RADVISION®
an Avaya company

Scopia XT Desktop Server for IP Office

8.2.1

Table of Contents

Chapter 5: Securing Your Scopia XT Desktop Deployment

Chapter 1 | About Scopia XT Desktop Server for IP Office

Scopia XT Desktop Server extends the capabilities of videoconferences hosted on the Scopia XT Server for IP Office by enabling Scopia XT Desktop Clients and Scopia Mobile devices to join.
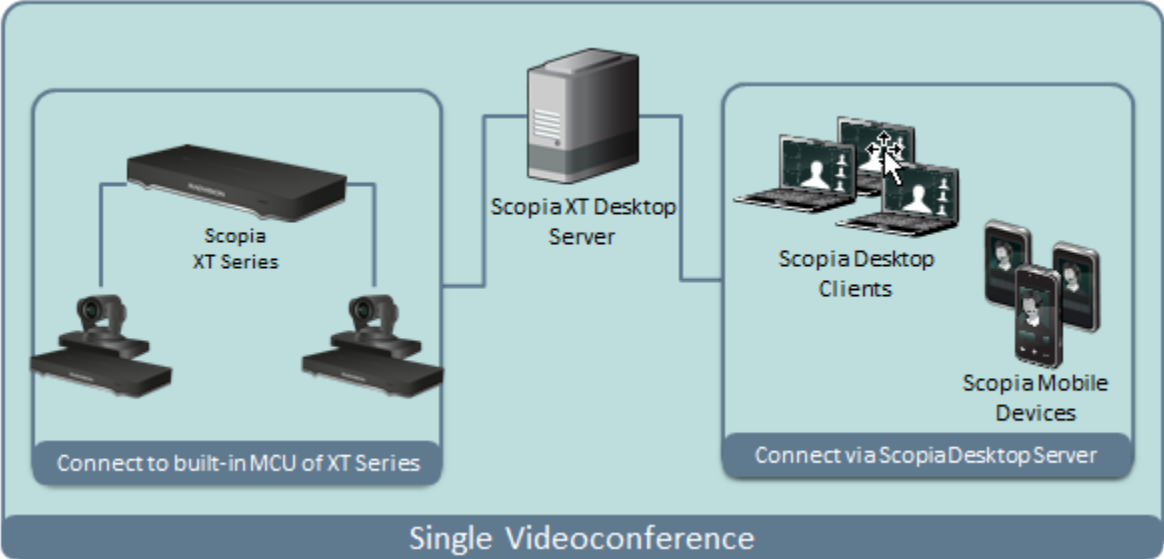
Figure 1: Scopia XT Desktop Server extends meetings to include Scopia XT Desktop Clients

The Scopia XT Server for IP Office solution is especially suited to the communication requirements of Small and Medium Businesses (SMB). Built on the XT Server HD room system, with the highest capacity embedded MCU in the industry today, the Scopia XT Server for IP Office 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.
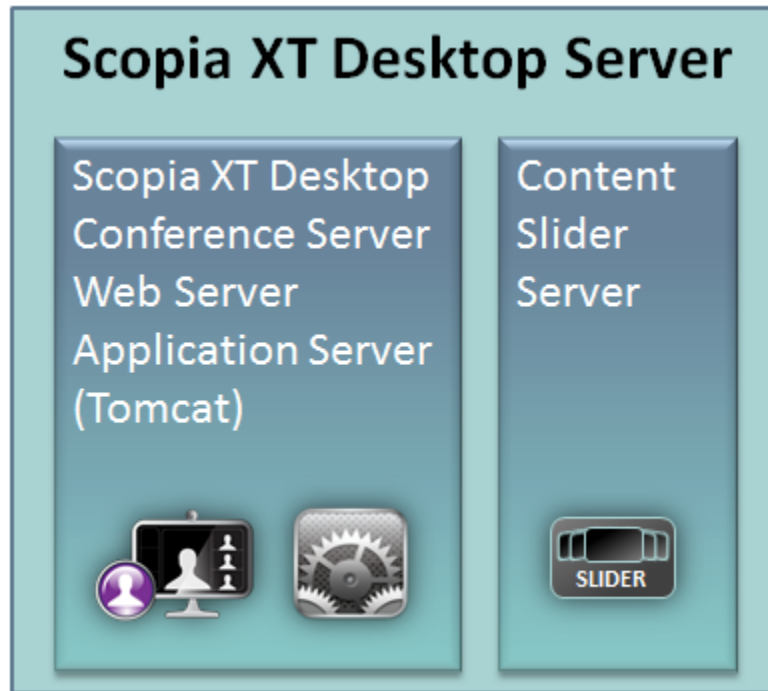
Figure 2: Components of the Scopia XT Desktop Server

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

> ❗ **Important:**
>
> Scopia XT Desktop Servers should be deployed on a physical server, not virtual machines like VMware.

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 20 or later (Mac and Windows)
- Safari 5 or later (Mac and Windows)
- Google Chrome 25 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
- 2 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 Scopia XT Server for IP Office.

- 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)
    - 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, both standard encryption with certificates and a proprietary secure protocol between the client and server:

- HTTPS protocol between Scopia XT Desktop Client and Scopia XT Desktop Server.
- SRTP encryption between Scopia XT Desktop Client/Scopia Mobile and Scopia XT Desktop Server
- TLS encryption between Scopia XT Desktop Server and Scopia Management

Planning the Topology of Scopia XT Server for IP Office with Scopia XT Desktop

Scopia XT Server for IP Office 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 Server 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 or use the full functionality of the system.

The main features of the Scopia XT Server for IP Office include:

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

  The deployment has very few components. You do not need additional hardware like an external MCU, Scopia PathFinder for firewall traversal, or 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 Scopia XT Server for IP Office includes the following:

