Polycom ContentConnect

Copyright and Trademark

Plantronics, Inc. (Poly — formerly Plantronics and Poly)
345 Encinal Street Santa Cruz, California 95060

End User License Agreement By installing, copying, or otherwise using this product, you acknowledge that you have read, understand and agree to be bound by the terms and conditions of the End User License Agreement for this product. The EULA for this product is available on the Poly Support page for the product.

Patent Information The accompanying product may be protected by one or more U.S. and foreign patents and/or pending patent applications held by Plantronics, Inc.

Open Source Software Used in this Product This product may contain open source software. You may receive the open source software from Poly up to three (3) years after the distribution date of the applicable product or software at a charge not greater than the cost to Poly of shipping or distributing the software to you. To receive software information, as well as the open source software code used in this product, contact Poly by email at typeapproval@poly.com.

Limitation of Liability Poly and/or its respective suppliers make no representations about the suitability of the information contained in this document for any purpose. Information is provided "as is" without warranty of any kind and is subject to change without notice. The entire risk arising out of its use remains with the recipient. In no event shall Poly and/or its respective suppliers be liable for any direct, consequential, incidental, special, punitive or other damages whatsoever (including without limitation, damages for loss of business profits, business interruption, or loss of business information), even if Poly has been advised of the possibility of such damages.

Disclaimer While Poly uses reasonable efforts to include accurate and up-to-date information in this document, Poly makes no warranties or representations as to its accuracy. Poly assumes no liability or responsibility for any typographical or other errors or omissions in the content of this document.

Customer Feedback We are striving to improve our documentation quality and we appreciate your feedback. Email your opinions and comments to DocumentationFeedback@poly.com.

Support Visit the Poly Support Center for End User License Agreements, software downloads, product documents, product licenses, troubleshooting tips, service requests, and more.

Contents

Before You Begin 7
Audience, Purpose, and Required Skills 8
Frequently Asked Questions 8
Getting Help 10
Getting Started 11
Product Overview of Polycom ContentConnect 12
Limitations in Add-on Mode 15
Supported Languages for Polycom ContentConnect Add-on for Microsoft Skype for Business 16
Setting Up Your Environment 17
Required Prerequisite Components 18
Optional Solution Components 19
Required ContentConnect Product Components 20
Installing Product Components 23
Installing the ContentConnect Server Components 24
Installing Lync Client Machine Components 40
Setting Up a High Availability (Hot Standby) Environment 46
Configuring Solution Components 49
Configure Lync Clients to Auto-Discover the ContentConnect Server Address 50
Configuring RealPresence Collaboration Server (RMX) for ContentConnect 52
Configuring DMA for ContentConnect 52
Configuring Session Border Controllers for ContentConnect 53
Configuring the ContentConnect Server 61
Administration and Maintenance Tasks 83
ContentConnect Server Tasks 84
ContentConnect Client Tasks 113
View and Share Content 115
Using Microsoft Lync to Share and View Content 116
View and Share Content over the Web 125
ContentConnect Port Usage 129
Troubleshooting 135
Getting System Logs 136
Installing and Upgrading Solution Components 136
Troubleshoot the ContentConnect Server 136
Troubleshoot the ContentConnect Client 138
Troubleshoot the Web Client 142
Encryption Information 143
Open Source Attributions and Licenses 145

Before You Begin

Polycom ContentConnect is a solution that enhances the conferencing experience between Microsoft Skype for Business and video endpoints that receive content from Polycom RealPresence Collaboration Server (RMX). This solution also enables you to share and view content with a web browser.

Note: Polycom ContentConnect supports Microsoft Skype for Business clients (Skype for Business is rebranded from Lync in 2015), with the same feature set as supported with Microsoft Lync 2013.

Audience, Purpose, and Required Skills

This guide is written for a technical audience, specifically admins who manage the company's video conferencing equipment.

For the purposes of this document, **video endpoints** refer only to those video endpoints that receive content from RealPresence Collaboration Server (RMX).

You must be familiar with the following before beginning:

- Current telecommunications practices, protocols, and principles
- Unified communications, video teleconferencing, and voice or data equipment
- Networking, security certificates, and software configuration
- Microsoft Skype for Business
- Polycom hardware and software

Frequently Asked Questions

Refer to the frequently asked questions (FAQs) to help answer questions you may have about the solution before you begin.

How do I obtain the ContentConnect software?
To obtain ContentConnect software and other ContentConnect related components, contact your Polycom Support team.

What endpoints does the ContentConnect apply to?
The solution applies to video endpoints that receive content from RealPresence Collaboration Server (RMX), and to Microsoft Lync clients.

What's the difference between the Add-On and Gateway mode?
In the Add-On mode, ContentConnect Content Add-on for Lync takes over the content stage and displays BFCP content. All Lync clients need to install the ContentConnect Content Add-on for Lync.

In the Gateway mode, the ContentConnect server works as an RDP-BFCP content gateway, fully transcoding RDP and BFCP H.264 content streams. Lync clients don't need to install ContentConnect add-ons. Existing add-ons are disabled automatically.

Gateway mode is not supported in ContentConnect server version 1.3 or earlier.

How to decide which ContentConnect mode should I use?
Use the Gateway mode in Polycom RealConnect™ deployment.

Use the Add-on mode only when you want to make direct VMR calls (dialing in to a VMR from Lync client).

Note: As the Add-on mode requires you to install Polycom ContentConnect Add-on for Microsoft Lync, Polycom recommends you to use Polycom Soft Blade instead. The Soft Blade provides RDP content media to Microsoft Skype for Business without the need to install client-side plugins. For more information, refer to Polycom RealPresence® Collaboration Server version 8.7.1 or later documentation available on Polycom Support.

Are there any differences in the licensing mechanism for the Gateway and Add-on modes?
In the gateway mode, each conference consumes one ContentConnect license. In the Add-on mode, each Lync user that joins VMR consumes one ContentConnect license. Web client is supported for both Gateway and Add-on mode, and each web client that joins VMR consumes one ContentConnect license.

What types of content-sharing does ContentConnect support?
You can share your desktop or a program. For this release of ContentConnect, you are unable to share whiteboards or create polls. You can share Microsoft® PowerPoint slides by sharing your desktop.

What does my environment require before I deploy ContentConnect?
There are several required prerequisite components that you need to install and set up before you deploy ContentConnect. These components include Microsoft Active Directory Server, Lync Server, Lync Client, RealPresence Distributed Media Application (DMA), RealPresence Collaboration Server (RMX), and video endpoints (one or more). There are also optional components that, if used, also need to be installed and set up before you install ContentConnect software. Optional prerequisite components include RealPresence® Access Director, Acme Packet Net-Net Enterprise Session Director (ESD), RealPresence Capture Server, and a load balancer.

What else do I require to deploy the solution?
Before you deploy the ContentConnect, your existing environment requires several components. To deploy ContentConnect, you also require several ContentConnect product components, including ContentConnect server (with VMware or Hyper-V installed on it), an OVA-formatted virtual appliance software installation package or a VHD-formatted virtual appliance software installation package for Hyper-V. If your ContentConnect server running mode is Add-On, you also need a Polycom ContentConnect Add-on for Microsoft Lync installation file (to install on the Lync Client PC).

What version of Microsoft Lync Client is required?
Polycom recommends you to use Microsoft Skype for Business clients (Skype for Business is rebranded from Lync in 2015) for the ContentConnect Gateway mode.

Use Lync 2013 or Lync 2010 only for the ContentConnect Add-on mode.

Does this solution apply to Lync and video endpoints in point-to-point calls?
The solution only applies to conference participants who meet in a RealPresence Collaboration Server (RMX)/RealPresence Distributed Media Application (DMA) Virtual Meeting Room (VMR). Point-to-point calls between Lync and other endpoints can't share content.

Does this solution work among users in different enterprises?
Yes. Federated users are supported when you select Gateway as the ContentConnect working mode. Gateway mode is supported only in Polycom RealConnect deployment.

Does this solution have any specific requirements on Lync AVMCU location?
In Content Sharing Suite version 1.4.1 and earlier, Lync users must have their Polycom infrastructure and Lync AVMCU in the same network domain. From ContentConnect V1.6, content support when Lync AVMCU resides in federated environment is supported.

I have several users calling into meetings from outside the company firewall. Can these users benefit from ContentConnect?
Yes, the ContentConnect solution works with users calling from inside and outside the company firewall.

In the Add-on mode, your setup must include a ContentConnect-supported firewall traversal product, such as RealPresence Access Director or Acme Packet Net-Net Enterprise Session Director (ESD).

In the Gateway mode, your setup must include a Microsoft Lync Edge Server.

Where can I find more information about ContentConnect?
For more information about ContentConnect, see the Polycom ContentConnect support page. For more information about installing, configuring, and administering Polycom products, refer to Polycom Support.

Getting Help

For more information about installing, configuring, and administering Polycom products, refer to Documents & Software at Polycom Support.

Polycom and Partner Resources

For more information about ContentConnect, see the Polycom ContentConnect support page.

In addition to this document, the support page contains the following documentation:

- *Polycom ContentConnect Quick User Guide*
- *Polycom ContentConnect Release Notes*

To configure Polycom products to work within a Lync environment, see the *Polycom Unified Communications Deployment Guide for Microsoft Environments* at Polycom Support.

To find information for all Polycom partner solutions, see Strategic Partner Solutions.

The Polycom Community

The Polycom Community gives you access to the latest developer and support information.

Participate in discussion forums to share ideas and solve problems with your colleagues. To register with the Polycom Community, simply create a Polycom online account. When logged in, you can access Polycom support personnel and participate in developer and support forums to find the latest information on hardware, software, and partner solutions topics.

Getting Started

Polycom ContentConnect is a video collaboration application that enables users on disparate devices and clients (including Microsoft Skype for Business clients, H.323 and SIP video endpoints, and audio-only participants) to participate in full content sharing during meetings.

Product Overview of Polycom ContentConnect

The Polycom ContentConnect is a video collaboration application that enables users on disparate devices and clients, including Lync client, H.323 and SIP video endpoints, and audio only participants, to participate in the full content sharing session.

Through the ContentConnect, high quality content sharing is possible for everybody, including home workers and B2B access. The ContentConnect is a pure software extension of the Polycom RealPresence Platform and works with other appliance-based or virtual RealPresence Platform products for scalable and reliable content sharing experience.

The ContentConnect enables the following:

- Microsoft Lync users to share applications or their computer desktop with other conference participants calling from video endpoints that receive content from RealPresence Collaboration Server (RMX).
- Conference participants calling from video endpoints that receive content from RealPresence Collaboration Server (RMX) to share programs or their computer desktop with conference participants that use Microsoft Lync.

Essentially, the ContentConnect enables Microsoft Lync endpoints to use BFCP - rather than Microsoft RDP - to stream content. By enabling Microsoft Lync endpoints to use the same video content channel that video endpoints use, all conference participants can enjoy a high-quality content-sharing experience.

The ContentConnect is comprised of several hardware and software components. Key ContentConnect software components are installed on a server running VMware or Hyper-V, and on the Lync Client's server. Other required hardware components include Polycom RealPresence Collaboration Server (RMX), Polycom RealPresence Distributed Media Application (DMA), and - if firewall traversal is required - Polycom RealPresence Access Director or Acme Packet® Net-Net Enterprise Session Director (ESD).

Note: Instead of viewing and sharing content using Lync, you can view and share content over the Web by entering a special URL ((https://<server IP>/css/) in a Web browser.

Related Tasks

View and Share Content over the Web on page 125

If you don't have access to Lync, you can access ContentConnect content over the Web by entering a special URL - https://<server IP>/css/ - in a Web browser.

ContentConnect Features and Capabilities

Through ContentConnect, everyone can share high-quality content, including home workers and those with B2B access.

ContentConnect enables the following options:

- Microsoft Skype for Business users can share applications or their computer desktop with other conference participants calling from video endpoints that receive content from RealPresence Collaboration Server (RMX).

- Conference participants calling from video endpoints that receive content from RealPresence Collaboration Server (RMX) can share programs or their computer desktop with conference participants that use Microsoft Lync.

ContentConnect enables Microsoft Skype for Business endpoints to use BFCP (rather than Microsoft RDP) to stream content. By enabling Microsoft Skype for Business endpoints to use the same video content channel that video endpoints use, all conference participants can enjoy a high-quality content-sharing experience.

Note: Instead of viewing and sharing content using Microsoft Skype for Business, you can view and share content over the web by entering a special URL (https://<server IP>/css/) in a web browser.

Solution Components

The Polycom ContentConnect solution comprises the following components:

- **ContentConnect server**: Provides enhanced conferencing experience between Microsoft® Lync™ and video endpoints that receive content from RealPresence Collaboration Server (RMX).
- **(Optional) Content Add-on for Lync**: Provides the native BFCP support for the Lync endpoint to enable Lync and video endpoints to share content. This component is required only when your ContentConnect server runs in the Add-On mode. An administrator or end user installs the Content Add-on for Lync on the Lync client's machine. The content Add-on finds the ContentConnect server automatically, logs on to the server, and obtains provisioning data for the user - such as DMA's address, and the content rate to use. When a Lync user makes a call to a VMR meeting, the Content Add-on detects and connects to the VMR using SIP as well, and encodes and decodes content streams. A plug-in - the BFCP Content-Only Client Plug-in- is embedded in the Content Add-on for Lync. The Plug-in places a separate SIP call to the VMR, controls the content sharing using BFCP, and encodes and decodes content streams.
- **Polycom RealPresence Distributed Media Application (DMA)**: A network-based virtualization application for managing and distributing calls across collaboration networks. The DMA call processing software engine allows users to connect regardless of protocol standard, device, network, or location. DMA allows you to interact with Polycom RealPresence Collaboration Server (RMX). For more information about DMA, see the Polycom Distributed Media Application support page.
- **Polycom RealPresence Collaboration Server (RMX)**: For multiparty video, voice, and content collaboration. For more information about RealPresence Collaboration Server (RMX), navigate to your system's support page from the Collaboration & Conferencing Platforms support page.
- **Microsoft Active Directory Server**: A server (provided by the customer) that is used by the ContentConnect server as an authentication provider to authenticate client connections. For more information about Active Directory, see the Microsoft TechNet web site.
- **Microsoft Lync Server**: Software that provides a unified communications infrastructure for instant messaging (IM), voice and video calling, and conferencing. For more information about Lync Server, see the Microsoft TechNet web site.
- **Lync Client**: The instant messaging, voice and video calling, and conferencing client for Lync Server, which is installed on individual user machines. The Lync client can be installed on Lync room systems, computers running Windows or Mac operating systems, or mobile devices running iOS, Android, or Windows mobile platforms. For more information about Lync client, see the Microsoft TechNet web site.
- **Polycom RealPresence Platform Director or Polycom RealPresence Resource Manager**: Provides the flexibility to deploy and monitor the Polycom RealPresence Platform Virtual Edition, using general purpose hardware in an organization's data

center or in the cloud. The RealPresence Platform Director is needed only when you activate licenses using the solution mode. For more information, see the Polycom RealPresence Platform Director or Polycom RealPresence Resource Manager support page

- **Video endpoints that receive content from RealPresence Collaboration Server (RMX)**: ContentConnect supports content sharing between Microsoft Lync and several endpoints in the same VMR.
- **(Optional) Polycom RealPresence Access Director**: An optional ContentConnect component that allows users outside the corporate network to join meetings with users inside the corporate network. For more information about RealPresence Access Director, see the Polycom RealPresence Access Director support page.
- **(Optional) Acme Packet Net-Net Enterprise Session Director (ESD)**: an optional ContentConnect component that allows users outside the corporate network to join meetings with users inside the corporate network. For more information about Acme Packet Net-Net Enterprise Session Director (ESD), see the Acme Packet documentation online.
- **(Optional) Polycom RealPresence Capture Server**: A network server that enables users to easily record, stream and archive media content. For more information about Polycom RealPresence Capture Server, see the Polycom® RealPresence™ Capture Server support page.
- **(Optional) Load Balancer**: An optional ContentConnect component to increase efficiency and network performance.

  Note: To support remote access, your setup requires RealPresence Access Director, Acme Packet Net-Net Enterprise Session Director (ESD), or a Lync Edge server.

Solution Architecture

The following information provides the solution architecture options for your Polycom ContentConnect deployment.

Gateway Mode (default)

In Gateway mode, the ContentConnect server works as an RDP-BFCP content gateway, fully transcoding RDP and BFCP H.264 content streams. Lync clients don't need to install ContentConnect add-ons. Existing add-ons are disabled automatically.

Note: Gateway mode works only in a Polycom RealConnect deployment. Polycom RealConnect for Microsoft Lync unifies video collaboration across Lync and non-Lync environments seamlessly. For more information, see Polycom Support.

The following diagram shows Gateway mode in a multipoint conference with video endpoints.

