



Symb I Technologies

For Smart Solutions!

Project Handover Document (PHD)

Project Name: CSA-VC

Version: 2.0

June 12, 2018





Contents

1. About This Design Document	1
1.1 Document purpose.....	1
1.2 Intended Audience.....	1
1.3 Scope	1
1.4 Document usage Guidelines	1
1.5 Assumptions.....	1
1.6 Naming Conventions	1
1.7 CSA-VC Network Topology	3
2. Server Configuration	3
2.1 Polycom RealPresence Resource Manager	3
2.1.1 Meta Data	3
2.1.2 Configuration.....	4
2.1.2.1 Configuring Site Topology	4
2.1.2.2 Configuring provisioning profile.....	6
2.1.2.3 Editing Network Profile	8
2.1.2.4 Editing Admin Profile	13
2.1.2.5 Editing RPAD Server Provisioning Profile	15
2.1.2.6 Managing Provisioning Rules	17
2.1.2.7 Define an E.164 Address Scheme	22
2.1.2.8 Managing Instances.....	24
2.1.2.8.1 View Network Device Instance	24
2.1.2.9 Managing users.....	26
2.1.3 Managing license	28
2.2 Polycom Realpresence DMA	32
2.2.1 Meta Data	32
2.2.2 Configuration	32
2.2.2.1 Licensing	32
2.2.2.3 Setup Signaling.....	33
2.3 Polycom Realpresence Media Suit	37



- 2.3.1 Meta Data 38
- 2.3.2 Configuration 38
 - 2.3.2.1 Signaling setting..... 41
 - 2.3.2.2 Configuring templates..... 44
 - 2.3.2.2.1 Recording template 44
 - 2.3.2.2.2 Transcoding Template..... 46
 - 2.3.2.2.3 VRR template 46
 - 2.3.2.3 Playing Back and Downloading Records 47
- 2.4 Polycom Collaboration Server 1800..... 49
 - 2.4.1 Meta Data 49
 - 2.4.2 Configuration 50
 - 2.4.2.1 IP network service and properties 51
 - 2.4.2.2 IVR services 53
 - 2.4.2.3 Recording link..... 55
 - 2.4.2.4 Conference Profiles 56
 - 2.4.2.5 Meeting Rooms 60
- 2.5 Polycom Access Director 62
 - 2.5.1 Meta Data 62
 - 2.5.2 Configuration 63
 - 2.5.2.1 SIP & H.323 Signaling..... 63
 - 2.5.2.2 Network settings 64
 - 2.5.2.3 Configuring Access Proxy 66
- 3 Endpoint Management 68
- 4 Project Handover Document (PHD) Document Approval Form 70



i. Document Control

Document Reference	
Document Reference	2.0
Customer Name	CSA
Project Title	CSA-VC
File Name	CSA-VC-PHD_v.2.doc
Last Save date:	12/6/18
Pages:	70

Table 1 – Document reference

ii. Document History

Ver	Date	Authors	Change Description
2.0	12/6/18	Amado Ergana	Version 2

Table 2 – Document author

iii. Document Review

Ver	Date	Reviewers	Change Description
2.0	12/6/18	Kennedy Bizuayehu	Version 2

Table 3 – Review Details



1. About This Design Document

1.1 Document purpose

The objective of this document is to provide CSA with detailed design material explaining how the proposed VC solution will meet the CSA Requirements for a video conference. This document will act as a project handover document (PHD) for the IT solution project at CSA. It contains configuration information specifically done to CSA. As such, CSA is expected to sign off on this project handover document.

1.2 Intended Audience

- ❖ CSA Systems and Networking Team.
- ❖ CSA Project Management Team.

1.3 Scope

The scope of this document is to provide CSA engineers with detailed VC design and configurations for all parts of the video conference. It will describe the integration of all components done in order to provide a complete connectivity.

1.4 Document usage Guidelines

A Project Handover Document (PHD) consists of a number of components. These include

- Best Practice Guidance

1.5 Assumptions

Symbol Technologies project team has successfully installed and configured this video conferencing solution for CSA based on the high-level design, which was done at the beginning of the project.

1.6 Naming Conventions

Since network administrators usually access network devices, device naming should be designed and implemented wisely. It is difficult to know in which device they are logged in if the naming convention implemented is not clear enough, especially if they are functionally similar devices. So, device naming must be uniquely identify a device. The following naming convention has been followed in this design is.

For end points

CSA@*Site name*. Example:- Bahirdar branch VC endpoint is named CSA@Bahirdar



Site	Name	IP Address
Addis Ababa Main	CSA@MAIN	172.16.2.10
Addis Ababa Mini	CSA@MINI	172.16.3.10
Ambo	CSA@AMBO	
Hawassa	CSA@HAWASSA	
Mekelle	CSA@MEKELLE	
Bahirdar	CSA@BAHIRDAR	

Note: the above table is incomplete because at the time of compiling this document only the above sites with IP were operational. All endpoints have the same credentials for accessing the web portal.

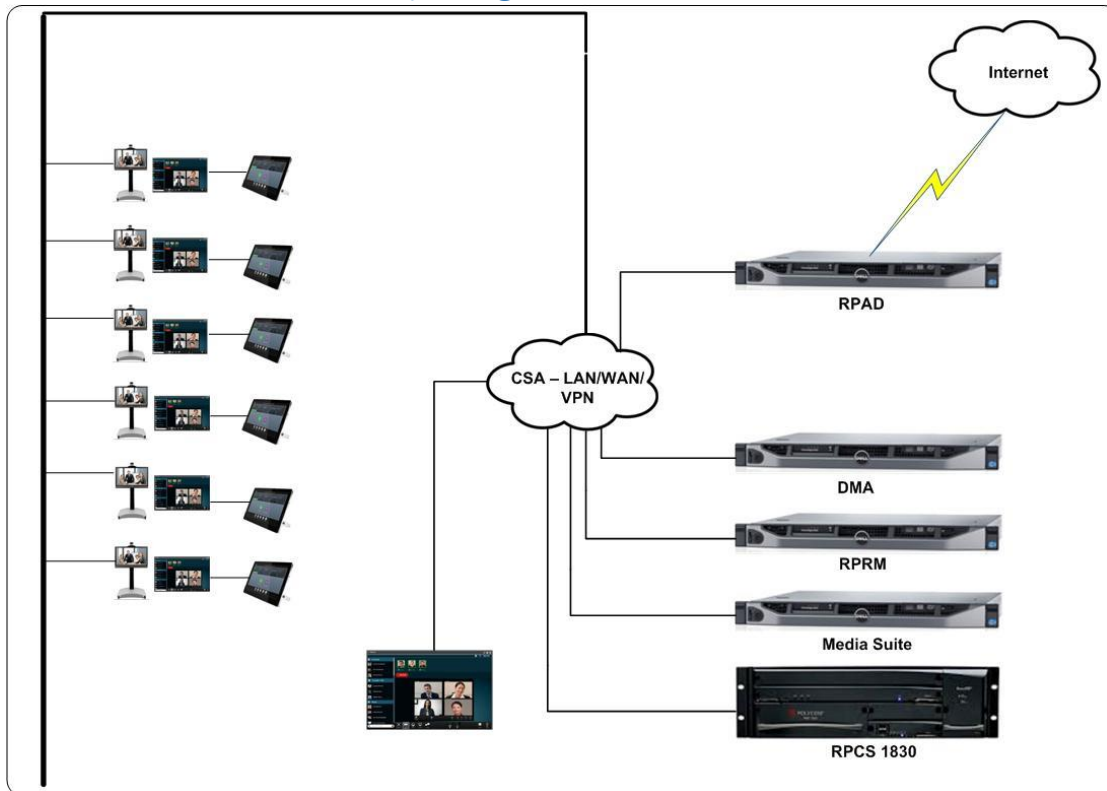
For Servers

The servers are named using FQDN (Fully Qualified Domain Name) and the naming convention goes as follows.

Server	FQDN	IP Address	Public IP
Realpresence Access Director (RPAD)	csa-rpad.csa.gov.et	192.168.251.10	
		192.168.100.9	197.156.82.226
Realpresence Resource Manager (RPRM)	csa-rprm.csa.gov.et	192.168.251.11	
Distributed Media Application (DMA)	csa-dma.csa.gov.et	192.168.251.12	
Media Suit (MS)	csa-ms.csa.gov.et	192.168.251.13	
Realpresence Collaboration Server (RPCS)	csa-rpcs.csa.gov.et	192.168.251.14	
		192.168.251.15	
DNS Server		192.168.0.119	
		192.168.0.53	
NTP Server		192.168.30.1	



1.7 CSA-VC Network Topology



2. Server Configuration

2.1 Polycom RealPresence Resource Manager

The RealPresence Resource Manager is an integrated scheduling and management platform for endpoints and video conferencing infrastructure management. It also functions as the management and licensing platform for Polycom RealPresence Clariti. RealPresence Resource Manager includes the following features and capabilities:

- Video Infrastructure Management
- Video Endpoint and Audio Phone Management
- Conference Scheduling
- Directory Services
- Session Border Control Integration
- Programmatic Access through API

2.1.1 Meta Data

- IP address: 192.168.251.11



2.1.2 Configuration

Please note that if a setting is left unmentioned or stated explicitly, it means we have not made any change to the default setting because it was not necessary for this particular project. However, if you want to dig more about it you can always refer the official administrator guide.

2.1.2.1 Configuring Site Topology

A site is a local area network (LAN) that generally corresponds with a geographic location such as an office or plant. A site contains one or more network subnets, so a device’s IP address identifies the site to which it belongs. The RealPresence DMA system inherits all site topology settings from the RealPresence Resource Manager. In CSA’s site we have created two subnets 192.168.0.0/16 for the servers and 172.16.0.0/16 for endpoints. To create new site or manage the already created one go to *Network Topology -> Site*

The screenshot shows the 'Add Site' configuration window in the Polycom interface. The 'General Info' tab is selected, and the following fields are visible:

- Site Name: CSA
- Description: CSA VC SITE
- Enable Mutual TLS:
- Override ITU Dialing Rules:
- PBX Access Code: (empty)
- Country Code: 251 (with a 'CC' button)
- Area Code: (empty)
- # Of Digits in Subscriber Num: (empty)
- Assignment Method: No Auto Assignment
- Territory: Default Resource Manager Territory
- Location: Addis Ababa, Adis Abeba Astedader, ET (with a 'Specify Location...' button)
- Latitude: 9.024 (9 1.439999999999948' 0" N)
- Longitude: 38.749 (38 44.940000000000014' 0" E)
- Total Bandwidth (Mbps): (empty)

Column	Description
Site Name	CSA
Description of the site	CSA VC Site
Country Code	251
Location	Addis Ababa, Ethiopia



Polycom® Add Site

General Info
ISDN Number Assignment
H.323 Routing
SIP Routing
Subnets

Site Name: Internet/W

Count: 1

2017 Polycom, Inc. Help

Add Subnet

IP Address: 192.168.0.0

Mask length: 16

Total Bandwidth: Mbps

Call Max Bit Rate: kbps

OK Cancel

OK Cancel

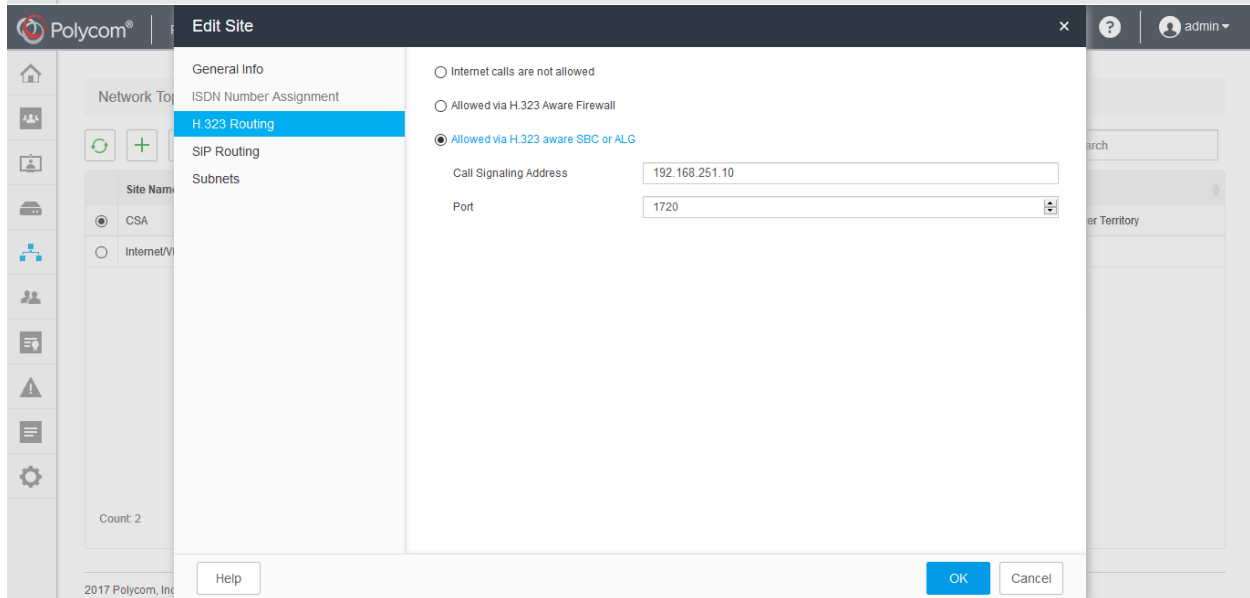
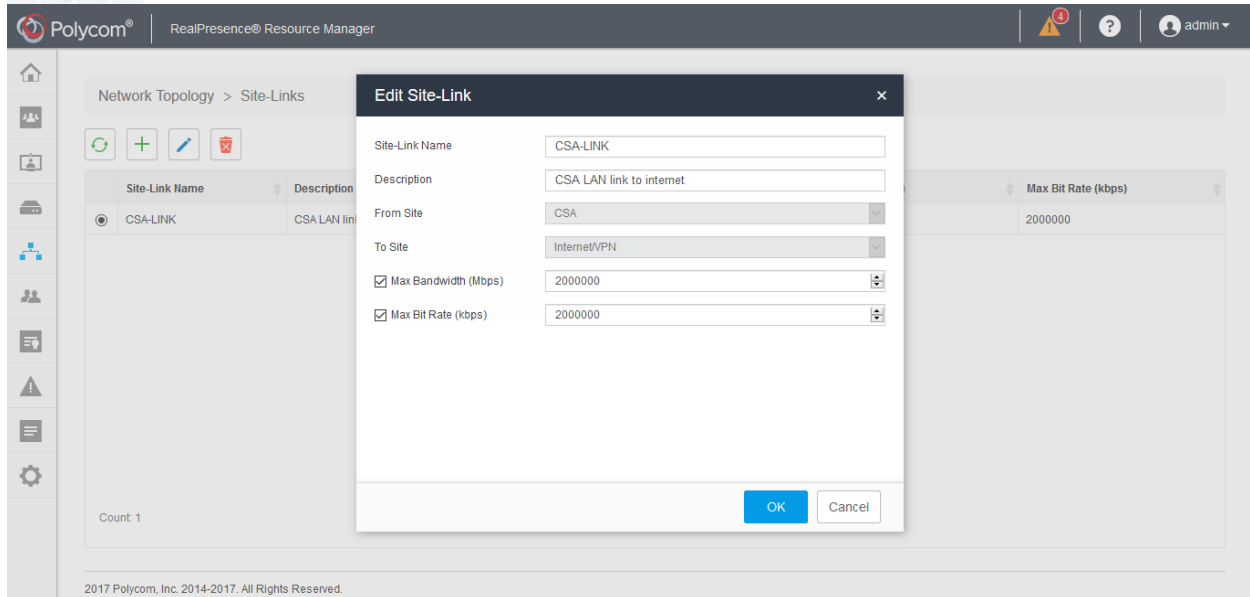
Polycom® RealPresence® Resource Manager

Network Topology > Site-Links

Site-Link Name	Description	From Site	To Site	Max Bandwidth (Mbps)	Max Bit Rate (kbps)
CSA-LINK	CSA LAN link to internet	CSA	Internet/VPN	2000000	2000000

Count: 1

2017 Polycom, Inc. 2014-2017. All Rights Reserved.



2.1.2.2 Configuring provisioning profile

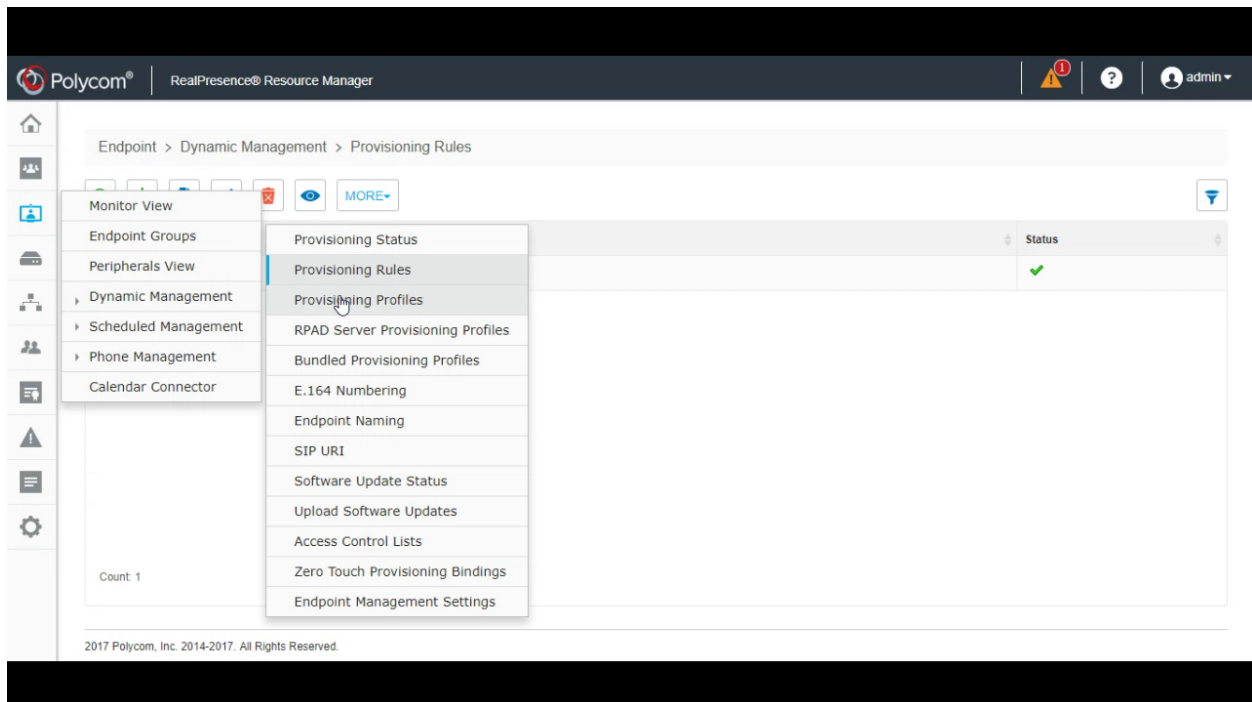
Create Video Endpoint Provisioning Profiles Dynamic provisioning enables endpoints to poll the RealPresence Resource Manager automatically to get provisioning updates (configuration settings) on a dynamic basis. The provisioning profiles the endpoint receives are based provisioning rules you define. When you dynamically manage endpoints (have the endpoint use the RealPresence Resource Manager as its provisioning server), you can automatically configure them by using provisioning profiles. You need to modify and create three types of video endpoint provisioning profiles:

- **Network Provisioning profiles** define Network settings such as security, quality of service, and gatekeeper address, SIP server address, and so on.



- **Admin Config Provisioning profiles** define endpoint administrative settings such as maximum and preferred call speeds for H.323 settings, calendaring settings, Microsoft Lync settings, and so on.
- **Bundled Provisioning profiles** allow you to control system settings that affect user experience.

To manage a profile go to endpoints on the left pane -> Dynamic management -> provisioning profile



Once you did the above, you will be redirected to a page that lists four profiles. Two starting with “Default” and two with “CSA”. We have configured two profile specifically for CSA VC project named CSA-ADMIN-PROFILE and CSA-NETWORK-PROFILE. The other two profiles are default profiles that come pre-configured by Polycom. It is recommended not to alter the default profiles. Any changes that are required to be applied should be made to the CSA profiles.

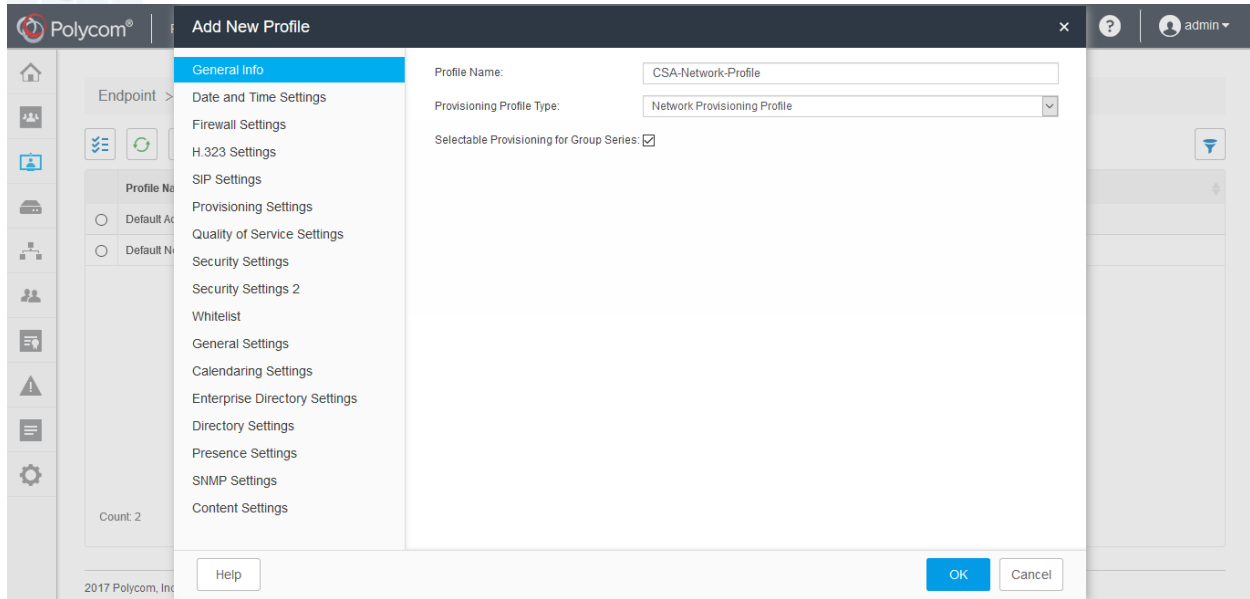


2.1.2.3 Editing Network Profile

Click on the CSA-NETWORK-PROFILE radio button. Now on top of the profile list the icons will change into this order



Click on the pencil icon and a modal with the profile's setting will be opened.

