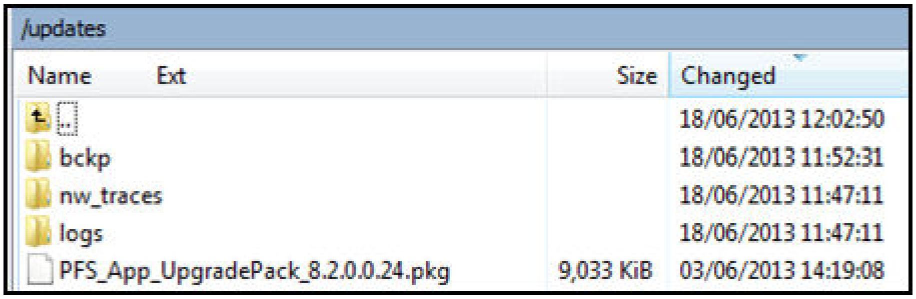
Table 19: Configuring WinSCP settings

Field	Description
Host name	Enter the IP address of the Scopia PathFinder Server.
User name	Enter the username to access Scopia PathFinder Server. This is always **uadmin**.

Field	Description
Password	Enter the password. The default is **admin**. If you modified the default password, enter the new value here.
File protocol	Select **SFTP** to enable the SSH File Transfer Protocol capability.

3. Select **Login**.

4. Drag the new *.pkg* update file to the */updates* folder in the Scopia PathFinder Server and select **Copy** when prompted (Figure 51: Screen showing the application upgrade file in the Scopia PathFinder Server on page 71).



/updates

Name	Ext	Size	Changed
..			18/06/2013 12:02:50
bckp			18/06/2013 11:52:31
nw_traces			18/06/2013 11:47:11
logs			18/06/2013 11:47:11
PFS_App_UpgradePack_8.2.0.0.24.pkg		9,033 KiB	03/06/2013 14:19:08

Figure 51: Screen showing the application upgrade file in the Scopia PathFinder Server

5. Run PuTTY to connect to the Scopia PathFinder Server.

6. Configure the connection to the Scopia PathFinder Server in the **Session** tab of the **PuTTY Configuration** dialog box, as follows:

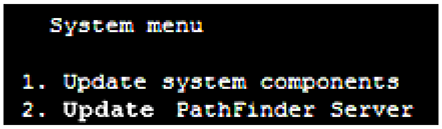
Table 20: Configuring the PuTTY session

Field	Description
Host Name (or IP address)	Enter the IP address of the Scopia PathFinder Server.
SSH	Verify the Secure Shell protocol is enabled.

7. Install the update as follows:

   a. Enter **4** in the **Main menu** to access the **System Menu**.

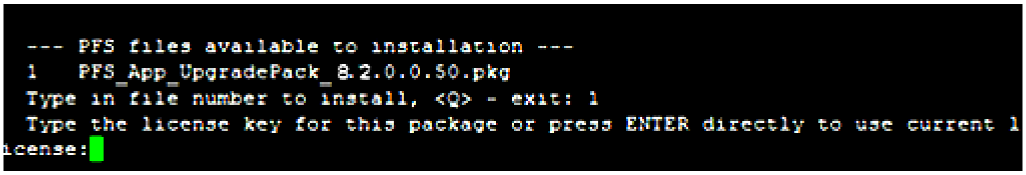
   b. Enter the menu item corresponding to the required update (Figure 52: Updating the Scopia PathFinder Server application version on page 71): **1** to update the operating system components, or **2** to upgrade the Scopia PathFinder Server version.



```
   System menu

 1. Update system components
 2. Update  PathFinder Server
```

Figure 52: Updating the Scopia PathFinder Server application version

c. Enter the menu item corresponding to the installation file you just transferred to the Scopia PathFinder Server (Figure 53: Screen showing the installation of the Scopia PathFinder Server application update on page 72).



```
 --- PFS files available to installation ---
 1   PFS_App_UpgradePack_8.2.0.0.50.pkg
 Type in file number to install, <Q> - exit: 1
 Type the license key for this package or press ENTER directly to use current l
icense:
```

Figure 53: Screen showing the installation of the Scopia PathFinder Server application update

d. If this is a major update of the Scopia PathFinder Server application, enter the license key (Figure 53: Screen showing the installation of the Scopia PathFinder Server application update on page 72). Otherwise, press **Enter** to use the current license key.