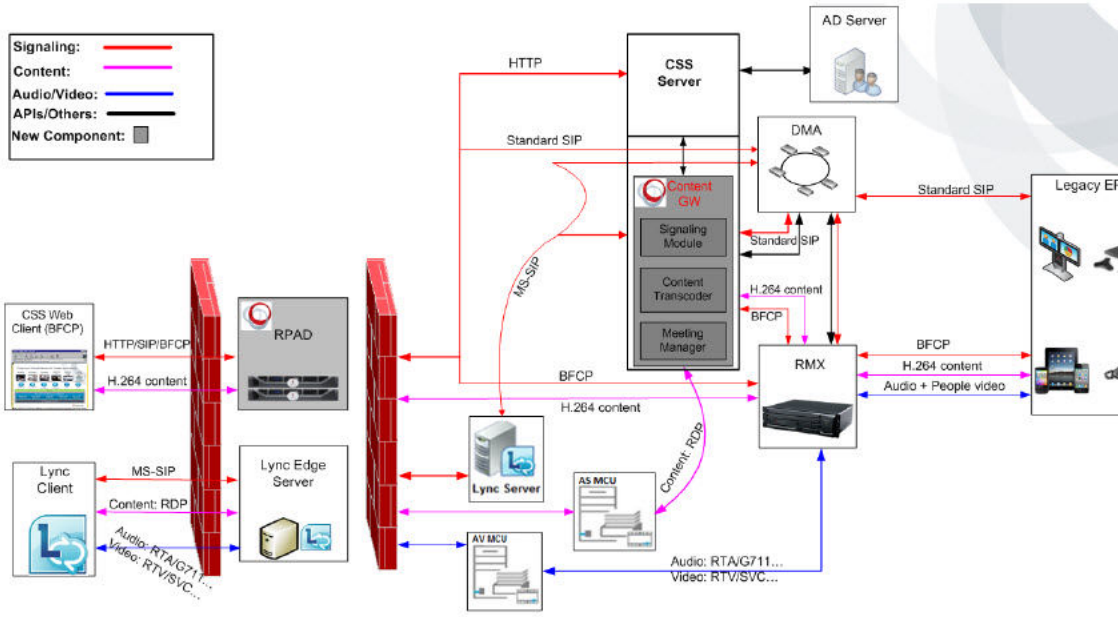


Figure 1: Gateway Mode Network Diagram

Add-on Mode

In Add-on mode, the ContentConnect Content Add-on for Lync processes RDP-BFCP transcoding. All Lync clients must install the ContentConnect Content Add-on for Lync.

The following diagram shows Add-on mode in a multipoint conference with video endpoints.

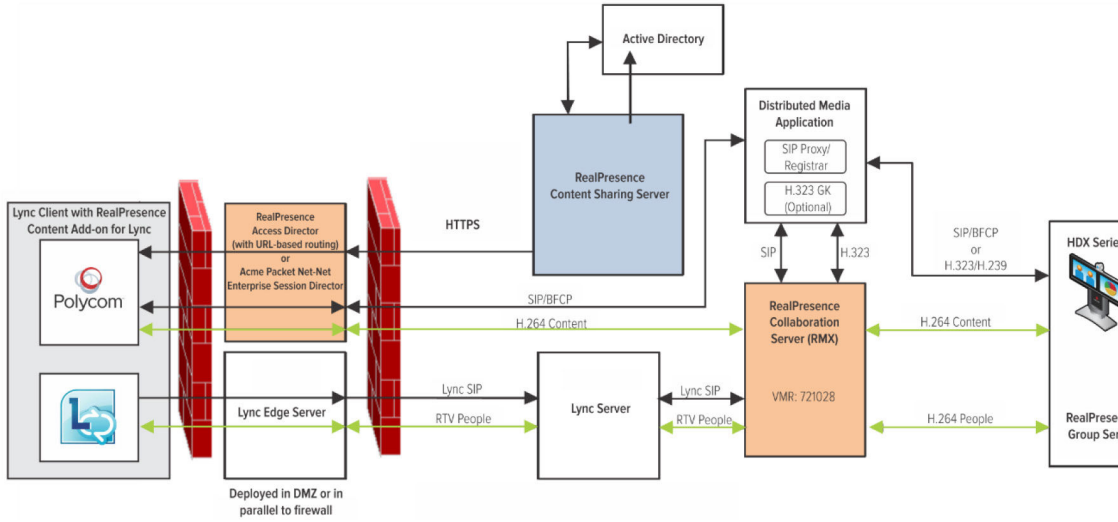


Figure 2: Add-on Mode Network Diagram

Limitations in Add-on Mode

Polycom ContentConnect has some limitations when running your server in Add-on mode.

If you run your ContentConnect server in Add-on mode, you must install the Polycom ContentConnect Add-on for Microsoft Lync.

The ContentConnect Content Add-on has the following limitations:

- The Polycom ContentConnect Add-on for Microsoft Lync doesn't launch if both Lync 2010 and 2013 are installed on the same client machine.
- If you sign in to your computer using multiple accounts simultaneously, the Polycom ContentConnect Add-on for Microsoft Lync may not run in one of the accounts, because it's still running in the other account. The issue arises when you do the following:

  1. Log on to your computer with Account A.
  2. Successfully sign in to the Lync client and Polycom ContentConnect Add-on for Microsoft Lync.
  3. Switch from Account A to Account B.
  4. Sign in to the Lync client again.
     In this scenario, the Polycom ContentConnect Add-on for Microsoft Lync continues to run on Account A and doesn't run on Account B.

Supported Languages for Polycom ContentConnect Add-on for Microsoft Skype for Business

You can determine the language for your Polycom ContentConnect Add-on for Microsoft Skype for Business installation.

The Polycom ContentConnect Add-on for Microsoft Lync installation file is available in the following languages:

- Chinese (Simplified)
- English
- French
- German
- Italian
- Japanese
- Korean
- Portuguese (Brazilian)
- Russian
- Spanish (International)

Setting Up Your Environment

To deploy ContentConnect, your environment requires several components.

There are also several optional components that ContentConnect supports that you can set up in your environment. This section divides these components into two categories: your existing environment - which describes optional and required prerequisite components - and required components, which are included in the ContentConnect product.

After reading this section, you'll understand what components your environment requires to deploy ContentConnect, and what components are optional, but supported by ContentConnect.

Required Prerequisite Components

The following table lists required components that must be set up in your environment before you deploy ContentConnect.

For information on versions of compatible components, refer to the Interoperability List in the Release Notes of Polycom ContentConnect available on support.polycom.com.

Note: Your environment also requires VMware 5.0 or later or Hyper-V build in Windows Server 2012 or later.

Note: Gateway mode works only in the Polycom RealConnect deployment.

Required Prerequisite Components

Component
Management Systems and Recorders
Microsoft Active Directory Server
Gatekeepers, Gateways, and MCUs
Microsoft Lync Server
Polycom RealPresence Distributed Media Application (DMA) 7000
Polycom RealPresence Collaboration Server (RMX) 1500/1800/2000/4000
Microsoft Endpoints • Gateway Mode Microsoft Skype for Business client installed on Windows, Mac, mobile platforms (iOS, Android, Windows), Lync Web App, and Lync Room Systems. • Add-on Mode Microsoft Lync Client installed on Windows

Video Endpoints

Your environment requires one or more video endpoints that receive content from RealPresence Collaboration Server (RMX). For more information on interoperability, see the Interoperability Tables section in the *RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 Release Notes*, available by navigating to your system from the Collaboration & Conferencing Platforms support page.

Related Tasks

Install the OVA-Formatted Installation Package on VMware vSphere on page 24

To install the ContentConnect server, you need the Open Virtualization Appliance (OVA) installation package.

Install the VHD-Formatted Installation Package in a Hyper-V Environment on page 31

For information on installing the Hyper-V Role on Windows Server, refer to the Hyper-V Role web site.

Optional Solution Components

The following table lists optional and compatible components that you can install and set up before you deploy ContentConnect.

Optional Solution Components

Component
NATS, Firewall, Border Controllers
Lync Edge Server
Polycom RealPresence Access Director
Acme Packet® Net-Net Enterprise Session Director (ESD)
Recorders
Polycom RSS 4000 or RealPresence Capture Server
Load Balancers Polycom RealPresence® Distributed Media Application™ (DMA®) F5 Load Balancer

Related Tasks

[Install the OVA-Formatted Installation Package on VMware vSphere](#) on page 24

To install the ContentConnect server, you need the Open Virtualization Appliance (OVA) installation package.

[Install the VHD-Formatted Installation Package in a Hyper-V Environment](#) on page 31

For information on installing the Hyper-V Role on Windows Server, refer to the Hyper-V Role web site.

Required ContentConnect Product Components

To deploy the ContentConnect solution, the following ContentConnect product components are required:

- VMware or Hyper-V software, as the host of the ContentConnect server.
- ContentConnect server OVA-formatted virtual appliance installation package (to install on the ContentConnect server).
- Polycom ContentConnect Add-on for Microsoft Lync installation file (to install on the Lync Client PC). This is required if your ContentConnect server runs in the Add-On mode.

The following table lists the required ContentConnect product components, required versions, and relevant specifications.

Required ContentConnect Components

ContentConnect Product Component
VMware or Hyper-V software, as the host of the ContentConnect server
OVA-formatted Virtual Appliance Software Installation Package/VHD-Formatted Virtual Appliance Software Installation Package
Polycom ContentConnect Add-on for Microsoft Lync installation file (to be installed on the Lync Client PC) This is required if your ContentConnect server runs in the Add-On mode

Related Tasks

[Install the OVA-Formatted Installation Package on VMware vSphere](#) on page 24

To install the ContentConnect server, you need the Open Virtualization Appliance (OVA) installation package.

[Install the VHD-Formatted Installation Package in a Hyper-V Environment](#) on page 31

For information on installing the Hyper-V Role on Windows Server, refer to the Hyper-V Role web site.

Installing Product Components

This section describes how to install the product components for ContentConnect.

The components include:

- ContentConnect server components - VMware or Hyper-V build with the associated virtual appliance package
- Lync client machine components - Microsoft .NET Framework 4 Client Profile and the Polycom ContentConnect Add-on for Microsoft Lync
- High Availability environment requirements

Note: If your ContentConnect server runs in Add-on mode, you must install the same versions of the ContentConnect server and the Polycom ContentConnect Add-on for Microsoft Lync. For example, if you install version 1.2 of the Polycom ContentConnect server pre-configured VHD installation package, you must install version 1.2 of the Polycom ContentConnect Add-on for Microsoft Lync on each Lync client machine. If the ContentConnect server and the Polycom ContentConnect Add-on for Microsoft Lync are different versions, your ContentConnect solution doesn't work properly.

Installing the ContentConnect Server Components

Once your ContentConnect server is installed and set up with the minimum system server requirements, install the following server components:

- OVA-Formatted Virtual Appliance Installation Package on VMware vSphere
- VHD-Formatted Virtual Appliance Installation Package on Hyper-V

For more information on hardware and software requirements, refer to Polycom® ContentConnect™ Release Notes.

Related Tasks

Activate Licenses in High Availability (Hot Standby) or Multi-Server Environments on page 47

You need to buy additional license to enable High Availability on the active ContentConnect server.

Install the OVA-Formatted Installation Package on VMware vSphere

To install the ContentConnect server, you need the Open Virtualization Appliance (OVA) installation package.

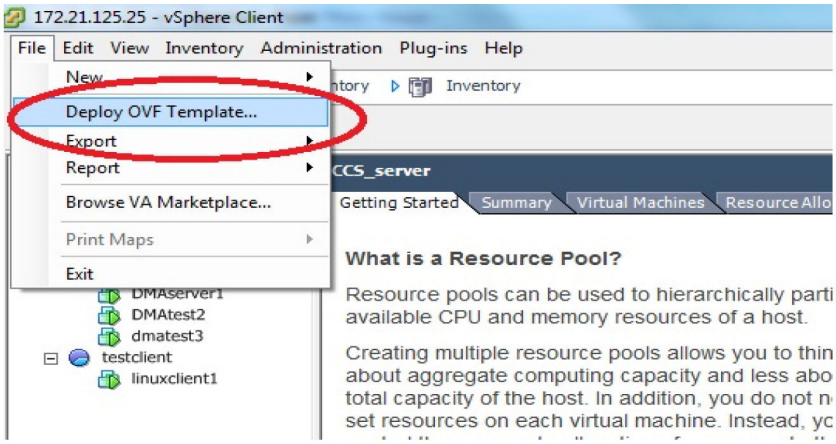
The package contains three files. Download these files to a location on your computer, so you can navigate to them during the install.

For information on installing VMware, refer to the VMware web site. For VMware vSphere documentation, refer to the VMware vSphere support page. ContentConnect supports VMware 5.0 and later.

Ensure your server meets the VMware Server specifications. In addition, make sure to edit the BIOS of your server to enable Virtualization of the CPUs.

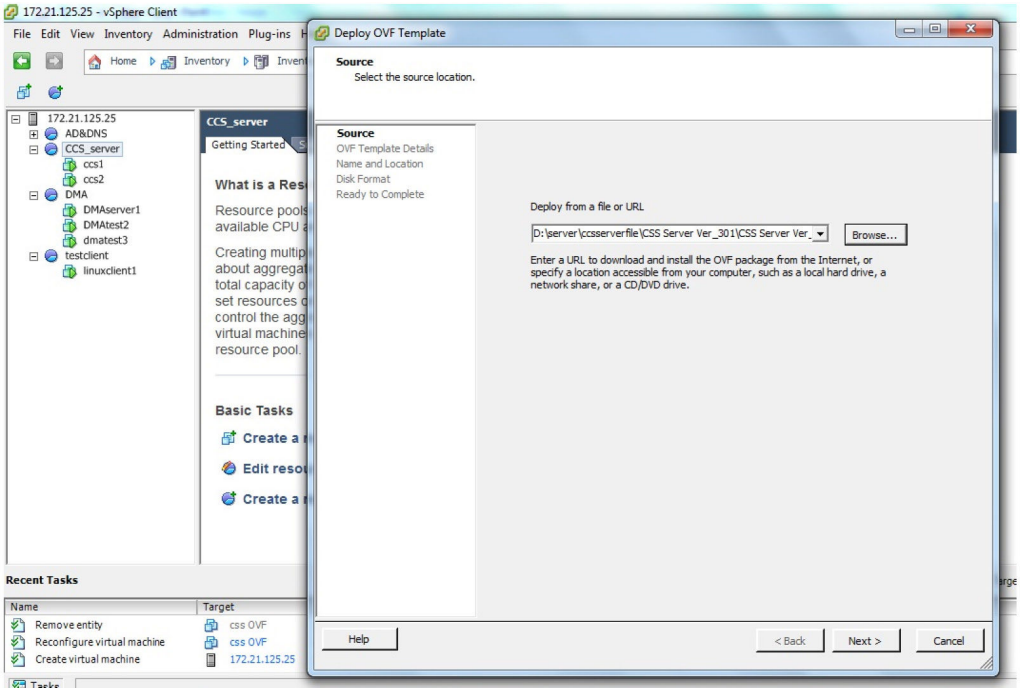
Note: To align with other Polycom products, from version 1.3.1 and later, OVA-format installation packages are used for VMware vSphere installation.

1. Log in to VMware with vSphere Client.
2. From the vSphere Client, select File > Deploy OVF Template, as shown next.

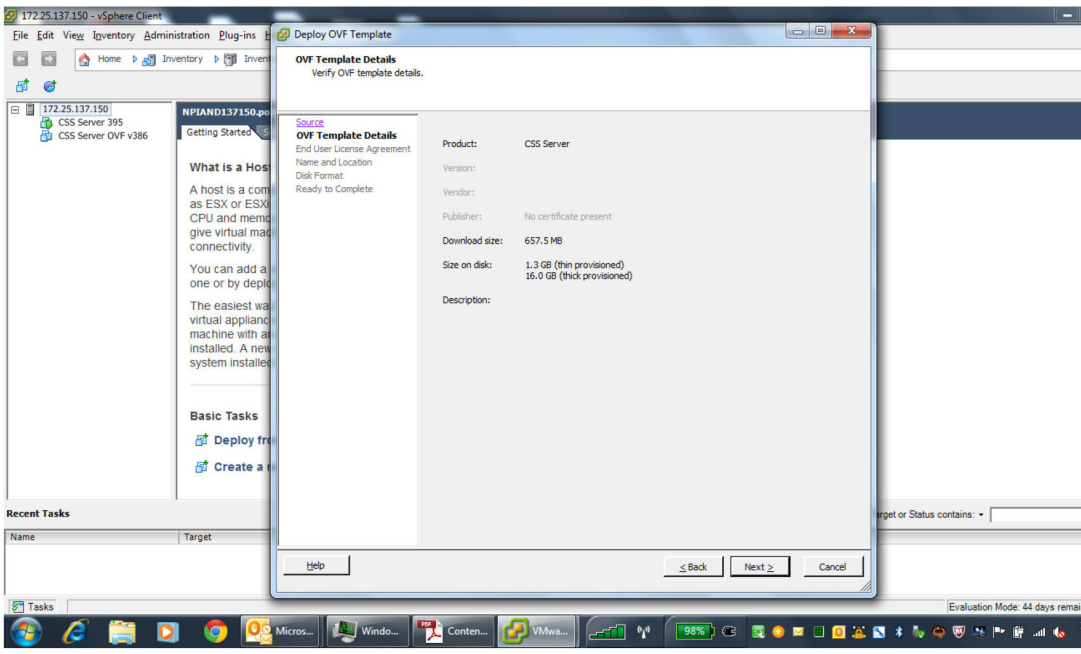


The Deploy OVF Template page displays.