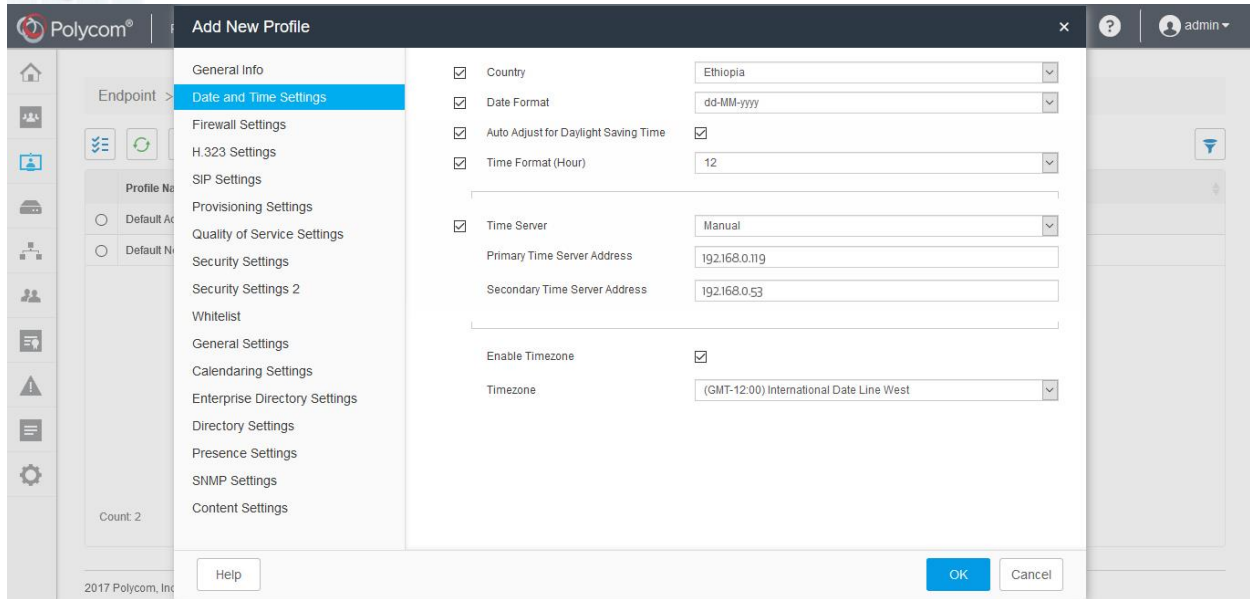


General Info

Profile Name: CSA-Network-Profile

Provisioning Profile Type: Network provisioning profile

Selectable Provisioning for Group Series: by mark this check box, you can manually select which settings within the provisioning profile are sent to a RealPresence Group Series system. Only the selected settings will be provisioned to RealPresence Group Series systems. Within the provisioning profile, only the settings that you select are set to the RealPresence Group Series system. For example, if a provisioning setting is blank but still checked, the blank value is still be provisioned to the system. By default, all settings are checked. If you don't want to provision the setting to the RealPresence Group Series system, you must uncheck the individual settings.



Date and Time Settings

Country: Ethiopia

Date Format: dd-mm-yy

Auto Adjust for Daylight Saving Time: check to adjust the endpoint's system clock for daylight savings time.

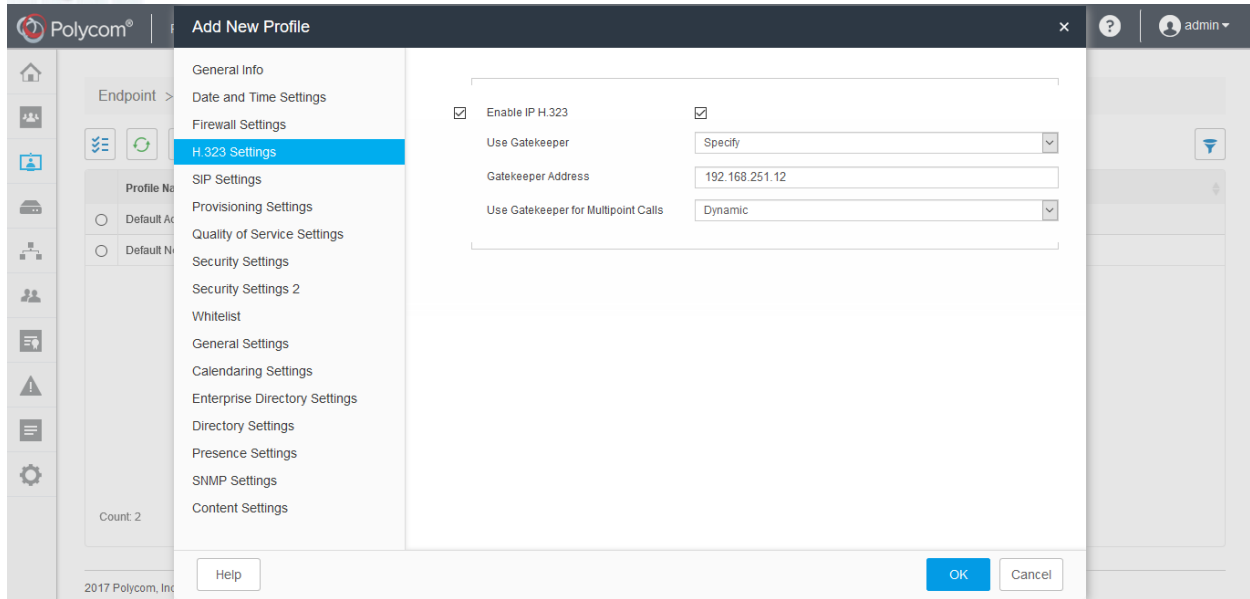
Time Format: 12

Time Server:

Primary Time Server Address: 192.168.0.119

Secondary Time Server Address: 192.168.0.53

Time zone: GMT+3



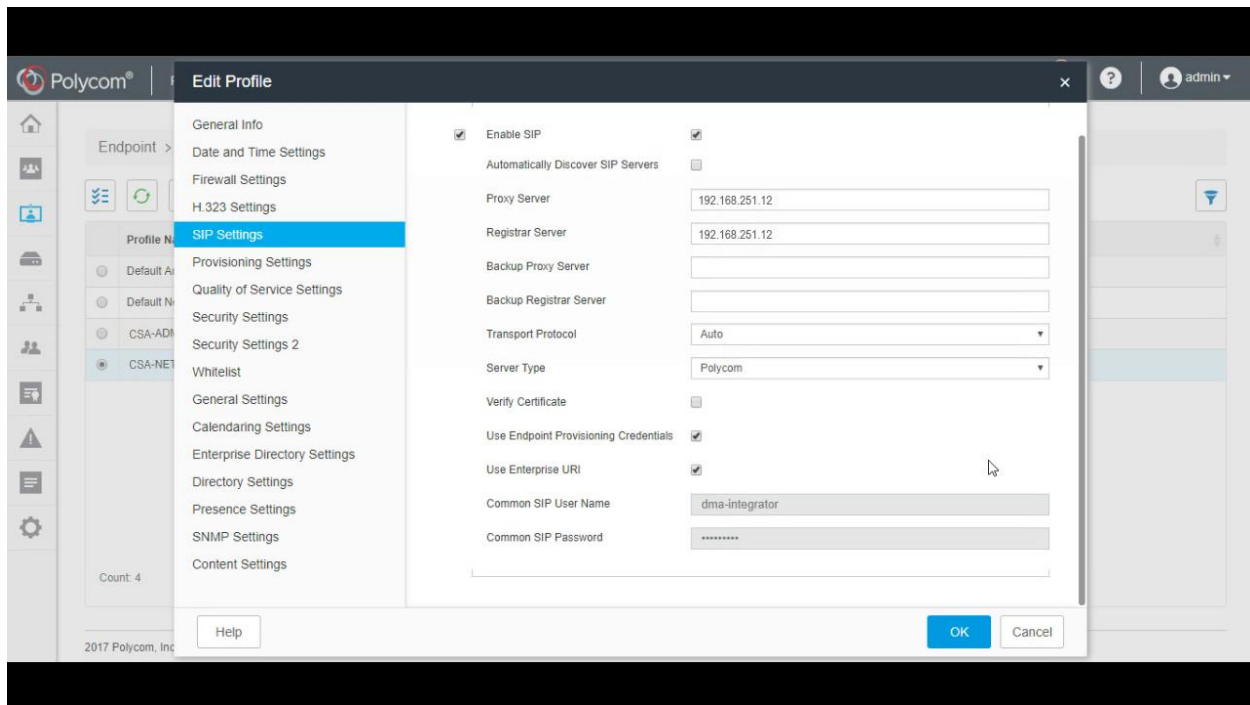
H323 Settings

Enable IP H.323: checked

Use Gatekeeper: specify

Gatekeeper Address: 192.168.251.12

Use Gatekeeper for Multipoint Calls: dynamic



SIP Settings



Enable SIP: checked

Automatically Discover SIP Servers: unchecked

Proxy Server: 192.168.251.12

Registrar Server: 192.168.251.12

Backup Proxy Server: null

Backup Registrar Server: null

Transport Protocol: Auto

Server Type: Polycom

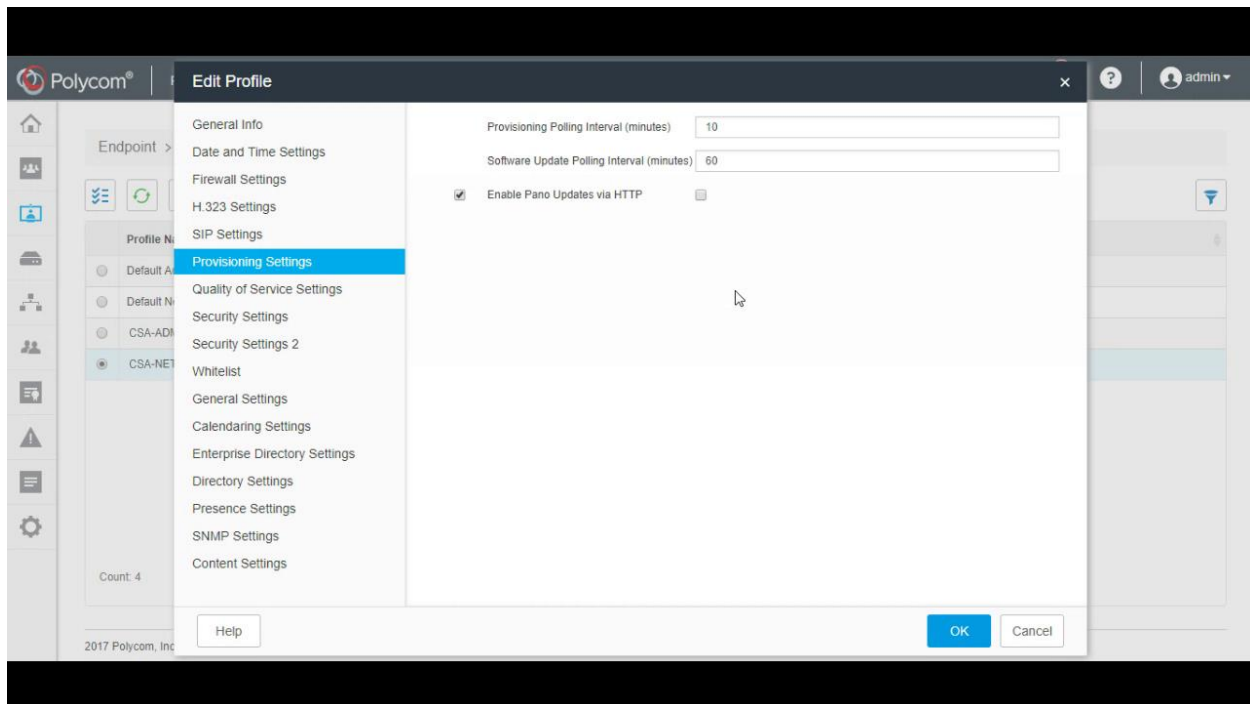
Verify Certificate: unchecked

Use Endpoint Provisioning Credentials: checked

Use Enterprise URI: checked

Common SIP User Name: the user name used to integrate with the SIP server (DMA). We have created a user for each server that is used for integration purposes.

Common SIP Password: the password used to integrate with the DMA



Provisioning Settings

Provisioning Polling Interval (minutes): 10



Software Update Polling Interval (minutes): 60

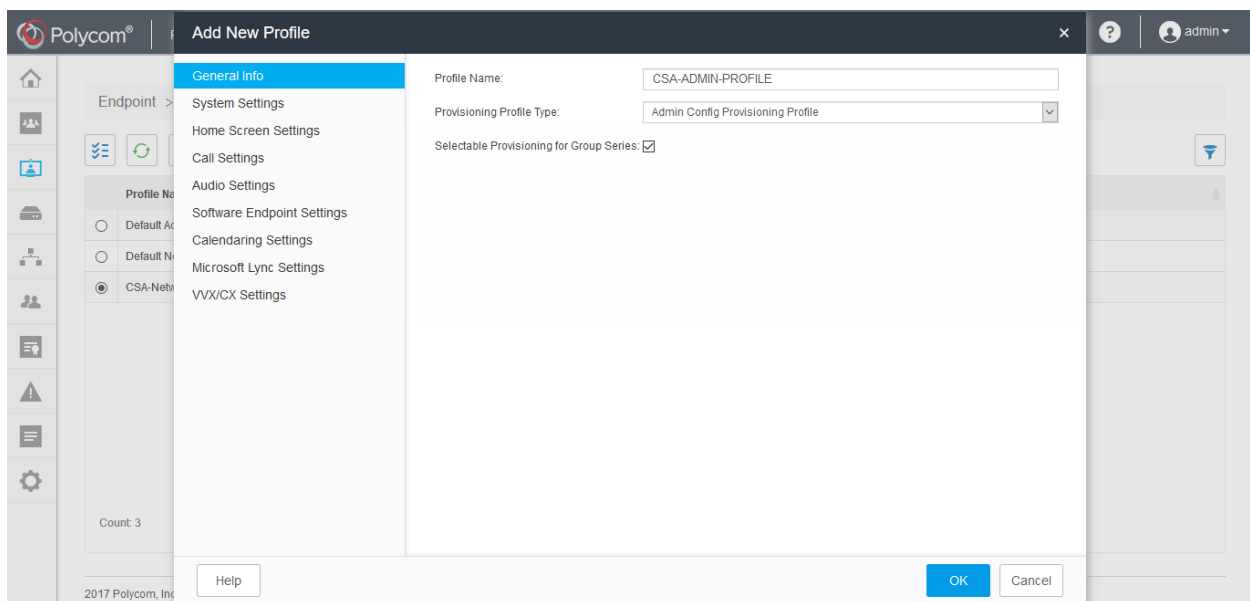
2.1.2.4 Editing Admin Profile

Admin Config provisioning profiles, allow you to create provisioning profiles that include maximum and preferred call speeds for H.323 settings, calendaring settings, Microsoft Lync settings, and so on.

Click on the CSA-ADMIN-PROFILE radio button. Now on top of the profile list the icons will change into this order



Click on the pencil icon and a modal with the profile's setting will be opened.