- Full SMB9 - Advanced MCU level, with up to 8 participants:
  - Eight endpoints

    Or
  - Seven mixed endpoints and PC clients

Figure 3: Scopia XT Server for IP Office Deployment on page 10 shows a typical topology for the Scopia XT Server for IP Office solution. For more information, see the *Solution Guide for Scopia Solution*.
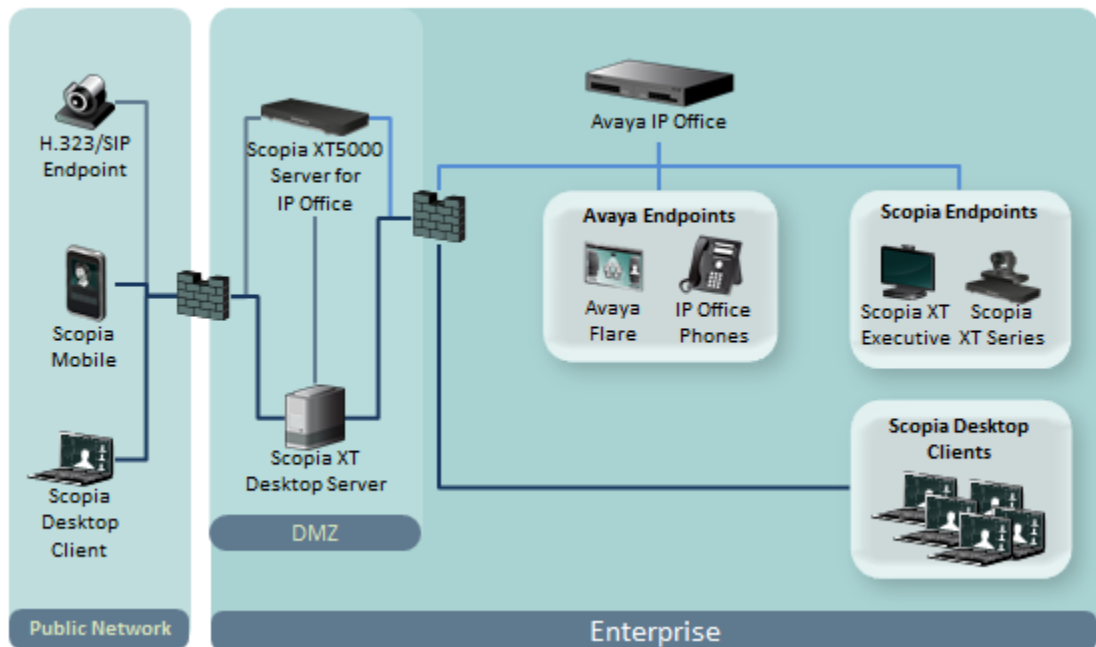
Figure 3: Scopia XT Server for IP Office Deployment

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 Scopia XT Server for IP Office, while using another NIC for Scopia XT Desktop Client connections (Figure 4: 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 28.

Figure 4: 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.

Planning your Bandwidth Requirements

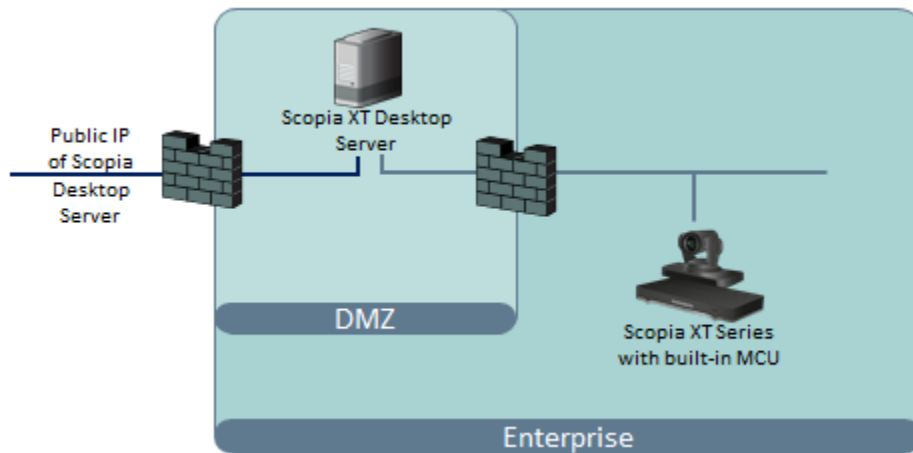The Scopia Solution supports a number of technologies designed to minimize the bandwidth used in videoconferences. For more information on the bandwidth-saving features of Scopia Solution, see *Scopia Solution Guide*. Even so, there are policy decisions you can make to reduce bandwidth further by deciding on the location of video network components and setting bandwidth management policies in your organization. You can estimate the total bandwidth required for Scopia XT Desktop, which includes:

- Bandwidth consumed by videoconference participants connecting to the Scopia XT Desktop Server (Scopia XT Desktop Clients and Scopia Mobile devices)

Use your Scopia XT Desktop bandwidth estimation to do the following:

- Calculate your bandwidth costs, for both external and internal bandwidth (see Calculating the Bandwidth Used by Scopia XT Desktop Participants on page 11).

  For example, to reduce bandwidth, you may decide that all calls going outside your organization are limited to standard definition (SD), or that all calls are SD by default.

Navigation

Calculating the Bandwidth Used by Scopia XT Desktop Participants

This section describes how to calculate the bandwidth required for videoconferences with Scopia XT Desktop participants (both Scopia XT Desktop Clients and Scopia Mobile devices).

The Scopia XT Desktop Server coordinates videoconferences between Scopia XT Desktop Clients/Scopia Mobile devices and the Scopia XT Server for IP Office.

Table 1: Default bandwidth used for one connection on page 12 lists the default bandwidth used for each connection between the participant and the Scopia XT Desktop Server.

Table 1: Default bandwidth used for one connection

Type of connection	Default bandwidth required
Upload bandwidth for one SD participant	384 kbps
Download bandwidth for one SD participant	384 kbps
Upload bandwidth for one HD participant	1024 kbps
Download bandwidth for one HD participant	1024 kbps