3 From the Source window (shown next), enter the directory (or click Browse to browse to the location) that contains the ContentConnect server OVA files, and click Next.

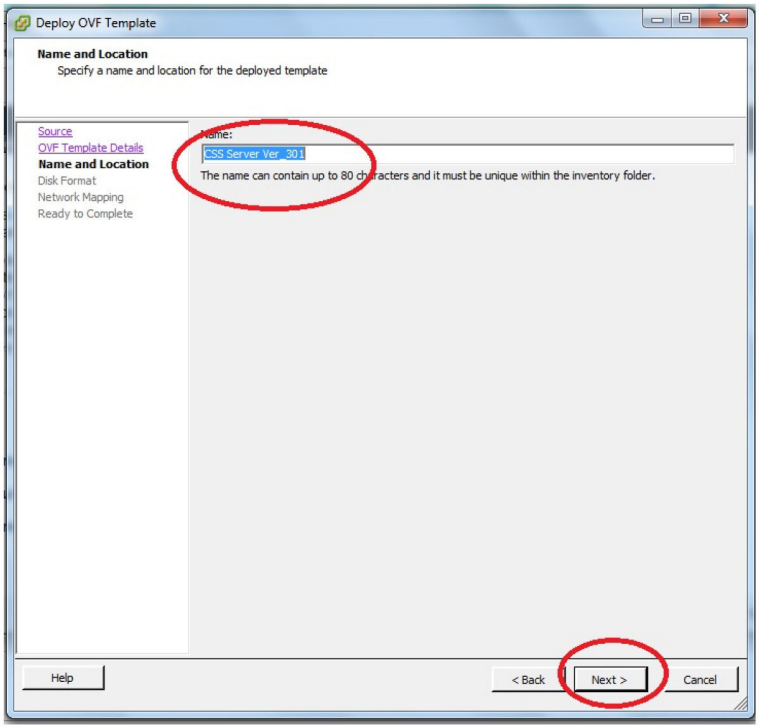


4 From the OVF Template Details window (shown next), confirm the details of the OVF template, and click Next.

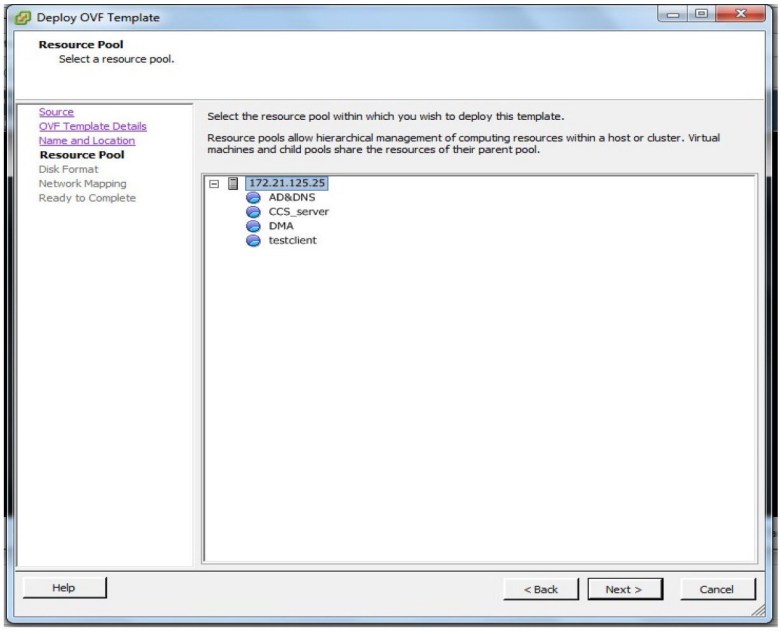


5 From the End User License Agreement window (shown next), review the license agreement, and if you accept the terms, click Accept, and then click Next.

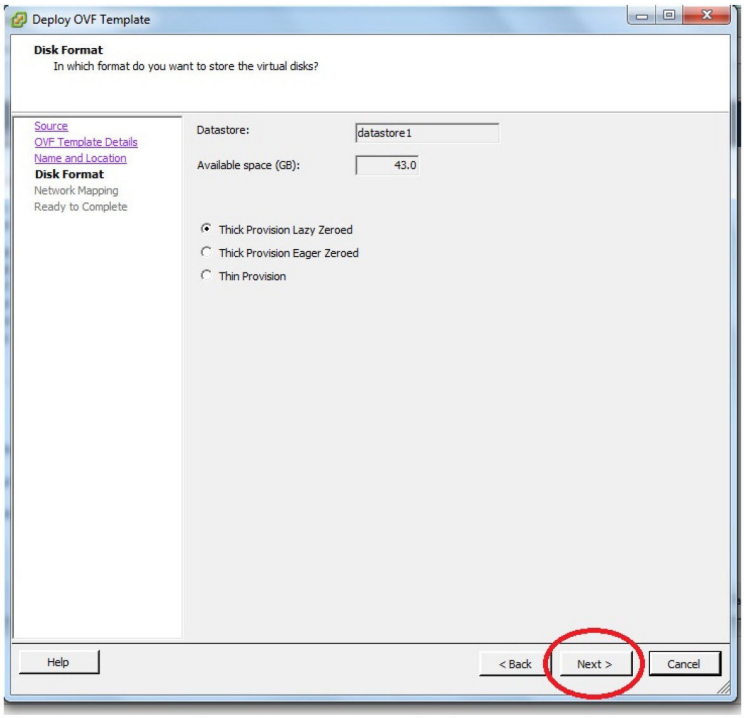
6 From the Name and Location window (shown next), enter the name of the ContentConnect server that you want to display in the VMware virtual machine list, and click Next.



7 From the Resource Pool window (shown next), choose the resource (the top-level IP address) to deploy the template from, and click Next.
This will classify the virtual machine.

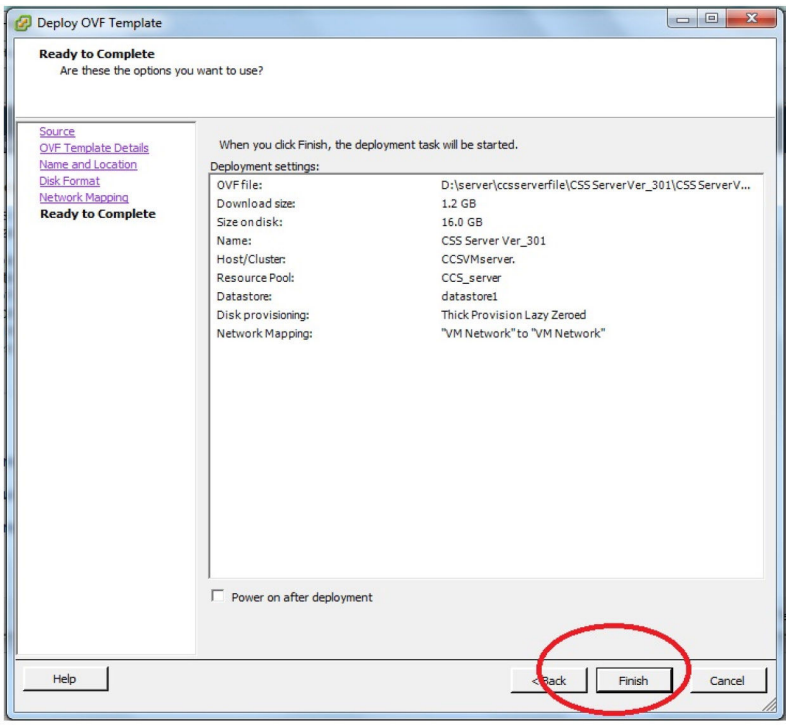


8 From the Disk Format window (shown next), accept the default disk format and click Next.



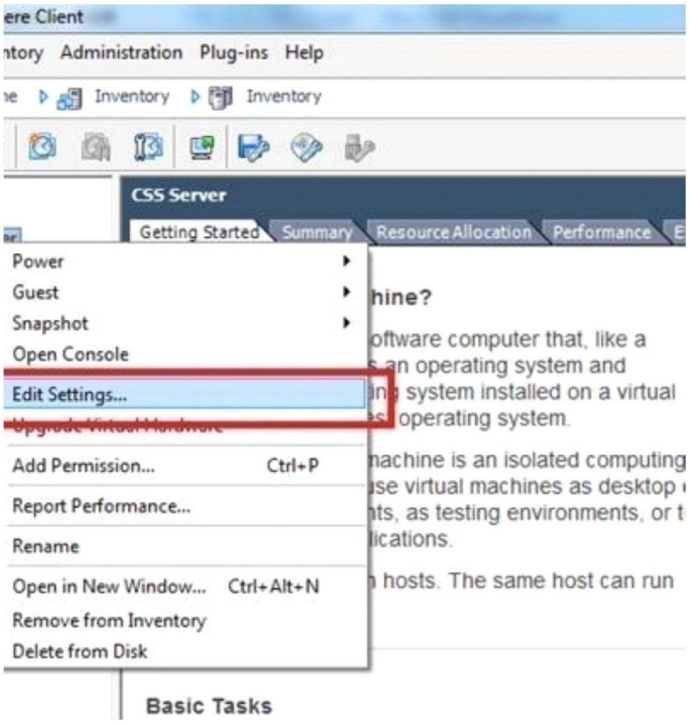
9 From the Network Mapping window, accept the default mapping and click Next. Note that this window displays when multiple NIC port groups are created in VMware. The window won't display if VMware just contains the default port group

10 From the Ready to Complete window (shown next) review the options you selected, and click Finish.

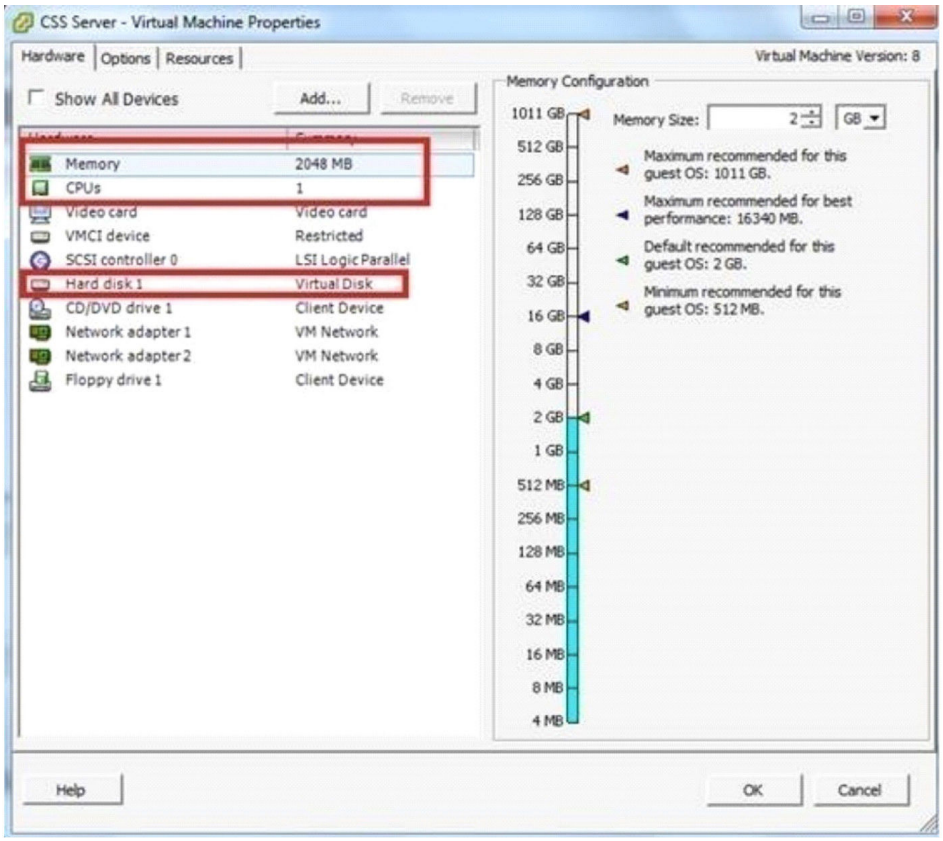


A Deploying window (as shown next) displays. Wait while the deployment process completes. The process completes when Cancel changes to Ok, and the message Completed Successfully displays. Click OK.

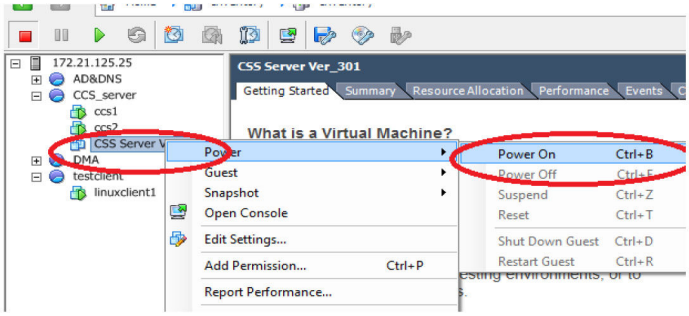
11 Navigate to your virtual server (as shown next), and select Edit Settings.



12 From the Virtual Machine Properties window (as shown next), update the virtual host's memory, CPU, and hard disk settings.
Refer to Polycom RealPresence ContentConnect Release Notes, *Hardware and Software Requirements* for host memory requirement.

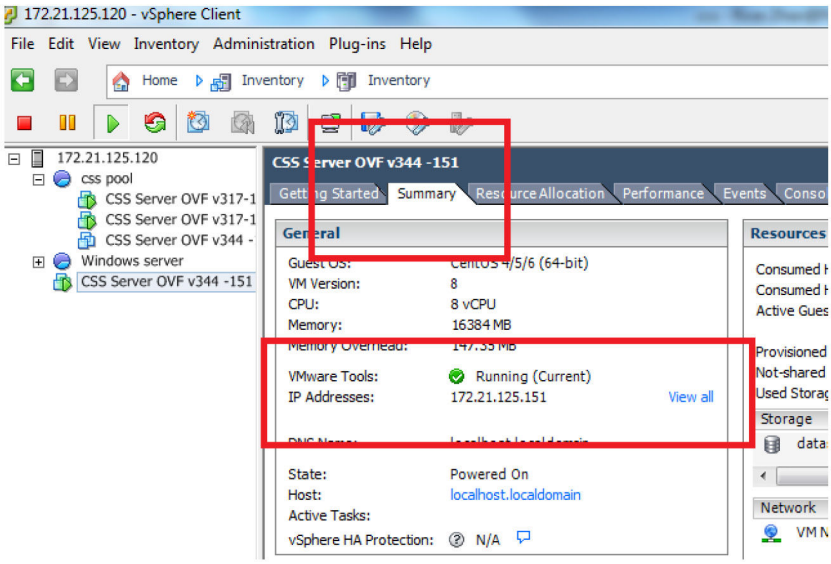


13 Navigate to your virtual server (as shown next), and select Power > Power On.



14 Configure network settings.
Network settings can be configured dynamically (the default method) or statically. If network settings are configured dynamically, all network settings will be obtained from the DHCP server. If you configure static network settings, you need to enter IP addresses for the network parameters manually.

- Dynamic configuration The ContentConnect server works in DHCP mode by default after installation, it can obtain network configuration (IP, gateway, DNS and so on) from DHCP server after server starts up. The obtained IP address could be observed by navigating to the ContentConnect server from vSphere Client, and then reviewing the summary screen for the server you just installed. This screen contains the DHCP IP address that is assigned to the server. To view the summary screen, navigate to your ContentConnect server, and select the Summary tab, as shown next.



- Static configuration If you need to configure network settings statically, manually configure the network settings. From vSphere client, open a console window and press Enter to obtain a prompt. Enter polycom and polycom for your user name and password. Follow the on-screen instructions to change the following:
- Change Host Name (Optional)
- Configure DNS (Required)
- Configure Network (Required)
- Change Password (Optional)

The ContentConnect server is installed. You can now access the ContentConnect server Web Configuration Tool and configure the server. To access the tool enter http://<your server ip address>/admin in your Browser's address bar.

Related Concepts

Required ContentConnect Product Components on page 20

Optional Solution Components on page 19

The following table lists optional and compatible components that you can install and set up before you deploy ContentConnect.

Required Prerequisite Components on page 18

The following table lists required components that must be set up in your environment before you deploy ContentConnect.

Installing the Polycom ContentConnect Add-on for Microsoft Lync on page 41

You must install RealPresence Content Add-on only if you choose to run your ContentConnect server under Add-On mode.

Configuring the ContentConnect Server on page 61

To configure the ContentConnect server, you need to access the ContentConnect server Web Configuration Tool, which enables you to configure and update the ContentConnect settings from a remote PC.