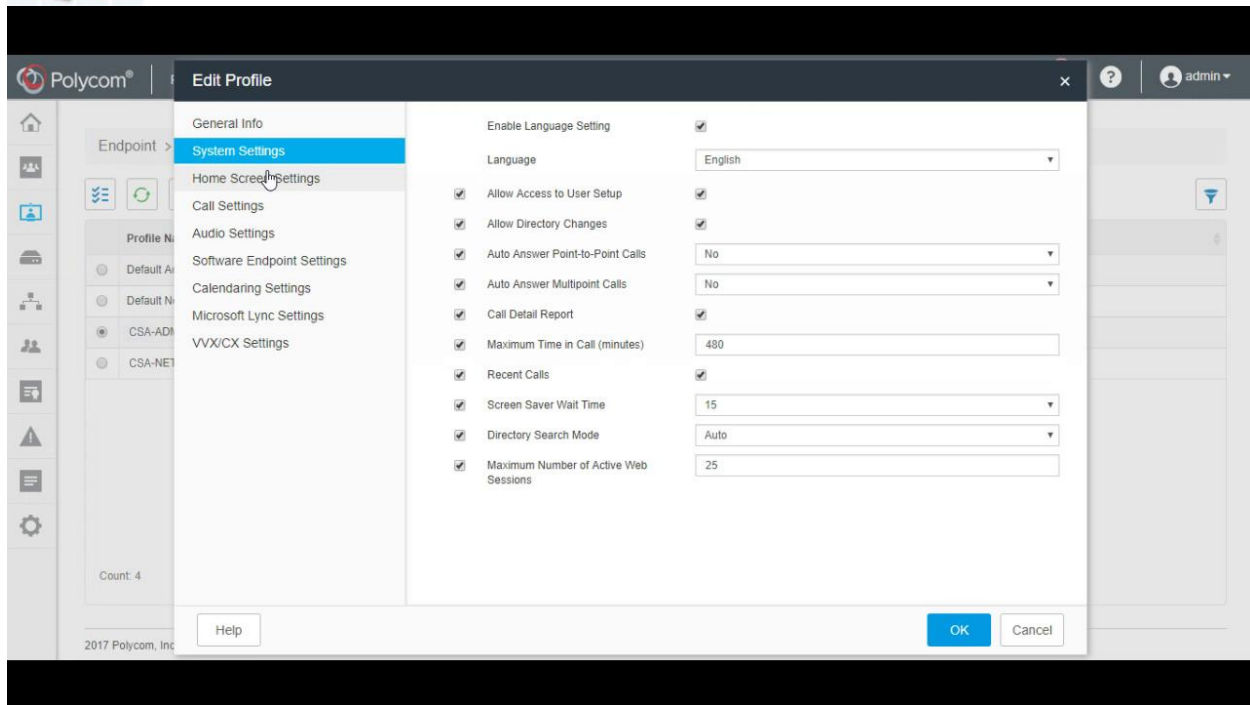


General Info

Name: CSA-ADMIN-PROFILE

Provisioning Profile Type: admin config provisioning profile

Selectable Provisioning for Group Series: checked



System Settings

Enable Language Settings: checked

Allow Access to User Setup: checked

Allow Directory Changes: checked

Auto-answer Point to Point Calls: no

Auto-answer Multipoint calls: no

Call Detail Report: checked

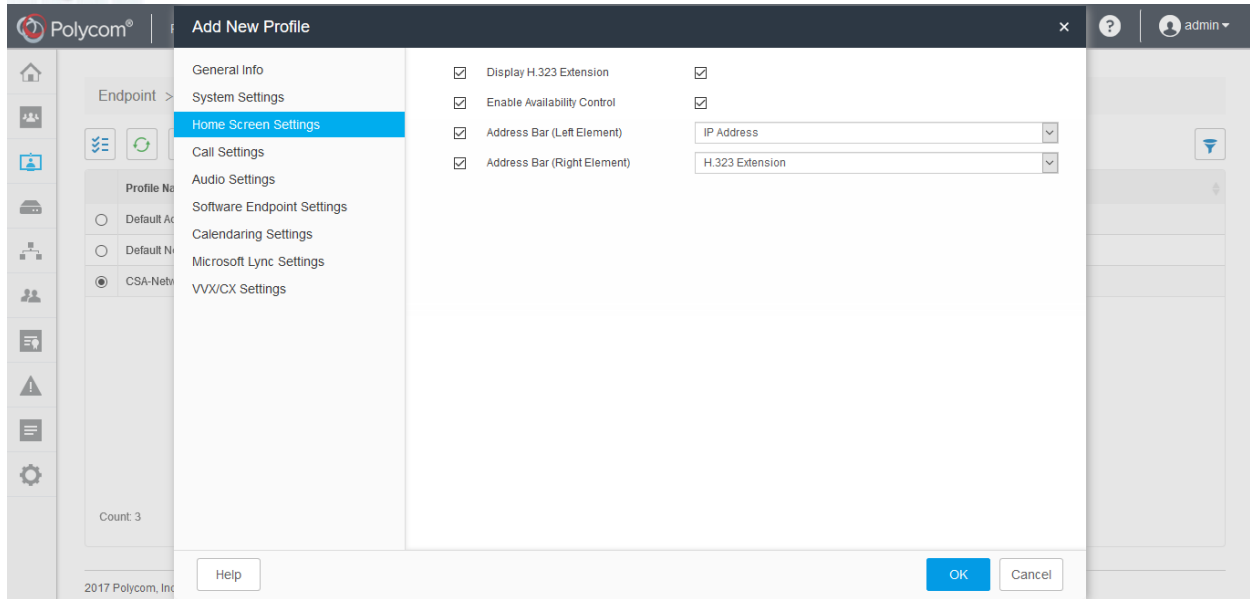
Maximum Time in Call (minutes): 480

Recent Calls: checked

Screen Saver Wait Time: 15

Directory Search Mode: auto

Maximum Number of Active Web Sessions: 25



Home Screen Settings

Display H.323 Extension: checked

Enable Availability Control: checked

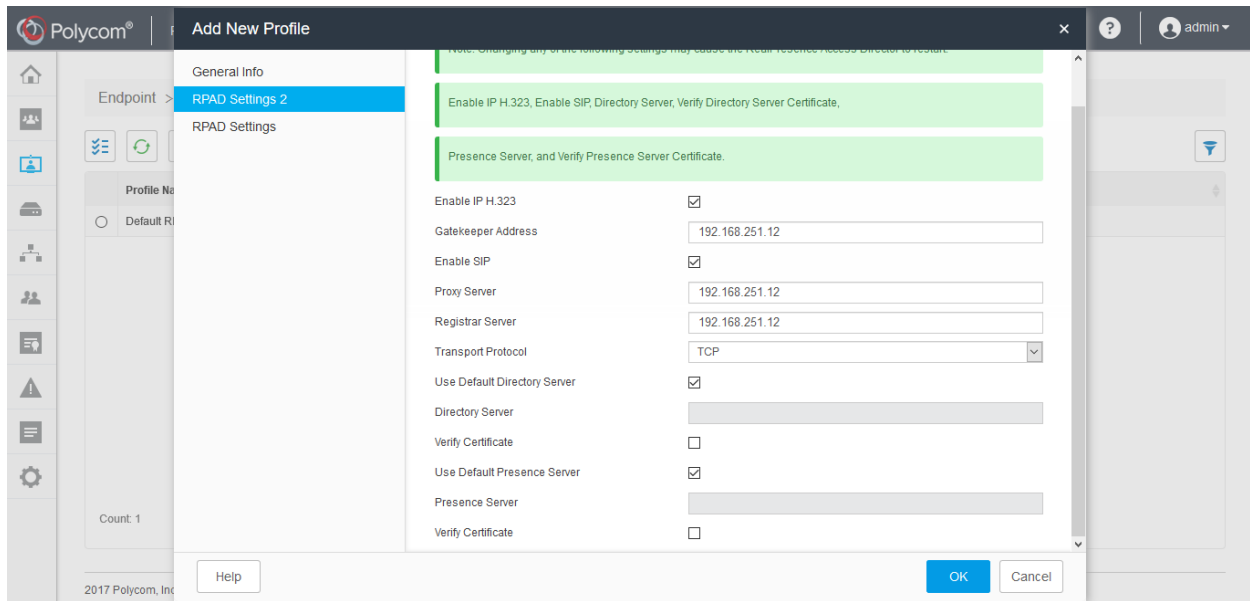
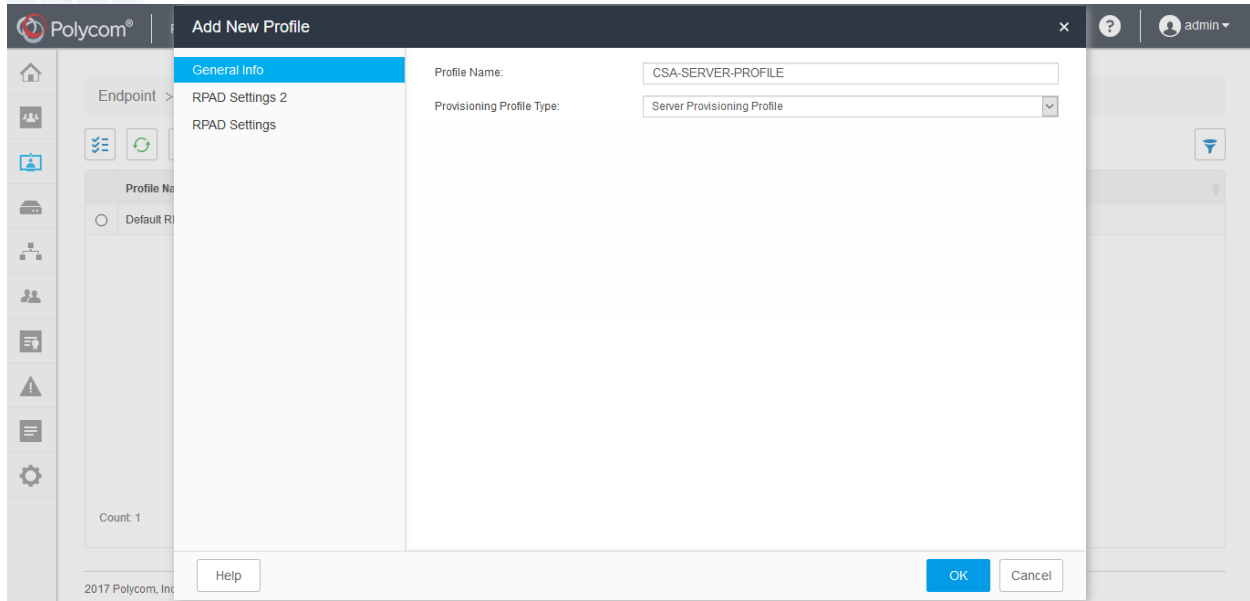
Address Bar (Left Element): ip address

Address Bar (Right Element): h.323 extension

2.1.2.5 Editing RPAD Server Provisioning Profile

You can use a RealPresence Access Director server provisioning profile to dynamically manage the RealPresence Access Director system and configure it with the right network information to allow for firewall traversal in your video infrastructure environment.

You can always create a profile but we have already created a profile with the best possible setting for CSA VC infrastructure. Therefore, in this document we will see how to edit the already created profile by name CSA-SERVER-PROFILE. Server Provisioning setting is found Endpoint->dynamic provisioning->RPAD server provisioning profile.



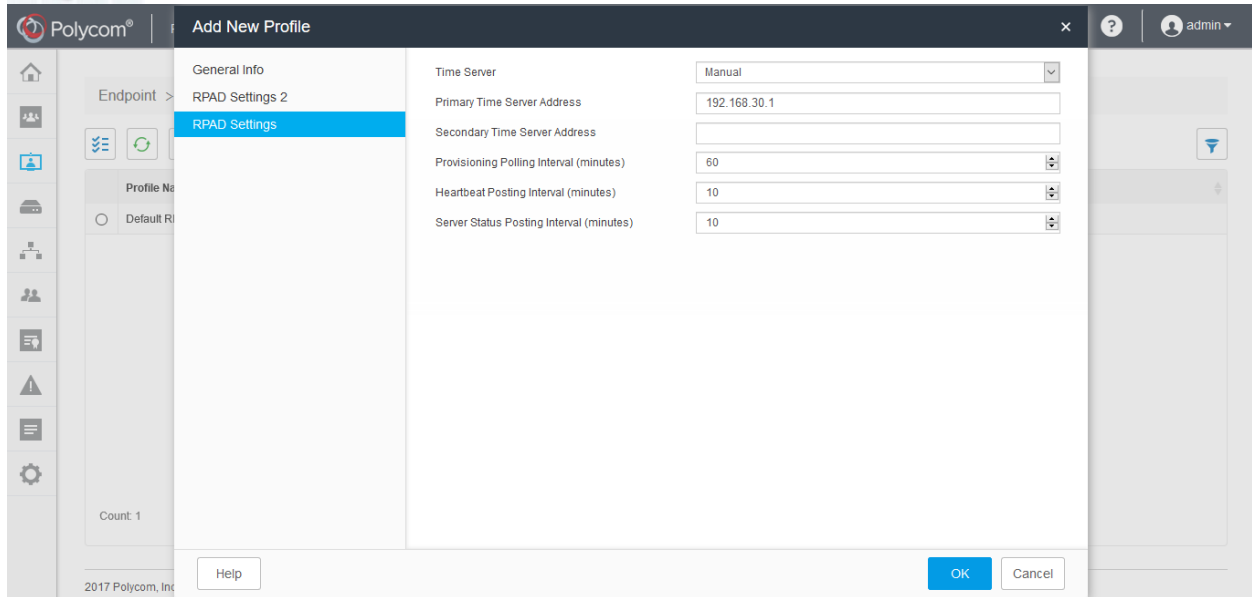
Enable IP H.323: checked

Gatekeeper IP Address: 192.168.251.12

Enable SIP: checked

Proxy Server: 192.168.251.12

Registrar Server: 192.168.251.12



Time Server: Manual

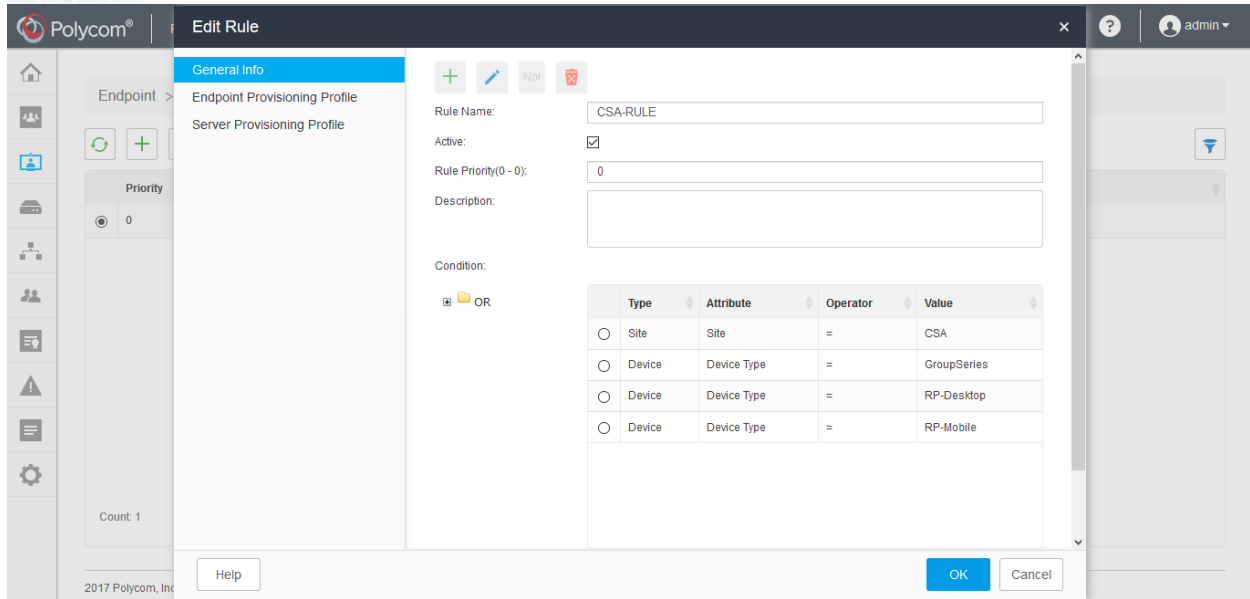
Primary Time Server Address: 192.168.30.1

2.1.2.6 Managing Provisioning Rules

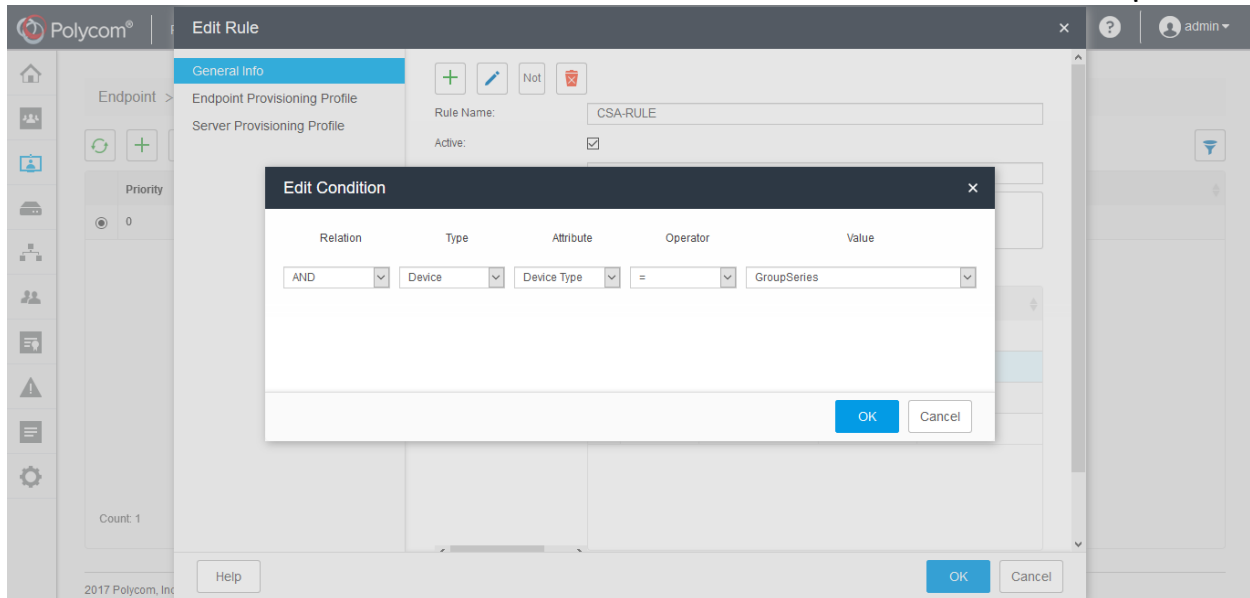
You apply dynamic provisioning profiles by using provisioning rules. A provisioning rule consists of one or more conditions that must be met before the dynamic provisioning profile can be applied. You can create multiple rules and associate a profile with more than one rule at a time. For example, you can use provisioning rules to provision different endpoints within the same site with different network settings. If a dynamically managed endpoint does not meet any conditions of any rule, it is provisioned with the default profiles.

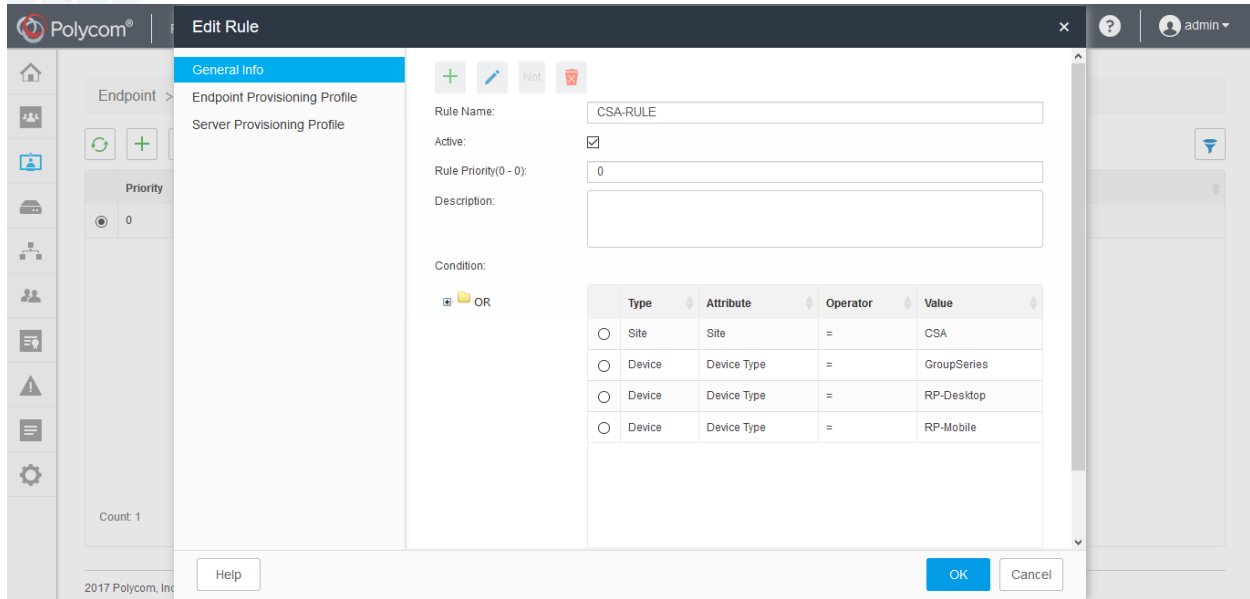
To access the rules go to endpoint->dynamic provisioning->Provisioning Rules

Then you will be redirected to a page that has only one rule by the name CSA-PROVISIONING-RULE. To edit this rule, click on the radio button as shown above and click on the pen icon above the list. It is recommended not to change the setting of the rules unless you have to.



When you click on the edit button, you will be asked if you are sure to edit it and the rule will be deactivated until edit is over. Press ok and proceed.





Rule Name: CSA-RULE

Active: checked

Rule Priority: 0

Condition:

site = CSA or

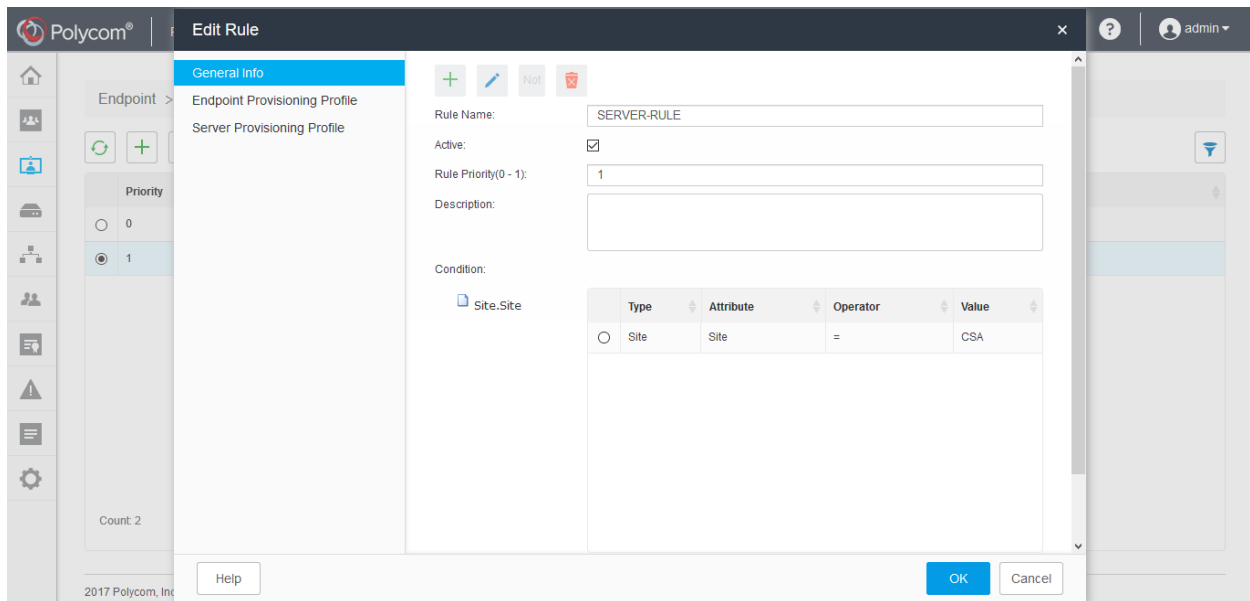
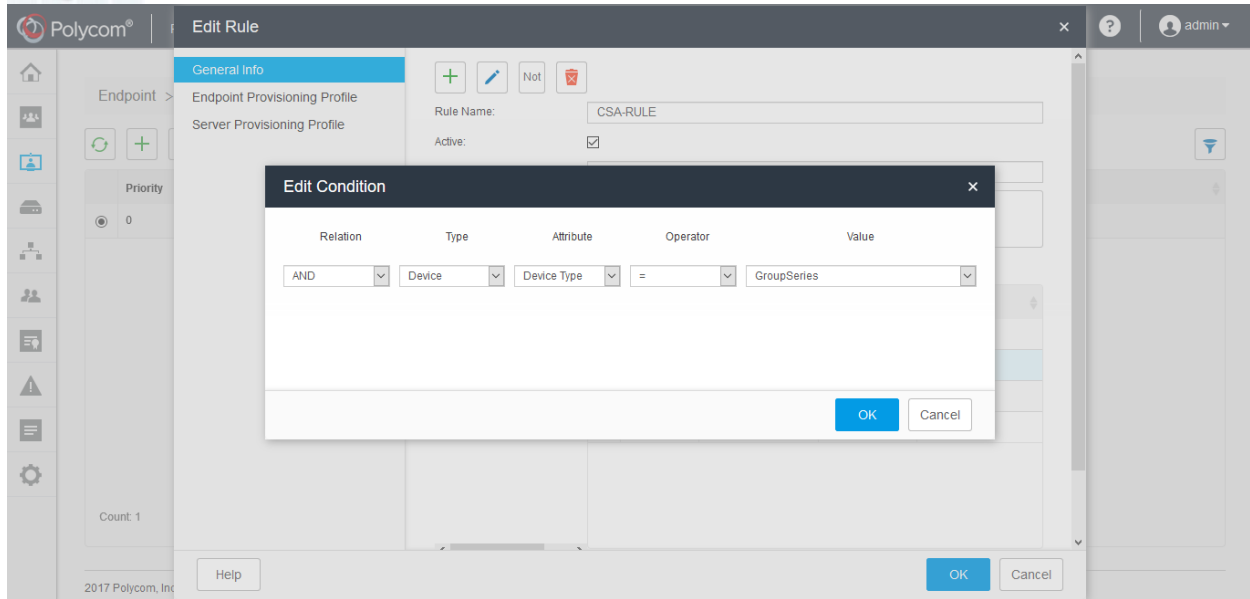
device type = GroupSeries or

device type = RP-Desktop or

device type = RP-Mobile

We have created four conditions for our rule to be applied. The first one checks if the endpoint is inside the CSA site. The other three will check if the endpoints belongs to Polycom Groupseries, Realpresence Desktop or Realpresence Mobile.

You can edit the conditions by clicking on them and the edit button at the top.



Rule Name: SERVER-RULE

Active: checked

Rule Priority: 1

Condition:

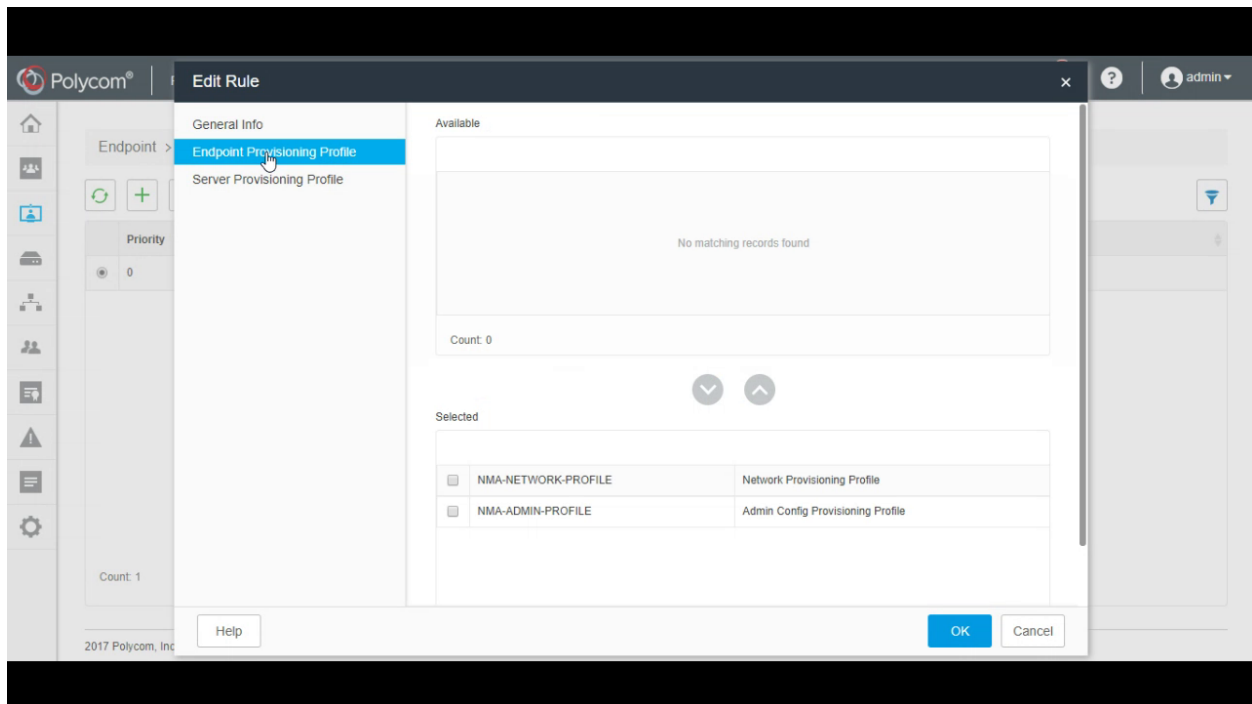
site = CSA

After you have created your condition(s), you need to select which provisioning profiles to associate with this rule. You must have already created the provisioning profiles you need. A provisioning rule must have at least one profile associated with the rule.