Calculating Scopia XT Desktop Bandwidth Usage

This topic describes how to calculate the bandwidth required for adding Scopia XT Desktop Clients and Scopia Mobile devices to a videoconference hosted on the Scopia XT Server for IP Office using it's built-in MCU (see Figure 5: Upload and download bandwidths for Scopia XT Desktop on page 12)
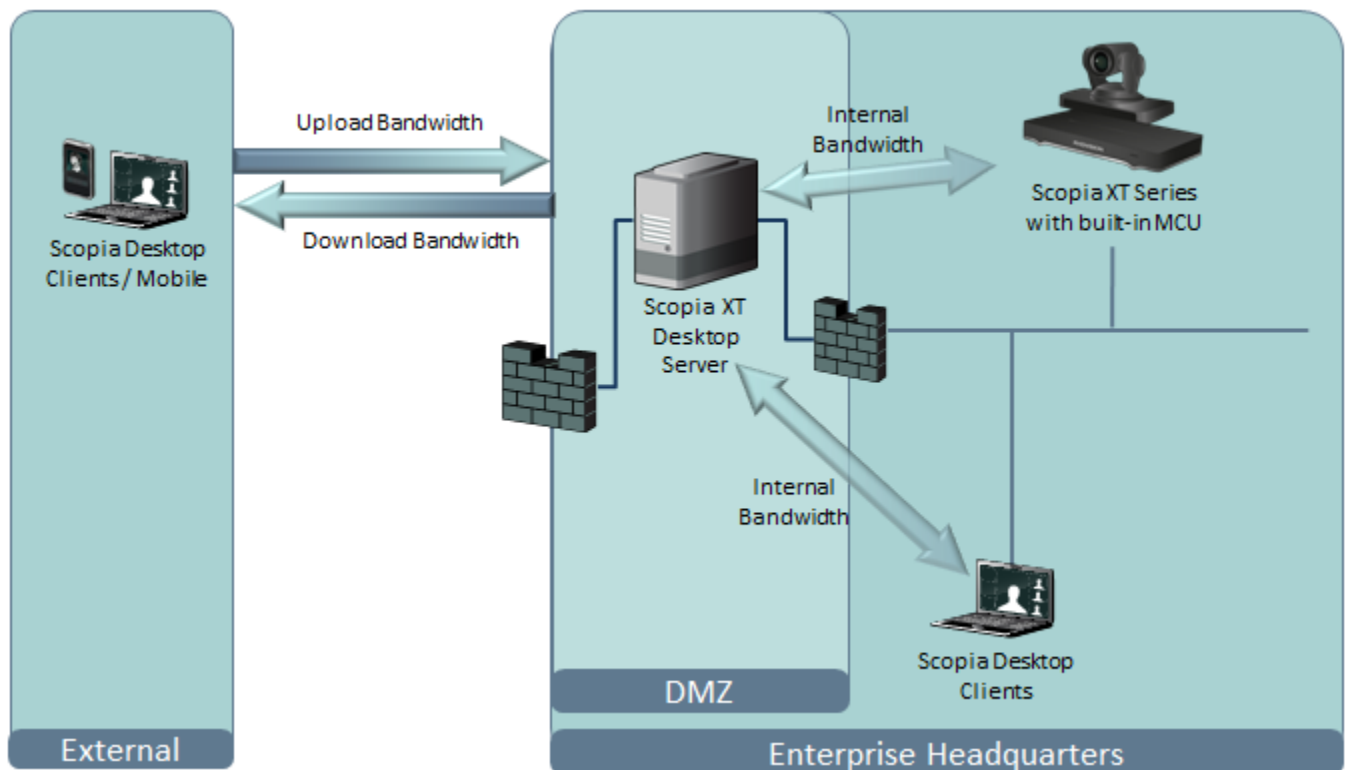
Figure 5: Upload and download bandwidths for Scopia XT Desktop

The bandwidth used for each Scopia XT Desktop Client participant is defined in the server settings (see Figure 6: Setting maximum bandwidth in Scopia XT Desktop Server on page 13).
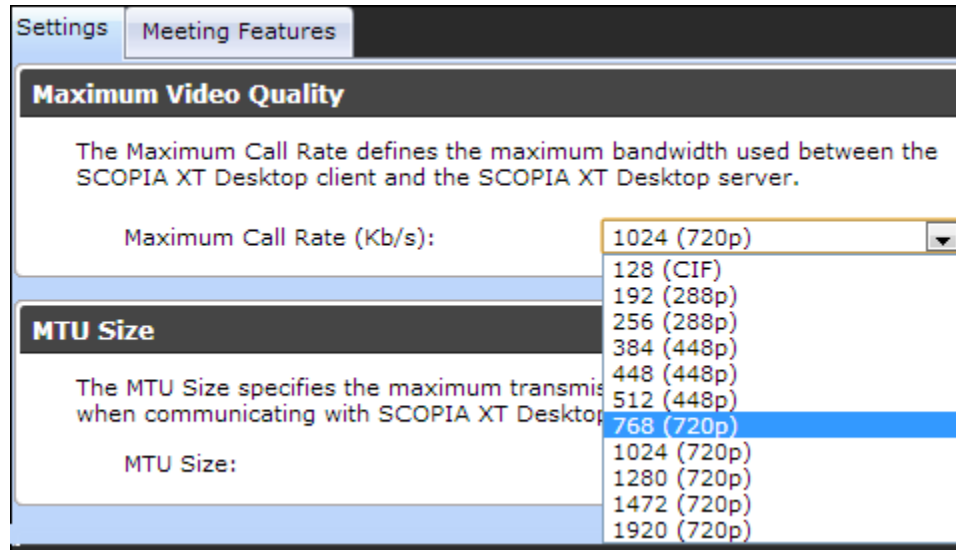
Figure 6: Setting maximum bandwidth in Scopia XT Desktop Server

The formula for calculating external bandwidth is as follows:

```
Total upload bandwidth = upload bandwidth per participant × num of internet participants
Total download bandwidth = download bandwidth per participant × num of internet participants
```

For example, if the defined call rate is 384 kbps, each participant uses 384 kbps for uploading and 384 kbps for downloading. So if 5 Scopia XT Desktop participants connect to a videoconference from the external internet at 384 kbps, the bandwidth for these participants is 384 x 5 = 1920 kbps for upload and 1920 kbps for download.

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.
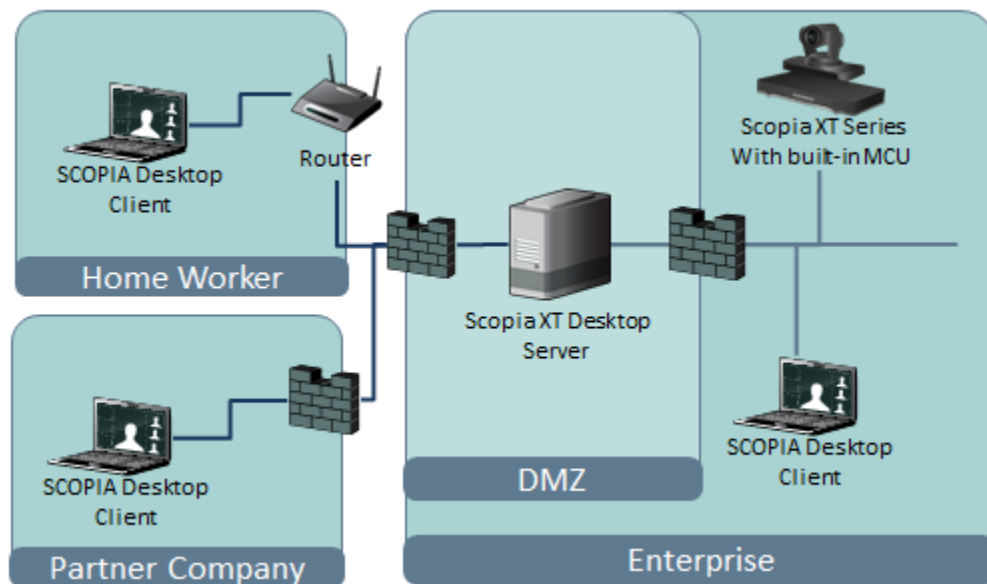
Figure 7: Locating the Scopia XT Desktop Server in the DMZ

