Administering the Avaya Scopia® Streaming and Recording Server

Release 8.3.3
December 2015

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

“Hosted Service” means a hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES IF YOU PURCHASE A HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA’S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail

account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than one Instance of the same database.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

Contents

Chapter 1: Introducing Avaya Scopia® Streaming and Recording

Avaya Scopia® Streaming and Recording server

Avaya has introduced a new component, the Avaya Scopia® Streaming and Recording server (Scopia® SR). Scopia® SR is the Avaya next generation HD streaming and recording platform, bringing significant enhancements to the Avaya Scopia® solution for streaming and recording. The Avaya Scopia® Streaming and Recording server replaces the Avaya Scopia® Content Center Recording server (SCC) server.

Before you install Scopia® SR, you must make a number of decisions in order to ensure that the solution exactly matches the requirements of your deployment. For example, you must make a decision about scalability in accordance with the size of your enterprise. For a small enterprise, you can choose a single appliance which houses all of the Scopia® SR components. For a large enterprise, you can choose a distributed solution with multiple media nodes. Scopia® SR is highly flexible and easily adaptable, whatever your requirements. In addition, you must decide if you require a high degree of redundancy and whether you would like to enable external access and storage in the 'cloud'.

If you would like users outside of the enterprise to access recordings, you can deploy Scopia® SR in a Demilitarized Zone (DMZ) or use a reverse proxy server. In this way, the Scopia® SR is similar to the Avaya Scopia® Web Collaboration server (WCS). If you would like users outside of the enterprise to access the videoconference, you must deploy the WCS in a DMZ or use a reverse proxy server. Scopia® SR and WCS also support a Network Address Translation NAT Firewall configuration in a DMZ deployment. NAT Firewall is an additional layer of security. It blocks unrequested inbound traffic.

For more information, see the *Avaya Scopia® Solution Solution Guide*, which is available on https://support.avaya.com/.

Components

The Scopia® SR consists of the following components:

- Scopia® SR Conference Point™ (CP)
- Scopia® SR Delivery Node™ (DN)
- Scopia® SR Virtual Delivery Node™ (VDN)
- Scopia® SR Manager™

Scopia® SR Conference Point™

You must configure a conference point to capture H.323 video content and deliver live and on demand webcasting. The Scopia® SR conference point includes an embedded transcoder to convert H.323 calls into Windows Media or .MP4 format.

Each conference point must be associated with a delivery node. A delivery node streams and optionally archives the content captured by the conference point and delivers it to client systems.

You can configure a conference point to be in a geographic location. This means that you can assign a location to one or more conference points which coincide with locations set for Scopia® MCUs in Scopia® Management. When a program starts, Scopia® Management includes the desired location, and a conference point close to the MCU can be selected. If there are no conference points matching the location passed by Scopia® Management, then any conference points without a location are treated as a single pool of conference points, and one of those is selected. If there are no conference points available, the call fails.

Each conference point has a limit to the number of simultaneous high definition or standard definition calls it can handle.

The CP includes the following features:

- Video conferencing H.323 capture and transcoding
- High definition support
- Scalability for up to 10 high definition (1080p) or 30 standard definition (480p) calls, which include an audio/video and data stream each
- G.711 and AAC-LC audio capture and transcoding
- H.263, H.263+, H.264 capture and transcoding

The media node or all-in-one server can include the CP and transcoder components. The H.323 video and audio and the optional H.239 stream received by the CP are sent to the internal encoder for transcoding into Windows Media™ format or H.264/AAC MP4/MPEGTS/HLS formats.

- Operating Systems: The transcoder runs on the Windows Server 2012 R2 64-bit operating system with Hyper-V (an add-on to Windows Server 2012 that allows a Linux operating system to run on the same server). The CP runs on the CentOS 6.6 64-bit operating system. Using virtualization software, this enables both applications to run two different operating systems on the same server.
- Licensing: The server requires a single media node license for the CP. The license defines the number of simultaneous H.323 connections. An H.323 connection includes audio, video, and an optional H.239 secondary stream.
- Transcoding H.323 audio and Video: The CP connects H.323 calls to the Scopia® MCUs (Multipoint Control Units). When it establishes a video connection, the CP sends the audio and video data from the MCU to the internal transcoder. The transcoder converts the data into a format that is suitable for streaming.
- Transcoding with H.239: H.239 is an ITU recommendation that allows for establishment of multiple channels within a single H.323 session. Existing videoconference equipment can be used to stream audio and video and a secondary channel can stream a slide presentation or another data stream to the viewers of a program. This function is typically used to stream slide presentations synchronized with live audio and video. If a program uses a secondary H.239 channel, the encoder inputs the second stream, decodes, scales and mixes it with the main

video input for transcoding/streaming. The streams are then sent to the DN for delivery to the distribution network. The dual stream can also be recorded as a single MP4 program.

- High definition support: The CP supports high definition video and higher rate streaming quality and bandwidth. The CP supports the following ITU recommendations:
  - H.261 up to CIF Video
  - H.262 up to CIF video
  - H.263 up to CIF video
  - H.264 up to 1080p video
  - H.263+ up to 1024 x 768 H.239 data
  - H.264 up to 1080p H.239 data
  - G.711 audio
  - AAC-LC audio

  The CP negotiates up to H.264 Level 3.2 video at 1.92 Mbps, and accepts up to 1080p and down to H.261 QCIF along with G.711 or AAC-LC audio. The streaming resolution and bandwidth rate depend on what you select for the bitrate when creating the program and what the Scopia® MCU negotiates.

Scopia® SR Delivery Node™

The DN provides on-demand and broadcast video delivery. Used alone or in a hierarchy of devices, the DN supports thousands of concurrent streams. The DN uses intelligent routing, content caching, and inherent redundancy to ensure transparent delivery of high-quality video.

Delivery nodes (DN) store all content that is created by the conference point and deliver the content to client systems. You must associate the conference point with the delivery nodes.

The Delivery Node Details dialog displays a list of **Source Programs** and **Distributed Programs**. Source programs are programs for which this delivery node is the main source for storage. Distributed programs are programs which other delivery nodes have forwarded to this delivery node.

Scopia® SR Virtual Delivery Node™ (VDN)

A virtual delivery node (VDN) delivers content to a global content delivery network (CDN) provider for cloud-based viewer playback. The appliance and the network of the CDN act as one delivery mechanism. Therefore, the VDN appliance and the CDN together create the Scopia® SR VDN solution.

Upon program creation, the publisher includes the options of distributing the program to delivery nodes and to the Scopia® SR VDN solution. VDN supports publishing recordings as well as live broadcast.

You can view the programs distributed to the VDN appliance and to be delivered to the CDN with the associated status of the program.

Scopia® SR currently only supports the HighWinds™CDN.

Scopia® SR Manager™

The Scopia® SR Manager provides a web-based interface to configure and manage streaming and recording software, devices, services, and users. The Scopia® SR Manager application resides on a single hardware platform and provides access to all content in the Scopia® SR environment.

There are two Scopia® SR Manager portals:

- Scopia® SR Manager Administrator Portal: Administrators use this portal to perform the following tasks:
  - Configure and manage video communications devices
  - Manipulate content
  - Monitor user roles
  - Create and set global policies
  - Identify best practices and usage effectiveness through comprehensive reporting
  - Allow access to the VDN for CDN deployment or programs
  - Manage organizations, in a multi-tenant deployment (including what profiles, categories and CDN settings they can access)
  - Create and manage viewer mappings to associate viewers with the appropriate distribution node location
- Scopia® SR Manager Viewer Portal: Viewers select the **Recordings and Events** tab on the main Avaya Scopia® Desktop page to access the viewer portal. Viewers can perform the following tasks:
  - View programs
  - Navigate categories
  - View live or on-demand programs

Related links

Example of a direct DMZ deployment on page 13
Example of a reverse proxy deployment on page 15
Example of a distributed deployment on page 16
Example of a cloud deployment on page 19
Scalability on page 20
System requirements on page 21

Example of a direct DMZ deployment

Figure 1: Direct DMZ Deployment on page 14 displays an example of a Scopia® SR deployment that is situated directly in the demilitarized zone (DMZ). The deployment is a centralized or all-in-one solution, which means that all of the Scopia® SR components reside on a single server. An all-in-one solution is suitable for a small or medium deployment that does not require redundancy.

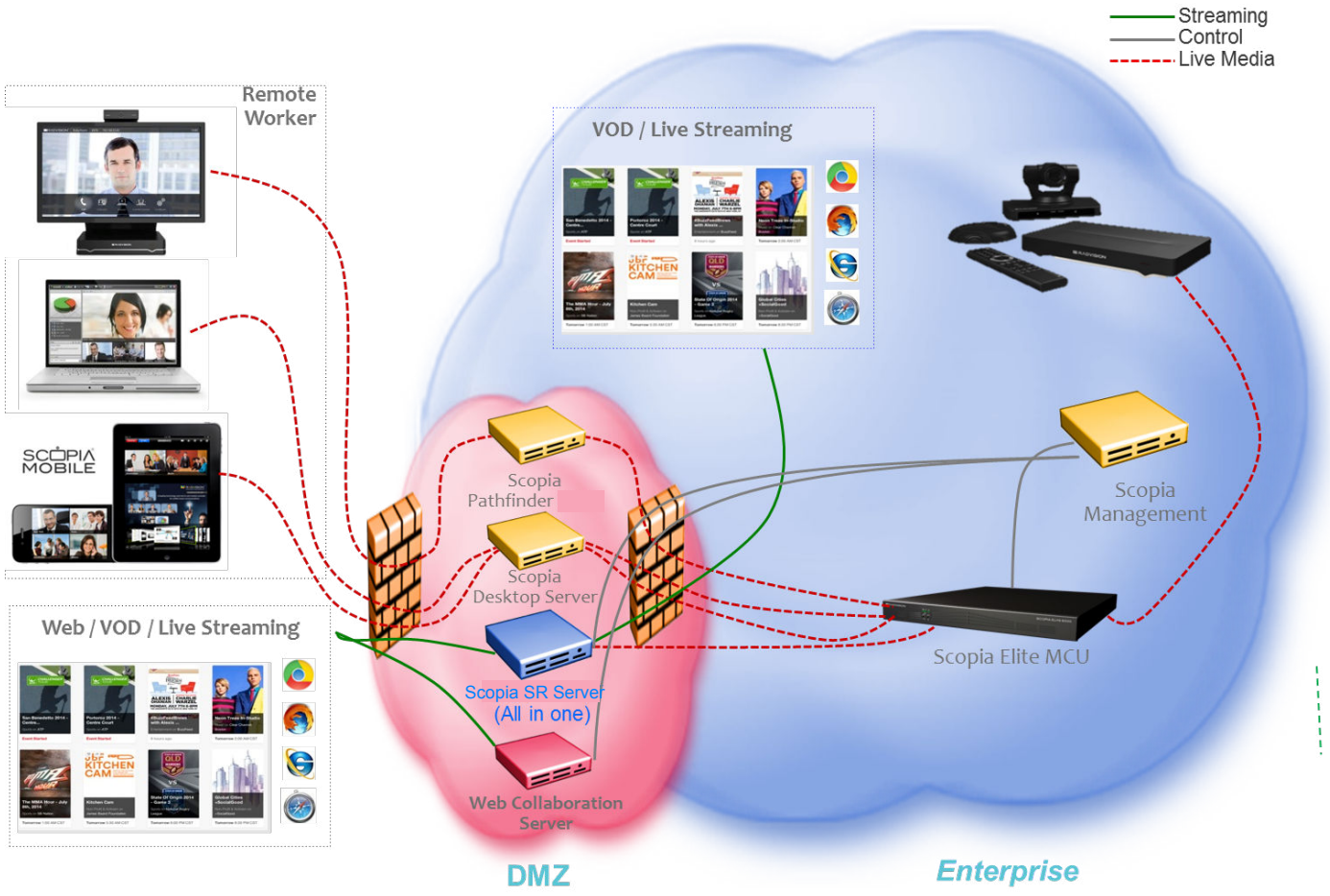


Figure 1: Direct DMZ Deployment

In a typical small deployment, all of the Scopia® SR components reside on a single server. The Scopia® SR Manager and the transcoder run directly on the host server. The conference point (CP), delivery node (DN), and, optionally, a virtual delivery node (VDN) run as virtual servers. VDNs enable enterprises to host recordings in the cloud.

Figure 2: Components in an All-In-One Deployment

Related links

Avaya Scopia Streaming and Recording server on page 10

Example of a reverse proxy deployment

Figure 3: Reverse Proxy Deployment on page 16 displays an example of a Scopia® SR deployment that includes a reverse proxy server. The deployment is a centralized or all-in-one solution.

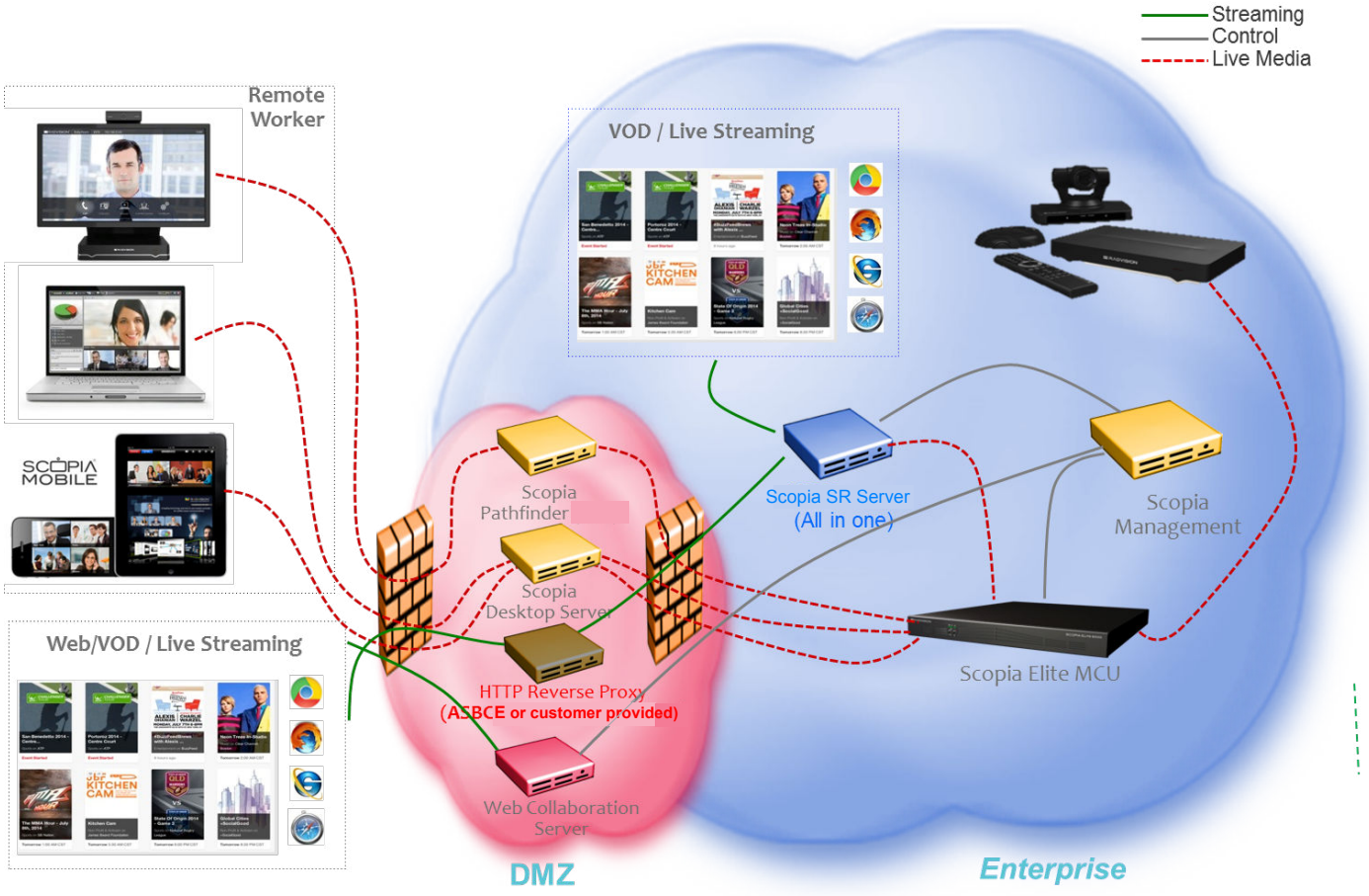


Figure 3: Reverse Proxy Deployment

Related links

Avaya Scopia Streaming and Recording server on page 10
Reverse proxy servers on page 148

Example of a distributed deployment

Figure 4: Distributed Deployment on page 17 displays an example of a distributed Scopia® SR deployment. The deployment also uses a reverse proxy server. In this example, there are several delivery nodes (DNs) and/or conference points (CPs). This configuration enables Scopia® SR to host large numbers of recordings. A configuration with multiple media nodes can also provide redundancy.

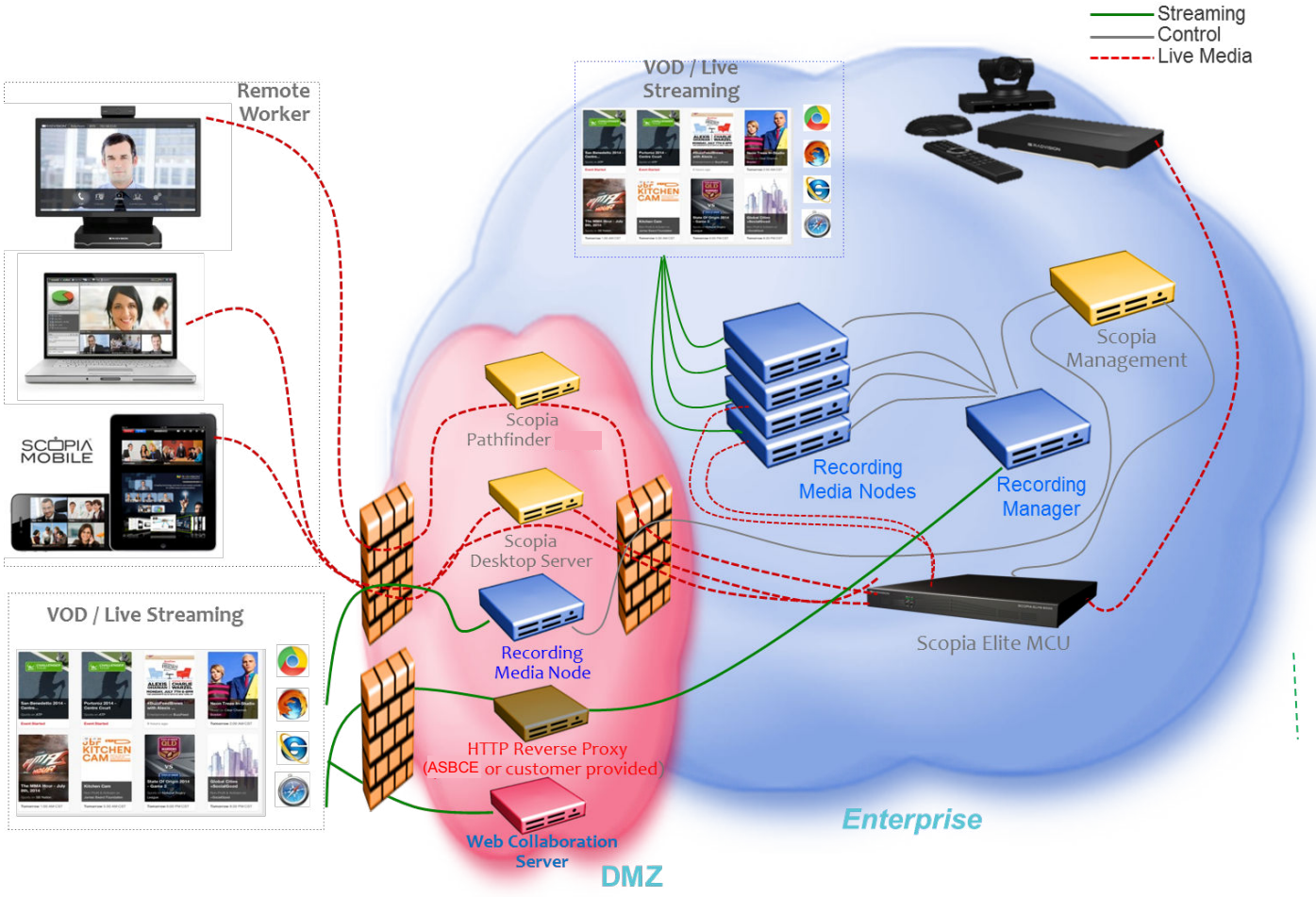


Figure 4: Distributed Deployment

In a typical distributed deployment, the Scopia® SR Manager resides on a separate, dedicated server. The various media nodes can operate as CPs, DNs, or virtual delivery nodes (VDNs). VDNs enable enterprises to host recordings in the cloud.

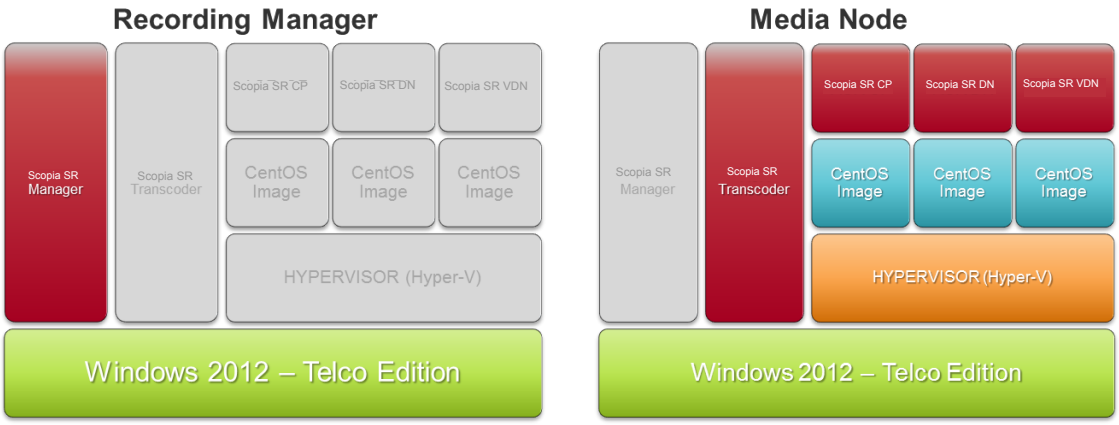


Figure 5: Components in a Distributed Deployment

Related links

Avaya Scopia Streaming and Recording server on page 10
Deployment choices for centralized and distributed solutions on page 18

Deployment choices for centralized and distributed solutions

The Scopia® SR server performs three functions:

- Content recording
- Content delivery
- Content management

Content delivery, in this context, refers to streaming.

When you run the configuration utility (or *wizard*), you choose between three deployment options for the Avaya Scopia® Streaming and Recording server (Scopia® SR). You can choose to house all three functions on a single server. Alternatively, you can choose to house the management function on one server and the recording and delivery functions on another server or servers. This configuration involving multiple servers is called a distributed system.

If you intend to house all three functions on a single server, you must run the configuration utility on that server. On the selection screen, you must choose **All-in-One**.

If you intend to install a distributed system, you must run the configuration utility on each server in the system. On the selection screen, you must choose whether the server will house the content management or the recording and delivery functions.

Related links

Example of a distributed deployment on page 16
All-in-one on page 19
Content Management components only on page 19
Media Node only on page 19

All-in-one

If your Scopia® SRdeployment is an all-in-one system, all Scopia® SR components reside on a single server.

Related links

Deployment choices for centralized and distributed solutions on page 18

Content Management components only

If your Scopia® SR deployment is a distributed system, the Scopia® SR components reside on multiple servers. You must install the content management components on one server and install the recording and delivery components on another server or servers.

For a distributed system, you must run the Scopia® SR Configuration Utility on each of the servers. When you are running the configuration utility on the server which will act as the content management server, you must select **Content management components only** on the Select Configuration dialog of the configuration wizard.

Related links

Deployment choices for centralized and distributed solutions on page 18

Media Node only

If your Scopia® SR deployment is a distributed system, the Scopia® SR components reside on multiple servers. You must install the content management components on one server and install the recording and delivery components on another server or servers.

For a distributed system, you must run the Scopia® SR Configuration Utility on each of the servers. You can install the recording component on one server and the delivery component on another server. Alternatively, you can install both aspects on a single server. In this distributed configuration, these servers act as media nodes. When you are running the configuration utility on a server which will act a media node, you must select **Media Node only** on the Select Configuration dialog of the configuration wizard.

A media node that is used for the recording component is called a Conference Point (CP).

A media node that is used for the delivery component is called a Delivery Node (DN).

Related links

Deployment choices for centralized and distributed solutions on page 18

Example of a cloud deployment

Figure 6: Cloud Deployment on page 20 displays an example of a Scopia® SR deployment that hosts recordings in the cloud. The deployment is a centralized or all-in-one solution that uses a reverse proxy server. A cloud deployment uses a virtual delivery node (VDN) to host recordings remotely.

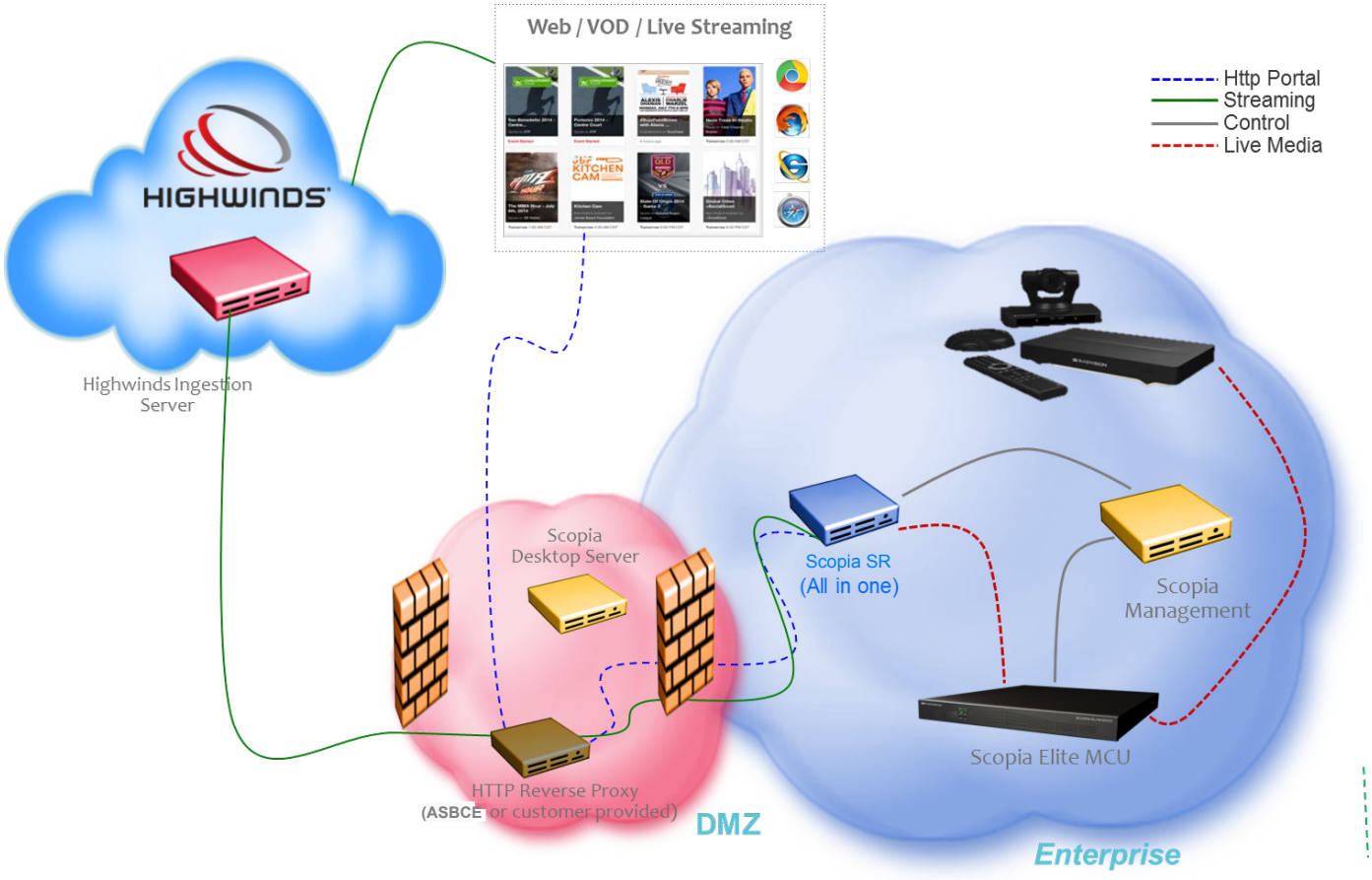


Figure 6: Cloud Deployment

Related links

Avaya Scopia Streaming and Recording server on page 10
About content delivery networks on page 115

Scalability

Recording

Scopia® SR supports up to 10 high definition (1080p) or 30 standard definition (480p) recordings with H.239 simultaneously. The system negotiates high definition whenever possible.

The resolution negotiated is based on the configuration of the MCU service as well as the Scopia® SR profile. By limiting the profile to 480p or less, you can do 30 simultaneous recordings (trading off higher quality recordings versus the ability to do more recordings).

Scopia® SR supports a mix of resolutions, and can do three standard definition calls for every one high definition call. So, for example, if the system is licensed for 10 concurrent recordings, you can do any of the combinations of calls in Table 1: Call Combinations on page 21.

Table 1: Call Combinations

High Definition	Standard Definition
0	30
1	27
2	24
3	21
4	18
5	15
6	12
7	9
8	6
9	3
10	0

Playback

On a standalone media node configured for DN only, Scopia® SR supports up to 3,500 viewers at 720p / 768K for live broadcast or video on demand playback simultaneously.

On all-in-one servers or media nodes configured with DN and CP, Scopia® SR supports up to 1,500 viewers at 720p / 768K for live broadcast or video on demand playback simultaneously.

Related links

Avaya Scopia Streaming and Recording server on page 10

System requirements

Before you log on to Scopia® SR Manager administration pages, your client system must meet the system requirements listed in Table 2: Requirements on page 21.

Table 2: Requirements

Component	Requirement
Operating system	• Mac OS X 10.7 (Lion) or later • Windows Vista™ • Windows 20XX • Windows 7™ (32 and 64 Bit) • Windows 8™ • Windows 10™
Web browser	• Microsoft Internet Explorer 8.0™ or later

Table continues…

Component	Requirement
	• Microsoft Edge™ • Mozilla Firefox 35™ or later (Mac or Windows) • Chrome 30™ or later (Mac or Windows) • Safari 6™ or later (Mac) JavaScript must be enabled.

Before you log on to Scopia® SR Manager user pages, your client system must meet the system requirements listed in Table 3: Requirements on page 22.

Table 3: Requirements

Component	Requirement
Web browser	• Microsoft Internet Explorer 8.0™ or later • Microsoft Edge™ • Mozilla Firefox 35™ or later (Mac or Windows) • Chrome 30™ or later (Mac, Windows, or Android) • Safari 6™ or later (Mac, iOS) JavaScript must be enabled.
Operating system	• Mac OS X 10.7 (Lion) or later • Windows Vista™ • Windows 20XX • Windows 7™ (32 and 64 Bit) • Windows 8™ • Windows 10™ • iOS • Android
Media Player	Microsoft Windows Media Player™ Release 9.0, 10.0, or 11.0 to view programs.
Silverlight	Microsoft Silverlight™ player to view programs.
HTMLV5 Browsers	A select number of browsers support video playback directly for MP4 VoD files including: • Internet Explorer 9, 10, 11 • Safari 6™ or later • Chrome 30™ or later • Microsoft Edge™
IOS Tablet and Phones, Android Tablets and Phones, Windows Phones/Tablets	Playback function for MP4 VoD files

Note:

To support non-Western language character sets, install the particular language pack on the client system from which you are accessing the Scopia® SR Manager. Refer to the operating system documentation for your system.

Related links

Avaya Scopia Streaming and Recording server on page 10

Chapter 2: Installing the new streaming and recording server

Installation checklist

Follow the steps in this checklist to install the Avaya Scopia® Streaming and Recording server (Scopia® SR).

Tip:

It is a good idea to print out this checklist and to mark each task as you complete it.

No.	Task	Description	Notes	✔
1	Learn more about the new streaming and recording server and figure out your deployment type.	Avaya Scopia® Streaming and Recording server on page 10		
2	Connect the LAN cables, keyboard, mouse, and monitor.	Physically connecting the new server on page 25		
3	Start up the server.	Starting the new server on page 29	You require the Microsoft Windows product key.	
4	Configure the server using the Avaya Scopia® Streaming and Recording server Configuration Wizard.	Configuring the new server on page 31		
5	Set the IP addresses and apply the licenses.	Licensing the new server on page 33		
6	Configure the network that each device will use to communicate with the Scopia® SR Manager.	Configuring external addresses for public interfaces on page 118	Before registering devices, you may want to set which network each device uses to communicate	

Table continues…

No.	Task	Description	Notes	✔
			with the Scopia® SR Manager. This forces the proper communication path to and from the Scopia® SR Manager no matter which IP the Scopia® SR Manager uses to communicate with the Scopia® SR device.	
7	Register each of the components with the main server.	Registering each of the components on page 42		
8	On the delivery node (DN), configure the parent delivery node.	Configuring delivery nodes on page 44		
9	On the conference point (CP), configure the gatekeeper IP and source DN.	Configuring conference points on page 48		
10	On Scopia® SR, configure the network address for device communication.	Specifying polling intervals and the network address on page 50		
11	Register Scopia® SR with Scopia® Management.	Adding and Modifying Recording and Streaming servers in Scopia® Management on page 51		

Physically connecting the new server

Before you begin

You require a keyboard, a mouse, and a monitor. You also require several IP addresses and up to four category 5e LAN cables. Ensure that you received the following items with your Avaya Scopia® Streaming and Recording server (Scopia® SR):

- Power cords
- Rack mount kit

Procedure

1. Connect the keyboard, mouse, and monitor.
2. Connect the LAN cable(s).

   All of the Avaya Scopia® Streaming and Recording server NICs are 1GBit bonded. Connect to at least one. They all respond with a single IP address.
3. Connect the power cable.
4. Power up the unit.

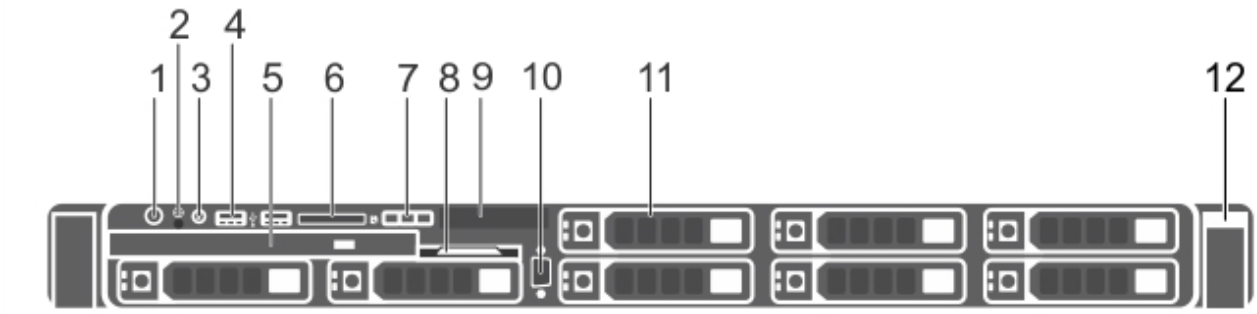
Next steps

Return to the Installation checklist on page 24 to see your next task.

Related links

Front view of Dell PowerEdge R630 Server on page 26
Back view of Dell PowerEdge R630 Server on page 28

Front view of Dell™ PowerEdge™ R630 Server



No.	Item	Icon	Description
1	Power-On Indicator, Power Button	⏻	The power-on indicator lights when the system power is on. The power button controls the power supply output to the system. **Note:** On ACPI-compliant operating systems, turning off the system using the power button causes the system to perform a graceful shutdown before power to the system is turned off.

