Deployment Guide for Avaya Scopia® XT Desktop Server for IP Office

Version 8.3
For Solution 8.3
March 2014

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

Avaya Inc. reserves the right to revise this publication and make changes without obligation to notify any person of such revisions or changes. Avaya Inc 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 Avaya Inc and a copy will be provided to you.

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

Deployment Guide for Avaya Scopia® XT Desktop Server for IP Office Version 8.3, March 19, 2014

http://support.avaya.com

Table of Contents

Chapter 1: About Scopia® XT Desktop server for IP Office

Chapter 2: Planning your Scopia® XT Desktop server Deployment

Chapter 3: Installing the Scopia® XT Desktop server

Chapter 4: Configuring Your Deployment

Chapter 5: Securing Your Scopia® XT Desktop Deployment

Glossary of Terms for Scopia® Solution

Chapter 1 | About Scopia® XT Desktop server for IP Office

Scopia® XT Desktop server extends the capabilities of videoconferences hosted on the Avaya Scopia® XT Series SMB Edition by enabling Scopia® XT Desktop Clients and Scopia® Mobile devices to join.

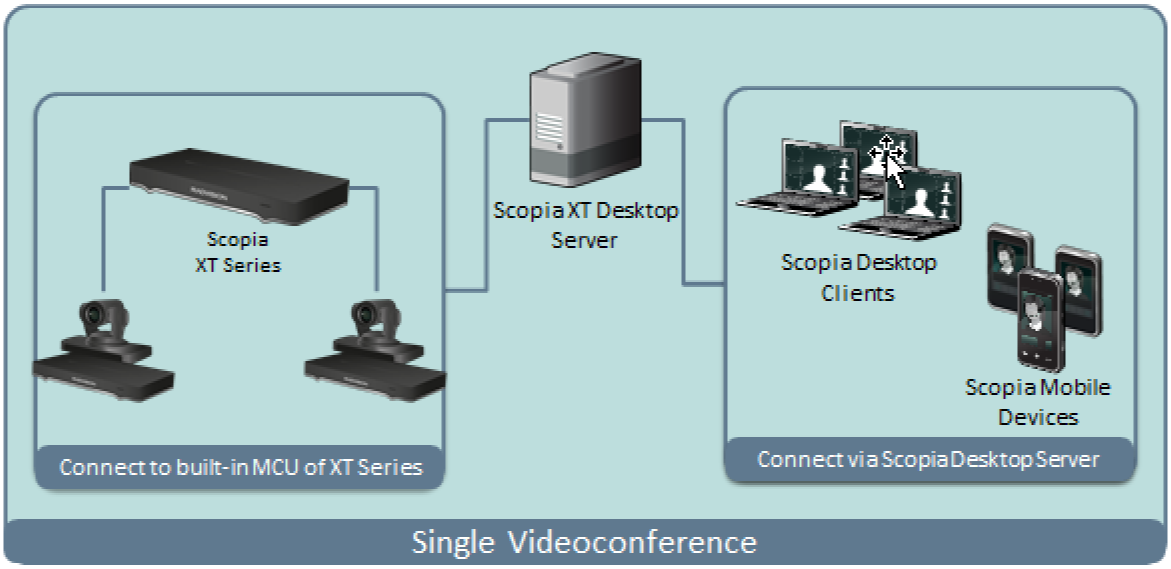


Figure 1: Scopia® XT Desktop server extends meetings to include Scopia® XT Desktop Clients

The Avaya Scopia® XT Series SMB Edition solution is especially suited to the communication requirements of Small and Medium Businesses (SMB). Built on the XT Series HD room system, with the highest capacity embedded MCU in the industry today, the Avaya Scopia® XT Series SMB Edition combines HD room system capabilities, embedded multi-party conferencing, desktop conferencing and firewall traversal into the only integrated solution of its kind available.

About Components of the Scopia® XT Desktop server

Scopia® XT Desktop server includes several different servers, each fulfilling its own function.

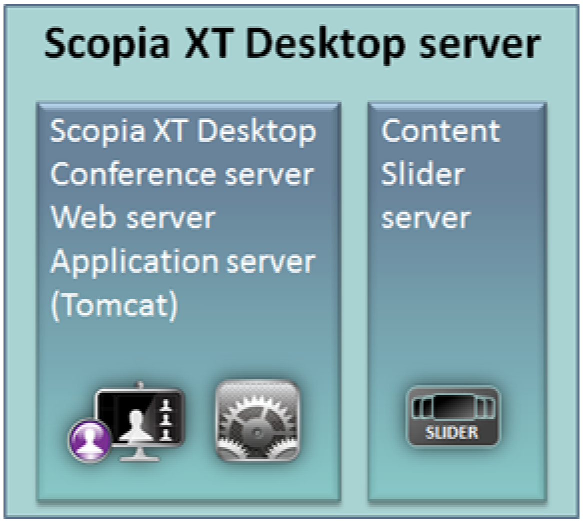

Scopia XT Desktop server
Scopia XT Desktop Conference server Web server Application server (Tomcat)
Content Slider server
SLIDER

Figure 2: Components of the Scopia® XT Desktop server

- Scopia® XT Desktop Conference Server

  At the center of Scopia® XT Desktop server, the conference server creates conferences with Scopia® XT Desktop Clients and Scopia® Mobile devices, relaying media to the MCU to enable transparent connectivity with H.323 and SIP endpoints.

- Scopia® XT Desktop Application Server (Tomcat)

  The underlying Scopia® XT Desktop web server and application server is implemented by Tomcat. It serves as the update server, the Scopia® Content Slider server and the Scopia® XT Desktop web portal.

- Scopia® Content Slider server

  Part of the Tomcat Application Server, it stores the data already presented in the videoconference and makes it available for participants to view during the meeting.

Chapter 2 | Planning your Scopia® XT Desktop server Deployment

When planning your Scopia® XT Desktop server deployment, consider the following:

- Will most Scopia® XT Desktop Clients connect to videoconferences from within the enterprise, or from outside? For example, if there are many internal Scopia® XT Desktop Clients, consider placing a dedicated Conference Server in the enterprise.
- What is your network's security policy?

  Depending on where you deploy the Scopia® XT Desktop server and other video network devices, you may need to open different ports on the firewall.
- How much internal and external bandwidth is required, based on the number of simultaneous users joining videoconferences? Consider also whether most users will be joining in standard or high definition.

See the following sections for details on the different deployment options and how to plan your bandwidth:

Navigation

Minimum Requirements and Specifications of Scopia® XT Desktop server

This section details the system specifications of your Scopia® XT Desktop server. Refer to this data when preparing system setup and afterwards as a means of verifying that the environment still complies with these requirements.

Scopia® XT Desktop server Software Requirements

The minimum software requirements for the Scopia® XT Desktop server are:

Operating systems:

- Windows® 2012 Server and Windows® 2012 R2 Server
- Windows® 2008 SP2 or Windows® 2008 R2, 32 and 64 bit (English, Japanese)
- Windows 7 Professional

Important:

Scopia® XT Desktop servers can be deployed using the VMware Sphere v5 virtual machine.

Web browsers (for the Scopia® XT Desktop server Administration):

Scopia® XT Desktop is tested with the latest internet browser versions available at the time of release.

- Internet Explorer 6 or later (Windows)
- Firefox 25 or later (Mac and Windows)
- Safari 5 or later (Mac and Windows)
- Google Chrome 30 or later (Mac and Windows)

Scopia® XT Desktop server Hardware Requirements

The minimum hardware requirements for Scopia® XT Desktop server are:

- Intel® Core™ i3 Processor, 2GHz and up
- 4 GB or more RAM

Scopia® XT Desktop server Audio and Video Specifications

Scopia® XT Desktop interoperates with both SIP and H.323 endpoints to provide a seamless user experience joining the ease of use of Scopia® XT Desktop Clients and Scopia® Mobile devices with dedicated endpoints like Scopia® XT Executive and the Avaya Scopia® XT Series.

- Audio support:
    - G.722.1 codec
    - DTMF tone detection (in-band, H.245 tones, and RFC2833)
- Video support:
    - High Definition (HD) Continuous Presence video with a maximum resolution of 720p at 30 frames per second (fps).
    - Video codec: H.264 with SVC (Scalable Video Coding) and H.264 High Profile
    - Video send resolutions: Up to HD 720p
    - Video receive resolution: HD 720p
    - Video bandwidth: HD up to 4Mbps for 720p resolutions; standard definition up to 448 kbps for 352p or lower
    - Presentation video: H.239 dual stream
    - Scopia® Content Slider can function with presentation set to H.263 or H.264 on the MCU.

Scopia® XT Desktop server Security Specifications

Scopia® XT Desktop server has extensive support for security inside private networks as well as across sites. In addition to a proprietary secure protocol between the client and server, Scopia® XT Desktop server has the following security specifications:

- Using HTTPS protocol for protecting signaling, management and media over TCP data streams between Scopia® XT Desktop Client/Scopia® Mobile and Scopia® XT Desktop server.
- Using SRTP encryption for protecting media over UDP data stream between Scopia® XT Desktop Client/Scopia® Mobile and Scopia® XT Desktop server.

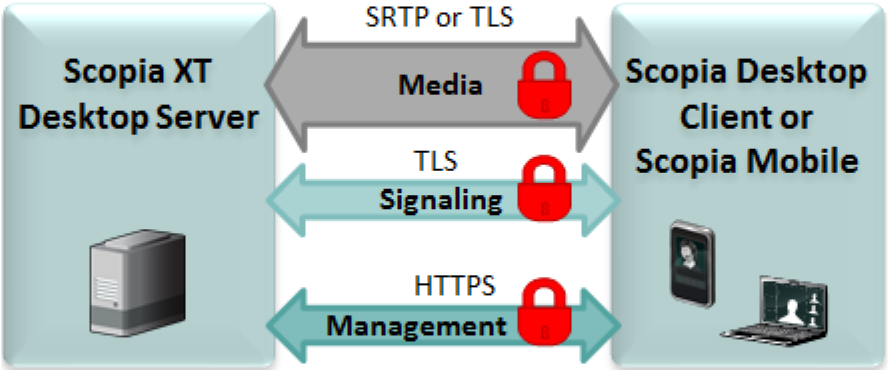


Figure 3: Securing Scopia® XT Desktop server communications

Planning the Topology of Avaya Scopia® XT Series with Scopia® XT Desktop

Avaya Scopia® XT Series SMB Edition enables you to locally host videoconferences using its built-in MCU, and extends your videoconferences to participants joining from a computer (with Scopia® XT Desktop Client) or a mobile device (using Scopia® Mobile).

For example, when you start a videoconference with the XT Series hosting the call, you can add other participants by asking them to connect via a web link to the Scopia® XT Desktop server, which would automatically install and launch Scopia® XT Desktop Client on their computers, or Scopia® Mobile on their mobile devices.

If you do not register to IP Office, you cannot host videoconferences on the built-in MCU.

The main features of the Avaya Scopia® XT Series SMB Edition include:

- Remote users can easily connect to a meeting hosted by the built-in MCU on the XT Series, by connecting via the Scopia® XT Desktop server.

  The deployment has very few components. You do not need additional hardware like an external MCU, Avaya Scopia® PathFinder for firewall traversal, or Avaya Scopia® ECS Gatekeeper for routing calls.
- The included Scopia® XT Desktop provides built-in NAT and firewall traversal functionality, enabling secure remote connections from Scopia® Mobile and Scopia® XT Desktop Clients.

The Avaya Scopia® XT Series SMB Edition includes the following:

- Full SMB9 - Advanced MCU level, with one local participant and up to eight remote endpoints or PC clients.

There is no local endpoint if you deploy the XT Series as a server.

Figure 4: Avaya Scopia® XT Series SMB Edition Deployment on page 10 shows a typical topology for the Avaya Scopia® XT Series SMB Edition solution. For more information, see the *Solution Guide for Scopia® Solution*.

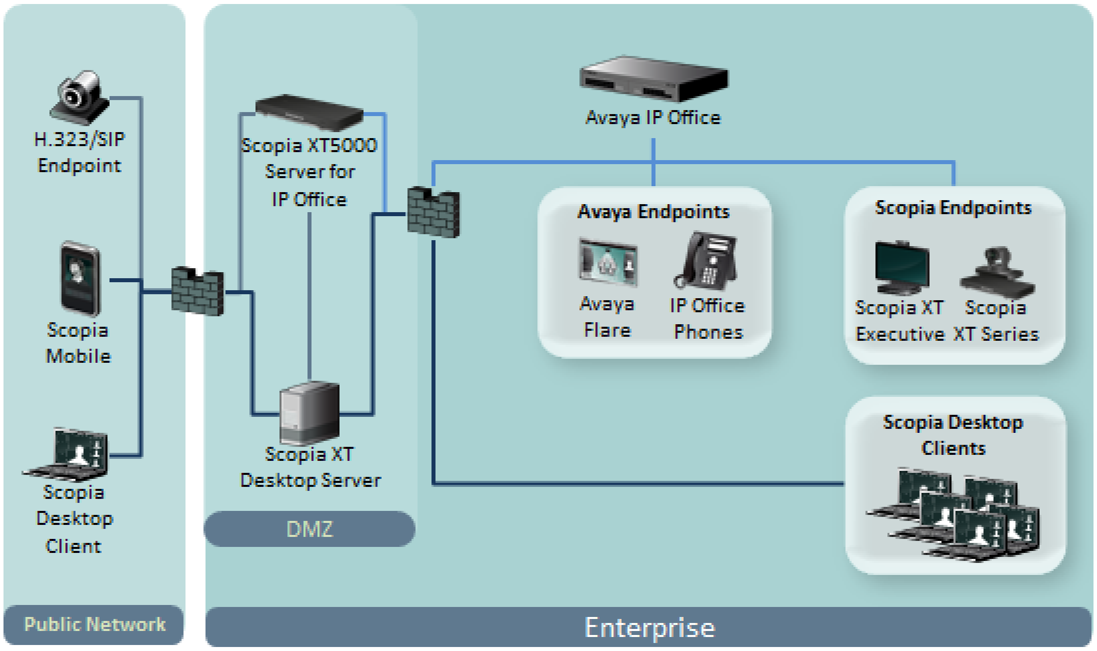


Figure 4: Avaya Scopia® XT Series SMB Edition Deployment

As you add more XT Series endpoints, you can also manage them centrally with Scopia® Management. This would enable centralized updating, backing up and control.

Deploying Scopia® XT Desktop server with Dual-NIC

Scopia® XT Desktop server can be installed on servers with multiple Network Interface Cards (NICs). Depending on the deployment and network configuration, you may want to control which NIC is used for various server communications.

Important:

The minimum requirement is to use a 100 Mbit NIC. It is recommended that you use a Gigabyte NIC for better performance. Bandwidth shown is for Standard Definition (384 kbps) or High Definition (1024 kbps).

For example, in secure multiple NIC deployments you can use a NIC configured behind the firewall to communicate with the Avaya Scopia® XT Series, while using another NIC for Scopia® XT Desktop Client connections (Figure 5: Scopia® XT Desktop server with a dual-NIC deployment on page 11). In this case, configure the Scopia® XT Desktop IP address to represent the NIC behind the firewall. For the

Scopia® XT Desktop public address, use a DNS name which resolves to the NIC outside the firewall, and is accessible both inside and outside the enterprise.

For more information and to configure the public address, see Defining Scopia® XT Desktop server Public Address and Other Client Connection Settings on page 29.

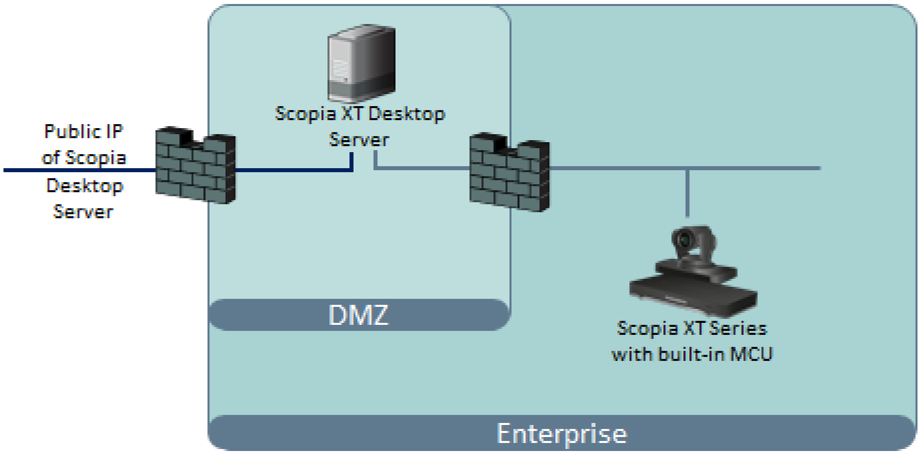

Public IP of Scopia Desktop Server
Scopia XT Desktop Server
DMZ
Scopia XT Series with built-in MCU
Enterprise

Figure 5: Scopia® XT Desktop server with a dual-NIC deployment

Scopia® XT Desktop Clients can connect to the Scopia® XT Desktop server either by an IP address or a DNS name. In many deployments the Scopia® XT Desktop server IP address is not accessible to clients outside the enterprise due to NAT or firewall restrictions. Therefore, Scopia® XT Desktop server has a public address, which must be a DNS name resolving to the correct Scopia® XT Desktop server IP address both inside and outside the corporate network.