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 2: 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 3: 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 4: 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 5: 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 6: 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 2: 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)	Scopia XT Server for IP Office	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)	Scopia XT Server for IP Office or Scopia XT Desktop Client	Enables media connection to the Scopia XT Server for IP Office, and the Scopia XT Desktop Client or Scopia Mobile.	Media cannot be passed from the Scopia XT Server for IP Office 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 3: 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	Scopia XT Server for IP Office	Enables connection to Scopia XT Desktop meetings.	Cannot connect to the meeting	Mandatory
3337	TCP (XML)	Scopia XT Server for IP Office	Enables meeting cascading connection to the Scopia XT Server for IP Office	Meeting cascading connection is disabled	Mandatory
3336	TCP	Scopia XT Server for IP Office	Enables meeting control with Scopia XT Server for IP Office	Meeting control is disabled	Mandatory

Table 4: 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 5: 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 6: 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).

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 Securing Web Connections and Media Traffic to Scopia XT Desktop Server on page 37).

  > ❗ **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 Scopia XT Server for IP Office, your XT Server 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**.

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 Scopia XT Server for IP Office which hosts videoconferences with its built-in MCU in the **XT Server Address** window, and select **Next**.
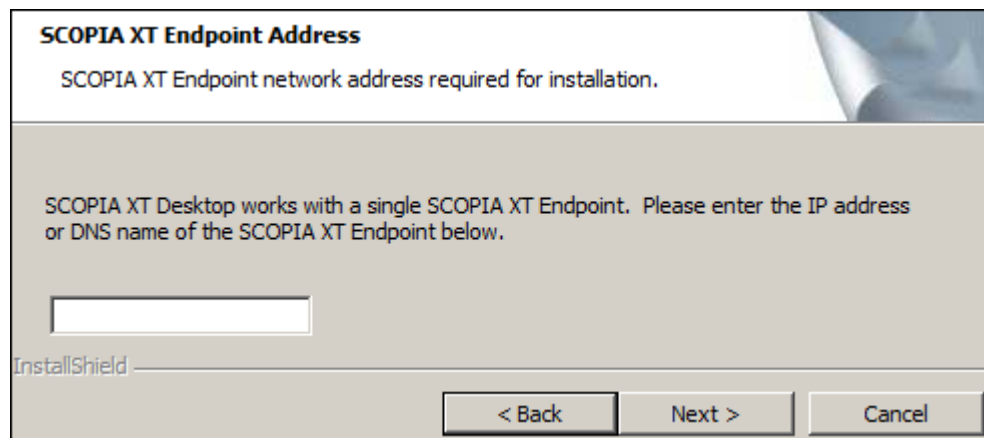

Figure 10: Specifying the XT Server with built-in MCU

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 Scopia XT Server for IP Office.

   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
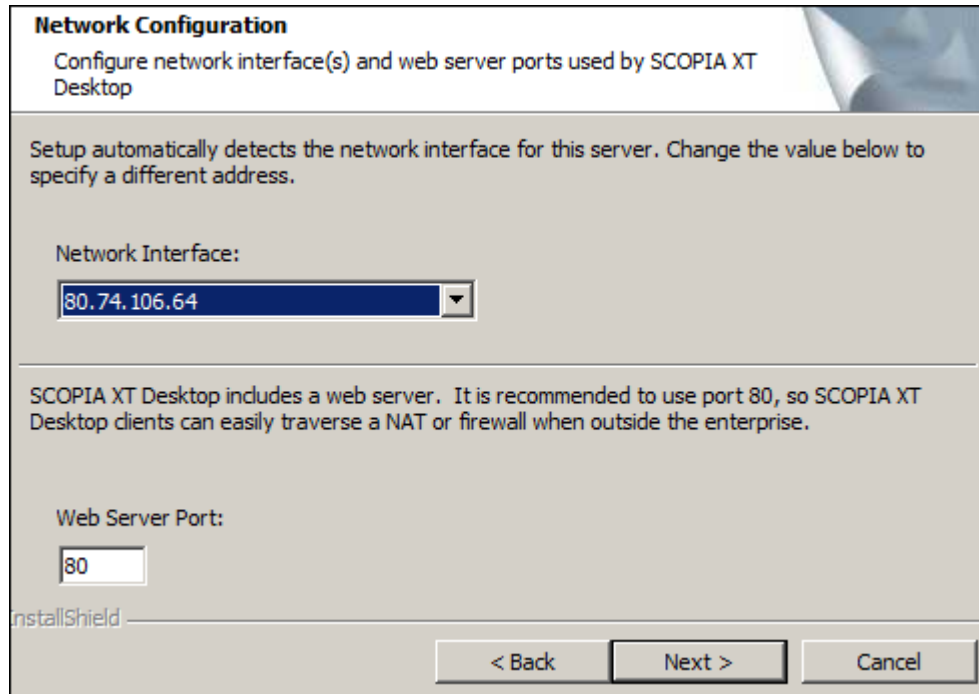
Figure 11: Selecting the NIC pointing to the internal network

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.
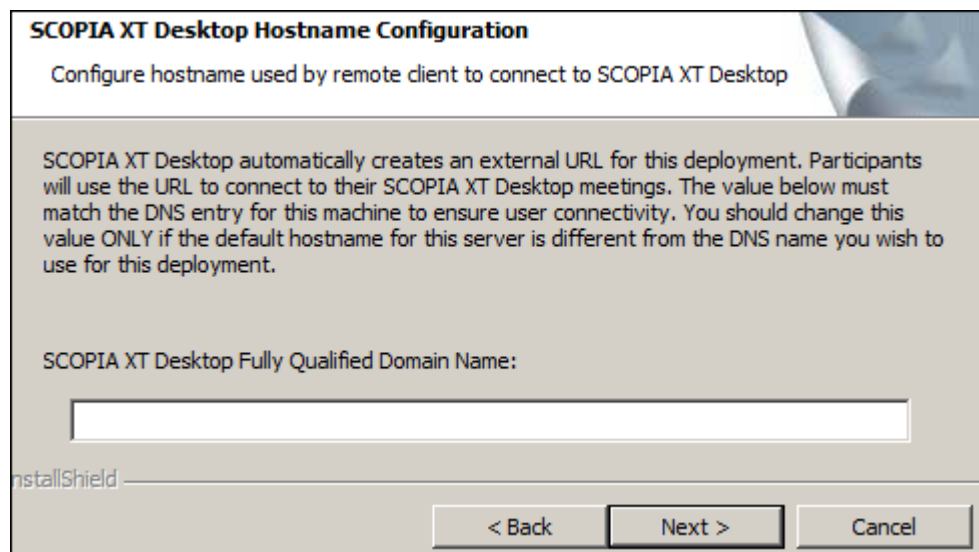