Table continues…

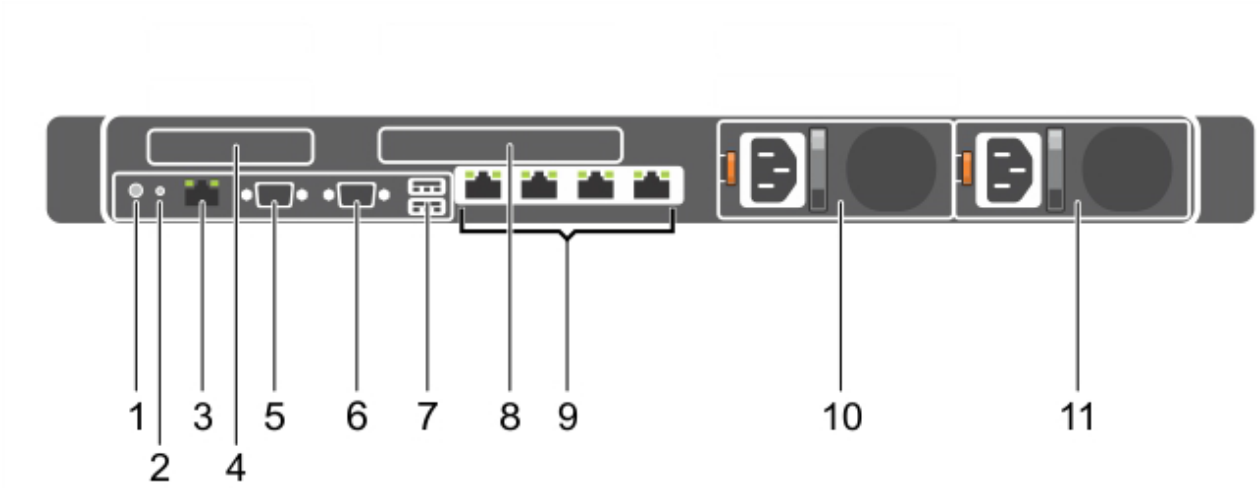
No.	Item	Icon	Description
2	NMI Button		Used to troubleshoot software and device driver errors when running certain operating systems. This button can be pressed using the end of a paper clip. Use this button only if directed to do so by qualified support personnel or by the operating system documentation.
3	System Identification Button		The identification buttons on the front and back panels can be used to locate a particular system within a rack. When one of these buttons is pressed, the LCD panel on the front and the system status indicator on the back flashes blue until one of the buttons are pressed again. Press to toggle the system ID on and off. If the system stops responding during POST, press and hold the system ID button for more than five seconds to enter BIOS progress mode. To reset the iDRAC (if not disabled in F2 iDRAC setup) press and hold the button for more than 15 seconds.
4	USB Connectors (2)		Allows you to insert USB devices to the system. The ports are USB 2.0-compliant.
5	Optical Drive		One DVD+/-RW drive. **Note:** DVD devices are data only.
6	vFlash Media Card Slot		Not used in Avaya configurations.
7	LCD Menu Buttons		Allows you to navigate the control panel LCD menu.
8	Information Tag		A slide-out label panel, which allows you to record system information, such as Service Tag, NIC, MAC address.
9	LCD Panel		Displays system ID, status information, and system error messages. The LCD lights blue during normal system operation. When the system needs attention, the LCD lights amber and the LCD panel displays an error code followed by descriptive text. **Note:** If the system is connected to AC power and an error is detected, the LCD lights amber regardless of whether the system is turned on or off.
10	Video Connector		Allows you to connect a VGA display to the system.
11	Hard Drives		Support for up to eight 2.5 inch hot-swappable hard drives.* * The first 2 HDDs are placed in the slots under the DVD Drive and read left to right, the remaining HDDs read top to bottom, left to right.
12	Quick Sync		Not used in Avaya configurations.

More information can be found in the *Front-panel features and indicators* section of the Dell Owner's Manual.

Related links

Physically connecting the new server on page 25

Back view of Dell™ PowerEdge™ R630 Server



No.	Item	Icon	Description
1	System Identification Button		The identification buttons on the front and back panels can be used to locate a particular system within a rack. When one of these buttons is pressed, the LCD panel on the front and the system status indicator on the back blink until one of the buttons are pressed again. Press to toggle the system ID on and off. If the system stops responding during POST, press and hold the system ID button for more than five seconds to enter BIOS progress mode. If you are directed by services to reset the iDRAC port, press and hold the button for more than 15 seconds.
2	System Identification Connector		Allows you to connect the optional system status indicator assembly through the optional cable management arm.
3	iDRAC8 Enterprise Port		Dedicated management port. **Note:** The port is available for iDRAC8 Express features only. Avaya systems do not come with an Enterprise license. (Not normally used in Avaya systems.)
4	PCIe Expansion Card Slot 1 (riser 2)		Allows you to connect a low profile PCIe expansion card.

Table continues…

No.	Item	Icon	Description
			Note: If your server is equipped with 6 or 8 NIC ports this slot can contain two port 10/100/1000 Mbps NIC connectors or two 100 Mbps/ 1Gbps/10 Gbps SFP + connectors, 2 CPUs must be installed for this slot to be available for use.
5	Serial Connector		Allows you to connect a serial device to the system.
6	Video Connector		Allows you to connect a VGA display to the system.
7	USB Connectors (2)		Allows you to connect USB devices to the system. The ports are USB 3.0-compliant.
8	PCIe Expansion Card Slot 2 (riser 3)		Allows you to connect a full-height half-length PCIe expansion card. **Note:** If your server is equipped with 6 or 8 NIC ports this slot can contain two port 10/100/1000 Mbps NIC connectors or two 100 Mbps/ 1Gbps/10 Gbps SFP + connectors.
9	Ethernet Connectors (4)		Four integrated 10/100/1000 Mbps NIC connectors (Avaya Standard). **Note:** NIC port numbers are read from left to right, starting with Port 1, then continuing to Ports 2, 3, and 4.
10	Power Supply (PSU1)		Wattage and voltage type depends on configuration.
11	Power Supply (PSU2)		Wattage and voltage type depends on configuration.

More information can be found in the *Back-panel features and indicators* section of the Dell Owner's Manual.

Related links

Physically connecting the new server on page 25

Starting the new server

The Microsoft Windows™ 2012 R2 license is already configured on your server.

Procedure

1. Start up the server.
2. Press Ctrl+Alt+Delete to log in.
3. Choose **C** to configure the network settings.

You can configure the network addresses statically or dynamically. Avaya recommends using statically assigned IP addresses, as the IP address needs to remain constant. If you do choose to use dynamically assigned IP addresses, your network must be DHCP-enabled.

4. Choose **S** for statically assigned IP addresses or **D** for dynamically assigned IP addresses.

   If you choose **D**, the setup tries to obtain an address. If you choose **S**, you are prompted to enter the IP address.

5. Enter your subnet mask by choosing an appropriate prefix length.
6. Enter the gateway address.

   You must enter a valid gateway address that fits within the IP and subnet mask that you previously entered. The system provides a valid range of IPs that you can use for the gateway. You must pick one of these IP addresses.

7. Enter your primary DNS Server IP.

   This is a mandatory step.

8. **(Optional)** Enter a secondary DNS IP or press **Enter** if you want to skip this step.
9. **(Optional)** Enter a DNS suffix.

   You should enter a DNS suffix for FQDN/SSL configurations.

10. Enter the server host name, or press **Enter** to use the default generated hostname.

    You should enter a hostname for FQDN/SSL configurations.

11. Confirm the configuration and select **Y** if it is correct, or **N** if you would like to reenter the data.

    When you enter **Y**, the server reboots.

12. When the server starts up again, press Ctrl+Alt+Delete to log in.
13. **(Optional)** Synchronize the time on the new server with the time on your NTP server.
    a. Click on the time and date in the task bar.
    b. Click **(Change date and time settings...)**.
    c. On the Date and Time tab, perform the following actions:
       - Set the correct date and time using the **Change date and time** button.
       - Set the correct timezone using the **Change timezone** button.
    d. On the Internet Time tab, click **Change settings...** and perform the following actions:
       - Ensure that **Synchronize with an Internet time server** is selected.
       - Enter the NTP server in the **Server** list.
       - Click **OK**.
14. Click **OK**.

Next steps

Return to the Installation checklist on page 24 to see your next task.

Configuring the new server

The Avaya Scopia® Streaming and Recording server Configuration Utility launches automatically when the operating system is loaded for the first time. You can also run the configuration utility at any time from the Start menu or from the desktop shortcut.

If you previously installed a Delivery Node (DN), either as part of an all-in-one deployment or on its own, you can add or remove a Virtual Delivery Node (VDN) without disrupting the server configuration. If you have not previously installed a DN, the configuration utility erases any previous configurations on the Scopia® SR server.

About this task

Ths task describes how to configure Scopia® SR in an enterprise deployment. If yours is a service provider deployment, the steps vary slightly.

Procedure

1. On the Choose Setup Language dialog, select your preferred language.
2. On the next screen, click **Next**.

   The first time you run the configuration utility, a Welcome screen is displayed.

   If you have not configured a delivery node (DN) and you run the configuration utility again, a Warning screen is displayed because you may be about to perform a harmful action.

   If you have configured a DN and you run the configuration utility again, you can add or remove a virtual delivery node (VDN) without disturbing the server configuration.
3. On the End-User License Agreement screen, select **I accept the terms of the License Agreement** to accept the license agreement.
4. Click **Next**.
5. On the Select Configuration screen, select your deployment type.

   For more information, see Deployment types on page 18.

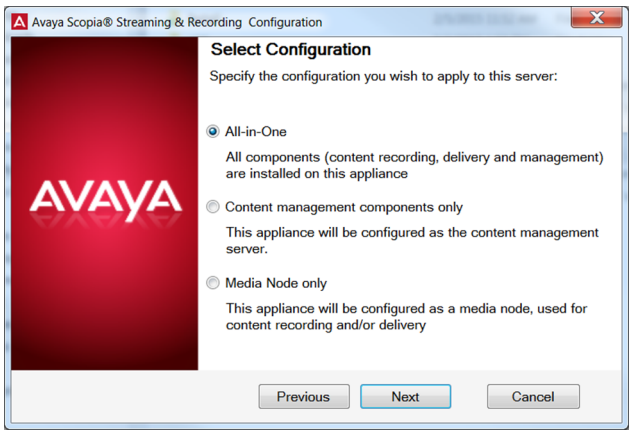


Figure 7: Select Configuration

6. On the Deployment Type screen, perform one of the following actions:
   - If you have selected **All-in-One** on the Select Configuration screen, select **Enterprise deployment** or **Multi-tenant** to match your Scopia® Management deployment.

Figure 8: Deployment Type

   - If you have selected **Content management components only** on the Select Configuration screen, select **Enterprise deployment** or **Multi-tenant** to match your Scopia® Management deployment. The screen is similar to Figure 8: Deployment Type on page 32.
   - If you have selected **Media Node only** on the Select Configuration screen, select whether you want to install the recording and delivery (streaming) components, the recording components, or the delivery components by selecting **Configure content recording and streaming components**, **Configure content recording components only**, or **Configure content streaming components only**.

Figure 9: Deployment Type

7. Click **Next**.
8. **(Optional)** At this point, you can choose to install a Virtual Delivery Node (VDN).

You should only use a VDN if you subscribe to the HighWinds Content Delivery Network (CDN). CDN is a cloud-based streaming system.

a. Select **Install a Virtual Delivery Node (VDN) on this server**.

b. Click **Next**.

9. On the Finish Configuration screen, click **Finish**.

   The Scopia® SR Configuration Utility installs the Scopia® SR components.

10. On the Complete Configuration screen, click **View Addresses** to display the MAC addresses of the Scopia® SR.

    You require these MAC addresses in order to license the Scopia® SR. The MAC addresses are also stored in `C:\assrconfigtool\MAC_Addresses.txt`.

11. Make note of the MAC addresses.

    This information is required when you access the Avaya PLDS system to obtain a license key.

Next steps

Return to the Installation checklist on page 24 to see your next task.

Licensing checklist

Follow the steps in this checklist to license the Avaya Scopia® Streaming and Recording server (Scopia® SR).

No.	Task	Description	Notes	✔
1	Set the IP address of each of the remaining components. You have already set the IP address of the Scopia® SR Manager.	Setting the IP address of the recording component (Conference Point) on page 34 Setting the IP address of the delivery component (Delivery Node) on page 37		
2	Restart services.	Restarting services on page 38		
3	Apply the license to each of the components.	Applying the license to the management component on page 38 Applying the license to the recording component (Conference Point) on page 39 Applying the license to the delivery component (Delivery Node) on page 40	You must apply the license to all components.	

Related links

Setting the IP address of the recording component (Conference Point) on page 34
Setting the IP address of the delivery component (Delivery Node) on page 37
Restarting services on page 38
Applying the license to the management component on page 38
Applying the license to the recording component (Conference Point) on page 39
Applying the license to the delivery component (Delivery Node or Virtual Delivery Node) on page 40

Setting the IP address of the recording component (Conference Point)

The recording component is known as the conference point or CP.

About this task

You should set an IPv4 address.

Before you begin

Obtain the Avaya Scopia® Streaming and Recording server license keys from the Avaya Product Licensing and Delivery System (PLDS).

Procedure

1. Double-click on the Hyper-V Manager shortcut on the desktop.
2. In the Virtual Machines panel, double-click on the **CP** entry.

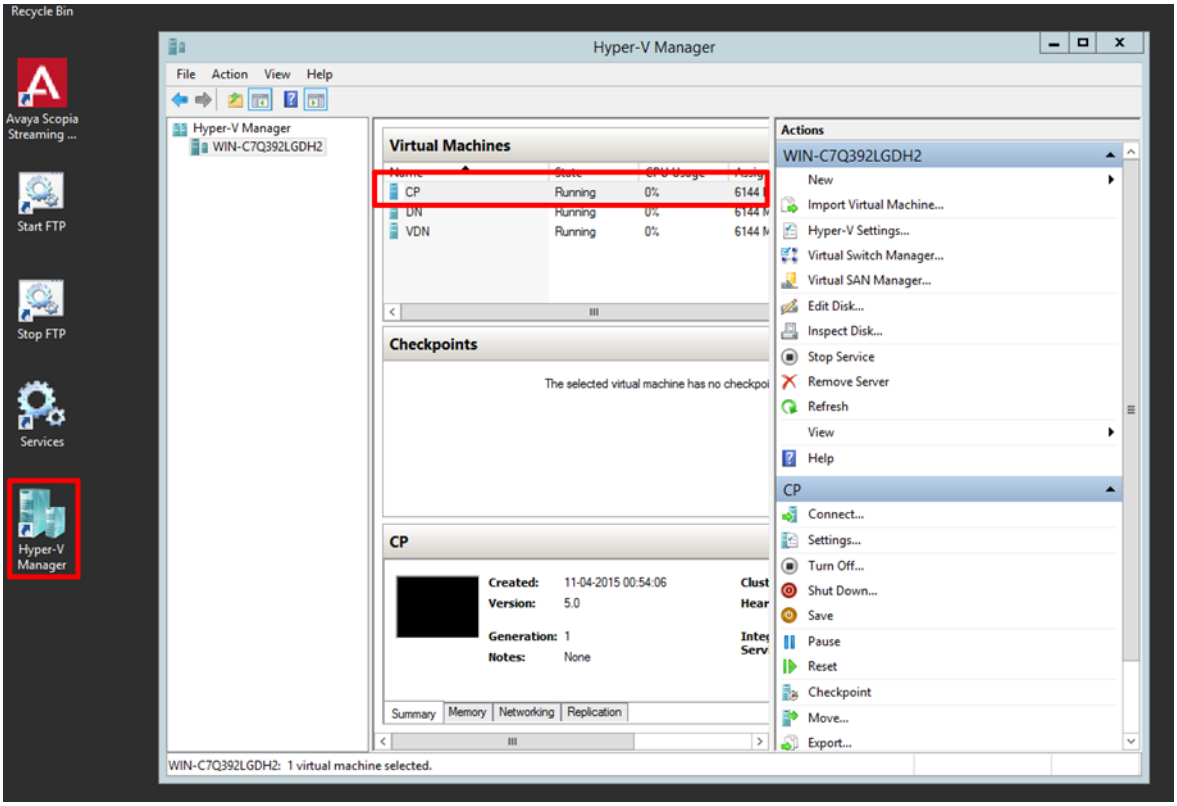


Figure 10: Hyper-V Manager

3. On the Log-in screen, select **Other** and enter `root` in the **Username** field.
4. Click **Log-in**.
5. Enter `Avaya123!` in the **Password** field.

   This is the default password.
6. On the CP Virtual Machine Connection screen, double-click on the **Network** icon.
7. On the Terminal window, highlight **Device configuration** and press `Enter`.

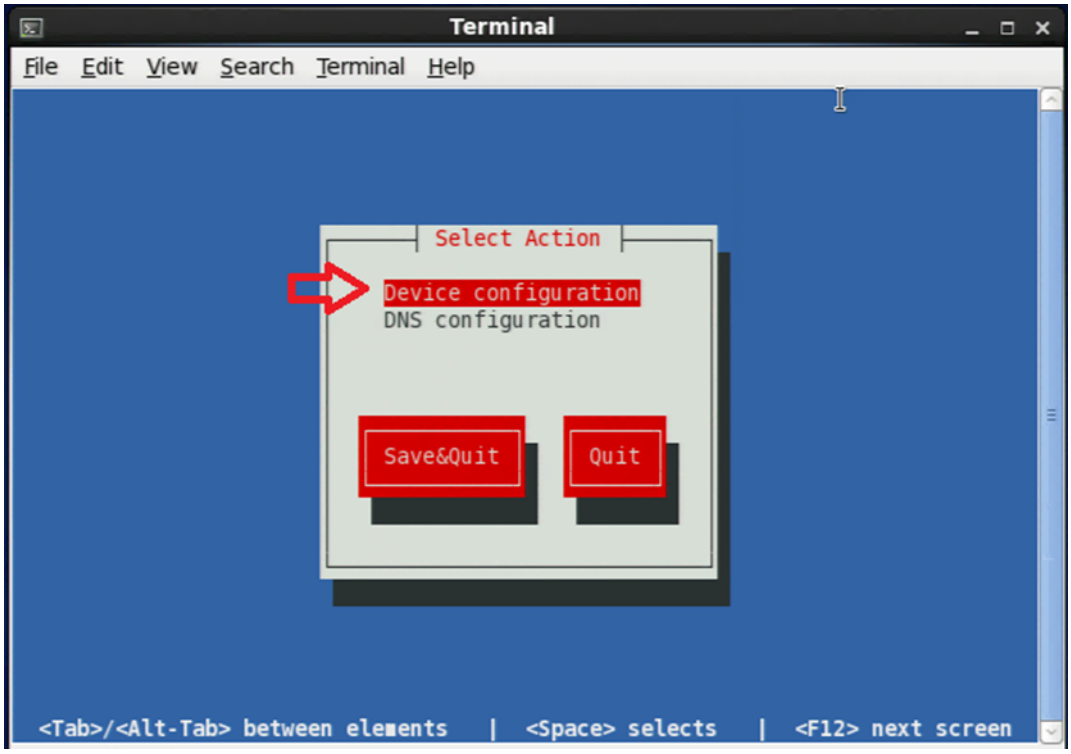


Figure 11: Device Configuration

8. On the Select A Device window, highlight **eth0** and press `Enter`.

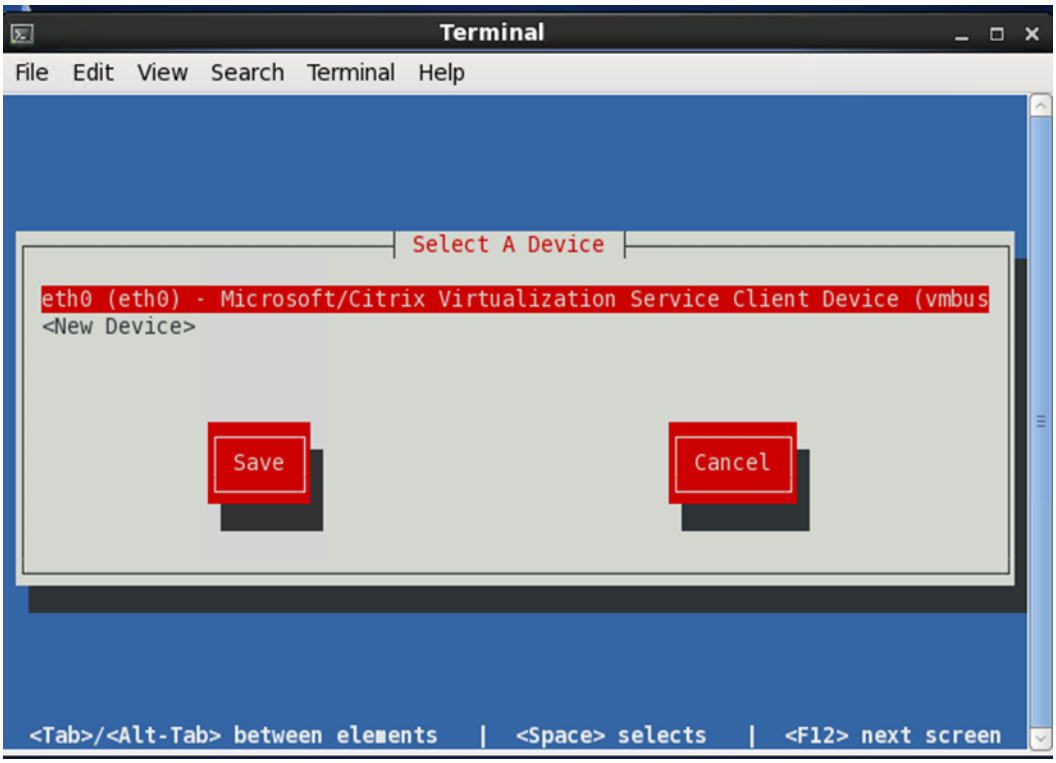


Figure 12: eth0

9. Use the **Tab** key to highlight **Use DHCP** and press the **Spacebar** key to disable DHCP.
10. Use the **Tab** key to navigate to the other fields and enter the following details:
    - Static IP
    - Netmask
    - Default gateway IP
    - Primary DNS Server
    - Secondary DNS Server

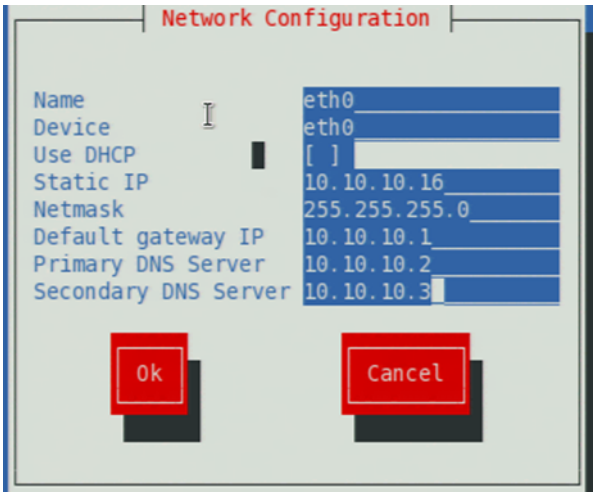


Figure 13: Network Configuration

11. Use the **Tab** key to highlight **Ok** and press `Enter`.
12. On the Select A Device window, use the **Tab** key to highlight **Save** and press `Enter`.
13. Restart Network Services:
    a. Right-click on the desktop and select **Open in Terminal** from the right-click menu options.
    b. In the terminal window, type `service network restart`.

Next steps

Return to the Licensing checklist on page 33 to see your next task.

Related links

Licensing checklist on page 33

Setting the IP address of the delivery component (Delivery Node)

A Delivery Node (DN) can be a Virtual Delivery Node (VDN). You should only use a VDN if you subscribe to the HighWinds Content Delivery Network (CDN). CDN is a cloud-based streaming system. The delivery component is also called streaming.

Procedure

Use the same set of steps that you used for Setting the IP address of the recording component (Conference Point) on page 34.

Next steps

Return to the Licensing checklist on page 33 to see your next task.

Related links

Licensing checklist on page 33

Restarting services

About this task

The services that you must restart are:

- Apache Tomcat
- Apache 2.2
- Avaya Scopia® Streaming and Recording server Transcoder

Procedure

1. Double-click on the Services icon on the desktop.
2. On the Services screen, right-click **Apache Tomcat 7.0 Tomcat7** and select **Restart** from the right-click menu options.
3. Repeat 2 on page 38 for **Apache2.2** and the **Avaya Scopia Streaming & Recording Transcoder**.

Next steps

Return to the Licensing checklist on page 33 to see your next task.

Related links

Licensing checklist on page 33

Applying the license to the management component

Procedure

1. Type `https://<Scopia SR Manager FQDN/IP address>` in a web browser.
2. Log in using the following credentials:
   - Username: `admin`
   - Password: `admin`
3. At the prompt, enter the license key in the **License Information** field and click **Update**.
4. Refresh the browser.

Next steps

Return to the Licensing checklist on page 33 to see your next task.

Related links

Licensing checklist on page 33

Applying the license to the recording component (Conference Point)

Procedure

1. Double-click on the Hyper-V Manager shortcut on the desktop.
2. In the Virtual Machines panel, double-click on the **CP** entry.

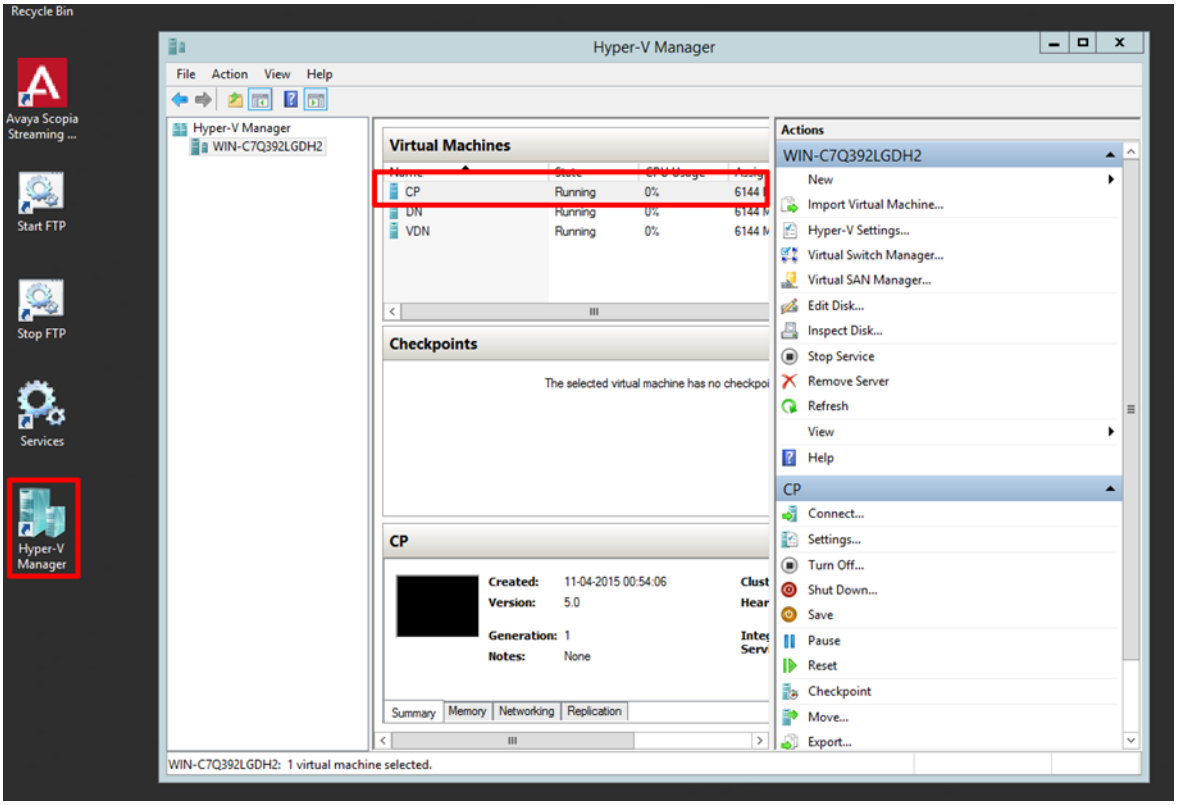


Figure 14: Hyper-V Manager

3. On the Log-in screen, select **Other** and enter `root` in the **Username** field.
4. Click **Log-in**.
5. Enter `Avaya123!` in the **Password** field.

   This is the default password.
6. Double-click on the **Conference Point Web Interface** icon to launch a web browser.

7. On the Conference Point license screen, enter the license key in the **License Key** field and click **Submit**.

Figure 15: Conference Point

Next steps

Return to the Licensing checklist on page 33 to see your next task.

Related links

Licensing checklist on page 33

Applying the license to the delivery component (Delivery Node or Virtual Delivery Node)

There can only be a single virtual delivery node (VDN) in a deployment.

Procedure

1. Double-click on the Hyper-V Manager shortcut on the desktop.
2. In the Virtual Machines panel, double-click on the **DN** or **VDN** entry.

   You should only use a VDN if you subscribe to the HighWinds Content Delivery Network (CDN). CDN is a cloud-based streaming system.
3. On the Log-in screen, select **Other** and enter `root` in the **Username** field.

4. Click **Log-in**.
5. Enter `Avaya123!` in the **Password** field.

   This is the default password.
6. Double-click on the **Delivery Node Web Interface** icon to launch a web browser.
7. On the Delivery Node license screen, enter the license key in the **License Key** field and click **Submit**.
8. Select the type of delivery node.

   The available options are:

   - DN (Delivery Node)
   - VDN (Virtual Delivery Node)

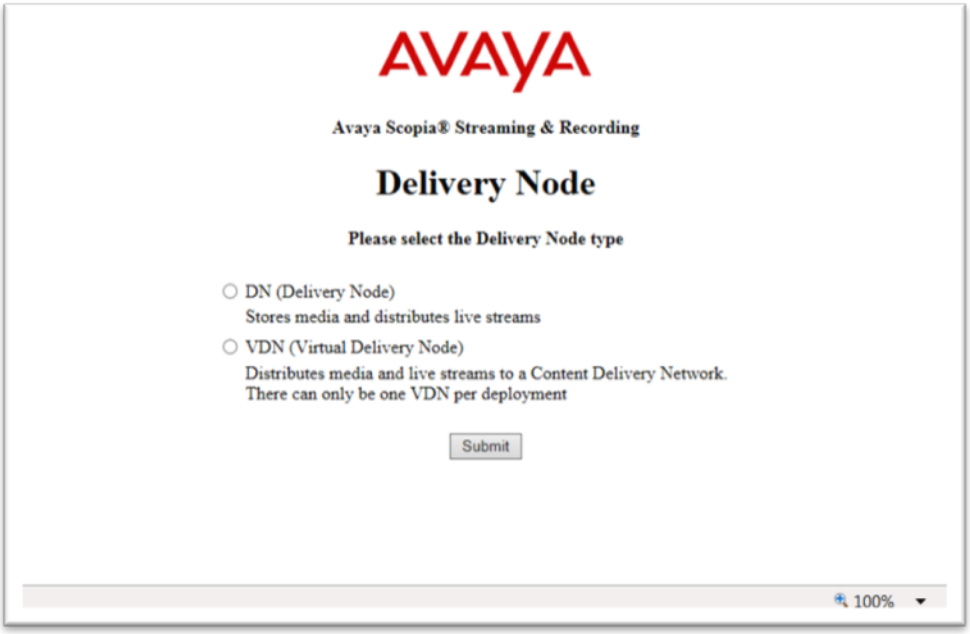


Figure 16: Delivery Node

9. Click **Submit**.

   The DN or VDN is ready for use. The login screen is displayed.

Next steps

Return to the Installation checklist on page 24 to see your next task.

Related links

Licensing checklist on page 33

Registering each of the components

After you have applied a license to each of the components of the Avaya Scopia® Streaming and Recording server, you must register them with the Avaya Scopia® Streaming and Recording server Manager.

You must register all delivery nodes, virtual delivery nodes, and conference points with the Manager. In addition, you must register the transcoder with the conference point. You do not have to register the transcoder with the Manager.

About this task

The registration process is the same for all delivery nodes, virtual delivery nodes, and conference points.

Procedure

1. Type `https://<Scopia® SR manager FQDN/IP address>` in a web browser.
2. Log in to Scopia® SR using the following credentials:
   - Username: `admin`
   - Password: `admin`
3. Select the **Devices** tab.
4. Click on **Register Devices** from the left **Actions** menu.
5. Enter the IP address or FQDN of the component that you want to register and click **Register**.
6. Repeat 5 on page 42 for each of the components.
7. **(Optional)** Verify the registration for the conference point.
   a. Type `https://<CP FQDN/IP Address>` in a web browser.
   b. Log in using the following credentials:
      - Username: `administrator`
      - Password: `administrator`
   c. From the left menu bar, click **System Configuration**.
   d. Click **Enable Services**.
   e. Under Manage Device, click **Configure**.
   f. Verify that the **Manage Registration State** is Registered and the **Manager Host** is the proper manager IP.
8. **(Optional)** Verify the registration for the delivery node or virtual delivery node.
   a. Type `https://<DN FQDN/IP Address>` in a web browser.
   b. Log in using the following credentials:
      - Username: `administrator`
      - Password: `administrator`

c. From the menu bar, click **Configuration**.

d. Verify that the **Manage Registration State** is Registered and the **Network Address** is the proper manager IP.

9. Register the transcoder.

a. Type `https://<CP FQDN/IP Address>` in a web browser.

b. Log in using the following credentials:

- Username: `administrator`
- Password: `administrator`

c. From the left menu bar, click **System Configuration**.

d. Click **Transcoder Configuration**.

e. Enter the IP address of the transcoder and click **Finish**.

The transcoder is running on the host operating system. The CP is running on a virtual machine which runs on the host. The IP address of the transcoder is the IP of the host Windows™ 2012 server.

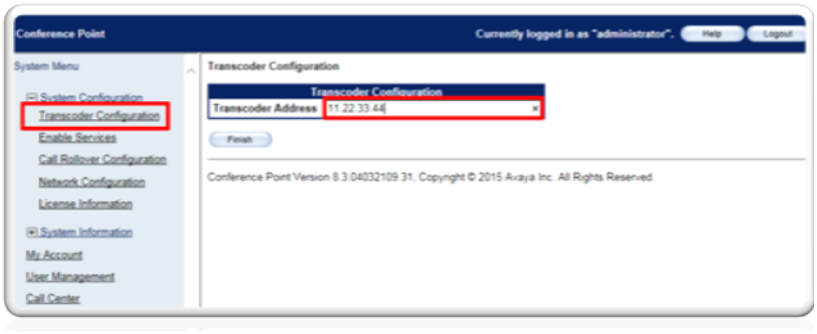


Figure 17: Transcoder Registration

Next steps

Return to the Installation checklist on page 24 to see your next task.

Related links

Unregistering each of the components on page 43
Troubleshooting devices on page 172
Unregistering each of the components on page 43

Unregistering each of the components

If you plan to move a device to a different Scopia® SR environment, unregister the device before changing its location. If you do not unregister the device using the Scopia® SR Manager, you must unregister it using its local web interface before you can register it to the new Scopia® SR environment.

About this task

The process of unregistering is the same for all delivery nodes, virtual delivery nodes, and conference points.

Procedure

1. Log in to Scopia® SR.
2. Click the **Devices** tab.
3. From the **Browse** menu, select the device you want to access.

   A list of devices of that type is displayed.
4. Select one of the devices.

   The device details dialog is displayed.
5. Click **Unregister**.

Related links

Registering each of the components on page 42
Registering each of the components on page 42

Configuring delivery nodes

Delivery nodes (DN) store all content that is created by the conference point and deliver the content to client systems. You must associate the conference point with the delivery nodes.

The Delivery Node Details dialog displays a list of **Source Programs** and **Distributed Programs**. Source programs are programs for which this delivery node is the main source for storage. Distributed programs are programs which other delivery nodes have forwarded to this delivery node.

Procedure

1. Log in to Scopia® SR using the following credentials:
   - Username: `admin`
   - Password: `admin`
2. Select the **Devices** tab.
3. From the **Browse** menu on the left, click **Delivery Nodes**.
4. Click the name of the delivery node to display the delivery node details.

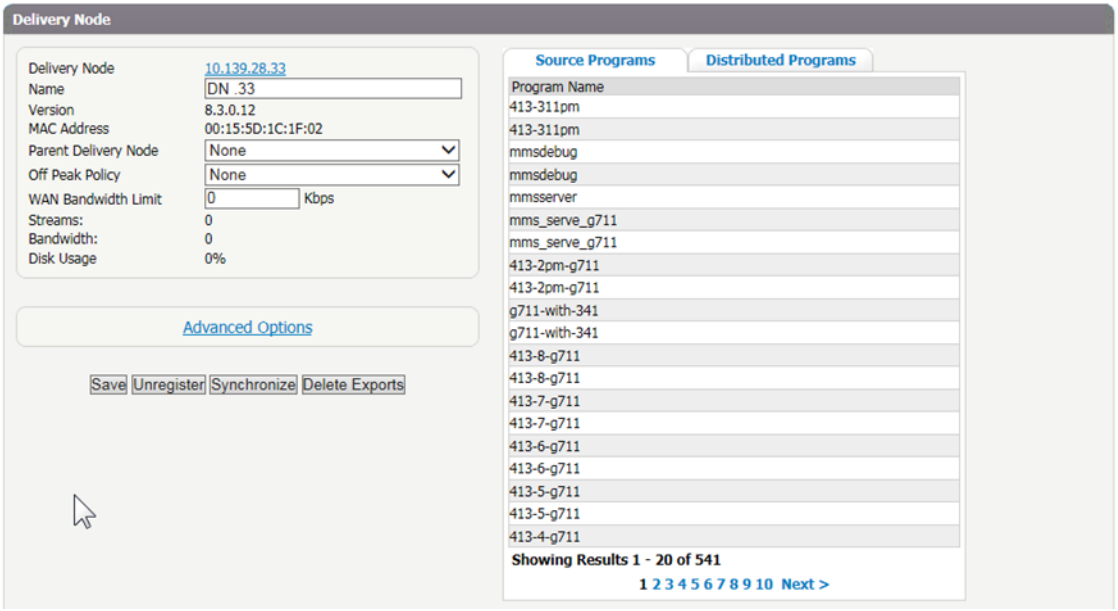


Figure 18: Delivery Node Details

5. Configure the settings, as described in Table 4: Delivery Node Details on page 45.

Table 4: Delivery Node Details

Field Name	Description
Name	Enter a name for the delivery node.
Version	Verify the version and MAC address of the delivery node.
Parent Delivery Node	Select a delivery node. The **Parent Delivery Node** distributes content to the delivery node. If this is a core or parent for the system then leave this set to **None**.
WAN Bandwidth Limit	Specify the maximum bandwidth, in Kbps, that this delivery node can use when receiving/ transferring content. If you enter **0** (zero), the bandwidth is unlimited. If you have an edge delivery node that has a lower bandwidth access, you should set this value to be lower than the remote network's capability.