Estimating and Planning your Bandwidth Requirements

We recommend estimating Scopia® XT Desktop's impact on bandwidth to determine if your current infrastructure needs updating. Planning bandwidth may help reduce costs in your organization.

This section explains how to estimate the bandwidth for external Scopia® XT Desktop users connecting to your network.

Important:

You do not need to estimate bandwidth required by users who connect from within the internal network, because, typically, internal bandwidth is sufficient for videoconferencing.

You can allocate the bandwidth depending on the needs of your organization.

To assess the overall bandwidth for the videoconferencing solution including other types of endpoints, refer to the Avaya Scopia® Solution Guide.

Calculating the Bandwidth Used by Scopia® XT Desktop Participants

About this task

Videoconference participants consume most of the bandwidth in your Avaya Scopia® XT Desktop deployment, because they both upload and download live media.

Important:

You do not need to estimate bandwidth required by users who connect from within the internal network, because, typically, internal bandwidth is sufficient for videoconferencing.

The amount of bandwidth consumed by participants mainly depends on the chosen topology and the maximum bandwidth you allow per participant. You configure the maximum bandwidth per participant in the Scopia® XT Desktop server which is the maximum possible bandwidth for any participant connecting to this server.

You calculate the maximum bandwidth used by Scopia® XT Desktop participants in the following steps:

Procedure

1. Estimate the number of Scopia® XT Desktop participants connecting externally, as shown in Figure 1:

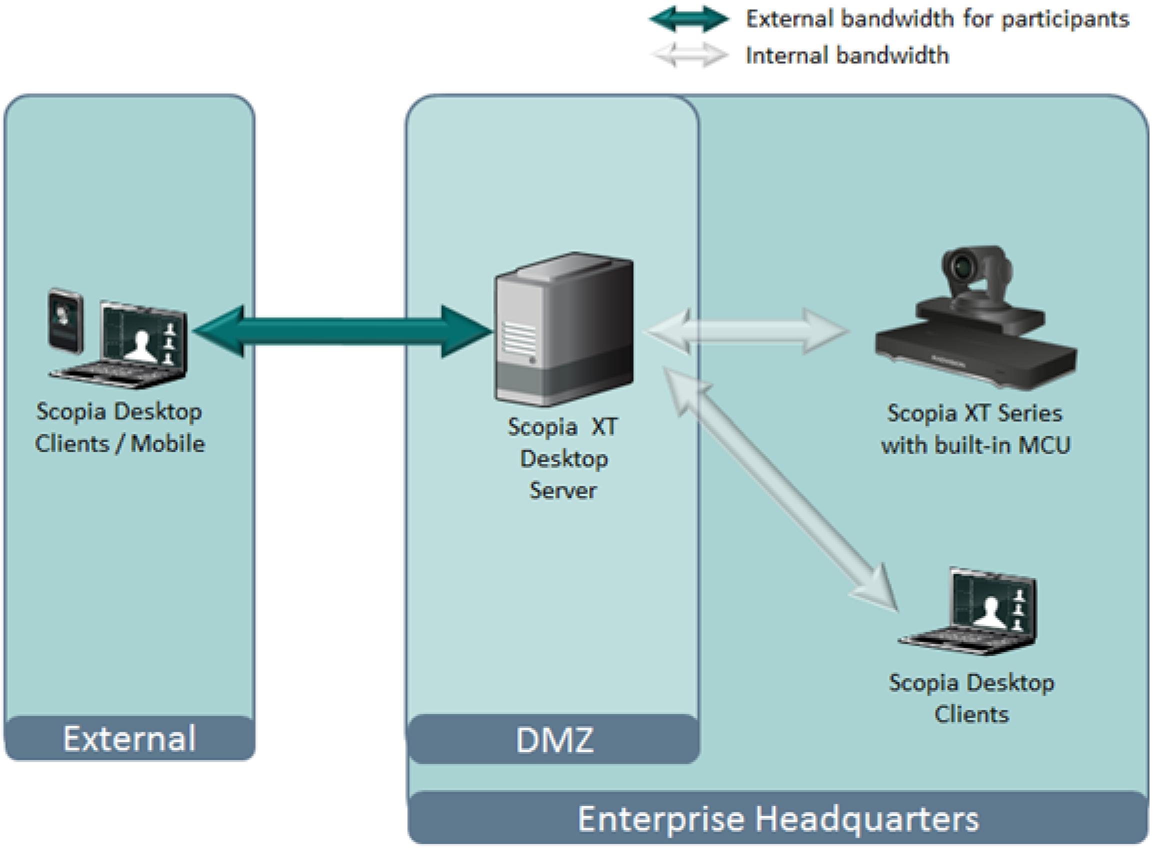

External bandwidth for participants
Internal bandwidth
Scopia Desktop Clients / Mobile
Scopia XT Desktop Server
Scopia XT Series with built-in MCU
Scopia Desktop Clients
External
DMZ
Enterprise Headquarters

Figure 6: External bandwidth required for centralized deployments

2. Decide on the maximum bandwidth per Scopia® XT Desktop Client (measured as its bitrate).
3. Calculate the peak bandwidth according to the following formula:

```
Peak bandwidth = maximum number of participants x maximum
bandwidth per participant
```

   The maximum number of participants in a meeting depends on the license deployed on the XT Series with built-in MCU.

   For example, if the chosen maximum bandwidth is 768 Kbps and the maximum number of participants is 9,the peak bandwidth equals 6912 kbps. This is the rough estimation of the bandwidth required for videoconference participants.

4. Add margins to make sure that even in poor network conditions video quality does not drop below the standard you decided on.

   Important:

   An average margin is 20% of your fine-tuned estimation.

Ports to Open on Scopia® XT Desktop

The Scopia® XT Desktop server is typically located in the DMZ (see Figure 7: Locating the Scopia® XT Desktop server in the DMZ on page 14) and is therefore connected to both the enterprise and the public networks. Scopia® XT Desktop Clients can be located in the internal enterprise network, in the public network, or in a partner network.

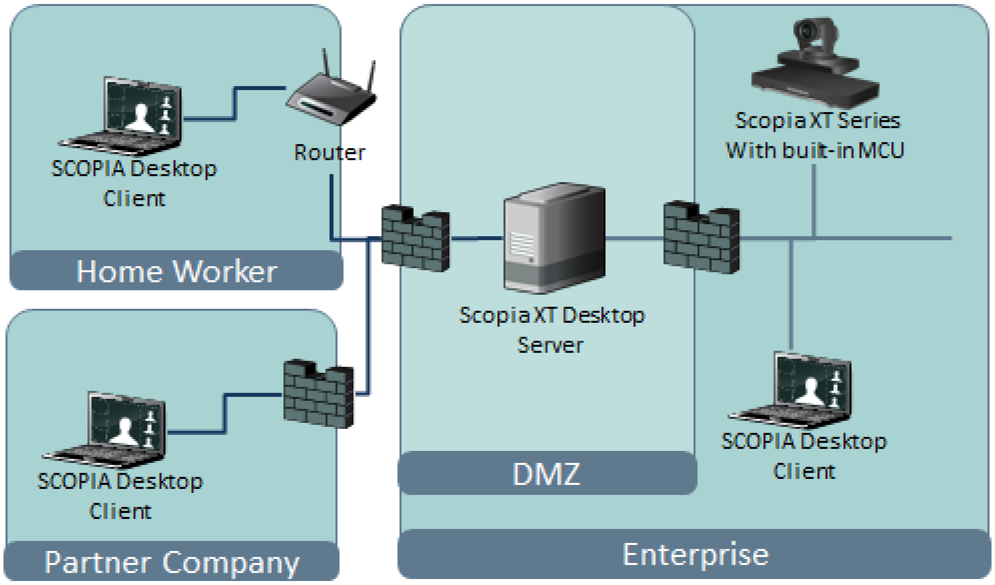


Figure 7: Locating the Scopia® XT Desktop server in the DMZ

When opening ports between the DMZ and the enterprise on the Scopia® XT Desktop server, use the following as a reference:

- When opening ports that are both in and out of the Scopia® XT Desktop server, see Table 1: Bidirectional Ports to Open Between the Scopia® XT Desktop server and the Enterprise on page 15.
- When opening ports that are outbound from the Scopia® XT Desktop server, see Table 2: Outbound Ports to Open from the Scopia® XT Desktop server to the Enterprise on page 15.
- When opening ports that are inbound to the Scopia® XT Desktop server, see Table 3: Inbound Ports to Open from the Enterprise to the Scopia® XT Desktop server on page 16.

When opening ports between the DMZ and the public on the Scopia® XT Desktop server, use the following as a reference:

- When opening ports that are both in and out of the Scopia® XT Desktop server, see Table 4: Bidirectional Ports to Open Between the Scopia® XT Desktop server and the Public on page 16.
- When opening ports that are inbound from the Scopia® XT Desktop server, see Table 5: Inbound Ports to Open from the Public to the Scopia® XT Desktop server on page 17.

Important:

The specific firewalls you need to open ports on depends on where your Scopia® XT Desktop and other Scopia® Solution products are deployed.

Table 1: Bidirectional Ports to Open Between the Scopia® XT Desktop server and the Enterprise

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
1024- 65535	TCP (H.245/ Q.931)	Avaya Scopia® XT Series SMB Edition	Enables connection to Scopia® XT Desktop meetings.	Cannot connect to the meeting	Mandatory To limit range, see Limiting the TCP Port Range for H.245/Q.931 on the Scopia® XT Desktop server on page 18
10000-65535	UDP (RTP)	Avaya Scopia® XT Series SMB Edition or Scopia® XT Desktop Client	Enables media connection to the Avaya Scopia® XT Series SMB Edition, and the Scopia® XT Desktop Client or Scopia® Mobile.	Media cannot be passed from the Avaya Scopia® XT Series SMB Edition to Scopia® XT Desktop Clients. Also, connection is tunneled via TCP port 443 resulting in a drop in performance.	Mandatory To limit range, see Limiting the UDP Port Range for RTP/RTCP on the Scopia® XT Desktop server on page 17

Table 2: Outbound Ports to Open from the Scopia® XT Desktop server to the Enterprise

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
1720	TCP	Avaya Scopia® XT Series SMB Edition	Enables connection to Scopia® XT Desktop meetings.	Cannot connect to the meeting	Mandatory
3337	TCP (XML)	Avaya Scopia® XT Series SMB Edition	Enables meeting cascading connection to the Avaya Scopia® XT Series SMB Edition	Meeting cascading connection is disabled	Mandatory
3336	TCP	Avaya Scopia® XT Series SMB Edition	Enables meeting control with Avaya Scopia® XT Series SMB Edition	Meeting control is disabled	Mandatory

Table 3: Inbound Ports to Open from the Enterprise to the Scopia® XT Desktop server

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
80	TCP (HTTP)	Web client	Provides access to the Scopia® XT Desktop server Web Portal (you can configure port 443 instead)	Cannot access the Scopia® XT Desktop server Web Portal	Mandatory if using HTTP. You can configure this port during installation. For more information, see Installing the Scopia® XT Desktop server.
443	TCP (TLS)	Scopia® XT Desktop Clients and Scopia® Mobile	Enables sending control messages between the Scopia® XT Desktop server and Clients, and is also used to tunnel RTP media if the UDP ports are blocked	Scopia® XT Desktop Client or Scopia® Mobile cannot connect to the Scopia® XT Desktop server	Mandatory

Table 4: Bidirectional Ports to Open Between the Scopia® XT Desktop server and the Public

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
10000-65535	UDP (RTP/ RTCP)	Scopia® XT Desktop Client or Scopia® Mobile	Enables media connection with the Scopia® XT Desktop Client or Scopia® Mobile	Connection is tunneled via TCP port 443 and performance is not optimal	Recommended To configure, see Limiting the UDP Port Range for RTP/RTCP on the Scopia® XT Desktop server on page 17

Table 5: Inbound Ports to Open from the Public to the Scopia® XT Desktop server

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
80	TCP (HTTP)	Web client	Provides access to the web user interface (you can configure port 443 instead)	Cannot access the web user interface	Mandatory if using HTTP. You can configure this port during installation. For more information, see Installing the Scopia® XT Desktop server.
443	TCP (TLS)	Scopia® XT Desktop Clients and Scopia® Mobile	Enables sending control messages between the Scopia® XT Desktop server and Clients, and is also used to tunnel RTP media if the UDP ports are blocked	Scopia® XT Desktop Clients cannot connect to the Scopia® XT Desktop server	Mandatory

Limiting Port Ranges on the Scopia® XT Desktop server

About this task

This section provides instructions of how to limit the following port ranges on the Scopia® XT Desktop server:

Navigation

- Limiting the UDP Port Range for RTP/RTCP on the Scopia® XT Desktop server on page 17
- Limiting the TCP Port Range for H.245/Q.931 on the Scopia® XT Desktop server on page 18

Limiting the UDP Port Range for RTP/RTCP on the Scopia® XT Desktop server

About this task

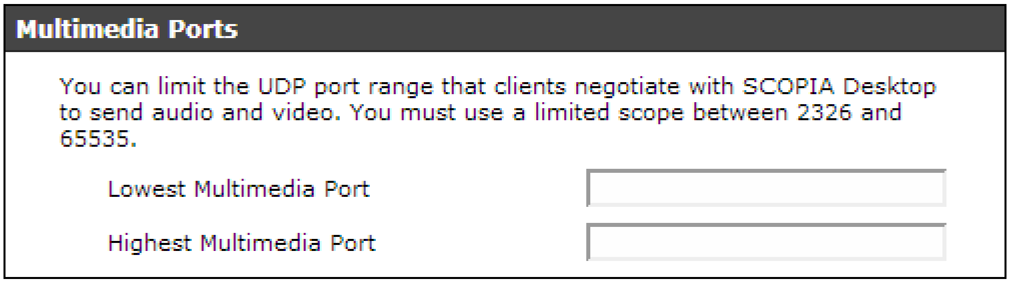
The Scopia® XT Desktop server has designated 10000-65535 as the default port range for UDP (RTP/RTCP). To provide additional security for your firewall, you can limit this range.

To calculate approximately how many ports the Scopia® XT Desktop server uses, multiply the number of license connections by 14, which amounts to reserving 14 ports per client.

Procedure

1. Log in to the Scopia® XT Desktop server Administrator web user interface.
2. Select **Client > Settings.**

3. Locate the **Multimedia Ports** section (see Figure 8: Multimedia Ports Area on page 18).



Multimedia Ports

You can limit the UDP port range that clients negotiate with SCOPIA Desktop to send audio and video. You must use a limited scope between 2326 and 65535.

Lowest Multimedia Port

Highest Multimedia Port

Figure 8: Multimedia Ports Area

4. Configure your port range (using any values between 2326 and 65535) by doing the following:

   a. Enter the base port value in the **Lowest Multimedia Port** field.

   b. Enter the upper port value in the **Highest Multimedia Port** field.

5. Select **OK** or **Apply**.

Limiting the TCP Port Range for H.245/Q.931 on the Scopia® XT Desktop server

About this task

The Scopia® XT Desktop server has designated ports 1024-65535 for TCP for H.245 and Q.931 signaling. To provide additional security for your firewall, you can limit this range.

For each conference, the Scopia® XT Desktop server uses 2 ports. In addition, add extra ports for:

- Add 2 ports for each participating Scopia® XT Desktop Client client.
- Add 1 port per conference when presenting using the content slider.