Figure 12: Defining the public address of the Scopia XT Desktop Server

> **❗ 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 22) and enable the following programs:

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

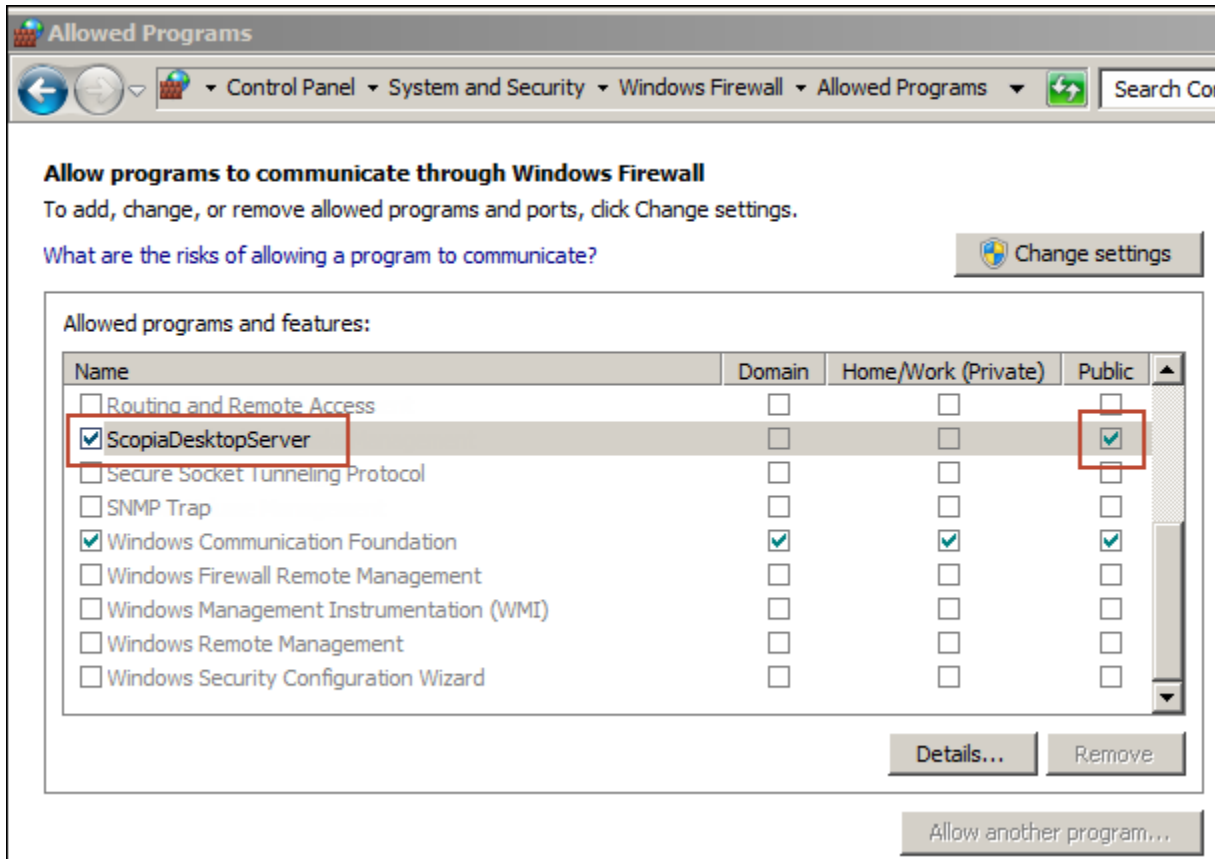- **ScopiaDesktopServer**, located at *<install_dir>\ConfSrv\ConfSrv.exe*

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 Scopia XT Server for IP Office 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**.
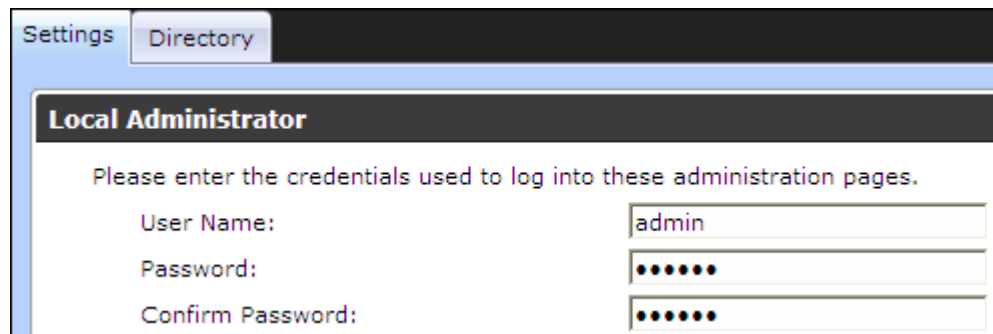
3. Select **Sign In**.

_____

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.

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 Server

About this task

This section describes how to connect the Scopia XT Desktop Server with the Scopia XT Server for IP Office with its built-in MCU.

Procedure

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

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

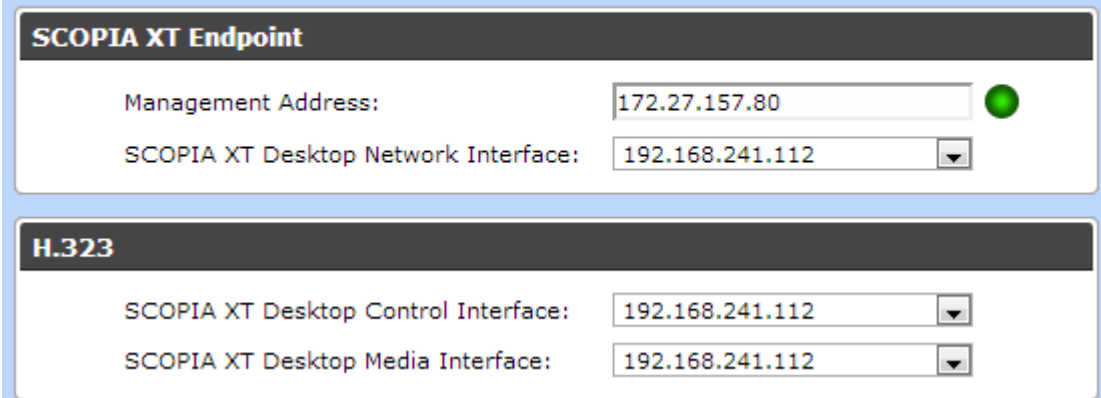3. Enter the IP address of the XT Server with its built-in MCU in the **Management Address** field.