6. **(Optional)** If you have configured your system to enable individual delivery nodes to specify the distribution policy, then an additional panel is displayed. Configure the settings, as described in Table 5: Override Default Distribution Policy Panel on page 46.

Table 5: Override Default Distribution Policy Panel

Field	Description
Unicast Only	Select to enable only unicasting from the source delivery node.
Multicast Only	Select to enable only multicasting from the source delivery node. If you select this option and the client technically supports the playing of multicast but the network location does not support multicasting, viewers cannot view the program.
Multicast and Unicast (Unicast Rollover if Multicast is Unsuccessful)	Select to enable the stream to be unicast from the source delivery node if the client does not support multicasting. If you select this option but multicast facilities are not available on the source delivery node, the unicast rollover does not occur.

Note:

These settings only impact MMS streams. You can specify **Multicast Only** and still deliver HLS streams.

7. **(Optional)** Click **Synchronize** to ensure that all programs are distributed to their assigned delivery nodes. Only perform this step if programs have indicated failure or pending for some time.

   When you click **Synchronize**, Scopia® SR attempts to complete any failed or pending distributions for a given DN. You can check the progress of the synchronization by checking the DN program listing on the Delivery Node screen. This feature is useful when adding a new DN, or moving an existing DN within a DN hierarchy. The programs are not updated until you click **Synchronize** . You may also want to click **Synchronize** if a delivery node has been offline for some time and needs to synchronize programs that have occurred during this time.

8. **(Optional)** Click **Advanced Options** and configure the settings as described in Table 6: Advanced Options on page 46.

Table 6: Advanced Options

Field	Description
Distribute All Programs	Select to take all the programs in the system from other source nodes and copy them to this delivery node.
Replace with new DN	Use this setting when bringing on a replacement delivery node for an older or broken system.

9. Click **Save**.

Configuring virtual delivery nodes

A virtual delivery node (VDN) delivers content to a global content delivery network (CDN) provider for cloud-based viewer playback. The appliance and the network of the CDN act as one delivery mechanism. Therefore, the VDN appliance and the CDN together create the Scopia® SR VDN solution.

Upon program creation, the publisher includes the options of distributing the program to delivery nodes and to the Scopia® SR VDN solution. VDN supports publishing recordings as well as live broadcast.

You can view the programs distributed to the VDN appliance and to be delivered to the CDN with the associated status of the program.

Procedure

1. Log in to Scopia® SR using the following credentials:
   - Username: `admin`
   - Password: `admin`
2. Select the **Devices** tab.
3. From the **Browse** menu on the left, click **VDN**.
4. Click the name of the VDN to display the VDN details.

   Scopia® SR supports a single VDN in any deployment.

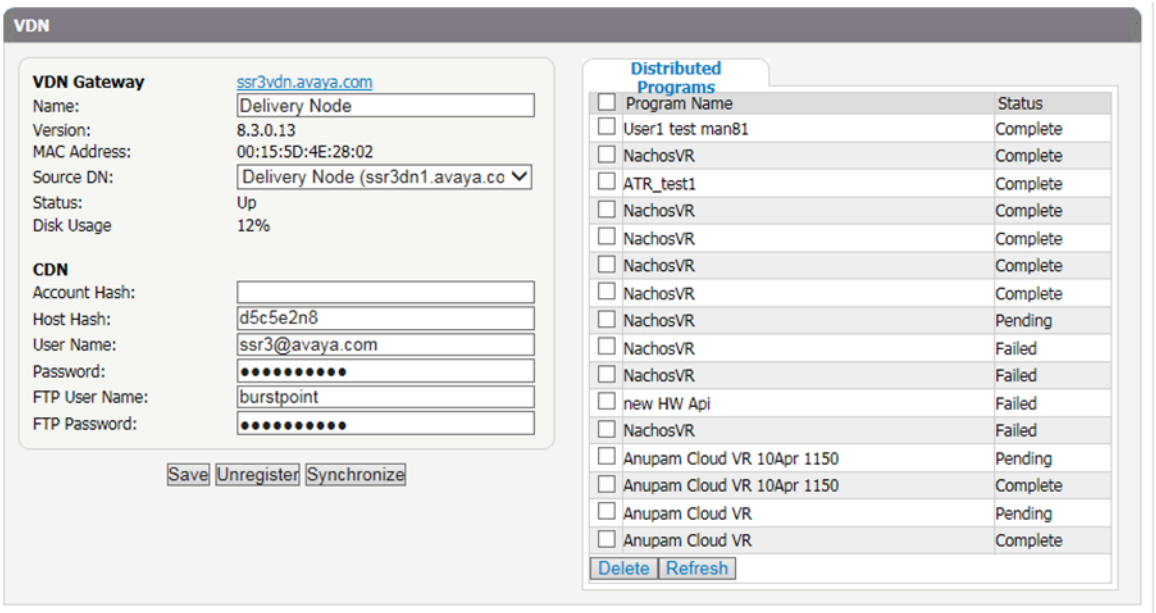


Figure 19: VDN Details

5. Configure the settings, as described in #unique_36/unique_36_Connect_42_VDN on page 47.

Table 7: VDN Details

Field Name	Description
Name	Enter a name for the delivery node.
Version MAC Address	Verify the version and MAC address of the delivery node.
Source DN	Select a delivery node from where this VDN retrieves content.
Status Disk Usage	View the status of the VDN. It can be Up or Unreachable. View the disk usage. The delivery node supports a total of approximately 600 (GB) at RAID level 1.
If this system is in enterprise mode, the CDN panel is displayed here. If this system is in multi-tenant mode, the CDN panel is displayed in the **Organizations** tab.	
Account Hash	Enter the account hash value taken from Strike Tracker 3 Portal.
Host Hash	Enter the host hash value taken from Strike Tracker 3 Portal Host Configuration.
Username Password	Enter the StrikeTracker 3 username and password that you used to purchase the CDN service.
FTP User Name FTP Password	This field enables the uploading of recordings to the CDN. Enter proper cloud storage FTP credentials specific to the customer account. You receive these credentials when you purchase the CDN service.

6. Click **Save**.

Next steps

In order for the VDN to push content to the CDN, you must configure your network to enable external access because the VDN must have access to the Internet in order to communicate with the CDN. If you have a firewall, you can place the VDN in a DMZ or you can open the appropriate ports on the firewall to enable external communication. Specifically, the VDN must be able to access `upload.hwcdn.net` using FTP on port 21. In addition, the VDN requires HTTP or HTTPS acccess to the CDN.

Configuring conference points

You must configure a conference point to capture H.323 video content and deliver live and on demand webcasting. The Scopia® SR conference point includes an embedded transcoder to convert H.323 calls into Windows Media or .MP4 format.

Each conference point must be associated with a delivery node. A delivery node streams and optionally archives the content captured by the conference point and delivers it to client systems.

You can configure a conference point to be in a geographic location. This means that you can assign a location to one or more conference points which coincide with locations set for Scopia® MCUs in Scopia® Management. When a program starts, Scopia® Management includes the desired location, and a conference point close to the MCU can be selected. If there are no conference points matching the location passed by Scopia® Management, then any conference points without a location are treated as a single pool of conference points, and one of those is selected. If there are no conference points available, the call fails.

Each conference point has a limit to the number of simultaneous high definition or standard definition calls it can handle.

Procedure

1. Log in to Scopia® SR using the following credentials:
   - Username: `admin`
   - Password: `admin`
2. Select the **Devices** tab.
3. From the **Browse** menu on the left, click **Conference Points**.
4. Click the name of the conference point to display the conference point details.

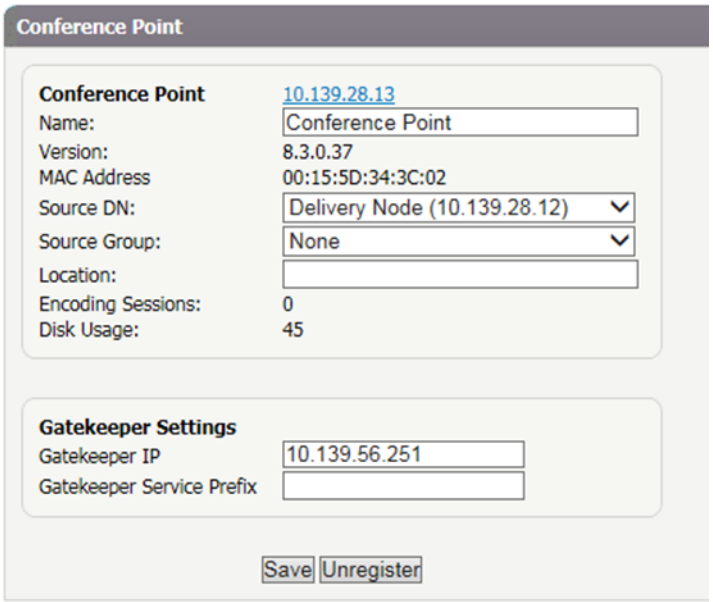


Figure 20: Conference Point Details

5. Configure the settings, as described in Table 8: Conference Point Details on page 50.

Table 8: Conference Point Details

Field Name	Description
Name	Enter a name for the conference point.
Version	Verify the version and MAC address of the conference point.
Source DN	Select a delivery node. Alternatively, you can select a delivery node from the **Source Group** field.
Source Group	Select a delivery node distribution group. Alternatively, you can select a delivery node from the **Source DN** field. The Source Group field displays any distribution groups. A distribution group is a group of delivery nodes and these groups offer redundancy. If one of the delivery nodes in a group is not available, an alternative delivery node from the same group is selected.
Location	Enter a location. The location must match a location specified for a Scopia® MCU in Scopia® Management. If you are not specifying locations in Scopia® Management, you should leave it blank.
Gatekeeper IP	Enter the IP address for the gatekeeper with which you plan to register. The gatekeeper must be the same as the one used by Scopia® Management.
Gatekeeper Service Prefix	This is an optional field. Enter the service prefix designator for this conference point. You should leave this field as blank.

6. Click **Save**.

Specifying polling intervals and the network address

About this task

You must specify how frequently the Scopia® SR communicates with the other components, such as the conference points and delivery nodes. You must also specify the network on which the Scopia® SR resides. The polling interval should be in proportion to the number of devices. The fewer the devices, the shorter the intervals. For example, if you have over 200 delivery nodes, Avaya recommends setting the polling to 5 minutes.

The polling frequency affects the latency between the status transitions of the remote device and the appearance of the status on the details page for the device.

Procedure

1. Log in to Scopia® SR.
2. Click the **Global Policies** tab.
3. Click **General Options**.
4. Configure the settings, as described in Table 9: Polling Settings on page 51.

Table 9: Polling Settings

Field Name	Description
Conference Point Polling Frequency	Specify how often the Scopia® SR Manager checks for device configuration or status changes for each of the conference points.
Delivery Node Polling Frequency	Specify how often the Scopia® SR Manager checks for device configuration or status changes for each of the delivery nodes.
Network Address for Device Communication	Enter the IP address or DNS name of the Scopia® SR Manager. This is the address that the other devices (delivery nodes, conference points, virtual delivery nodes) will use to communicate with the Scopia® SR Manager. If split-horizon DNS is being used, use the DNS name for the Scopia® SR Manager. Since this address is used by the other devices to communicate back to the Scopia® SR Manager, it is important to specify the correct routable address.

5. Click **Save**.

Adding and Modifying Scopia® Streaming and Recording servers in Scopia® Management

About this task

This section explains how to configure Avaya Scopia® Streaming and Recording server settings in Scopia® Management. For example, you can configure the URL of the Avaya Scopia® Desktop server that users connect to in order to see broadcasts.

Important:

If you are using the Avaya Scopia® Content Center Recording server or the Avaya Scopia® Content Center Streaming server , you need to configure and manage the servers using the Avaya Scopia® Desktop server. For more information, see the *Administrator Guide for Avaya Scopia® Desktop server*.

Important:

Once you configure a Scopia® Streaming and Recording server you cannot revert back to the Scopia® Content Center Streaming server or the Scopia® Content Center Recording server .

Procedure

1. Access the Scopia® Management administrator portal.
2. In the **Devices** tab, select **Streaming & Recording Server**.
3. If you are modifying the Scopia® Streaming and Recording server select the link in the **Name** column , or select **Add** to create the Scopia® Streaming and Recording server profile. The **Add Streaming & Recording Server** page appears (Figure 21: Adding an Avaya Scopia Streaming and Recording server on page 52).

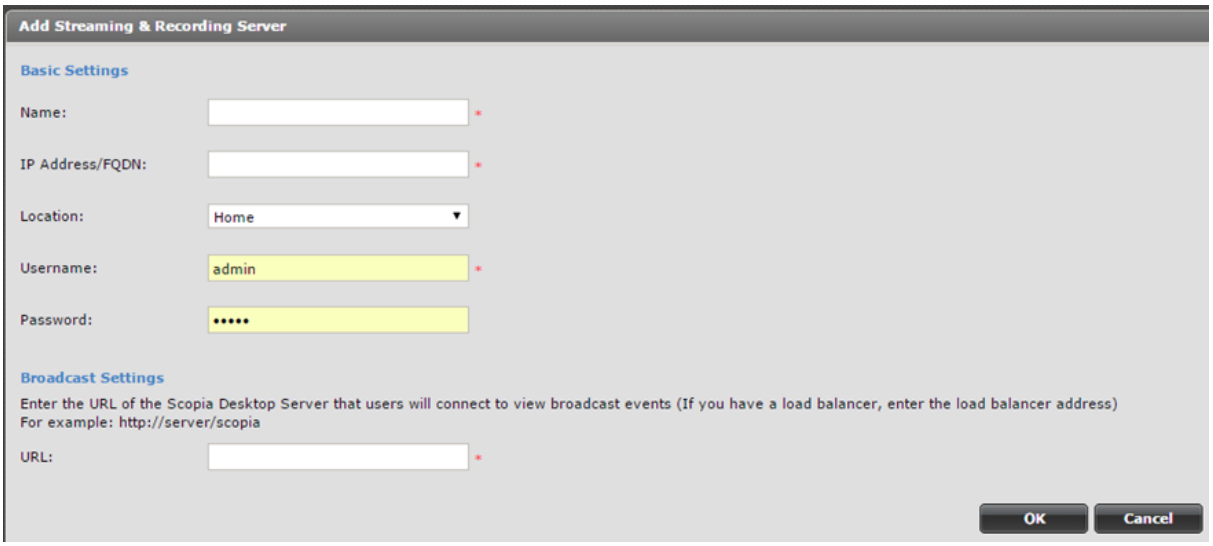


Figure 21: Adding an Avaya Scopia® Streaming and Recording server

4. Configure the Scopia® Streaming and Recording server's settings, as described in (Table 10: Configuring the Avaya Scopia Streaming and Recording on page 52).

Table 10: Configuring the Avaya Scopia® Streaming and Recording

Field Name	Description
Name	Enter a name to identify the Scopia® Streaming and Recording server.
IP address/FQDN	Enter the management IP address or the FQDN of the Scopia® Streaming and Recording server. This is the address that clients use to access the Scopia® Streaming and Recording server portal within Scopia® Desktop. If the server is being deployed in the DMZ, this value must be an FQDN or an IP address that everyone can access. If the server is being deployed inside the network but is accessible externally using reverse proxy, this value must be an FQDN which resolves to the reverse proxy when outside the network.

Table continues…

Field Name	Description
Username	Enter the administrative username used to login to the Scopia® Streaming and Recording server portal. The default is **admin**. If you change the username in the Scopia® Streaming and Recording server, you must update the username here.
Password	Enter the administrative password used to login to the Scopia® Streaming and Recording server portal. The default is **admin**. If you change the password in the Scopia® Streaming and Recording server, you must update the password here.
Secure connection using HTTPS	**Important:** This option is not available until you first configure the server in Scopia® Management, and it connects to the Scopia® Streaming and Recording server. When you subsequently open this screen, the option only becomes available if you have a regular license. If you have a non-encrypted license you cannot secure the connection. Select to enable HTTPS, which encrypts the communication between the Scopia® Streaming and Recording server and the client. It is important to be consistent. If the Avaya Scopia® Desktop server is configured for HTTPS, you must select this checkbox to ensure that the Scopia® Streaming and Recording server matches the Avaya Scopia® Desktop server. To enable HTTP deselect the checkbox. 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.
URL	Enter the URL of the Avaya Scopia® Desktop server you are using to view broadcasts. The URL must be in the format *http://<web URL>:<port number>/scopia*. If you are using a load balancer, enter the URL of the load balancer.

5. Select **OK** to save your changes.

Related links

Enabling secure and encrypted authentication on page 117

Chapter 3: Getting started with the streaming and recording server

Logging in to the Scopia® Streaming and Recording server

Procedure

1. Navigate to the URL of the Scopia® Management administrator portal, as defined during installation. This should be in the following format:http://host-URL:port-number/iview, where the host-URL is the name of the application server on the Scopia® Management server.
2. Log in to the Scopia® Management administrator portal using the credentials specified in the installation process.

   The Dashboard appears.

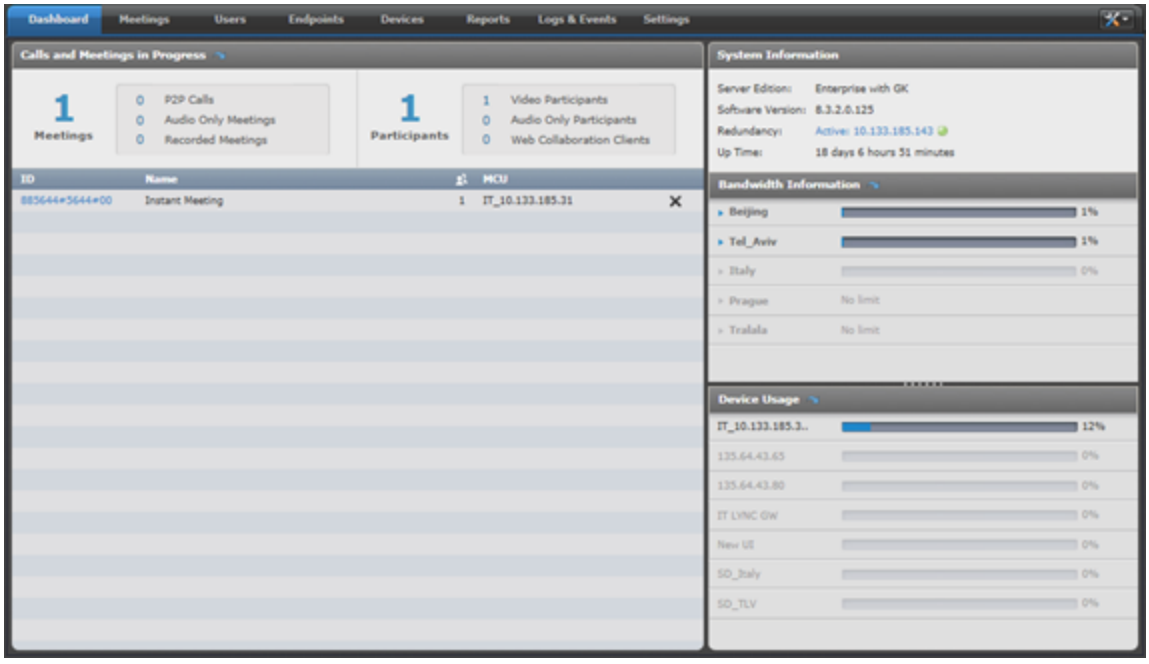


Figure 22: Administrator portal's dashboard

3. Navigate to the **Devices** tab.
4. Click on the IP address for the Scopia® SR.

   The Scopia® SR launches in a new window. You are already logged in to it.

Related links

Logging in to conference points and delivery nodes on page 55

Logging in to conference points and delivery nodes

You can log in to a device's web interface to change its configuration settings or services. You should only change the settings when the system is not in use.

Procedure

1. Log in to Scopia® SR Manager.
2. Click the **Devices** tab.
3. From the **Browse** menu, select the device you want to access.

   A list of devices of that type is displayed.
4. Select one of the devices.

   The device details dialog is displayed.
5. Click the hostname or IP address of the device.

   A Login window is displayed.
6. Enter your credentials and click **Login** to log in to the device.

Related links

Logging in to the Scopia Streaming and Recording server on page 54
Accessing conference point logs on page 170
Accessing delivery node logs on page 171
Troubleshooting conference points on page 172
Troubleshooting delivery nodes and virtual delivery nodes on page 173

Viewing the status of your devices

Procedure

1. Log in to Scopia® SR using the following credentials:
   - Username: `admin`
   - Password: `admin`
2. Select the **Devices** tab.
3. From the **Browse** menu on the left, select the device category, such as **Conference Points**.

   A list of devices is displayed.

4. View the **Status** field.
   - **Up**: The device is accessible.
   - **Unreachable**: The device is inaccessible.

   Note:

   After you register or reboot a device, it may take over a minute before the device status changes to **Up**.

Next steps

If the device is not accessible, click on the device hostname or IP address to access its web interface.

Chapter 4: Managing passwords

Password configuration

Avaya recommends changing all default passwords for Scopia® SR.

You should also change the Linux root password on each device as well. Using Hyper-V Manager, you can access the operating system and change the default.

Changing the password for the Scopia® Streaming and Recording server

By default, the username and password for Scopia® SR are admin/admin. Avaya recommends updating them.

Procedure

1. Log in to Scopia® SR.
2. Click the **Global Policies** tab.
3. Click **User Authentication** on the **Policies** menu.
4. Specify new values for the username and password.
5. Click **Save**.

Next steps

If you change the username and password for Scopia® SR, you must also change the credentials for Scopia® SR within Scopia® Management.

Changing the password for conference points

Procedure

1. Type `https://<CP FQDN/IP Address>` in a web browser.

2. Log in using the following credentials:
   - Username: `administrator`
   - Password: `administrator`
3. Update the password using the **My Account** menu.
4. Click **Finish**.

Changing the password for delivery nodes

Procedure

1. Type `https://<DN FQDN/IP Address>` in a web browser.
2. Log in using the following credentials:
   - Username: `administrator`
   - Password: `administrator`
3. Update the password using the **Configuration** menu.
4. Click **Submit**.

Chapter 5: Managing users and roles

Enabling streaming and recording for specific users

In the Scopia® Solution environment, there are two types of profiles. There are user profiles and there are recording profiles.

You can create user profiles using the Scopia® Management interface. When you create a user profile using the Scopia® Management interface, you can optionally enable recording and broadcasting for that user profile. When you enable recording and broadcasting for the user profile in Scopia® Management, you can assign a recording profile to that user profile. Figure 23: Determining user profile settings on page 60 displays the **Can recording meetings** checkbox, the **Can broadcast meetings** checkbox, and **Profile** drop-down menu. The **Profile** drop-down menu displays the available recording profiles.

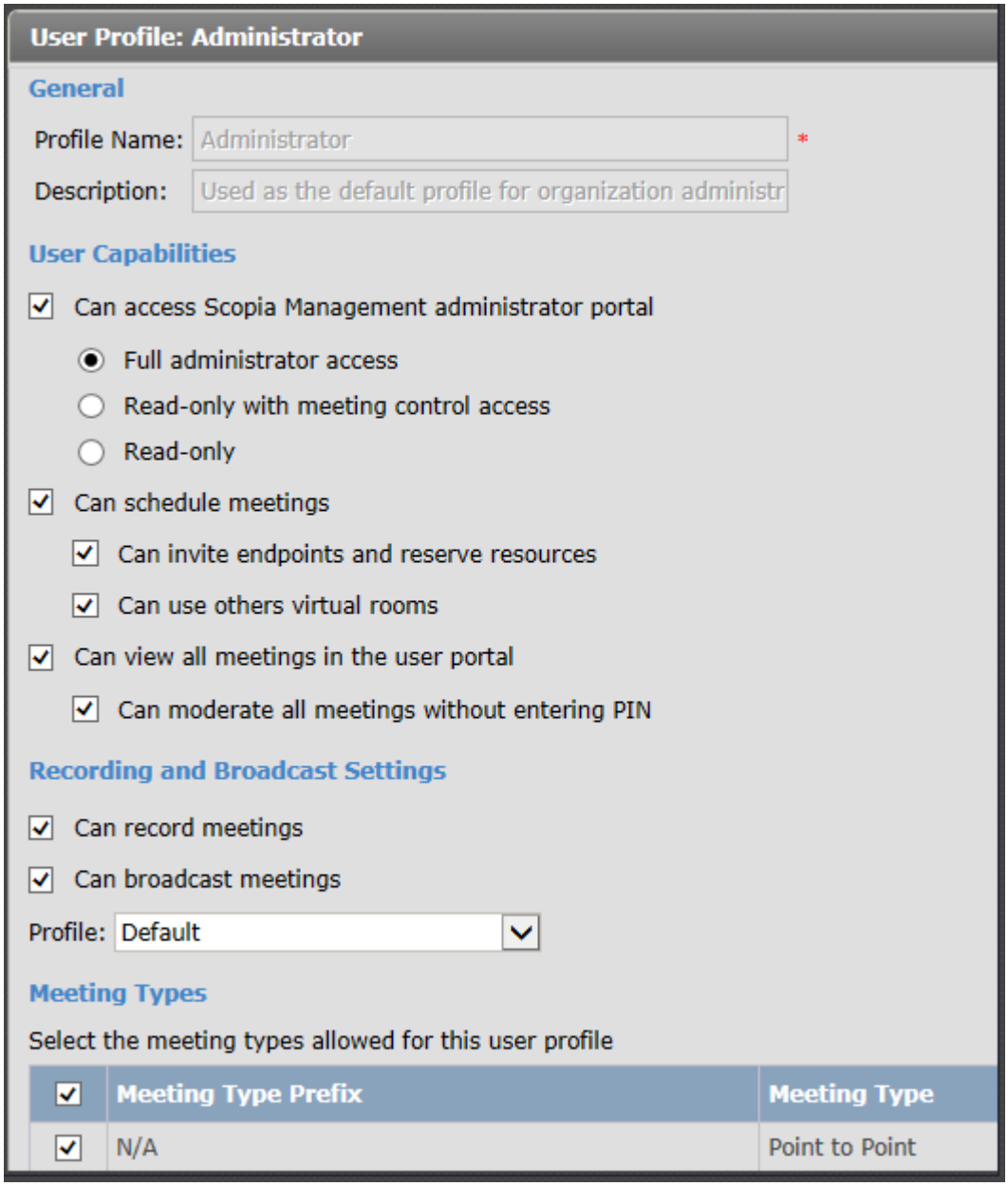


Figure 23: Determining user profile settings

Important:

You use the Scopia® Management interface to manage user profiles.

You use the Scopia® SR Manager interface to manage recording profiles.

A user profile is a compilation of user-related capabilities and rights, such as available meeting types, ability to schedule meetings, access to the Scopia® Desktop and Scopia® Mobile functionality, allowed bandwidth for Scopia® Desktop calls. The purpose of having user profiles in Scopia® Management is to configure and modify rights and capabilities for all users sharing this profile, instead of doing it for every user individually. Typically you create profiles that correlate with

user roles in the organization (for example, administrators, read-only users) or profiles using different features (for example, users who use the lecture meeting type and are not allowed to schedule meetings).

There are four preconfigured user profiles:

- Administrator
- Meeting Organizer
- Meeting Operator
- Regular User

You can modify settings for the preconfigured profiles, except their names and short descriptions. You cannot delete preconfigured profiles.

You can assign profiles to individual users and to user groups. When you assign a user profile to a group, you can still assign a different profile to individual users within this group.

When streaming and recording is enabled in Scopia® Management, you can narrow the streaming and recording services by granting streaming and recording permissions to specific user profiles. Users with streaming and recording permissions can configure their virtual room settings to always stream or record meetings, or they can enable streaming and recording when scheduling a specific meeting.

The *Scopia® Management Administrator Guide* describes how to create user profiles to enable streaming and recording for specific users. It also describes how to enable streaming and recording for specific virtual rooms.

For more information, see the *Avaya Scopia® Management Administrator Guide*, which is available on https://support.avaya.com/.

Creating user profiles in the Scopia® Management interface

Note:

Scopia® Management synchronizes with Scopia® SR. This means that the list of users that you have created using the Scopia® Management interface synchronizes with the list of users displayed on the Scopia® SR Manager interface.

For more information, see the *Avaya Scopia® Management Administrator Guide*, which is available on https://support.avaya.com/.

Understanding roles

A Scopia® SR user account includes a user ID, e-mail address, and a set of roles. Roles are used to determine user capabilities. By default, the roles are:

- Administrator: Users with this role can manage the system, devices, and recordings. Any Scopia® Management user designated as an administrator with full administrator access also has administrator privileges in Scopia® SR.
- Organization Administrator: Users with this role can manage the recordings for all users within his organization. Any Scopia® Management user designated as an organization administrator also has organization administrator privileges in Scopia® SR. This user cannot log into the Scopia® SR administrator GUI, but can see all recordings within the organization and can edit attributes or delete the recording.
- Publisher: Users with this role can create and view programs. Publishers record meetings, and add, edit, and delete program information. Any user with the ability to record or broadcast a meeting in Scopia® Management is considered a publisher
- Viewer: Users with this role can view programs based on the permissions assigned to the programs. All other users are considered viewers.

Viewing users and roles

Note:

Scopia® Management synchronizes with Scopia® SR. This means that the list of users that you have created using the Scopia® Management interface synchronizes with the list of users displayed on the Scopia® SR Manager interface.

Procedure

1. Log in to Scopia® SR.
2. Click the **Users** tab to view the list of users.
3. **(Optional)** Filter the list of users by selecting from the list of **Roles**.
4. **(Optional)** Search the list by entering a name or ID information in the **Search** field.
5. **(Optional)** Click **View** to see more details a selected user.

Verifying that roles have been synchronized from Scopia® Management

Note:

Scopia® Management synchronizes with Scopia® SR. This means that the list of users that you have created using the Scopia® Management interface synchronizes with the list of users displayed on the Scopia® SR Manager interface.

Procedure

1. Log in to Scopia® SR.
2. Click the **Users** tab to view the list of users.
3. **(Optional)** Filter the list by selecting from the list of **Roles**.
4. **(Optional)** Search the list by entering a name or ID information in the **Search** field.
5. **(Optional)** Click **View** to see more details a selected user.
6. Check the **Roles** panel to ensure that the user has the correct roles assigned.

Chapter 6: Managing profiles

Recording profiles

In the Scopia® Solution environment, there are two types of profiles. There are user profiles and there are recording profiles.

A recording profile defines the properties of a recording, such as resolution, video size, and video position. By default, when a user creates a recording, Scopia® SR uses the default recording profile. As an administrator, you can create, modify, and delete recording profiles using the Scopia® SR Manager interface.

Important:

You use the Scopia® Management interface to manage user profiles.

You use the Scopia® SR Manager interface to manage recording profiles.

Creating recording profiles in the Scopia® SR interface

Note:

Scopia® Management synchronizes with Scopia® SR. This means that the list of users that you have created using the Scopia® Management interface synchronizes with the list of users displayed on the Scopia® SR Manager interface.

As an administrator, you can create profiles which define the attributes used for recordings and broadcasts created using those profiles. A recording profile can be assigned to a user or group of users in Scopia® Management. By default, the Default Profile is used when that user creates a recording. When the user is scheduling a broadcast, they can choose the profile which they would like to use.

Procedure

1. Log in to Scopia® SR.
2. Click the **Profiles** tab to view the list of recording profiles.
3. Click **New**.
4. Configure the settings, as described in Table 11: Profiles on page 65.

Table 11: Profiles

Field Name	Description
Name	Enter a name for the profile. This name is displayed in the Scopia® Management administration GUI and the web scheduler.
Description	Optionally, enter a description for the profile.
Thumbnail	Upload a thumbnail image using the **Choose File** button. All recordings and broadcasts using this profile display this graphic as their thumbnail. The thumbnail can be changed by the end-user from the portal when editing the program details, or when scheduling the broadcast.
Capture Resolution	Select a capture resolution/bitrate from the drop-down menu.
Enable Multi-Bitrate	Optionally, enable multi-bitrate. This is used for live broadcasts. If selected, additional lower bitrate versions of the session are captured to allow for smoother playback on bandwidth-constrained devices. This requires more processing power, so multi-bitrate broadcasts reduce the total amount of simultaneous recordings a conference point can handle.
Enable MMS	Optionally, enable Microsoft™ Media Server (MMS). This is used for live broadcasts. If selected, in addition to the HLS video stream, a Windows media stream is created that can be streamed by way of multicast if the network and delivery node are configured for it. Windows media cannot handle Advanced Audio Coding (AAC-LC), so selecting MMS forces the meeting to be broadcast using G.711
Mixing Mode Video Position Video Size	The three drop-down menus: Mixing Mode, Video Position, and Video Size define behavior of the recording when Scopia® SR receives dual-stream (video and H.239) from the MCU. The system uses a best efforts approach to receive gallery layout, in which case, these values are not used. **Mixing mode**: • Video or Presentation: When someone is presenting, the user only sees the presentation. When there is no presentation, the user sees the video.

Table continues…

Field Name	Description
	• Video Over Presentation: This value refers to picture-in-picture. The video is overlaid on top of the presentation. If no one is presenting, the user only sees video. • Video next to Presentation: When someone is presenting, the user sees the video next to the presentation. If no one is presenting, the user only sees video. **Video Position**: If you choose **Video Over Presentation** as the **Mixing Mode**, this value specifies the quadrant where the video appears. **Video Size:** This value specifies the size of the video which is either over or next to the presentation. Small = 20%, Medium = 30%, and Large = 40%
Distribute to CDN	If you would like the users who are assigned this profile to be able to distribute their recordings to the content delivery network (CDN), select this checkbox. The CDN enables cloud storage and access.

5. Click **Save**.

Editing profiles

Procedure

1. Log in to Scopia® SR.
2. Click the **Profiles** tab to view the list of profiles.
3. Select a profile.
4. Click **Edit**.
5. Change the values as described in Table 11: Profiles on page 65.
6. Click **Save**.

Deleting profiles

Procedure

1. Log in to Scopia® SR.
2. Click the **Profiles** tab to view the list of profiles.

3. Select one or more profiles.
4. Click **Delete**.

Estimating disk space usage

When you define a recording profile, you must specify the capture resolution. Each resolution is configured to use a specific bitrate, so it is easy to determine the approximate size that a recording will use on your disk when using the profile.

The bitrate is specified in Kilobits per second. To determine how many Kilobits per hour, you can multiply the bitrate by 3600. Divide the answer by eight to yield KiloBytes per hour. Divide that by 1024 to get MegaBytes per hour.

Assuming total disk space of 650G, Table 12: Estimated Disk Space Usage for 650G on page 67 shows approximate usage per hour, per profile. It also shows how many hours of video can be stored. Assuming total disk space of 925G, Table 13: Estimated Disk Space Usage for 925G on page 67 shows approximate usage per hour, per profile. It also shows how many hours of video can be stored.

Table 12: Estimated Disk Space Usage for 650G

Capture Resolution	Bitrate (Kb/S)	MB / Hour	Hours of Video
1080p – 2M	2048	900	740
720p – 768K	768	337.5	1972
480p – 512K	512	225	2958
360p – 384K	384	168.75	3944
240p – 256K	256	112.5	5916

Table 13: Estimated Disk Space Usage for 925G

Capture Resolution	Bitrate (Kb/S)	MB / Hour	Hours of Video
1080p – 2M	2048	900	1055
720p – 768K	768	337.5	2813
480p – 512K	512	225	4219
360p – 384K	384	168.75	5625
240p – 256K	256	112.5	8438

Chapter 7: Managing programs

Programs

A program is a recording or a live broadcast, along with the meta-data that defines program details, such as name, description, and visibility. You can create programs by starting a recording from within an Avaya Scopia® meeting, or by scheduling a broadcast in the Scopia® Management web scheduler.

Viewing programs

Procedure

1. Log in to Scopia® SR.
2. Click the **Programs** tab to view the list of programs.
3. **(Optional)** Filter the list by selecting from the list of **Categories**.
4. **(Optional)** Search the list by entering a program name or description in the **Search** field.