Install the VHD-Formatted Installation Package in a Hyper-V Environment

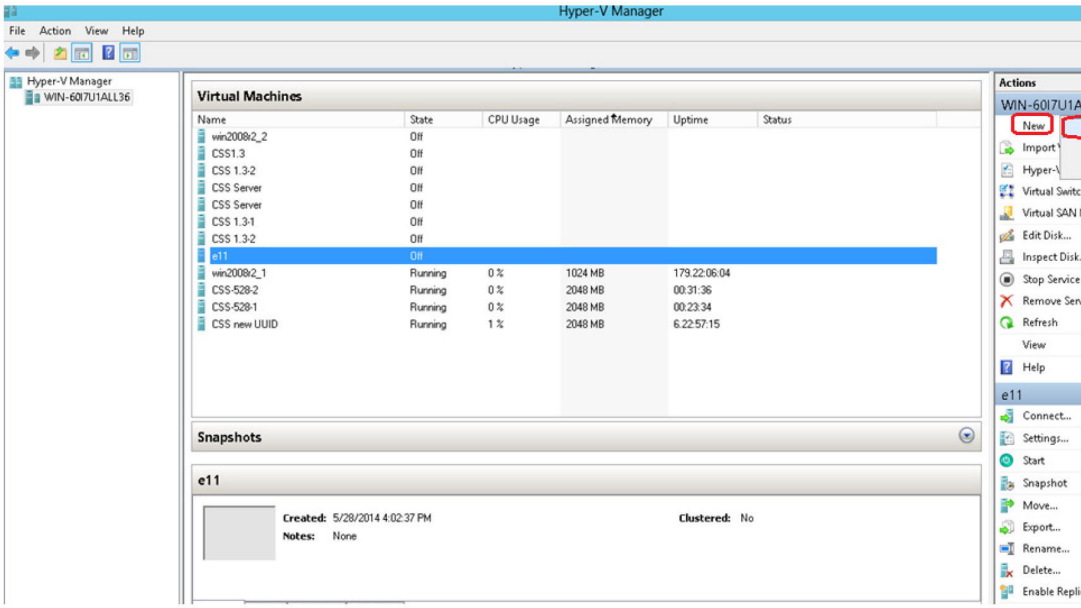
For information on installing the Hyper-V Role on Windows Server, refer to the Hyper-V Role web site.

Ensure your server meets the Hyper-V Role specifications. In addition, make sure to edit the BIOS of your server to enable Virtualization of the CPUs.

To install the ContentConnect server, you need the pre-configured VHD installation package. Download these files to a location on your computer, so you can navigate to them during the install.

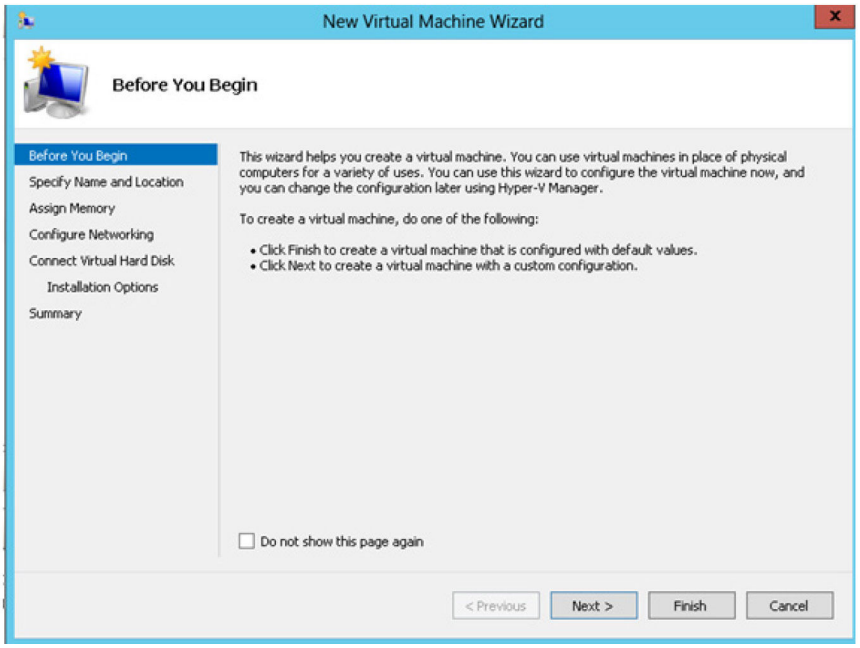
Note: A VHD package cannot be installed twice from the same directory. If you plan to install the VHD package more than once, for example, to set up a ContentConnect cluster, you are recommended to copy the original VHD file to another folder first and install each time from the new directory.

1. Log in to Hyper-V Manager.
2. From the Hyper-V Manager Action panel, select New > Virtual Machine.

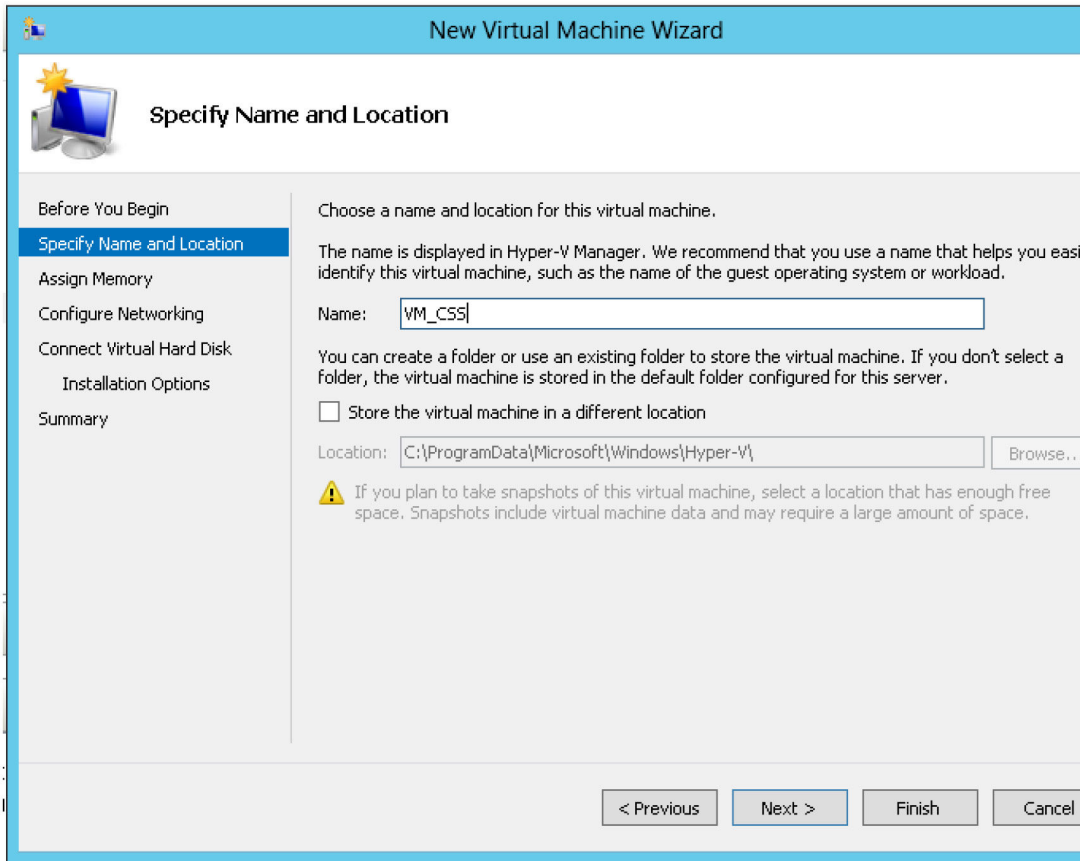


The New Virtual Machine Wizard displays.

3 From the Before you Begin window (shown next), click Next.



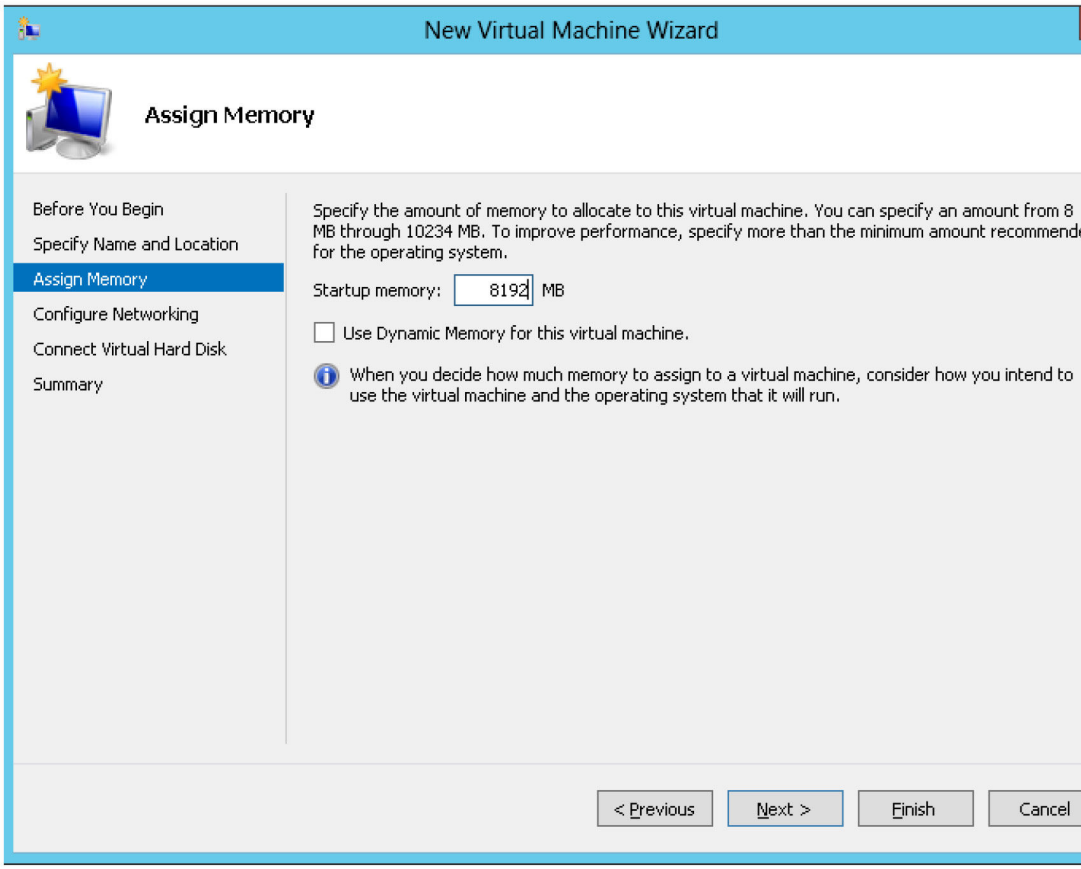
4 Enter a name for your virtual machine.
Click Next.



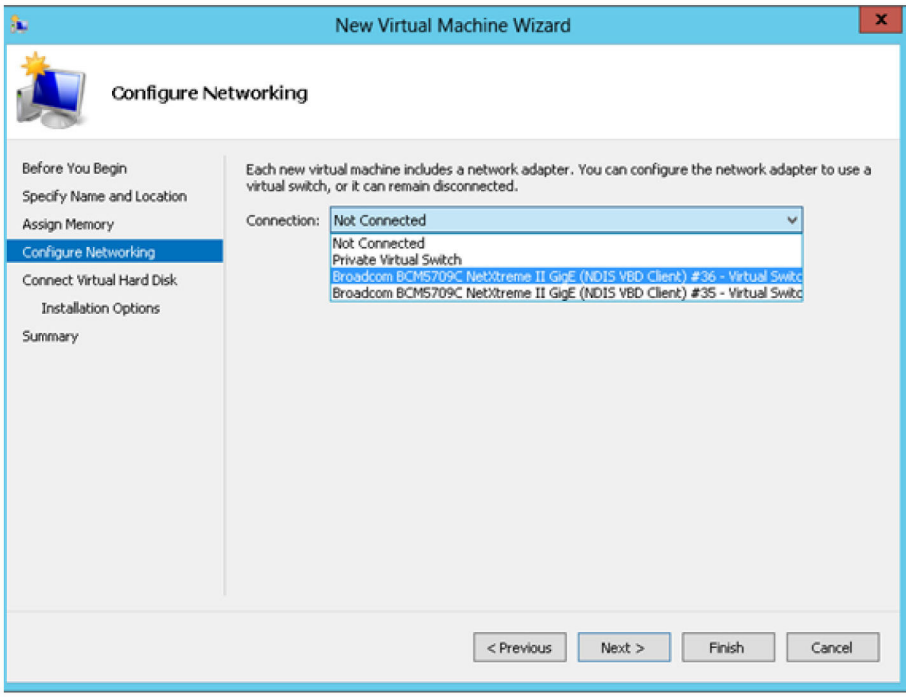
You can also select Store the virtual machine in a difference location, and then select Browse to specify a location.

5 Enter the amount of memory to allocate to this virtual machine.
Click Next.

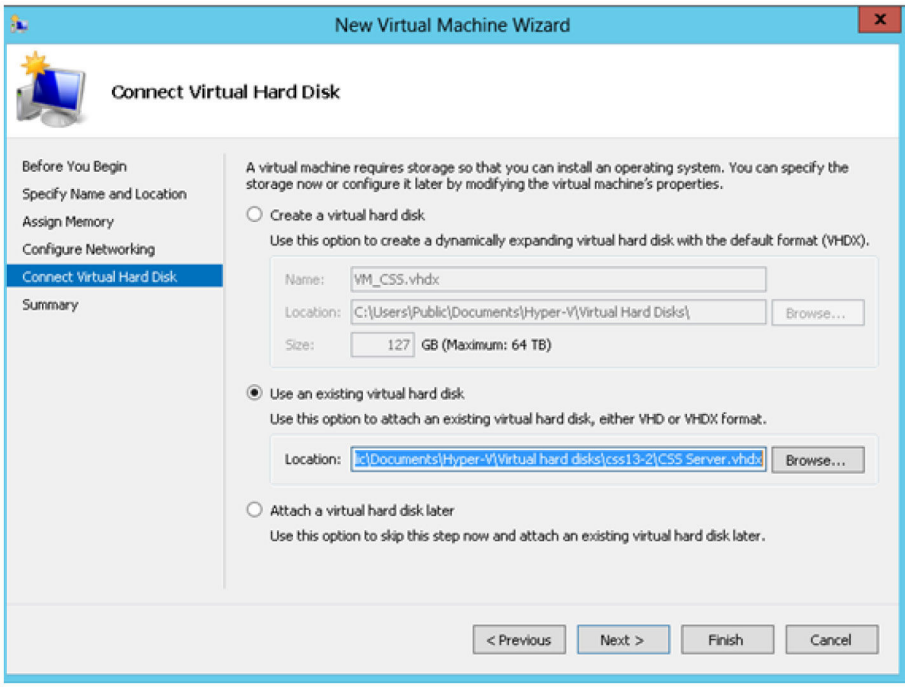
Refer to Polycom® RealPresence® ContentConnect Release Notes, *Hardware and Software Requirements* for host memory requirements.



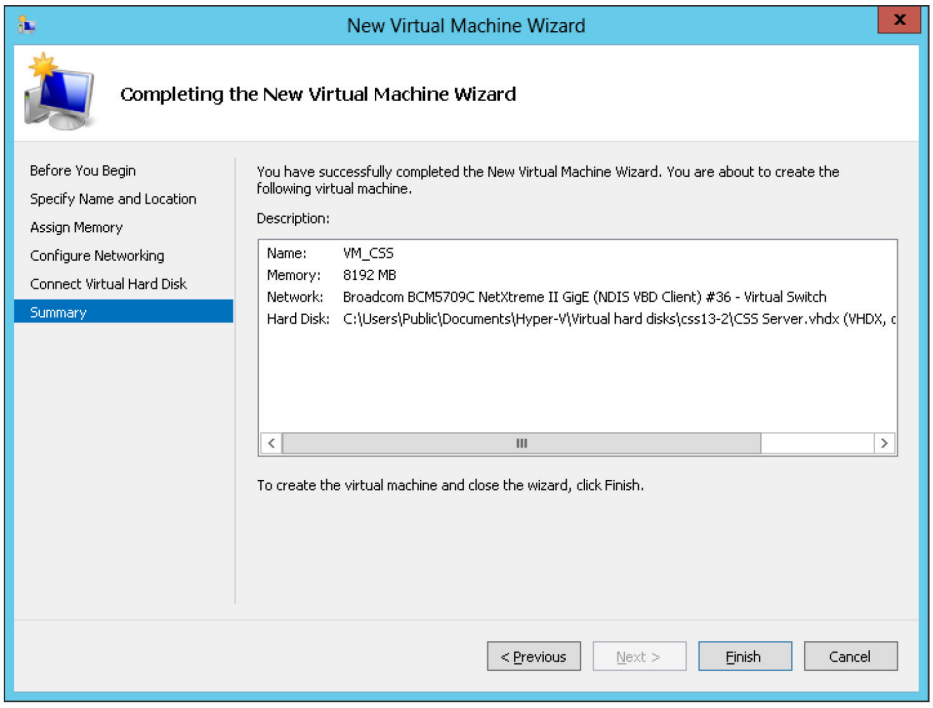
6 Select a network adaptor from the Connection drop-down list to use with a virtual switch.
Click Next.