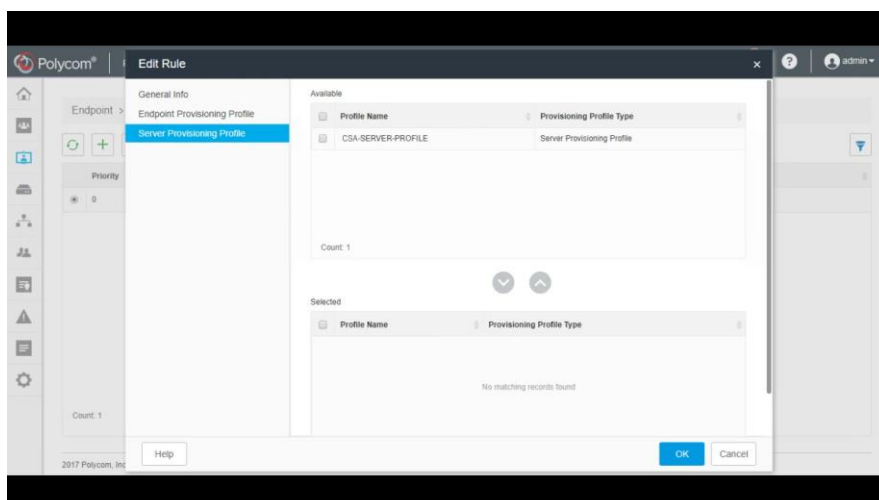


To associate provisioning profiles with a provisioning rule:

1. To associate an endpoint provisioning profile such as a Network Provisioning profile or Admin Config profile, navigate to the Endpoint Provisioning Profile page in the Add New Rule dialog box. You can associate one or more profile to the rule.
2. Select the Available Profiles you want to associate with the rule you created and click the down arrow to move them to the Selected Profiles section. In this example, you can select the HDX system profile, which is an Admin Config provisioning profile.
- 3 You have now finished creating a provisioning rule. Click OK to save the rule.



The same process is applied for server provisioning profile





2.1.2.7 Define an E.164 Address Scheme

You can define an E.164 address scheme that will be used when provisioning E.164 addresses to all dynamically managed endpoints. This E.164 is used as an extension number for H323 calls.

To define an E.164 address scheme for dynamically managed endpoints:

1. Navigate to Endpoint > Dynamic Management > E.164 Numbering.
2. Define your numbering scheme according to the options provided. The administrator has the following options when implementing an E.164 numbering scheme
 - **Select Area:** When areas are enabled, you can select an area to which you want to apply this E.164 numbering scheme. This field is only available to users who manage more than one area. The drop-down list lists only those areas that the user has permission to manage. Users with the administrator role can always select an area when areas are enabled.
 - **Prefix**
 - No Prefix—The system will not append a prefix to create the E.164 assignment.
 - Number —The system appends the prefix specified to create the E.164 assignment.
 - Based on Endpoint Type—The system appends an Endpoint Type prefix to create the E.164 assignment.
 - **Base Field:** You can define a specific number range or indicate that a phone number be used for the Base Field:
 - To specify a Number Range:
 - In the Base Field, select Specify Number Range.
 - Use the To and From fields to define the number range
 - **Suffix:** No Suffix—The system will not append a suffix to create the E.164 assignment.



Polycom® RealPresence® Resource Manager

Endpoint > Dynamic Management > E.164 Numbering

Prefix: Based on Endpoint Type

Endpoint Type	Device Number
RP-Mobile	<input type="text" value="55"/>
ITP	<input type="text" value="77"/>
CX	<input type="text" value="12"/>
RP-Desktop	<input type="text" value="66"/>
CMA-Desktop	<input type="text" value="22"/>
VVX	<input type="text" value="33"/>
RP-Debut	<input type="text" value="88"/>
HDX	<input type="text" value="11"/>
RP-Centro	<input type="text" value="99"/>

2017 Polycom, Inc. 2014-2017. All Rights Reserved.

Polycom® RealPresence® Resource Manager

Endpoint > Dynamic Management > E.164 Numbering

HDX	<input type="text" value="11"/>
RP-Centro	<input type="text" value="99"/>
GroupSeries	<input type="text" value="44"/>

Base Field: Specify Number Range...

From To

Suffix: No Suffix

Total Digits Specified: 6

[Update](#)

2017 Polycom, Inc. 2014-2017. All Rights Reserved.

As you can see above we have selected “44” as our prefix for groupseries devices, so our groupseries endpoints’ extension number start with “44” and polycom desktop “66” followed by four digits in between 1000 and 9999.



2.1.2.8 Managing Instances

An instance is a Polycom video infrastructure component (network device) that runs on a virtual machine or a hardware appliance. When you add a component to the RealPresence Resource Manager system, you can choose to use RealPresence Resource Manager to monitor the alarms, manage licensing for the components, or/and integrate this component with the RealPresence Resource Manager system.

2.1.2.8.1 View Network Device Instance

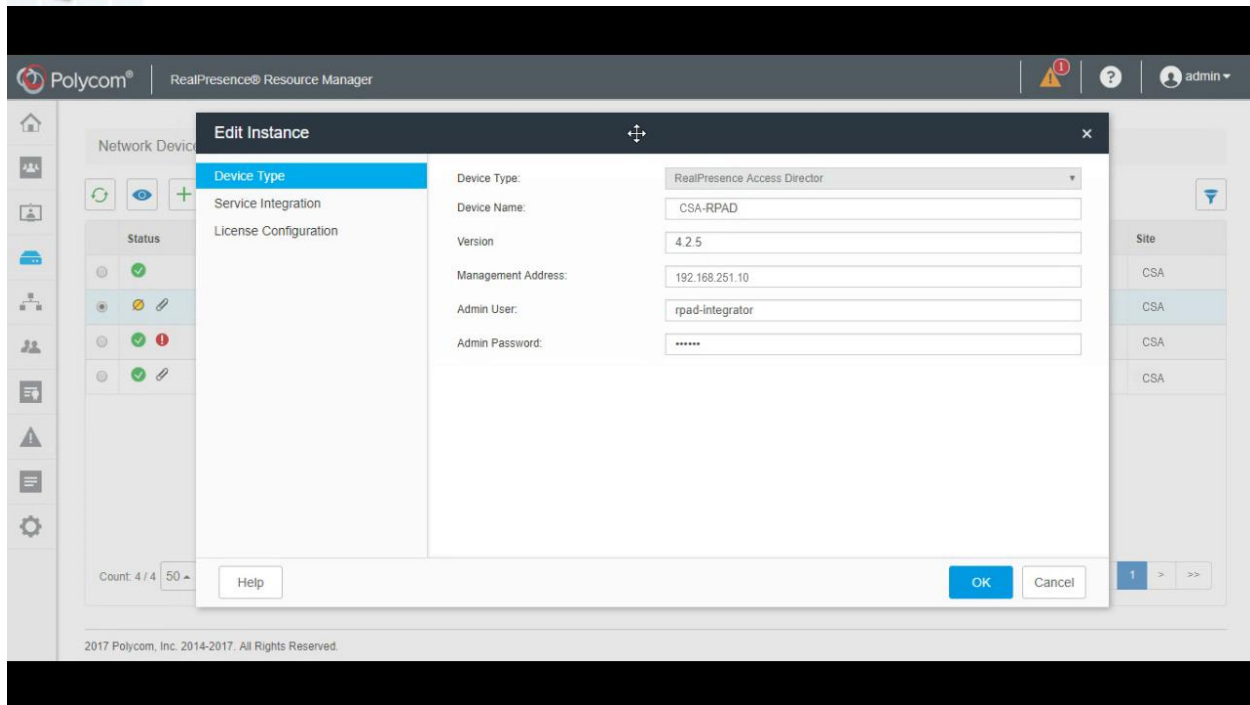
By default, all the instances that you have added are displayed on the Instances page. To view network device instances:

1. Go to Network Device > Instances.
2. Click to filter the instances that you want to display. You can filter instances by Device Type, Device Name, IP Address, or Site.
3. Select an instance that you want to view.
4. Click to display a summary of this instance.

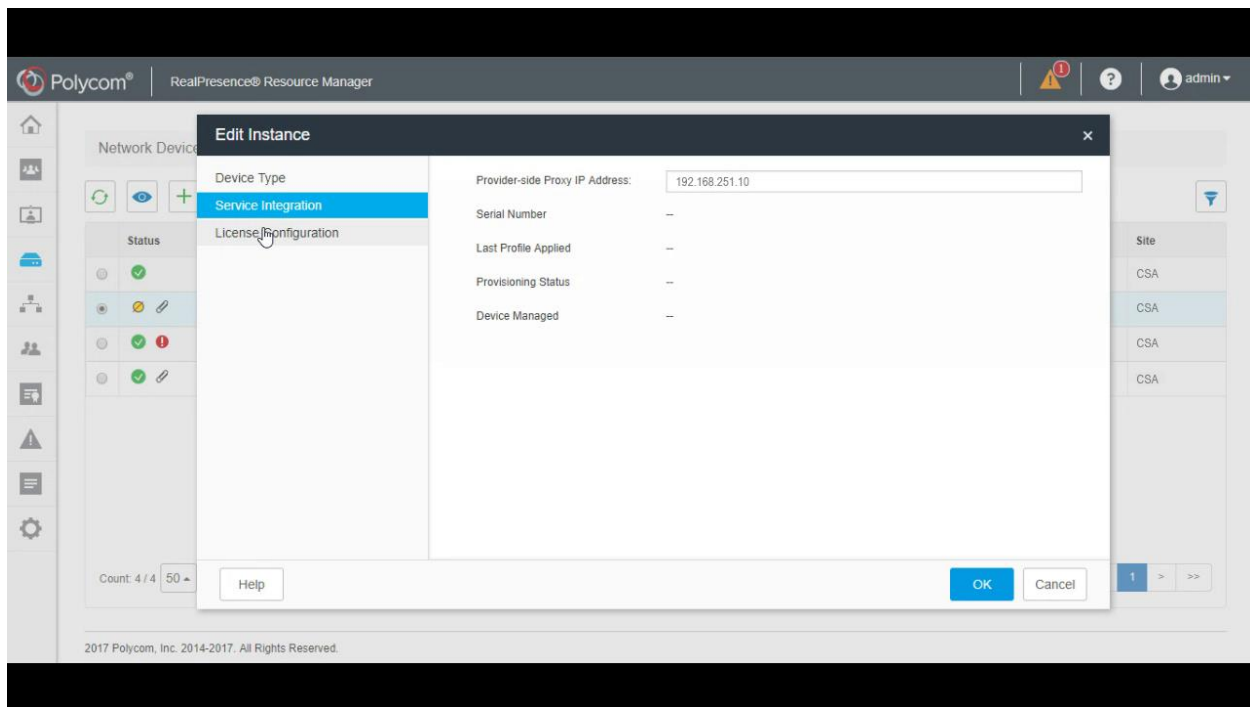
We have integrated the Media Suit, Access-Director and DMA with resource manager to monitor the alarms and manage licensing. The integration process is repetition except the values entered are specific to each server. So here we show you how we added Access Director as a sample.

To add a RealPresence Access Director System by IP address:

1. Ensure your RealPresence Access Director system is reachable via ping.
2. Go to Network Device > Instances and click the plus sign
3. Select RealPresence Access Director as Device Type.
4. Select IP or FQDN Address in the Add By drop-down list.
5. Specify the parameters in the table below
 - **Name:** CSA-RPAD
 - **Version:** 4.2.5
 - **Management Address:** 192.168.251.10
 - **Admin User:** rpad-integrator
 - **Admin Password:** Access Director system user password



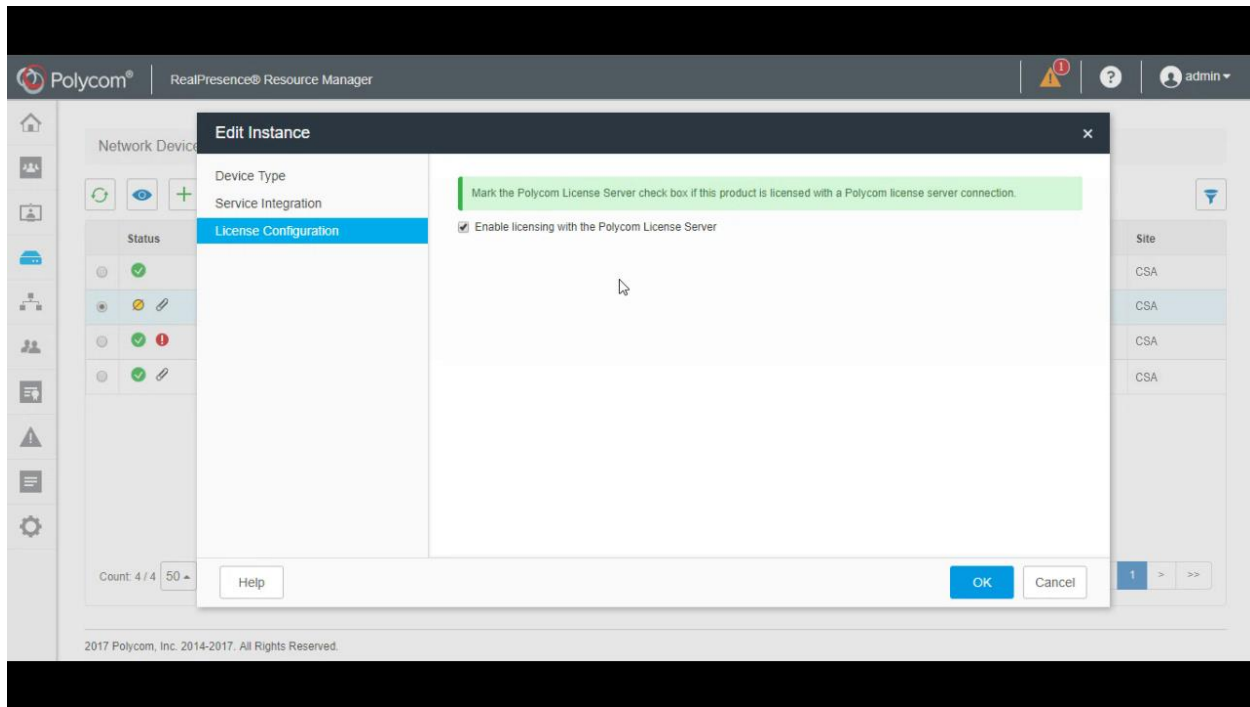
On service integration pane, the setting might vary depending on the server. Refer the admin guide for each server for detailed explanation. On the Access Director server all you need to enter is the internal ip address of the server.



At last on the license configuration pane make sure the “Enable licensing with the polycom license server” is checked ONLY for DMA and Access Director because we use Clariti license

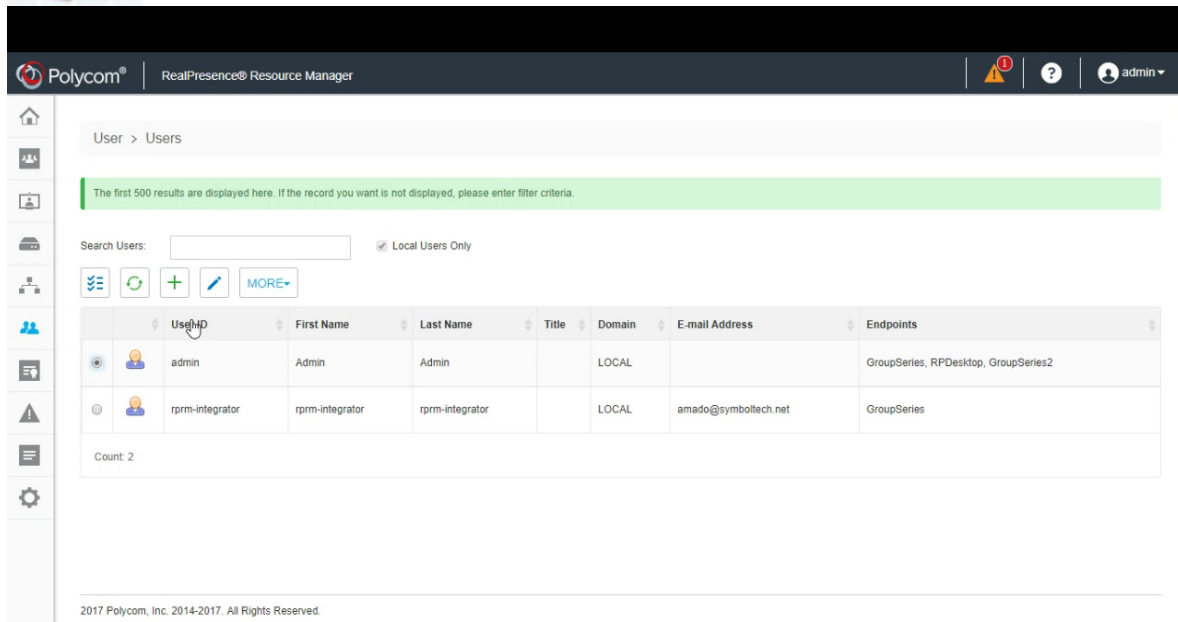


for those servers including the resource manager itself, which needs to connect with Polycom licensing server online. But for the media suit we use base license so this setting has to be unchecked.

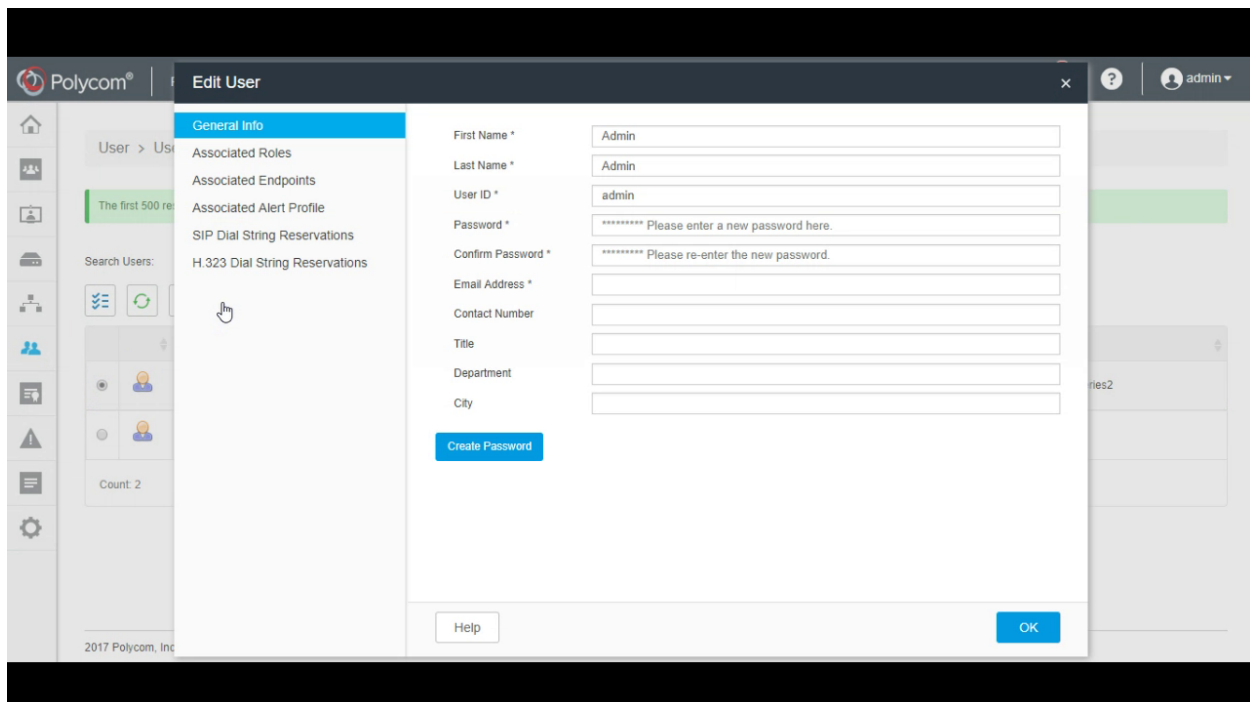


2.1.2.9 Managing users

Creating users is very direct go to User->users and click on the plus icon. However, on this document we discuss on how to manage users that are already created. We have two users named “admin” and “rprm-integrator”. We use “admin” for server configuration and “rprm-integrator” for integration purposes.



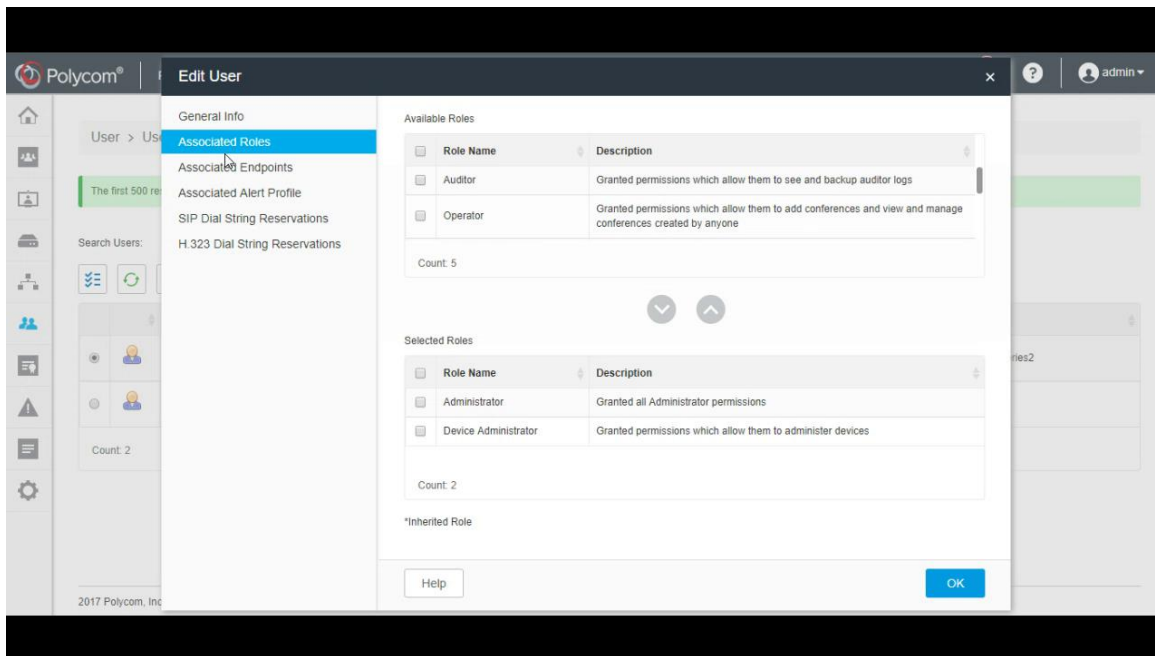
On the first tab of editing a user you will find “General Info” this is where you update the name, password and other information about the user.