Table 14: Columns on the Programs Tab

Field	Description
Name	Name of the program.
Type	Program type: It can be **Broadcast** or **Recording**.
Status	The status values are: • **Available**: Programs that have been created successfully and are available for viewing. • **Scheduled**: Programs that have not started yet, but have been scheduled by Scopia® Management. • **Failed**: Programs that did not get created due to setup issues. It is likely that there are issues with the delivery node. Check the logs for details.

Table continues…

Field	Description
	• **Failed (Insufficient Ports)**: Programs that have not been created because there were no ports available on the conference point. • **Failed (Connection)**: Programs that did not get created due to connection issues. It is likely that there are issues with the conference point. Check the logs for details. • **Failed (Duration)**: Programs that did not get created because the duration of the recording was too short. Recordings must be greater than 30 seconds in length. • **Failed (Setup)**: Programs that did not get created due to setup issues. It is likely that there are issues with gatekeeper communication. Ensure that the Conference Point is properly registered to the Gatekeeper, and that the Gatekeeper is running properly. Check the logs for details. • **Starting**: Programs that are in the process of starting. • **Started**: Program that are currently in progress. • **Complete**: A live program that is running.
Date	The date that the program was created.
Owner	Owner of the program.
Organization	When the system is configured in multi-tenant mode, this field displays the organization to which the program belongs.
Category	Category (if any) associated with the program.
Size	Size of the program in MB.

Assigning a new owner to a program

About this task

Only the program owner or the administrator can modify program properties. Program properties include the name, the category, and whether a program is displayed in the public list of programs.

Procedure

1. Log in to Scopia® SR.
2. Click the **Programs** tab to view the list of programs.

3. Select one or more programs.
4. Click **Set Owner**.

   The Select User dialog is displayed.
5. **(Optional)** Filter the list of users by selecting from the list of **Roles**.
6. **(Optional)** Search the list by entering a name or ID information in the **Search** field.
7. Select a user and click **Select User**.

Example

You might want to assign a new owner to a program if the previous owner has left the company or if the recording was created on behalf of another person.

Deleting programs

Procedure

1. Log in to Scopia® SR.
2. Click the **Programs** tab to view the list of programs.
3. Select one or more programs you want to delete.
4. Click **Delete**.
5. Click **OK** on the confirmation dialog.

Creating programs

All recordings are initially only visible to the user who created that recording. It is this user's responsibility to edit the program. They can upload a thumbnail, modify the name or description, define a PIN, specify visibility, and so on.

Related links

Creating recordings on page 70
Creating live broadcasts on page 71

Creating recordings

You can create a recording from Scopia® Desktop, Scopia® Management, or from the Interactive Voice Response (IVR) menu from any H.323 endpoint.

Example

If you are using...	You can...
Scopia® Desktop Client	Start, stop, or pause a recording from the moderator menu.
Virtual room settings (from Scopia® Desktop or Scopia® Management)	Configure your virtual room to always record the meeting.
Scopia® Management Conference Control	Start, stop, or pause a recording from the moderator menu.
H.323 endpoint	Start or stop a recording from the DTMF menu.
XT Series endpoint	Start or stop a recording from the Recording menu.
Microsoft™ Outlook Add-in	Configure your scheduled meeting to record when it starts.
Scopia® Management Web Scheduler	Schedule a live broadcast event. This is the only place from which you can create a broadcast. Configure your scheduled meeting to record when it starts.

Related links

Creating programs on page 70

Creating live broadcasts

You can use the Avaya Scopia® Management user portal to schedule meetings and reserve the necessary video network resources for the meeting.

For more information, see the *Avaya Scopia® Management Administrator Guide*, which is available on https://support.avaya.com/.

Procedure

1. As a user, access the Scopia® Management user portal and select **Schedule**.

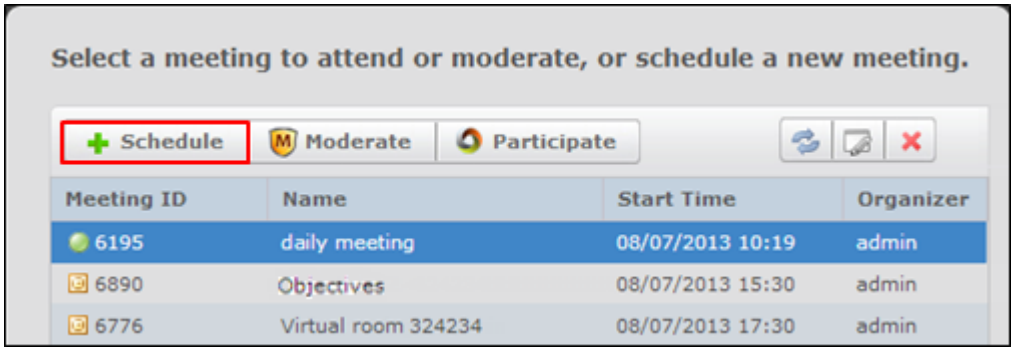


Figure 24: Access meeting scheduling from the Scopia® Management user portal

Or

2. As an administrator, access the Scopia® Management administrator portal select **Meetings** > **Meetings** > **Schedule a Meeting**.

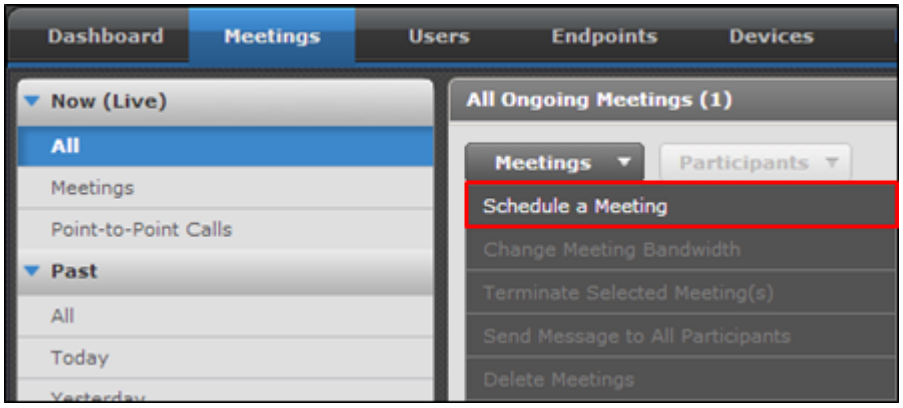


Figure 25: Access meeting scheduling in the Scopia® Management administrator portal

Enter the meeting invitation details.

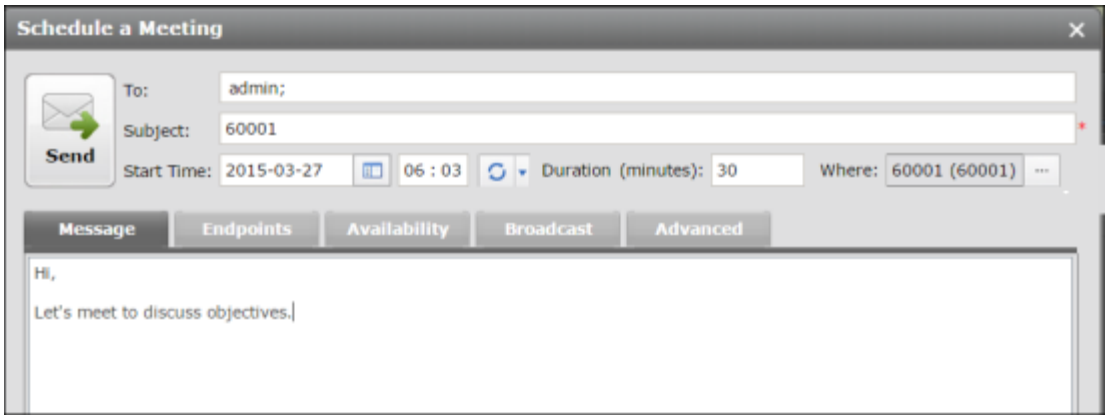


Figure 26: The Schedule a Meeting page

3. To configure whether to only record this meeting without broadcasting, select the **Advanced** tab, and select the **Record the meeting** checkbox.

   To configure streaming for this meeting, select the **Broadcast** tab.

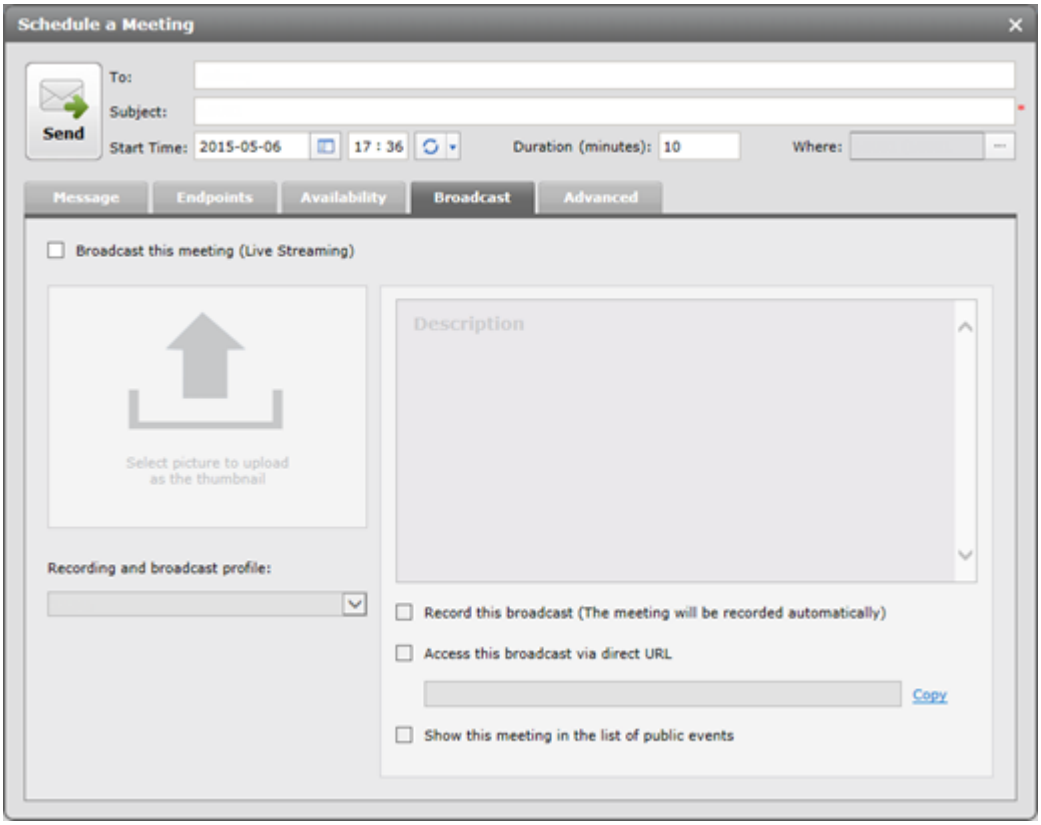


Figure 27: The Broadcast tab

Configure the broadcast meeting properties.

Table 15: Broadcast meeting properties

Field	Description
Broadcast this meeting (Live Streaming)	Select to automatically broadcast this meeting when it begins. You can view the broadcast on Scopia® Desktop Client.
Select picture to upload as the thumbnail	Select a thumbnail for this broadcast. You see this thumbnail when you view the meeting on the Scopia® Desktop Client.
Recording and broadcast profile	Select a profile for the broadcast.
Description	Enter a description for the meeting. When you search for recordings in Scopia® Desktop server it scans the descriptions.
Record this broadcast	When you select **Broadcast this meeting**, the system automatically selects this checkbox to also record the meeting. (You cannot select this option independently.) To broadcast the meeting without recording it, deselect this checkbox. To record a meeting without broadcasting, select the **Advanced** tab, and select the **Record the meeting** checkbox.

Table continues…

Field	Description
Access this broadcast via direct URL	Select **Copy** to the right of the field, to generate a URL where you can view the broadcast. The URL appears in the field.
Show this meeting in the list of public events	Select to enable all users in the organization to see the broadcast from the Scopia® Desktop Client.

Related links

Creating programs on page 70

Editing program details

The owner of a program can edit the program details from within the Scopia® SR portal page, which is accessible from the Scopia® Desktop Client. An administrator or tenant administrator also has the rights to edit any program detail.

For more information, see the *Avaya Scopia® Desktop Client User Guide*, which is available on https://support.avaya.com/.

Related links

Accessing the Scopia® Desktop Web Portal on page 74
Logging in to the Scopia® Desktop Web Portal on page 75
Editing the details of a Scopia® Desktop Recording on page 77

Accessing the Scopia® Desktop Web Portal

About this task

The Scopia® Desktop web portal is the entry point to start or join a meeting. You can also use the web portal to watch a webcast or recording, or access Scopia® Desktop Client settings.

Procedure

Enter the Scopia® Desktop public address in your Internet browser. For example, *http://sd.company.com*

Or

Right-click the Scopia® Desktop icon in the Windows system tray, and then select **Meeting Portal**.

The Scopia® Desktop web portal opens at the **Join Meeting** screen.

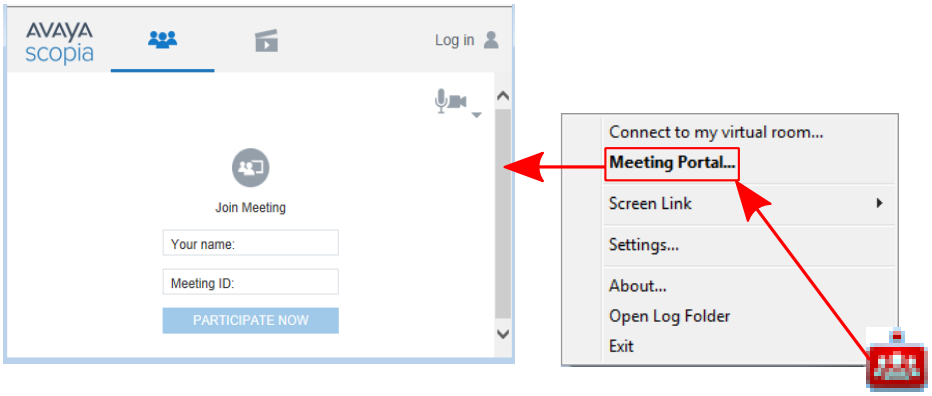


Figure 28: Scopia® Desktop web portal

Important:

Unless you change the default settings, the Scopia® Desktop web portal always opens at the **Join Meeting** screen.

Related links

Editing program details on page 74

Logging in to the Scopia® Desktop Web Portal

About this task

You can log in to the Scopia® Desktop web portal to get access to your own virtual room and the complete Scopia® Desktop functionality. For example, when you log in to the Scopia® Desktop, you can manage your videoconference recordings. Without logging in, you may have no or limited access to Scopia® Desktop functionality. For example, without logging in, you can still see the list of public recordings.

Before you begin

Contact your video network administrator to find out your Scopia® Desktop credentials.

Procedure

1. Access the Scopia® Desktop web portal, as described in Accessing the Scopia® Desktop Web Portal on page 74.
2. Ensure that the **Join Meeting** screen is displayed.

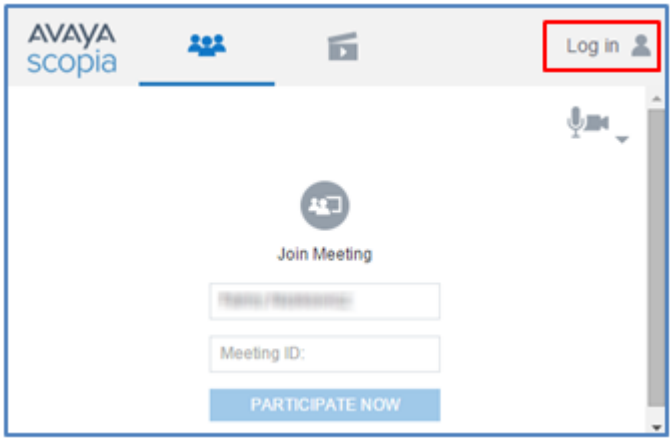
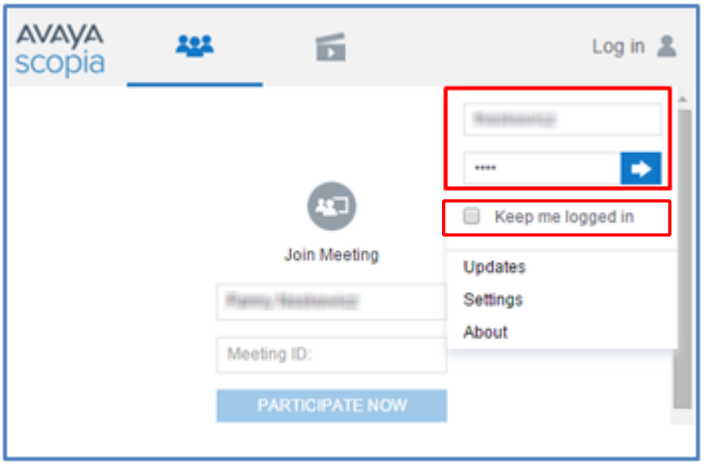


Figure 29: Join Meeting screen with the Log In link

3. Select **Log In**.
4. Enter your user name.



5. Enter your password.
6. (Optional) Select **Keep me logged in** to automatically log in the next time you launch the web portal.
7. Select .

Related links

Editing program details on page 74

Editing the details of a Scopia® Desktop Recording

Procedure

1. Access the Scopia® Desktop web portal as described in Accessing the Scopia® Desktop Web Portal on page 74.
2. Select the **Recordings and Events** tab.

   The list of available recordings is displayed.

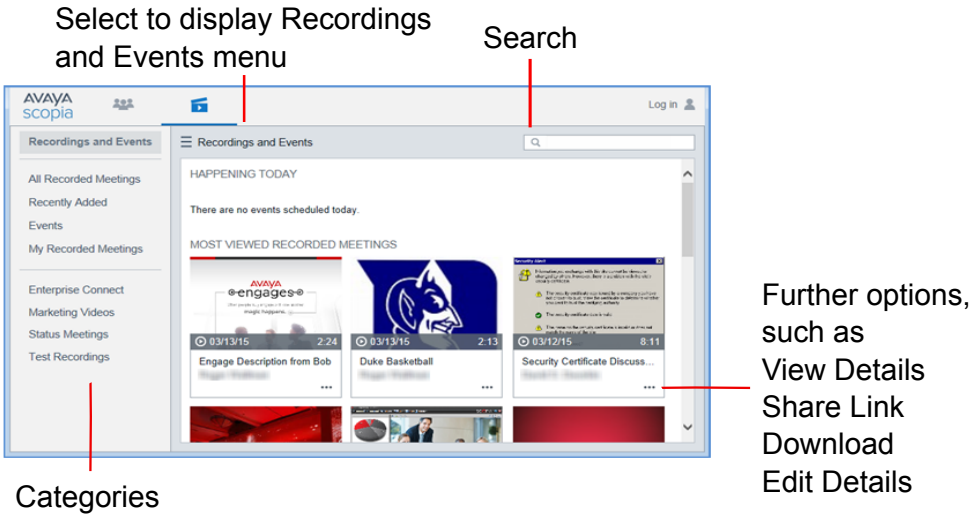


Figure 30: Recordings and Events tab of the Scopia® Desktop web portal

3. Find the recording:
   - To search by the meeting ID, name or owner, enter the value in the **Search** field and select **Search** .

     To return to the complete list of recordings, select **Recordings and Events** from the left-hand menu.
4. Select the **Further Options** button ... next to the recording.

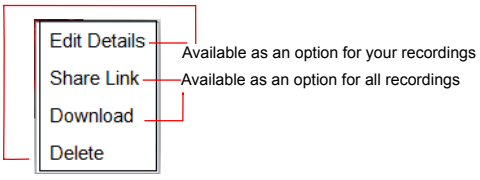


Figure 31: Further Options menu

5. Select **Edit Details**.

   The Edit details window opens.

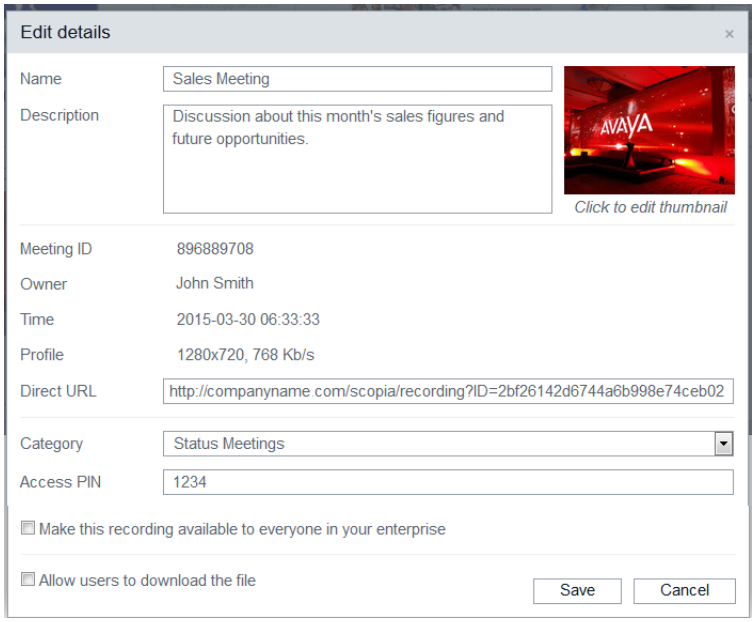


Figure 32: Edit details window

6. You can change a recording's properties as described in Table 16: Editing properties of a recording on page 78.

Table 16: Editing properties of a recording

Element	Description
Name	You can change the name which appears at the **Recordings and Events** tab of the Scopia® Desktop web portal.
Description	Edit the short description that appears in the Recording Information window (upon selecting the **View Details** button).
Category	Use the list to assign a category.
Access PIN	To protect the recording by limiting access to it, enter the access PIN. You can use any combination of alphanumeric characters.
Make this recording available to everyone in your enterprise	Select to make the recording public and clear it to make it private. **Note:** Even if a recording is private, users can still access it if they have the direct URL address of the recording.
Allow users to download the file	Select to enable users to save the file to their computer and clear it to prevent users from saving the file to their computer.
Thumbnail picture	You can change the default thumbnail by clicking on it. Your thumbnail should represent the program. It should be 4x3 aspect ratio, and ideally should be <100Kb. In terms of file types, Scopia® Desktop supports .png, .jpg, .gif.

7. Select **Save** to save the changes you made to the recording's properties.

Related links

Editing program details on page 74

Chapter 8: Managing categories

Categories

As an administrator, you can define categories that publishers can use when they edit their program information.

A category is a subject heading that contains various subtopics. You use categories to group programs that contain similar subject matter. For example, you can create a "Human Resources" category to contain programs for employees.

Creating categories

Procedure

1. Log in to Scopia® SR.
2. Click the **Categories** tab to view the list of categories.
3. Click **New**.
4. In the **Categories Information** dialog, in the **Name** field, enter a name for the category.
5. Click **Save**.

Editing categories

If you edit a category, all the programs associated with the category are moved to the new name.

Procedure

1. Log in to Scopia® SR.
2. Click the **Categories** tab to view the list of categories.
3. Select a category.
4. Click **Edit**.
5. In the **Categories Information** dialog, in the **Name** field, update the name for the category.

6. Click **Submit**.

Deleting categories

If you delete a category, all programs previously associated with it are unassociated with that category.

Procedure

1. Log in to Scopia® SR.
2. Click the **Categories** tab to view the list of categories.
3. Select a category.
4. Click **Delete**.

Chapter 9: Backing up and restoring Scopia® SR

About backups

You can back up:

- The Scopia® SR configuration settings
- The Scopia® SR Manager
- The saved programs (videoconferences) and the database which are stored on a delivery node (DN)

You may have several DNs in your configuration, however, you only need to back up one of the DNs.

Backing up the Scopia® SR configuration

Once you install and configure Scopia® SR, you should back up the configuration. You can restore this backup in the case of a hardware failure or if you have to re-image the computer.

Procedure

1. Open a Powershell window.
2. Type `C:\Program Files\Avaya\scripts\assr_config.ps1 -b <folder>`

   `<folder>` is the optional path to the folder where you want to create the backup file. If you do not specify a folder, Scopia® SR creates the backup in `<C:\Program Files\Avaya\backups>`

   When you execute this command, a backup file is created: **ASSR-Config-yyyy-MM-ddThh-mm-ss.ini**.

Example

If you want to create a backup in the temp directory, type this command: `C:\Program Files\Avaya\scripts\assr_config.ps1 -b %TEMP%`

Next steps

Avaya recommends moving your backup to another computer.

Restoring the Scopia® SR configuration

About this task

If you restore a backup, Scopia® SR restores the Hyper-V virtual machines' MAC address so that they still operate properly with the Scopia® SR Manager. If you restore the configuration, Scopia® SR stops the virtual machines, reconfigures their mac addresses and then restarts the virtual machines.

Before you begin

Ensure that there are no recordings in progress.

Procedure

1. Open a Command Prompt window.
2. Type `C:\Program Files\Avaya\scripts\assr_config.ps1 -r <backupFile>`

   `<backupFile>` is the full path to the INI backup file.

Backing up the Scopia® SR Manager

The Scopia® SR data is stored in a database and in specific folders. Avaya recommends capturing this data for backup purposes.

The Scopia® SR Manager contains all of the application logic for Scopia® SR. There is a single Scopia® SR Manager present.

By default, Scopia® SR runs a scheduled backup task daily at midnight. This task creates Scopia® SR Manager backups in the folder: `C:\Program Files\Avaya\backups`

Avaya recommends moving your backup to another computer.

Before you begin

You require access to the Scopia® SR Manager console.

Procedure

1. Open a Command Prompt window.
2. Type `assr_installer –b <folder>`

   `<folder>` is the path to the folder where you want to create the backup file.

   When you execute this command, a backup zip file is created: **ASSR-Manager-yyyy-MM-ddThh-mm-ss.zip**.

Example

If you want to create a backup in the temp directory, type this command: `assr_installer -b %TEMP%`

Next steps

You must now back up the DN in order to preserve content.

Restoring the Scopia® SR Manager

Before you begin

You require access to the Scopia® SR Manager console.

Procedure

1. Open a Command Prompt window.
2. Type `assr_installer –r <path to zip>`

   `<path to zip>` is the full path to the backup file.

   When you execute this command, your backup file is restored.

   Any recordings that you created after you created the backup file will not be restored.

   When you restore the Scopia® SR Manager, you restore the software version as well. Therefore, if you backed up version 8.3.0.100 and have since upgraded to 8.3.0.105, the restore operation restores version 8.3.0.100. You must then perform a software upgrade to bring the Scopia® SR Manager to 8.3.0.105.

Backing up delivery nodes

The delivery node stores much of the information in a database and content is stored in files in specific directories. Avaya recommends backing up this data.

You may have several DNs in your configuration, however, you only need to back up one of the DNs.

You require login access to the delivery node console or you can SSH to the delivery node using a terminal emulator, such as PuTTY. PuTTY is a Windows SSH client that allows you to connect to other machines, giving you a terminal window. You can download PuTTY from http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html.

There are two methods that can be used to backup and restore a DN.

- Using `tar`: Performed using the `backupdn_tar.sh` shell script.
- Using `rsync`: Performed using the `backupdn_rsync.sh` shell script.

Backing up using `tar` is straightforward. However, it has limitations:

- The script creates a compressed tar file. If your DN is currently using more than half of its capacity, you must create the tar file on a network-mounted or USB drive.

- The script is time consuming. Every backup performed is a full backup is more time consuming than an incremental backup.

Avaya recommends using `rsync`. `rsync` mirrors the DN on another file system. You should either mount a USB drive or mount a remote Linux server.

- In order to use `rsync`, you must either mount a USB drive or mount a remote Linux server
- The target file system must have 650G free space

After initial synchronization, `rsync` backups are incremental – only modified files are copied to the remote system.

You may want to configure a cronjob to perform the `rsync` command on a nightly basis. Make an entry in your cron table such as:

```
0 0 * * * <cmd>
```

Where `<cmd>` is the full `rsync` shell script specified below to run the `rsync` command every night at midnight.

Related links

Making a USB drive accessible on page 85
Backing up delivery nodes on page 90
Restoring delivery nodes on page 91

Making a USB drive accessible

You may want to insert a USB drive into the Scopia® SR server and access it for backups. You must mount the disk to the delivery node (DN) machine and format it.

About this task

When you format the USB drive, you erase all data on the USB, so perform this task before you copy important data to the USB drive.

Procedure

1. Plug the USB disk into the Scopia® SR server hosting your DN.
2. Set the disk to **Offline** in Windows.
   a. Open Disk Management by entering `diskmgmt.msc` in the **Run** field.
   b. Find your removable disk in the lower panel.

      It should be displayed as **Disk 1**.
   c. Right-click on the blue disk partition and select **Change Drive Letter and Paths...**
   d. Select the assigned drive letter and click **Remove** to remove it.
   e. Click **OK**.
   f. Right-click on the disk itself, to the left of the blue partition area, and select **Offline** to put the disk into offline mode.

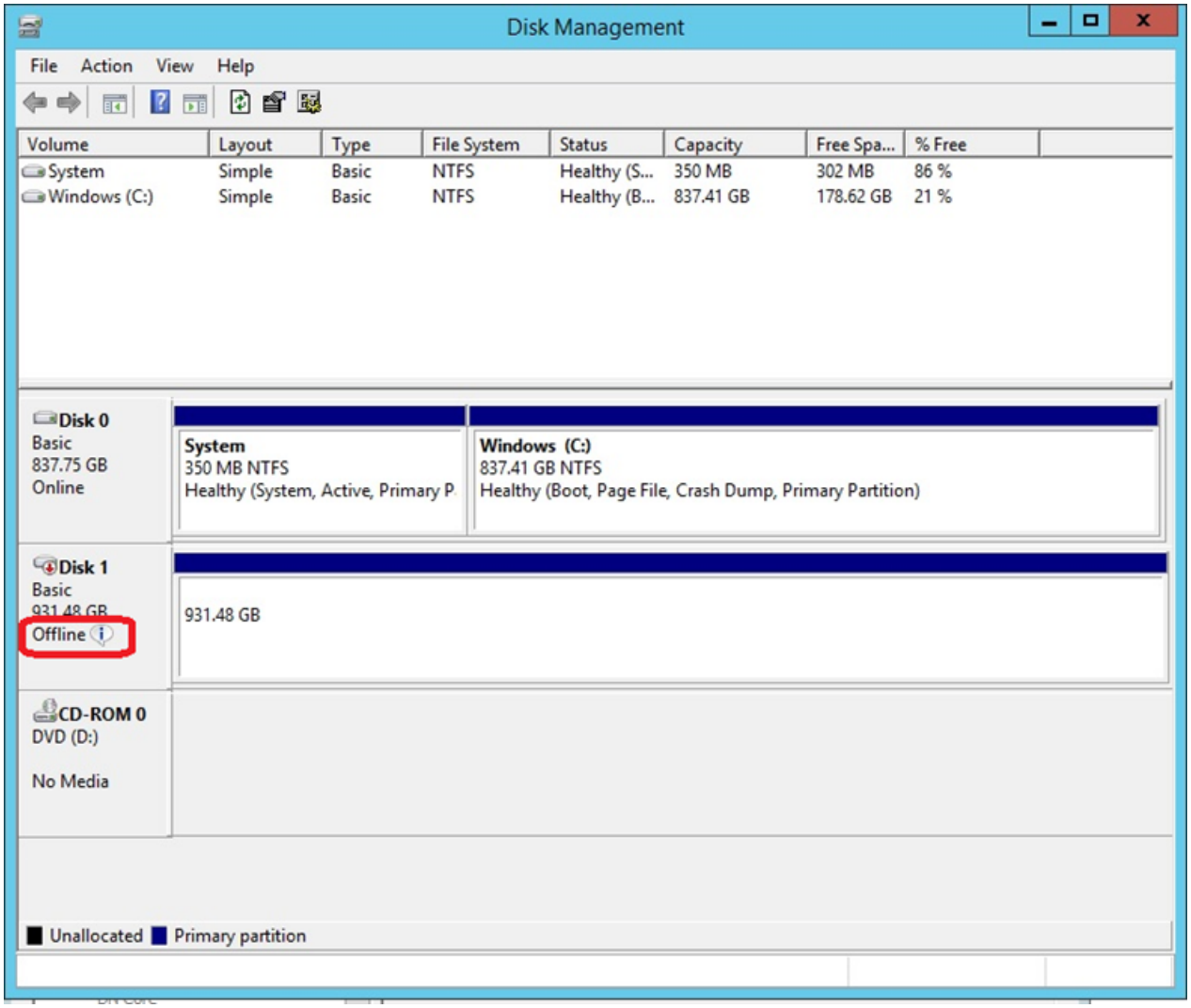


Figure 33: Disk Management

3. Connect the disk to DN virtual machine (VM).
    a. Open Hyper-V Manager by entering `virtmgmt.msc` in the **Run** field.
    b. Right-click on the DN virtual machine, and select **Settings**.
    c. Open the **SCSI Controller** section using the list on the left.
    d. Select **Hard Drive** in the section on the right and click **Add**.
    e. Select the **Physical Hard Disk** radio button and pick the USB hard disk that you wish to mount.

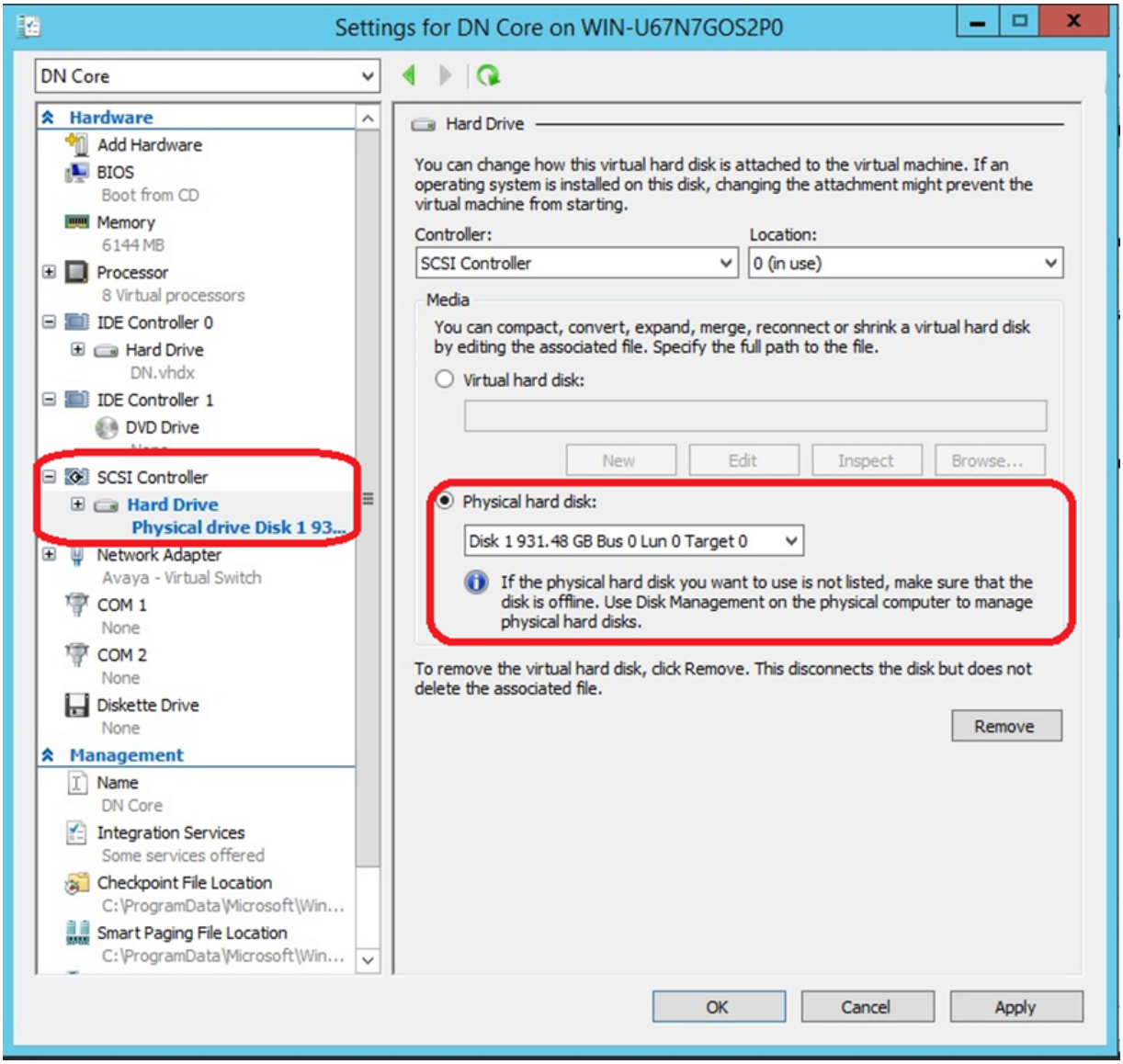


Figure 34: Settings for DN Core

4. Configure the disk in Linux.
   a. Open a terminal into the DN using SSH or PuTTY.
   b. Rescan the SCSI host by entering this command:

      ```
      echo "- - -" > /sys/class/scsi_host/host1/scan
      ```

   c. Check that the disk appears in the disk list by entering this command:

      ```
      fdisk -l
      ```

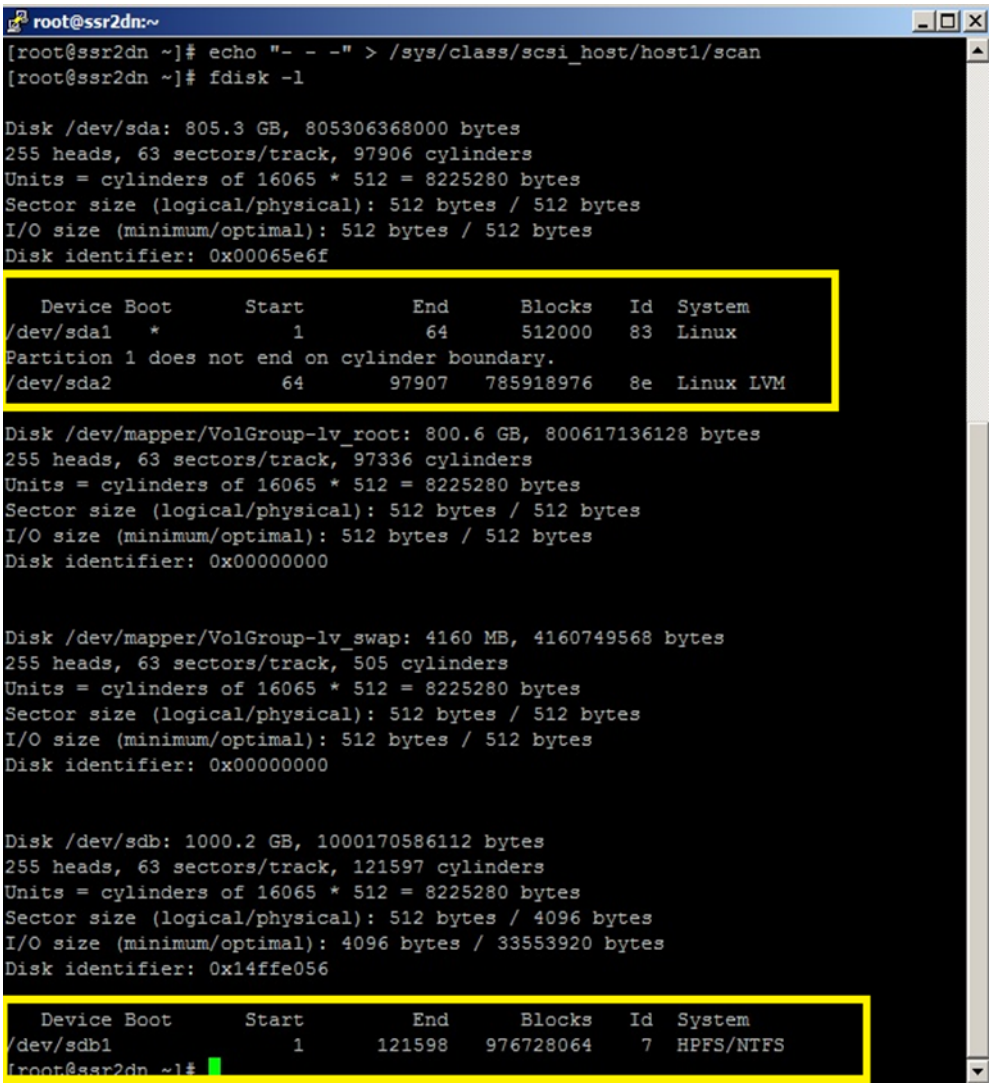


Figure 35: Rescan SCSI and run fdisk to check that the disk is in the list

d. Format the disk in ext2.