Procedure

1. Navigate to *<Scopia® XT Desktop install_dir>\ConfSrv*.

2. Edit the *config.val* file as follows:

   a. Locate the text `1 system`.

   b. At the bottom of that section, add two lines:

```
2 portFrom = <lowest range limit>
2 portTo = <highest range limit>
```

Where `<lowest range limit>` is the base port of your port range and `<highest range limit>` is the upper value of your port range.

3. Access the Windows services and restart the **Scopia® XT Desktop - Conference Server** service.

Chapter 3 | Installing the Scopia® XT Desktop server

About this task

Follow these recommendations when installing the Scopia® XT Desktop server components:

- Do not install the Scopia® XT Desktop Client on the same PC as any Scopia® XT Desktop component.
- If you want to encrypt communication with HTTPS, configure the Conference Server for Scopia® XT Desktop to port 443 after the installation is completed (see *Administrator Guide for Scopia Desktop Server*).

> ❗ **Important:**
>
> Using encryption is subject to local regulation. In some countries it is restricted or limited for usage. For more information, consult your local reseller.

Follow this procedure to install the Scopia® XT Desktop server.

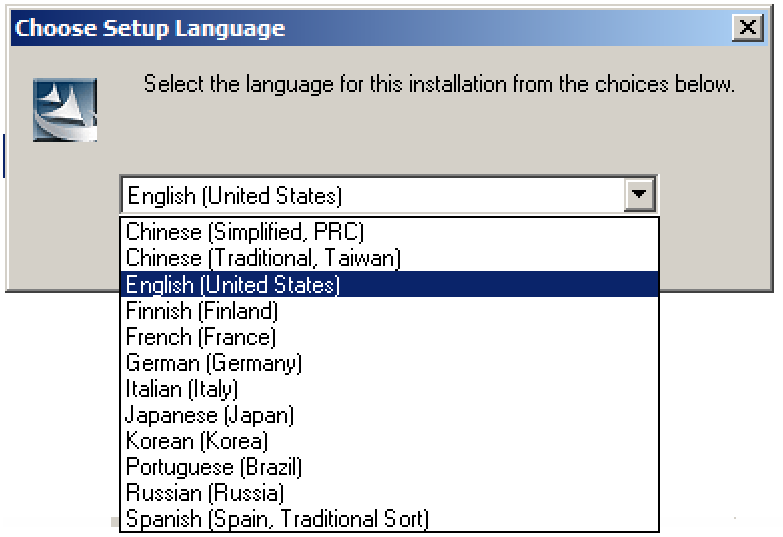
Before you begin

To enable Scopia® XT Desktop to work with the Avaya Scopia® XT Series, your XT Series must have two licenses: an MCU license and a Scopia® XT Desktop license.

- Before installing, verify the computer meets the minimum hardware requirements for the number of intended users. For more information, see Minimum Requirements and Specifications of Scopia® XT Desktop server on page 7.
- By default, Scopia® XT Desktop Clients access the Scopia® XT Desktop server via port 80. If other applications on this PC use port 80, and you nevertheless want to use this port, access the Services panel in Windows and disable the IIS Administration, HTTP SSL, and World Wide Web Publishing services before installing the Conference Server.

Procedure

1. Launch the *setup.exe* file to start the Scopia® XT Desktop Setup Wizard.
2. Select the installation language in the **Choose Setup Language** window, and select **OK**.



Choose Setup Language

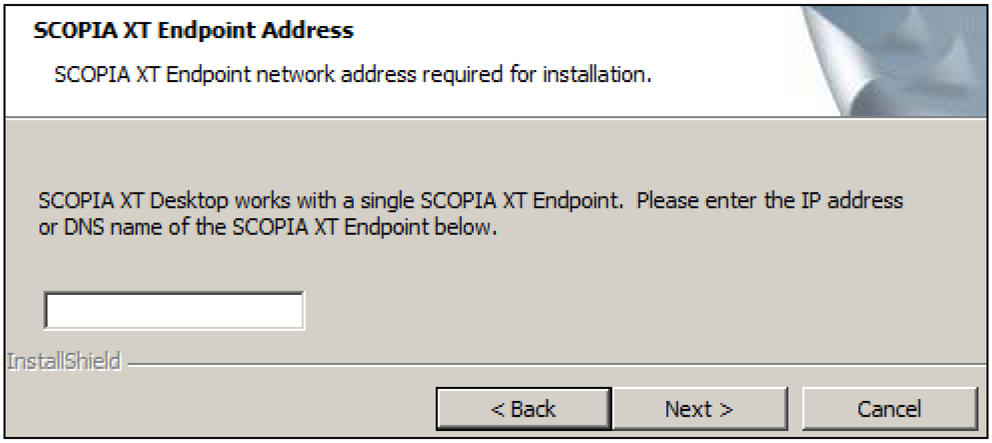
Select the language for this installation from the choices below.

English (United States)

Figure 9: Choosing language for the installation

3. Select **Next** and accept the license agreement.

4. Enter the IP address or DNS name of the Avaya Scopia® XT Series SMB Edition which hosts videoconferences with its built-in MCU in the **XT Series Address** window, and select **Next**.



SCOPIA XT Endpoint Address

SCOPIA XT Endpoint network address required for installation.

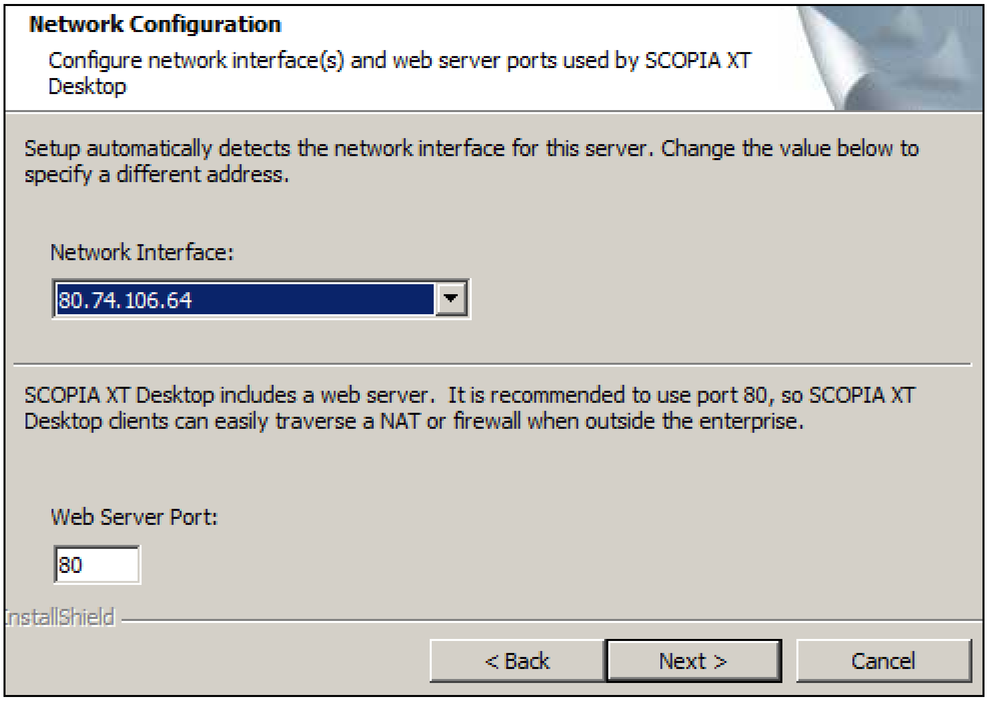
SCOPIA XT Desktop works with a single SCOPIA XT Endpoint. Please enter the IP address or DNS name of the SCOPIA XT Endpoint below.

Figure 10: Specifying the XT Series with built-in MCU

5. Change the installation folder if required, and select **Next**.

6. In the **Network Configuration** window, select the IP address used for communicating with the Avaya Scopia® XT Series SMB Edition.

   If the server has one NIC card, the **Network Interface** field has only one value to choose, the IP of the NIC. For dual-NIC servers, select the network IP address pointing to the internal firewall. For more information on dual-NIC setups, see Deploying Scopia® XT Desktop server with Dual-NIC on page 10.



Network Configuration

Configure network interface(s) and web server ports used by SCOPIA XT Desktop

Setup automatically detects the network interface for this server. Change the value below to specify a different address.

Network Interface: 80.74.106.64

SCOPIA XT Desktop includes a web server. It is recommended to use port 80, so SCOPIA XT Desktop clients can easily traverse a NAT or firewall when outside the enterprise.

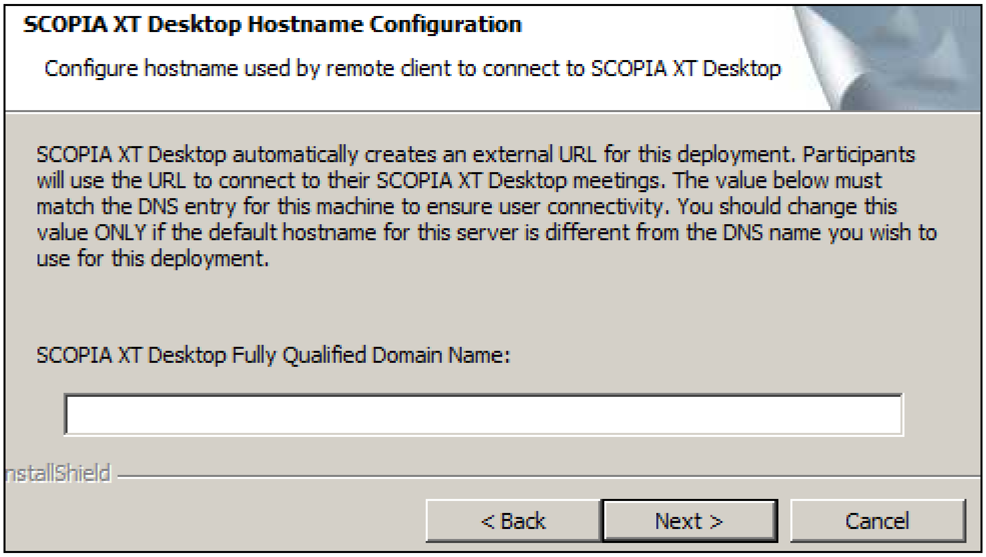
Web Server Port: 80

Figure 11: Selecting the NIC pointing to the internal network

7. Change the default web server port if required, and then select **Next**.

   For more information on port changes, see Ports to Open on Scopia® XT Desktop on page 13.

8. In the **Hostname Configuration** window specify the public name of the Scopia® XT Desktop server, to be used later as part of the URL sent to Scopia® XT Desktop Clients to connect to videoconferences.



SCOPIA XT Desktop Hostname Configuration

Configure hostname used by remote client to connect to SCOPIA XT Desktop

SCOPIA XT Desktop automatically creates an external URL for this deployment. Participants will use the URL to connect to their SCOPIA XT Desktop meetings. The value below must match the DNS entry for this machine to ensure user connectivity. You should change this value ONLY if the default hostname for this server is different from the DNS name you wish to use for this deployment.

SCOPIA XT Desktop Fully Qualified Domain Name:

Figure 12: Defining the public address of the Scopia® XT Desktop server

Important:

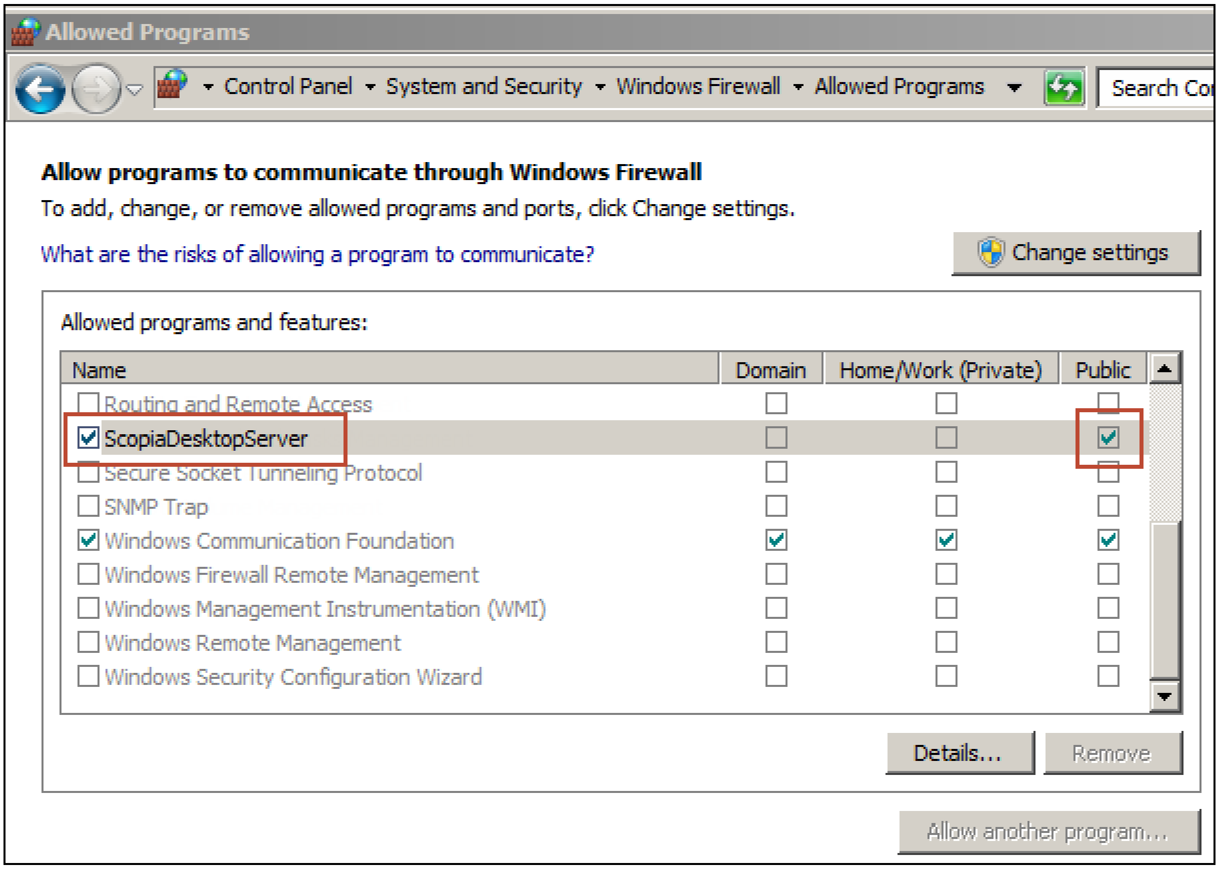
An external Scopia® XT Desktop Client must be able to resolve the server's hostname to the correct IP address from its location outside the enterprise. For example, do not use an internal DNS name if you have clients connecting from the public Internet.

9. Select **Install** in the **Ready to Install the Program** window.

10. Select **Finish**.

11. If the local Windows Firewall is active on the Scopia® XT Desktop server, two core services which must have permission to communicate through the firewall. Navigate to the Windows Firewall Control Panel (Figure 13: Enabling public access for essential services on page 23) and enable the following programs:

    - **Commons Daemon Service Runner**, located at <*install_dir*>*tomcat**bin**tomcat7.exe*.
    - **ScopiaDesktopServer**, located at <*install_dir*>*ConfSrv**ConfSrv.exe*



Allow programs to communicate through Windows Firewall

To add, change, or remove allowed programs and ports, click Change settings.

What are the risks of allowing a program to communicate?

Allowed programs and features:

Name	Domain	Home/Work (Private)	Public
□ Routing and Remote Access	□	□	□
☑ ScopiaDesktopServer	□	□	☑
□ Secure Socket Tunneling Protocol	□	□	□
□ SNMP Trap	□	□	□
☑ Windows Communication Foundation	☑	☑	☑
□ Windows Firewall Remote Management	□	□	□
□ Windows Management Instrumentation (WMI)	□	□	□
□ Windows Remote Management	□	□	□
□ Windows Security Configuration Wizard	□	□	□

Figure 13: Enabling public access for essential services

Chapter 4 | Configuring Your Deployment

This section describes how to access the Scopia® XT Desktop Administration web interface, configure your Scopia® XT Desktop, define a local administrator account, and verify that the Avaya Scopia® XT Series SMB Edition and Scopia® XT Desktop are successfully connected.

Navigation

Accessing the Scopia® XT Desktop server Web Administration Interface

About this task

The Scopia® XT Desktop server web administration interface is a web-based application to configure the settings of your Scopia® XT Desktop server.