On the second tab we have settings related to users role. We can assign six kind of role for the user operator, advanced scheduler, scheduler, view only scheduler, administrator and device administrator. You can find details about each roles on the official administrator guide but for this documentation we see only administrator role and device administrator



role. You can add a role to a user using by selecting the role from the upper list and clicking the down button in between the lists. And vice versa to remove a role.



The Administrator role is for those users who administrate the RealPresence Resource Manager system itself. Users assigned the Administrator role can generally do almost all system functions, however they cannot schedule conferences, monitor conferences, or manage endpoints or other network devices.

The Device Administrator role is for those users who administrate endpoints, bridges, and other network devices. For the areas to which they belong, users assigned the Device Administrator role can:

1. Monitor endpoints, peripherals, and network devices.
2. Add, edit, and delete endpoints and network devices.
3. Provision endpoints using scheduled management.
4. Update endpoints using scheduled management

2.1.3 Managing license

Polycom RealPresence Resource Manager is available as part of Polycom RealPresence Clariti, a Polycom collaboration infrastructure offer that features simplified concurrent user licensing and add-on options. You must use the RealPresence Resource Manager system to license the DMA, Access Director and Media Suit.

Even though you do not have to do the following licensing procedure, it will be helpful to know in the end. To license the resource manager with clarit:



1. go to <https://polycom.flexnetoperations.com> and login with the credentials that were sent by Polycom during license purchase.
2. Create a server for the license by clicking on the create a server link on the side pane. After the license server is successfully created, the View Server page displays your valid License Server ID, ID Type, and Site Name.

You are logged into Central Statistics Agency as Jemal Abdela | Logout

© 2018 Flexera. All rights reserved. [EU Safe Harbor Notice](#)

Field	Value Description
License Server ID	Copy and paste the System Identifier number from the RealPresence [®] Resource Manager License Setup page.
Backup Device	Currently not supported. Leave this field blank.
ID Type	Select PUBLISHER_DEFINED. Note: This is a change from previous versions, which required an ID Type of VM_UUID.
Alias	(Optional) A unique name for your license server. If your organization deploys more than one, aliases make it easier to identify each specific instance.
Site Name	(Optional) A descriptive name for your Polycom RealPresence license management site.

3. After setting up RealPresence Resource Manager as your license server, you must activate the available licenses. You can manage licenses for individual components



of your RealPresence systems after those components have been added to the system. click Map Add-Ons to show a list of available units for features your organization has purchased

You are logged into Central Statistics Agency as Jemal Abdella | Logout

Software & Services
 Home
 Product Search
 Order History
 Search Line Items
 Files Not Downloaded
 Recent Product Releases
 Recent Files Posted
 Recent Email Notifications

Devices
 Search Devices
 Search Servers
 Create Server
 Search Served Clients
 Upload Capability Request

Administration
 Account Administrators
 Allocation Accounts
 Account Members
 Change Password
 Email Preferences
 Product Preferences
 Your Profile

Get Help
 Download Help
 Table of Contents
 FAQs
 Support

Map Add-Ons

Search Add-Ons for Server [4C4C4544-0035-3010-804C-B3C04F4B4832](#)

Activation Code:
 Entitlement ID:
 Add-On Name:
 Feature Name:

Add-On Name	Activation Code	Entitlement	License Term Expiration	Available Units in Line Item	Total Units in Line Item	Qty to Add
SW,2REC,1 LIVE,MEDIA SUITE,PP	C85B-5C1E-125B-AEE4	2100018258-100399015 <small>(295156667)</small>	Permanent	2	2	<input type="text" value="2"/>
CLARIT,USER LIC,PP	D508-2B5F-3A44-CEEE	2100018258-100399015 <small>(295156667)</small>	Permanent	15	15	<input type="text" value="15"/>
CLARIT,ENABLE LIC,PP	A621-8109-B711-0686	2100018258-100399015 <small>(295156667)</small>	Permanent	15	15	<input type="text" value="15"/>
SW,MEDIA SUITE,ENABLE,PP	8496-E175-4F56-FC5A	2100018258-100399015 <small>(295156667)</small>	Permanent	100	100	<input type="text" value="100"/>
SW,PLATINUM,MEDIA SUITE,PP	B7CB-3105-31AD-B434	2100018258-100399015 <small>(295156667)</small>	Permanent	100	100	<input type="text" value="100"/>
SW,CONVERT,SCALABILITY,PP	720C-3759-6E59-32E5	2100018258-100399015 <small>(295156667)</small>	Permanent	100	100	<input type="text" value="100"/>
SW,MEDIA SUITE PRO,PP	C08B-A6E7-39D2-C2C6	2100018258-100399015 <small>(295156667)</small>	Permanent	100	100	<input type="text" value="100"/>
SW_ADD_STREAM,1,MEDIA SUITE,PP	CB87-3A78-3A8C-0F67	2100018258-100399015 <small>(295156667)</small>	Permanent	100	100	<input type="text" value="100"/>
CLARIT,ENCRYP T LIC,TERM	DD57-B4DE-7101-364C	2100018258-100399015 <small>(295156667)</small>	Oct 23, 2018	1	1	<input type="text" value="1"/>

© 2018 Flexera. All rights reserved. [EU Safe Harbor Notice](#)

Please note that since we have mapped all the add-ons for the server already the map add-ons page will be empty. However, to illustrate, it is the same as the remove add-on page except the work “Remove” will be replaced with “Map”.

In the Qty to add column for the available licenses, enter the number to allocate to the RealPresence Resource Manager instance, which is 15 in this case, since CSA bought license for 15 calls.

- Now go to the resource manager license setup page. Select online and click update to finalize the licensing.



The screenshot shows the 'License > Setup' page in the Polycom RealPresence Resource Manager. The page displays the following information:

- System Identifier:** 4C4C4544-0052-3010-8039-C8C04F333832
- Activation Mode:** Online (selected) / Offline
- Status:** License Active (indicated by a green checkmark)

There is a blue 'Update' button below the status information. The footer of the page reads: '2017 Polycom, Inc. 2014-2017. All Rights Reserved.'

once server instance has been created we have to allocate the licenses to their respective servers. To do that go to *License->Allocation*

The screenshot shows the 'License > Allocation' page. It features a table of server instances and their associated capabilities.

Allocate By	Type
RealPresence® RealPresence Access Director™ (1)	CSA-RMS
CSA-RPAD (15 / 15) RealPresence® RealPresence Access Director™ - 192.168.251.10	RealPresence Media Suite™
RealPresence® RealPresence DMA™ (1)	RealPresence Media Suite™
CSA-DMA (15 / 15) RealPresence® RealPresence DMA™ - 192.168.251.12	RealPresence Media Suite™
RealPresence® RealPresence Media Suite™ (1)	RealPresence Media Suite™
CSA-RMS (106 / 106) RealPresence® RealPresence Media Suite™ - 192.168.251.13	RealPresence Media Suite™

CSA-RMS Details:

- Status: online
- Instance Name: CSA-RMS
- Type: RealPresence Media Suite™
- IP Address: 192.168.251.13
- Version: 2.8.0.0
- Service Group: N/A
- Resource Group: Not Available

Allocated Capabilities (3):

- Max Live Streaming Ports for RealPresence Media Suite: 2
- Max Recording Ports for RealPresence Media Suite: 4
- Max Streaming Sessions for RealPresence Media Suite: 100

Other Capabilities(6):

- Base License for RealPresence Media Suite (RPMS): Perpetual License
- PRO Edition Enable for RealPresence Media Suite

A donut chart shows the license usage: 106 Claimed (blue), 0 Available (black), and 0 Reserved for Others (grey).

The footer of the page reads: '2017 Polycom, Inc. 2014-2017. All Rights Reserved.'

Based on CSA’s purchase here the media suit can be licensed for a maximum of 2 Live Streaming ports, 4 recording ports and 100 streaming sessions. You can always reduce this number. Once you are comfortable with the numbers hit save and the licenses will be allocated for the media suit. Follow the same procedure for the other servers except the RPCS in which the licensing is done manually.



2.2 Polycom Realpresence DMA

The Polycom RealPresence DMA system's Conference Manager facilitates multipoint video conferencing. A multipoint video conference is one in which multiple endpoints are connected, with all participants able to see and hear each other. The endpoints connect to a media server (Multipoint Control Unit, or MCU), which processes the audio and video from each and sends the conference audio and video streams back to them. Traditionally, such multipoint conferences had to be scheduled in advance, reserving ports on a specific MCU, in order to ensure the availability of resources. Conference Manager makes this unnecessary. Conference Manager uses advanced routing policies to distribute voice and video calls among multiple MCUs, creating a single virtual resource pool. This greatly simplifies multipoint video conferencing resource management and uses MCU resources more efficiently.

2.2.1 Meta Data

- IP address: 192.168.251.12

2.2.2 Configuration

Please note that if a setting is left unmentioned or not stated explicitly, it means we haven't made any change to the default setting because it wasn't necessary for this particular project. But if you want to dig more about it, you can always refer the official administrator guide.

2.2.2.1 Licensing

A Polycom RealPresence DMA system's license specifies the maximum number of concurrent calls that can touch the system. CSA has bought a license for 15 concurrent calls. CSA is Clariti customer so the DMA's license is managed from the resource manager.

To connect with the resource manager for licensing go to *admin-> server -> license* and select licensing server. Then add the ip address of the resource manager, which is 192.168.251.11, with the default port.



Polycom | RealPresence® DMA®

Monitoring | User | Integrations | Service Config | Reports | Admin | Help | admin

The RealPresence DMA system can be licensed with activation keys or by accessing the Polycom Licensing Server on the RealPresence Resource Manager system.

Activation keys:

Primary key:

DMA system serial number: 34ZMKH2

Licensing server:

License server address: : (default port 3333)

Last successful connection: 192.168.251.11:3333 on 2018-06-01 05:16:53.706 AM

DMA host ID: 34ZMKH2

Active License:

Licensed calls: 15

End User License Agreement:

Status: Accepted

Date accepted: 2018-05-22 10:49:18.308 AM

User: LOCAL\admin from IP address 172.16.13.56

Automatically send usage data:

2.2.2.3 Setup Signaling

Signaling setup includes configuring the following options:

- Enable H.323 signaling so that the Polycom RealPresence DMA system's call server operates as a gatekeeper. Go to *admin -> server -> H323* setting



The screenshot shows the 'H.323 Settings' page. At the top, there is a navigation bar with 'Polycom | RealPresence DMA' and various menu items like 'Monitoring', 'User', 'Integrations', 'Service Config', 'Reports', 'Admin', and 'Help'. A 'Device Authentication' link is visible on the right. Below the navigation bar is a yellow warning box: 'Caution: Changing signaling settings may terminate active calls and conferences involving the type of signaling adjusted.' The main content area has a section for 'Enable H.323 signaling' which is checked. Below this, the status is 'Active'. There are input fields for 'H.225 port:' (1720), 'RAS port:' (1719), and a dropdown for 'Dial plan:' (Default Dial Plan). The 'H.245 open firewall ports:' are set to '36000 to 61000'. There are also checkboxes for 'H.323 multicast' (checked) and 'Enable H.323 device authentication' (unchecked). At the bottom of the settings area are 'Update' and 'Restore Defaults' buttons.

- Enable SIP signaling so that the Polycom RealPresence DMA system's call server operates as a SIP registrar and proxy server. Go to *admin -> server -> sip* setting

The screenshot shows the 'SIP Settings' page. It features the same navigation bar as the H.323 settings page. A yellow warning box is present: 'Caution: Changing signaling settings may terminate active calls and conferences involving the type of signaling adjusted.' The 'Enable SIP signaling' checkbox is checked. Below it, 'Enable ANAT support' is unchecked. There is a 'Ports:' section with a '+', edit, and delete icon. A table lists the configured ports:

Port	Transport	Certificate Authentication	SIP Authentication	Dial Plan	Enabled
5060	UDP/TCP		None	Default Dial Plan	true
5061	TLS	Not required	None	Default Dial Plan	true

At the bottom of the settings area are 'Update' and 'Restore Defaults' buttons.



MCU

Polycorn | RealPresence® DMA®

Monitoring | User | Integrations | Service Config | Reports | Admin | Help

MCUs

MCU Pool Orders | MCU Pools

ACTIONS

- + Add
- Edit
- Delete
- Stop Using
- Busy Out
- Quarantine
- Block Registrations
- View Call History
- View Details

Search

Status and Alarm State	Name	Model	Version	IP Address...	Signaling Type	MCU Pools	Site
Connected Normal	CSA-RP...	Polycorn...	8.7.3.46	192.168...	SIP & H.		CSA
	CSA-RP...	Polycorn...	unknown	192.168...	SIP & H.		CSA

2 MCUs

MCU Info

MCU Name: CSA-RPCS
 Model: Polycorn RMX 1800
 Version: 8.7.3.46
 Aliases: 12
 Address of record:
 Contact address: sip:192.168.251.15:5060
 SIP user name:
 SIP registrar address:
 H.323 registrar address: 192.168.251.12
 Path header:
 SIP peer address:

Status

Capabilities

- MCU can provide conference recording
- Supports SVC conferences
- MCU has entry queues supporting shared number dialing

Device Info

Port Reservations

Topology

Configuration

Polycorn | RealPresence® DMA®

Monitoring | User | Integrations | Service Config | Reports | Admin | Help

Edit MCU: CSA-RPCS

MCU General Settings

Direct Access Settings

Bandwidth and Registration Settings

ISDN Gateway Settings

Postliminary

Name: * CSA-RPCS

Type: Polycorn MCU

Integrate with conference manager

Management IP address: * 192.168.251.14

Admin user ID: * rpcs-integrator

Password: *****

Port Reservations

CIF video ports reserved for non-DMA use: 0

Voice ports reserved for non-DMA use: 0

Cascade-for-size reserved CIF video ports:

Per-conference: 0

Overall: 0

Help OK Cancel

2 MCUs



Polycorn | RealF Edit MCU: CSA-RPCS

MCUs

ACTIONS

- + Add
- Edit
- Delete
- Stop Using
- Busy Out
- Quarantine
- Block Registrations
- View Call History
- View Details

MCU General Settings

Direct Access Settings

Bandwidth and Registration Settings

ISDN Gateway Settings

Postliminary

Enable direct access

IP Addresses

Signaling IP for H.323: 192.168.251.15:1720

Signaling IP for SIP: 192.168.251.15:5060

Transport: UDP

Media IP Addresses

192.168.251.15

Prefix settings

Direct dial-in prefix: 12

Strip prefix:

Help OK Cancel

2 MCUs

Polycorn | RealF Edit MCU: CSA-RPMS

MCUs

ACTIONS

- + Add
- Edit
- Delete
- Quarantine
- Block Registrations
- View Call History
- View Details

MCU General Settings

Direct Access Settings

Bandwidth and Registration Settings

ISDN Gateway Settings

Postliminary

Name: * CSA-RPMS

Type: Other MCU

Integrate with conference manager

Management IP address:

Admin user ID:

Password:

Port Reservations

CIF video ports reserved for non-DMA use: 0

Voice ports reserved for non-DMA use: 0

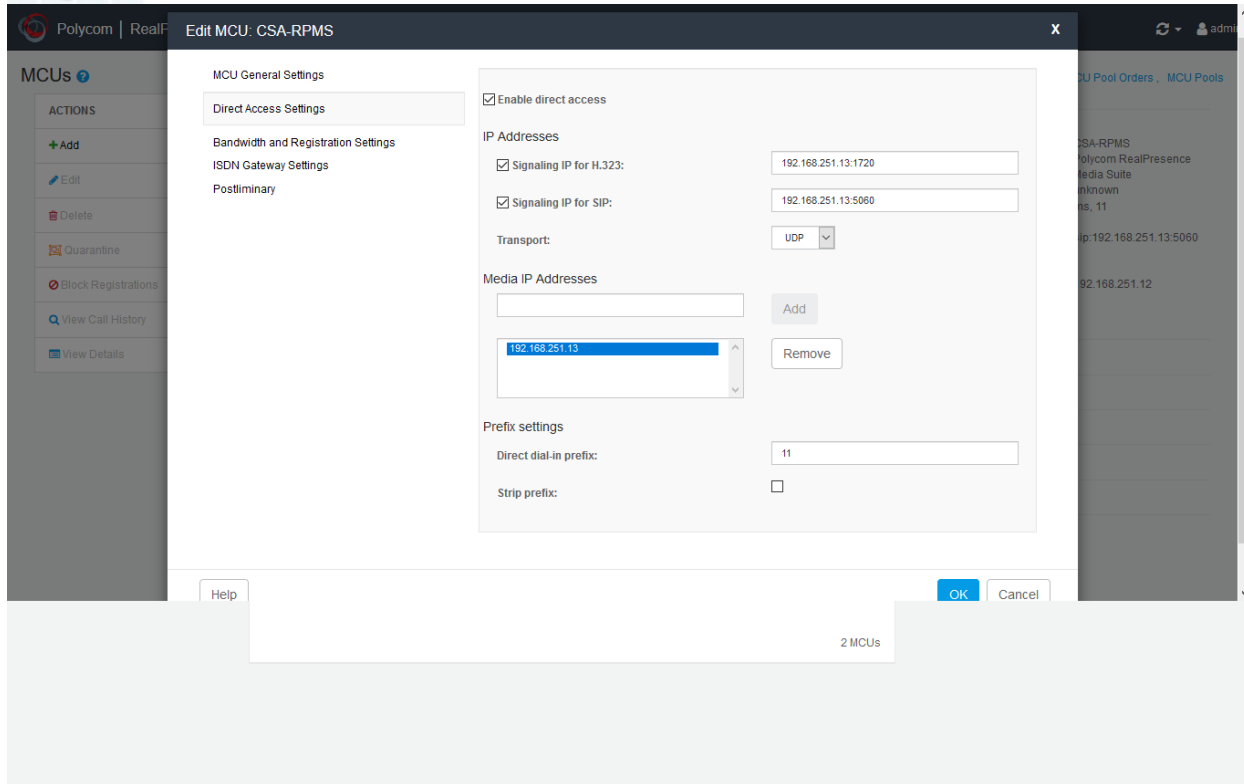
Cascade-for-size reserved CIF video ports:

Per-conference: 0

Overall: 0

Help OK Cancel

2 MCUs



2.3 Polycom Realpresence Media Suit

As a native part of the Polycom RealPresence Platform, the Polycom RealPresence Media Suite could participate in the standards-based video and telepresence calls, and record or live stream the meeting, also could archives, and playback on a variety of client devices including tablets, smartphones, desktop and laptop computers, and standards-based video endpoints. By leveraging RealPresence Media Suite with existing video infrastructure we can easily convert real-time conferences and events into reusable multimedia assets. RealPresence Media Suite:

- Integrates with Polycom endpoints, conference platforms, and other standards-based video endpoints for automated recording and playback.
- Supports SIP and H.323 standards for interoperability with third-party conferencing systems.
- Available with licenses for different recording and streaming ports. Optional licenses can be added for Pro features and Scalability Mode.
- Can output a maximum stream (live or video on demand) of 1080p HD (people+content combined).
- Provides access to live and video call archive streams on devices with compatible browsers including PC, MAC, iOS, and Android devices.
- Enables access to video call archives through any standard-based endpoint.
- Provides REST API support for third-party integrations.



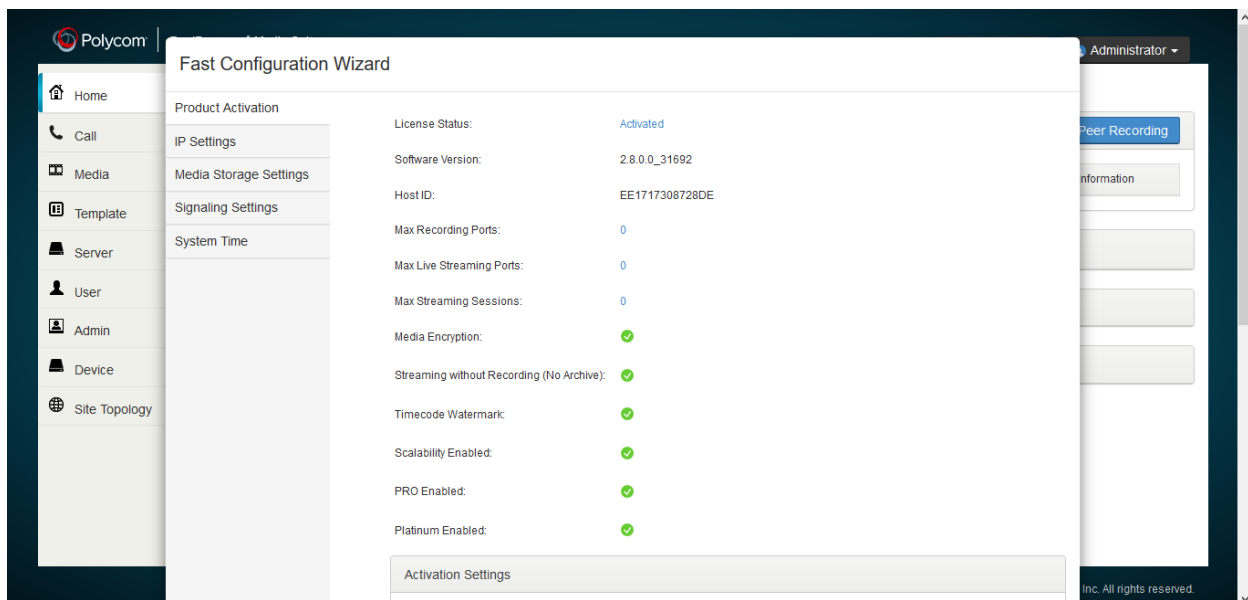
2.3.1 Meta Data

- IP address: 192.168.251.13

2.3.2 Configuration

For administrative tasks use the 192.168.251.13/admin URL but to view recorded videos use just 192.168.251.13 URL with the same web portal credential.