Figure 15: Setting the address of the managing Scopia XT Server for IP Office

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 Scopia XT Server for IP Office, 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.

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 Scopia XT Server for IP Office, 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.
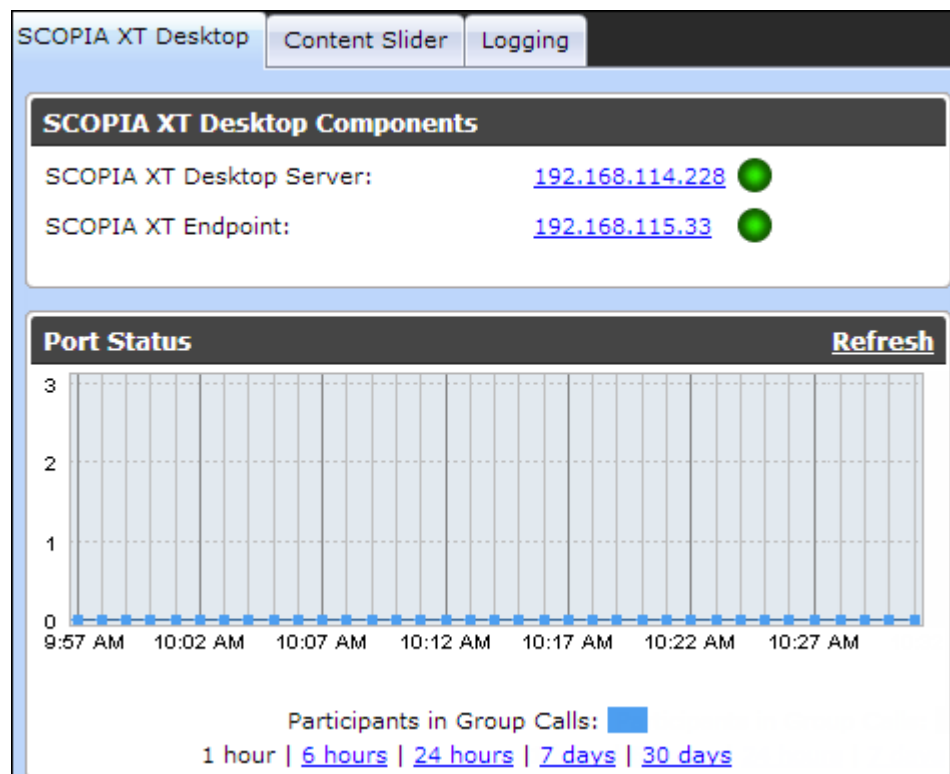

Figure 17: Viewing the connection status with Scopia XT Desktop Server

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 virtual room 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.
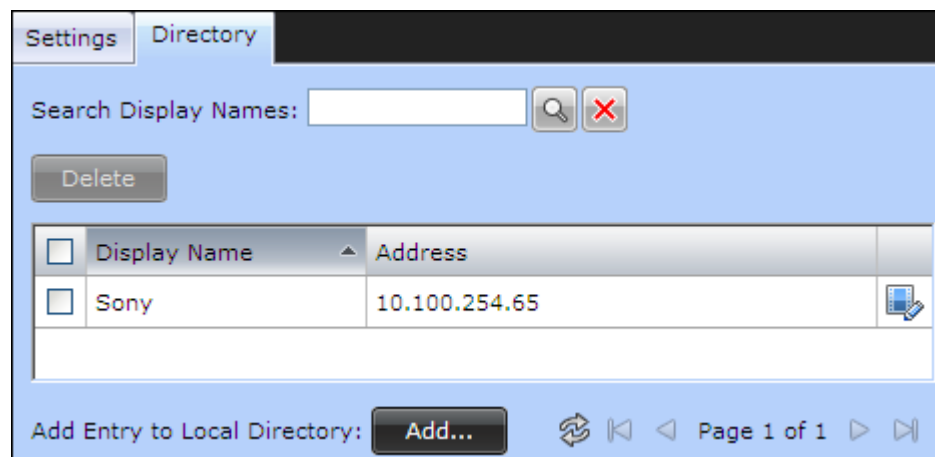
Figure 18: Local database of endpoints

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.

Procedure

1. Access the Scopia XT Desktop Server Administration web interface.

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

3. Select the **Settings** tab.

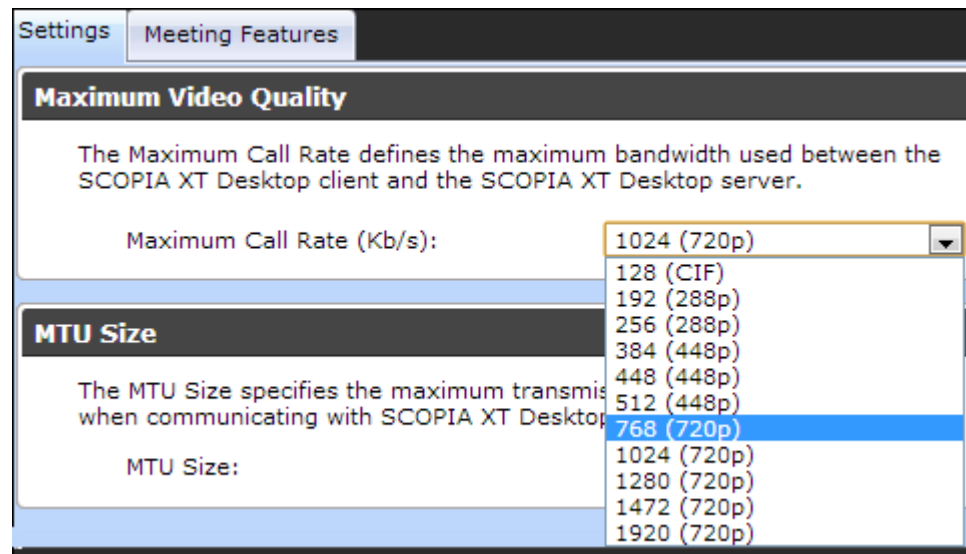4. Select the maximum call rate in the **Maximum Video Quality** section.