Perform this procedure to access the administration web interface.

Procedure

1. Access the Scopia® XT Desktop server Administration web interface in a browser at *http://<server_name>/scopia/admin*

   where <*server_name*> is the FQDN of your Scopia® XT Desktop server. If you have deployed a non-standard port to access the Scopia® XT Desktop server, enter the port number in the standard way: <*server_name*>*:*<*port_number*>. If you have implemented secure access to the server, use the *https://* prefix.

2. Enter your username and password.

The default username is **admin** and the password is **admin**.

3. Select **Sign In**.

Defining an Administrator Account

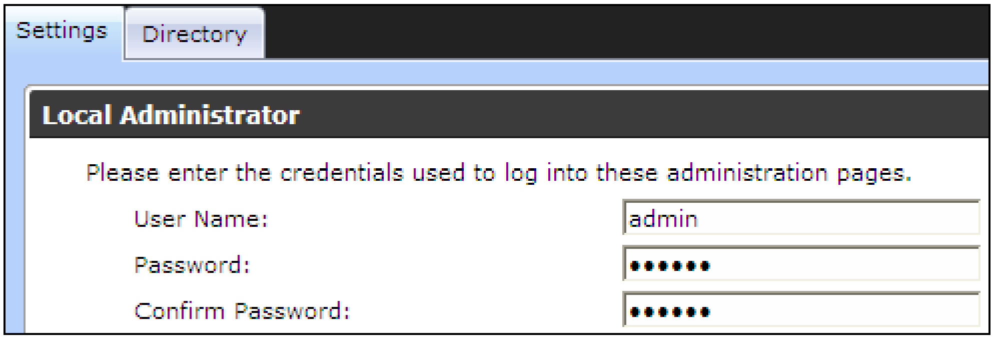
About this task

You can define a username and password for an administrator to access Scopia® XT Desktop server Administration web interface.

Procedure

1. Select **Directory and Authentication** in the sidebar.

   The **Settings** tab is displayed.



Local Administrator

Please enter the credentials used to log into these administration pages.

User Name: admin

Password: ••••••

Confirm Password: ••••••

Figure 14: Configuring the local administrator credentials

2. Enter a **User Name** and **Password** in the **Local Administrator** section.
3. Select **OK**.

Connecting Scopia® XT Desktop with the XT Series

About this task

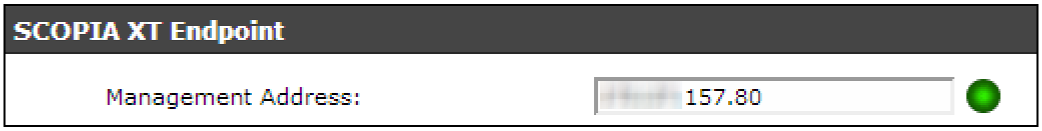
This section describes how to connect the Scopia® XT Desktop server with the Avaya Scopia® XT Series SMB Edition with its built-in MCU.

Procedure

1. Access the Scopia® XT Desktop server administration web interface.

2. Select **Deployment** in the sidebar.

3. Enter the IP address of the XT Series with its built-in MCU in the **Management Address** field.



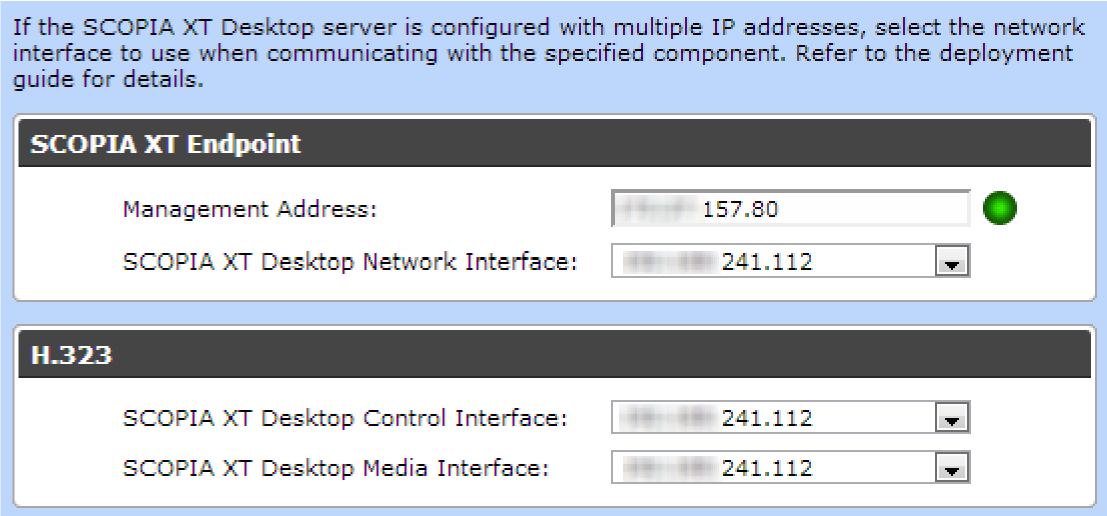
SCOPIA XT Endpoint

Management Address: [redacted]157.80

Figure 15: Setting the address of the managing Avaya Scopia® XT Series

4. For dual-NIC deployments only, select the correct NIC address from the drop-down menu for the following fields:

Field	Description
Scopia® XT Desktop Network Interface	Select the NIC address used to communicate management messages with the Avaya Scopia® XT Series, like configuring via the administration web interface.
Scopia® XT Desktop Control Interface	Select the NIC address used for signaling and control in your deployment, such as call routing, establishing media channels (codecs), starting presentations, and so on.
Scopia® XT Desktop Media Interface	Select the NIC address used to transmit the actual audio and video media.



If the SCOPIA XT Desktop server is configured with multiple IP addresses, select the network interface to use when communicating with the specified component. Refer to the deployment guide for details.

SCOPIA XT Endpoint

Management Address: [redacted]157.80

SCOPIA XT Desktop Network Interface: [redacted]241.112

H.323

SCOPIA XT Desktop Control Interface: [redacted]241.112

SCOPIA XT Desktop Media Interface: [redacted]241.112

Figure 16: Configuring a dual-NIC Scopia® XT Desktop server

5. Select **OK**.

Verifying Scopia® XT Desktop server Installation and Connection with Other Components

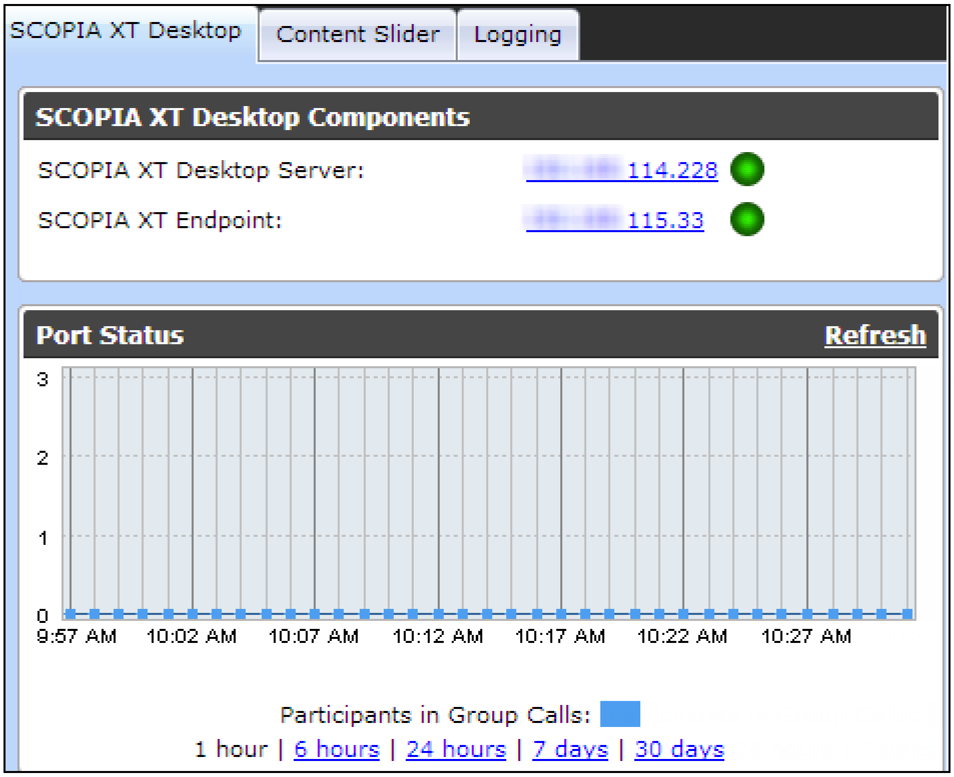
About this task

The Scopia® XT Desktop Administrator web interface displays the connectivity status of your deployment. The indicators next to each link shows whether or not the connection or registration to the target server is successful. When the indicator is red, hover over the indicator to view the tooltip containing the error details.

Procedure

1. To verify that Scopia® XT Desktop Server is connected to the Avaya Scopia® XT Series, select **Status** in the sidebar.

2. View the connection status for each server or component. If necessary, select any red indicators to view further error information.



SCOPIA XT Desktop Components

SCOPIA XT Desktop Server: [redacted]114.228 ●

SCOPIA XT Endpoint: [redacted]115.33 ●

Port Status

Refresh
3
2
1
0
9:57 AM
10:02 AM
10:07 AM
10:12 AM
10:17 AM
10:22 AM
10:27 AM
Participants in Group Calls: 🟦
1 hour | 6 hours | 24 hours | 7 days | 30 days

Figure 17: Viewing the connection status with Scopia® XT Desktop server

3. (Optional) View the connection status of the Scopia® Content Slider by selecting the **Content Slider** tab. For more information on the Content Slider, see About Components of the Scopia® XT Desktop server on page 5.

4. If necessary, select any red indicators to view further error information.

Defining a Local Directory of Endpoints

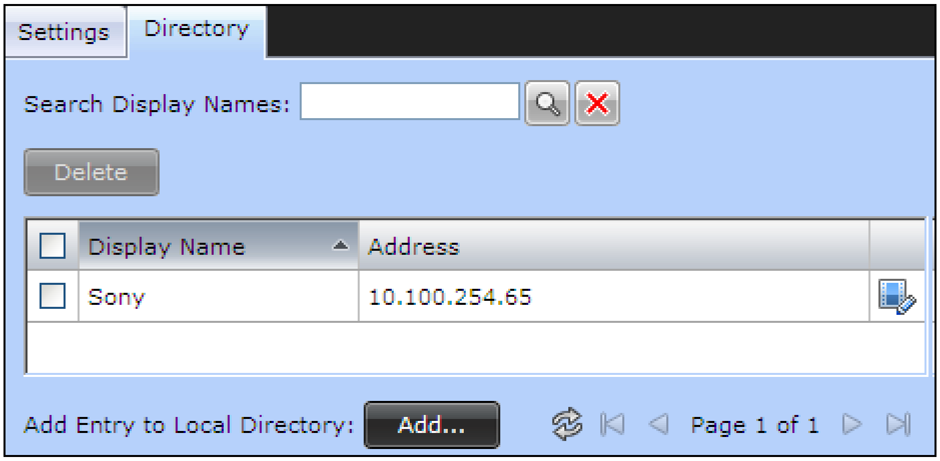
About this task

The local directory is a local database containing names and IP addresses of endpoints on the Scopia® XT Desktop server deployment. Typically, a local directory of endpoints is maintained in deployments which do not include Scopia® Management.

This list of endpoints is displayed when users select **Moderate > Invite** in their **Meeting** window in Scopia® XT Desktop Client.

Procedure

1. Access the Scopia® XT Desktop server Administration web interface.
2. Select **Directory and Authentication** icon in the sidebar.
3. Select the **Directory** tab.



□	Display Name	Address
□	Sony	10.100.254.65

Figure 18: Local database of endpoints

4. To add a new endpoint to your local directory:
   a. Select **Add**.
   b. Enter the endpoint name and IP address.
   c. Select **OK**.
5. To edit properties for an endpoint:
   a. Select the **Edit** icon next to the endpoint whose properties you want to edit.
   b. In the **Edit Entry** window, edit properties as needed.
   c. Select **OK**.
6. To delete an endpoint from the database:
   a. Select the check boxes for the endpoints you want to delete.

b. Select the **Delete** button.

Defining Bandwidth Settings in Scopia® XT Desktop server

About this task

This section details how to define the maximum bandwidth used between the Scopia® XT Desktop Client and the Scopia® XT Desktop server. Calculating the Bandwidth Used by Scopia® XT Desktop Participants explains how to assess the maximum bandwidth per Scopia® XT Desktop Client.

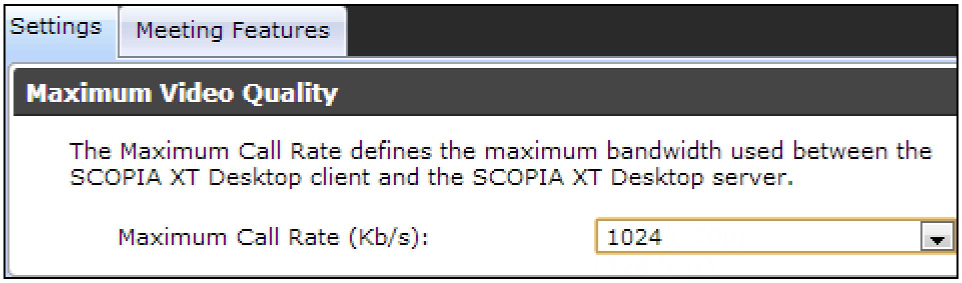
This value determines the maximum bandwidth used by a Scopia® XT Desktop participant uploading and downloading media during a videoconference. A webcast viewer uses half of this bandwidth because media is only downloaded from the Scopia® XT Desktop server when a videoconference is streamed.

Before you begin

Decide on the maximum bandwidth per Scopia® XT Desktop Client as explained in Calculating the Bandwidth Used by Scopia® XT Desktop Participants.

Procedure

1. Access the Scopia® XT Desktop server Administration web interface.
2. Select the **Client** icon in the sidebar.
3. Select the **Settings** tab.
4. Select the maximum call rate in the **Maximum Video Quality** section.



Maximum Video Quality

The Maximum Call Rate defines the maximum bandwidth used between the SCOPIA XT Desktop client and the SCOPIA XT Desktop server.

Maximum Call Rate (Kb/s): 1024

Figure 19: Setting maximum bandwidth in Scopia® XT Desktop server

Defining Scopia® XT Desktop server Public Address and Other Client Connection Settings

About this task

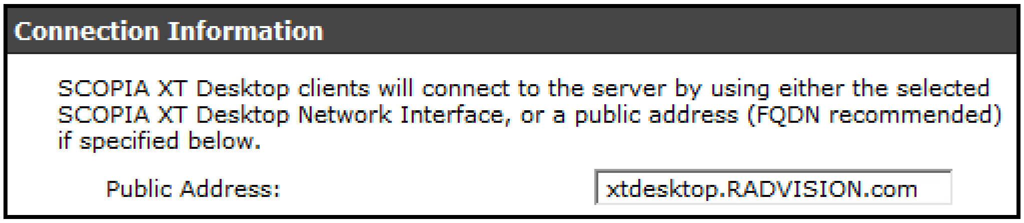
This section details how to define the public address of the Scopia® XT Desktop server, which is pushed to Scopia® XT Desktop Clients participating in a videoconference on that server.

You can also define Scopia® XT Desktop server's size of network packets (MTU size). The MTU, or Maximum Transmission Unit, is the maximum size of data packets sent around your network.

Procedure

1. Access the Scopia® XT Desktop server Administration web interface.
2. Select the **Client** icon in the sidebar.
3. Select the **Settings** tab.
4. Insert the public address of the Scopia® XT Desktop server to be accessed by the client. Use a FQDN which Scopia® XT Desktop Clients can resolve from their location, to arrive at the correct IP address of the server.

   If a DNS name is not specified in the **Public Address** field, the Scopia® XT Desktop server network interface address is used.