For first-time start up, we can use the RealPresence Media Suite Fast Configuration Wizard to get up and running quickly. If you cannot activate the license, the system will not let you pass the fast wizard. Since our media suit is part of clarity, we can temporarily add an ip address from the console so that we can create an instance on the resource manager for the media suit for licensing purposes. Once we done that the system will be activated. Then the system will be up and running.





Scalability Enabled:

PRO Enabled:

Platinum Enabled:

Activation Settings

Product Activation Mode: Polycom License Server

Polycom License Server Status: Connected

Last Attempt to Connect to Polycom License Server Time: 05-24-2018 08:52:55PM

Last Successful Connection to Polycom License Server Time: 05-24-2018 08:52:55PM

Polycom License Server Address: 192.168.251.11

Polycom License Server Port: 3333

[Sync Up](#)

Product Activation

IP Settings

Media Storage Settings

Signaling Settings

System Time

Enable Network Separation

Network Settings | General System Network Settings

Obtain an IP address automatically using DHCP

Using the following IP address

IP Address:

Subnet Mask:

Default IPv4 Gateway:

Enable IPv6

Enable ICMP Echo

MTU:

LAN Speed:

NAT Public (WAN) Address:



Product Activation

IP Settings

Media Storage Settings

Signaling Settings

System Time

Enable Network Separation

Network Settings General System Network Settings

Hostname: CSA-RMS

Domain: csa.gov.et

FQDN: CSA-RMS.csa.gov.et

Preferred DNS Server: 192.168.0.119

Alternate DNS Server: 192.168.0.53

Route Settings:

<input type="checkbox"/> Destination	Gateway	Subnet Mask	Ethernet
<input type="checkbox"/> 0.0.0.0	192.168.251.1	0.0.0.0	eth0

Add Delete

Cancel Back Next OK

Administrator

Peer Recording

Information

Inc. All rights reserved.

Product Activation

IP Settings

Media Storage Settings

Signaling Settings

System Time

H.323 SIP

Register to Gatekeeper

Gatekeeper Type: Polycom

Primary Gatekeeper: Online

Gatekeeper Address: 192.168.251.12

Gatekeeper Port: 1719

Register User's Information for Gatekeeper:

Gatekeeper User: *

Gatekeeper Password: *

Alternate Gatekeeper:

Gatekeeper Address: *

Gatekeeper Port: 1719

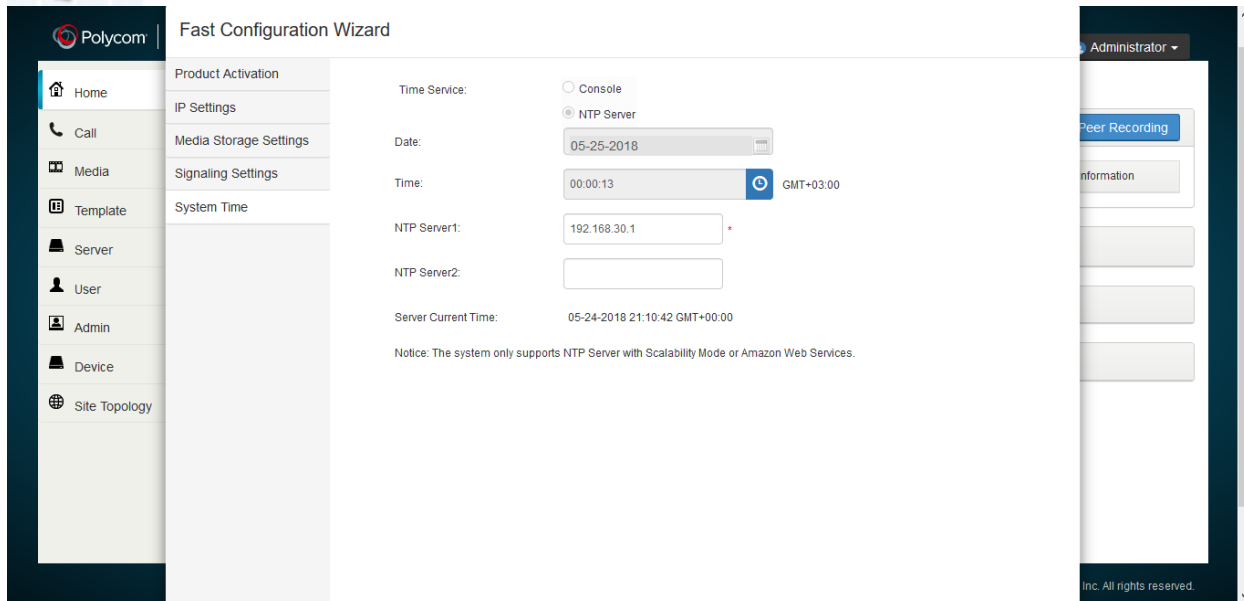
Register User's Information for Gatekeeper:

Administrator

Peer Recording

Information

Inc. All rights reserved.



2.3.2.1 Signaling setting

For H.323 and SIP it is possible to register RealPresence Media Suite to the gatekeeper/ registrar to simplify calling. A gatekeeper/registrar manages functions such as bandwidth control and admission control. A gatekeeper/registrar also handles address translation, which allows you to make calls using static aliases instead of IP addresses that may change each day.

To register the system to a gatekeeper to make H.323 calls:

- Go to Configuration > Signaling Settings > H.323
- Select Register To Gatekeeper
- Configure the settings listed in the following table. After you finish the configuration, click OK



Gatekeeper Type: Polycom

Primary Gatekeeper:

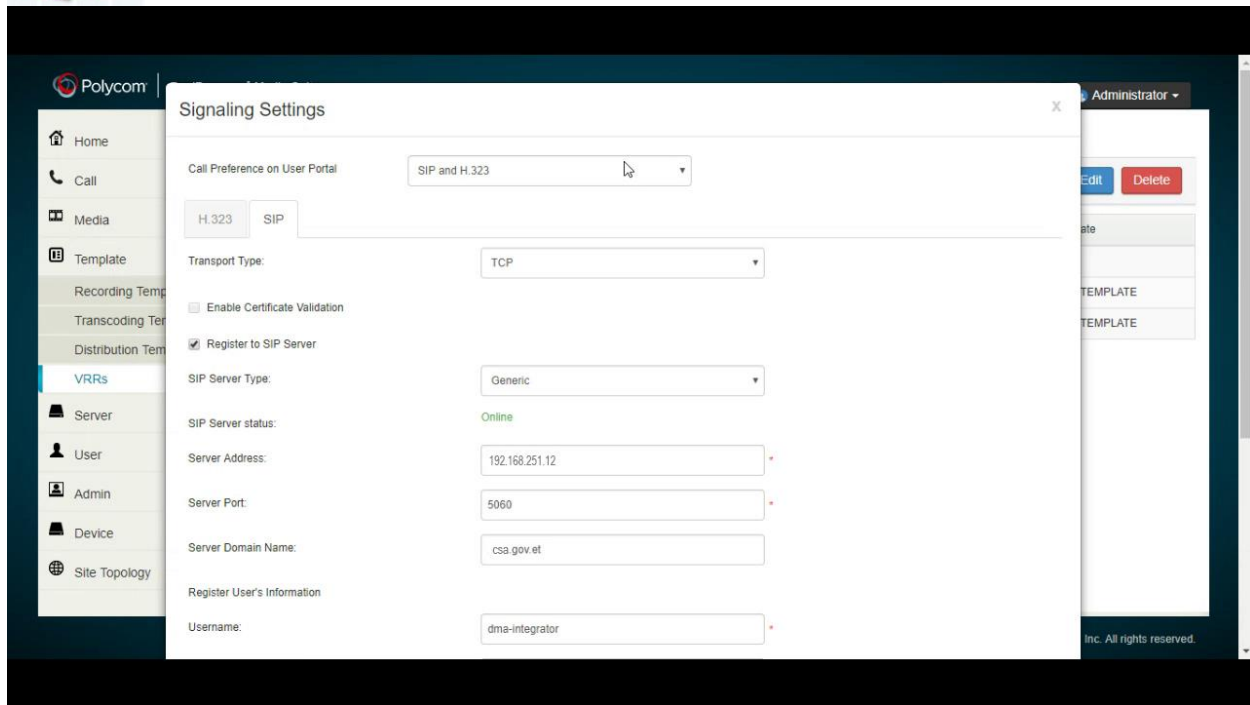
Gatekeeper Address: 192.168.251.12

Gatekeeper Port: 1719

Register User Information for Gatekeeper: unchecked

Gatekeeper User: disabled

Gatekeeper Password: disabled



Transport Type: TCP

Enable Certificate Validation: unchecked

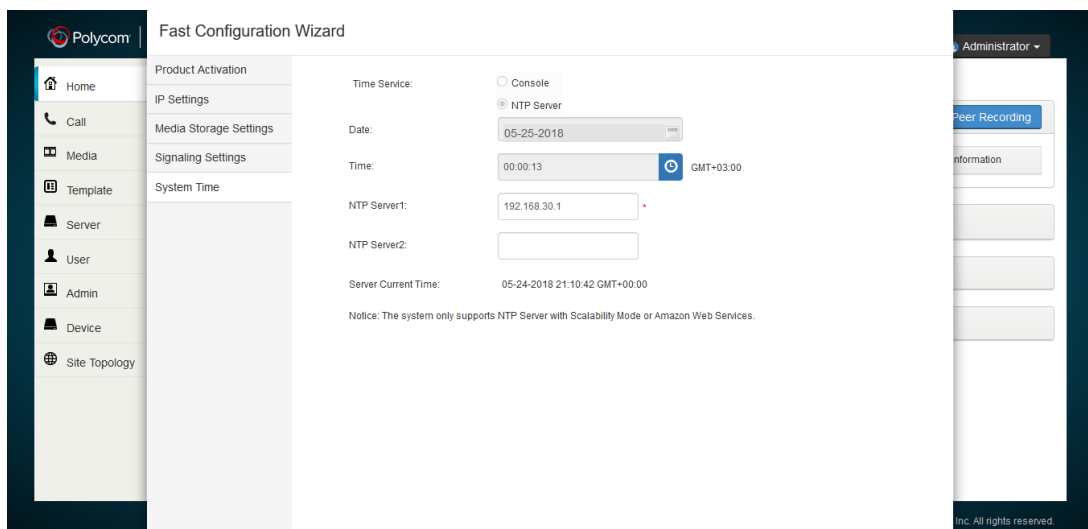
Register to SIP Server: checked

Server Address: 192.168.251.12

Server Port: 5060

Server Domain Name: csa.gov.et

Register User's Information Specify: dma-integrator





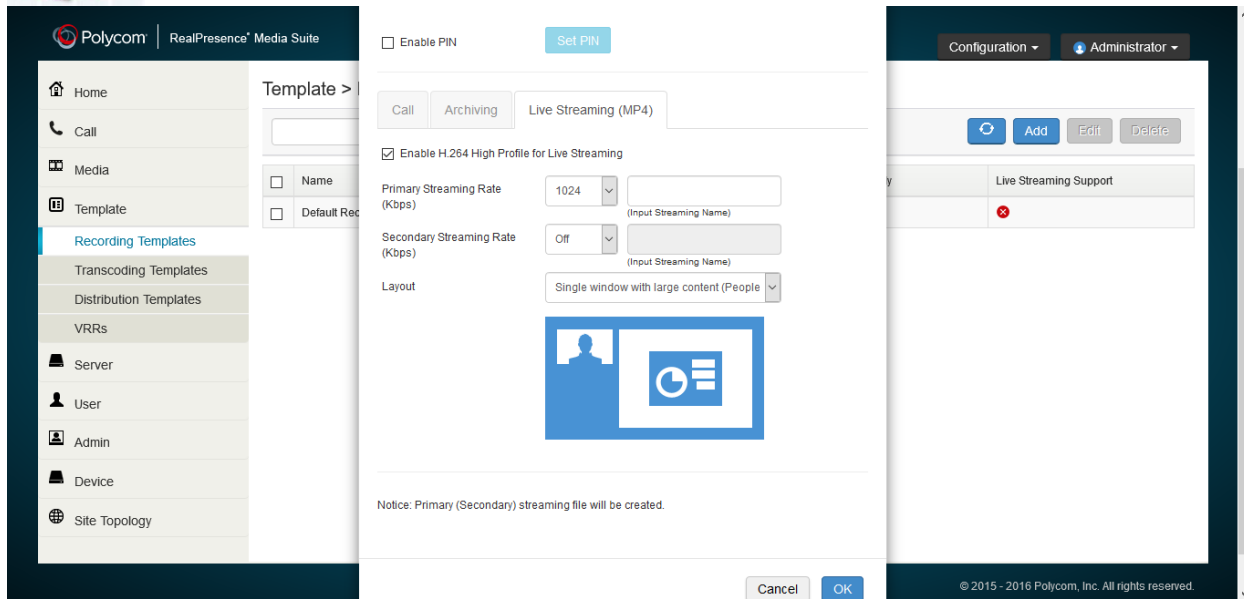
2.3.2.2 Configuring templates

A template is used to define a set of basic recording parameters, such as call rate of recording, video quality, whether to live stream, and streaming rate. All Virtual Recording Rooms (VRR) are created based on templates. Changing the parameters of a template may change the corresponding recording policies of the VRR using that template.

2.3.2.2.1 Recording template

This template is used to define the parameters of the record. Its resolution, call rate and so on. We have created a template called CSA Recording template.

The image displays two screenshots of the Polycom RealPresence Media Suite interface. The top screenshot shows the 'Template >' configuration page for a template named 'CSA-RECORDING-TEMPLATE'. The interface includes a sidebar with navigation options like Home, Call, Media, Template, and Recording Templates. The main configuration area has several sections: 'Template Name' (CSA-RECORDING-TEMPLATE), 'Enable Live Streaming' (checked), 'Disable Recording' (unchecked), 'Enable PIN' (unchecked), 'Call' (selected), 'Archiving', and 'Live Streaming (MP4)'. Below these are settings for 'Max Call Rate (Kbps)' (1024), 'Max Resolution (People)' (1280x720P), 'Enable LPR' (checked), 'Indication Tone' (Off), 'Media Encryption Type' (When Available), 'Max Call Length' (Auto), and 'Conference Layout' (Auto). The bottom screenshot shows the 'Add Recording Template' dialog box, which includes the same template name and settings as the top screenshot, plus 'Start Recording Immediately' (checked) and 'Archive Name Prefix' (CSA_VC). Both screenshots show a 'Live Streaming Support' section with a red 'x' icon and a copyright notice at the bottom: '© 2015 - 2016 Polycom, Inc. All rights reserved.'



Template Name: CSA-RECORDING-TEMPLATE

Enable Live Streaming: checked

Disable Recording: unchecked

Enable PIN: unchecked

Call

Audio Only: unchecked

Max Call Rate: 1024

Max Resolution: 1280x720p

Archiving

Start Recording Immediately: checked

Enable LPR: Once this function is selected, in case of packet loss during network transmission, it can effectively improve the decreased video quality caused by packet loss.

Indication Tone: Indicate that recording is ongoing, and typically the tone is a very short beep with intervals between beeps, measured in seconds. This is enabled by default.

Live Streaming (MP4)

Enable H.264 High Profile for Live Streaming: checked

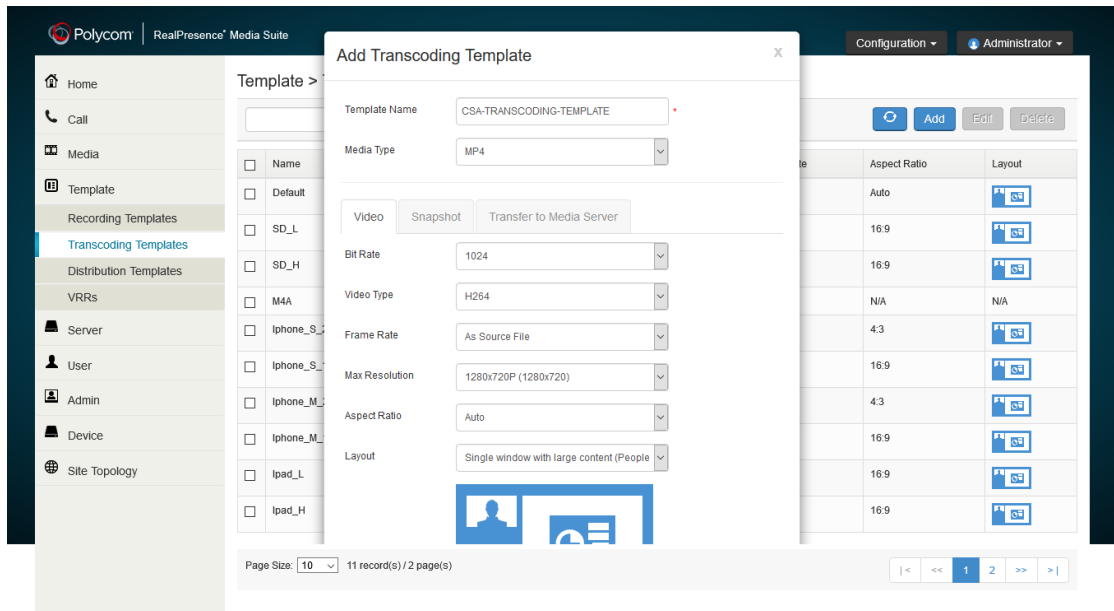
Primary Streaming Rate (Kbps): 1024

Secondary Streaming Rate (Kbps): null



2.3.2.2.2 Transcoding Template

Transcoding template is where you define the format of the video to be recorded and its format detail. We have setup a template called CSA TRANSCODING TEMPLATE with 1024 bit rate, 720p resolution and H.264 high profile video type.



© 2015 - 2016 Polycom, Inc. All rights reserved.

Template Name: CSA-TRANSCODING-TEMPLATE

Media Type: MP4

Video Bit Rate: 1024

Video Type: H254

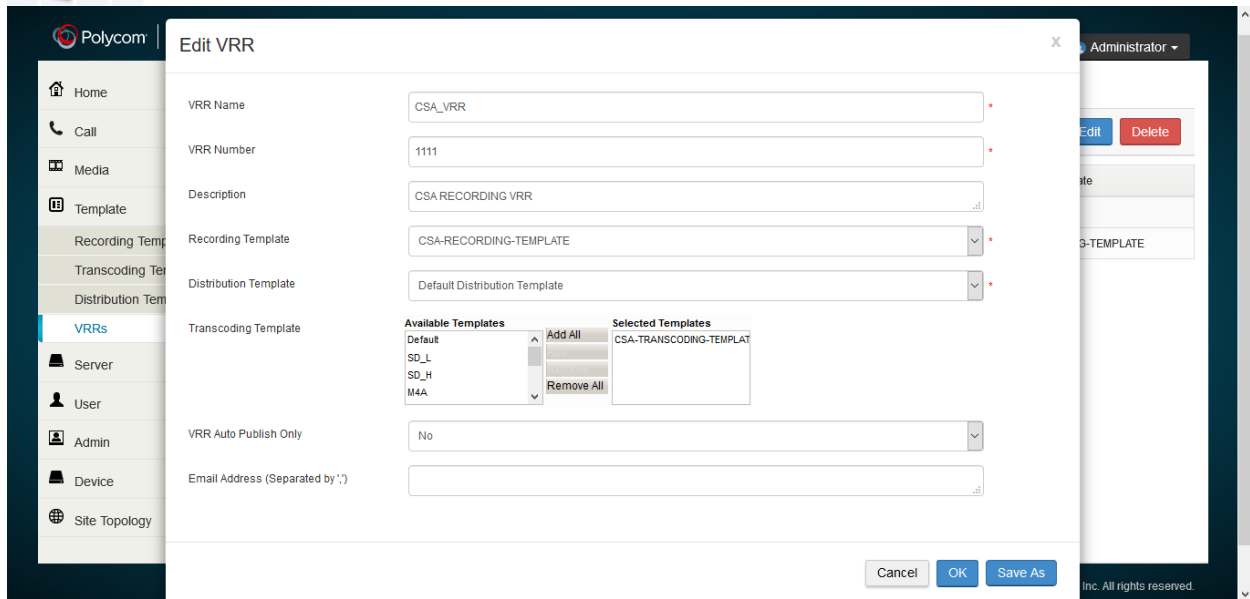
Frame Rate: As source file

Max Resolution: 1280x720p

Aspect Ratio: auto

2.3.2.2.3 VRR template

A VRR defines recording parameters. You can create a VRR basing on recording templates. A VRR is identified by digits, and you can directly start recording using a specified VRR by adding the VRR number to the dial-in number. We have created a template called CSA VRR with dial-in number 111 based on the above recording and transcoding templates



2.3.2.3 Playing Back and Downloading Records

After your conference has been recorded Polycom Realpresence Media Suit can let you play the record either to a specific endpoint or to a virtual meeting room. You can also download the media in 720p or 1080p quality.