7 Select Use an existing virtual hard disk and click Browse to navigate to the ContentConnect virtual hard disk.
Click Next.

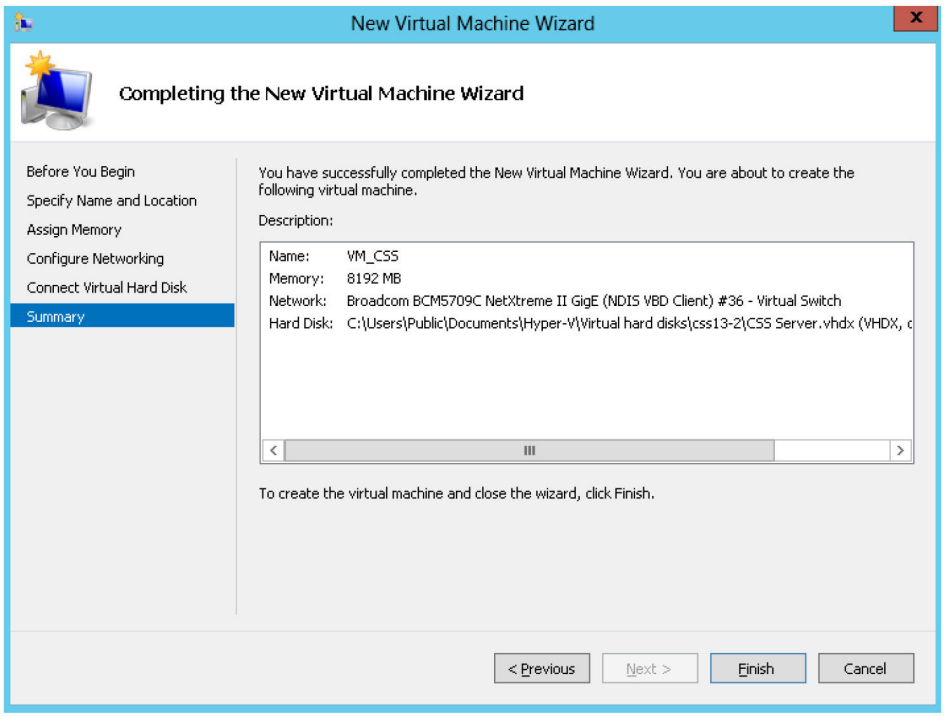


8 Verify the information in the Summary list.
Click Finish to close the wizard.

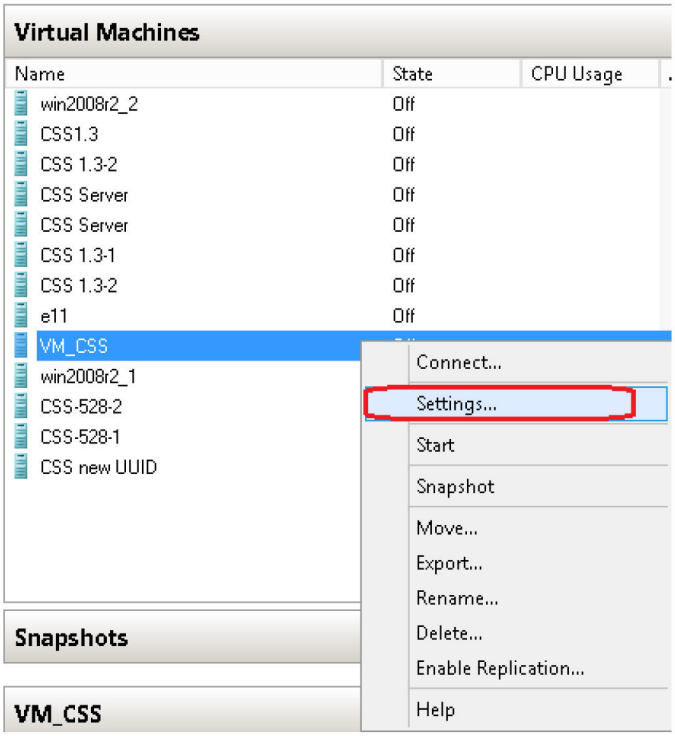


You can find your ContentConnect virtual machine in the Virtual Machines pane.

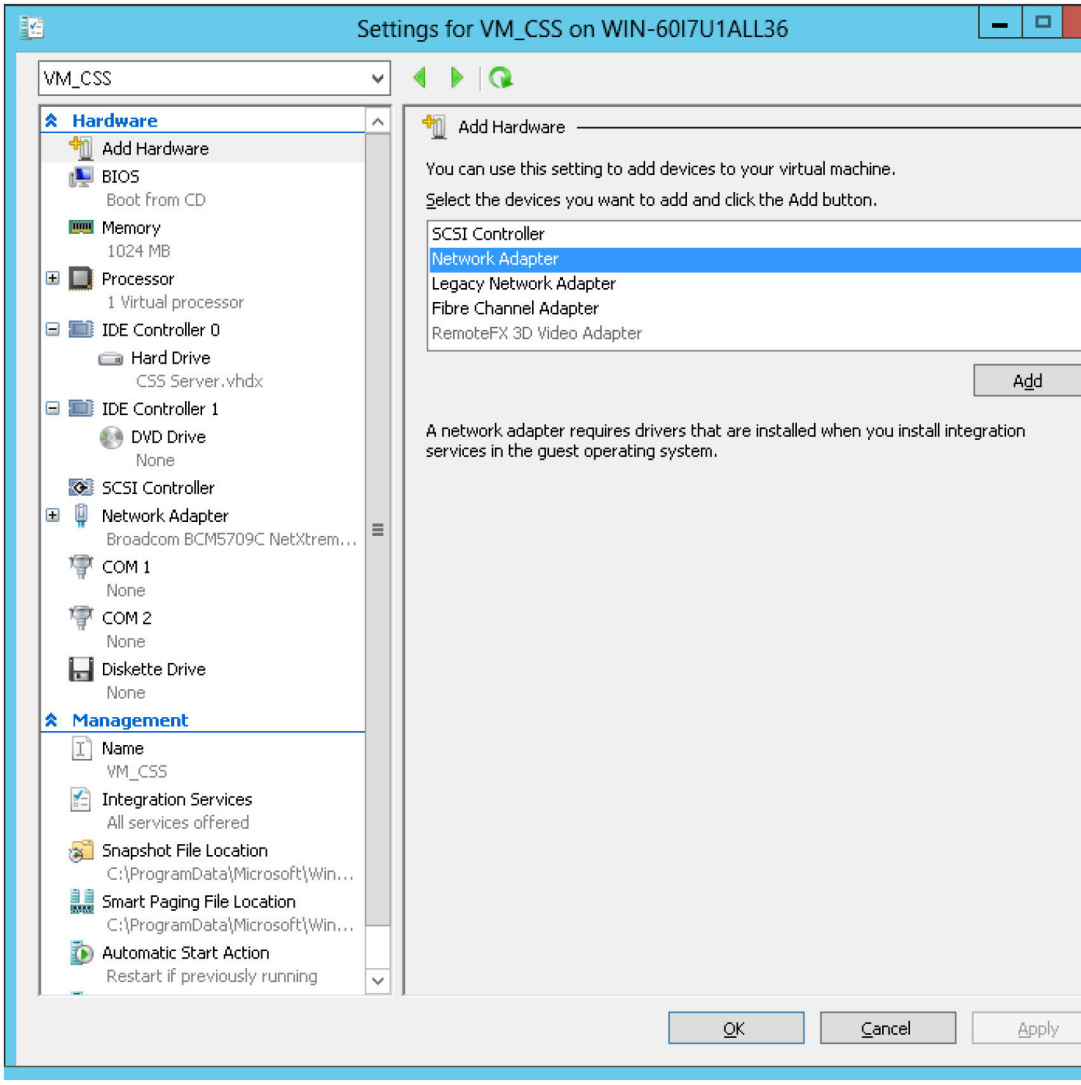
9 Select your virtual machine and click Settings.



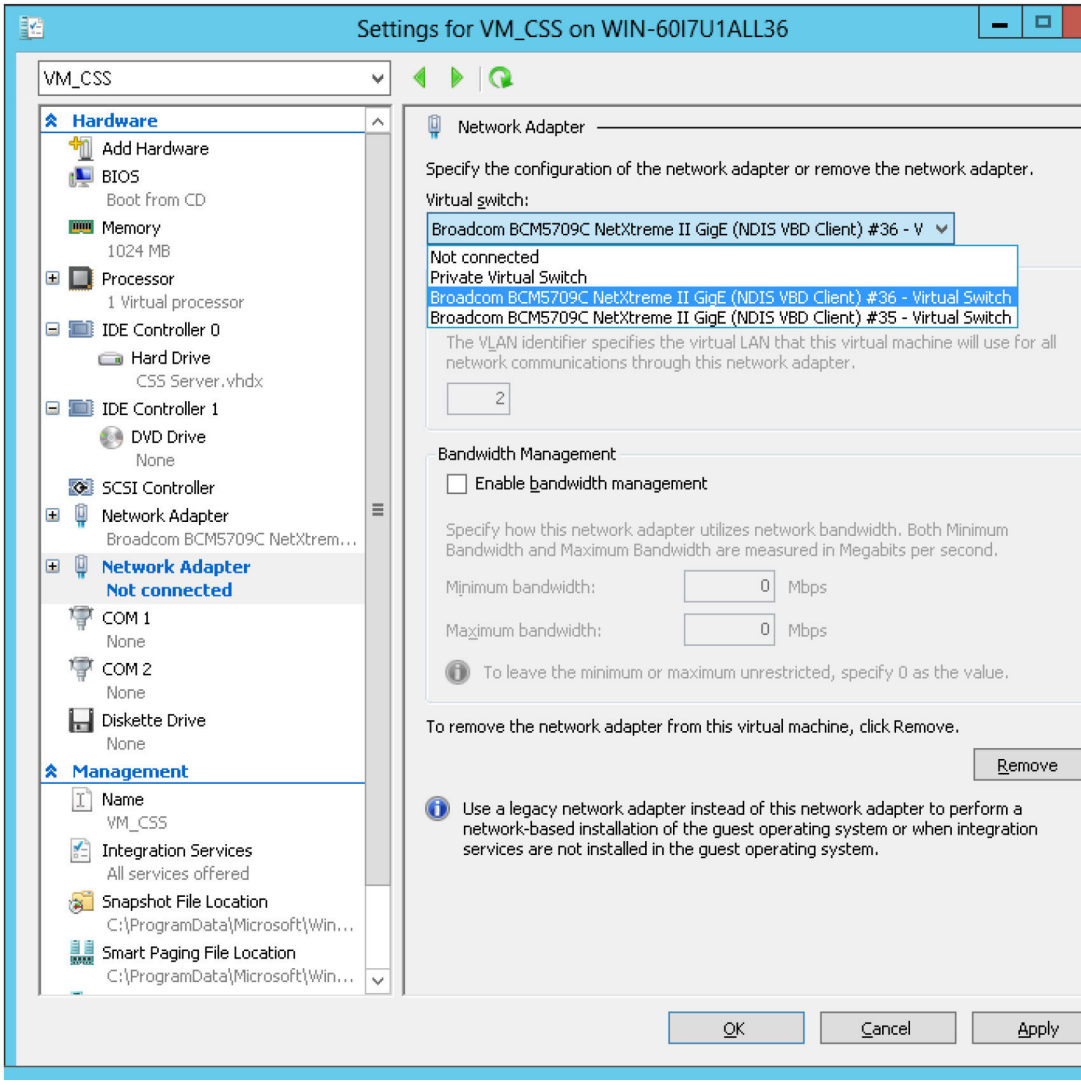
10 Navigate to your virtual server, right-click the virtual server name and select Settings.



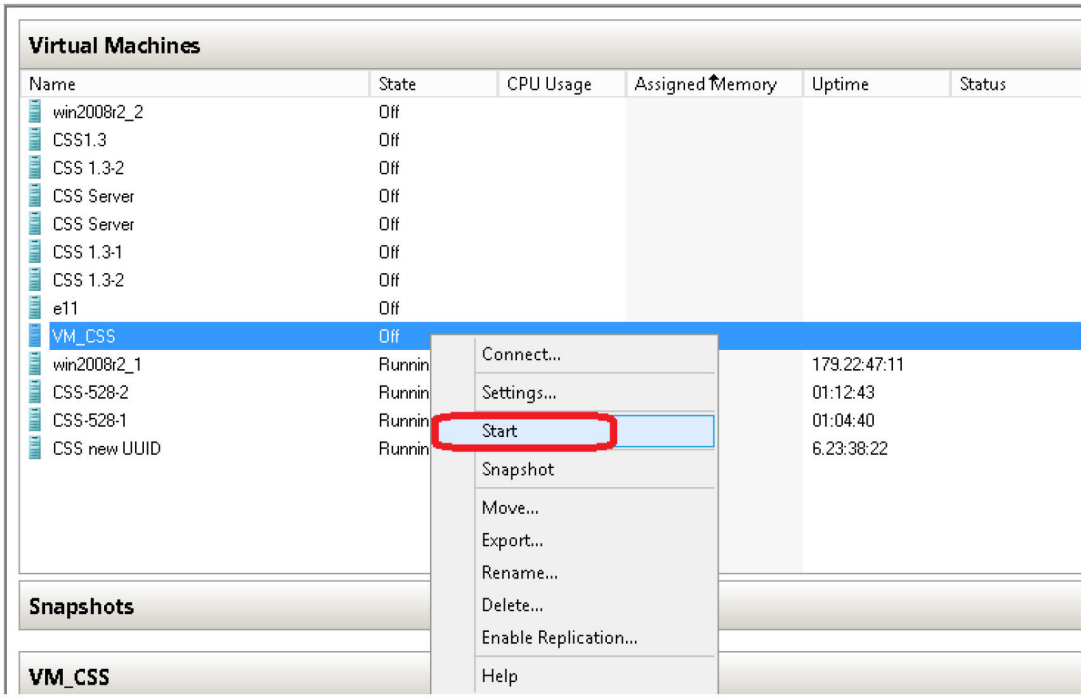
11 The ContentConnect virtual machine needs two network adaptors to work. Add another network adaptor. From the Add Hardware window, select Network Adapter, and then click Add.



12 Select the network adapter you selected in step 6.
Click OK.



13 Navigate to your virtual server, right-click the virtual server name and select Start.



14 Configure network settings.
Network settings can be configured dynamically (the default method) or statically. If network settings are configured dynamically, all network settings will be obtained from the DHCP server. If you configure static network settings, you need to enter IP addresses for the network parameters manually.

- Dynamic configuration If you installed the ContentConnect server using DHCP mode, you can obtain the ContentConnect server's IP address by navigating to the ContentConnect server from Hyper-V Manager, and then open a console. Enter cssadmin and CssNET*76 for your user name and password, and then run “ifconfig” commands.
- Static configuration If you need to configure network settings statically, manually configure the network settings. From Hyper-V Manager, open a console window and press Enter to obtain a prompt. Enter polycom and polycom for your user name and password.
- Follow the on-screen instructions to change the following:
- Change Host Name (Optional)
- Configure DNS (Required)
- Configure Network (Required)
- Change Password (Optional)

The ContentConnect server is installed. You can now access the ContentConnect server Web Configuration Tool and configure the server. To access the tool, enter http://<your server ip address>/admin in your browser's address bar.

Related Concepts

[Required ContentConnect Product Components](#) on page 20

[Optional Solution Components](#) on page 19

The following table lists optional and compatible components that you can install and set up before you deploy ContentConnect.

[Required Prerequisite Components](#) on page 18

The following table lists required components that must be set up in your environment before you deploy ContentConnect.

Installing the Polycom ContentConnect Add-on for Microsoft Lync on page 41

You must install RealPresence Content Add-on only if you choose to run your ContentConnect server under Add-On mode.

Configuring the ContentConnect Server on page 61

To configure the ContentConnect server, you need to access the ContentConnect server Web Configuration Tool, which enables you to configure and update the ContentConnect settings from a remote PC.

Statically Configure the Network

After you install the ContentConnect server, you must log in to it remotely by console using PuTTY or another SSH Client tool to statically configure the network.

Note: You can update the ContentConnect server network settings using the ContentConnect server Web Configuration Tool.

ContentConnect supports only the first two NICs on the server (called eth0 and eth1). Even though the server can handle four NICs, ContentConnect uses only the first two.

1 Configure the following basic options:

   A Enter the ContentConnect server IP address in the Host Name (or IP address) field.

   B Enter 22 in the Port field.

   C Select SSH for the Connection type.

2 Click Open.

3 Enter the user name (cssadmin) and password (CssNET*76).

Installing Lync Client Machine Components

You need to install the following two components on each Lync Client machine:

- Microsoft .NET Framework 4 Client Profile
- Polycom ContentConnect Add-on for Microsoft Lync (required only if your ContentConnect server runs in the Add-On mode)

Microsoft .NET Framework 4 Client Profile must be installed on the Lync client machine before you install Polycom ContentConnect Add-on for Microsoft Lync.

Install and Deploy the .NET Framework 4 Client Profile

You need to install and deploy the Microsoft .