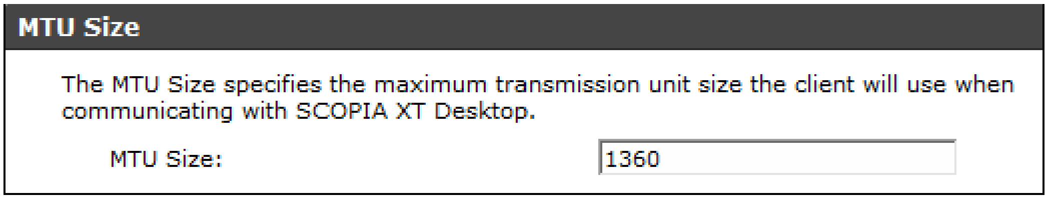
Connection Information

SCOPIA XT Desktop clients will connect to the server by using either the selected SCOPIA XT Desktop Network Interface, or a public address (FQDN recommended) if specified below.

Public Address: xtdesktop.RADVISION.com

Figure 20: The public address for Scopia® XT Desktop Clients to connect to the server

5. Define the **MTU Size** if your network routers and the XT Series are configured to accept network packets of a different size. The default value is **1360**.



MTU Size

The MTU Size specifies the maximum transmission unit size the client will use when communicating with SCOPIA XT Desktop.

MTU Size: 1360

Figure 21: Setting the MTU size for Scopia® XT Desktop Client

Important:

This value must remain the same across all network components to guard against packet fragmentation.

6. Select **OK** or **Apply**.

Enabling Scopia® XT Desktop Client Features

About this task

This section describes how to enable or disable features in the **Meeting** window of the Scopia® XT Desktop Client for all users logged in to the Scopia® XT Desktop server. You can:

- Enable or disable presentations (desktop sharing).
- Enable or disable text chat.
- Enable or disable encryption.

  Important:

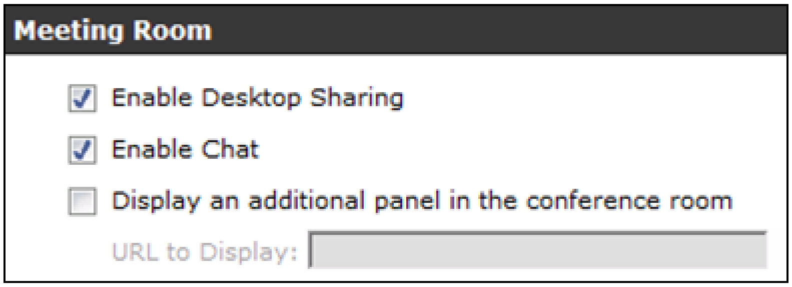
  Using encryption is subject to local regulation. In some countries it is restricted or limited for usage. For more information, consult your local reseller.

- Add a pane in the videoconferencing window containing web content for all users in your organization.

The changes you make in this procedure are global and affect all Scopia® XT Desktop Clients connecting to this Scopia® XT Desktop server.

Procedure

1. Access the Scopia® XT Desktop server Administrator web user interface, as described in Accessing the Scopia® XT Desktop server Web Administration Interface on page 24.
2. Select the **Client** icon in the sidebar.
3. Select the **Meeting Features** tab.



Meeting Room

☑ Enable Desktop Sharing

☑ Enable Chat

□ Display an additional panel in the conference room

URL to Display:

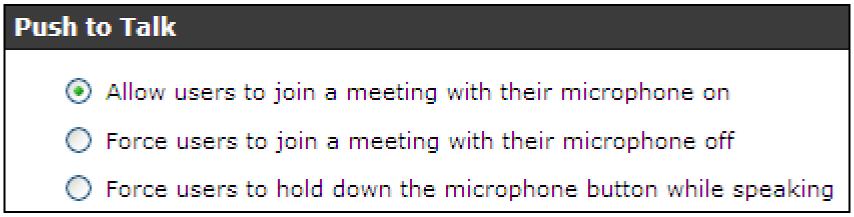
Figure 22: Enabling or disabling client videoconferencing features

4. Enter the fields as described in Table 6: Settings for the Scopia® XT Desktop Client Meeting window on page 32.

Table 6: Settings for the Scopia® XT Desktop Client Meeting window

Field	Description
Enable Desktop Sharing	Determines whether participants can share their PC desktop content with others in the videoconference. If desktop sharing disabled, the **Present** button does not appear in the **Meeting** window of Scopia® XT Desktop Client.
Enable Chat	Determines whether to display the chat window pane in the **Meeting** window of Scopia® XT Desktop Client.
Display an additional panel in the conference room	Determines whether to display an additional pane in Scopia® XT Desktop Client's **Meeting** window within your organization. The pane's contents are drawn from an external web address.
URL to Display	Enter the web address in this field. When the system accesses the web address, it automatically appends two parameters: the current meeting ID and the participant's nickname. This enables your external web content to relate to the meeting and participant if required. The parameters added are: `?meetingid=NNN&nickname=XXX`. If your external web content already takes different parameters in its URL, these parameters are appended to the URL string. Use standard URL-encoding in this field, for example '&' is `%26`, '=' is `%3D` and so on.

5. Configure the **Push to Talk** section to define how participants use the microphone button in the **Meeting** window of Scopia® XT Desktop Client.



Push to Talk

● Allow users to join a meeting with their microphone on

○ Force users to join a meeting with their microphone off

○ Force users to hold down the microphone button while speaking

Figure 23: Push to Talk Settings

Enter the fields as described in Table 7: Defining microphone behavior during a meeting on page 33.

Table 7: Defining microphone behavior during a meeting

Field	Description
Allow users to join a meeting with their microphone on	When selected, this field enables the microphone by default, so participants must select the microphone button to mute themselves.
Force users to join a meeting with their microphone off	(Recommended) When selected, this field disables the microphone by default, so participants must select the microphone button to unmute themselves. This is eliminates background noise from a videoconference until the participant is ready to contribute.
Force users to hold down their microphone button while speaking	When selected, this field requires participants to select and hold down the microphone button to activate their microphones and send their audio.

6. Select **Encrypt Media** to encrypt audio and video over UDP between Scopia® XT Desktop server and Scopia® XT Desktop Client.

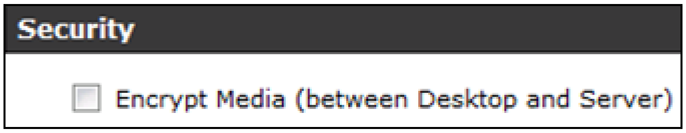


Figure 24: Security Settings

7. Select **OK** or **Apply**.

Rolling-Out Scopia® XT Desktop Client to End Users

About this task

This section provides the recommended procedures for rolling-out your deployment to end users.

The section includes these topics:

Navigation

- Minimum Requirements for Scopia® XT Desktop Client on page 33
- Installing Scopia® XT Desktop Client Locally on a PC on page 35
- Centrally Deploying Scopia® XT Desktop Clients in your Organization on page 36

Minimum Requirements for Scopia® XT Desktop Client

This section details the minimum hardware and software requirements of the Scopia® XT Desktop Client.

The minimum hardware requirements for the Scopia® XT Desktop Client depend on the video resolution.

- Standard definition hardware specifications:
  - PC Intel Pentium 4, 3.0 GHz or faster
  - PC AMD Athlon 3.0 GHz or faster
  - PC Intel Centrino Mobile Processor 1.8 GHz or faster
  - Mac with Intel Core Duo 1.8 GHz or faster
  - Netbook Intel Atom Processor 1.6 GHz or faster
  - 1GB of RAM or more
- Enhanced definition hardware specifications:
  - PC Intel true dual core processors - Core 2 Duo 1.8 GHz or faster
  - PC AMD true dual core processors - e.g. Phenom IIx4 91- 2.X GHz or faster
  - Minimum 2GB of RAM
- High definition hardware specifications:
  - Intel PC architecture
    - 2nd Generation Intel® Core™ i3, i5 or i7 processors (Sandy Bridge) or newer

      Or
    - Any Intel generation with quad-core processors
    - i5 or i7 recommended
  - PC AMD Quad-Core Opteron
  - Mac with Intel Core 2 Duo 2.7 GHz or faster
  - Minimum 2GB of RAM, 3GB of RAM or more recommended

The minimum software requirements of the Scopia® XT Desktop Client are:

- Operating systems:
  - Windows XP (SP3, 32 and 64-bit)
  - Windows Vista (SP2 or higher, 32 and 64-bit)
  - Windows 7 (32 and 64-bit)
  - Windows 8 and 8.1 (desktop mode, 32 and 64-bit)
  - Mac OS X version 10.6 (Snow Leopard) or higher, Intel CPU only

  We recommend using the latest service pack of the Windows operating systems listed in this section.
- Internet browsers:

  Scopia® XT Desktop is tested with the latest internet browser versions available at the time of release.

  Important:

  Internet Explorer must be installed on your Windows PC when using the Scopia® XT Desktop Client, even if you access meeting with other web browsers like Firefox or Chrome.

  - Google Chrome (version 30 and later)
  - Internet Explorer (version 6 and later, for windows)
  - Firefox (version 25 and later)

– Safari (version 5 and later)

Installing Scopia® XT Desktop Client Locally on a PC

About this task

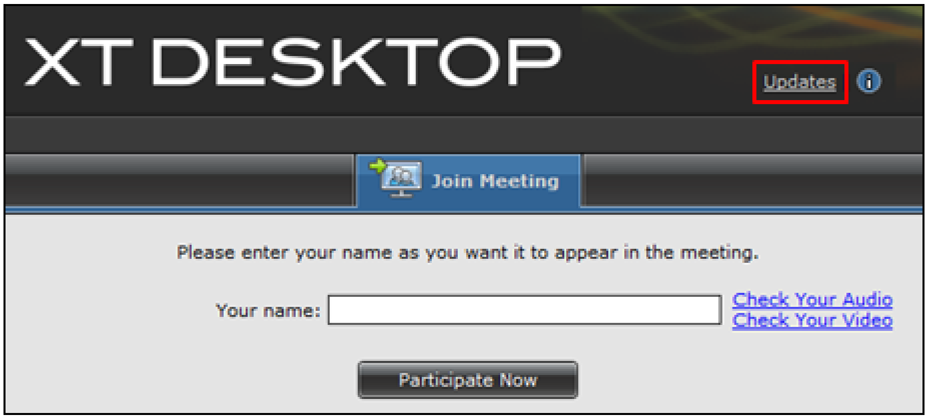
The Scopia® XT Desktop Client Web Portal provides an automatic download and update manager. When you select the **Updates** link, it displays any currently installed components and versions, and enables you to install components.

Before you begin

- Connect a headset or speaker and microphone to your computer, and ensure it is configured in the control panel or system settings.
- Connect a video camera or webcam to your computer.

Procedure

1. To activate Scopia® XT Desktop for the first time, go to the Scopia® XT Desktop web portal page at *http://<Scopia® XT Desktop domain name>/scopia*
2. Select **Updates** in the top-right corner of the web portal.

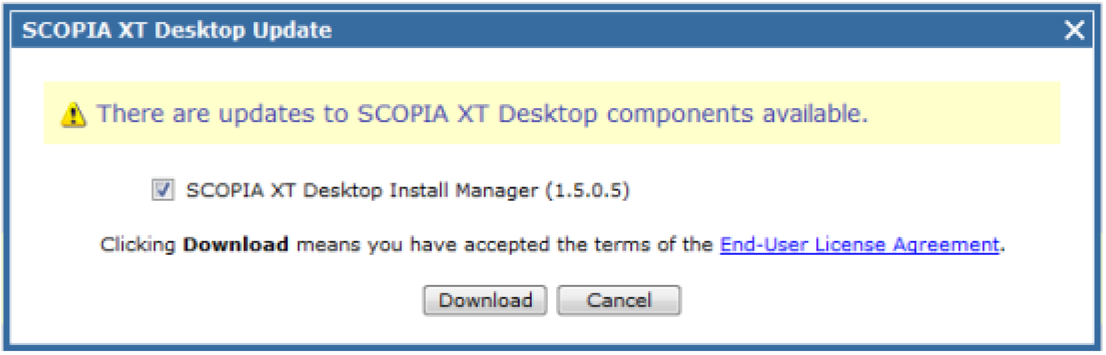


Please enter your name as you want it to appear in the meeting.

Your name:

Figure 25: The Updates link in the top right corner of the web portal

The **Scopia® XT Desktop Update** window opens.



SCOPIA XT Desktop Update

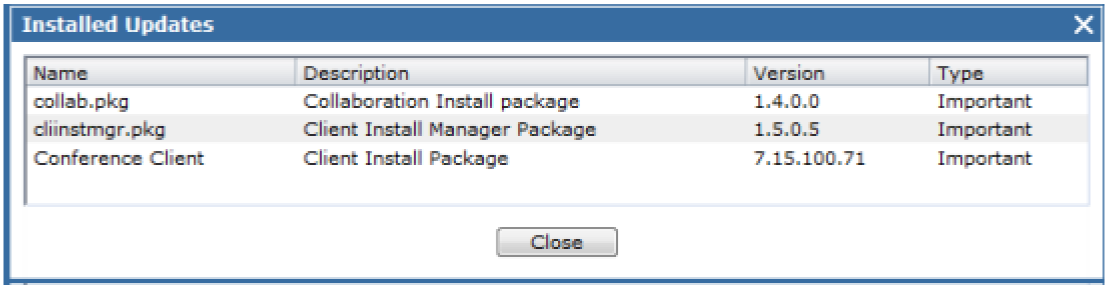
⚠ There are updates to SCOPIA XT Desktop components available.

☑ SCOPIA XT Desktop Install Manager (1.5.0.5)

Clicking **Download** means you have accepted the terms of the End-User License Agreement.

Figure 26: Updating Scopia® XT Desktop Client

3. Select **Conference Client** to install or update the Scopia® XT Desktop Client.
4. Select **Install**. When the Scopia® XT Desktop Client installation is complete, you should see the following icon in the task tray at the lower right corner of the screen:
5. To verify that any optional components were installed, select the **View Installed Updates** link. A list of installed components appears.



Installed Updates

Name	Description	Version	Type
collab.pkg	Collaboration Install package	1.4.0.0	Important
cliinstmgr.pkg	Client Install Manager Package	1.5.0.5	Important
Conference Client	Client Install Package	7.15.100.71	Important

Figure 27: Installed Updates and Components

Centrally Deploying Scopia® XT Desktop Clients in your Organization

About this task

You can push Scopia® XT Desktop Clients simultaneously to end users using one of these standard Microsoft server tools:

- Microsoft Active Directory (AD)
- Microsoft Systems Management Server (SMS).

Contact Customer Support to obtain pre-prepared scripts which can run using either of these infrastructures. There is also accompanying documentation on how to deploy throughout your organization using either of these infrastructures.

Chapter 5 | Securing Your Scopia® XT Desktop Deployment

This section describes how you can enhance the security of your Scopia® XT Desktop deployment by encrypting Scopia® XT Desktop communications and by protecting meetings .

Important:

Using encryption is subject to local regulation. In some countries it is restricted or limited for usage. For more information, consult your local reseller.

Navigation

- Encrypting Scopia® XT Desktop server Communications on page 37
- Protecting Meetings with a PIN on page 45

Encrypting Scopia® XT Desktop server Communications

You can secure Scopia® XT Desktop server communications by encrypting its traffic.

There are several data streams between Scopia® XT Desktop server and Scopia® XT Desktop Client which are transmitted using different protocols as shown in Figure 28: Protocols used in an unsecure environment on page 37:

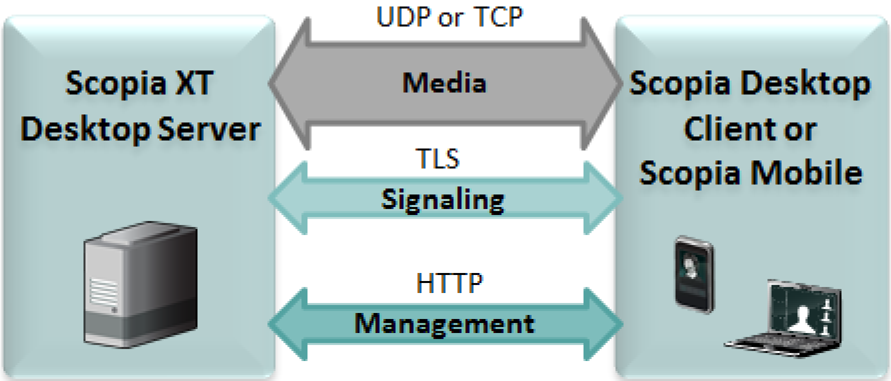


Figure 28: Protocols used in an unsecure environment

The media stream consists of audio, video and presentation. Audio and video are sent over UDP by default. If the UDP connection fails, for example, if the UDP port is closed, TCP is used instead. Presentation always uses TCP.