Note:

This step erases all the data on the USB drive.

a. Unmount the disk by entering this command:

```
umount /dev/sdb1
```

b. Use `fdisk` to delete the current partition, create a new partition, and write the partition table.

```
fdisk -c /dev/sdb
```

- Use the `fdisk d` command to delete the current drive.
- Use the `fdisk n` command to create a new partition that encompasses the entire drive.

- Use the `fdisk w` command to write the partition table.

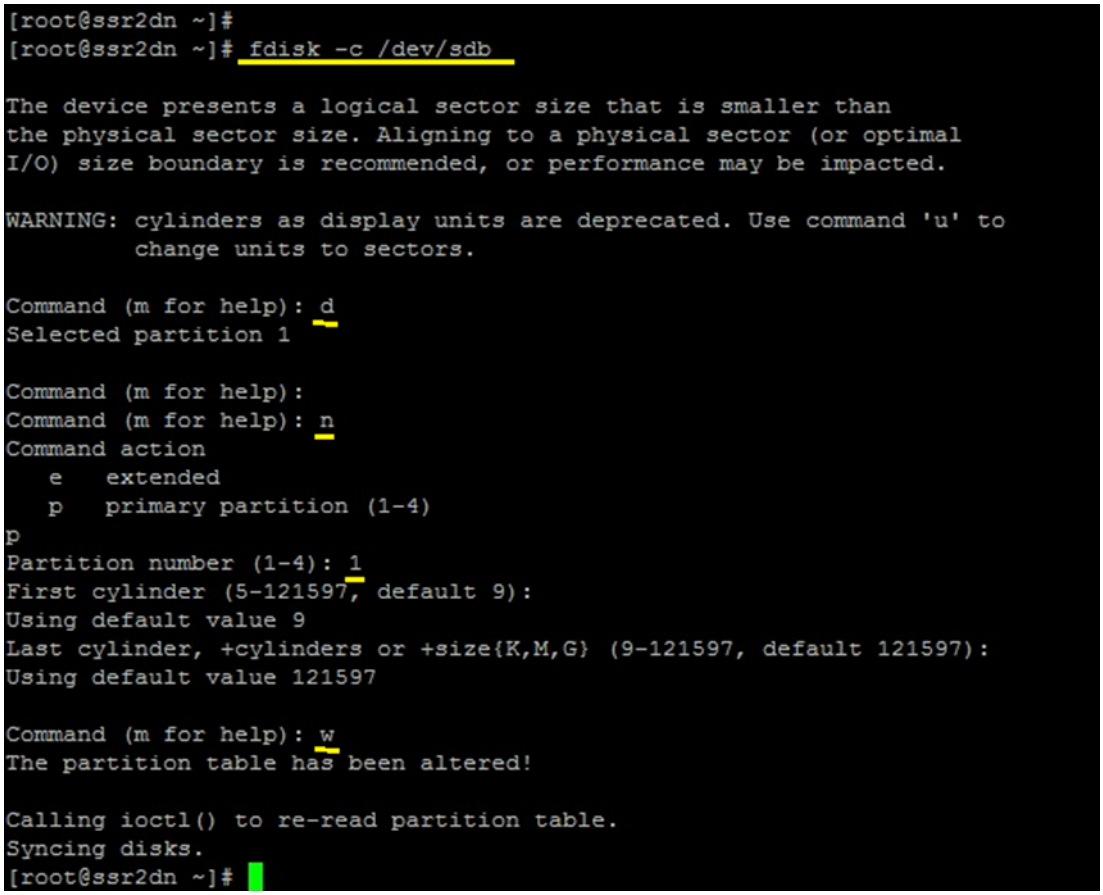


Figure 36: fdisk command

e. Verify that the disk is formatted properly by entering this command:

```
fdisk -l

Device Boot      Start         End      Blocks   Id  System
 /dev/sdb1               1       30401   244195008+  83  Linux
```

f. Reformat the attached disk using ext2.

```
mkfs.ext2 /dev/sdb1
```

g. Mount the disk by entering the following command:

```
mkdir /media/backup
mount /dev/sdb1 /media/backup
```

The disk is now available at `/media/backup`, and can be used in either of the methods for backing up and restoring the DN.

Related links

Backing up delivery nodes on page 84

Backing up delivery nodes

The delivery node stores much of the information in a database and content is stored in files in specific directories. Avaya recommends backing up this data.

You may have several DNs in your configuration, however, you only need to back up one of the DNs.

There are two methods that can be used to backup and restore a DN.

- Using `tar`: Performed using the `backupdn_tar.sh` shell script.
- Using `rsync`: Performed using the `backupdn_rsync.sh` shell script.

Avaya recommends using `rsync`. `rsync` mirrors the DN on another file system. You should either mount a USB drive or mount a remote Linux server.

About this task

You require login access to the delivery node console or you can SSH to the delivery node using a terminal emulator, such as PuTTY. PuTTY is a Windows SSH client that allows you to connect to other machines, giving you a terminal window. You can download PuTTY from http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html.

Before you begin

You require access to the Scopia® SR Manager console.

Procedure

1. Log in to the delivery node.
2. Execute the following script.

   ```
   /opt/stream/bin/backupdn_rsync.sh <backupDir>
   ```

   You must substitute `<backupDir>` for your backup server. If backing up using a remote server,`<backupDir>` should be of the form:`root@address-of-backup-server:/path/to/backup-location/`

   If you are backing up using a mounted USB drive, `<backupDir>` should be of the form:`/path/to/backup-location/`

   For example, if the USB drive was mounted to `/media/backup`, issue the command: `/opt/stream/bin/backupdn_rsync.sh /media/backup/dn-backup/`
   Where:

   - `root`: Username of privileged account on destination server.
   - `address-of-backup-server`: IP address or DNS name of destination server.
   - `/path/to/backup-location/`: Full path to the location with which the DN will synchronize (the trailing slash is required).
3. **(Optional)** Alternatively, you can use the `tar` script.
   a. Log in to the delivery node.

b. Execute the following script.

```
/opt/stream/bin/backupdn_tar.sh <backupDir>
```

The <backupDir> argument is optional. If present, the backup file is placed in this directory. If not present, the backup is written to /opt/stream/movies/backup. The <backupDir> folder must exist prior to running the script.

c. Save the resulting ASSR_DN.<date>.tar file.

Related links

Backing up delivery nodes on page 84

Restoring delivery nodes

About this task

You require login access to the delivery node console or you can SSH to the delivery node.

If you want to restore the backup to a different server, you must replace the original DN in the Scopia® SR Administration GUI.

Any programs created, or media uploaded after the backup was made are lost. You should backup and restore the Scopia® SR Manager and DN at the same time. The restore script stops the DN services, performs the restore, and then restarts the DN services.

Before you begin

You must have backed up the delivery and have a backup file.

If you are using the recommended rsync script, you must mount the drive that was used when the backup was performed.

Procedure

1. Log in to the delivery node.
2. Execute the following script.

```
/opt/stream/bin/restoredn_rsync.sh <backupDir>
```

You must substitute <backupDir> for your backup server. If restoring using a remote server,<backupDir> should be of the form:root@address-of-backup-server:/path/to/backup-location/

If you are restoring using a mounted USB drive, <backupDir> should be of the form:/path/to/backup-location/

For example, if the USB drive was mounted to /media/backup, issue the command: /opt/stream/bin/restoredn_rsync.sh /media/backup/dn-backup/
Where:

- root: Username of privileged account on destination server.
- address-of-backup-server: IP address or DNS name of destination server.

- `/path/to/backup-location/`: Full path to the location with which the DN will synchronize (the trailing slash is required).

3. **(Optional)** Alternatively, you can use the `tar` script.
   a. Log in to the delivery node.
   b. Execute the following script.

      ```
      /opt/stream/bin/restoredn_tar.sh <backupDir>
      ```

      `<backupDir>` should be the full path to the backup file.
   c. Save the resulting `ASSR_DN.<date>.tar` file.

Related links

Backing up delivery nodes on page 84
Installing a new DN if have only one DN and you have fixed the hard drive or replaced the appliance on page 165

Chapter 10: Upgrading or patching Scopia® SR

About Scopia® SR patches

Avaya makes patches available for Scopia® SR. You can update an individual component of Scopia® SR without having to update the entire solution. There are two methods for applying a patch:

- You can push a patch to a component using the Scopia® SR Manager administration interface.
- You can install a patch directly on an appliance, using an executable file.

Table 17: Components

Component	How to upgrade or patch
Installer utility (assr_installer.exe)	You can upgrade it using assr_installer.exe.
Configuration utility	You can upgrade it using assr_installer.exe.
Converter utility	You can upgrade it using assr_installer.exe.
Configuration backup script	You can upgrade it using assr_installer.exe.
Migration utility (for migrating recordings from Scopia® Content Center Recording server)	This is a zip file which you can extract and run on the Scopia® Content Center Recording server .
Scopia® SR Manager	You can upgrade it using assr_installer.exe.
Delivery node (DN)	You can upgrade it using the Scopia® SR Manager administration interface.
Virtual delivery node (VDN)	You can upgrade it using the Scopia® SR Manager administration interface.
Conference point (CP)	You can upgrade it using the Scopia® SR Manager administration interface.
Transcoder	You can upgrade it using the Scopia® SR Manager administration interface.

Downloading software from PLDS

About this task

Note:

You can download product software from http://support.avaya.com also.

Procedure

1. Type http://plds.avaya.com in your web browser to go to the Avaya PLDS website.
2. Enter your Login ID and password to log on to the PLDS website.
3. On the Home page, select **Assets**.
4. Select **View Downloads**.
5. Search for the available downloads by using one of the following:
   - Select an application type from the list and the version number.
   - By download name
6. Click the download icon from the appropriate download.
7. When the system displays the confirmation box, select **Click to download your file now**.
8. If you receive an error message, click the message, install Active X, and continue with the download.
9. When the system displays the security warning, click **Install**.

   When the installation is complete, PLDS displays the downloads again with a check mark next to the downloads that have completed successfully.

Enabling remote desktop

About this task

In order to install a patch using the installer utility, you must have physical or remote access to the Scopia® SR appliance. To enable remote access, you must open a firewall port.

Procedure

1. On the Scopia® SR appliance, open **Server Manager** and navigate to **Tools** > **Windows Firewall with Advanced Security**.
2. Click **Inbound Rules**.
3. Scroll down the page and double-click **Remote Desktop – User Mode (TCP-In)**.
4. Click the **Advanced** tab.
5. In the **Profiles** panel, select the **Public** checkbox.

6. Click **Apply**.
7. Click **OK**.

Upgrading or patching the components using assr_installer.exe

About this task

You can upgrade the Scopia® SR Configuration Utility, the Scopia® SR Manager, and the Scopia® SR installer itself, amongst other components, using the assr_installer.exe. This file is already installed on the server, in:

```
C:\Program Files\Avaya
```

The assr_installer.exe can perform a number of functions:

- It automatically backups and restores the Scopia® SR Manager
- It installs and upgrades the components

Procedure

1. Download the component , which is delivered as a ZIP file.
2. Open a command prompt window.
3. Navigate to the folder where you downloaded the component.
4. Perform the following:
   - For upgrades, run the following command:

     ```
     assr_intaller.exe <options> \path\to\ZIP
     ```

   - For patches, run the following command:

     ```
     assr_installer.exe <Patch>.zip
     ```

5. **(Optional)** If you are performing an upgrade, you can use the following flags:
   - `-i`: Forces a fresh installation, rather than an upgrade. Any previous settings are lost. You should only use this flag when installing the Scopia® SR Manager. Use this flag only when instructed.
   - `-q`: (Quiet) Suppresses warnings when doing a fresh installation.
   - `-f`: (Force) Overrides version validation, allowing you to upgrade an older version over a newer version. Avaya does not recommend this flag. If the database schema has changed between versions, for example, results can be unexpected. Use this flag only when instructed.

Upgrading or patching the components using the Scopia® SR Manager administration interface

You can upgrade conference points, delivery nodes, virtual delivery nodes, and transcoders using the Scopia® SR Manager interface. You must upgrade the Scopia® SR Manager before you upgrade the conference points and delivery nodes.

Before you begin

If upgrades of all components are available, you must upgrade the Scopia® SR Manager before you upgrade the conference points and delivery nodes.

You must have a support and maintenance agreement with Avaya. Contact your Avaya Support Representative for more information.

Procedure

1. Contact Avaya to obtain the latest upgrade images and access keys.
2. Copy the images to a web server within your network.

   If you do not have a web server available, you can copy them to a special directory on the Scopia® SR Manager.

   a. On the Scopia® SR Manager server, navigate to the folder: `C:\Program Files\Apache Software Foundation\Tomcat 7.0\webapps\ROOT`

   b. Ensure the directory `upgrades` exists and create it if it does not exist.

   c. Copy the upgrade images into `C:\Program Files\Apache Software Foundation\Tomcat 7.0\webapps\ROOT\upgrades`

      The URL for the image will be `http://<ip_of_manager>/upgrades/<ZIP_file>`
3. Log in to Scopia® SR.
4. Click the **Devices** tab.
5. From the **Actions** menu, select **Upgrade Devices**.
6. Select the devices to upgrade:
   - To upgrade one device, select **Single Device** and select the device from the drop-down list.
   - To upgrade all devices of a particular type, select **All Devices of Type** and select the type from the drop-down list.
7. In the **URL of Software Image** field, enter the location of the upgrade image that you copied to the network.
8. Click **Submit**.
9. Confirm the details.
10. Click **Finish**.

Next steps

Wait for several minutes and then verify the upgrade.

Verifying the upgrade of conference points and delivery nodes

Before you begin

Upgrade the conference points and delivery nodes.

Procedure

1. Log in to Scopia® SR.
2. Click the **Devices** tab.
3. From the **Browse** menu, select the device you want to verify.

   The list of devices of the type you selected is displayed.
4. Check that the version displayed is the version to which you upgraded.

Verifying the upgrade of the transcoder

Before you begin

Upgrade the conference points and delivery nodes.

Procedure

1. Retrieve the transcoder log file directly from the transcoder.

   The log file is at: `https://<transcoder IP address>:8443/transcoder_log.txt`
2. Search for `Starting service` in the logs.

   The version number of the transcoder is in the line above the phrase `Starting service`.
3. Check that the version displayed is the version to which you upgraded.

Chapter 11: Publishing external content

Publishing recordings that were created using older Avaya Scopia® solutions

Avaya has created a migration utility, called the Avaya Scopia® Streaming and Recording server Migration Utility, to help customers to upgrade from older Avaya Scopia® solutions to the Avaya Scopia® 8.3.2 solution. As part of the migration process, the utility converts recordings from the .MOV format to the .MP4 format.

You can use the functionality of this migration utility to publish MP4 recordings that have been created outside of the scope of Scopia® SR.

Scopia® SR also imports all of the information related to the recordings, including categories and meta data. Meta data refers to information associated with each recording, such as the recording description, the owner name, and the access level.

Meta data files must have the extension .XML. When Scopia® SR Manager detects a meta data file, it automatically uploads and publishes the specified video file within the description. When in Enterprise mode, it uses the default system profile. When in multi-tenant mode, it uses the organization's default profile for the specified publisher.

If a recording does not have an owner, it is publicly available on the Scopia® SR server. Only an administrator can edit it.

About this task

Note:

Avaya recommends limiting the size of the recordings that you are migrating to 600GB so that the Scopia® SR has room for new recordings.

Procedure

1. Enable the Autopublish utility.
   a. On the Scopia® SR, log in to the Scopia® SR Manager Administration interface.
   b. Navigate to **Global Policies** > **Media AutoPublish**.
   c. Select **Enabled**.
   d. Enter the destination folder to use for auto-publishing.

      If you are using the converter utility to import recordings from Avaya Scopia® Content Center Recording server , use this folder as the **Destination Path** in the converter utility.

e. Enter a polling interval in the **Polling Interval** field. The default is two minutes.

f. Select **Save**.

2. Ensure that the media file has the same name as the meta data file.

   For example, samplevideo.mp4 and samplevideo.xml.

3. Ensure that the `<program>` tags in the .xml file are populated.

   For more information, see XML File on page 99 and Table 18: XML File on page 99.

   If there is no value in the `<program>` tag, the import process fails.

4. Copy the media file into the AutoPublish directory before you copy the meta data file into the same directory.

   The system automatically imports and publishes the file.

XML File

```
<media>
<name>nameOfMP4.mp4</name>
<description>Program Description</description>
<folder>demo</folder>
<type>video</type>
<publisher>admin</publisher>
<ownerId>3</ownerId>
<accessLevel>private</accessLevel>
<tenantId>999</tenantId>
<category>Marketing</category>
<program>
    <name>Name of Program</name>
    <description>Program Description</description>
    <password>123</password>
    <meetingId>711</meetingId>
    <startDate>1351898567737</startDate>
</program>
</media>
```

Table 18: XML File

Element	Required?	Default	Description
name	Yes	N/A	The name of the media file to be imported. It must match the file on disk.
description	no	Empty	Description of the media file.
folder	no	“Default”	This must be “Default” (case sensitive) or omitted entirely.
type	no	“video”	The type of media file. Currently, only ‘video’ is supported.

Table continues…

Element	Required?	Default	Description
publisher	no	admin	User name which will own the media (and program). Either `publisher` or `ownerId` should be specified. Both values are not needed.
ownerId	no		Owner ID which will own the media (and program). Either `publisher` or `ownerId` should be specified. Both values are not needed.
accessLevel	no	“private”	Only the values `public` or `private` are supported.
tenantId	yes		Within a multi-tenant deployment, this is the ID of the organization to which the recording belongs. Within an enterprise deployment, use `999`.
category	no	None	Category to which the recording belongs.
program	yes	If you do not enter values in this section, the import process fails.	You must enter values in this section in order to successfully create the program.
<program>			
name	yes		The name of the program to be published.
description	no	Empty	A description of the program to be published.
password	no	None	The PIN used to protect the program. If a PIN is specified, a user must specify a PIN to watch the program.

Next steps

If the import process is successful, the system removes the media file and the meta data file from the AutoPublish directory. In addition, the system creates a .status file per recording. This .status file remains for one day after the publishing.

If there is an error, an err file is generated.

Chapter 12: Distributing content

About streaming methods

Scopia® SR enables users to view recordings as streamed content. Scopia® SR also enables users to download the content file and view it locally. Streamed content plays across a network and downloaded content plays from a local system.

Delivery nodes can distribute content using two streaming methods:

- Unicast streaming
- Multicast streaming

Unicast streaming sends streams from one system to one client using HTTP Live Streaming (HLS). Multicast streaming sends streams from one system to many clients using Microsoft™ Media Server (MMS) and Advanced Systems Format (ASF) streaming protocols. Multicast streams must be routed between addresses 224.0.0.0 to 239.255.255.255.

The main method that Scopia® SR uses is the unicast method. However, you can also enable multicast and Scopia® SR generates a secondary multicast stream for distribution to an internally-enabled multicast network of Windows and Mac desktop computers. In this scenario, Scopia® SR still uses the unicast method to stream to mobile devices.

You can configure the streaming settings for each separate delivery node. For example, you can enable unicast streaming to send streams to external clients and enable multicast streaming to send streams to internal clients that reside on the WAN. Alternatively, you can send simultaneous unicast and multicast streams from a source delivery node. For example, you could configure a particular source delivery node to multicast the stream and to also push the content to an edge delivery node.

If you specify multicasting, Scopia® SR attempts to stream the content to Windows and MAC desktops using the MMS protocol. If that method fails, it does not attempt unicasting to Windows and MAC desktops. It will however, use unicasting to stream to mobile devices.

Configuring broadcast settings

About this task

Use this task to configure the broadcast and delivery settings for content and the settings for the delivery nodes.

Procedure

1. Log in to Scopia® SR.
2. Click the **Global Policies** tab.
3. Click **Distribution** on the **Policies** menu.
4. Configure the settings, as described in Table 19: Distribution Settings on page 102.

Table 19: Distribution Settings

Field Name	Description
Source DN Delivery	• Unicast Only: Select to enable only unicasting from the source delivery node. • Multicast Only: Select to enable only multicasting from the source delivery node. If you select this option and the client does not support multicasting, viewers cannot view the program. • Multicast and Unicast (Unicast Rollover if Multicast is unsuccessful): Select to enable Scopia® SR to unicast the stream if multicasting is not available. If you select **Multicast and Unicast** and multicast resources are unavailable on the delivery node, Scopia® SR does not attempt to unicast the stream. Ensure that the multicast resources on your delivery node are configured correctly.
Edge DN Delivery	• Unicast Only: Select to enable only unicasting from the edge delivery node. • Multicast Only: Select to enable only multicasting from the edge delivery node. If you select this option and the client does not support multicasting, viewers cannot view the program. • Multicast and Unicast (Unicast Rollover if Multicast is unsuccessful): Select to enable Scopia® SR to unicast the stream from the edge delivery node if multicasting is not available. If you select **Multicast and Unicast** and multicast resources are unavailable on the delivery node, Scopia® SR does not attempt to unicast the stream. Ensure that the multicast resources on your delivery node are configured correctly.

Table continues…

Field Name	Description
Allow individual DN's to override Broadcast settings	Select to enable an administrator to change the broadcast settings, including multicast and unicast for a specific delivery node. When this check box is checked, a new section appears in the configuration settings for that particular delivery node. These new settings are displayed at **Devices** > **Delivery Nodes**. For more information, see Table 5: Override Default Distribution Policy Panel on page 46.

5. Click **Save**.

Configuring multicast and quality of service (QoS) settings

Only Windows Media Player and Silverlight™ can play a multicast stream.

Procedure

1. Log in to Scopia® SR.
2. Click the **Global Policies** tab.
3. Click **Network** on the **Policies** menu.
4. Configure the settings, as described in Table 20: Network Settings on page 103.

Table 20: Network Settings

Field Name	Description
Multicast IP Addresses from	Enter starting and ending IP addresses. The range of IP addresses must be from 224.0.0.4 to 239.255.255.255. Depending on the span of the range, it may take several minutes to identify the systems to use for multicasting. There are many reserved multicast addresses that you should not use in the 224.X.X.X range, so you should start at least at 225.0.0.0. If you enter a single IP address, you must enter a range of ports. If you do not enter a range of ports, you will be unable to select any of the multicasting options in the **Live Event Settings** on the **Distribution** screen.
Multicast ports from	Enter the starting and ending ports. This is the range of ports that the delivery nodes use for multicasting.

Table continues…

Field Name	Description
	Port numbers must be greater than 1024. Ports 1024 and lower are reserved and cannot be used for multicasting.
TTL	Enter the maximum number of routers that the multicast stream routes through from the source delivery node to reach the multicast target. You may have to enter one more router than the maximum, depending on your network configuration. Enter a number that is high enough to reach all of the intended IP addresses in your network, but low enough to remain within your network's limits. If your network is configured so that the TTL decrements as the packet leaves the network, enter the maximum number of routers that the stream can pass through in the **TTL** field. If your network is configured so that the TTL decrements as soon as the packet reaches the router, enter one more than the number of hops in the **TTL** field.
QoS Priority – Live Programs	Enter a Differentiated Services Code Point (DSCP) value between 0 to 63. This value is marked on all packets for live programs. The default is 0 and this value equates to **Best Effort**. You can change the quality of service settings without impacting multicasting. You cannot change the quality of service settings without impacting unicasting streams that are currently open.
QoS Priority – On-demand Programs	Enter a Differentiated Services Code Point (DSCP) value between 0 to 63. This value is marked on all packets for on-demand programs. The default is 0 and this value equates to **Best Effort**. You can change the quality of service settings without impacting multicasting. You cannot change the quality of service settings without impacting unicasting streams that are currently open.

5. Click **Save**.

Viewing the distribution status of recordings

You can view the distribution status of each recording to check whether it has been distributed to each of the delivery nodes. You can also view the status of all recordings associated with a particular delivery node.

Procedure

1. Log in to Scopia® SR.
2. Click the **Reports** tab.
3. Click **Distribution Status** on the **Reports** menu.

   Scopia® SR displays the status of the current recordings.
4. **(Optional)** If a particular recording or program has a **Failed** status, you can click **Retry Distribution**.

   If Scopia® SR is distributing a program from a source Delivery Node to an intermediate Delivery Node, it displays the status **Pending** on the Distribution Status page until it finishes distributing the program.

Viewing the distribution status of delivery nodes

Source programs originate on the current DN. Distributed programs do not originate on the current DN, but are distributed from another DN.

Procedure

1. Log in to Scopia® SR.
2. Select the **Devices** tab.
3. From the **Browse** menu on the left, click **Delivery Nodes**.
4. Click the name of the delivery node to display the delivery node details.

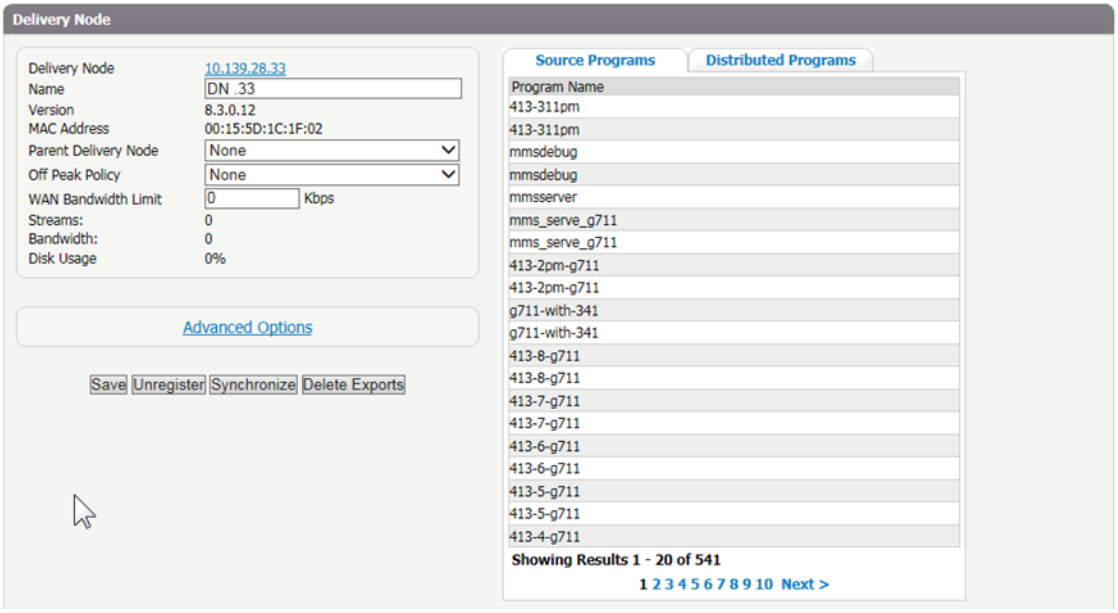


Figure 37: Delivery Node Details

5. View the **Source Programs** and **Distributed Programs** tabs.

   Note:

   You can remove a distributed program from the current DN by selecting a program and clicking **Delete** on the **Distributed Programs** tab. If you delete a program from a DN, viewers mapped to that DN will not be able to play the program. If you want to restore all deleted distributed programs, you must expand **Advanced Options** and click **Distribute All Programs** .

6. **(Optional)** Click **Synchronize** to ensure that all programs are distributed to their assigned delivery nodes. Only perform this step if programs have indicated failure or pending for some time.

   When you click **Synchronize**, Scopia® SR attempts to complete any failed or pending distributions for a given DN. You can check the progress of the synchronization by checking the DN program listing on the Delivery Node screen. This feature is useful when adding a new DN, or moving an existing DN within a DN hierarchy. The programs are not updated until you click **Synchronize** . You may also want to click **Synchronize** if a delivery node has been offline for some time and needs to synchronize programs that have occurred during this time.

Related links

Installing a new DN if have only one DN and you have fixed the hard drive or replaced the appliance on page 165

Managing distribution groups

Distribution groups are groups of delivery nodes. Avaya recommends creating groups of delivery nodes for the purposes of redundancy, scalability, and load-balancing.

Distribution groups:

- Enable redundancy if individual delivery nodes are not responding.
- Can be mapped to a conference point.

Related links

Creating distribution groups on page 107
Deleting distribution groups on page 107
Merging distribution groups on page 108
Mapping viewers to devices or distribution groups on page 108

Creating distribution groups

Procedure

1. Log in to Scopia® SR.
2. Click the **Devices** tab.
3. Click **Distribution Groups** on the **Browse** menu.
4. Click **Create New**.
5. Enter a name in the **Distribution Group** field.
6. Click **Add** to select delivery nodes for inclusion in this distribution group.
7. Select one or more delivery nodes from the list and click **Add Delivery Nodes**.

   The selection dialog continues to display to enable you to select additional delivery nodes. You can close the dialog but clicking the close icon in the top right corner.

   The delivery nodes display in the **Group Members** list.
8. Click **Save**.

Related links

Managing distribution groups on page 107

Deleting distribution groups

Procedure

1. Log in to Scopia® SR.
2. Click the **Devices** tab.

3. Click **Distribution Groups** on the **Browse** menu.
4. Select the check box next to the name of the distribution group.
5. Click **Delete**.

Related links

Managing distribution groups on page 107

Merging distribution groups

Procedure

1. Log in to Scopia® SR.
2. Click the **Devices** tab.
3. Click **Distribution Groups** on the **Browse** menu.
4. Select the check boxes next to the name of the distribution groups that you want to merge.
5. Click **Merge**.

   The **Merge Distribution Groups** dialog is displayed.
6. Enter a new name for the distribution group in the **Group Name** field.

Related links

Managing distribution groups on page 107

Mapping viewers to devices or distribution groups

One of the key benefits of distribution groups is that they enable redundancy. The delivery nodes in the group share the load of serving content to the mapped users.

A virtual delivery node (VDN) serves content through a content delivery network (CDN).

The redundancy logic operates according to the following rules:

- VDN/CDN failure: To route a viewer to the CDN, you should specify the VDN as the primary device. If a program is not successfully published to the CDN, viewer mapping enables you to specify a secondary delivery node fallback. This allows for local delivery node routing for distributed delivery node systems. If the fallback delivery node fails as well, users see a **Resource Unavailable** message when they try to view the program.
- Delivery node failure: If a program is not successfully published to the primary delivery node or if the primary delivery node is offline, users see a **Resource Unavailable** message when they try to view the program. Viewer mapping enables you to specify a secondary delivery node fallback which the system uses if the primary delivery node is offline. If the fallback delivery node fails as well, users see a **Resource Unavailable** message when they try to view the program.

- Source delivery node failure: If a source delivery node fails, you can specify a secondary source delivery node. However, fallback only occurs if the program has not yet been distributed to the primary delivery node or distribution group and if there is no viewing mapping for the IP address of the viewer.

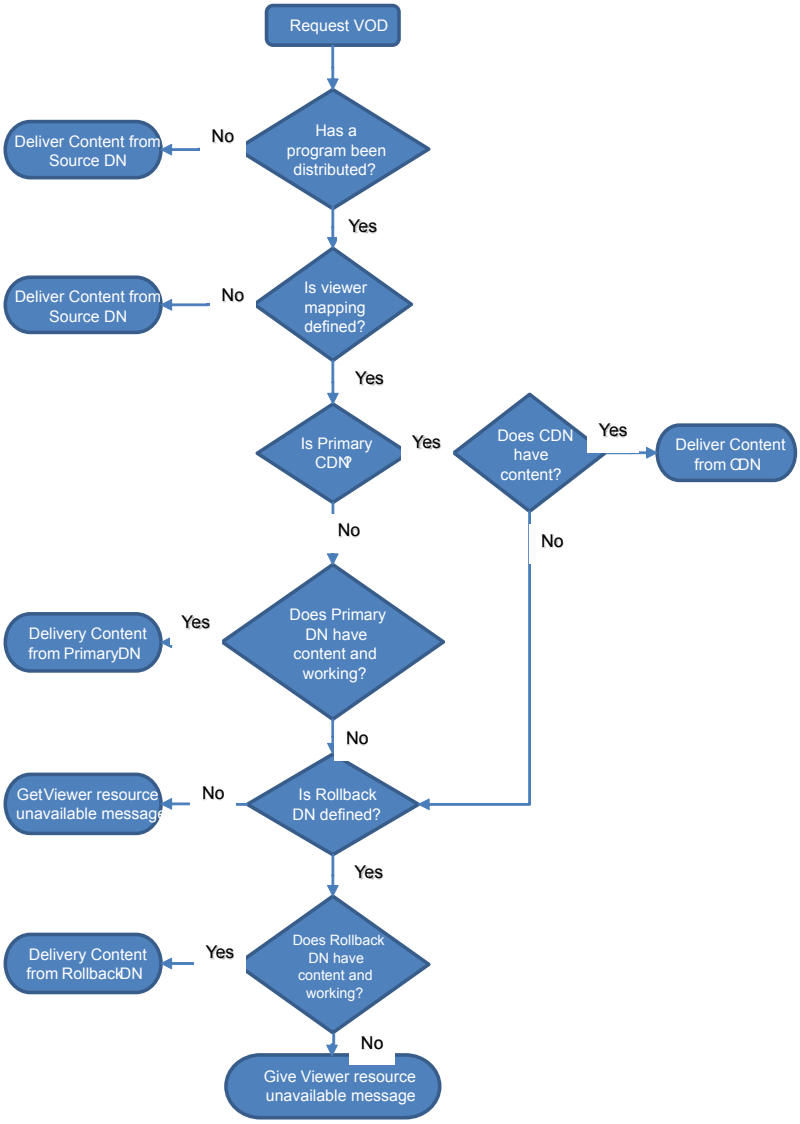


Figure 38: Viewer Mapping Flow Diagram

When creating or editing a viewer mapping, you can select to restrict an IP address or range from accessing the system at all. If you select the **Restricted Mapping DN (0.0.0.0)** for the primary device, users/viewers see a error message and are denied access when they attempt to view the program.