NET Framework 4 Client Profile on each Lync client machine before you can install the Polycom ContentConnect Add-on for Microsoft Lync.

Check to see if Microsoft .NET Framework 4 Client Profile is already installed on your machine. If it is, you are ready to install the Polycom ContentConnect Add-on for Microsoft Lync. Microsoft .NET Framework 4 Client Profile is a default component of Windows 7.

1 Download the Microsoft .NET Framework 4 Client Profile installation package (dotNetFx40_Client_x86_x64.exe) from www.microsoft.com/en/download/details.aspx?id=24872.

2 Install and deploy the Microsoft .NET Framework 4 Client Profile on the Lync Client machine.
To do this, see the *.NET Framework Deployment Guide for Administrators*, available from Microsoft web site.

Note: You can silently install the Microsoft .NET Framework 4 Client Profile to Lync Client machines. To do this, use the following command:

```
dotNetFx40_Client_x86_x64.exe /q
```

Upgrading Windows Installer

Windows Installer is the application installation and configuration service for Windows.

To install the Polycom ContentConnect Add-on for Microsoft Lync, your PC's Windows Installer software should be version 4.5 or later.

Installing the Polycom ContentConnect Add-on for Microsoft Lync

You must install RealPresence Content Add-on only if you choose to run your ContentConnect server under Add-On mode.

If the Microsoft .NET Framework 4 Client Profile is installed on the Lync client's machine, you can install the Content Add-on for Lync on the Lync client's machine. The Content Add-on for Lync installation file is provided in two different formats, .exe and .msi.

An administrator can push the Content Add-on for Lync to multiple users (using the .msi file), or an end user can install the add-on on their computer (using the .exe file).

After you install the Content Add-on for Lync, verify that it installed successfully.

Related Tasks

Install the OVA-Formatted Installation Package on VMware vSphere on page 24

To install the ContentConnect server, you need the Open Virtualization Appliance (OVA) installation package.

Install the VHD-Formatted Installation Package in a Hyper-V Environment on page 31

For information on installing the Hyper-V Role on Windows Server, refer to the Hyper-V Role web site.

Verify that the Content Add-on for Lync Installed Successfully on page 45

You can verify that the Content Add-on for Lync installed correctly.

Configure ContentConnect Server Running Mode on page 64

Using the .msi file

The .

msi file is intended for use by experienced Windows administrators to support pushed and silent installations. These procedures use mechanisms such as Group Policy Objects. You should already be familiar with these mechanisms to use the .msi installation file.

Note that you must exit Lync before you perform the silent installation. If you don't exit Lync, error messages will display near your Window's taskbar after the install. Exit and restart Lync. In addition, a progress bar (which also displays near your taskbar) will not go away. If you receive the error message and the progress bar won't go away, click the red X on both screens and restart the Lync Client application.

You must reboot your system after the installation for changes to take effect.

Note: The .msi file cannot be used for local standalone installation by simply running it in a non-silent way (such as double clicking it), because some of the components cannot be installed successfully in this way.

Note: Before you execute any of the commands described in this section, right click cmd (within Windows 7) and select Run as Administrator. If you don't do this, the commands won't run.

Build a Desktop Management or Group Policy Object

You can build a desktop management or group policy object.

1. Write the .msi installation file to a directory (for example, c:\temp) on the user's local system.
2. Use msiexec to install, uninstall, upgrade, or downgrade the ContentConnect program.
   - The following is an example of using the installer from the directory where the Content Add-On for Lync .msi file resides (make sure you're at the C: prompt before running this command): msiexec /qn /i "RealPresenceContentAddonForLync.msi" [CSSSAUTOFIND=0|1] [CSSSADDRESS=Server_IP] [CSSSHOWDOWNLOAD=0|1] /l*v CSS_install.txt
   - When running the installation from a directory other than the directory where the executable resides, include the full path in the command. Here is an example: msiexec /qn /i " c:\temp\RealPresenceContentAddonForLync.msi" [CSSSAUTOFIND=0|1] [CSSSADDRESS=Server_IP] [CSSSHOWDOWNLOAD=0|1] /l*v CSS_install.txt The following parameters are optional:
   - CSSSAUTOFIND 0: auto find ContentConnect server (default); 1: specify ContentConnect server
   - CSSSADDRESS Specify ContentConnect server address
   - CSSSHOWDOWNLOAD 0: do not show download dialog; 1: show download dialog, (default);
3. To verify that the software is installed, see Verify that the Content Add-on for Lync Installed Successfully.

   Note: You can upgrade or downgrade from different versions of the server using an .msi or .exe file. During this process, the old configuration data will be removed. When installing a newer version, set your preferred install directory, or else the directory will be set to default.

Uninstall Content Add-On for Lync

You can uninstall content add-on for Lync.

Do one of the following:

- Use the following command from the directory where the Content Add-On for Lync .msi file resides: msiexec /qn /x "RealPresenceContentAddonForLync.msi" /l CSS_Uninstall.txt
- When running the uninstallation from a directory other than the directory where the executable resides, include the full path in the command. Here's an example: msiexec /qn /x "c:\temp\RealPresenceContentAddonForLync.msi" /l CSS_Uninstall.txt

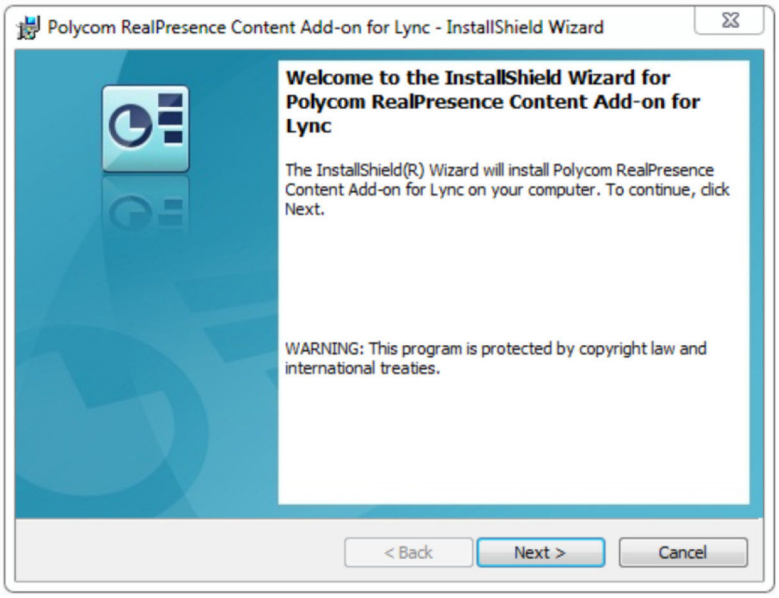
Note: While uninstalling the Content Add-on for Lync, the Content Add-on for Web won't be uninstalled automatically and must be uninstalled manually from the computer's Control Panel.

Use the .exe file

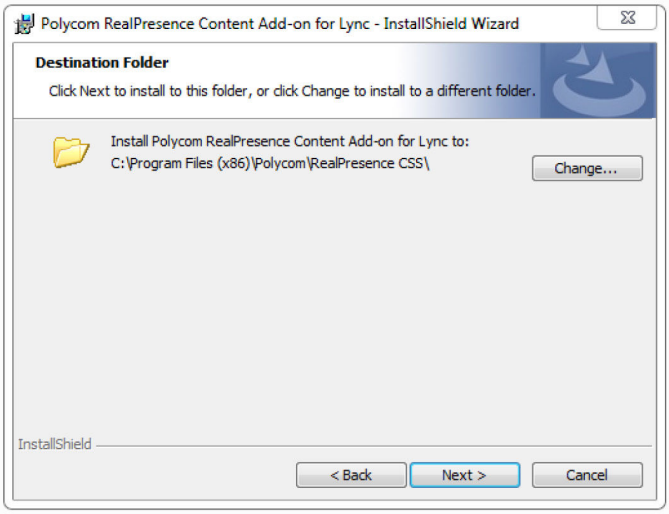
The Content Add-On for Lync .

exe file is intended for easy, interactive installations by end users who do not require extensive customization.

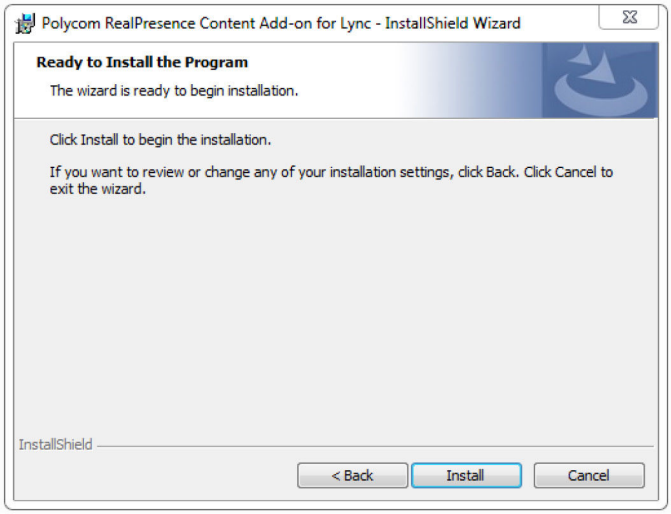
1. Exit Lync.
2. Download the Polycom ContentConnect Add-on for Microsoft Lync .exe file to your computer.
3. Double-click the .exe file, and wait while the Content Add-on for Lync prepares the InstallShield Wizard.
4. When the InstallShield Wizard opens, click Next.



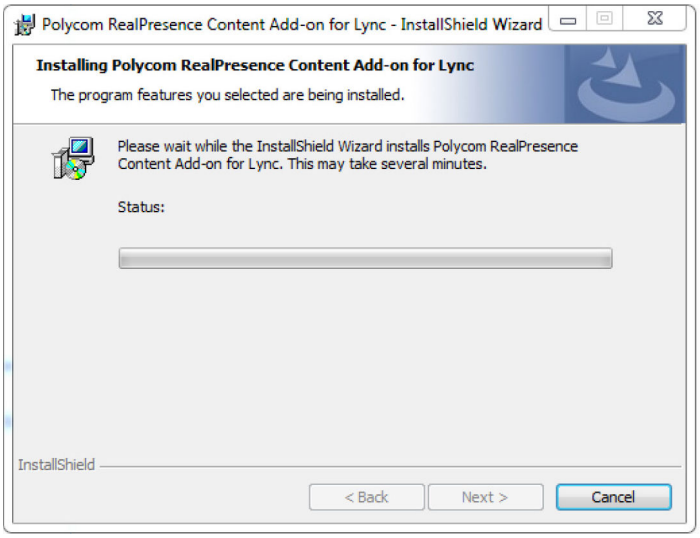
5. From the License Agreement window, review the license terms, and if you accept them, click Next.
6. From the Destination Folder window (shown next), accept the default location to install the Polycom ContentConnect Add-on for Microsoft Lync (or change the location), and click Next.



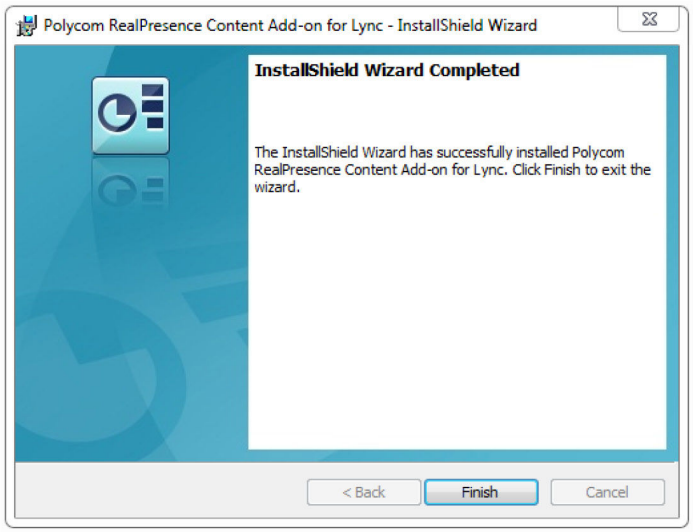
7 From the Ready to Install the Program window (shown next), click Install.



8 An Installing window displays and a message on your task bar that indicates the Content Add-on for Lync is loading.
Wait while the installation completes.



9 When the installation completes, the InstallShield Wizard Completed window displays (as shown next).
Click Finish.



10 The Polycom ContentConnect Add-on for Microsoft Lync is now installed. You'll see a system restart message box. Click Yes to complete installation.

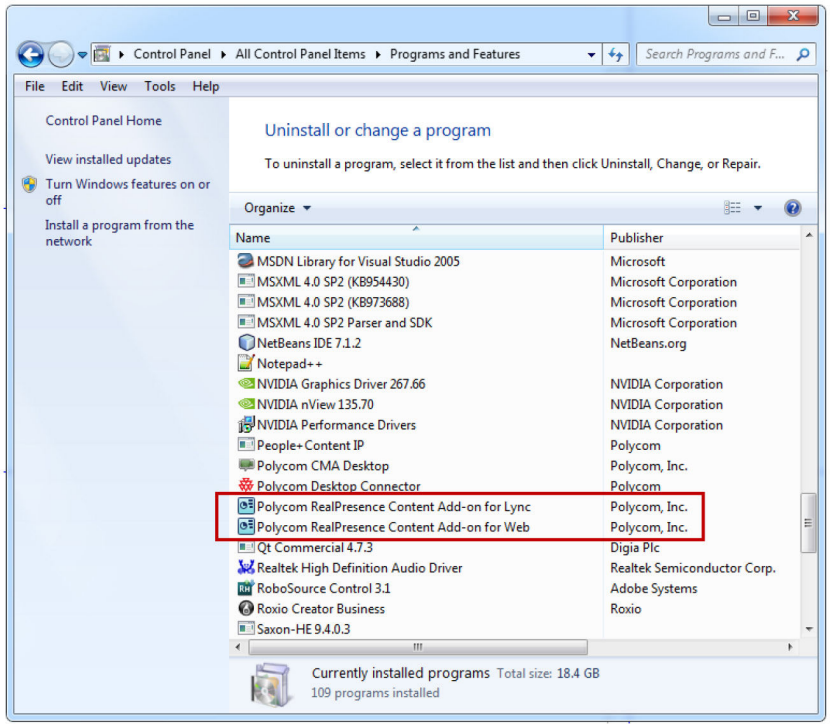
Note: A service - Polycom ContentConnect Add-on for Microsoft Lync Service - runs after you install the Content Add-on for Lync (as shown next). If you do not want to enable the Content Add-on for Lync, you can stop the service, exit the Lync Client, and then sign in to Lync again.

Verify that the Content Add-on for Lync Installed Successfully

You can verify that the Content Add-on for Lync installed correctly.

1 Open the computer's Control Panel.

2 Navigate to Programs and Features.
Two programs- Polycom ContentConnect Add-on for Microsoft Lync, and Polycom RealPresence Content Add-on for Web - will display in the Program list, as shown next.



When you install the Content Add-on for Lync on the computer, the Content Add-on for Web is automatically installed as well.

Related Concepts

Installing the Polycom ContentConnect Add-on for Microsoft Lync on page 41

You must install RealPresence Content Add-on only if you choose to run your ContentConnect server under Add-On mode.

Setting Up a High Availability (Hot Standby) Environment

You can set up your ContentConnect solution with two ContentConnect servers so that when one server (the master) fails, the other server (the slave) can take over.

This is called High Availability (or Hot Standby). In a High Availability (Hot Standby) environment, a master server sends regular heartbeat messages to a slave server. If the master server fails, or the Ethernet link to the master server is unavailable, the slave server takes over and works as the master server. If the original master resets, it works as the slave server.

To set up a High Availability (Hot Standby) environment, you'll need to deploy a master ContentConnect server virtual machine to one physical machine and a slave ContentConnect server virtual machine to another physical machine. You'll also have to ensure that each ContentConnect server has a physical interface to reach outside, and configure High Availability (Hot Standby) settings using the ContentConnect server Web Configuration Tool.

Note: Currently a ContentConnect server has two separate NIC's, NIC1 for heartbeat to keep live in High Availability and NIC2 for HTTPS service. The ContentConnect server has a limitation when configuring High Availability: The two NIC's cannot be configured with IP addresses in the same subnet. In addition to this, due to the way that the OS handles routing, the NIC1 cannot reside on the same subnet as any conferencing equipment that it may need to communicate with. For example, Polycom

Collaboration Server (RMX), Polycom RealPresence Distributed Media Application (DMA), Lync AVMCU, and so on.

Activate Licenses in High Availability (Hot Standby) or Multi-Server Environments

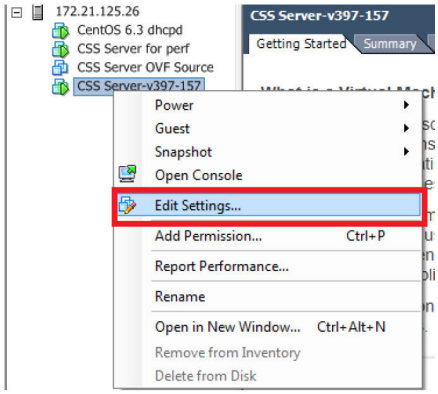
You need to buy additional license to enable High Availability on the active ContentConnect server.