In a secure environment you encrypt Scopia® XT Desktop server communications as shown in Table 8: Protocols used for encrypting Scopia® XT Desktop server communications on page 38.

Table 8: Protocols used for encrypting Scopia® XT Desktop server communications

Data stream	Unsecure environment	Secure environment
Audio and video	UDP	SRTP
	TCP	TLS
Signaling and presentation	TCP	TLS
Management	HTTP	HTTPS

Make sure that you protect all data streams and have a secure environment as shown in Figure 29: Protocols used in a secure environment on page 38.

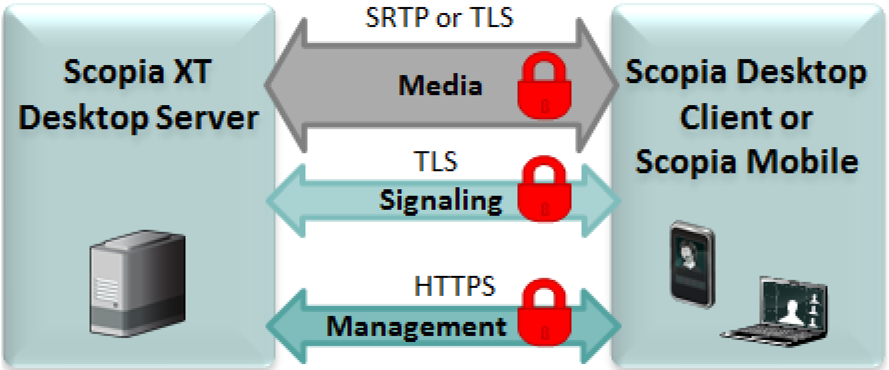


Figure 29: Protocols used in a secure environment

Navigation

- Encrypting Web Access to the Scopia® XT Desktop server on page 38
- Generating a Unique TLS Certificate for Scopia® XT Desktop server on page 41
- Encrypting Media over UDP between Scopia® XT Desktop server and Scopia® XT Desktop Client on page 44

Encrypting Web Access to the Scopia® XT Desktop server

About this task

You can secure access to the Scopia® XT Desktop server web administration interface and Scopia® XT Desktop web portal by enabling HTTPS encryption of the management traffic. HTTPS is the secured version of the standard web browser protocol HTTP. It secures communication between a web browser and a web server through authentication of the web site and encrypting communication between them.

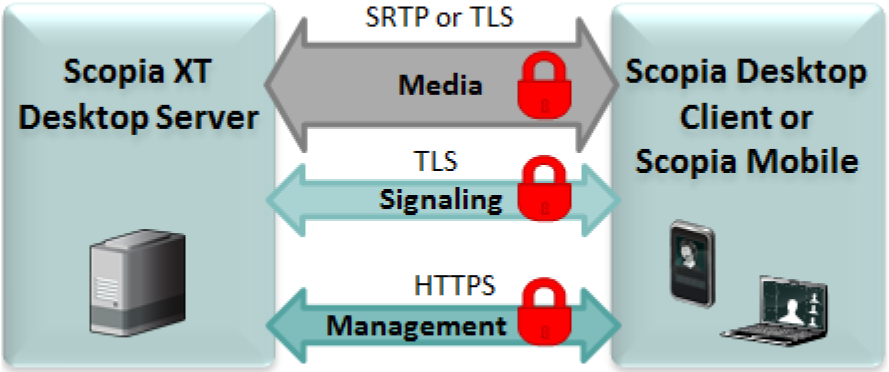


Figure 30: Encrypting communications between Scopia® XT Desktop server and Scopia® XT Desktop Client

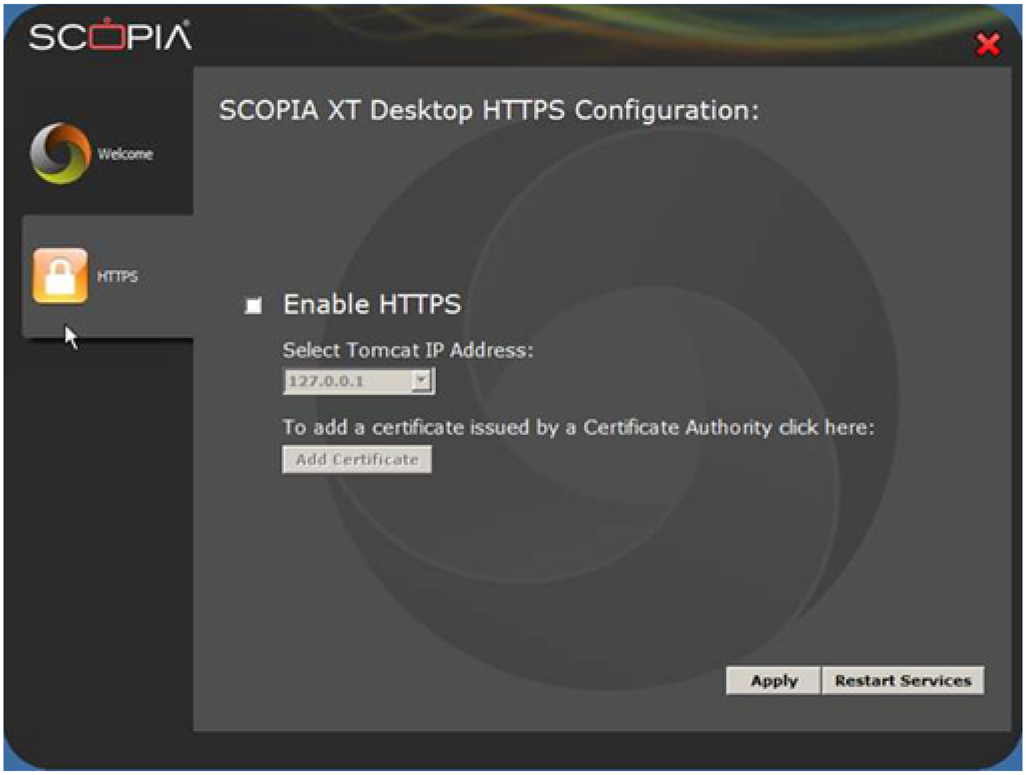
Encrypting web access to the Scopia® XT Desktop server requires a signed certificate for it. Scopia® XT Desktop server comes with a non-unique certificate pre-installed on the Scopia® XT Desktop Conference Server, however, we recommend that you use a unique certificate for stronger authentication as described in the procedure below.

Before you begin

For stronger authentication, make sure you have a unique HTTPS certificate on the Scopia® XT Desktop Conference Server.

Procedure

1. Select **Start > All Programs > Scopia® XT Desktop > ConfigTool**.
2. Select the **Enable HTTPS** check box in the **HTTPS** tab.



SCOPIA XT Desktop HTTPS Configuration:

■ Enable HTTPS

Select Tomcat IP Address: 127.0.0.1

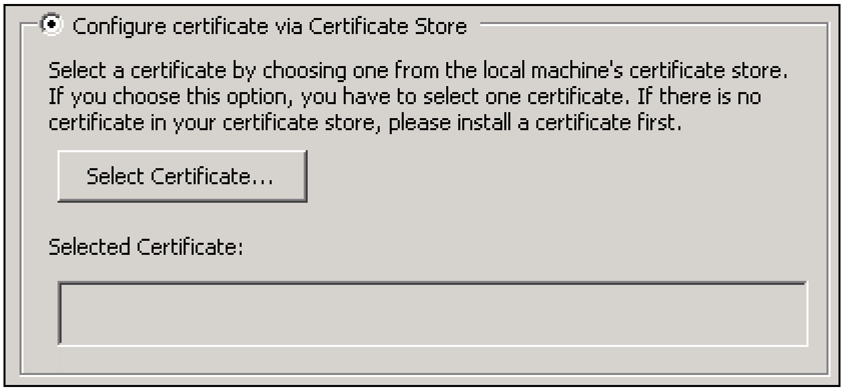
To add a certificate issued by a Certificate Authority click here:

Figure 31: Adding a certificate to Scopia® XT Desktop server

3. Ensure that the real IP address of Scopia® XT Desktop server is displayed in the **Select Tomcat IP Address** list.
4. Select **Apply**.

   You have enabled HTTPS with the pre-installed non-unique certificate. For stronger authentication, use a unique certificate by following the rest of this procedure.
5. Select **Add Certificate** to upload an existing signed certificate.
6. If the certificate is installed in the local machine's Windows Certificate Store (WCS):

   a. Select the **Configure Certificate via Certificate Store**.



● Configure certificate via Certificate Store

Select a certificate by choosing one from the local machine's certificate store. If you choose this option, you have to select one certificate. If there is no certificate in your certificate store, please install a certificate first.

Selected Certificate:

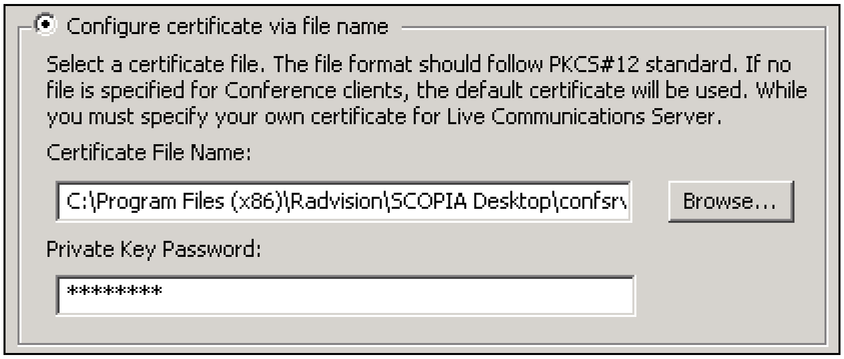
Figure 32: Configuring certificate using installed on the local machine

   b. Select **Select Certificate** to browse the WCS.

   c. Select the certificate from the list of certificates in the WCS.

7. To locate a certificate by its filename:

   a. Select **Configure Certificate via File Name**.



● Configure certificate via file name

Select a certificate file. The file format should follow PKCS#12 standard. If no file is specified for Conference clients, the default certificate will be used. While you must specify your own certificate for Live Communications Server.

Certificate File Name: C:\Program Files (x86)\Radvision\SCOPIA Desktop\confsrv

Private Key Password: ********

Figure 33: Configuring certificate using the file name

   b. Browse to the PKCS12 certificate and select it.

   c. Enter the private key password for the certificate.

8. Select **OK**.

9. Verify that the certificate information is listed in the **Selected Certificate** pane.

10. Select **Apply**.

11. Select **OK**, and then select **OK** again.

12. Select **Restart Services**.

Generating a Unique TLS Certificate for Scopia® XT Desktop server

About this task

You can secure Avaya Scopia® XT Desktop's media and signaling between Avaya Scopia® XT Desktop server and Avaya Scopia® Management using TLS encryption. TLS enables network devices to communicate securely using certificates, to provide authentication of the devices and encryption of the communication between them. This method also checks the data integrity of messages.

By default, audio and video between Scopia® XT Desktop server and Scopia® XT Desktop Client are transmitted using the UDP protocol. If Scopia® XT Desktop server fails to establish the UDP connection with its client, it sends media over TCP. If this is the case your media is protected using TLS together with other data streams between Scopia® XT Desktop server and Scopia® XT Desktop Client.

Important:

Using encryption is subject to local regulation. In some countries it is restricted or limited for usage. For more information, consult your local reseller.

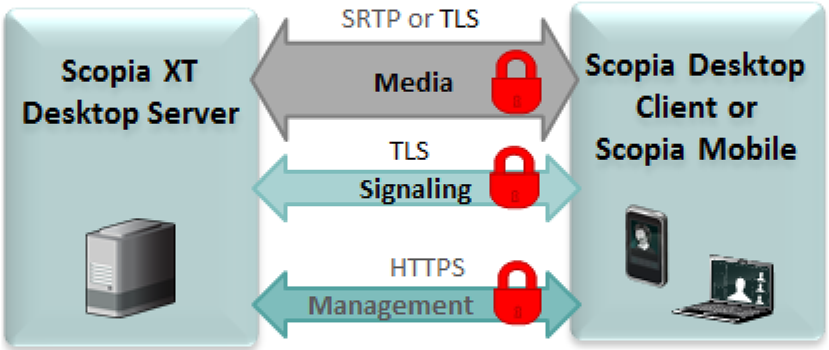


Figure 34: Encrypting communications using TLS

Each time a video network device starts the TLS communication session, it sends its own signed certificate together with the CA root certificate and requests the same certificates from the other devices to which it wants to connect. After both devices verify each other's identity, a secure TLS connection can be established. Exchanging certificates between devices is part of the TLS protocol; it happens in the background and is transparent to a user.

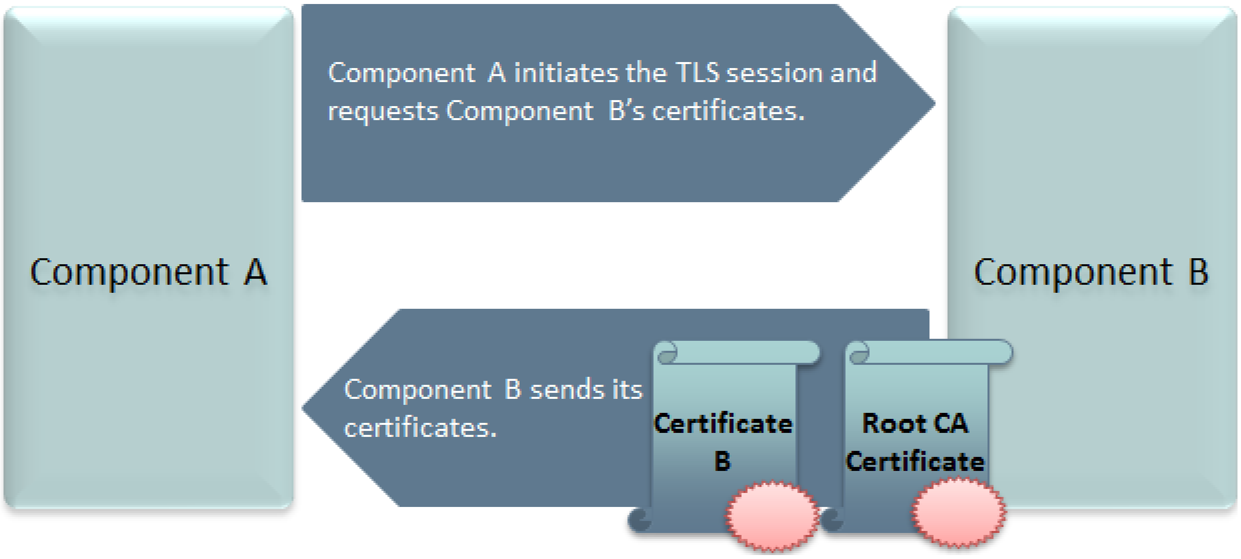

Component A
Component A initiates the TLS session and requests Component B's certificates.
Component B
Component B sends its certificates.
Certificate B
Root CA Certificate

Figure 35: Establishing TLS connection

Scopia® XT Desktop server is shipped with a pre-created and pre-installed certificate, but its encryption keys are non-unique. You can create a unique certificate for stronger authentication as described in this section.

You create a unique certificate by generating a certificate signing request (CSR) using the `keytool` utility and sending it to a certificate authority (CA) for signing. The `keytool` utility is part of the Java installation.

Important:

This section does not explain each of the parameters of the keytool command. For a full description of this Java utility, see http://docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html.

Procedure

1. Stop the **Scopia® XT Desktop - Apache Tomcat** service.
2. Copy the `.keystore` file located in *<SD_install_dir>\data\sds.keystore* to a temporary working folder, for example *C:\cert*. The keystore file holds the certificates on each server. Currently they hold the default non-unique certificates.

   Important:

   The password on the `.keystore` file is `radvision`.