The Scopia PathFinder Server reboots automatically after each installation procedure.

Backing Up the Configuration Settings

About this task

You can use this procedure to backup the Scopia PathFinder Server application or system configuration settings to a single file, which you can then archive elsewhere using FTP. You can also send the backup file to Customer Support, if required. To restore from the backup file to the Scopia PathFinder Server, see Restoring the Configuration Settings on page 73.

This is different from saving settings and logs into a Customer Support Package, along with other system log files. For more information, see Retrieving Application and Operating System Logs on page 63.

Important:

You cannot restore from a Customer Support Package; you can only restore from a backup.

Before you begin

- Verify you have the IP address of the Scopia PathFinder Server.
- You need a software tool to perform this procedure. We recommend PuTTY, a free SSH client, to connect to the Scopia PathFinder Server administration console to perform the procedure in this section. You can download this application from *http://www.chiark.greenend.org.uk/~sgtatham/putty/*

Procedure

1. Run PuTTY to connect to the Scopia PathFinder Server.
2. Configure the connection to the Scopia PathFinder Server in the **Session** tab of the **PuTTY Configuration** dialog box, as follows:

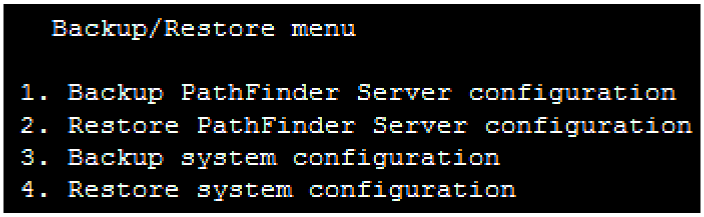
Table 21: Configuring the PuTTY session

Field	Description
Host Name (or IP address)	Enter the IP address of the Scopia PathFinder Server.
SSH	Verify the Secure Shell protocol is enabled.

3. Create a backup of the configuration settings as follows:

   a. Enter **3** in the **Main menu** to access the **Backup/Restore menu** option.

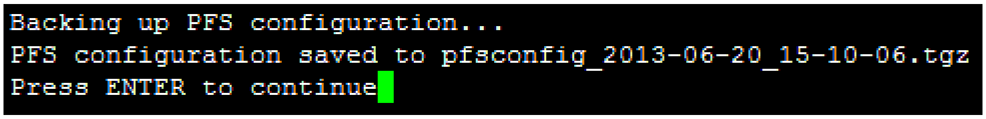
   b. Enter the menu item corresponding to the required backup (Figure 54: Selecting the configuration backup on page 73): **1** to backup the Scopia PathFinder Server configuration, or **3** to backup the operating system configuration.



```
   Backup/Restore menu

1. Backup PathFinder Server configuration
2. Restore PathFinder Server configuration
3. Backup system configuration
4. Restore system configuration
```

Figure 54: Selecting the configuration backup

Depending on the backup you selected, the configuration is saved to a file that has the format *<sysconfig_yyyy-mm-dd-hh-mm-ss.tgz>* or *<pfsconfig_yyyy-mm-dd-hh-mm-ss.tgz>* (Figure 55: Screen showing the backing up the Scopia PathFinder Serverapplication configuration on page 73). The file is located in the server folder */updates/bckp*.



```
Backing up PFS configuration...
PFS configuration saved to pfsconfig_2013-06-20_15-10-06.tgz
Press ENTER to continue
```

Figure 55: Screen showing the backing up the Scopia PathFinder Serverapplication configuration

   c. Press **Enter** to return to the **Main menu**.

   d. Enter **Q** to exit the session.