About this task

Use this task to map viewers to delivery nodes, virtual delivery nodes, or distribution groups.

Procedure

1. Log in to Scopia® SR.
2. Click the **Global Policies** tab.
3. Click **Viewer Mappings** on the **Policies** menu.
4. Click **Create New**.

   The **Create Viewer Mapping** dialog is displayed.
5. Configure the settings, as described in Table 21: Viewer Mapping on page 110.

Table 21: Viewer Mapping

Field Name	Description
Select either: • Primary Device • Primary Distribution Group	Primary Device is the primary method of delivery. Select the delivery node or VDN from the drop-down list. Alternatively, you can select the distribution group from the drop-down list. When you are creating or editing a viewer mapping, you can select to restrict an IP address or range from accessing the system at all. If you select as the **Primary Device** the Restricted Mapping DN (0.0.0.0), the viewer gets an error and is denied access.
Select either: • Secondary Device • Secondary Distribution Group	Secondary device is the secondary method of delivery. Scopia® SR uses this method of delivery if the primary method of delivery fails or does not contain the content. Select the delivery node from the drop-down list. Alternatively, you can select the distribution group from the drop-down list.
Multicast Enabled	Select the **Multicast Enabled** checkbox if multicast is enabled on the network You should only enable this setting if the subnet specified in the **Subnet Mask** is multicast-enabled and you intend to allow multicast broadcasts.
Host	Enter the IP address of the viewer system to associate with the device or distribution group.
Subnet Mask	Enter a subnet mask to indicate the range of IP addresses you want to match with the device. For more information, see Table 22: Subnet Mask Guidelines on page 111.

Table 22: Subnet Mask Guidelines

Use this Subnet Mask	To match
255.255.255.255	The IP address you entered. In this case, assign one viewer system to the delivery node.
255.255.255.0	The first three octets of the IP address. The range for the fourth octet is 0 to 255. For example, if the host IP address is 10.10.1.0, and you enter 255.255.255.0 in the **Subnet Mask** field, viewer systems from 10.10.1.0 to 10.10.1.255 are assigned to the delivery node.
Number similar to 255.255.255.128	The first three octets of the IP address. The range for the fourth octet is 128 to 255. For example, if the host IP address is 10.10.1.0, and you enter 255.255.255.128 in the **Subnet Mask** field, viewer systems from 10.10.1.129 to 10.10.1.255 are assigned to the delivery node.

Note:

Do not specify a subnet mask that masks actual IP address bits. For example, if you specify a subnet mask of 255.255.0.0, you must specify an IP address that includes only 0 in the last two octets. If you specify a specific system IP address such as 192.168.24.7, you must use a subnet mask of 255.255.255.255.

6. Click **Save**.

Example

Table 23: Examples of valid IP address/subnet pairs

IP Address	Subnet Mask	Range
192.168.192.0	255.255.192.0	192.168.192.0 to 192.168.255.255
192.168.191.0	255.255.255.0	192.168.191.0 to 192.168.191.255
192.168.192.2	255.255.255.254	192.168.192.2 to 192.168.192.3
192.168.193.0	255.255.255.255	192.168.193.0

Table 24: Examples of invalid IP address/subnet pairs

IP Address	Subnet Mask	Reason
192.168.192.0	255.255.0.0	The third octet of the address is set, but it is 0 in the subnet mask.
192.168.0.2	255.255.255.0	The fourth octet of the address is set, but it is 0 in the subnet mask.
192.168.193.0	0.0.0.255	The mask is probably inverted and should be 255.255.255.0

Related links

Managing distribution groups on page 107
Editing viewer mappings on page 112
Deleting viewer mappings on page 112

Editing viewer mappings

About this task

When you are creating or editing a viewer mapping, you can select to restrict an IP address or range from accessing the system at all. If you select as the **Primary Device** the Restricted Mapping DN (0.0.0.0), the viewer gets an error and is denied access.

Procedure

1. Log in to Scopia® SR.
2. Click the **Global Policies** tab.
3. Click **Viewer Mappings** on the **Policies** menu.
4. Select the check box next to the name of the viewer mapping that you want to edit.

   The **Edit Viewer Mapping** dialog is displayed.
5. Edit the viewer mapping.
6. Click **Save**.

Related links

Mapping viewers to devices or distribution groups on page 108

Deleting viewer mappings

Procedure

1. Log in to Scopia® SR.
2. Click the **Global Policies** tab.
3. Click **Viewer Mappings** on the **Policies** menu.
4. Select the check box next to the name of the viewer mapping that you want to delete.
5. Click **Delete**.

Related links

Mapping viewers to devices or distribution groups on page 108

Configuring video formats

About this task

Scopia® SR supports multiple file formats and viewer options. The delivery method is based on which of these file formats and viewer options that you choose to use in the program. Scopia® SR publishes and plays with HTTP as a fallback protocol, which ensures that content is always viewable (unless the user cannot access the web site at all). The program viewer attempts to use the technology listed in the specified order.Use this task to specify the order of preferred formats.

Procedure

1. Log in to Scopia® SR.
2. Click the **Global Policies** tab.
3. Click **Program Options** on the **Policies** menu.
4. Select a Priority for each supported format.

Table 25: Guidelines for Selecting an Appropriate Format

Player	Supported Containers	Type	Protocol	Windows	Mac	iOS	Android
HTML5	mpeg2ts (H.264/AAC)	Live	HLS over HTTP/ HTTPS	✔ Edge only	✔ Safari only	✔	✔
	MP4 (H.264/ AAC)	VoD	HTTP/ HTTPS	✔ IE9+	✔	✔	✔
Flash	mpeg2ts (H.264/AAC)	Live	HLS over HTTP/ HTTPS	✔	✔		
	MP4 (H.264/ AAC)	VoD	HTTP/ HTTPS	✔	✔		
Silverlight	ASF Container (VC1) Unicast Protocols: RTSP/UDP, RTSP/TCP, HTTP Multicast: UDP	Live	MMS	✔	✔		

Table continues…

Player	Supported Containers	Type	Protocol	Windows	Mac	iOS	Android
	No CDN Support						
	MP4 (H.264/ AAC)	VoD	HTTP/ HTTPS	✔	✔		
Windows Media Player	ASF Container (VC1) Unicast Protocols: RTSP/UDP, RTSP/TCP, HTTP Multicast: UDP No CDN Support	Live	MMS	✔ IE/FF			
	MP4 (H.264/ AAC)	VoD	HTTP/ HTTPS	✔ IE/FF			

Note:

You must separately configure formats on the Scopia® Management Administration GUI.

For more information, see the *Avaya Scopia® Management Administrator Guide*, which is available on https://support.avaya.com/.

5. Click **Save**.

Chapter 13: Managing your content delivery network

About content delivery networks

Scopia® SR enables you to publish content to the cloud, using a virtual delivery node (VDN) and a content delivery network (CDN). The VDN and the network of the CDN act as one delivery mechanism. When a user creates a recording (program), they can choose to distribute it to the CDN, as well as to the regular delivery node (DN).

Current limitations

- Scopia® SR currently only supports the HighWinds™ CDN.
- If you edit a program title, the change is not reflected on the VDN.
- A space in title names is replaced with an underscore.
- Programs downloaded from the CDN do not have a user-friendly name. Instead, they have a globally unique identifier (GUID).

Prerequisites

- A HighWinds™ StrikeTracker 3 account (username and password).
- A HighWinds™ Cloud Storage account (FTP username and password).
- A single VDN is installed as part of the Scopia® SR solution.

In a multi-tenant environment, each tenant could have a different CDN configuration.

Related links

Example of a cloud deployment on page 19

Distributing recordings to the content delivery network

A user cannot distribute existing recordings to the CDN. A user can only distribute new recordings to the CDN.

About this task

To enable a user to distribute their recordings to the CDN, you assign them to a profile that includes this function. You can create a profile, enable CDN distribution in that profile, and then assign users

to the profile. Scopia® SR will distribute each of the user's new recordings to the CDN, using the VDN.

Related links

Creating recording profiles in the Scopia SR interface on page 64

Chapter 14: Securing your system

Enabling secure and encrypted authentication

You can set up the Scopia® SR Manager to use secure and encrypted authentication and web access. By default, communication between the servers is encrypted for security but the actual media is not encrypted.

The Scopia® SR Manager uses SSL keys with up to 2048-bit encryption and certificates. The Scopia® SR Manager includes default pre-installed Avaya certificates that are not unique and associated with your fully qualified domain. If you enable the default certificates, the user sees browser security warnings. To avoid these browser warnings, install your own signed certificate on the Scopia® SR Manager and associate it with your Fully Qualified Domain Name (FQDN).

Procedure

1. Log in to Scopia® SR.
2. Click the **Global Policies** tab.
3. Click **Security** on the **Policies** menu.
4. Configure the settings, as described in Table 26: Security Options on page 117.

Table 26: Security Options

Field Name	Description
Stream/Resource authentication token expiration (minutes)	Enter the length of time for which a generated security token is valid. Do not set this to less than 10 minutes to ensure that it will have time to be used before timing out.
Secure Media Delivery	Select this check box to ensure that users receive HTTP Live Streaming (HLS) and Video on Demand (VoD) media over a secure HTTPS connection. Microsoft™ Media Server (MMS) is disabled when this option is enabled. To use this feature you must have the proper certificates installed and have a valid license key.

Note:

You must separately enable HTTPS on the Scopia® Management Administration GUI.

For more information, see the *Avaya Scopia® Management Administrator Guide*, which is available on https://support.avaya.com/.

5. Click **Save**.

Related links

Adding and Modifying Scopia® Streaming and Recording servers in Scopia® Management on page 51

Securing your Scopia® SR public interfaces

Scopia® SR has three public interfaces:

- The Scopia® SR Manager portal interface used to view the portal pages from Scopia® Desktop.
- The delivery node interface used for media playback.
- The virtual delivery node (VDN) interface used by the content delivery network (CDN) to fetch media for playback.

There are another two interfaces that are not accessed by users:

- The transcoder, which communicates with the Scopia® SR Manager, the conference point, and other delivery node.
- The conference point, which communicates with the Scopia® SR Manager and the transcoder.

You can enable settings in Scopia® SR Manager and Scopia® Management to secure the media, as well as the user portal pages.

For more information, see the *Avaya Scopia® Management Administrator Guide*, which is available on https://support.avaya.com/.

Related links

Configuring external addresses for public interfaces on page 118

Configuring external addresses for public interfaces

About this task

To secure the Scopia® SR public interfaces, proper certificates have to be generated. The certificates have to match the fully qualified domain name (FQDN) or the IP address of the machine. Avaya recommends setting the use of FQDNs.

When you configure your system to use FQDNs, they need to be used to register every device with the Scopia® SR Manager.

You must also configure Scopia® SR to use external addresses, using the FQDN, and not the IP address.

Procedure

1. Configure the external address of the delivery node.
   a. Type `https://<DN FQDN/IP Address>` in a web browser.
   b. Log in using the following credentials:
      - Username: `administrator`
      - Password: `administrator`
   c. Click the **Network** tab.
   d. Enter the external address in the **External Address (optional)** field in the **Global Network Configuration** section.
   e. Click **Submit**.
2. Configure the external address for the conference point.
   a. Type `https://<CP FQDN/IP Address>` in a web browser.
   b. Log in using the following credentials:
      - Username: `administrator`
      - Password: `administrator`
   c. Navigate to **System Configuration** > **Network Configuration**.
   d. Enter the external address in the **External Address (optional)** field in the **Global Network Configuration** section.

      You can now optionally enter a DNS name or specific external or internal IP address that you want to use when communicating with the Scopia® SR Manager. This functionality enables you to enter externally statically mapped IP addresses and so on. If you leave this field empty then Scopia® SR automatically uses the IP addresses assigned to the operating system statically or from DHCP. This address is passed to the Scopia® SR Manager when the device registers and is used by the Scopia® SR Manager to access the device. The Scopia® SR Web GUI reports the IP address and other network information and on some of the Scopia® SR devices, you can set the IP address and other key network settings. This functionality is especially helpful for the systems that are virtualized to ensure the proper network device IP address set. The CP and DN show up as one “eth0” virtualized NIC to the host windows machine taking advantage of the bonded NICS of the host.
   e. Click **Finish**.
3. Configure the external address for the transcoder.
   a. Type `https://<CP FQDN/IP Address>` in a web browser.
   b. Log in using the following credentials:
      - Username: `administrator`
      - Password: `administrator`

c. Navigate to **System Configuration** > **Transcoder Configuration**.

d. Enter the external address in the **Transcoder Address** field.

e. Click **Finish**.

Note:

If you are using IP addresses, the certificates have to be generated for the IP address. The IP address has to be included on both the **Common Name** field and the **Subject Alternative Name** field when generating the certificates. If the IP address is not included in the **Subject Alternative Name** field, certain devices, such as Mac computers or Android mobile devices may not operate correctly.

Related links

Securing your Scopia SR public interfaces on page 118

Securing your system using third party certificates

To secure Scopia® SR using third party certificates, you must have certificates and the corresponding private key for the different interfaces:

- Scopia® SR Manager FQDN or IP: The same certificate and the corresponding private key can be used for the transcoder if they reside on the same Windows™ operating system.
- Delivery node: If there are multiple delivery nodes or virtual delivery nodes (VDNs), you must have certificates and the corresponding private key for each one.
- Conference point

Note:

When generating your Certificate Signing Request (CSR) in order to obtain your certificate, do not use a pass phrase for your private key. Scopia® SR does not support private keys with a pass phrase.

Related links

Configuring Scopia SR Manager on page 120
Configuring conference points and delivery nodes on page 122
Configuring the transcoder on page 123
Generating signing requests on page 124

Configuring Scopia® SR Manager

About this task

To secure the Scopia® SR Manager web pages, you should create the externally generated certificates for the IP or FQDN.

Procedure

1. On the Scopia® SR Manager server, stop the **Apache Tomcat 7.0 Tomcat7** service.
2. Replace the files in Table 27: Certificates Required on page 121 with newly generated certificates.

   Table 27: Certificates Required

File	Description
C:\Program Files\Apache Software Foundation \Tomcat 7.0\conf\ssl.crt\server.crt	The Manager certificate that is signed by your authority.
C:\Program Files\Apache Software Foundation \Tomcat 7.0\conf\ssl.crt\ca.crt	The root certificate authority (CA) that is used to sign the certificate.
C:\Program Files\Apache Software Foundation \Tomcat 7.0\conf\ssl.key\server.key	The key generated when creating the certificate signing request (CSR). If the CSR is generated on this machine, this file does not need to be replaced.

3. Run the following script, which adds the certificates to the keystore:

   ```
   python C:\Program Files\Apache Software Foundation\Tomcat 7.0\conf\import_cert.py
   ```

4. Restart the Apache Tomcat 7.0 Tomcat7 service.
5. **(Optional)** If the certificates generated are self-signed, or if they are signed by a CA that is not well-known, you should also install the ca.crt certificate in the clients.

   This certificate is accessible via http://<Scopia® SR Manager server>/ca.crt
6. **(Optional)** If the certificates are going to be signed by an external authority and you wish to generate the signing requests from the Manager itself, you must perform these additional steps:
   a. Log in to the Scopia® SR Manager server, using SSH.
   b. Remove the `server.crt` if exists, by deleting: `C:\Program Files\Apache Software Foundation\Tomcat 7.0\conf\ssl.crt\server.crt`
   c. Run the following script that will generate the certificate signing request:

      ```
      python "C:\ Program Files\Apache Software Foundation\Tomcat 7.0\conf
      \new_cert.py" hostname.domainName
      ```

   d. Locate the signing request in the following folder: `C:\Program Files\Apache Software Foundation\Tomcat 7.0\conf\ssl.csr\server.csr`

      In this case, the private key will be in the proper folder and does not need to be replaced with any other key.
   e. Send the CSR to the certificate authority.

Related links

Securing your system using third party certificates on page 120

Configuring conference points and delivery nodes

About this task

You must install valid certificates on the conference points and delivery nodes. If you do not install them, HTTP requests will fail and the media does not play.

You should provide a valid certificates for the server. The certificate should have the correct domain name or the IP address of the machine. If you change the FQDN or IP, you must re-issue the certificates. However, if you perform an upgrade, the existing certificates are still valid.

Procedure

1. Replace the files in Table 28: Certificates Required on page 122 with newly generated certificates.

   Table 28: Certificates Required

File	Description
/opt/www/conf/ssl.crt/server.crt	The valid certificate that is signed by your authority.
/opt/www/conf/ssl.crt/ca.crt	The root certificate authority (CA) that is used to sign the certificate. This file contains the concatenated list of encoded CAs that form the chain for the server certificate.
/opt/www/conf/ssl.key/server.key	This is the private key associated with the above certificate. If the CSR is generated on this machine, this file does not need to be replaced.

2. Restart the httpd service after copying the certificates by running the following command.

   ```
   service httpd restart
   ```

3. **(Optional)** If the certificates generated are self-signed, or if they are signed by a CA that is not well-known, you should also install the ca.crt certificate in the clients.

4. **(Optional)** If the certificates are going to be signed by an external authority and you wish to generate the signing requests from the conference point or delivery node itself, you must perform these additional steps:

   a. Log in to the conference point or delivery node, using SSH.

   b. Run the following script that will generate the certificate signing request:

      ```
      /opt/stream/bin/new_cert.sh
      ```

   c. Locate the signing request in the following folder: `/opt/www/conf/ssl.csr/server.csr`

      In this case, the private key will in the proper folder and does not need to be replaced with any other key.

   d. Send the CSR to the certificate authority.

Related links

Securing your system using third party certificates on page 120

Configuring the transcoder

About this task

The transcoder also requires valid certificates to work.

You should provide valid certificates for the server. The certificate should have the correct domain name or the IP address of the machine.

The transcoder is co-resident with the Scopia® SR Manager. This means that the certificates and key should be the same, since they share the same domain name. Consequently, use the same certificates that were used with the Manager. Just copy them to a different location.

Procedure

1. Replace the files in Table 29: Certificates Required on page 123 with newly generated certificates.

   Table 29: Certificates Required

File	Description
C:\Program Files (x86)\Apache Software Foundation\Apache2.2\conf\ssl.crt\server.crt	The Manager certificate that is signed by your authority.
C:\Program Files (x86)\Apache Software Foundation\Apache2.2\conf\ssl.crt\ca.crt	The root certificate authority (CA) that is used to sign the certificate.
C:\Program Files (x86)\Apache Software Foundation\Apache2.2\conf\ssl.key\server.key	The key generated when creating the certificate signing request (CSR). If the CSR is generated on this machine, this file does not need to be replaced.

2. Restart the Apache2.2 service.
3. **(Optional)** If the certificates are going to be signed by an external authority and you wish to generate the signing requests from the Manager itself, you must perform these additional steps:
   a. Log in to the Scopia® SR Manager/Transcoder server, using SSH.
   b. Remove the `server.crt` if exists, by deleting: `C:\Program Files (x86)\Apache Software Foundation\Apache2.2\conf\ssl.crt\server.crt`.
   c. Run the following script that will generate the certificate signing request:

      ```
      python "C:\ Program Files (x86)\Apache Software Foundation\Apache2.2\conf
      \new_cert.py" hostname.domainName
      ```

   d. Locate the signing request in the following folder: `C:\Program Files (x86)\Apache Software Foundation\Apache2.2\conf\ssl.csr\server.csr`

In this case, the private key will in the proper folder and does not need to be replaced with any other key.

e. Send the CSR to the certificate authority.

Related links

Securing your system using third party certificates on page 120

Generating signing requests

About this task

At any time, you can generate certificate signing requests for the current machine or for any other FQDN/IP by running the `/opt/stream/bin/new_cert.sh` script

Procedure

- If you are generating a certificate signing request for the machine where the script is being run, just execute the script.

  The signing request is in the `/opt/www/conf/ssl.csr/server.csr` file.

  The private key is in the `/opt/www/conf/ssl.key/server.key` file.

- Alternatively, you can pass the IP address or the FQDN as a parameter to the script. For example `new_cert.sh 135.64.29.235`.

Related links

Securing your system using third party certificates on page 120

Installing the certificate authority on the devices

Installing the root certificate on Windows

For security to work properly, your browser and mobile devices must have the root certificate installed. If your certificates are signed by a well-known certificate authority (CA), such as Verisign or Thawte, your devices already have this certificate installed, and there is no need to install any additional root certificate. If you are testing your system using Avaya demonstration certificates, or any other self-signed CA, you must install that certificate on your devices.

About this task

These instructions describe how to install the root certificate for Windows devices with Microsoft™ Windows Explorer or Google™ Chrome. There are separate instructions for Mozilla™ Firefox.

Procedure

1. Start Microsoft Management Console (MMC).
   a. Click **Start** > **Run**.
   b. Type `MMC`.

c. Click **OK**.

2. On the Microsoft Management Console, navigate to **File** > **Add/Remove Snap-In**.
3. Add a certificate.
   a. Select **Certificates** in the left panel and click **Add** to move it to the right panel.
   b. Click **OK**.
4. On the **Certificates snap-in** dialog, select **Computer account** and click **Next**.
5. On the **Select Computer** dialog, click **Finish**.
6. Click **OK**.
7. Import the trusted root certificate.
   a. On the Microsoft Management Console, expand the **Certificates** node.
   b. Right-click **Trusted Root Certificates** and select **All Tasks** > **Import**.

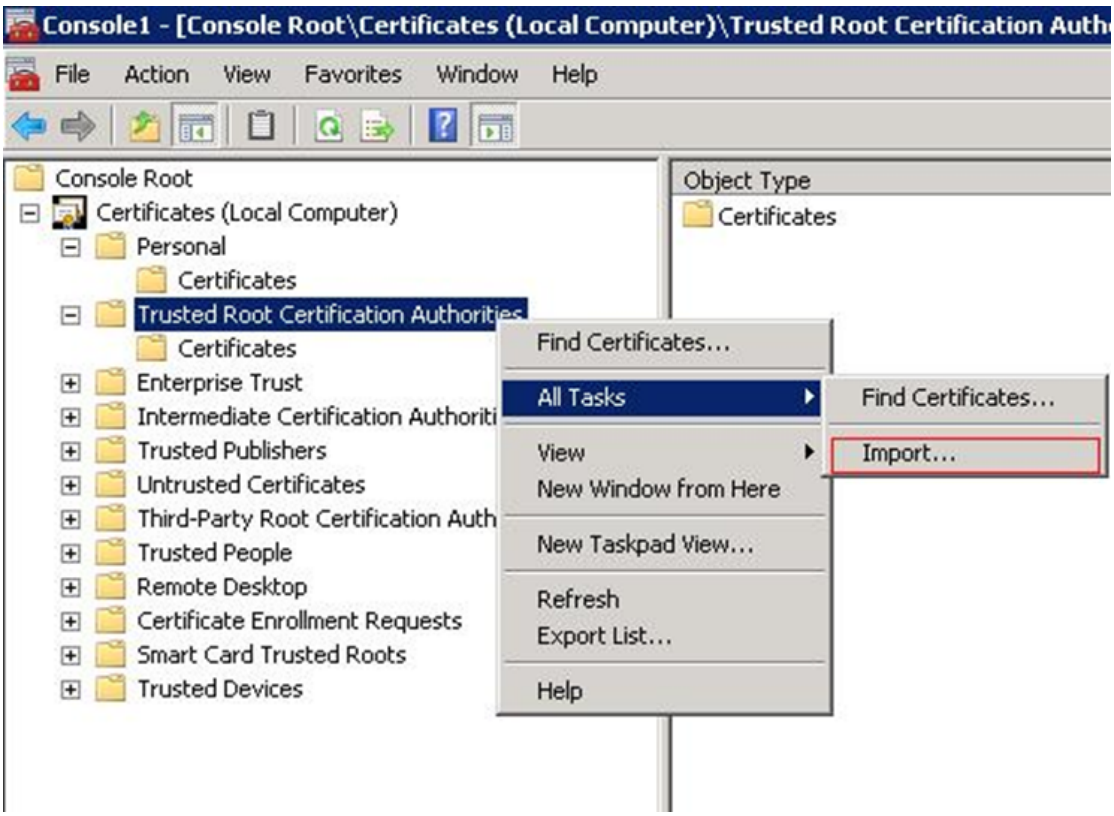


Figure 39: Trusted Root Certification Authorities

c. Click **Next** to start the **Certificate Import Wizard**.
d. Click **Browse** to select the correct certificate file and click **Next**.
e. Accept the default selection and click **Next**.

Figure 40: Certificate Store

f. Click **Finish**.

g. Click **OK**.

Related links

Securing your system using third party certificates on page 120

Adding and Modifying Scopia® Streaming and Recording servers in Scopia® Management on page 51

Installing the root certificate on Mac

For security to work properly, your browser and mobile devices must have the root certificate installed. If your certificates are signed by a well-known certificate authority (CA), such as Verisign or Thawte, your devices already have this certificate installed, and there is no need to install any additional root certificate. If you are testing your system using Avaya demonstration certificates, or any other self-signed CA, you must install that certificate on your devices.

Procedure

1. Start the Keychain Access program by double-clicking the certificate file.

   The **Add Certificates** dialog is displayed.

2. Select the **System** keychain from the drop-down menu.
3. Enter your administrator password.
4. On the next dialog, select the trust settings for this certificate.
    a. Expand the **Trust** section.
    b. Select **Always Trust** for both **X.509 Basic Policy** and the **When using this certificate** drop-down menu.
    c. Click the **Always Trust** button.
5. Enter your administrator password.

Related links

Securing your system using third party certificates on page 120
Adding and Modifying Scopia® Streaming and Recording servers in Scopia® Management on page 51

Installing the root certificate authority on Android

For security to work properly, your browser and mobile devices must have the root certificate installed. If your certificates are signed by a well-known certificate authority (CA), such as Verisign or Thawte, your devices already have this certificate installed, and there is no need to install any additional root certificate. If you are testing your system using Avaya demonstration certificates, or any other self-signed CA, you must install that certificate on your devices.

Before you begin

Email the certificate to your mobile device. Alternatively, download the certificate to your mobile device.

Procedure

1. Locate the certificate authority and make a note of where it is stored.

    It may be in the **Download** folder on your device.
2. Navigate to **Settings** > **Security**.
3. Tap **Install from phone storage** to find the certificate authority that you have just downloaded.

    For example, if it is in the **Download** folder on your device, on the **Open From** screen, navigate to **Internal storage** > **Download** and select the `.pfx` file.

Next steps

Now you can set the certificate name and use. The use is VPN and apps.

Related links

Securing your system using third party certificates on page 120
Adding and Modifying Scopia® Streaming and Recording servers in Scopia® Management on page 51

Installing the root certificate on iOS

For security to work properly, your browser and mobile devices must have the root certificate installed. If your certificates are signed by a well-known certificate authority (CA), such as Verisign or Thawte, your devices already have this certificate installed, and there is no need to install any additional root certificate. If you are testing your system using Avaya demonstration certificates, or any other self-signed CA, you must install that certificate on your devices.

Before you begin

Email the certificate to your mobile device. Alternatively, download the certificate to your mobile device.

Procedure

1. Tap the certificate authority (CA).
2. On the **Install Profile** screen, tap **Install**.

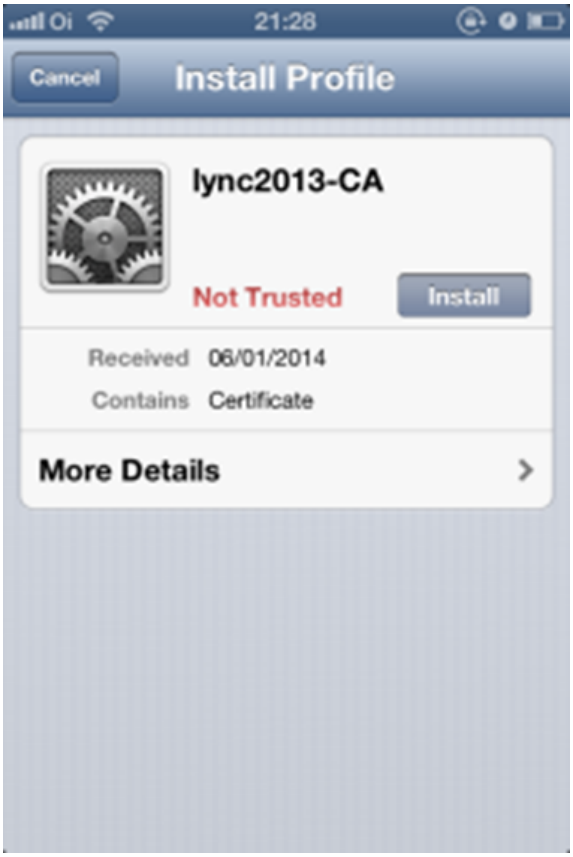


Figure 41: Install Profile

The device displays a warning screen.

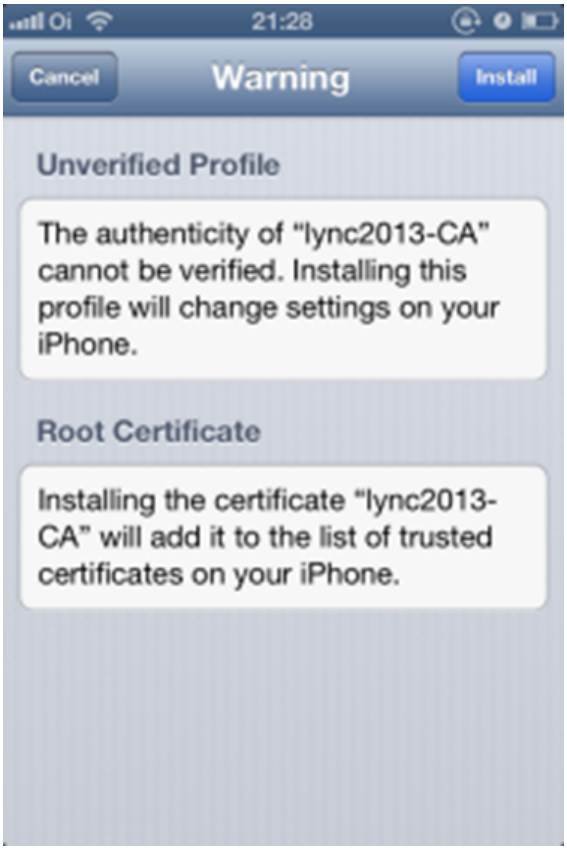


Figure 42: Warning

3. On the **Warning** screen, tap **Install**.

   The private root certificate authority is now trusted.

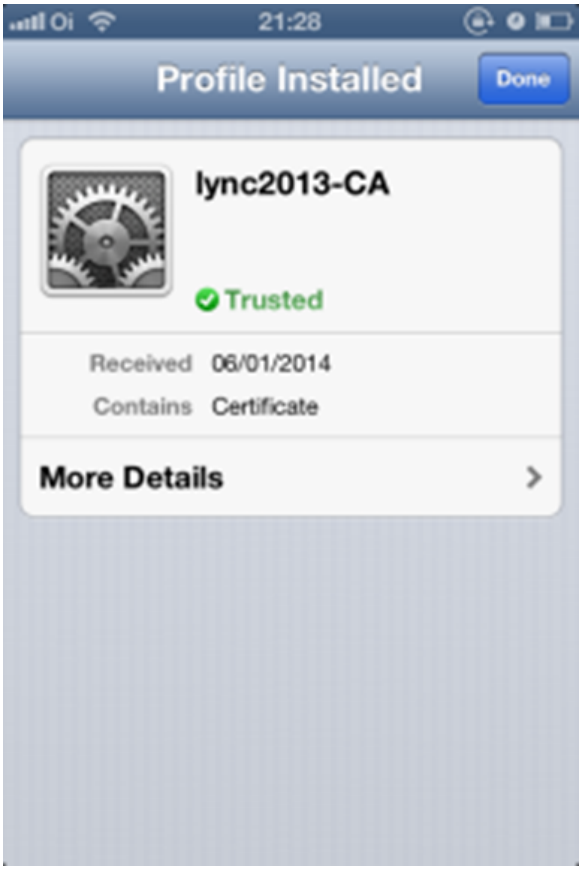


Figure 43: Profile Installed

Related links

Securing your system using third party certificates on page 120
Adding and Modifying Scopia® Streaming and Recording servers in Scopia® Management on page 51

Installing the root certificate for Mozilla™ Firefox

For security to work properly, your browser and mobile devices must have the root certificate installed. If your certificates are signed by a well-known certificate authority (CA), such as Verisign or Thawte, your devices already have this certificate installed, and there is no need to install any additional root certificate. If you are testing your system using Avaya demonstration certificates, or any other self-signed CA, you must install that certificate on your devices.

Before you begin

Save the certificate to your device.

Procedure

1. Locate the certificate.

If you have saved the certificate to the hard disk, navigate to **Tools** > **Options**. On the **Options** screen, select **Advanced** and click **Encryption** to view the **Encryption** tab. On the **Encryption** tab, click **View Certificates**.

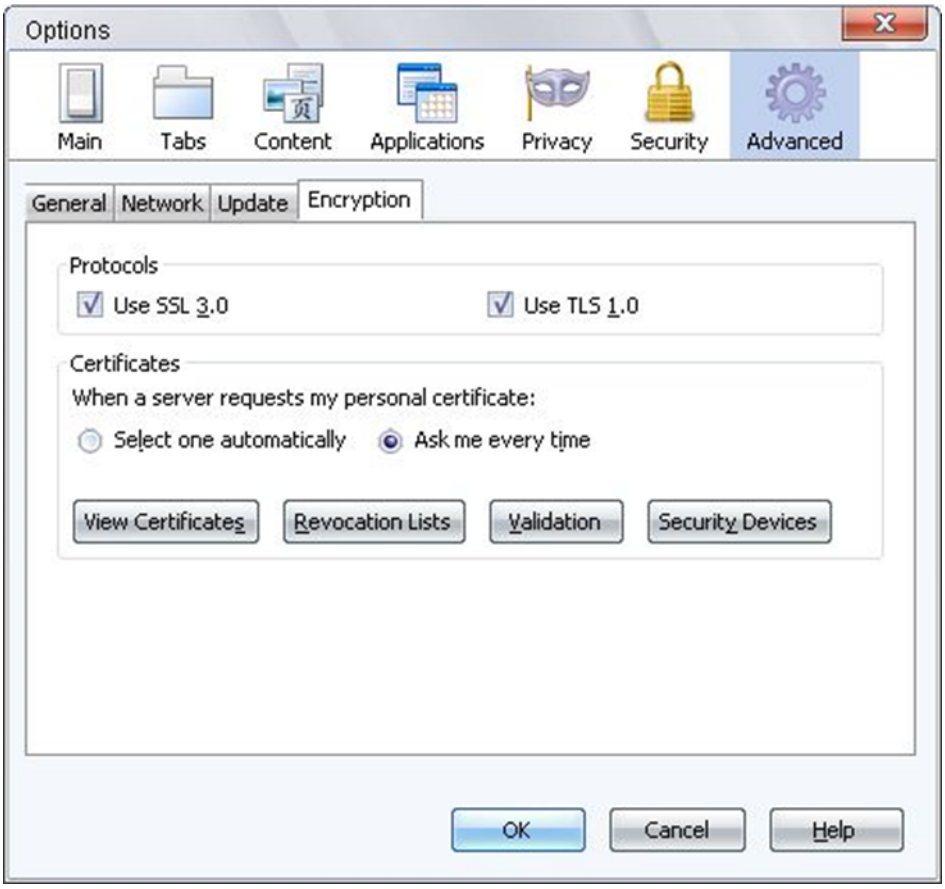


Figure 44: Options

2. On the **Certificate Manager** dialog, click the **Authorities** tab.
3. Click **Import**.
4. Browse to locate the certificate and click **Open**.
5. On the **Downloading Certificate** dialog, select the following checkboxes:
   - Trust this CA to identify web sites.
   - Trust this CA to identify email users.
   - Trust this CA to identify software developers.

Figure 45: Downloading Certificate

6. Click **OK**.

Next steps

You can now verify the certificate. On the **Certificate Manager** dialog, click the **Authorities** tab and scroll down to the bottom of the list of certificates. You should be able to see your certificate on this list. You can click **View** to verify that it is valid and that the validity period ends on 03/10/2035.

Related links

Securing your system using third party certificates on page 120
Adding and Modifying Scopia® Streaming and Recording servers in Scopia® Management on page 51

Securing your system using Avaya demonstration certificates

Each new installation of Scopia® SR automatically includes Avaya demonstration certificates. These certificates are self-signed. If the certificates generated are self-signed, or if they are signed by a CA that is not well-known, you should also install the ca.crt certificate in the clients.

Related links

Configuring Scopia SR Manager on page 133
Configuring conference points and delivery nodes for a new installation on page 133
Configuring conference points and delivery nodes for an upgrade on page 134
Configuring the transcoder for a new installation on page 134
Configuring the transcoder for an upgrade on page 134

Configuring Scopia® SR Manager

Before you begin

You should install or upgrade Scopia® SR and you should configure proper IP addresses or FQDNs. You should also enable media HTTPS security.