3. Open a command line window. The `keytool` utility is located in *<SD_install_dir>\JRE\bin*.
4. Use the `keytool` utility to remove the pre-installed certificate from the `.keystore` file with the `-delete` parameter. The default certificate has an alias of `default`:

   ```
   keytool -delete -alias default -keystore sds.keystore -storepass radvision
   ```

5. Generate a unique key pair using an appropriate DN with the `-genkeypair` parameter:

   ```
   keytool -genkeypair -keyalg RSA -alias sds -sigalg MD5withRSA -dname "CN=<FQDN of
   server>"
   -keystore sds.keystore -storepass radvision -validity 365 -keysize 1024
   ```

6. Create a certificate signing request file (CSR) for the newly generated key pair using the `-certreq` parameter:

   ```
   keytool -certreq -alias sds -sigalg MD5withRSA -keystore sds.keystore -storepass
   radvision
   -file C:\cert\certreq.csr
   ```

7. Send the certificate request to a Certificate Authority.

   Important:

   Make sure that you use the same CA for signing certificates for both Scopia® Management and Scopia® XT Desktop server for a more efficient process.

8. The CA returns the certificate signed in form of .crt file, for example `signed_cert.crt`. It also returns a root certificate, `root_cert.crt`.
9. Import the root certificate of the CA into the keystore file using the `-import` parameter:

   ```
   keytool -import -trustcacerts -alias root -file root_cert.crt -keystore
   sds.keystore
   -storepass radvision
   ```

   where `root_cert.crt` is the trusted root certificate.

   The `trustcacerts` parameter instructs `keytool` to check both the specific and the system`.keystore` file for the root certificate.

10. Import the signed certificate into the keystore file. Use the same alias you used in step 6.

    ```
    keytool -import -trustcacerts -alias sds -file signed_cert.crt -keystore
    sds.keystore
    -storepass radvision
    ```

    `Keytool` issues a confirmation message if the certificate was uploaded successfully.

11. Copy the `.keystore` file back to its original location.

12. Restart the services on the Scopia® XT Desktop server.

Encrypting Media over UDP between Scopia® XT Desktop server and Scopia® XT Desktop Client

About this task

By default, audio and video between Scopia® XT Desktop server and Scopia® XT Desktop Client are transmitted using the UDP protocol. You can configure your Scopia® XT Desktop server to encrypt this data stream using the SRTP protocol.

Secure Real-time Transport Protocol (SRTP) adds security to the standard RTP protocol, which is used to send media (video and audio) between devices in SIP calls. It offers security with encryption, authentication and message integrity. The encryption uses a symmetric key generated at the start of the call, and being symmetric, the same key locks and unlocks the data. So to secure transmission of the symmetric key, it is sent safely during call setup using TLS.

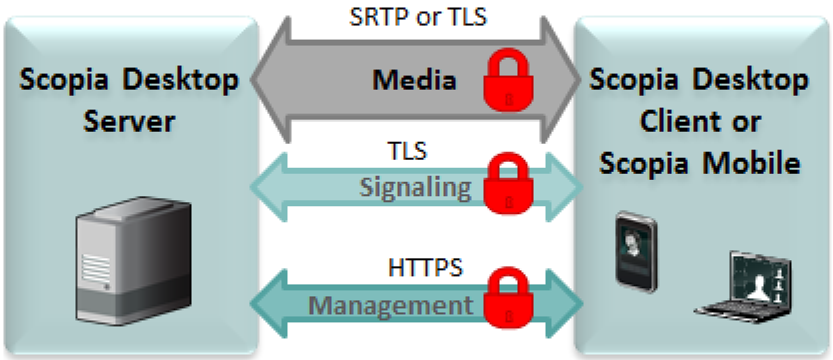


Figure 36: Encrypting media between Scopia® XT Desktop server and Scopia® Management

Important:

Encrypt signaling between Scopia® XT Desktop server and Scopia® XT Desktop Client to protect transmission of the symmetric key.

If Scopia® XT Desktop server fails to establish the UDP connection with its client, it sends media over TCP. If this is the case and you enabled HTTPS on the Scopia® XT Desktop server, your media is protected using HTTPS together with other data streams between Scopia® XT Desktop server and Scopia® XT Desktop Client.

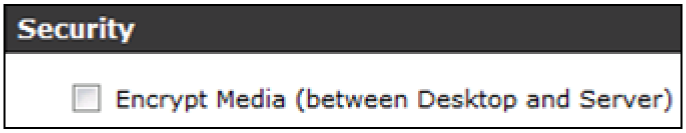
Procedure

1. Access the Scopia® XT Desktop web administration interface.

2. Select the **Client** icon in the sidebar.

3. Select the **Meeting Features** tab.

4. Select **Encrypt Media** to encrypt audio and video over UDP between Scopia® XT Desktop server and Scopia® XT Desktop Client.



Security

□ Encrypt Media (between Desktop and Server)

Figure 37: Security Settings

5. Select **OK** or **Apply**.

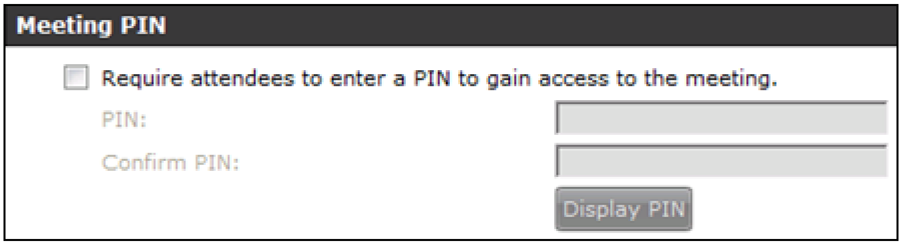
Protecting Meetings with a PIN

About this task

You can require all users whose endpoints access meetings through this server must enter a predefined PIN.

Procedure

1. Access the Scopia® XT Desktop server Administration web interface.
2. Select **Directory and Authentication** in the sidebar.
3. Select the **Require attendees to enter a PIN to gain access to the meeting** check box in the **Meeting PIN** section.



Meeting PIN

□ Require attendees to enter a PIN to gain access to the meeting.

PIN:

Confirm PIN:

Figure 38: Meeting PIN Section

4. Enter a PIN in the **PIN** field.
5. Enter the PIN again in the **Confirm PIN** field.
6. To check the PIN you have configured, select **Display PIN**.
7. Select **OK**.

Glossary of Terms for Scopia® Solution

1080p

See Full HD on page 50.

2CIF

2CIF describes a video resolution of 704 x 288 pixels (PAL) or 704 x 240 (NTSC). It is double the width of CIF, and is often found in CCTV products.

2SIF

2SIF describes a video resolution of 704 x 240 pixels (NTSC) or 704 x 288 (PAL). This is often adopted in IP security cameras.

4CIF

4CIF describes a video resolution of 704 x 576 pixels (PAL) or 704 x 480 (NTSC). It is four times the resolution of CIF and is most widespread as the standard analog TV resolution.

4SIF

4SIF describes a video resolution of 704 x 480 pixels (NTSC) or 704 x 576 (PAL). This is often adopted in IP security cameras.

720p

See HD on page 53.

AAC

AAC is an audio codec which compresses sound but with better results than MP3.

Alias

An alias in H.323 represents the unique name of an endpoint. Instead of dialing an IP address to reach an endpoint, you can dial an alias, and the gatekeeper resolves it to an IP address.

AGC (Automatic Gain Control)

Automatic Gain Control (AGC) smooths audio signals through normalization, by lowering sounds which are too strong and strengthening sounds which are too weak. This is relevant with microphones situated at some distance from the speaker, like room systems. The result is a more consistent audio signal within the required range of volume.

Auto-Attendant

Auto-Attendant, also known as video IVR, offers quick access to meetings hosted on MCUs, via a set of visual menus. Participants can select menu options using standard DTMF tones (numeric keypad). Auto-Attendant works with both H.323 and SIP endpoints.

Balanced Microphone

A balanced microphone uses a cable that is built to reduce noise and interference even when the cable is long. This reduces audio disruptions resulting from surrounding electromagnetic interference.

BFCP (Binary Floor Control Protocol)

BFCP is a protocol which coordinates shared videoconference features in SIP calls, often used by one participant at a time. For example, when sharing content to others in the meeting, one participant is designated as the presenter, and is granted the floor for presenting. All endpoints must be aware that the floor was granted to that participant and react appropriately.

Bitrate

Bitrate is the speed of data flow. Higher video resolutions require higher bitrates to ensure the video is constantly updated, thereby maintaining smooth motion. If you lower the bitrate, you lower the quality of the video. In some cases, you can select a lower bitrate without noticing a significant drop in video quality; for example during a presentation or when a lecturer is speaking and there is very little motion. In video recordings, the bitrate determines the file size for each minute of recording. Bitrate is often measured in kilobits per second (kbps).

Call Control

See Signaling on page 61.

Cascaded Videoconference

A cascaded videoconference is a meeting distributed over more than one physical Scopia® Elite MCU, where a master MCU connects to one or more slave MCUs to create a single videoconference. It increases the meeting capacity by combining the resources of several MCUs. This can be especially useful for distributed deployments across several locations, reducing bandwidth usage.

CIF

CIF, or Common Intermediate Format, describes a video resolution of 352 × 288 pixels (PAL) or 352 x 240 (NTSC). This is sometimes referred to as Standard Definition (SD).

Content Slider

The Scopia® Content Slider stores the data already presented in the videoconference and makes it available for participants to view during the meeting.

Continuous Presence

Continuous presence enables viewing multiple participants of a videoconference at the same time, including the active speaker. This graphics-intensive work requires scaling and mixing the images together into one of the predefined video layouts. The range of video layouts depends on the type of media processing supported, typically located in the MCU.

Control

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, or by SDP in SIP endpoints. Control occurs within the framework of an established call, after signaling.

CP

See Continuous Presence on page 48.

Dedicated Endpoint

A dedicated endpoint is a hardware endpoint for videoconferencing assigned to a single user. It is often referred to as a personal or executive endpoint, and serves as the main means of video communications for this user. For example, Scopia® XT Executive. It is listed in the organization's LDAP directory as associated exclusively with this user.

Dial Plan

A dial plan defines a way to route a call and to determine its characteristics. In traditional telephone networks, prefixes often denote geographic locations. In videoconferencing deployments, prefixes are also used to define the type and quality of a call. For example, dial 8 before a number for a lower bandwidth call, or 6 for an audio-only call, or 5 to route the call to a different branch.

Dial Prefix

A dial prefix is a number added at the beginning of a dial string to route it to the correct destination, or to determine the type of call. Dial prefixes are defined in the organization's dial plan. For example, dial 9 for an outside line, or dial 6 for an audio only call.

Distributed Deployment

A distributed deployment describes a deployment where the solution components are geographically distributed in more than one network location.

DNS Server

A DNS server is responsible for resolving domain names in your network by translating them into IP addresses.

DTMF

DTMF, or touch-tone, is the method of dialing on touch-tone phones, where each number is translated and transmitted as an audio tone.

Dual Video

Dual video is the transmitting of two video streams during a videoconference, one with the live video while the other is a shared data stream, like a presentation.

Dynamic Video Layout

The dynamic video layout is a meeting layout that switches dynamically to include the maximum number of participants it can display on the screen (up to 9 on the XT Series, or up to 28 on Scopia® Elite MCU). The largest image always shows the active speaker.

E.164

E.164 is an address format for dialing an endpoint with a standard telephone numeric keypad, which only has numbers 0 - 9 and the symbols: * and #.

Endpoint

An endpoint is a tool through which people can participate in a videoconference. Its display enables you to see and hear others in the meeting, while its microphone and camera enable you to be seen and heard by others. Endpoints include dedicated endpoints, like Scopia® XT Executive, software endpoints like Scopia® XT Desktop Client, mobile device endpoints like Scopia® Mobile, room systems like XT Series, and telepresence systems like Scopia® XT Telepresence.

Endpoint Alias

See Alias on page 46.

FEC

Forward Error Correction (FEC) is a proactive method of sending redundant information in the video stream to preempt quality degradation. FEC identifies the key frames in the video stream that should be protected by FEC. There are several variants of the FEC algorithm. The Reed-Solomon algorithm (FEC-RS) sends redundant packets per block of information, enabling the sender (like the Scopia® Elite MCU) to manage up to ten percent packet loss in the video stream with minimal impact on the smoothness and quality of the video.

FECC

Far End Camera Control (FECC) is a feature of endpoint cameras, where the camera can be controlled remotely by another endpoint in the call.

Forward Error Correction

See FEC on page 50.

FPS

See Frames Per Second on page 50.

Frame Rate

See Frames Per Second on page 50.

Frames Per Second

Frames Per Second (fps), also known as the frame rate, is a key measure in video quality, describing the number of image updates per second. The average human eye can register up to 50 frames per second. The higher the frame rate, the smoother the video.

Full HD

Full HD, or Full High Definition, also known as 1080p, describes a video resolution of 1920 x 1080 pixels.

Full screen Video Layout

The full screen view shows one video image. Typically, it displays the remote presentation, or, if there is no presentation, it displays the other meeting participant(s).

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 Avaya Scopia® Gatekeeper, while ECS is a standalone gatekeeper.

Gateway

A gateway is a component in a video solution which routes information between two subnets or acts as a translator between different protocols. For example, a gateway can route data between the headquarters and a partner site, or between two protocols like the TIP Gateway, or the Scopia® 100 Gateway.

GLAN

GLAN, or gigabit LAN, is the name of the network port on the XT Series. It is used on the XT Series to identify a 10/100/1000MBit ethernet port.

H.225

H.225 is part of the set of H.323 protocols. It defines the messages and procedures used by gatekeepers to set up calls.

H.235

H.235 is the protocol used to authenticate trusted H.323 endpoints and encrypt the media stream during meetings.

H.239

H.239 is a widespread protocol used with H.323 endpoints, to define the additional media channel for data sharing (like presentations) alongside the videoconference, and ensures only one presenter at a time.

H.243

H.243 is the protocol used with H.323 endpoints enabling them to remotely manage a videoconference.

H.245

H.245 is the protocol used to negotiate call parameters between endpoints, and can control a remote endpoint from your local endpoint. It is part of the H.323 set of protocols.

H.261

H.261 is an older protocol used to compress CIF and QCIF video resolutions. This protocol is not supported by the XT Series.

H.263

H.263 is an older a protocol used to compress video. It is an enhancement to the H.261 protocol.

H.264

H.264 is a widespread protocol used with SIP and H.323 endpoints, which defines video compression. Compression algorithms include 4x4 transforms and a basic motion comparison algorithm called P-slices. There are several profiles within H.264. The default profile is the H.264 Baseline Profile, but H.264 High Profile uses more sophisticated compression techniques.

H.264 Baseline Profile

See H.264 on page 52.

H.264 High Profile

H.264 High Profile is a standard for compressing video by up to 25% over the H.264 Baseline Profile, enabling high definition calls to be held over lower call speeds. It requires both sides of the transmission (sending and receiving endpoints) to support this protocol. H.264 High Profile uses compression algorithms like:

- CABAC compression (Context-Based Adaptive Binary Arithmetic Coding)
- 8x8 transforms which more effectively compress images containing areas of high correlation

These compression algorithms demand higher computation requirements, which are offered with the dedicated hardware available in Scopia® Solution components. Using H.264 High Profile in videoconferencing requires that both the sender and receiver's endpoints support it. This is different from SVC which is an adaptive technology working to improve quality even when only one side supports the standard.

H.320

H.320 is a protocol for defining videoconferencing over ISDN networks.

H.323

H.323 is a widespread set of protocols governing the communication between endpoints in videoconferences and point-to-point calls. It defines the call signaling, control, media flow, and bandwidth regulation.

H.323 Alias

See Alias on page 46.

H.350

H.350 is the protocol used to enhance LDAP user databases to add video endpoint information for users and groups.

H.460

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 PathFinder server, where the endpoint acts as an H.460 client to the PathFinder server which acts as an H.460 server.

HD

A HD ready device describes its high definition resolution capabilities of 720p, a video resolution of 1280 x 720 pixels.

High Availability

High availability is a state where you ensure better service and less downtime by deploying additional servers. There are several strategies for achieving high availability, including deployment of redundant servers managed by load balancing systems.

High Definition

See HD on page 53.

High Profile

See H.264 High Profile on page 52.

HTTPS

HTTPS is the secured version of the standard web browser protocol HTTP. It secures communication between a web browser and a web server through authentication of the web site and encrypting communication between them. For example, you can use HTTPS to secure web browser access to the web interface of many Scopia® Solution products.

Image Resolution

See Resolution on page 59.

kbps

Kilobits per second (kbps) is the standard unit to measure bitrate, measuring the throughput of data communication between two devices. Since this counts the number of individual bits (ones or zeros), you must divide by eight to calculate the number of kilobytes per second (KBps).