Figure 19: Setting maximum bandwidth in Scopia XT Desktop Server

Defining Scopia XT Desktop Server Public Address and Other Client Connection Settings
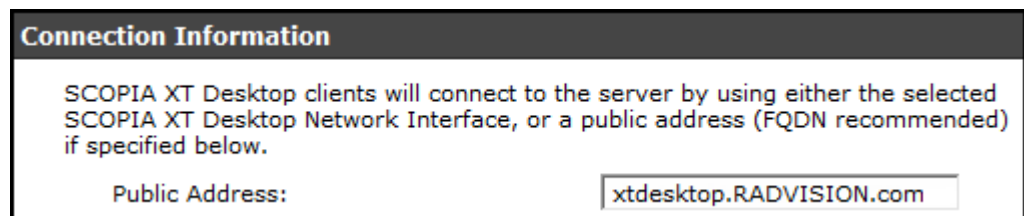
About this task

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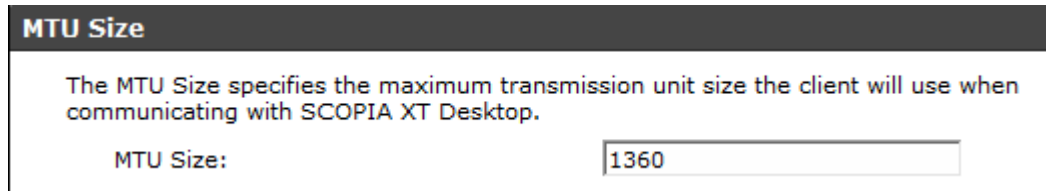
   If a DNS name is not specified in the **Public Address** field, the Scopia XT Desktop Server network interface address is used.

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 Server 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

> **❶ Important:**
>
> This value must remain the same across all network components to guard against packet fragmentation.

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

Enabling or Disabling Scopia XT Desktop Client Features

About this task

This section describes how to enable or disable features in the Virtual Room 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.

> **❶ 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.

This section describes how to make global changes for the virtual rooms of all Scopia XT Desktop Server users.

Procedure

1. Access the Scopia XT Desktop Server Administration web interface.

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

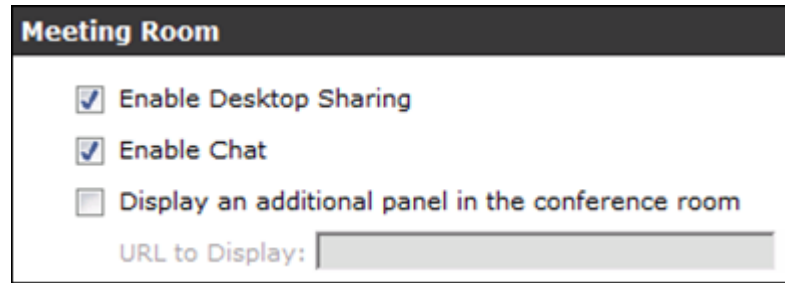3. Select the **Meeting Features** tab.

Figure 22: Enabling or disabling client videoconferencing features

4. Enter the fields as described in

Table 7: Settings for the Scopia XT Desktop Client Virtual Room 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 Virtual Room window of Scopia XT Desktop Client.
Enable Chat	Determines whether to display the chat window pane in the Virtual Room 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 Virtual Room 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 Virtual Room window of Scopia XT Desktop Client.
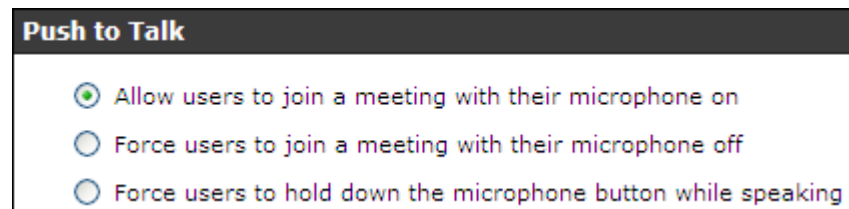

Figure 23: Push to Talk Settings

Enter the fields as described in

Table 8: 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. Configure the **Security** section to determine encryption parameters.

Figure 24: Security Settings

Enter the fields as described in

Table 9: Defining security settings between Scopia XT Desktop Server and Scopia XT Desktop Client

Field	Description
Encrypt Media	Determines whether to encrypt the media (audio, video and presentation) using SRTP between the Scopia XT Desktop Server and Scopia XT Desktop Client/Scopia Mobile. **❶ 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.

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

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 (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 25 and later)
- Internet Explorer (version 6 and later, for windows)
- Firefox (version 20 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*

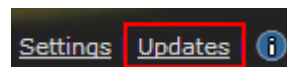2. Select **Updates** in the top-right corner of the web portal.

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

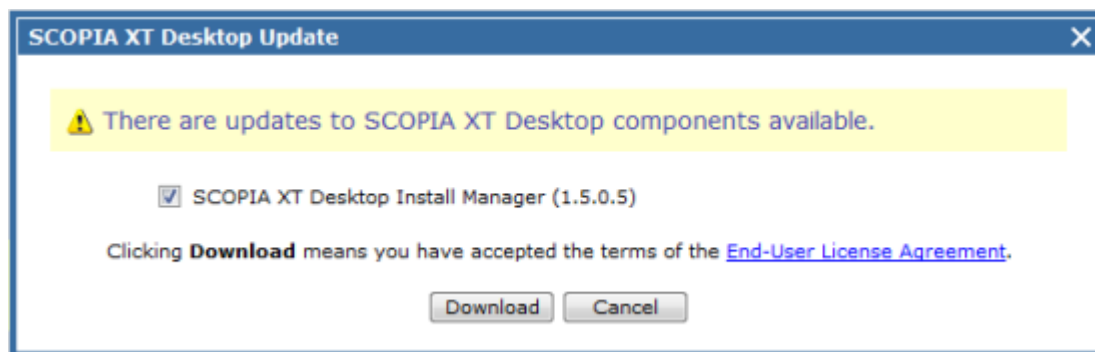The **Scopia XT Desktop Update** window opens.

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.
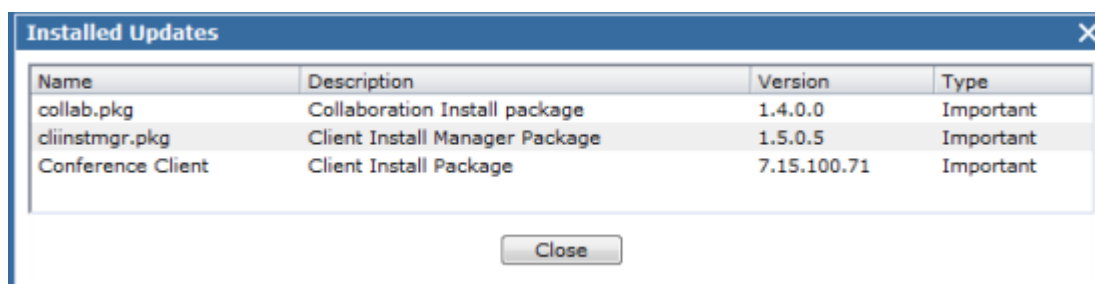
Figure 27: Installed Updates and Components

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 communications using the encryption keys held in certificates which are uploaded to the various deployment components.