To playback the media go to the avatar on the top left and click

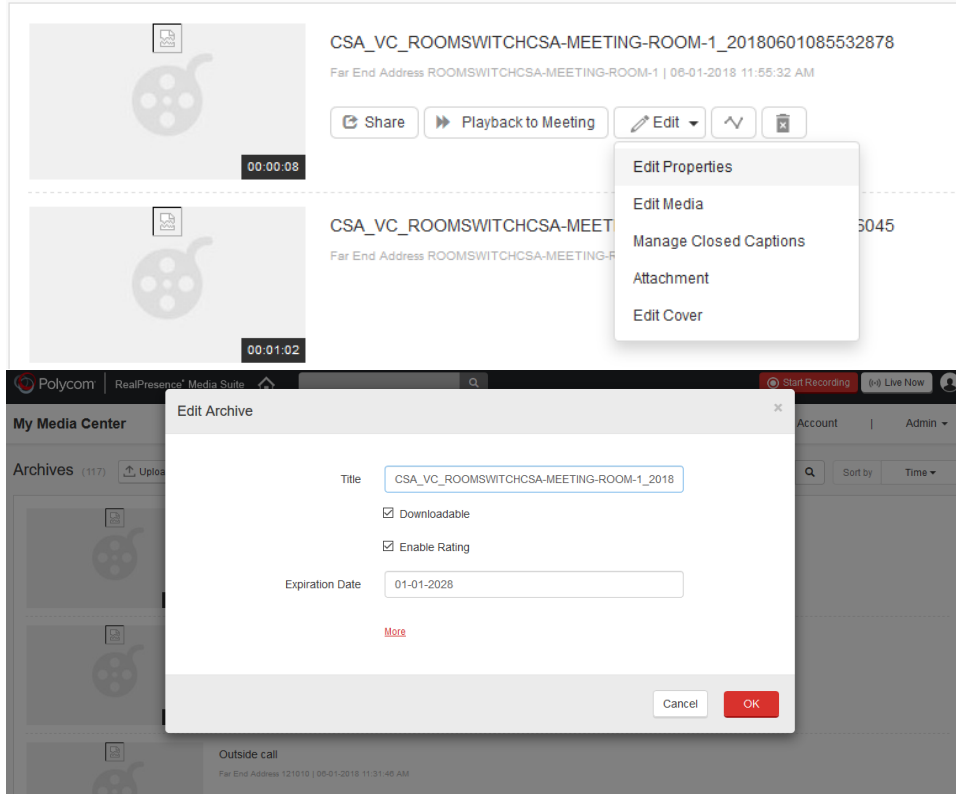


The screenshot shows the Polycom RealPresence Media Suite interface. At the top, there is a navigation bar with 'My Media Center' and tabs for 'Media', 'Events', 'Channel', 'Survey & Test', 'Account', and 'Admin'. Below this is a list of media archives. The first archive is titled 'CSA_VC_ROOMSWITCHCSA-MEETING-ROOM-1_20180601085532678' with a duration of 00:00:08. The second is 'CSA_VC_ROOMSWITCHCSA-MEETING-ROOM-1_20180601083436045' with a duration of 00:01:02. The third is 'Outside call' with a duration of 00:01:04. A 'Start Playback' dialog box is open in the foreground, containing the following fields and options:

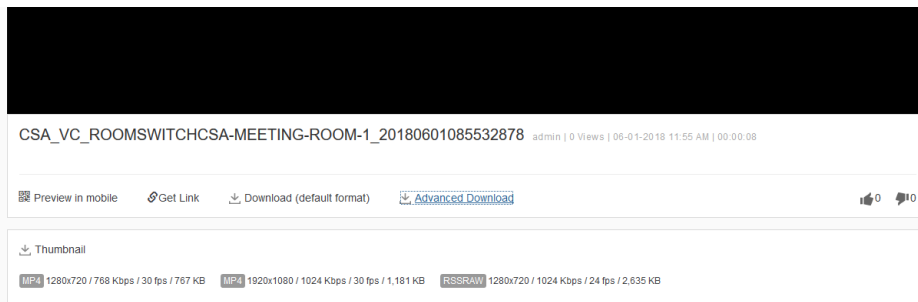
- Meeting Room (or Endpoint): 121010
- Playback: Immediately Manually
- Signaling Type: SIP H.323
- Conference Layout: Auto

Buttons for 'Cancel' and 'OK' are at the bottom of the dialog box.

By default, the media are not downloadable; we have to explicitly make them downloadable



Now you can download the media



2.4 Polycom Collaboration Server 1800

The polycom rmx 1800 multipoint control unit (MCU) is a high performance, scalable, ip network and ISDN solution that provides the user with feature rich and easy to use multipoint voice and video conferencing. It can be controlled via the LAN, by the RMX web client application, using internet explorer installed on the user’s workstation or the RMX manager application.

2.4.1 Meta Data

- IP address: 192.168.251.14



2.4.2 Configuration

The Realpresence Collaboration server alike the others can only be accessed using Internet Explorer or its own RMX manager software which can be downloaded directly from the server. It is highly recommended to use the software.

Just like the Media suit there is a fast configuration wizard that can setup our management interface.

The screenshot shows the 'Management Network Properties' dialog box with the 'IP' tab selected. The configuration includes:

- Network Service Name: Management Network
- IP Version: IPv4
- Control Unit IP Address:
 - IPv4: 192.168.251.14
 - IPv6: (empty)
- Subnet Mask: 255.255.255.0

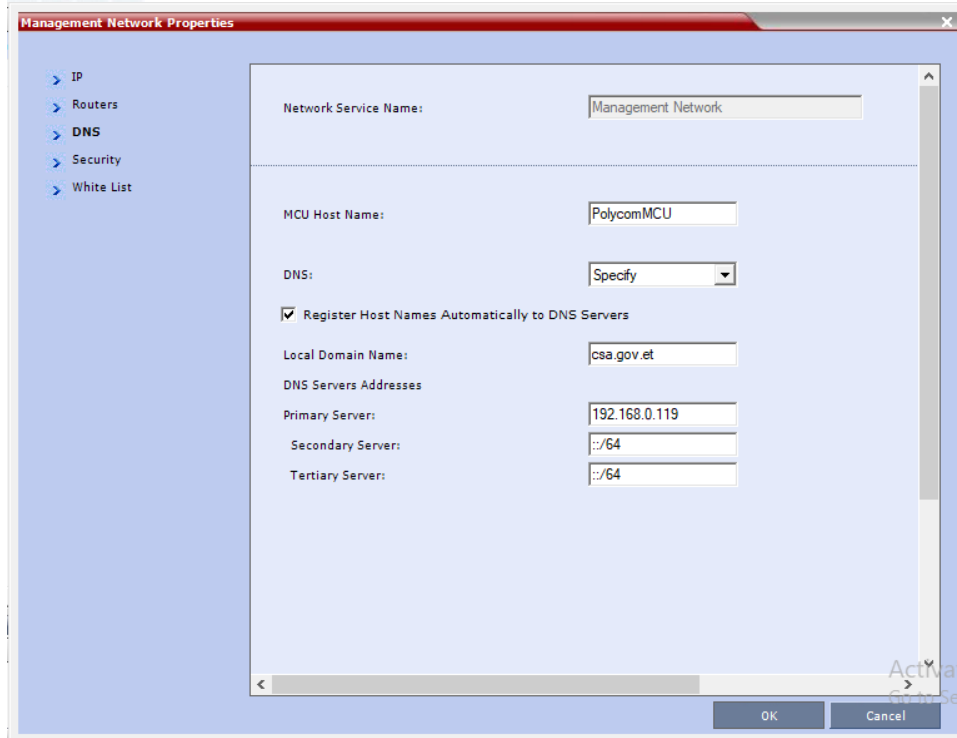
Buttons for 'OK' and 'Cancel' are visible at the bottom right.

The screenshot shows the 'Management Network Properties' dialog box with the 'Routers' tab selected. The configuration includes:

- Network Service Name: Management Network
- Default Router IP Address:
 - IPv4: 192.168.251.1
 - IPv6: (empty)
- Static Routes table:

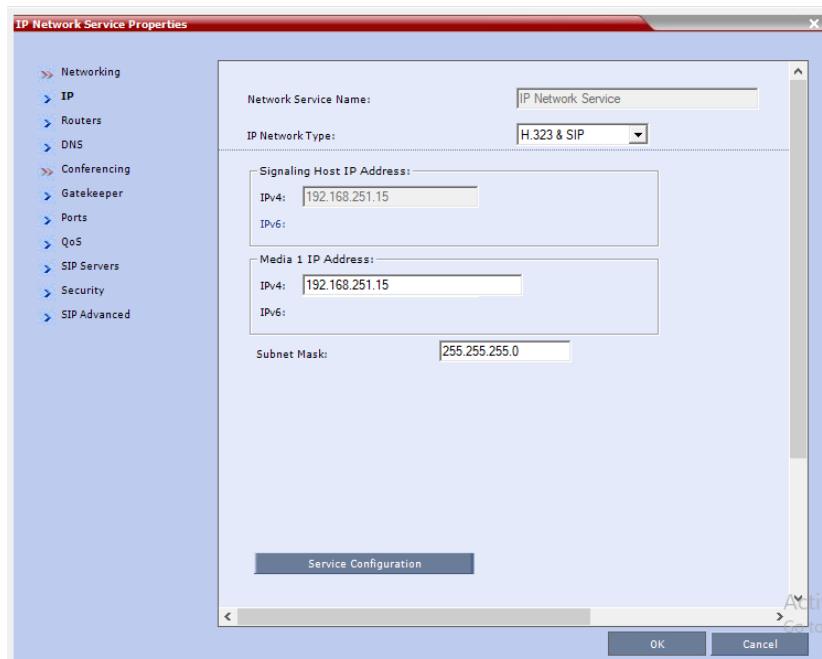
Router IP Address	Remote IP Address	Subnet Mask	Remote Type
0.0.0.0	0.0.0.0	0.0.0.0	Network
0.0.0.0	0.0.0.0	0.0.0.0	Network
0.0.0.0	0.0.0.0	0.0.0.0	Network
0.0.0.0	0.0.0.0	0.0.0.0	Network
0.0.0.0	0.0.0.0	0.0.0.0	Network

Buttons for 'OK' and 'Cancel' are visible at the bottom right.



2.4.2.1 IP network service and properties

The IP service (Conferencing Service) is used to configure and manage communications between the RMX and conferencing devices such as endpoints, gatekeepers, SIP servers, etc. conferencing related definitions such as environment (H.323 or SIP) are also defined in this service. Changes made to any of these parameters only take effect when the RMX is reset. An active alarm is created when changes made to the system have not yet been implemented and the MCU must be reset.





The screenshot shows the 'IP Network Service Properties' dialog box with the 'DNS' tab selected. The left-hand navigation pane shows a tree view with 'DNS' highlighted. The main area contains the following fields:

- Network Service Name: IP Network Service
- IP Network Type: H.323 & SIP
- Service Name (FQDN): PolycomMCU
- DNS: Specify
- Register Host Names Automatically to DNS Servers
- Local Domain Name: csa.gov.et
- DNS Server Address: 192.168.0.119

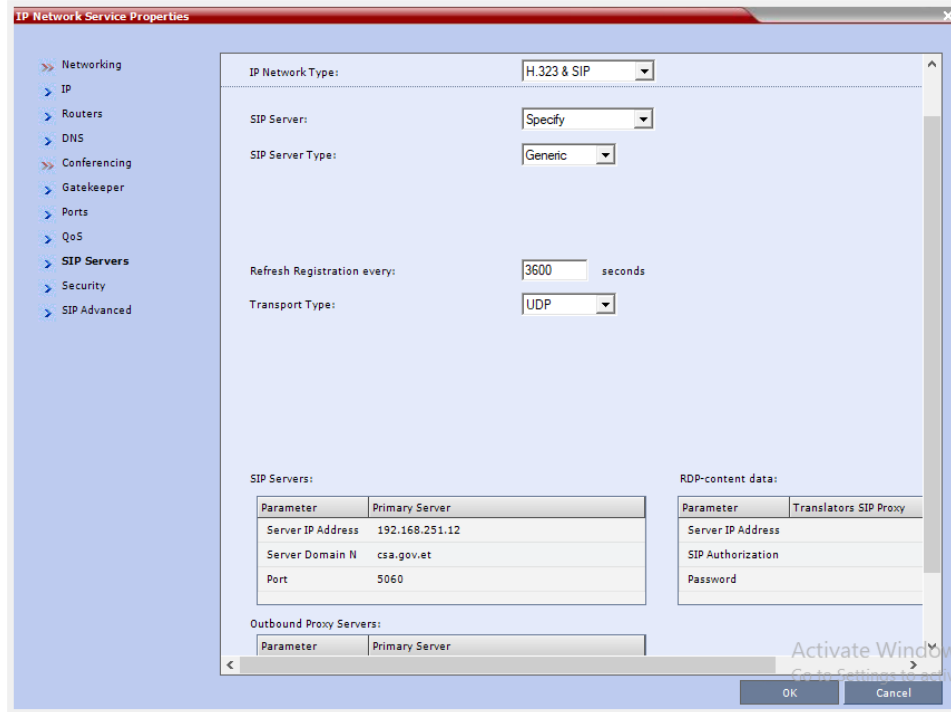
Buttons for 'OK' and 'Cancel' are visible at the bottom right.

The screenshot shows the 'IP Network Service Properties' dialog box with the 'Gatekeeper' tab selected. The left-hand navigation pane shows a tree view with 'Gatekeeper' highlighted. The main area contains the following fields:

- Network Service Name: IP Network Service
- IP Network Type: H.323 & SIP
- Gatekeeper: Specify
- Primary Gatekeeper IP Address or Name: 192.168.251.12
- Backup Gatekeeper IP Address or Name: (empty)
- MCU Prefix in Gatekeeper: 12
- Register as Gateway
- Service Mode: board_hunting
- Refresh Registration every: 120 seconds
- Aliases:

Alias	Type
	None
	None
	None
	None
	None

Buttons for 'OK' and 'Cancel' are visible at the bottom right.



2.4.2.2 IVR services

IVR service is a service that a conference participant gets when he joins the conference and before the conference starts. It guides the participants on what to do next, in other words it is a reception service for the conference room. It only works if it is connected with conference profile which will be explained later.

Out of the services you can configure:

- Choose service language. English is the default
- Customize welcome message
- Customize conference chair person settings



RMX Manager EMA-V8.7.3.1 - MCU selected: 192.168.15.14(192.168.15.14)

Polycom | RMX Manager

View Administration Setup Help RMX IP Address: 192.168.15.14 Signaling Host: 192.168.15.13 MCU Prefix in GC: 99

New Conference IVR Service

- Global
 - Welcome
 - Conference Chairperson
 - Conference Password
 - General
 - Roll Call/Notifications
 - Video Services
 - DTMF Codes
 - Operator Assistance

Conference IVR Service Name:

Language:

External Server Authentication:

Number of User Input Retries:

Timeout for User Input(Sec):

DTMF Delimiter:

100 MCU State: NORMAL

RMX Manager EMA-V8.7.3.1 - MCU selected: 192.168.15.14(192.168.15.14)

Polycom | RMX Manager

View Administration Setup Help RMX IP Address: 192.168.15.14 Signaling Host: 192.168.15.13 MCU Prefix in GC: 99

New Conference IVR Service

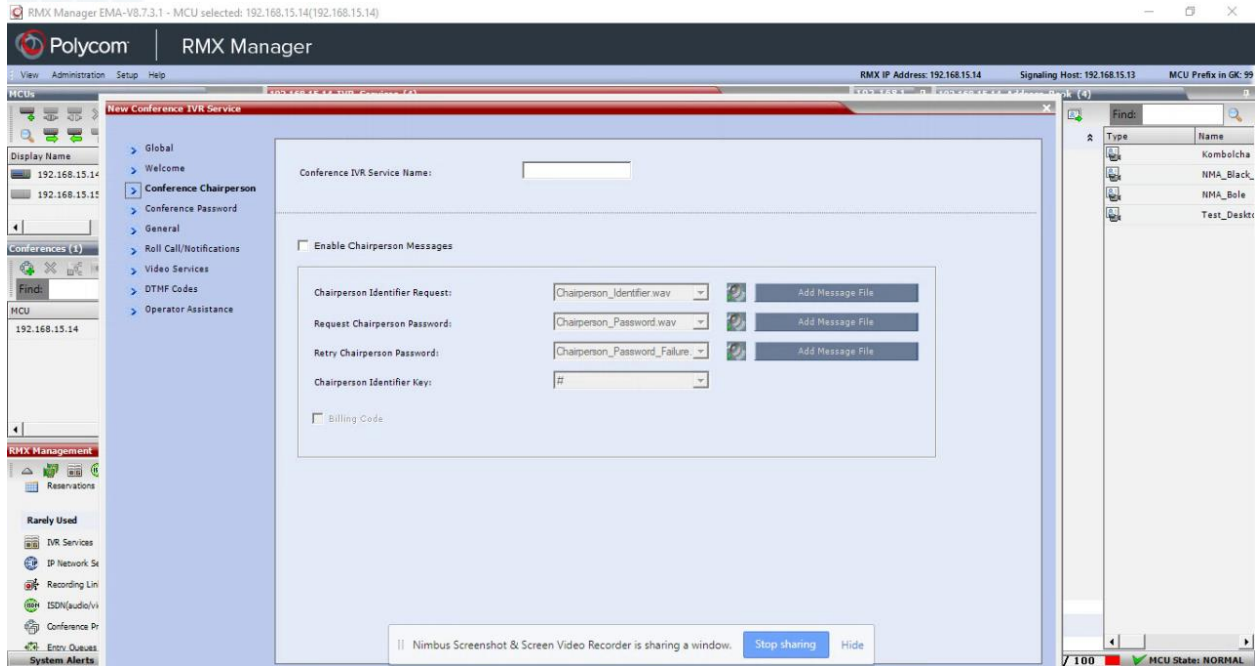
- Global
 - Welcome
 - Conference Chairperson
 - Conference Password
 - General
 - Roll Call/Notifications
 - Video Services
 - DTMF Codes
 - Operator Assistance

Conference IVR Service Name:

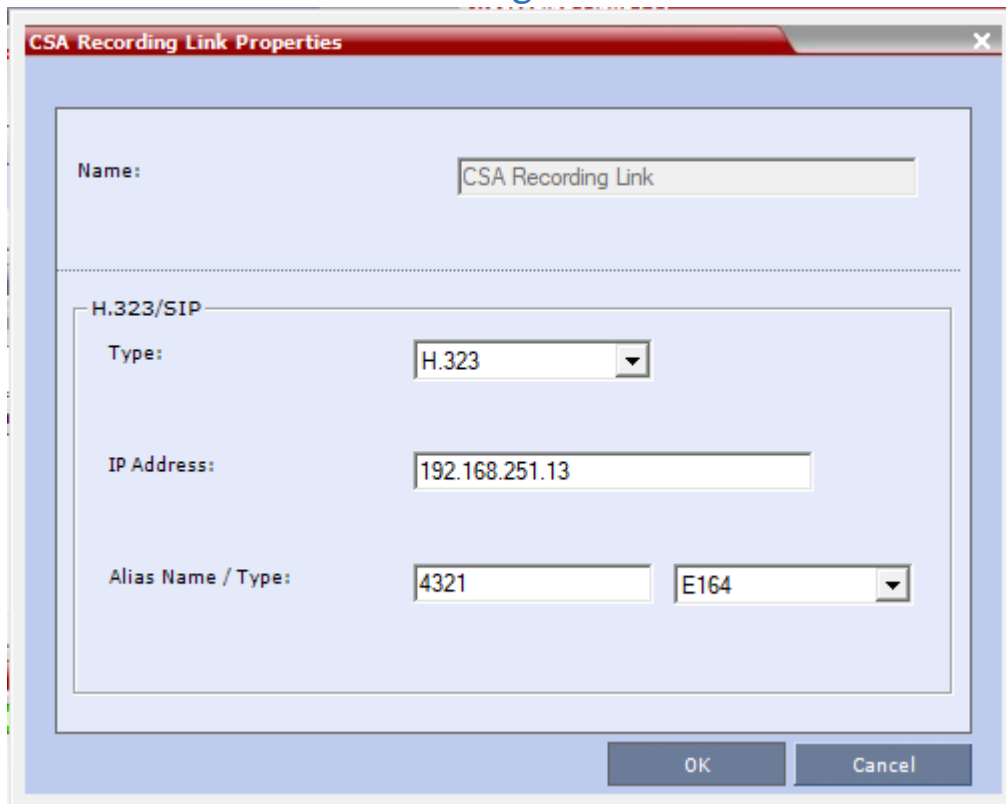
Enable Welcome Messages

General Welcome Message:

100 MCU State: NORMAL



2.4.2.3 Recording link



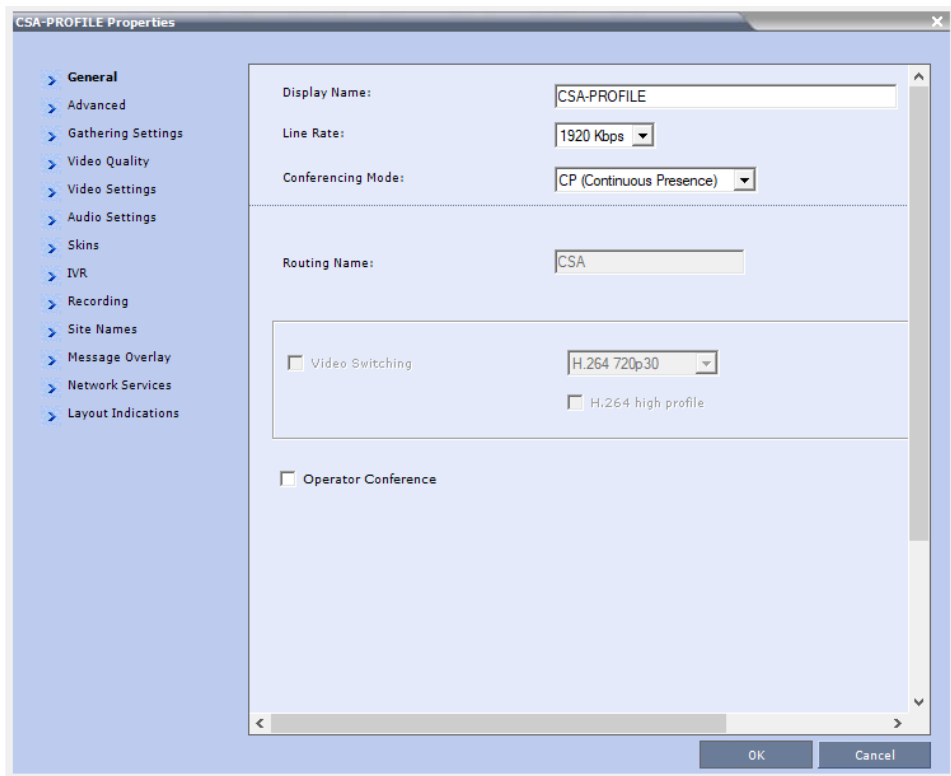


Conference running on the RMX can be recorded using the media suit. This feature is enabled via a recording link, which is a dial-out connection from the conference to the recording system. Recording can start automatically, when the first participant connects to a conference, or on request, when the RMX user initiates it. Each recording link can be associated with one VRR saved on the RMX. The alias that is seen on the above screen shot is the extension number for the virtual room created on the media suit.

2.4.2.4 Conference Profiles

Profiles stored on the MCU enable you to define all types of conferences. Profiles include conference parameters such as conferencing mode, conference session type, conference line rate, people and content resolution and settings, video layout, encryption, lost packet recovery. They are assigned to conferences, meeting rooms, reservations and entry queues.

We have used CP (continuous presence) as our conferencing mode. CP conferencing is based on the CP video protocol and SAC audio protocol. CP conferencing offers high resolution video conferencing with low end to end latency and improved error resiliency without video transcoding by the MCU, hence using less video resources.