Restoring the Configuration Settings

About this task

The restore tool of Scopia PathFinder Server offers the safest and most reliable method to restore a backup of Scopia PathFinder Server application or system configurations. Depending on the backup you selected, the file has the name format *<pfsconfig_yyyy-mm-dd_hh-mm-ss.tgz>* (application) or *<sysconfig_yyyy-mm-dd_hh-mm-ss.tgz>* (system). The file is located in the Scopia PathFinder Server under the folder */updates/bckp*. For more information on creating a backup, see Backing Up the Configuration Settings on page 72.

Important:

You cannot restore from a Customer Support Package; you can only restore from a backup.

Before you begin

- Verify you have the IP address of the Scopia PathFinder Server.
- You need a software tool to perform this procedure. We recommend PuTTY, a free SSH client, to connect to the Scopia PathFinder Server administration console to perform the procedure in this section. You can download this application from *http://www.chiark.greenend.org.uk/~sgtatham/putty/*

Procedure

1. Run PuTTY to connect to the Scopia PathFinder Server.
2. Configure the connection to the Scopia PathFinder Server in the **Session** tab of the **PuTTY Configuration** dialog box, as follows:

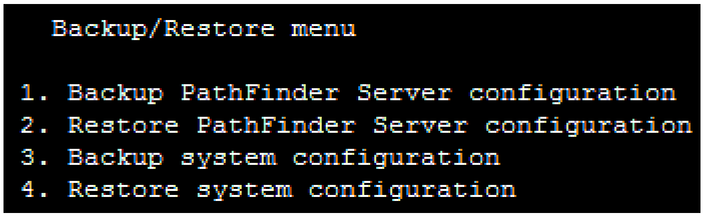
Table 22: Configuring the PuTTY session

Field	Description
Host Name (or IP address)	Enter the IP address of the Scopia PathFinder Server.
SSH	Verify the Secure Shell protocol is enabled.

3. Restore the configuration backup to the Scopia PathFinder Server as follows:

   a. Enter **3** in the **Main menu** to access the **Backup/Restore menu** option.

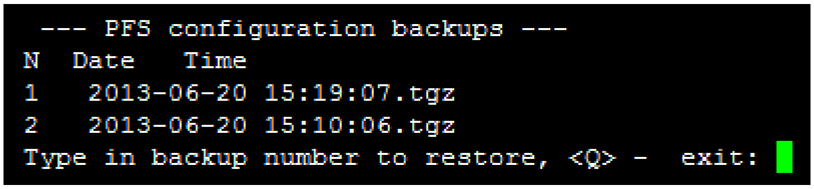
   b. Enter the menu item corresponding to the required configuration restore (Figure 56: Restoring the Scopia PathFinder Server configuration settings on page 74): **2** to restore the Scopia PathFinder Server configuration, or **4** to restore the operating system configuration.



```
   Backup/Restore menu

 1. Backup PathFinder Server configuration
 2. Restore PathFinder Server configuration
 3. Backup system configuration
 4. Restore system configuration
```

Figure 56: Restoring the Scopia PathFinder Server configuration settings

   c. Enter the item number corresponding to the configuration restore (Figure 57: Screen showing how to restore the Scopia PathFinder Server application configuration on page 75).



```
 --- PFS configuration backups ---
N   Date    Time
1    2013-06-20 15:19:07.tgz
2    2013-06-20 15:10:06.tgz
Type in backup number to restore, <Q> -  exit: 
```

Figure 57: Screen showing how to restore the Scopia PathFinder Server application configuration

d. Press **Enter**. After the configuration is restored, the display returns to the **Backup/Restore menu**.

RADVISION®
an Avaya company

About Radvision
Radvision, an Avaya company, is a leading provider of videoconferencing and telepresence technologies over IP and wireless networks. We offer end-to-end visual communications that help businesses collaborate more efficiently. Together, Radvision and Avaya are propelling the unified communications evolution forward with unique technologies that harness the power of video, voice, and data over any network.
www.radvision.com