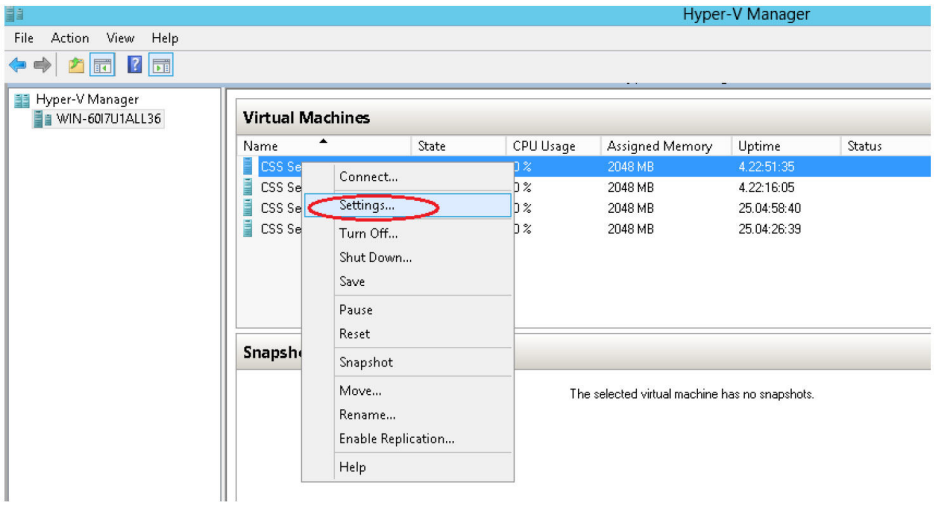
Please check Price List for SKU information.

High Availability license should be activated on the active server. The redundant server does not need additional license; it shares it from the active server.

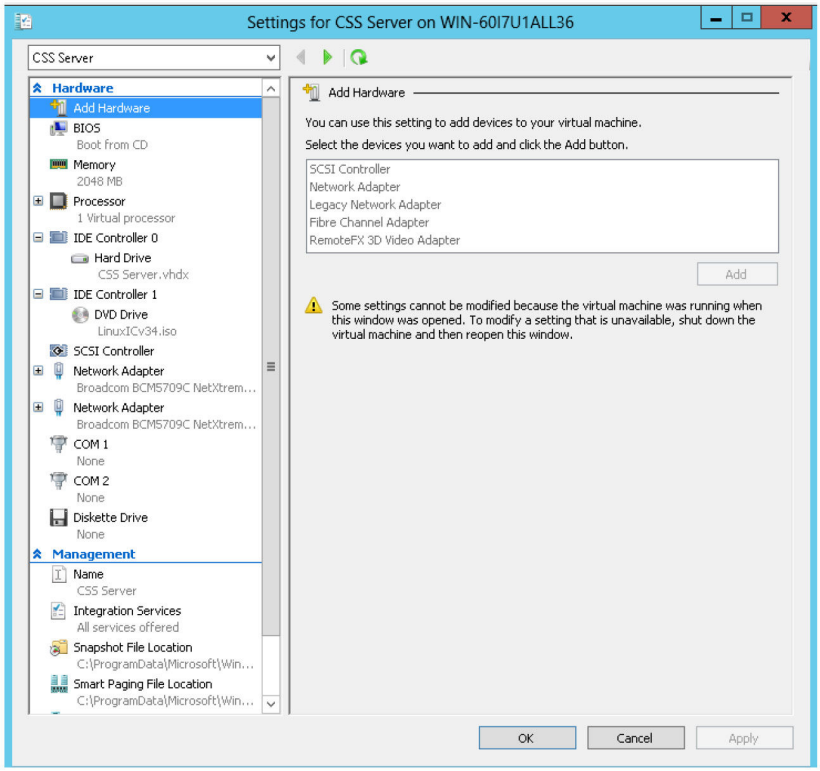
Note: In a High Availability (Hot Standby) environment, if you update your ContentConnect from version 1.2 to 1.3 or later, HA configuration is lost and HA is unavailable. You must activate the master ContentConnect and then re-configure the HA to make it work again. The slave ContentConnect is activated automatically after the master is activated. Earlier versions of ContentConnect have a different licensing mechanism. Refer to the respective Administrator's Guide for more information.

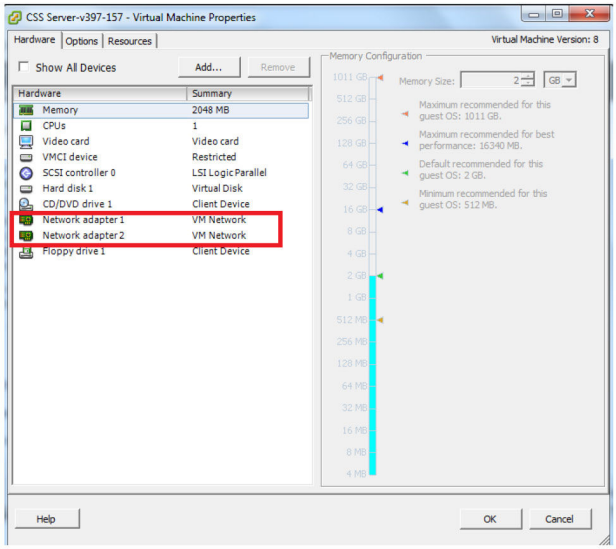
1. Install two ContentConnect servers.
   Each ContentConnect server must be installed in its own physical machine.
2. Check the NIC settings for the two ContentConnect servers:
3. From the vSphere Client or Hyper-V Manager, navigate to the candidate High Availability server, right-click the server and select Polycom RealPresence Content Add-on for Web(for vSphere Client) or Settings (for Hyper-V Manager).





4 Confirm that both network adapters are on the same virtual switch (as shown).





5 Configure High Availability (Hot Standby) settings using the ContentConnect server Web Configuration Tool.
To configure these settings, see Enabling High Availability (Hot Standby).

Related Concepts

Installing the ContentConnect Server Components on page 24

Configuring Solution Components

The following sections show you how to configure ContentConnect solution components so the solution will work properly.

If a solution component does not require special configuration to work with ContentConnect, it is not addressed.

You'll learn how to set up the Lync client to find the ContentConnect server address, and how to configure RealPresence Collaboration Server (RMX) and DMA. You'll also learn how to configure optional components - RealPresence Access Director Acme Packet® Net-Net Enterprise Session Director (ESD), and a load balancer - and how to use the ContentConnect server Web Configuration Tool to configure the ContentConnect server.

The following discussion assumes that the prerequisite components are already set up for a typical deployment, and configured to work in a Microsoft Lync environment.

To configure Polycom products to work within a Lync environment, see the *Polycom Unified Communications Deployment Guide for Microsoft Environments*.

To review general configuration information for Polycom products, refer to the relevant documentation on the Polycom Support site.

Configure Lync Clients to Auto-Discover the ContentConnect Server Address

Note: Auto-Discover the ContentConnect server Address applies to the Add-On mode only.

You must configure the Lync 2010 or Lync 2013 client to auto-discover the ContentConnect server address. To do this, you must configure the DNS server, so that it can resolve ContentConnect queries by the ContentConnect server's host name or IP address. Polycom recommends that you configure the DNS server to find the ContentConnect server by its Fully Qualified Domain Name (FQDN). This ensures that the Lync client can access the ContentConnect server. The DNS should also have entries for your Active Directory server (if different from the DNS.)

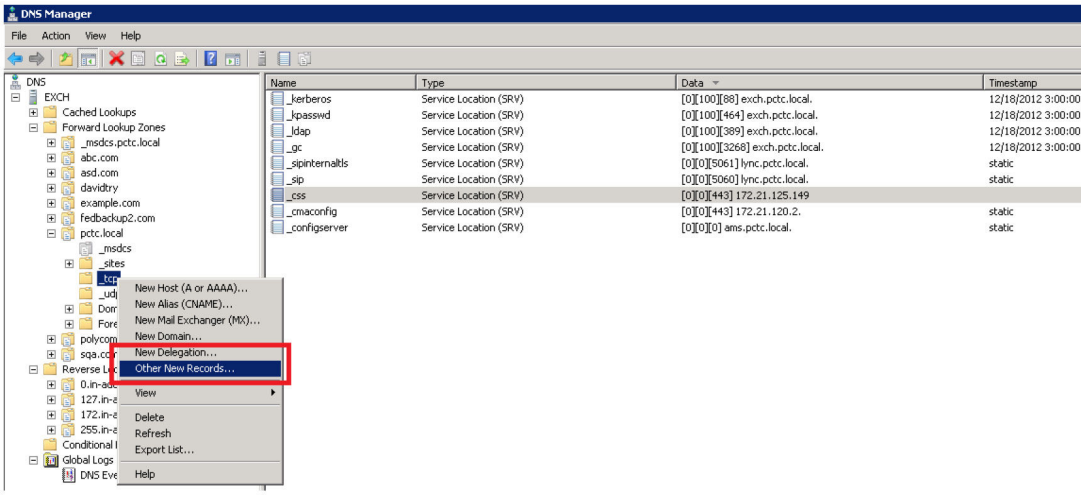
A Lync client must be able to automatically discover the address for the ContentConnect server. This means you must add the DNS service record (SRV record) for the ContentConnect server. The lookup key for this service record is _css_tcp. So the record will resemble this:

_css._tcp.customerdomain.com 86400 IN SRV 0 0 443 css.customerdomain.com

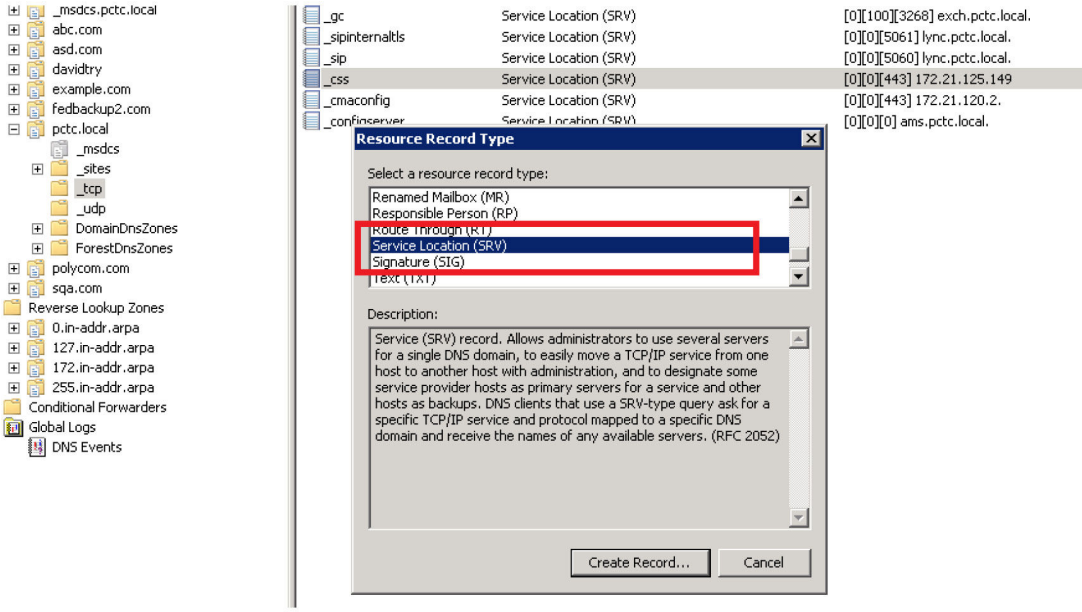
The SRV record _css_tcp is required for the domain suffix of the Lync user sign-in address.

For more information about DNS, DNS records, and how DNS works, see Microsoft Technet.

1 From the DNS Server, DNS Manager, select Forward Lookup Zones > your domain > _tcp > Other New Records, as shown next.

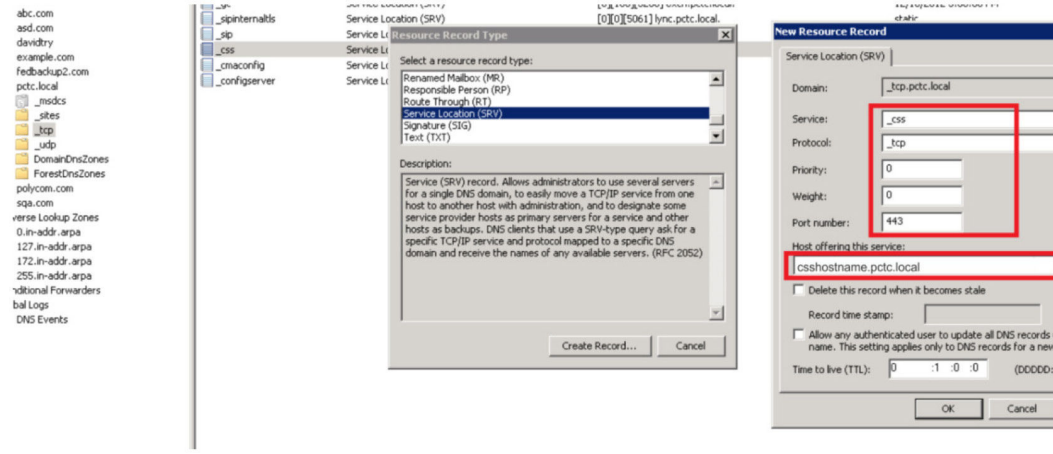


2 From the Resource Record Type dialog box, select Service Location (SRV), as shown next.



3 From the New Resource Record dialog box (as shown next), configure the following:

- Service _css
- Protocol _tcp
- Port number 443
- Host offering this service the IP address or FQDN of the ContentConnect server inside the company, or the IP address or FQDN of REALPRESENCE ACCESS DIRECTOR or ACME outside the company



4 To validate, query for the record from a Window Command prompt. Here's an example:

```
nslookup -q=srv _css._tcp.<domain>.com
```

Configuring RealPresence Collaboration Server (RMX) for ContentConnect

For ContentConnect, RealPresence Collaboration Server (RMX) 8.

1 is the minimum requirement.

To configure the RealPresence Collaboration Server to work within a Lync environment, see *Configure RealPresence Collaboration Server (RMX) for Polycom ContentConnect Software* in the *Polycom Unified Communications Deployment Guide for Microsoft Environments*, available from the Polycom Unified Communications Solution for Microsoft Environments support page.

Configuring DMA for ContentConnect

There are no ContentConnect-specific DMA settings you need to configure.

However, you need to configure certain DMA settings to deploy DMA in a Microsoft Lync environment. To configure DMA to work within a Lync environment, see *Deployment Process for Polycom DMA Systems* in the *Polycom Unified Communications Deployment Guide for Microsoft Environments*, available from the Polycom Unified Communications Solution for Microsoft Environments support page.

For your DMA setup, consider the following:

- Make sure you configure a DMA system SIP peer for the Lync server. Within the DMA system, you need to configure an external SIP peer for the Microsoft Lync Server. This allows SIP calls routed from the DMA system to reach devices registered to the Lync Server. For more information, see the *Polycom Unified Communications Deployment Guide for Microsoft Environments*.

- If you didn't configure a conference profile to utilize ContentConnect in RealPresence Collaboration Server (RMX), you'll need to create a conference template in DMA. For the template, make sure you select the Send content to legacy endpoints (MPM+ or newer). Selecting this setting enables endpoints that don't support H.239 to receive the Content channel over the video (People) channel. For information on creating conference templates in DMA, see the *Operations Guide* for your DMA system, available from the Polycom Distributed Media Application support page.
- If your running mode is Gateway, add a dial rule for authorized calls for external SIP peers, with the following settings:
  - Description External Lync SIP peer.
  - Action Resolve to external SIP peer.
  - Preliminary Enabled No.
  - Enabled Enabled.

Configuring Session Border Controllers for ContentConnect

If your ContentConnect solution deploys the ContentConnect server behind a firewall, you need to install and configure either RealPresence Access Director or an Acme Packet system.

In this section, you'll learn how to configure your RealPresence Access Director and Acme Packet system for ContentConnect.

Configure RealPresence Access Director for ContentConnect

To download ContentConnect client package from ContentConnect server through RealPresence Access Director, the RealPresence Access Director version must be 3.1 or higher.

1 Configure HTTPS proxy settings

- For the Next hop address, enter the IP address of the ContentConnect server. Access Proxy forwards requests to this address.
- For the Port, enter 443.
- From the System list, select Polycom ContentConnect.

  Note: Do not select the Require client certificate from the remote endpoint check box. The RealPresence Content Add-on does not support this functionality.

2 Configure SIP settings

- For the SIP registrar (Next hop) address, Port, and Transport type, enter the IP address of DMA, the DMA port, and the DMA transport type.
- For the SIP proxy (Next hop) address, Port, and Transport type, enter the IP address of DMA, the DMA port, and the DMA transport type.

For more information on how to configure these settings, refer to the RealPresence Access Director Administrator's Guide available on BARhttps://support.polycom.com.

Configuring Acme Packet Net-Net ESD for Using with RealPresence Desktop/RealPresence Mobile and RealPresence Resource Manager

Your ContentConnect solution may include an Acme Packet system as the session border controller (SBC), so that users outside the company firewall can share and view content.