ⓘ 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.

There are two types of certificates which can be installed.

- Install certificates on the Conference Server to encrypt the media travelling between Scopia XT Desktop Clients and the Scopia XT Desktop Server. These certificates also secure all web traffic to the Scopia XT Desktop Server, for example, when you access the server's web administration user interface or when a user accesses their meeting portal.

- Install certificates in the server's keystore file, part of the Java installation, to secure communications with Scopia Management and other components. Mutual authentication requires a certificate stored on each side of the communication line.

The details of each certificate type and their configuration are detailed in the sections below:

Navigation

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.

Figure 28: 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**.

Securing Web Connections and Media Traffic to Scopia XT Desktop Server

About this task

This procedure explains how to secure all web traffic to the Scopia XT Desktop Server with HTTPS, including the administrator interface and user portals. This also secures the actual media (audio and video) of any videoconferences which take place.

The certificate which secures web traffic and videoconference media is installed in the Scopia XT Desktop Conference Server.

❶ Important:

This procedure requires a signed certificate ready for the Scopia XT Desktop Server. You can either use the certificate shipped with the server, or create your own unique certificate.

Procedure

1. Select **Start > All Programs > Scopia XT Desktop > ConfigTool**.

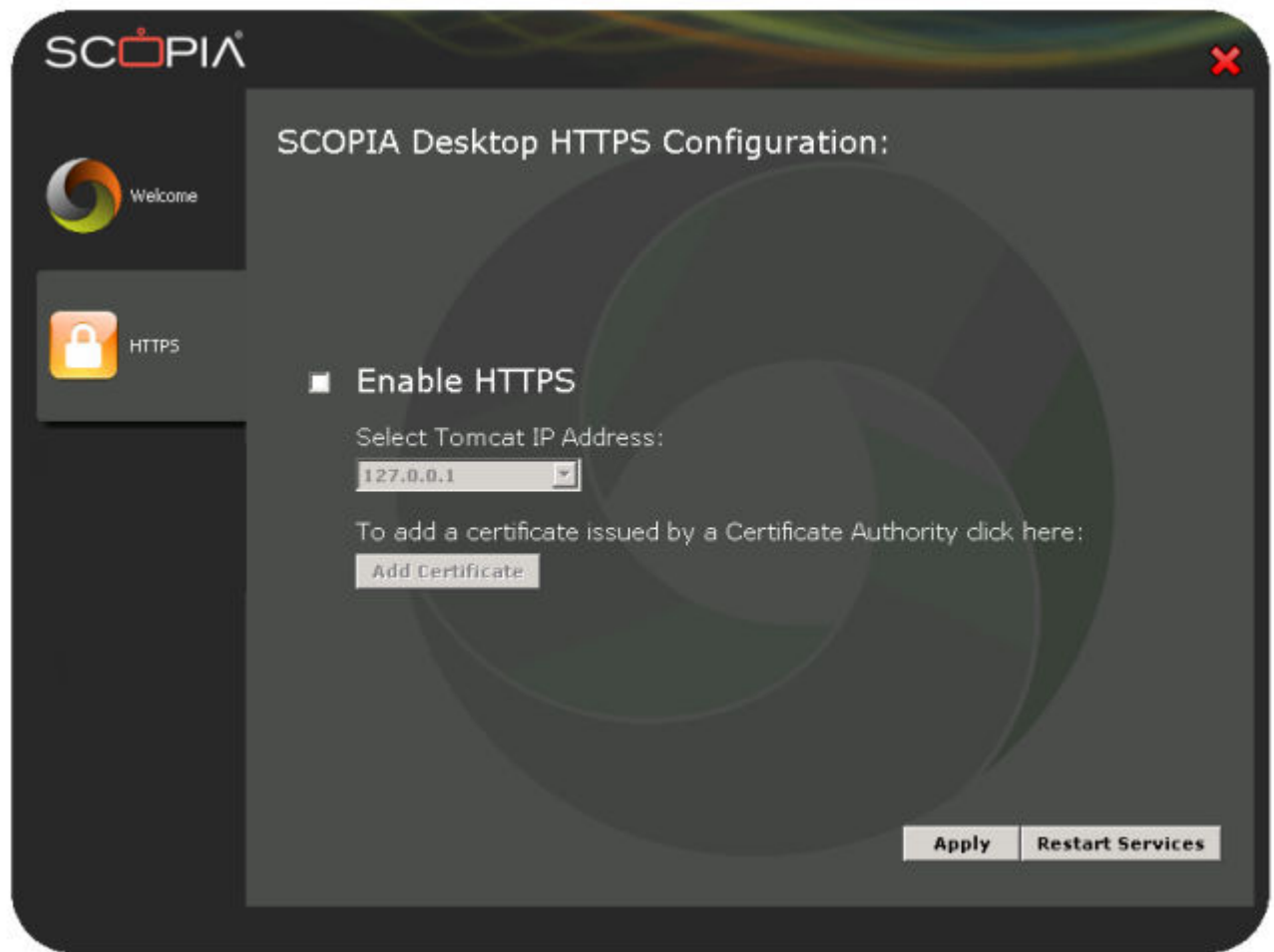2. Select the **Enable HTTPS** check box in the **HTTPS** tab.

Figure 29: Adding a certificate to Scopia XT Desktop Server

3. Select **Apply**.

4. Select **Add Certificate** to upload an existing signed certificate.

5. Stop the service **Scopia XT Desktop Conference Server**.

6. Navigate to *<SD_install_dir>\Confsrv*

7. Run the **Certificate Configuration Utility** by launching *CertificateConfiguration.exe* file.

8. If the certificate is installed in the local machine's certificate store:

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

   b. Select **Select Certificate**.

   c. Select the certificate from the list.

9. If the certificate is in PKCS12 format:

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

   b. Browse to the PKCS12 certificate and select it.

   c. Enter the private key password for the certificate.

10. Select **OK**.

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

12. Select **Apply**.

13. Select **OK**.

14. Select **OK**.

15. Start the service **Scopia XT Desktop Conference Server**.

16. Select **Restart Services**.

17. Change the URL in the **Invitations** section of the Scopia XT Desktop Administration web interface to use the secure HTTPS protocol:

    a. Log into the Scopia XT Desktop Administration web interface.

    b. Select **Messages and Invitations** on the sidebar.

    c. Select the **Invitations** tab.

    d. In the **Desktop Access** section, verify all URLs have the prefix of `https`.

    ❶ **Important:**

    By default, there are two URLs present in this section.

RADVISION®
an Avaya company

About Radvision

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