Procedure

1. On the Scopia® SR Manager server, stop the Apache Tomcat 7.0 Tomcat7 service.
2. Delete this file: `C:\Program Files\Apache Software Foundation\Tomcat 7.0\conf\ssl.crt\server.crt`.
3. Run the following script that will generate the certificates automatically:

```
CD "C:\Program Files\Apache Software Foundation\Tomcat 7.0\conf"
C:\python27\python.exe new_cert.py <IP or hostname>
```

4. Restart the Apache Tomcat 7.0 Tomcat7 service.

Example

```
C:\python27\python.exe new_cert.py 10.139.55.168
```

```
C:\python27\python.exe new_cert.py your.server.com
```

Related links

Securing your system using Avaya demonstration certificates on page 132

Configuring conference points and delivery nodes for a new installation

About this task

In a new installation, if you configure the IP or FQDNs before you run Scopia® SR, the certificates are generated automatically and there is no need for any extra steps.

Ensure the following:

- If the devices have an FQDN that is resolvable by way of a DNS, use this FQDN to register the device with the Scopia® SR Manager
- If the devices use an IP address, there should be no FQDN configured for the device. In other words, the localhost is the domain name.

Related links

Securing your system using Avaya demonstration certificates on page 132

Configuring conference points and delivery nodes for an upgrade

About this task

If the system is an upgrade and it did not have HTTPS working successfully in previous versions, you must perform these steps.

You must also ensure that:

If the devices have an FQDN that is resolvable by way of a DNS, use this FQDN to register the device with the Scopia® SR Manager

Procedure

1. Overwrite the ca.crt and ca.eky files:

```
cp -f /opt/www/conf/ssl.crt/ca.crt.rpmnew  /opt/www/conf/ssl.crt/ca.crt
cp -f /opt/www/conf/ssl.key/ca.key.rpmnew  /opt/www/conf/ssl.key/ca.key
```

2. Run this script to manually generate the demonstration certificates:

```
/opt/stream/bin/new_cert.sh
```

3. Restart the httpd service after copying the certificates by running the following command.

```
service httpd restart
```

4. **(Optional)** If the certificates generated are self-signed, or if they are signed by a CA that is not well-known, you should also install the ca.crt certificate in the clients.

Related links

Securing your system using Avaya demonstration certificates on page 132

Configuring the transcoder for a new installation

Procedure

1. Log in to the Scopia® SR Manager/Transcoder server, using SSH.
2. Run the following script:

```
python "C:\Program Files (x86)\BurstPoint Networks\Transcoder\new_cert.py"
```

Related links

Securing your system using Avaya demonstration certificates on page 132

Configuring the transcoder for an upgrade

Procedure

1. Delete the following files:
   - C:\Program Files (x86)\Apache Software Foundation\Apache2.2\conf\ssl.crt\server.crt
   - C:\Program Files (x86)\Apache Software Foundation\Apache2.2\conf\ssl.key\server.key

- C:\Program Files (x86)\Apache Software Foundation\Apache2.2\conf\ssl.csr\server.csr

2. Copy C:\Program Files (x86)\Apache Software Foundation\Apache2.2\conf\ssl.crt \ca_default.crt, onto ca.crt, as follows:

```
copy "C:\Program Files (x86)\Apache Software Foundation\Apache2.2\conf\ssl.crt
\ca_default.crt" "C:\Program Files (x86)\Apache Software Foundation\Apache2.2\conf
\ssl.crt\ca.crt"
```

3. Replace C:\Program Files (x86)\Apache Software Foundation\Apache2.2\conf\ssl.key \ca.key, with the one that is in the same folder called ca_default.key, as follows:

```
copy "C:\Program Files (x86)\Apache Software Foundation\Apache2.2\conf\ssl.key
\ca_default.key" "C:\Program Files (x86)\Apache Software Foundation\Apache2.2\conf
\ssl.key\ca.key"
```

4. Delete the files and run the following script:

```
python "C:\Program Files (x86)\BurstPoint Networks\Transcoder\new_cert.py"
```

5. At any time you can generate certificate signing requests (CSR) for the machine or for any other FQDN/IP by running the `/opt/stream/bin/new_cert.sh` script:

   - If you want to generate a CSR for the machine on which the script is being run, just execute the script. The CSR will be in the `/opt/www/conf/ssl.csr/server.csr` file and the private key will be in the `/opt/www/conf/ssl.key/server.key` file.
   - Alternatively, you can pass the IP address or the FQDN as a parameter to the script. For example `"new_cert.sh 135.64.29.235"`.

Related links

Securing your system using Avaya demonstration certificates on page 132

Chapter 15: Managing multiple tenants

Managing multiple tenants

A multi-tenant system is a system which serves multiple separate organizations. The database of organizations must be synchronized with Scopia® Management.

For more information, see the *Avaya Scopia® Management Administrator Guide*, which is available on https://support.avaya.com/.

The graphic user interface (GUI) of a multi-tenant system is slightly different than a single-tenant system. For example, there is a new tab for **Organizations**.

Configuring streaming and recording settings for all organizations

Procedure

1. Log in to Scopia® SR.
2. Click the **Organizations** tab.

   The list of all organizations is displayed. The default settings impact all organizations.
3. Click on **Default Settings**.
4. Configure the settings, as described in Table 30: Organization Settings on page 136.

Table 30: Organization Settings

Field Name	Description
Select the Profiles which will be available	Select all of the profiles which you want to be available to all organizations.
Default Profile	Select the default profile to use for an organization if you do not configure a specific profile.
Select the Categories which will be available	Select all categories which you want to be available to all organizations.

Table continues…

Field Name	Description
CDN Settings	Specify content delivery network (CDN) settings, which you want to be available to all organizations.
Reset Organization Settings	Select to reset all organization settings. If you select this checkbox, the system resets any custom changes that you have made to individual organizations.

5. Click **Save**.

Configuring streaming and recording settings for a single organization

Procedure

1. Log in to Scopia® SR.
2. Click the **Organizations** tab.

   The list of all organizations is displayed. The default settings impact all organizations.
3. Click an individual organization from the list of organizations.

   You can also use the **Search** feature to search for a specific organization.

   The **Edit Organization** screen is displayed.
4. Select the **Override Defaults** checkbox.
5. Configure the settings, as described in Table 30: Organization Settings on page 136.
6. Click **Save**.

Chapter 16: Managing alarms and logs

Receiving notifications about system events

About this task

Perform these steps to receive automated e-mail messages about system events, such as devices going offline.

Procedure

1. Log in to Scopia® SR.
2. Click the **Global Policies** tab.
3. Click **Email Settings** on the **Policies** menu.
4. Configure the settings, as described in Table 31: Email Settings on page 138.

Table 31: Email Settings

Field Name	Description
Email Alarms and Events to	Enter the e-mail address to which the Scopia® SR Manager sends system alerts. Typically, this is the e-mail account of the system administrator.
Email From Address	Enter the e-mail address from which the Scopia® SR Manager messages are sent. You may want to set this to the e-mail address that users reply to if they have a problem with an invitation.
Email Server	Enter the IP address or DNS name of the e-mail server that routes the e-mail messages.
Email User Account	Enter the user account with which the Scopia® SR Manager authenticates the e-mail server before it can send e-mail through that server.
Email User Password/Confirm Password	Enter and confirm the password for the user account specified in the **Email From Address** field.

5. Click **Save**.

Viewing user audit logs

The audit log enables you to inspect the “who, when and what was done” on Scopia® SR. You can track actions by users and by administrators. Each action has a date, time, success indicator, and details of the user responsible. Table 32: Audit Logs on page 139 shows the tracked actions.

Table 32: Audit Logs

Area tracked	Details
Login	Success or failure
Publisher actions	• Program creation, start, and deletion • Program editing • Program moderation - start/stop recording • Failures relating to AutoPublish
Administrator actions	• Device registration or un-registration • Delivery node synchronization • Delivery node replacement • Device upgrade

Procedure

1. Log in to Scopia® SR.
2. Click the **Reports** tab.
3. Click **Audit Log** on the **Reports** menu.

   Scopia® SR displays a link to the audit log.
4. Download the audit log.

   The audit log grows to 10 Mbytes before rolling over to a new log. Scopia® SR retains up to four previous logs. Only the most recent log is available through the GUI.
5. **(Optional)** If you want to view the older logs, you can access them on the Scopia® SR Manager, at:

   ```
   C:\Program Files\Apache Software Foundation\Tomcat 7.0\logs\audit.log.[1-4]
   ```

Viewing the number of times someone clicks the link to a recording

The Program Access report lists the number of times a site visitor clicks a content link for each program. You can enter the delivery node IP address to view the number of times that a delivery node accesses a particular program.

Procedure

1. Log in to Scopia® SR.
2. Click the **Reports** tab.
3. Click **Program Access** on the **Reports** menu.

   Scopia® SR displays the Program Access Report screen.
4. Select the dates to include in the report results.

   You can select:

   - **Last Week**
   - **Last Month**
   - **Last 3 Months**
   - A particular date range
5. Select from the list of filters, as described in Table 33: Polling Settings on page 140.

   Table 33: Polling Settings

Field Name	Description
Organization	The name of the organization to which the program's owner belongs. This field is only displayed in a multi-tenant environment.
Program Name	The name of the program.
Category	If the program is associated with a category, you can select a category.
User ID	The user's identifier.
User IP Address	The client's IP address.
DN Name	Delivery node name.
DN IP Address	Delivery node IP address.
User Agent	This is the type of browser. You can select from desktop or mobile.

6. Select the format of the report.

   You can select:

   - **HTML**: Report is displayed in the browser.
   - **CSV**: Report results are generated as a comma-separated values file that can be opened in a spreadsheet program such as Microsoft™ Excel.
7. Click **Run Report**.

Viewing the number of page views, media views, and megabytes streamed

The Summary Program Access report contains information for each recording including page and media views, and the number of megabytes streamed.

Procedure

1. Log in to Scopia® SR.
2. Click the **Reports** tab.
3. Click **Summary Access** on the **Reports** menu.

   Scopia® SR displays the Reports Summary Access screen.
4. Select the dates to include in the report results.

   You can select:

   - **Last Week**
   - **Last Month**
   - **Last 3 Months**
   - A particular date range
5. **(Optional)** Enter the name of a program to include in the report.

   If you do not specify a program, the report includes all programs. In multi-tenant deployments, you can also optionally select an organization.
6. Select the format of the report.

   You can select:

   - **HTML**: Report is displayed in the browser.
   - **CSV**: Report results are generated as a comma-separated values file that can be opened in a spreadsheet program such as Microsoft™ Excel.
7. Click **Run Report**.

Viewing detailed information about the content delivery network

The VDN Access report contains detailed information for all access related to the CDN. This report supplements the Summary Access Report.

Procedure

1. Log in to Scopia® SR.

2. Click the **Reports** tab.
3. Click **VDN Access** on the **Reports** menu.

   Scopia® SR displays a link to log in to the CDN.
4. Click the link.

   The Highwinds™ Strike Tracker website is displayed.
5. Log in to the Highwinds using the credentials that you received when you bought the Highwinds tool.

   These are your original Highwinds login details. They are not the credentials you used to register the device with Scopia® SR.

   A new portal page appears which has a number of different pages to view statistics, such as:

   - Overall disk and network usage
   - Top files and media downloaded
   - Top region access to media
   - A global topographic view with usage indicators

Chapter 17: Migrating recordings

Recordings

Avaya has introduced a new component, the Avaya Scopia® Streaming and Recording server (Scopia® SR). Scopia® SR is the Avaya next generation HD streaming and recording platform, bringing significant enhancements to the Avaya Scopia® solution for streaming and recording. The Avaya Scopia® Streaming and Recording server replaces the Avaya Scopia® Content Center Recording server (SCC) server.

If you choose to upgrade from the Avaya Scopia® Content Center Recording server to the Avaya Scopia® Streaming and Recording server, you can easily transfer all of your existing recordings to Scopia® SR using the Avaya Scopia® Streaming and Recording server Migration Utility.

Scopia® SR imports the SCC recordings as .mp4 files.

Scopia® SR also imports all of the information related to the recordings, including categories and meta data. Meta data refers to information associated with each recording, such as the recording description, the owner name, and the access level.

Categories are labels that SCC and Scopia® SR use to classify recordings. SCC supports multiple categories. For example, a recording can belong to the “Sales” category and the “Marketing” category. Scopia® SR supports a single category. For example, a recording can belong to the “Sales” category only. During the migration, if there are multiple categories associated with a recording, Scopia® SR assigns the first category in the list to the recording.

If a recording does not have an owner, it is publicly available on the Scopia® SR server. Only an administrator can edit it.

The process of transferring recordings from the SCC to the Scopia® SR consists of three stages:

- Installing prerequisites
- Migrating recordings
- Converting recordings

Migrating recordings

Before you begin

- Configure Scopia® Management with Scopia® SR so that Scopia® SR has access to the user database prior to the migration of the recordings.
- Ensure that the .NET 3.5 framework is installed on the SCC.

- Ensure that you have the FTP username and password. The default username and password are `assrftp` and `P@ssw0rd`. You can change the default by editing the user at **Administrative Tools** > **Computer Management** > **Local Users and Groups** > **Users**.

Note:

Avaya recommends limiting the size of the recordings that you are migrating to 600GB so that the Scopia® SR has room for new recordings.

Procedure

1. On the Scopia® SR, enable FTP.
   a. Double-click the **Start FTP** shortcut on the desktop.

      FTP is enabled and the FTP folder is `C:\inetpub\ftproot`.

   b. **(Optional)** Change the FTP password by navigating to **Administrative Tools** > **Computer Management** > **Local Users and Groups** > **Users**.

      The default username and password are **assrftp** and **P@ssw0rd**. Right-click on the user to change the password. Select the **Set Password...** option.
2. Obtain the Avaya Scopia® Migration Utility using the Avaya Product Licensing and Delivery System (PLDS).

   The PLDS download ID is ASSR830000013.
3. On the SCC, run the Avaya Scopia® Migration Utility.
4. Read the welcome message and click **Next**.

   The Source Recordings Location page displays. You can use this page to identify the location of the existing recordings on the SCC server.
5. Perform the following steps.
   a. Accept the default location or browse to and select an alternative location for recordings in the **Recordings** field.
   b. Accept the default location or browse to and select an alternative location for meta-data in the **Meta data** field.
   c. Accept the default location or browse to and select an alternative location for categories in the **Categories** field.
6. Click **Next**.

   The Destination Avaya Streaming & Recordings Server page displays. You can use this page to identify the location on the Scopia® SR server to which the utility will migrate the files
7. Perform the following steps.
   a. Enter the Scopia® SR Manager server IP address in the **Server IP** field.
   b. Enter the FTP user name in the **User Name** field.
   c. Enter the FTP administrator password in the **Password** field.
   d. Enter the folder into which you want to migrate the recordings in the **Root Folder** field.

e. Click **Test Connection**.

The utility tests the connection between the SCC and Scopia® SR servers. It displays an information dialog to indicate the result of the test.

The **Next** button is enabled if there is a successful connection.

f. Click **Next**.

The Categories screen displays.

8. **(Optional)** Click **Migrate** to migrate the categories file.

All categories created on the SCC are imported into the Scopia® SR.

9. Click **Next**.

The Recordings screen displays. Use this page to select the recordings you wish to migrate. You can sort the recordings using a number of attributes, such as size and status. The total size of all the recordings is displayed on the bottom left and the size of your current selection is displayed next to it.

10. Perform the following steps.

a. Select the recordings you want to migrate.

b. Click **Migrate**.

c. **(Optional)** Click **Rescan** to update the list of recordings.

If this is your first time using the tool, there is no need to rescan. However, if you continued to use the SCC after you performed an initial migration, you can run the tool again. The rescan feature detects any additional recordings that have been added since the tool was initially run.

d. Click **Close**.

The Avaya Scopia® Migration Utility migrates the identified files from the SCC server to the Scopia® SR server.

11. On the Scopia® SR, disable FTP.

Double-click the **Stop FTP** shortcut on the desktop.

Converting recordings

A converter utility runs on the Scopia® SR Manager and it monitors the FTP folder to look for categories and recordings from the SCC, which are transferred to the Scopia® SR using the migration tool. When the converter utility finds files, it converts them from the .mov format to the .mp4 format and moves the converted files into a specified `autopublish` folder.

You must enable the AutoPublish feature in the Scopia® SR Manager administration interface. When you enable the AutoPublish feature, it monitors the `autopublish` folder and imports files into the Scopia® SR as it finds them.

To obtain the converter utility, you must download it from PLDS. The PLDS download ID is: ASSR830000014.

Note:

Depending on the size of recordings and the speed of your network, it can take some time to convert all of the recordings.

Procedure

1. Enable the Autopublish utility.
   a. On the Scopia® SR, log in to the Scopia® SR Manager Administration interface.
   b. Navigate to **Global Policies** > **Media AutoPublish**.
   c. Select **Enabled**.
   d. Enter the destination folder to use for auto-publishing.

      If you are using the converter utility to import recordings from Avaya Scopia® Content Center Recording server , use this folder as the **Destination Path** in the converter utility.
   e. Enter a polling interval in the **Polling Interval** field. The default is two minutes.
   f. Select **Save**.
2. Configure the converter utility.
   a. On the Scopia® SR, run the Avaya Scopia® Streaming and Recording Converter Utility.
   b. Read the welcome message and click **Next**.

      The Configuration page displays.
   c. Enter your Scopia® SR Manager administrator username in the **User name** field.

      The default username is `admin`.
   d. Enter your Scopia® SR Manager administrator password in the **Password** field.

      The default password is `admin`.
   e. Enter the destination location of the recordings in the **Destination Path** field. This is a folder on the Scopia® SR.

      Ensure that you use the same folder that you specified the destination folder for auto-publishing.

      The **Source Path** field is pre-configured with the FTP root folder. You can change it by clicking **Browse**.
   f. Click **Next**.

      The converter utility is configured and the Monitoring page displays.
   g. Use the Monitoring page to view the live status of the conversion process. You can view a description of the columns in Table 34: Monitoring Page columns on page 147.

Table 34: Monitoring Page columns

Status	Description
MeetingID	Scopia® Solution Meeting ID for the meeting that was recorded.
Name	Name of the recording.
Size (MB)	Size of the recording.
Date	Date when the recording was made.
Status	Status of the conversion (see Table 35: Monitoring Page status values on page 147).
Organization	Organization that the recording belongs to (in an enterprise solution, this is always 999).
File	Name of the file on disk.

You can remove or retry any failed conversions. See Table 35: Monitoring Page status values on page 147.

Table 35: Monitoring Page status values

Status	Description
Pending	The file is in the FTP folder but is not processed yet.
Convert Error	There has been an error converting the .mov or the .xml. An .err file has been created.
Converted	The file is converted and moved to the autoimport folder, but not imported yet.
Import Error	The file is in the Autopublish folder but there has been an error importing it. An .err file has been created.
Complete	The file has been successfully imported.
Import Pending	The file has not yet been imported from the Autopublish folder.

Next steps

If there is an error, an err file is generated.

The err file contains a description of the error. You can read it and try and resolve the error. You can delete the .err file, and the utility automatically tries the import again. Alternatively, you can check the checkbox next to the recording and click the **Retry** button. The tool then deletes the .err file and retries the action.

Chapter 18: Working with a reverse proxy server

Reverse proxy servers

If you would like users outside of the enterprise network to access recordings and broadcasts, you must place Scopia® SR in a Demilitarized Zone (DMZ) or install a reverse proxy. Avaya supports the following reverse proxy servers:

- Avaya Session Border Controller for Enterprise
- Apache HTTP Server
- A10 Network AX Series Application Delivery Controller (ADC)

The Avaya SBCE can route the internet traffic from the external internet clients to the internal Scopia® SR servers which are located within the enterprise network. Figure 46: Reverse Proxy Communications on page 149 shows the communication between the various devices and the internet, using the reverse proxy.

The Scopia® SR components that require internet connectivity are:

- The Scopia® SR Manager: Provides the HTTP portal to access recordings and live streams
- The delivery node (DN): Provides the media streaming capabilities
- The virtual delivery node (VDN): Integrates with the content delivery network (CDN)

Each of these components requires its own internet available IP address.

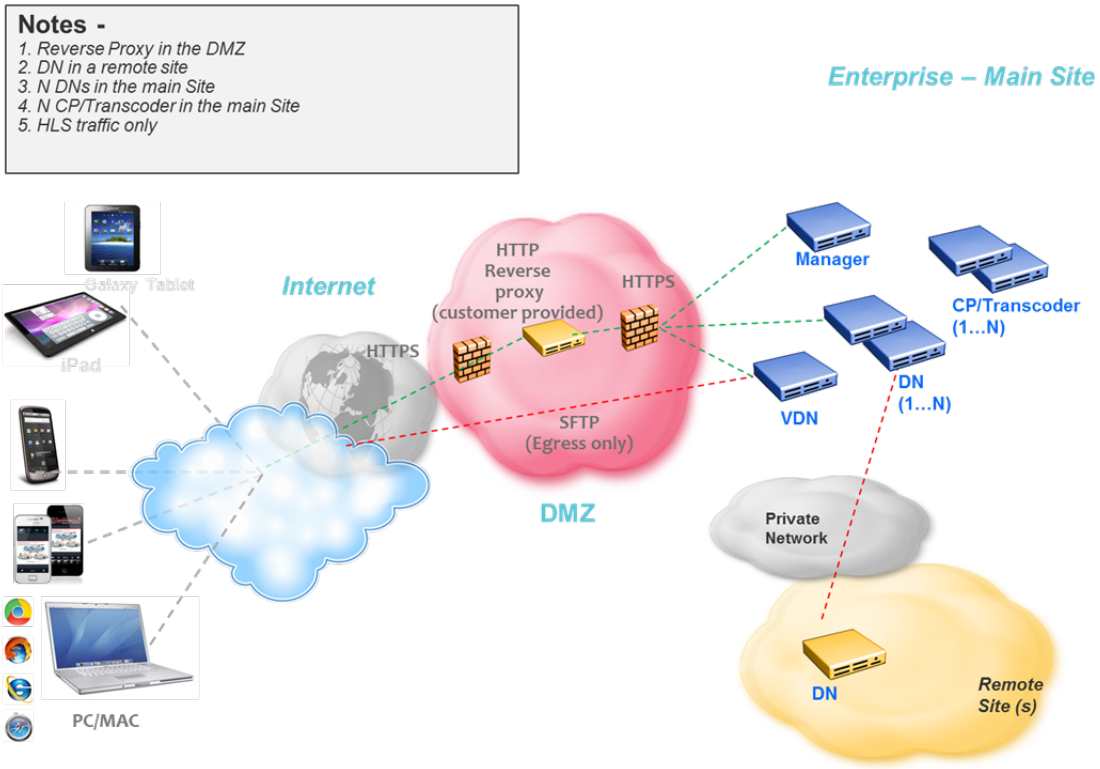


Figure 46: Reverse Proxy Communications

The Scopia® SR system can only operate with a split horizon DNS, A split horizon DNS requires the DNS server to resolve the same domain name to the internal IP addresses for clients that are within the enterprise network and to the external IP addresses when the clients are outside of the enterprise network.

Table 36: Tasks required on page 149 lists the tasks that you must complete in order to configure the Avaya SBCE.

Table 36: Tasks required

No.	Task	Description	Notes	✔
1	Ensure that you have all the required prerequisites, including Avaya SBCE 6.3.2 Patch 1+ and Avaya WebLM, amongst other components.	For more information, see the *Administering Avaya Session Border Controller for Enterprise Guide*, which is available on https://support.avaya.com/.		
2	Create an interface for each external IP address.	Creating an interface for each external IP address on page 150		
3	If you are configuring your deployment to support HTTP communications, create a	Configuring HTTP on page 151	This step configures the system for	

Table continues…

No.	Task	Description	Notes	✔
	profile for each of the internal web servers.		HTTP communications.	
4	If you are configuring your deployment to support HTTPS communications, there are a number of steps. 1. Install a root CA for the client side. 2. Install certificates for the external interfaces. These are the interfaces facing towards the internet. 3. If the certificate signing requests (CSR) are generated outside of the system, then you must upload the certificate and the private key associated with it at the same time. 4. Create new TLS profiles for the client and server. The client profile is the interface facing towards the Scopia® SR servers, and the server profile is for the interface facing towards the Internet. 5. Create an HTTPS Reverse Proxy entry for each external interface.	1. Installing CA Certificates on page 152 2. Installing certificates for the external interfaces on page 153 3. Uploading the certificate and private key together on page 154 4. Creating a client profile on page 156 and Creating a server profile on page 158 5. Configuring HTTPS on page 161	This step configures the system for HTTPS communications.	

Related links

Example of a reverse proxy deployment on page 15

Creating an interface for each external IP address

The Scopia® SR components that require internet connectivity are:

- The Scopia® SR Manager: Provides the HTTP portal to access recordings and live streams
- The delivery node (DN): Provides the media streaming capabilities
- The virtual delivery node (VDN): Integrates with the content delivery network (CDN)

Each of these components requires its own internet available IP address.

Procedure

1. Log on to the EMS web interface using the administrator credentials.
2. In the left navigation pane, click **Device Specific Settings** > **Network Management**.
3. On the Network Management page, click **Networks**.
4. Edit the External Interface.
5. Click **Add**.
6. Add an IP address for each component.
7. Click **Finish**.
8. Validate that the interfaces are active by pinging each IP address.

Configuring for regular communications

You can configure the reverse proxy for HTTP communications.

Related links

Configuring HTTP on page 151

Configuring HTTP

The Scopia® SR components that require internet connectivity are:

- The Scopia® SR Manager: Provides the HTTP portal to access recordings and live streams
- The delivery node (DN): Provides the media streaming capabilities
- The virtual delivery node (VDN): Integrates with the content delivery network (CDN)

Each of these components requires its own internet available IP address.

About this task

This set of steps shows an example of a delivery node configuration. You must repeat these steps for each component.

Procedure

1. Log on to the EMS web interface using the administrator credentials.
2. In the left navigation pane, click **Device Specific Settings** > **DMZ Services** > **Relay Services**.

   The system displays the Relay Services page.
3. In the **Reverse Proxy** tab, click **Add**.

4. On the Add Reverse Proxy Profile page, do the following:
   a. In the **Service Name** field, type the reverse proxy profile name. For example, ASSRDN.
   b. Select the **Enabled** check box.
   c. In the **Listen IP** field, click the external IP address associated with the DN.
   d. In the **Listen Port** field, type the port for remote workers.

      The default value is 443 for HTTPS and 80 for HTTP.
   e. In the **Connect IP** field, click the internal interface IP address that Avaya SBCE must use for communicating.
   f. In the **Server Addresses** field, type the internal DN server IP address and port number.
5. Click **Finish**.

Next steps

Repeat this set of steps for each component.

Related links

Configuring for regular communications on page 151

Configuring for secure communications

You can configure the reverse proxy for HTTPS communications. For secure communications, you require:

- One certificate for each component that requires an external interface.
- Certificate Authority (CA) for each server certificate (this can be self-signed)

There are many different ways to install certificates on the Avaya SBCE. These examples show how to install third part externally-generated certificates.

Related links

Installing CA certificate on page 152
Installing the root certificate authority (CA) certificate for the client side on page 153
Installing the certificates for the external interfaces on page 153
Uploading the certificate and private key together on page 154
Creating TLS profiles for the client and the server on page 155
Configuring HTTPS on page 161

Installing CA certificate

Procedure

1. In the left navigation pane, click **TLS Management** > **Certificates**.

2. Click **Install**.
3. In the **Type** field, select **CA Certificate**.
4. In the **Name** field, type a name for the certificate.
5. Click **Browse** to locate the certificate file.
6. Click **Upload**.

Related links

Configuring for secure communications on page 152

Installing the root certificate authority (CA) certificate for the client side

In this content, client-side refers to the interface facing towards the Scopia® SR components.

Procedure

1. In the left navigation pane, click **TLS Management** > **Certificates**.
2. Click **Install**.
3. In the **Type** field, select **CA Certificate**.
4. In the **Name** field, type a name for the certificate.
5. Click **Browse** to locate the certificate file.
6. Click **Upload**.

Related links

Configuring for secure communications on page 152

Installing the certificates for the external interfaces

In this context, client-side refers to the interface facing towards the Scopia® SR components.

After you complete these steps, you must verify that the certificates are synchronized to the Avaya SBCE otherwise the reverse proxy service will not function.

Procedure

1. In the left navigation pane, click **TLS Management** > **Certificate**.
2. Click **Generate CSR**.
3. Enter appropriate information in the Generate CSR screen, and click **Generate CSR**.

   If you have any other method available, you need not generate CSR using the Avaya SBCE EMS web interface.

4. Use the following settings if you want to generate CSR using alternate methods:
   - Certificate: keyUsage = keyEncipherment
   - Private Key: SHA1 hash with at least 1024-bit size or SHA256 with 2048–bit size

   These settings are generated automatically when you generate CSR using the Avaya SBCE EMS web interface.
5. If you generate CSR using the Avaya SBCE EMS web interface, download the CSR to your computer.
6. Send the CSR to the Certificate Authority (CA) for signing.

   The CA signs the CSR by using the methods that are acceptable at the site.

Next steps

Upload the signed X.509 certificate, the key file, and the trust chain, if necessary, to the EMS through the EMS GUI.

Related links

Configuring for secure communications on page 152

Uploading the certificate and private key together

If you are using certificate signing requests that are generated outside of the system, then you must upload both the certificate and the private key associated with it at the same time using the Install Certificate page.

Procedure

1. In the left navigation pane, click **TLS Management** > **Certificates**.
2. Click **Install**.
3. In the **Type** field, select **Certificate**.
4. In the **Name** field, type the name of the Certificate file.

   Note:

   You can type only letters, numbers, and underscores in the **Name** field. Enter the name of the Certificate file that is uploaded to the EMS. If the name of the Certificate file that you browse for uploading has a different name, that name will be changed with the Certificate name that is uploaded to the EMS.
5. In the **Certificate File** field, click **Browse** and browse to the location of the Certificate file.
6. In the **Key** field, select one of the following options:
   - **Use Existing Key from Filesystem**: Select this option if you generated a CSR from the Generate CSR screen. In this option, the key file is already in the correct location on the EMS.

Note:

If you are using this option, ensure that the Common Name in the Generate CSR screen matches with the name of the install certificate.

- **Upload Key File**: Select this option if you generated a CSR by using an alternate method than the built-in Generate CSR screen.

  In this option, you must upload the private key as described in Step 7.

7. **(Optional)** In the **Key File** field, click **Browse** and browse to the location of the key file
8. In the **Trust Chain File** field, click **Browse** and browse to the location of the trust chain file.

   This step is required if the CA provided a separate certificate trust chain.

   If the third party CA provides separate Root CA and Intermediate certificates, you must combine both files into a single certificate file for Avaya SBCE. To combine the files, add the contents of each certificate file one after the other, with the root certificate at the end.
9. Click **Upload**.

   The system uploads the signed X.509 certificate, and the key file, if necessary, to the EMS.

Example

Next steps

Related links

Configuring for secure communications on page 152

Creating TLS profiles for the client and the server

After you install the certificates, you must create new TLS profiles for the client and the server. In this context, the client profile faces towards Scopia® SR and the server profile faces towards the internet.

One client profile should be enough for the complete Scopia® SR solution. However, you must create a server profile for each external interface component.

The Scopia® SR components that require internet connectivity are:

- The Scopia® SR Manager: Provides the HTTP portal to access recordings and live streams
- The delivery node (DN): Provides the media streaming capabilities
- The virtual delivery node (VDN): Integrates with the content delivery network (CDN)

Related links

Configuring for secure communications on page 152
Creating a client profile on page 156
Creating a new TLS server profile on page 158

Creating a client profile

Procedure

1. Log in to Avaya SBCE EMS web interface with administrator credentials.
2. In the left navigation pane, click **TLS Management** > **Client Profiles**.
3. Click **Add**.

   The system displays the **New Profile** window.
4. Enter the requested information in the appropriate fields.
5. Click **Finish**.

   The system installs and displays the new TLS client profile.

Related links

Creating TLS profiles for the client and the server on page 155
TLS client profile screen field descriptions on page 156

TLS client profile screen field descriptions

Both TLS Server Profiles and TLS Client Profiles share the same configuration parameters. Therefore, the parameter descriptions in the following table match those in the table in TLS server profile pop-up window field descriptions on page 158.

Note:

The only exception is regarding the Peer Verification parameter setting. This setting determines whether a peer verification operation must be performed. In a TLS client profile, the Peer Verification parameter setting cannot be changed and is locked to: **Required**. In a TLS server profile, the Peer Verification parameter can be set to one of three possible values: **Required**, **Optional**,or **None**.

Nmae	Description
TLS Profile	
Profile Name	A descriptive name used to identify this profile.
Certificate	The certificate presented when requested by a peer.
Certificate Info	
Peer Verification	The incoming connection must provide a certificate, the certificate must be signed by one of the Peer Certificate Authorities, and not be contained in a Peer Certificate Revocation List. In a client profile configuration screen, the **Required** checkbox is a locked setting and cannot be cleared. **Note:** Peer Verification is always required for TLS Client Profiles, therefore the **Peer Certificate Authorities**, **Peer Certificate Revocation Lists**, and **Verification Depth** fields will be active.

Table continues…

Nmae	Description
Peer Certificate Authorities	The CA certificates to be used to verify the remote entity identity certificate, if one has been provided. **Note:** Using **Ctrl** or **Ctrl+Shift**, any combination of selections can be made from this list. Using **Ctrl+Shift** , the user can drag to select multiple lines, and using **Ctrl**, the user can click to toggle individual lines.
Peer Certificate Revocation Lists	Revocation lists that are to be used to verify whether a peer certificate is valid. **Note:** Using **Ctrl** or **Ctrl+Shift**, any combination of selections can be made from this list. Using **Ctrl+Shift** , the user can drag to select multiple lines, and using **Ctrl**, the user can click to toggle individual lines.
Verification Depth	The maximum depth used for the certificate trust chain verification. Each CA certificate might also have its own depth setting, referred to as the path length constraint. If both are set, the lower of these two values is used.
Renegotiation Parameters	
Renegotiation Time (optional)	The amount of time after which the TLS connection must be renegotiated. This field is optional and must be set to 0 to disable.
Renegotiation Byte Count (optional)	The number of bytes after which the TLS connection must be renegotiated. This field is optional and must be set to 0 to disable.
Cipher Suite Options	
Ciphers	The level of security to be used for encrypting data. Available selections are: • All: Support all cipher suite options. This option is equivalent to the OpenSSL ALL cipher suite. • Strong: Encryption support that is strong enough for most business or government needs. For use within the United States only. This option is equivalent to the OpenSSL HIGH cipher suite. • Export Only: The strongest level of encryption allowed by federal law for exportable products. This option is equivalent to the OpenSSL EXPORT cipher suite. • Null Only (For Debugging): No encryption is used. This should be only used for debugging. This option is equivalent to the OpenSSL NULL cipher suite. • Custom: Selecting the Custom radio button enables a user-defined level of encryption that can be configured by using the Value field described below.
Options	Additional options to be used with the ciphers listed above. **Note:** The following cipher options are considered insecure and should not be used unless absolutely required. • DH — Enable cipher suites using Diffie-Hellman key exchange.

Table continues…

Nmae	Description
	• ADH — Enable cipher suites using anonymous Diffie-Hellman. • MD5 — Enable cipher suites using MD5 for message authentication.
Value	A field provided to contain a textual representation of the ciphers settings used by OpenSSL. For a full list of possible values, see the OpenSSL ciphers documentation at http://www.openssl.org/docs/apps/ciphers.html. **Note:** The Value field is an advanced setting that must not be changed without an understanding of how OpenSSL handles ciphers. Invalid or incorrect settings in this field can cause insecure communications or even catastrophic failure.

Related links

Creating a client profile on page 156

Creating a new TLS server profile

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **TLS Management** > **Server Profiles**.

   The system displays the Server Profiles screen.
3. Click **Add**.

   The system displays the New Profile window.
4. Enter the requested information into the appropriate fields.
5. Click **Finish**.

   The TLS Server profile is created, installed, and listed in the application pane.

Related links

Creating TLS profiles for the client and the server on page 155
TLS server profile screen field descriptions on page 158

TLS server profile screen field descriptions

Both TLS Server Profiles and TLS Client Profiles share the same configuration parameters. Therefore, the parameter descriptions in the following table match those in the table in TLS Client Profile Pop-up Screen Field Descriptions on page 156

Note:

The only exception is regarding the Peer Verification parameter setting (see description below). This setting determines if a peer verification operation should be performed. In a TLS client profile, the Peer Verification parameter setting cannot be changed and is locked to: **Required**, while in a TLS server profile, the Peer Verification parameter may be set to one of three possible values: **Required**, **Optional**, or **None**.