CSA-PROFILE Properties

- General
- Advanced**
- Gathering Settings
- Video Quality
- Video Settings
- Audio Settings
- Skins
- IVR
- Recording
- Site Names
- Message Overlay
- Network Services
- Layout Indications

Display Name: CSA-PROFILE

Line Rate: 1920 Kbps

Conferencing Mode: CP (Continuous Presence)

Encryption: No Encryption

Packet Loss Compensation (LPR and DBA)

Auto Terminate

Before First Joins: 10 Minutes

At the End: 0 Minutes

After last participant quits

When last participant remains

Auto Redialing

Exclusive Content Mode

Enable FECC

FW NAT Keep Alive

Interval: 0 Seconds

T10 Compatibility: None

OK Cancel

CSA-PROFILE Properties

- General
- Advanced
- Gathering Settings
- Video Quality
- Video Settings**
- Audio Settings
- Skins
- IVR
- Recording
- Site Names
- Message Overlay
- Network Services
- Layout Indications

Display Name: CSA-PROFILE

Line Rate: 1920 Kbps

Conferencing Mode: CP (Continuous Presence)

Presentation Mode

Same Layout

Lecturer View Switching

Auto Layout

Telepresence Mode:

Telepresence Layout Mode:

Auto Scan Interval(s):

1

OK Cancel



CSA-PROFILE Properties

- General
- Advanced
- Gathering Settings
- Video Quality
- Video Settings
- Audio Settings
- Skins
- IVR
- Recording
- Site Names
- Message Overlay
- Network Services
- Layout Indications

Display Name: CSA-PROFILE

Line Rate: 1920 Kbps

Conferencing Mode: CP (Continuous Presence)

Note: When enabled, Site Names text is displayed without a background.

OK Cancel

CSA-PROFILE Properties

- General
- Advanced
- Gathering Settings
- Video Quality
- Video Settings
- Audio Settings
- Skins
- IVR
- Recording
- Site Names
- Message Overlay
- Network Services
- Layout Indications

Display Name: CSA-PROFILE

Line Rate: 1920 Kbps

Conferencing Mode: CP (Continuous Presence)

Conference IVR Service: Conference IVR Service

Conference Requires Chairperson

Terminate Conference after Chairperson leaves

OK Cancel



CSA-PROFILE Properties

- General
- Advanced
- Gathering Settings
- Video Quality
- Video Settings
- Audio Settings
- Skins
- IVR
- Recording**
- Site Names
- Message Overlay
- Network Services
- Layout Indications

Display Name: CSA-PROFILE

Line Rate: 1920 Kbps

Conferencing Mode: CP (Continuous Presence)

Enable Recording

Dial Out Recording Link: CSA Recording Link

Start Recording: Immediately

Audio Only

Display Recording Icon

Play Recording Message

OK Cancel

CSA-PROFILE Properties

- General
- Advanced
- Gathering Settings
- Video Quality
- Video Settings
- Audio Settings
- Skins
- IVR
- Recording
- Site Names**
- Message Overlay
- Network Services
- Layout Indications

Display Name: CSA-PROFILE

Line Rate: 1920 Kbps

Conferencing Mode: CP (Continuous Presence)

Display Mode: Off

Font Size: 12

Color: AaBbCc

Display Position: Left Top

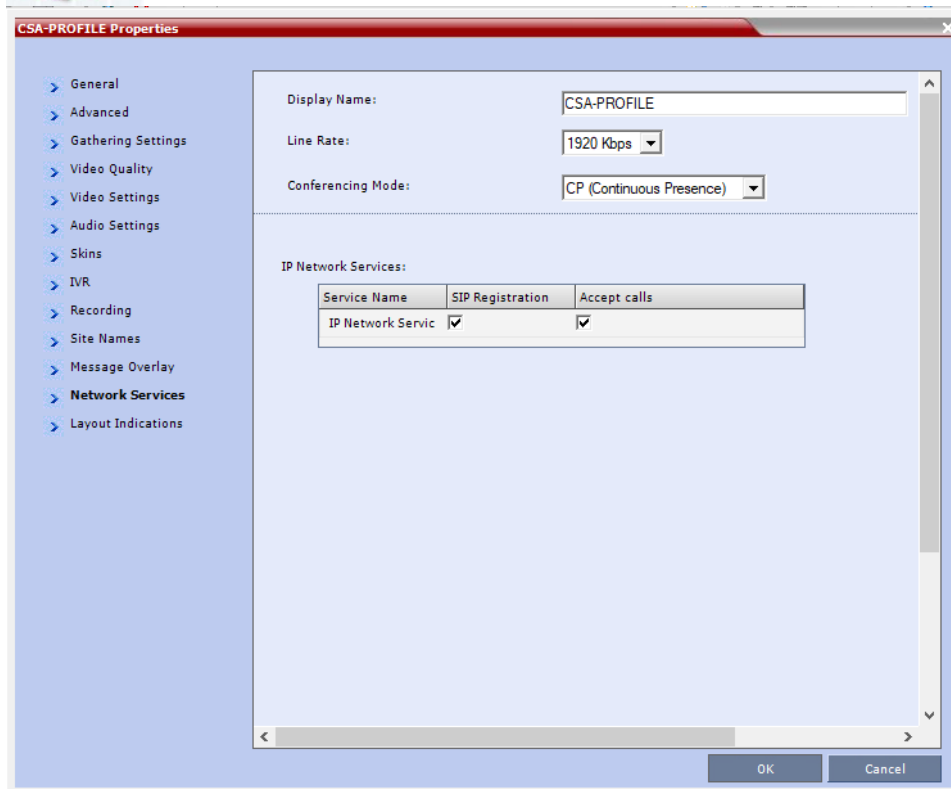
Horizontal Position: 0 50 100

Vertical Position: 0 50 100

Background Transparency: 0 50 100

Preview: AaBbCc

OK Cancel



2.4.2.5 Meeting Rooms

A meeting room is a conference saved on the MCU in passive mode, without using any of the system resources. A meeting room is automatically activated when the first participant dials into it. Meeting rooms can be activated as many as required. Once activated, a meeting room functions as any ongoing conference.

We have configured a three meeting rooms with ID 1010,1011 and 1012 respectively. Any endpoint can dial any of these rooms and can easily start or join already started conference without the need for IT personnel. Note: don't forget to add the prefix extension number "12" of the RMX given by the DMA during dial. For example to dial room 1(ID 1010) dial 121010.

Each room is configured to last for four hours without any interruption and any conference hosted on these rooms will be recorded automatically.



CSA-MEETING-ROOM-1 Properties

- > General
- > Participants
- > Information
- > Media Sources
- > Network Services

Display Name: CSA-MEETING-ROOM-1

Duration: 4 : 00 Permanent Conference

Routing Name: CSA_MEETING

Profile: CSA-PROFILE

ID: 1010

Conference Password:

Chairperson Password:

Reserve Resources for Video Participants: 0

Reserve Resources for Voice Participants: 0

Maximum Number of Participants: Automatic

Enable ISDN(audio/video) Dial-in

ISDN(audio/video) Network Service: [Default Service]

Dial-in Number (1):

Dial-in Number (2):

OK Cancel

You can set the layout of how the conference should look like here but it is best to leave it on auto layout.

CSA-MEETING-ROOM-1 Properties

- > General
- > Participants
- > Information
- > Media Sources
- > Network Services

Display Name: CSA-MEETING-ROOM-1

Duration: 4 : 00 Permanent Conference

Override layout from profile

Auto Layout

1

2

3

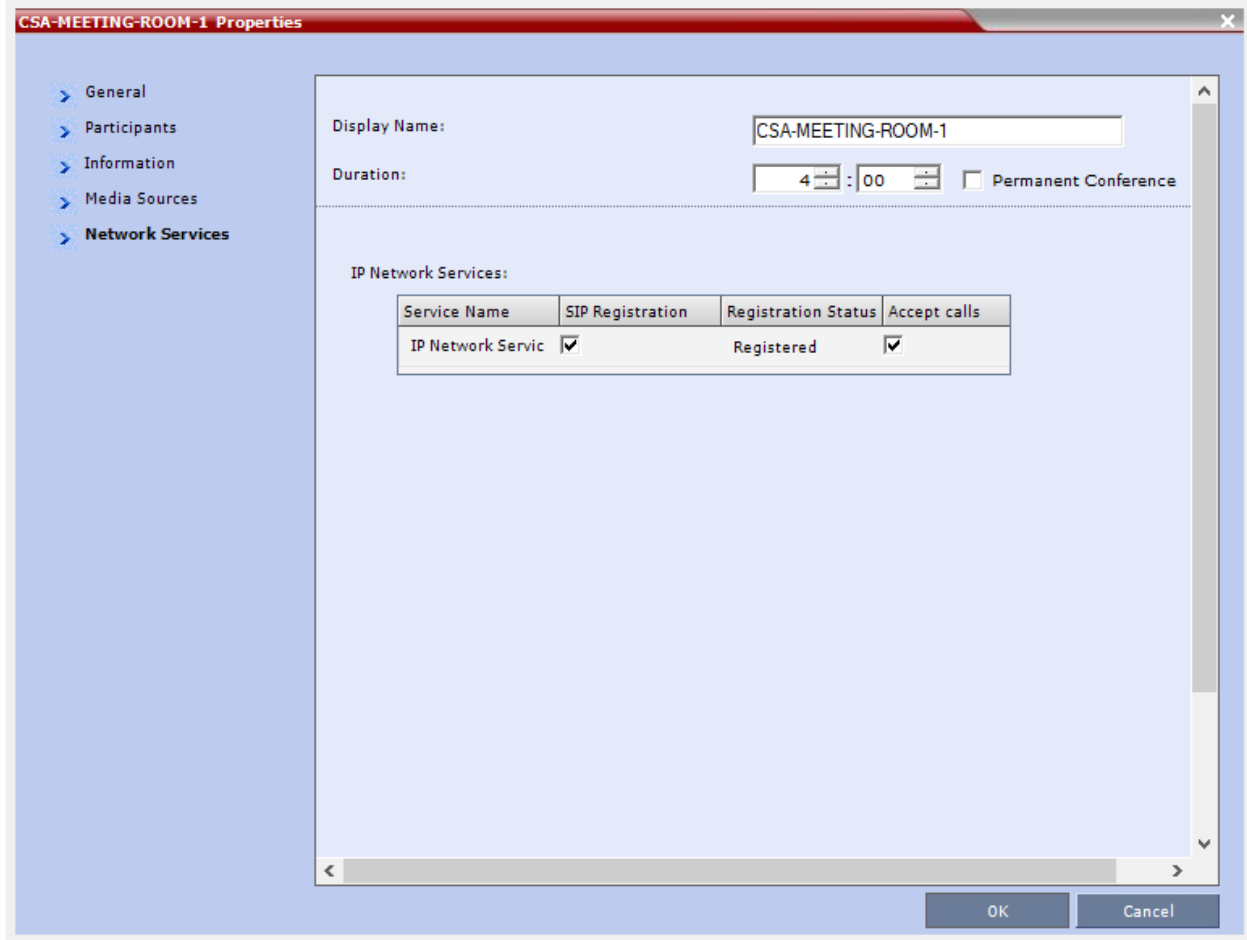
4

5+

9

10+

OK Cancel



2.5 Polycom Access Director

The RealPresence Access Director system enables users within and beyond your firewall to securely access voice, video, and multimedia sessions across IP network borders. The system securely routes communication, management, and content traffic through firewalls without requiring special dialing methods or additional client hardware or software. Specifically, the RealPresence Access Director system supports SIP and H.323 video calls (including H.460 firewall/NAT traversal) from registered users, guests, and federated enterprises or divisions.

2.5.1 Meta Data

- IP address: 192.168.251.10 for management



2.5.2 Configuration

2.5.2.1 SIP & H.323 Signaling

The RealPresence Access Director system provides connectivity for SIP (both SVC and AVC) or H.323 users, enabling them to securely collaborate over video from different locations and devices. Specifically, the RealPresence Access Director system enables:

- SIP and H.323 remote users (registered/provisioned endpoints) to securely connect to your enterprise network as managed users, with the same functionality they would have if they were inside your enterprise network firewall
- SIP and H.323 guest users (unregistered/unprovisioned endpoints, such as customers, partners, and vendors) to securely connect to your enterprise network
- SIP and H.323 B2B calling through trusted (federated or neighbored) connections to other enterprises' networks
- Open SIP and H.323 calling to and from users outside your network
- SIP RealPresence Web Suite guest users with browser-based clients to connect to RealPresence Web Suite video conferences within your enterprise network (The HTTPS tunnel proxy does not support SVC video conferencing.)

The screenshot shows the Polycom RealPresence Access Director configuration interface. The top navigation bar includes 'User', 'Configuration', 'Maintenance', 'Admin', 'Diagnostics', and 'Help'. The breadcrumb trail indicates 'You are here: Configuration > SIP Settings'. The user is identified as 'LOCAL\admin' and the date is 'Friday, June 01, 2018 12:18:29 PM'. The left sidebar contains a 'NAVIGATION' menu with options like 'Access Proxy Settings', 'SIP Settings', 'H.323 Settings', 'TURN Settings', 'Media Traversal Settings', 'Federation Settings', and 'Two-box Tunnel Settings'. The main content area is titled 'SIP Settings' and features a checkbox for 'Enable SIP signaling'. Below this is the 'External Port Settings' section, which contains a table with columns for 'Port name', 'Port number', 'Transport', 'Require certifi...', 'Default contact', 'Dial string poli...', 'Prefix of User', and 'Host'. The table lists 'Unencrypted port' (5060, UDP/TCP) and 'Encrypted port' (5061, TLS). To the right of the table are 'Add', 'Delete', and 'Edit' buttons. The 'Internal Port Settings' section includes fields for 'Unencrypted port' (5070, UDP/TCP) and 'TLS port' (5071), both with validation ranges. It also includes fields for 'SIP registrar (Next hop) address' (192.168.251.12, Port 5060, Transport TCP), 'SIP proxy (Next hop) address' (192.168.251.12, Port 5060, Transport TCP), 'Registration refresh interval' (300 seconds), and 'RFC5626 keep-alive interval' (120 seconds). A checkbox for 'Skip validating TLS certificate from remote server' is present. An 'Update' button is at the bottom.

Port name	Port number	Transport	Require certifi...	Default contact	Dial string poli...	Prefix of User	Host
Unencrypted port	5060	UDP/TCP	false	true	false		
Encrypted port	5061	TLS	false	true	false		



The screenshot shows the 'H.323 Settings' page in the Polycom RealPresence Access Director. The 'Enable H.323 signaling' checkbox is checked. Under 'Internal port settings', both 'H.225 RAS port' and 'H.225 call signaling port' are set to 1719. Under 'External port settings', both 'H.225 RAS port' and 'H.225 call signaling port' are set to 1719. The 'Gatekeeper (Next hop) address' is set to 192.168.251.12, with 'RAS Port' at 1719 and 'H.225 call signaling port' at 1720. There are 'Add' and 'Delete' buttons for the CIDR field. Under 'Bypass H.323 Federation Restrictions', 'Allow any incoming LRQ' and 'Allow any outgoing LRQ' are unchecked. 'Enable H.323 guest policy' and 'Enable H.323 default policy' are also unchecked.

The screenshot shows the 'TURN Settings' page in the Polycom RealPresence Access Director. The 'Enable TURN server' checkbox is checked. Under 'Listening IPs', the 'Available IPs' dropdown is set to 192.168.251.10. The 'External NAT address' field is empty. A table lists the listening IPs and external NAT addresses:

Listening IPs:	External NAT address:
192.168.100.9	197.156.82.226

There is a 'Delete' button for the table. Below the table, 'TURN port (UDP)' is set to 3478, 'Relay port range (UDP)' is set to 49152 - 65535, and 'Default authentication realm' is set to polycom.com. At the bottom, there is a 'TURN Users' table with columns for 'Username' and 'Realm', and an 'Add' button.

Note: the SIP registrar address and the H.323 gatekeeper address is 192.168.251.12.

2.5.2.2 Network settings

We have two network interfaces for the RPAD and we can configure each network interface for the type of service, or traffic, it communicates. We have set 192.168.251.10 for internal signaling, media relay and management. And 192.168.100.9 for external signaling and media relay this interface will be translated to 197.156.82.226 during external communication.



Configure Network Settings

Step 1 of 3: General Network Settings

The system's network settings can be changed below.

Hostname:

Primary DNS:

Secondary DNS:

Tertiary DNS:

Search Domain:

Domain:

Configure Network Settings

Step 2 of 3: Advanced Network Settings

Note: If you change the network interface configuration, the static route configuration will be reset.

Edit Network Interface

eth0

Mode:

Device:

IPv4 Address:

IPv4 Subnet Mask:

IPv4 Default Gateway:

eth1

eth2

eth3

Configure Network Settings

Step 2 of 3: Advanced Network Settings

Note: If you change the network interface configuration, the static route configuration will be reset.

Edit Network Interface

eth0

eth1

Mode:

Device:

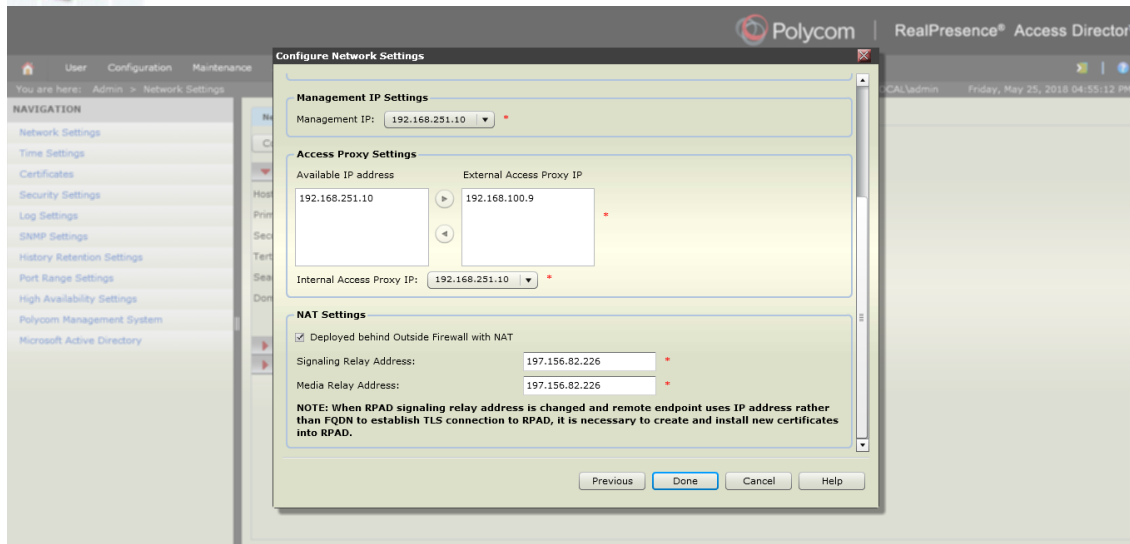
IPv4 Address:

IPv4 Subnet Mask:

IPv4 Default Gateway:

eth2

eth3



2.5.2.3 Configuring Access Proxy

The access proxy feature in the RealPresence Access Director system provides reverse proxy services for external devices. You can configure access proxy settings to enable firewall/NAT traversal for login, registration, and call requests. When the RealPresence Access Director system receives a request from a remote user, the system accepts or denies the request, based on your basic Access Control List (ACL) settings. If the request is accepted, the RealPresence Access Director system sends a new request on behalf of the remote user to the appropriate application server. The RealPresence Access Director system is configured with three default reverse proxies that route communication requests based on the type of target application server:

- HTTPS_proxy–HTTPS servers that provide management services. In our case RealPresence Resource Manager system
- LDAP_proxy–LDAP servers that provide directory services
- XMPP_proxy–XMPP servers that provide message, presence, or other XMPP services



Edit Access Proxy

Step 2 of 2: Detailed Settings

Enter the proxy settings in the fields below

HTTPS settings

Name: *

External IP address: *

External listening port: *

Internal IP address:

Require client certificate from the remote endpoint

Verify certificate from internal server

Next hops

Priority	Name	Type	System	Address	Port

Buttons: Add, Delete, Edit, Priority Up, Priority Down

Buttons: Previous, Done, Cancel, Help

Edit Access Proxy

Step 2 of 2: Detailed Settings

Enter the proxy settings in the fields below

HTTPS settings

Name: *

External IP address: *

External listening port: *

Internal IP address:

Require client certificate from the remote endpoint

Verify certificate from internal server

Next hops

Priority	Name	Type	System	Address	Port
1	CSA-RPRM	Request-URI			

Edit next hop

Type:

Name: *

System: *

Address: *

Port: *

Buttons: OK, Cancel, Help

Buttons: Add, Delete, Edit, Priority Up, Priority Down

Buttons: Previous, Done, Cancel, Help



Edit Access Proxy
Step 2 of 2: Detailed Settings
Enter the proxy settings in the fields below

XMPP settings

Name: XMPP_proxy *

External IP address: 192.168.100.9 *

External listening port: 5222 *

Internal IP address: 192.168.251.10 *

Next hop address: 192.168.251.11 *

Next hop port: 5222 *

Require client certificate from the remote endpoint

Verify certificate from internal server

Buttons: Previous, Done, Cancel, Help

Edit Access Proxy
Step 2 of 2: Detailed Settings
Enter the proxy settings in the fields below

LDAP settings

Name: LDAP_proxy *

External IP address: 192.168.100.9 *

External listening port: 389 *

Internal IP address: 192.168.251.10 *

Next hop address: 192.168.251.11 *

Next hop port: 389 *

Require client certificate from the remote endpoint

Verify certificate from internal server

Buttons: Previous, Done, Cancel, Help

3 Endpoint Management

Almost no configuration is done on the endpoints, they sync settings from the resource manager. The only configuration we do is connecting the end point with the resource manager. To do that login to the endpoint web portal by entering the endpoint's ip address and login using the following as the credential:

User name: admin

Password:

Once logged in go to Servers->Provisioning Service and enter the following:



- Server Type: RPRM
- Domain Name: local
- User Name: rprm-integrator
- Password:
- Server Address: 192.168.251.11

The screenshot shows the Polycom Admin interface for an AdminAdminGroupSeries RealPresence Group 310. The IP Address is 192.168.3.17 and the H.323 Extension (E.164) is 441000. The language is set to American English. The main menu on the left includes Place a Call, System, Manage Favorites, Admin Settings (General Settings, Network, Audio / Video, Security, Servers), Directory Servers, and SNMP. The Provisioning Service page is active, showing the following configuration:

Enable Provisioning:	<input checked="" type="checkbox"/>
Registration Status:	Registered
Server Type:	RPRM
Domain Name:	local
User Name:	rprm-integrator
Password:	*****
Server Address:	192.168.251.11

Buttons for Update and Save are visible at the top right of the configuration area.



4 Project Handover Document (PHD) Document Approval Form

Approval Certificate

System Description: CSA-VC Project, Implementation

Document Version 2.0

This Project Handover Document (PHD) document has prepared to make the whole implementation process meet all the required network services.

For and on behalf of CSA:

Full Name:	Signature	Date
_____	_____	_____

For and on behalf of Symbol Technologies PLC:

Full Name:	Signature	Date
_____	_____	_____

Comments, variations or caveats:

This PHD document approval Form is to be signed and returned to Symbol Technologies PLC.