KBps

Kilobytes per second (KBps) measures the bitrate in kilobytes per second, not kilobits, by dividing the number of kilobits by eight. Bitrate is normally quoted as kilobits per second (kbps) and then converted to kilobytes per second (KBps). Bitrate measures the throughput of data communication between two devices.

LDAP

LDAP is a widespread standard database format which stores network users. The format is hierarchical, where nodes are often represented as *branch location* > *department* > *sub-department*, or *executives* > *managers* > *staff members*. The database standard is employed by most user directories including Microsoft Active Directory, IBM Sametime and others. H.350 is an extension to the LDAP standard for the videoconferencing industry.

Lecture Mode

Scopia® XT Desktop's lecture mode allows the participant defined as the lecturer to see all the participants, while they see only the lecturer. All participants are muted except the lecturer, unless a participant asks permission to speak and is unmuted by the lecturer. This mode is tailored for distance learning, but you can also use it for other purposes like when an executive addresses employees during company-wide gatherings.

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).

Location

A location is a physical space (building) or a network (subnet) where video devices can share a single set of addresses. A distributed deployment places these components in different locations, often connected via a VPN.

Management

Management refers to the administration messages sent between components of the Scopia® Solution as they manage and synchronize data between them. Management also includes front-end browser interfaces configuring server settings on the server. Management messages are usually transmitted via protocols like HTTP, SNMP, FTP or XML. For example, Scopia® Management uses management messages to monitor the activities of an MCU, or when it authorizes the MCU to allow a call to proceed.

MBps

Megabytes per second (MBps) is a unit of measure for the bitrate. The bitrate is normally quoted as kilobits per second (kbps) and then converted by dividing it by eight to reach the number of kilobytes per second (KBps) and then by a further 1000 to calculate the MBps.

MCU

An MCU, or Multipoint Control Unit, connects several endpoints to a single videoconference. It manages the audio mixing and creates the video layouts, adjusting the output to suit each endpoint's capabilities.

MCU service

See Meeting Type on page 56.

Media

Media refers to the live audio, video and shared data streams sent during a call. Presentation and Far end camera control (FECC) are examples of information carried on the data stream. Media is transmitted via the RTP and RTCP protocols in both SIP and H.323 calls. The parallel data stream of both live video and presentation, is known as dual video.

Media Control

See Control on page 48.

Meeting Type

Meeting types (also known as MCU services) are meeting templates which determine the core characteristics of a meeting. For example, they determine if the meeting is audio only or audio and video, they determine the default video layout, the type of encryption, PIN protection and many other features. You can invoke a meeting type by dialing its prefix in front of the meeting ID. Meeting types are created and stored in the MCU, with additional properties in Scopia® Management.

Moderator

A moderator has special rights in a videoconference, including blocking the sound and video of other participants, inviting new participants, disconnecting others, determining video layouts, and closing meetings. In Scopia® XT Desktop Client, an owner of a virtual room is the moderator when the room is protected by a PIN. Without this protection, any participant can assume moderator rights.

MTU

The MTU, or Maximum Transmission Unit, is the maximum size of data packets sent around your network. This value must remain consistent for all network components, including servers like the MCU and Scopia® XT Desktop server, endpoints like XT Series and other network devices like LDAP servers and network routers.

Multicast Streaming

Multicast streaming sends a videoconference to multiple viewers across a range of addresses, reducing network traffic significantly. Scopia® XT Desktop server multicasts to a single IP address, and streaming clients must tune in to this IP address to view the meeting. Multicasts require that routers, switches and other equipment know how to forward multicast traffic.

Multi-Point

A multi-point conference has more than two participants.

Multi-tenant

Service provider, or multi-tenant, deployments enable one installation to manage multiple organizations. All the organizations can reside as tenants within a single service provider deployment. For example, Scopia® Management can manage a separate set of users for each organization, separate local administrators, separate bandwidth policies etc. all within a single multi-tenant installation.

NAT

A NAT, or Network Address Translation device, translates external IP addresses to internal addresses housed in a private network. This enables a collection of devices like endpoints in a private network, each with their own internal IP address, can be represented publicly by a single, unique IP address. The

NAT translates between public and private addresses, enabling users toplace calls between public network users and private network users.

NetSense

NetSense is a proprietary Scopia® Solution technology which optimizes the video quality according to the available bandwidth to minimize packet loss. As the available bandwidth of a connection varies depending on data traffic, NetSense's sophisticated algorithm dynamically scans the video stream, and then reduces or improves the video resolution to maximize quality with the available bandwidth.

Packet Loss

Packet loss occurs when some of the data transmitted from one endpoint is not received by the other endpoint. This can be caused by narrow bandwidth connections or unreliable signal reception on wireless networks.

PaP Video Layout

The PaP (Picture and Picture) view shows up to three images of the same size.

Phantom Power

Microphones which use phantom power draw their electrical power from the same cable as the audio signal. For example, if your microphone is powered by a single cable, it serves both to power the microphone and transmit the audio data. Microphones which have two cables, one for sound and a separate power cable, do not use phantom power.

PiP Video Layout

The PiP (Picture In Picture) view shows a video image in the main screen, with an additional smaller image overlapping in the corner. Typically, a remote presentation is displayed in the main part of the screen, and the remote video is in the small image. If the remote endpoint does not show any content, the display shows the remote video in the main part of the screen, and the local presentation in the small image.

Point-to-Point

Point-to-point is a feature where only two endpoints communicate with each other without using MCU resources.

PoP Video Layout

The PoP (Picture out Picture) view shows up to three images of different size, presented side by side, where the image on the left is larger than the two smaller images on the right.

Prefix

See Dial Prefix on page 49.

PTZ Camera

A PTZ camera can pan to swivel horizontally, tilt to move vertically, and optically zoom to devote all the camera's pixels to one area of the image. For example, the XT Standard Camera is a PTZ camera with its own power supply and remote control, and uses powerful lenses to achieve superb visual quality. In contrast, fixed cameras like webcams only offer digital PTZ, where the zoom crops the camera image, displaying only a portion of the original, resulting in fewer pixels of the zoomed image, which effectively lowers the resolution. Fixed cameras also offer digital pan and tilt only after zooming, where you can pan up to the width or length of the original camera image.

Q.931

Q.931 is a telephony protocol used to start and end the connection in H.323 calls.

QCIF

QCIF, or Quarter CIF, defines a video resolution of 176 × 144 pixels (PAL) or 176 x 120 (NTSC). It is often used in older mobile handsets (3G-324M) limited by screen resolution and processing power.

Quality of Service (QoS)

Quality of Service (QoS) determines the priorities of different types of network traffic (audio, video and control/signaling), so in poor network conditions, prioritized traffic is still fully transmitted.

Recordings

A recording of a videoconference can be played back at any time. Recordings include audio, video and shared data (if presented). In Scopia® XT Desktop, any participant with moderator rights can record a meeting. Users can access Scopia® XT Desktop recordings from the Scopia® XT Desktop web portal or using a web link to the recording on the portal.

Redundancy

Redundancy is a way to deploy a network component, in which you deploy extra units as 'spares', to be used as backups in case one of the components fails.

Registrar

A SIP Registrar manages the SIP domain by requiring that all SIP devices register their IP addresses with it. For example, once a SIP endpoint registers its IP address with the Registrar, it can place or receive calls with other registered endpoints.

Resolution

Resolution, or image/video resolution, is the number of pixels which make up an image frame in the video, measured as the number of horizontal pixels x the number of vertical pixels. Increasing resolution improves video quality but typically requires higher bandwidth and more computing power. Techniques like SVC, H.264 High Profile and FEC reduce bandwidth usage by compressing the data to a smaller footprint and compensating for packet loss.

Restricted Mode

Restricted mode is used for ISDN endpoints only, when the PBX and line uses a restricted form of communication, reserving the top 8k of each packet for control data only. If enabled, the bandwidth values on these lines are in multiples of 56kbps, instead of multiples of 64kbps.

Room System

A room system is a hardware videoconferencing endpoint installed in a physical conference room. Essential features include its camera's ability to PTZ (pan, tilt, zoom) to allow maximum flexibility of camera angles enabling participants to see all those in the meeting room or just one part of the room.

RTP

RTP or Real-time Transport Protocol is a network protocol which supports video and voice transmission over IP. It underpins most videoconferencing protocols today, including H.323, SIP and the streaming control protocol known as RTSP. The secured version of RTP is SRTP.

RTCP

Real-time Control Transport Protocol, used alongside RTP for sending statistical information about the media sent over RTP.

RTSP

RTSP or Real-Time Streaming Protocol controls the delivery of streamed live or playback video over IP, with functions like pause, fast forward and reverse. While the media itself is sent via RTP, these control functions are managed by RTSP

Sampling Rate

The sampling rate is a measure of the accuracy of the audio when it is digitized. To convert analog audio to digital, it must collect or sample the audio at specific intervals. As the rate of sampling increases, it raises audio quality.

SBC

A Session Border Controller (SBC) is a relay device between two different networks. It can be used in firewall/NAT traversal, protocol translations and load balancing.

Scalability

Scalability describes the ability to increase the capacity of a network device by adding another identical device (one or more) to your existing deployment. In contrast, a non-scalable solution would require replacing existing components to increase capacity.

Scopia® Content Slider

See Content Slider on page 48.

SD

Standard Definition (SD), is a term used to refer to video resolutions which are lower than HD. There is no consensus defining one video resolution for SD.

Service

Also known as MCU service. See Meeting Type on page 56.

SIF

SIF defines a video resolution of 352 x 240 pixels (NTSC) or 352 x 288 (PAL). This is often used in security cameras.

Signaling

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, or by the SIP headers in SIP calls. Signaling occurs before the control aspect of call setup.

SIP

Session Initiation Protocol (SIP) is a signaling protocol for starting, managing and ending voice and video sessions over TCP, TLS or UDP. Videoconferencing endpoints typically are compatible with SIP or H.323, and in some cases (like Avaya Scopia® XT Series), an endpoint can be compatible with both protocols. As a protocol, it uses fewer resources than H.323.

SIP Server

A SIP server is a network device communicating via the SIP protocol.

SIP URI

See URI on page 64.

SIP Registrar

See Registrar on page 59.

Single Sign On

Single Sign On (SSO) automatically uses your network login and password to access different enterprise systems. Using SSO, you do not need to separately login to each system or service in your organization.

Slider

See Content Slider on page 48.

SNMP

Simple Network Management Protocol (SNMP) is a protocol used to monitor network devices by sending messages and alerts to their registered SNMP server.

Software endpoint

A software endpoint turns a computer or portable device into a videoconferencing endpoint via a software application only. It uses the system's camera and microphone to send image and sound to the other participants, and displays their images on the screen. For example, Scopia® XT Desktop Client or Scopia® Mobile.

SRTP

Secure Real-time Transport Protocol (SRTP) adds security to the standard RTP protocol, which is used to send media (video and audio) between devices in SIP calls. It offers security with encryption, authentication and message integrity. The encryption uses a symmetric key generated at the start of the call, and being symmetric, the same key locks and unlocks the data. So to secure transmission of the symmetric key, it is sent safely during call setup using TLS.

SSO

See Single Sign On on page 61.

Standard Definition

See SD on page 60.

STUN

A STUN server enables you to directly dial an endpoint behind a NAT or firewall by giving that computer's public internet address.

SVC

SVC extends the H.264 codec standard to dramatically increase error resiliency and video quality without the need for higher bandwidth. It is especially effective over networks with high packet loss (like wireless networks) which deliver low quality video. It splits the video stream into layers, comprising a small base layer and then additional layers on top which enhance resolution, frame rate and quality. Each additional layer is only transmitted when bandwidth permits. This allows for a steady video transmission when available bandwidth varies, providing better quality when the bandwidth is high, and adequate quality when available bandwidth is poor.

SVGA

SVGA defines a video resolution of 800 x 600 pixels.

SQCIF

SQCIF defines a video resolution of 128 x 96 pixels.

Switched video

Switching is the process of redirecting video as-is without transcoding, so you see only one endpoint's image at a time, usually the active speaker, without any video layouts or continuous presence (CP). Using video switching increases the port capacity of the Scopia® Elite MCU only by four times.

❗ **Important:**

Use switched video only when all endpoints participating in the videoconference support the same resolution. If a network experiences high packet loss, switched video might not be displayed properly for all endpoints in the videoconference.

SXGA

SXGA defines a video resolution of 1280 x 1024 pixels.

Telepresence

A telepresence system combines two or more endpoints together to create a wider image, simulating the experience of participants being present in the same room. Telepresence systems always designate one of the endpoints as the primary monitor/camera/codec unit, while the remainder are defined as auxiliary or secondary endpoints. This ensures that you can issue commands via a remote control to a single codec base which leads and controls the others to work together as a single telepresence endpoint.

Telepresence - Dual row telepresence room

Dual row telepresence rooms are large telepresence rooms with two rows of tables that can host up to 18 participants.

TLS

TLS enables network devices to communicate securely using certificates, to provide authentication of the devices and encryption of the communication between them.

Transcoding

Transcoding is the process of converting video into different sizes, resolutions or formats. This enables multiple video streams to be combined into one view, enabling continuous presence, as in a typical videoconferencing window.

UC (Unified Communications)

UC, or unified communications deployments offer solutions covering a wide range of communication channels. These include audio (voice), video, text (IM or chat), data sharing (presentations), whiteboard sharing (interactive annotations on shared data).

Unbalanced Microphone

An unbalanced microphone uses a cable that is not especially built to reduce interference when the cable is long. As a result, these unbalanced line devices must have shorter cables to avoid audio disruptions.

Unicast Streaming

Unicast streaming sends a separate stream of a videoconference to each viewer. This is the default method of streaming in Scopia® XT Desktop server. To save bandwidth, consider multicast streaming.

URI

URI is an address format used to locate a device on a network, where the address consists of the endpoint's name or number, followed by the domain name of the server to which the endpoint is registered. For example, <*endpoint name*>@<*server_domain_name*>. When dialing URI between organizations, the server might often be the Avaya Scopia® PathFinder server of the organization.

URI Dialing

Accessing a device via its URI on page 64.

User profile

A user profile is a set of capabilities or parameter values which can be assigned to a user. This includes available meeting types (services), access to Scopia® XT Desktop and Scopia® Mobile functionality, and allowed bandwidth for calls.

VFU

See Video Fast Update (VFU) on page 65.

VGA

VGA defines a video resolution of 640 x 480 pixels.

Videoconference

A videoconference is a meeting of more than two participants with audio and video using endpoints. Professional videoconferencing systems can handle many participants in single meetings, and multiple simultaneous meetings, with a wide interoperability score to enable a wide variety of endpoints to join the same videoconference. Typically you can also share PC content, like presentations, to other participants.

Video Fast Update (VFU)

Video Fast Update (VFU) is a request for a refreshed video frame, sent when the received video is corrupted by packet loss. In response to a VFU request, the broadcasting endpoint sends a new intra-frame to serve as the baseline for the ongoing video stream.

Video Layout

A video layout is the arrangement of participant images as they appear on the monitor in a videoconference. If the meeting includes a presentation, a layout can also refer to the arrangement of the presentation image together with the meeting participants.

Video Resolution

See Resolution on page 59.

Video Switching

See Switched video on page 63.

Virtual Room

A virtual room in Scopia® XT Desktop and Scopia® Mobile offers a virtual meeting place for instant or scheduled videoconferences. An administrator can assign a virtual room to each member of the organization. Users can send invitations to each other via a web link which brings you directly into their virtual room. Virtual meeting rooms are also dialed like phone extension numbers, where a user's virtual room number is often based on that person's phone extension number. You can personalize your virtual room with PIN numbers, custom welcome slides and so on. External participants can download Scopia® XT Desktop or Scopia® Mobile free to access a registered user's virtual room and participate in a videoconference.

VISCA Cable

A crossed VISCA cable connects two PTZ cameras to enable you to use the same remote control on both.

Waiting Room

A waiting room is a holding place for participants waiting for the host or moderator to join the meeting. While waiting, participants see a static image with the name of the owner's virtual room, with an optional audio message periodically saying the meeting will start when the host arrives.

WUXGA

WUXGA defines a video resolution of 1920 x 1200 pixels.

XGA

XGA defines a Video resolution of 1024 x 768 pixels.

Zone

Gatekeepers like Avaya Scopia® ECS Gatekeeper split endpoints into zones, where a group of endpoints in a zone are registered to a gatekeeper. Often a zone is assigned a dial prefix, and usually corresponds to a physical location like an organization's department or branch.