Field	Description
TLS Profile	
Profile Name	The descriptive name used to identify this profile.
Certificate	The certificate presented when requested by a peer.
Certificate Info	
Peer Verification	One of three checkboxes indicating whether peer verification is required: • Required: The incoming connection must provide a certificate, the certificate must be signed by one of the Peer Certificate Authorities, and not be contained in a Peer Certificate Revocation List. In a client profile configuration screen, the **Required** checkbox is a locked setting and cannot be deselected. • Optional: The incoming connection may optionally provide a certificate. If a certificate is provided, but is not contained in the Peer Certificate Authority list, or is contained in a Peer Certificate Revocation List, the connection will be rejected. • None: No peer verification will be performed. **Note:** Peer Verification is always required for TLS Client Profiles, therefore the **Peer Certificate Authorities**, **Peer Certificate Revocation Lists**, and **Verification Depth** fields will be active. **Note:** For TLS Server Profiles, always set Peer Verification to **None** to ensure that iOS devices operate successfully.
Peer Certificate Authorities	The CA certificates to be used to verify the remote entity identity certificate, if one has been provided. **Note:** Using **Ctrl** or **Ctrl+Shift**, any combination of selections can be made from this list. Using **Ctrl+Shift** , the user can drag to select multiple lines, and using **Ctrl**, the user can click to toggle individual lines.
Peer Certificate Revocation Lists	Revocation lists that are to be used to verify whether or not a peer certificate is valid. **Note:** Using **Ctrl** or **Ctrl+Shift**, any combination of selections can be made from this list. Using **Ctrl+Shift** , the user can drag to select multiple lines, and using **Ctrl**, the user can click to toggle individual lines.
Verification Depth	The maximum depth used for the certificate trust chain verification. Each CA certificate might also have its own depth setting, referred to as the path length constraint. If both are set, the lower of these two values is used.

Table continues…

Field	Description
Renegotiation Parameters	
Renegotiation Time (optional)	The amount of time after which the TLS connection must be renegotiated. This field is optional and must be set to 0 to disable.
Renegotiation Byte Count (optional)	The amount of bytes after which the TLS connection must be renegotiated. This field is optional and must be set to 0 to disable.
Cipher Suite Options	
Cipher Suites	The level of security to be used for encrypting data. Available selections through radio button selections are: • All: Support all cipher suite options. This option is equivalent to the OpenSSL ALL cipher suite. • Strong Only: Encryption support that is strong enough for most business or government needs. For use within the United States only. This option is equivalent to the OpenSSL HIGH cipher suite. • Export Only: The strongest level of encryption allowed by federal law for exportable products. This option is equivalent to the OpenSSL EXPORT cipher suite. • Null Only: No encryption is used. This should be only used for debugging. This option is equivalent to the OpenSSL NULL cipher suite. • Custom: Selecting the Custom radio button enables a user-defined level of encryption that can be configured by using the Value field described below.
Options	Additional options to be used with the ciphers listed above. **Note:** The following cipher options are considered insecure and should be disabled unless absolutely required. • DH: Enable cipher suites using Diffie-Hellman key exchange. • ADH: Enable cipher suites using anonymous Diffie-Hellman. • MD5: Enable cipher suites using MD5 for message authentication.
Value	**Note:** The Value field is an advanced setting that should not be changed without an understanding of how OpenSSL handles ciphers. Invalid or incorrect settings in this field can cause insecure communications or even catastrophic failure. A field provided to contain a textual representation of the ciphers settings used by OpenSSL. For a full list of possible values, see the OpenSSL ciphers documentation at http://www.openssl.org/docs/apps/ciphers.html.

Related links

Creating a new TLS server profile on page 158

Configuring HTTPS

The Scopia® SR components that require internet connectivity are:

- The Scopia® SR Manager: Provides the HTTP portal to access recordings and live streams
- The delivery node (DN): Provides the media streaming capabilities
- The virtual delivery node (VDN): Integrates with the content delivery network (CDN)

Each of these components requires its own internet available IP address.

About this task

This set of steps shows an example of a delivery node configuration. You must repeat these steps for each component.

Procedure

1. Log on to the EMS web interface using the administrator credentials.
2. In the left navigation pane, click **Device Specific Settings** > **DMZ Services** > **Relay Services**.

   The system displays the Relay Services page.
3. In the **Reverse Proxy** tab, click **Add**.
4. On the Add Reverse Proxy Profile page, do the following:
   a. In the **Service Name** field, type the reverse proxy profile name. For example, ASSRDN_TLS.
   b. Select the **Enabled** check box.
   c. In the **Listen IP** field, click the external IP address associated with the DN.
   d. In the **Listen Port** field, type the port for remote workers.

      The default value is 443 for HTTPS and 80 for HTTP.
   e. In the **Listen Protocol** field, click HTTPS.
   f. In the **Listen TLS Profile** field, select the server profile associated with this entry.
   g. In the **Server Protocol** field, click HTTPS.
   h. In the **Server Profile** field, select the client profile you created previously. This is the internal server facing profile.
   i. In the **Connect IP** field, click the internal interface IP address that Avaya SBCE must use for communicating. This is the internal interface SBC IP
   j. In the **Server Addresses** field, type the internal DN server IP address and port number.
5. Click **Next**.
6. Click **Finish**.

Next steps

Repeat this set of steps for each component.

Related links

Configuring for secure communications on page 152

Chapter 19: Troubleshooting the streaming and recording server

Replacing a delivery node

You can replace a delivery node if the original delivery node fails. Do not unregister the original delivery node before replacing it. As soon as the new delivery node is operational, Scopia® SR automatically unregisters the original delivery node and registers the replacement delivery node. You require a license key to replace a delivery node.

You do not have to replace the entire delivery node in the event of a failed disk drive. If one disk drive fails, you can replace the disk drive and the Raid system can recover it. If both drives fail, replace the failed drives and use the replace delivery node feature to refresh it.

Related links

[Installing a new delivery node to replace an operational delivery node](#) on page 163
[Installing a new delivery node if the existing delivery node is unusable](#) on page 164
[Installing a new DN if have only one DN and you have fixed the hard drive or replaced the appliance](#) on page 165

Installing a new delivery node to replace an operational delivery node

Condition

You have an operational delivery node (DN) and are installing a new delivery node to replace it.

Solution

1. Keep the original DN on the network and do not unregister it.
2. Add the new DN to the network.

   Use a different hostname and IP address than the original DN.

   Do not register the new DN but it needs a valid license key.

   Note:

   You can temporarily use a DHCP IP address.
3. Log in to Scopia® SR.

4. Click the **Devices** tab.
5. From the **Browse** menu, select the device you want to access.

   A list of devices of that type is displayed.
6. Click the delivery node that you want to replace.
7. Click **Advanced Options** > **Replace with new DN**.
8. In the **Entry** field, enter the temporary IP address of the replacement DN.
9. Click **Replace**.

   Scopia® SR displays a confirmation message.

   When the replacement is complete, Scopia® SR changes the status of the DN to **Up**. Scopia® SR may still be distributing programs to the new DN so check the **Distributed Programs** tab to ensure that the transfer of content is complete before you move to the next step.
10. Remove the replaced DN from the network.

    Do not unregister the DN.
11. **(Optional)** Change the IP address of the new DN to match the replaced DN or give it a FQDN.
12. **(Optional)** If you want to give a DN an FQDN, you can register it using the Scopia® SR Manager GUI.

Related links

Replacing a delivery node on page 163
Setting the IP address of the delivery component (Delivery Node) on page 37

Installing a new delivery node if the existing delivery node is unusable

Condition

You have an failed delivery node (DN) and are installing a new delivery node to replace it. When a DN fails, programs are distributed from a different DN on the network, so you need to have a different operational DN.

Solution

1. Ensure that you have an operational and registered DN in your network.

   You will be copying data from this DN.
2. Add the new DN to the network.

   Use the same IP address as the unusable DN.

   Do not register the new DN.
3. Log in to Scopia® SR.
4. Click the **Devices** tab.

5. From the **Browse** menu, select the device you want to access.

   A list of devices of that type is displayed.
6. Click the delivery node that you want to replace.
7. Click **Advanced Options** > **Replace with new DN**.
8. In the **Entry** field, enter the same IP address or FQDN as the DN you are replacing.
9. Click **Replace**.

   Scopia® SR displays a confirmation message.

   When the replacement is complete, Scopia® SR changes the status of the DN to **Up**. Scopia® SR may still be distributing programs to the new DN so check the **Distributed Programs** tab to ensure that the transfer of content is complete before you move to the next step.
10. **(Optional)** Backup and restore Scopia® SR to recover any library media that was specifically sent to the unusable DN.

    The **Replace with new DN** option only copies published programs and the associated media.

Related links

Replacing a delivery node on page 163

Installing a new DN if have only one DN and you have fixed the hard drive or replaced the appliance

Condition

You have an failed delivery node (DN) and are installing a new delivery node to replace it, but your deployment only uses a single DN.

Solution

1. Obtain the latest backup of the existing DN.
2. Add the new DN to the network.

   Use the same IP address as the unusable DN.

   Do not register the new DN. You need to restore the backup onto the new DN.
3. Log in to Scopia® SR.
4. Click the **Devices** tab.
5. From the **Browse** menu, select the device you want to access.

   A list of devices of that type is displayed.
6. Click the delivery node that you want to replace.
7. Click **Advanced Options** > **Replace with new DN**.
8. In the **Entry** field, enter the same IP address or FQDN as the DN you are replacing.

9. Click **Replace**.

   Scopia® SR displays a confirmation message.

   When the replacement is complete, Scopia® SR changes the status of the DN to **Up**. Scopia® SR may still be distributing programs to the new DN so check the **Distributed Programs** tab to ensure that the transfer of content is complete before you move to the next step.

Related links

[Replacing a delivery node](#) on page 163
[Restoring delivery nodes](#) on page 91
[Viewing the distribution status of delivery nodes](#) on page 105

Troubleshooting upgrades

About this task

If the upgrade does not happen successfully, you can use the individual administration GUI interfaces of the conference points (CP) and delivery nodes (DN) to view the upgrade log from the **Log Type** list.

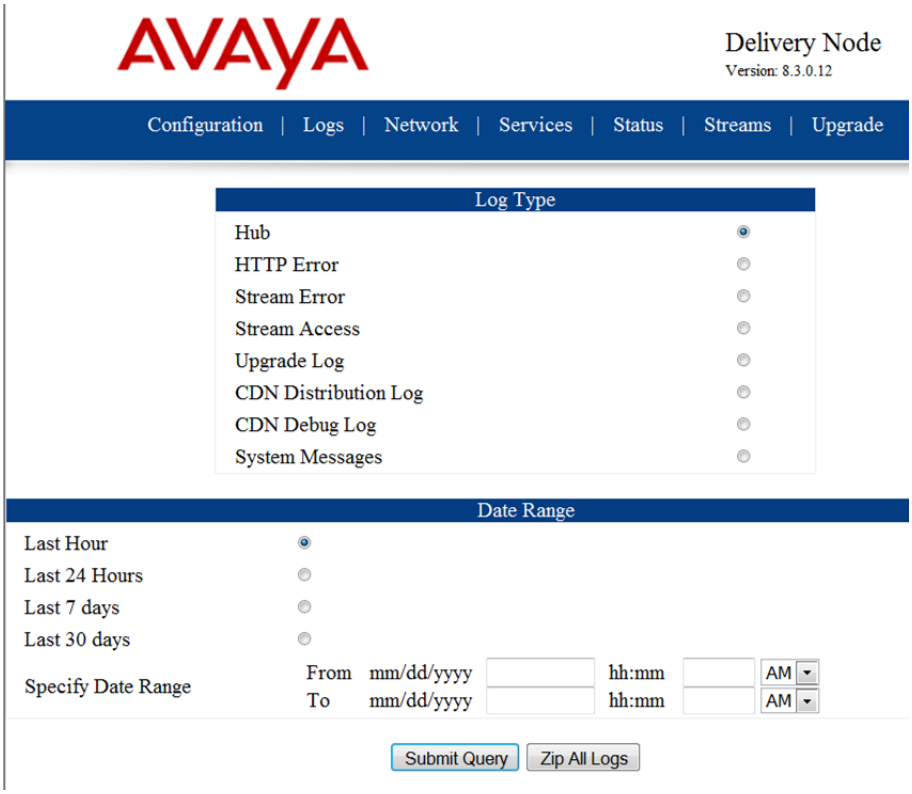


Figure 47: Device upgrade log example

Error message during migration of recordings: “Too many recordings selected”

The Avaya Scopia® Migration Utility can only migrate 600GB of recordings to the Scopia® SR.

Solution

1. Reduce the number of recordings that you are attempting to migrate.
2. Click **Rescan** to re-scan the recordings folder on the SCC.

Error when you test the connection during migration of recordings

The Avaya Scopia® Migration Utility requires FTP connectivity between the SCC and the Scopia® SR. If there is no FTP connectivity between the SCC and the Scopia® SR, you get an error with the message “Error: Failed to connect server, please make sure (1) Server IP address you entered is valid. (2) Server is reachable with FTP enabled”.

Solution

Do one of the following:

- Enable FTP on the Scopia® SR server.

  FTP is not enabled by default.
- Return to the Destination Avaya Scopia® Streaming and Recording server screen and check the details that you entered for the Scopia® SR

Error message during migration of recordings: “No recordings found”

If the Avaya Scopia® Migration Utility cannot locate any recording files on the SCC server, you get an error with the message “No recordings found”.

Solution

Do one of the following:

- Click **Rescan** to re-scan the recordings folder on the SCC.
- Return to the Source Recordings Location screen and check the details that you entered for the SCC

A recording has not migrated to the Scopia® SR

The Avaya Scopia® Migration Utility should migrate all of your selected recordings from the SCC to the Scopia® SR. It will not migrate a recording if:

- There is insufficient space on the Scopia® SR server.
- It cannot convert the recording from .mov to .mp4.
- If cannot convert the meta data from SCC XML format to Scopia® SR XML format.
- If there is a meta data file but no recording file.
- If there is a recording file but no meta data file.

Solution

1. On the Scopia® SR, navigate to `C:\autoimport`.

   This folder contains error files for each recording that the utility could not migrate. The files have the format <*name of recording*>.err.
2. Open the error files using a text editor, such as Notepad.

Changing the computer name

This is an optional task.

Procedure

1. On the Server Manager screen, select Local Server.
2. On the PROPERTIES panel, click the **Computer name** hyperlink.

   This is a randomly generated name.
3. In the **System Properties** dialog, on the Computer Name tab, click **Change...**.
4. Enter a new computer name in the **Computer Name** field and click **OK**.

   You need to reboot the server to apply these changes.
5. Click **OK** on the information message.
6. Click **Close**.
7. Click **Restart Now**.

POODLE security vulnerability

Padding Oracle On Downgraded Legacy Encryption (POODLE) is a Secure Socket Layer (SSL) security vulnerability. Taking advantage of this vulnerability, man-in-the-middle attackers can decrypt cipher text by using a padding oracle side-channel attack.

POODLE affects older standards of encryption, especially SSL version 3. This vulnerability does not affect the Transport Layer Security (TLS) encryption mechanism.

To prevent attacks that exploit the POODLE security vulnerability, disable SSL version 3. You can disable SSL version 2 and SSL version 3 while adding or editing client profiles.

Disabling SSL version 3 on Avaya SBCE

About this task

In Avaya SBCE, SSL version 2 is disabled by default. Use these steps to disable SSL version 3.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **TLS Management** > **Client Profiles**.
3. Click the client profile that you want to edit.

   The system displays the configuration of the selected client profile in the content area.
4. Click **Edit**.

   The system displays the Edit Profile window.
5. In the **Options** field, clear the **SSLv3** check box.
6. Click **Finish**.

   The system disables SSL version 3.

Accessing Scopia® SR Manager logs

You can access Scopia® SR Manager logs from the Scopia® SR administrative GUI or you can access the logs directly on the Scopia® SR machine in the following folder: `C:\Program Files\Apache Software Foundation\Tomcat 7.0\logs`.

About this task

Use this task to access the following logs:

GUI entry	File on disk
Debug Log (x)	debug.log.x
User Interface Log	localhost.date.log
Rest API Log (x)	rest.log.x
Device Polling Log	polling.log.x

Each log rolls over once it reaches 10MB. The three most recent logs for `Debug.log` and `rest.log` are available from the Scopia® SR administrative GUI.

Procedure

1. Log in to Scopia® SR.
2. Click the **Devices** tab.
3. From the **Browse** menu, click **Manager**.
4. Download logs from the **Logs** section.

Accessing transcoder logs

You can access the transcoder logs using a web browser. https://<Transcoder IP address>:8443/transcoder_log.txt.

If you are logged on to the machine directly, you can access the logs from: `C:\Program Files (x86)\BurstPoint Networks\Transcoder\htdocs`.

Alternatively, you can follow the steps to access the conference point logs and download the transcoder logs from the conference point.

Accessing conference point logs

You can access conference point logs from the administrative GUI or you can access the logs directly on the conference point machine in the following folder: `/opt/stream/logs`, `/opt/vcb/log` and `/opt/www/logs`.

About this task

Use this task to access the following logs:

GUI entry	File on disk
Conference Point Call Billing Log	/opt/stream/logs/export/vcg_call_export
Conference Point File Billing Log	/opt/stream/logs/export/vcg_file_export
H.323	/opt/vcb/log/h323.log
Hub	/opt/vcb/log/hub.log
Interface	/opt/www/logs/interface_log
HTTP Access	/opt/www/logs/access_log
HTTP Error	/opt/www/logs/error_log
RTSP	/opt/stream/logs/export/rtsp_export
MMS	/opt/stream/logs/export/wm_export
Stream Access	/opt/stream/logs/access_log

Table continues…

GUI entry	File on disk
Stream Error	/opt/stream/logs/error_log
Upgrade	/opt/stream/logs/upgrade_server.log

Procedure

1. Log in to the conference point.
2. Navigate to **System Information** > **Logs**.
3. Select the type of log that you want to access and the date range.
4. Click **Continue**.

   The log is displayed.

   You can save it locally.

Related links

Logging in to conference points and delivery nodes on page 55

Accessing delivery node logs

You can access delivery node logs from the administrative GUI or you can access the logs directly on the delivery node machine in the following folder: `/opt/stream/logs` and `/opt/www/logs`.

About this task

Use this task to access the following logs:

GUI entry	File on disk
Hub	/opt/stream/logs/hub.log
HTTP Error	/opt/www/logs/error_log
Stream Error	/opt/stream/logs/error_log
Stream Access	/opt/stream/logs/access_log
Upgrade Log	/opt/stream/logs/upgrade_server.log
CDN Distribution Log	/opt/stream/logs/cdn_dist.log
CDN Debug Log	/opt/stream/logs/ftp.log
System Messages	/opt/stream/logs/messages

Procedure

1. Log in to the delivery node.
2. Select **Logs**.
3. Select the type of log that you want to access and the date range.
4. Click **Submit**.

Alternatively, you can click **ZIP All Logs** to zip up the logs.

The log is displayed.

You can save it locally.

Related links

Logging in to conference points and delivery nodes on page 55

Accessing alerts

Procedure

1. Log in to Scopia® SR.
2. Click the **Reports** tab.
3. On the Reports menu, click **Alerts**.

   The System Alerts screen is displayed.

   Note:

   You can delete alerts by selecting individual checkboxes. Alternatively, you can select all checkboxes to delete all alerts. Click **Delete**.

Troubleshooting devices

You can use the Scopia® SR web interface to access the device logs and manage the device details. You can access device logs by logging on to the device's detail page. The default login is the same for all devices.

- Username: `administrator`
- Password: `administrator`

Follow the login steps that you used to verify the registration of each of the components.

Related links

Troubleshooting conference points on page 172
Troubleshooting delivery nodes and virtual delivery nodes on page 173
Registering each of the components on page 42

Troubleshooting conference points

Procedure

1. Log in to the conference point.

2. Select a task:

To do the following	Select this option
Start and stop services **Configure call rollover, network settings, or system clock** **Install license** **Customize interface**	**System Menu** > **System Configuration** > **Enable Services**
View streaming bandwidth summary, active stream list, or active multicast list	**System Information** > **Usage Statistics**
View general information, logs, network diagnostics, and storage utilization	**System Information** > **General Information**

Related links

Troubleshooting devices on page 172
Logging in to conference points and delivery nodes on page 55

Troubleshooting delivery nodes and virtual delivery nodes

In the case of virtual delivery nodes (VDN), Scopia® SR operates in the following way:

- For FTP file transfers, the VDN transfers one file at a time. This prevents flooding of your internet connection. The VDN internally creates a queue and transfers each file in the order they are requested.
- If a number of simultaneous requests occur, the VDN can take longer to publish a file to the content delivery network (CDN).
- The VDN retries FTP file transfers until it transfers each file successfully.
- On system failure or reboot, the VDN resumes the queue and retries the transfer of files that were not completed.
- If a file cannot be transferred for any reason, the VDN moves each file to the end of the queue and retries it after it tries all of the other files. This prevents locking of the queue.
- It retires distribution if a recoverable error is encountered when interacting with the CDN.

The VDN can handle the following recoverable system errors. It retires distribution if encounters a recoverable error when interacting with the CDN.

- Power loss
- Reboot
- Restarting of services
- Internet connection interruption
- Incorrect username and/or password
- Upload site is down
- FTP port is not open

If there is a continuous pending or failed status message in **Manage** > **Devices** > **VDN Distributed Programs**. Check the logs for incorrect or expired credentials or a network issue with access to the CDN.

Procedure

1. Log in to the delivery node or virtual delivery node.
2. Select a task:

To do the following	Select this option
Register the device and change the Web administrator account password	Configuration
View error logs and system messages	Logs
Start and stop services	Services
View system information, network information, and storage utilization	Status
View incoming and outgoing streams	Streams
View license information, upgrade a license, and upgrade software	Upgrade

Related links

Troubleshooting devices on page 172
Logging in to conference points and delivery nodes on page 55

Users cannot record

In order for a user to be able to record from the Scopia® Desktop client, you must enable Scopia® Desktop user authentication in Scopia® Management.

There is an additional policy in Scopia® Management that determines whether guests can access broadcasts and recordings. If this policy is switched off, then the **Recordings and Events** tab does not appear in the Scopia® Desktop portal page until the user logs in.

In addition, if a user clicks on a direct URL to a recording, instead of the recording opening directly, they will be prompted to log in to Scopia® Desktop first.

Recordings and Events tab is not present

In order for a user to be able to record from the Scopia® Desktop client, you must enable Scopia® Desktop user authentication in Scopia® Management.

There is an additional policy in Scopia® Management that determines whether guests can access broadcasts and recordings. If this policy is switched off, then the **Recordings and Events** tab does not appear in the Scopia® Desktop portal page until the user logs in.

In addition, if a user clicks on a direct URL to a recording, instead of the recording opening directly, they will be prompted to log in to Scopia® Desktop first.

Updating the license

Procedure

1. Log in to Scopia® SR.
2. Click the **Devices** tab.
3. From the **Browse** menu, select **Manager**.
4. In the **License Information** panel, enter a new license key and click **Update**.

Chapter 20: Implementing Port Security for the Avaya Scopia® Streaming and Recording server

Avaya has introduced a new component, the Avaya Scopia® Streaming and Recording server (Scopia® SR). Scopia® SR is the Avaya next generation HD streaming and recording platform, bringing significant enhancements to the Avaya Scopia® solution for streaming and recording. The Avaya Scopia® Streaming and Recording server replaces the Avaya Scopia® Content Center Recording server (SCC) server.

This section details the ports used for the Avaya Scopia® Streaming and Recording server.

Related links

Ports to open for the Avaya Scopia Streaming and Recording server on page 176

Ports to open for the Avaya Scopia® Streaming and Recording server

If your network includes a firewall, and the Avaya Scopia® Streaming and Recording server and devices are on opposite sides of the firewall, you must open ports on the firewall to enable streaming between the Scopia® SR components. When opening ports on the Avaya Scopia® Streaming and Recording server, use the following tables as a reference.

Important:

The specific firewalls you need to open ports on depends on where your Avaya Scopia® Streaming and Recording server and other Scopia® Solution products are deployed.

The Avaya Scopia® Streaming and Recording server is a solution that consists of several components and these components can be deployed in a highly flexible way. You could place all of the components on a single server or you could place the components on a series of distributed servers. If you place all of the components on a single server, you do not have to open ports that facilitate communications between components of the Avaya Scopia® Streaming and Recording server. If you place some of the components outside of the firewall, you must open more ports. The

tables in this section list the ports for each of the individual components. You must know the location of each of the components before you configure the ports.

- Inbound port means that the device is listening on that port
- Outbound port means that the device is connecting to that port

Table 37: Ports to Open on the Scopia® SR Manager

Port Range	Protocol	Direction	Destination	Functionality	Required
80 443	TCP (HTML)	Inbound	From Scopia® SR client (the end-user's web browser) to Scopia® SR Manager. It is either 80 or 443, depending on how the system is configured.	Client systems access the Scopia® SR Manager HTML	Mandatory
443	TCP (HTTP)	Inbound	From Scopia® Management to Scopia® SR Manager	REST API for management communication	Mandatory
443	TCP (XML)	Inbound	From the Scopia® SR transcoder to Scopia® SR Manager	Communication	Mandatory
443	TCP	Bidirectional	Conference points (CP)	Scopia® SR Manager communicate with other Scopia® SR devices XML for communication, also pushes media files	Mandatory
443	TCP	Bidirectional	Delivery nodes (DN)	Scopia® SR Manager communicate with other Scopia® SR devices XML for communication, also pushes media files	Mandatory
443	TCP	Bidirectional	Virtual delivery node (VDN)	Scopia® SR Manager communicate with other Scopia® SR	Mandatory

Table continues…

Port Range	Protocol	Direction	Destination	Functionality	Required
				devices (typically on 443, not 80) XML for communication, also pushes media files	
25	TCP	Outbound	From Scopia® SR Manager to the SMTP server	SMTP mail server communication	Optional
8443	TCP (XML)	Outbound	From Scopia® SR Manager to the Scopia® SR transcoder.	Communication with the transcoder	Mandatory
8080	TCP (HTTP)	Outbound	From Scopia® SR Manager to Scopia® Management	REST API (the port is defined by iVIEW)	Mandatory

Table 38: Ports to Open on the Conference Points (CP)

Port Range	Protocol	Direction	Destination	Functionality	Required
443	TCP (XML)	Bidirectional	Scopia® SR Manager		Mandatory
80	TCP (Media)	Inbound	From the Scopia® SR transcoder to the CP	Transcoder pulls ASF streams from CP	Mandatory
80	TCP (Media)	Inbound	From the delivery node (DN) to the CP	RTP media (windows media streaming). CP gets raw RTP from Scopia® Elite MCU then sends it to the transcoder to encode to Windows Media. Then, it pulls back from the transcoder and makes it available to the DN	Mandatory
1025 — 65535 (default is 4100 — 4400)	UDP	Inbound	From Scopia® Elite MCU to the CP	RTP Audio/Video/ Presentation	Mandatory

Table continues…

Port Range	Protocol	Direction	Destination	Functionality	Required
				Note: This can be limited in the CP administration GUI.	
9090 -> 9XXX	TCP (Windows Media Stream)	Outbound	From the CP to the Scopia® SR transcoder	Transcoder communicates to the CP for transcoding and broadcasting from the transcoder. CP Pulls media from the transcoder	Mandatory
1719	UDP	Outbound	From the CP to the gatekeeper	RAS communication with the gatekeeper	Mandatory
1720	TCP	Outbound	From the CP to the gatekeeper	RAS communication with the gatekeeper, H. 323 call setup (H. 225/Q.931)	Mandatory
1025 — 65535	TCP	Outbound	From the CP to the gatekeeper	RAS communication with the gatekeeper, H. 323 call setup (H. 225/Q.931) – dynamic port range that can be limited on the gatekeeper	Mandatory
1025 —65535	UDP (RTP)	Outbound	From the CP to the Scopia® Elite MCU	RTP Audio/Video/ Presentation (this range can be limited on the MCU)	Mandatory
8443	TCP (XML)	Outbound	From the CP to the Scopia® SR transcoder	Communication between devices	Mandatory

Table 39: Ports to Open on the Transcoder

Port Range	Protocol	Direction	Destination	Functionality	Required
8443	TCP (XML)	Inbound	From the CP to the Scopia® SR transcoder	Communication between devices	Mandatory
8080 8443	TCP (HLS: 8080 or 8443)	Inbound	From the DN to the Scopia® SR transcoder	Communication between devices Access to HLS media	Mandatory
8443	TCP (XML)	Inbound	From the Scopia® SR Manager to the transcoder	Communication between devices	Mandatory
9090 — 9XXX	TCP (Windows Media Stream)	Inbound	From the CP to the Scopia® SR transcoder	Transcoder communicates to the CP for transcoding and broadcasting from the transcoder	Mandatory
9090 — 9XXX	UDP (AAC-LC)	Inbound	From the CP to the Scopia® SR transcoder	Transcoder communicates to the CP for transcoding and broadcasting from the transcoder	Mandatory
443	TCP (XML)	Outbound	From the Scopia® SR transcoder to the Scopia® SR Manager	Communication between devices	Mandatory
80	TCP (Media)	Outbound	From the Scopia® SR transcoder to the CP	Communication between devices	Mandatory
1755	TCP (Windows Media Stream)	Outbound	From the Scopia® SR transcoder to the CP	Transcoder communicates to the CP for transcoding and broadcasting from the transcoder	Mandatory

Table 40: Ports to Open on the Virtual Delivery Node (VDN)

Port Range	Protocol	Direction	Destination	Functionality	Required
80 443	TCP (HLS Media)	Inbound	From the CDN to the VDN.	DN streams media to client	Mandatory
80	TCP (HLS Media)	Inbound	From the Session Border	DN streams media to client	Mandatory

Table continues…

Port Range	Protocol	Direction	Destination	Functionality	Required
443			Controller (SBC) to the VDN		
21	TCP (FTP)	Outbound	From the VDN to the content delivery network (CDN)	File upload from the VDN to the CDN.	Mandatory
80 443	TCP (80, 443)	Outbound	From the VDN to the DN	DN communicate with other DN (HLS Media) – pull the stream from DN	Mandatory
443	TCP (XML)	Bidirectional	Scopia® SR Manager	Communications	Mandatory

Table 41: Ports to Open on the Delivery Node (DN)

Port Range	Protocol	Direction	Destination	Functionality	Required
80 443	TCP (HLS Media, Progressive Download)	Inbound	From the Scopia® SR clients to the DN	DN streams media to clients	Mandatory
80 554 1755	TCP (Windows Media)	Inbound	From the Scopia® SR clients to the DN	DN streams media to clients (windows media streaming)	Mandatory
80 443	TCP (Windows Media – 80, HLS – 80, 443)	Bidirectional	From DN to DN	DN communicates with other DN (HLS Media)	Mandatory
443	TCP (XML)	Bidirectional	Scopia® SR Manager		Mandatory
8080 8443	TCP	Outbound	From the DN to the transcoder		Mandatory
1024-5000 1755 80	UDP, TCP, HTTP (Windows Media)	Outbound	From the DN to the Scopia® SR clients	Client will try UDP between port 1024-5000 (Only open the necessary number of ports), then TCP on port 1755, then TCP on port 80	Mandatory

Table continues…

Port Range	Protocol	Direction	Destination	Functionality	Required
Multicast port range	UDP	Outbound	From the DN to the Scopia® SR clients	When using MMS and the network is multicast-capable, the standard port range for multicast will be used	Mandatory

Table 42: Additional Ports to Open

Port Range	Protocol	Direction	Destination	Functionality	Required
3389	UDP, TCP	Inbound	Remote Desktop	Microsoft Remote Desktop	Optional
53	UDP, TCP	Outbound	DNS server	DNS servers	Optional
123	UDP	Bidirectional	NTP source	NTP	Mandatory
514	TCP	Outbound	Syslog Server	Remote Syslog Server	Mandatory

Related links

Implementing Port Security for the Avaya Scopia Streaming and Recording server on page 176
Limiting RTP/UDP Ports on the Conference Point on page 182

Limiting RTP/UDP Ports on the Conference Point

Procedure

1. Log in the conference point administration page.
   a. Type `https://<CP FQDN/IP Address>` in a web browser.
   b. Log in using the following credentials:
      - Username: `administrator`
      - Password: `administrator`
2. Navigate to **System Configuration** > **Enable Services**.
3. In the RTP Ports panel, enter the base port value in the **From** field, and the upper port value in the **To** field.
4. Click **Save**.

Related links

Ports to open for the Avaya Scopia Streaming and Recording server on page 176

Glossary

1080p	See Full HD on page 187.
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 189.
AAC	AAC is an audio codec which compresses sound but with better results than MP3.
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.
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.
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.
Avaya Scopia® Streaming and Recording Manager	The Avaya Scopia® Streaming and Recording Manager provides a web-based interface to configure and manage Scopia® Streaming and Recording server software, devices, services, and users. The Scopia® Streaming and Recording server Manager application resides on a single

	hardware platform and provides access to all content in the Scopia® Streaming and Recording server environment.
Avaya Scopia® Streaming and Recording Manager Portals	The Scopia® Streaming and Recording server Manager provides a portal for administering content. When you log in to the web interface, you can access the Administrator portal. The Manager also provides the Viewer portal. This portal is embedded within the Avaya Scopia® Desktop User portal. Use the User portal to schedule Scopia® Streaming and Recording server broadcasts.
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 194.
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.
CDN	Scopia® SR enables you to publish content to the cloud, using a virtual delivery node (VDN) and a content delivery network (CDN). The VDN and the network of the CDN act as one delivery mechanism. When a user creates a recording (program), they can choose to distribute it to the CDN, as well as to the regular delivery node (DN).
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).

Conference Point	The Avaya Scopia® Streaming and Recording Conference Point is a video conferencing gateway appliance that captures standard or high definition video conferences. It transcodes, creates, and records the video conferences in a streaming media format. You can use it to capture H.323 video for instant video webcasting or on-demand publishing.
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 185.
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.
Delivery Node	The Avaya Scopia® Streaming and Recording Delivery Node provides on-demand and broadcast video delivery. You can use it alone or in a hierarchy of devices. It supports thousands of concurrent streams. The Delivery Node uses intelligent routing, content caching, and inherent redundancy to ensure transparent delivery of high-quality video.
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® 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 183.
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 186.
FPS	See Frames Per Second on page 187.
Frame Rate	See Frames Per Second on page 187.
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.
FTP	The File Transfer Protocol (FTP) is a standard network protocol used to transfer computer files from one host to another host over a TCP-based network, such as the Internet. FTP is built on a client-server architecture and uses separate control and data connections between the client and the server. FTP users may authenticate themselves using a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it.
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 188.

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 183.

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 189.

High Profile See H.264 High Profile on page 188.

HTTP The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web.

Hypertext is structured text that uses logical links (hyperlinks) between nodes containing text. HTTP is the protocol to exchange or transfer hypertext.

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 193.

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.

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).

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® 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 191.

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 185.
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® 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® Desktop server, endpoints like XT Series and other network devices like LDAP servers and network routers.
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.
Multicast Streaming	Multicast streaming sends a videoconference to multiple viewers across a range of addresses, reducing network traffic significantly. Scopia® 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.
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 185.

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). Users can access recordings from the Scopia® 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.
RTCP	Real-time Control Transport Protocol, used alongside RTP for sending statistical information about the media sent over RTP.
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.
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 185.
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 191.
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.
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.
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 Registrar	See Registrar on page 193.
SIP Server	A SIP server is a network device communicating via the SIP protocol.
SIP URI	See URI on page 197.
Slider	See Content Slider on page 185.
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® Desktop Client or Scopia® Mobile.
SQCIF	SQCIF defines a video resolution of 128 x 96 pixels.
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 194.
Standard Definition	See SD on page 194.
Streaming	Streaming is a method to send live or recorded videoconferences in one direction to viewers. Recipients can only view the content; they cannot participate with a microphone or camera to communicate back to the meeting. There are two types of streaming supported in Scopia® Solution: unicast which sends a separate stream to each viewer, and multicast which sends one stream to a range of viewers.
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.
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® 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 197.
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® Desktop and Scopia® Mobile functionality, and allowed bandwidth for calls.
VFU	See Video Fast Update (VFU) on page 197.
VGA	VGA defines a video resolution of 640 x 480 pixels.
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 193.
Video Switching	See Switched video on page 196.
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.
Viewer Portal	The Avaya Scopia® Streaming and Recording Viewer Portal is embedded in the Avaya Scopia® Desktopuser portal. To access the Viewer Portal, you can select **Recordings and Events** on the main Scopia® Desktop page.

	From the Viewer Portal, you can watch recordings and navigate through the categories.
Virtual Delivery Node	The Avaya Scopia® Streaming and Recording Virtual Delivery Node (VDN) is a device to push content to an external Content Delivery Network (CDN). The method for publishing content to a CDN is tightly coupled to the Avaya Scopia® Streaming and Recording platform which allows a company's video assets to be managed from a central location. If you want to use a VDN and a CDN, you must buy cloud storage and services from Highwinds™, with the appropriate bandwidth and capacity for your needs. You apply the credentials you receive from Highwinds in the Avaya Scopia® Streaming and Recording Manager to securely access the CDN.
Virtual Room	A virtual room in Scopia® 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® 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.
Webcast	A webcast is a streamed live broadcast of a videoconference over the internet. Enable Scopia® Desktop webcasts by enabling the streaming feature. To invite users to the webcast, send an email or instant message containing the webcast link or a link to the Scopia® Desktop portal and the meeting ID.
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.

Index