If your solution utilizes an Acme Packet system, and RealPresence Desktop/ RealPresence Mobile and RealPresence Resource Manager are also deployed, service

port conflicts will exist. This occurs because the Acme Packet system cannot distinguish between HTTP traffic with different HTTP URLs. The Acme Packet system is therefore unable to distinguish between ContentConnect Client and RealPresence Resource Manager provisioning traffic (HTTPS).

You can solve this issue by doing one of the following, as discussed in upcoming sections:

- Distinguish HTTPS traffic using different service ports
- Distinguish HTTPS traffic using different Service IPs

For detailed information about Acme Packet Net-Net ESD, refer to the Acme Packet documentation online at Acme Packet Documentation.

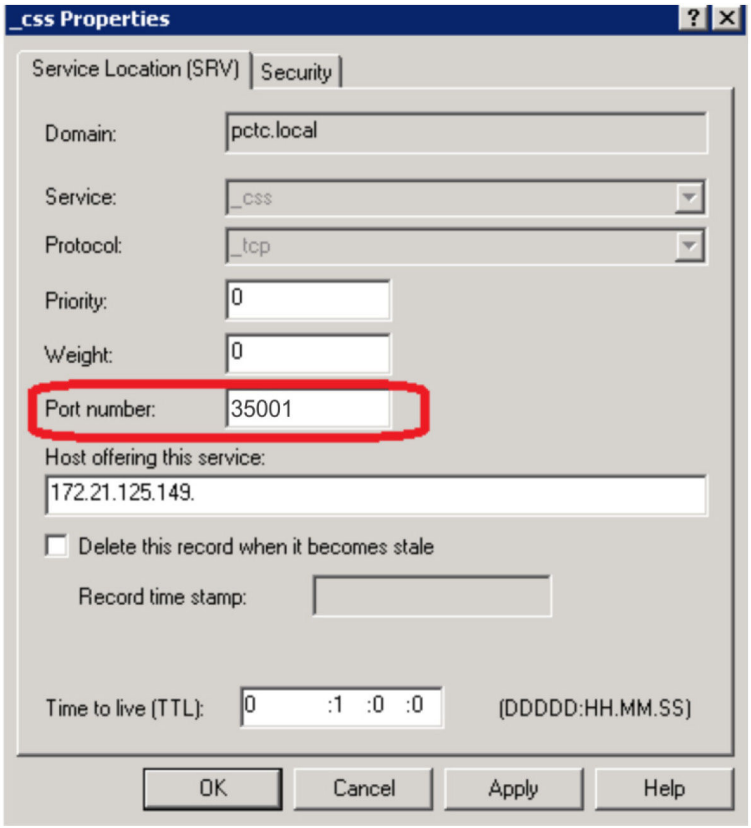
You can also find helpful information in Deploying Polycom Unified Communications in an Acme Packet Environment, available from the Polycom Unified Communications Solution Documentation Download for Acme Packet Net-Net Session Enterprise Director Environment support page.

Distinguish HTTPS Traffic Using Different Service Ports

One way to avoid ContentConnect client traffic conflicting with RealPresence Resource Manager provisioning traffic is to configure the ContentConnect client to send HTTPS traffic to a non-standard port.

To do this, you'll need to add a DNS SRV record on the DNS server so that the ContentConnect service will use the non-standard port.

1 Configure the DNS server by adding an SRV record for the ContentConnect service (as shown).
For the Configure static flow, specify Configure static flow.



2. Telnet to your Acme Packet system, and log in using your system username and password.
3. Type Configure static flow and press Configure static flow to enter Superuser mode.
4. Enter the Superuser password and press the Configure static flow key.
   The system prompt will end with a pound sign instead of a closed-angle-bracket to let you know you are in Superuser mode.
5. In Superuser mode, type Configure static flow (as shown next) and press Enter.

```
ACMEPACKET# configure terminal
```

6. Configure static flow:

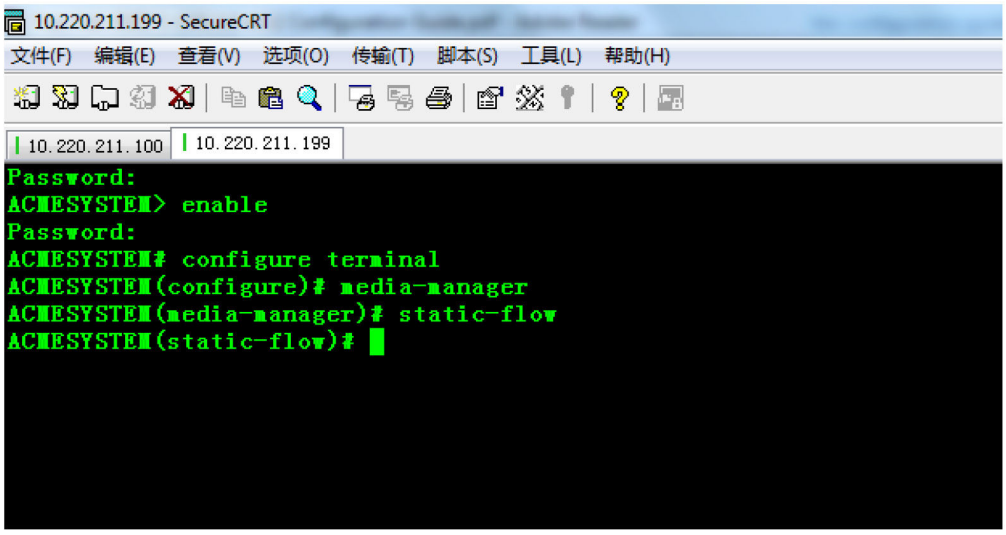
   A Type media-manager (as shown next) and press Enter to access the media-manager path.

   ```
   ACMEPACKET(configure)# media-manager
   ```

   B Type static-flow (as shown next) and press Enter.

   ```
   ACMEPACKET(media-manager)# static-flow
   ```

   - The system prompt changes to let you know that you can begin configuring parameters, as shown next.

7. Configure media policing parameters, as shown next.

```
ACMESYSTEM(static-flow)# select
<in-dest-ip>:
1: dest 10.220.211.100:443; src 0.0.0.0; Access-h323; TCP
2: dest 10.220.211.100:35001; src 0.0.0.0; Access; TCP

selection: 2
ACMESYSTEM(static-flow)# show
static-flow
        in-realm-id                     Access
        description
        in-source                       0.0.0.0
        in-destination                  10.220.211.100:35001
        out-realm-id                    Core
        out-source                      172.21.120.244
        out-destination                 172.21.125.149:443
        protocol                        TCP
        alg-type                        NAPT
        start-port                      30000
        end-port                        30999
        flow-time-limit                 0
        initial-guard-timer             60
        subsq-guard-timer               60
        average-rate-limit              0
        last-modified-by                admin@10.220.210.10
        last-modified-date              2013-03-11 13:07:43
ACMESYSTEM(static-flow)#
```

Note that the range of start-port and end-port on ACME should be identical with the range of udpPortStart and udpPortEnd in the ContentConnect server profile.

The following example shows a static-flow configuration element configured for a NAPT ALG.

in-realm-id

Access
description
in-source

0.0.0.0
in-destination

10.220.211.100:35001\\
(ACME external IP address and provisioning

port)
out-realm-id

Core
out-source

172.21.120.244
(ACME internal IP address)
out-destination

172.21.125.149:443\\
(Content Sharing Server internal IP address and

provisioning port)
Protocol

TCP
alg-type

```
NAPT
start-port

30000
end-port

30999
flow-time-limit

0
initial-guard-timer

60
subsq-guard-timer

60
average-rate-limit

0
last-modified-by

admin@10.220.210.10
last-modified-date

2013-03-11 13:07:43
```

8 Configure the SIP server to allow SIP anonymous calls.
To do this, do the following:

9 Type session-router (as shown next) and press Enter.

```
ACMESYSTEM(configure)# session-router
```

10 Type sip-interface (as shown next) and press Enter.

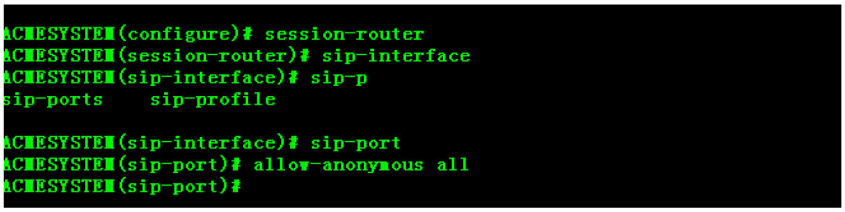
```
ACMESYSTEM(session-router)# sip-interface
```

11 Type sip-port (as shown next) and press Enter.

```
ACMESYSTEM(sip-interface)# sip-port
```

12 Type allow-anonymous all (as shown next) and press Enter.

```
ACMESYSTEM(sip-port)# allow-anonymous
all
```



Distinguish HTTPS Traffic Using Different Service IPs

Another way to avoid ContentConnect client traffic conflicting with RealPresence Resource Manager provisioning traffic is to configure two public IP addresses on the

Acme Packet system - one for the ContentConnect Client, and one for RealPresence Resource Manager.

1. Telnet to your Acme Packet system, and log in using your system username and password.
2. Type enable and press Enter to enter Superuser mode.
3. Enter the Superuser password and press the Enter key.
   The system prompt will end with a pound sign instead of a closed-angle-bracket to let you know you are in Superuser mode.
4. In Superuser mode, type configure terminal (as shown next) and press Enter.

   ```
   ACMEPACKET# configure terminal
   ```

5. Type system (as shown next) and press the Enter key to access the system-level configuration elements.

   ```
   ACMEPACKET(configure)# system
   ```

6. Type network-interface (as shown next) and press the Enter key.

   ```
   ACMEPACKET(system)# network-interface
   ```

   The system prompt changes to let you know you can configure network settings (as shown next).

   ```
   ACMESYSTEM#
   ACMESYSTEM# configure terminal
   ACMESYSTEM(configure)# system
   ACMESYSTEM(system)# network-interface
   ACMESYSTEM(network-interface)# se
   sec-utility-addr    sec-gateway         select

   ACMESYSTEM(network-interface)# select
   <name>:<sub-port-id>:
   1: M00:0      ip=10.220.211.100 gw=10.220.211.254
   2: M10:0      ip=172.21.120.244 gw=172.21.120.254

   selection: 1
   ACMESYSTEM(network-interface)# show
   network-interface
          name                          M00
          sub-port-id                   0
          description                   For External Connection
          hostname
          ip-address                    10.220.211.100
          pri-utility-addr
          sec-utility-addr
          netmask                       255.255.255.0
          gateway                       10.220.211.254
          sec-gateway
   ```

7. Configure physical interface parameters.
   To view all physical interfaces parameters, enter ? at the system prompt.

   To configure all possible IPv4 addresses on which you want the Acme Packet Net-Net SBC to accept administrative traffic, type Add-hip-ip.

   To Select and enter twice, select a network interface parameter to show and update.

The following is an example of what a network interface configuration might look like. Parameters not described in this section are omitted.

```
network-interface
name

M00
sub-port-id

0
description

For External Connection
hostname
ip-address

10.220.211.100\\(ACME external IP)
pri-utility-addr
sec-utility-addr
netmask

255.255.255.0
gateway

10.220.211.254
sec-gateway
gw-heartbeat
state

disabled
heartbeat

0
retry-count

0
retry-timeout

1
health-score

0
dns-ip-primary
dns-ip-backup1
dns-ip-backup2
dns-domain
dns-timeout

11
hip-ip-list

10.220.211.100\\(ACME 1st external IP)
10.220.211.99\\(ACME 2nd external IP)
ftp-address

10.220.211.100
icmp-address

10.220.211.100
10.220.211.99
snmp-address
telnet-address
```

```
10.220.211.100
ssh-address
signaling-mtu

0
```

8 Update the static flow for the second ACME IP address as shown next.
The following example shows a static-flow configuration element configured for a NAPT ALG.

```
in-realm-id

Access
description
in-source

0.0.0.0
in-destination

10.220.211.99:443\\(ACME 2nd external IP
address and provisioning port)
out-realm-id

Core
out-source

172.21.120.244\\(ACME internal IP address)
out-destination

172.21.125.149:443\\(Content Sharing
Server internal IP address and
provisioning port)
Protocol

TCP
alg-type

NAPT
start-port

30000
end-port

30999
flow-time-limit

0
initial-guard-timer

60
subsq-guard-timer

60
average-rate-limit

0
last-modified-by

admin@10.220.210.10
last-modified-date

2013-03-11 13:07:43
```

9 Configure the SIP server to allow SIP anonymous calls.
To do this, do the following:

10 Type session-router (as shown next) and press the Enter key.

```
ACMESYSTEM(configure)# session-router
```

11 Type sip-interface (as shown next) and press the Enter key.

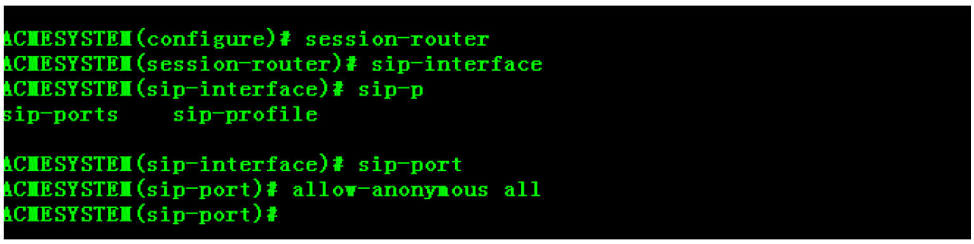
```
ACMESYSTEM(session-router)# sip-interface
```

12 Type sip-port (as shown next) and press the Enter key.

```
ACMESYSTEM(sip-interface)# sip-port
```

13 Type allow-anonymous all (as shown next) and press the Enter key.

```
ACMESYSTEM(sip-port)# allow-anonymous all
```



Configuring the ContentConnect Server

To configure the ContentConnect server, you need to access the ContentConnect server Web Configuration Tool, which enables you to configure and update the ContentConnect settings from a remote PC.

This section shows you how to access the ContentConnect server Web Configuration Tool, and how to navigate and use it. This section also describes the configuration tasks you must perform for the ContentConnect server to work. For information on maintaining and administering the ContentConnect server using the Web Configuration Tool, see Administration and Maintenance Tasks.

Related Tasks

Install the OVA-Formatted Installation Package on VMware vSphere on page 24

To install the ContentConnect server, you need the Open Virtualization Appliance (OVA) installation package.

Install the VHD-Formatted Installation Package in a Hyper-V Environment on page 31

For information on installing the Hyper-V Role on Windows Server, refer to the Hyper-V Role web site.

Access the ContentConnect Server Web Configuration Tool

You can access the ContentConnect server Web Configuration Tool using a web browser installed on your PC.

Before you begin, you will need to ensure that the ContentConnect server and PC are on the same virtual local area network (VLAN); otherwise you won't be able to connect

to the ContentConnect server Web Configuration Tool. To log in to the ContentConnect server Web Configuration Tool, you'll need the IP address of the ContentConnect server you want to configure, and your log in credentials.

Note: The default user credentials are:User ID: adminPassword: admin

If you installed the ContentConnect server using DHCP mode, you can obtain the ContentConnect Server's IP address by navigating to the ContentConnect server from vSphere Client or Hyper-V Manager, and then reviewing the Summary (for vSphere Client) or Networking screen (for Hyper-V Manager) for the server you just installed. This screen contains the DHCP IP address that is assigned to the server.

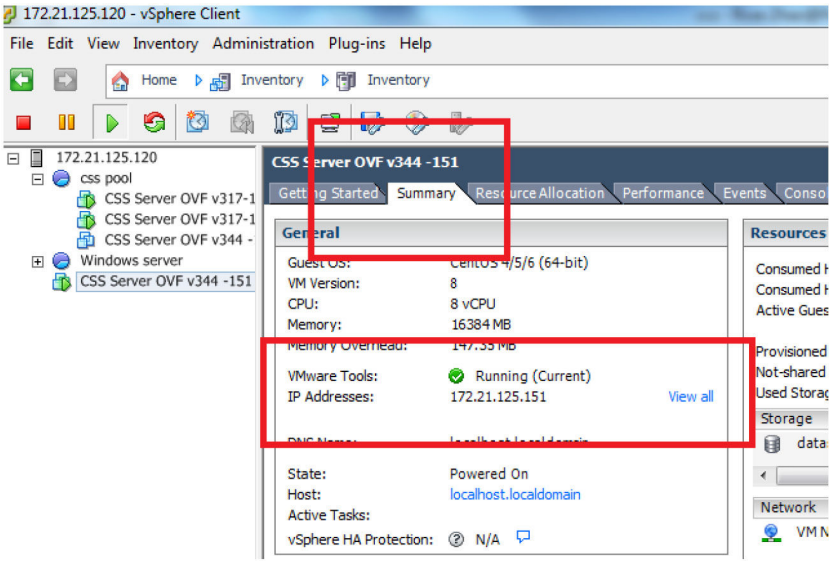


Figure 3: Summary screen showing the ContentConnect Server's IP address

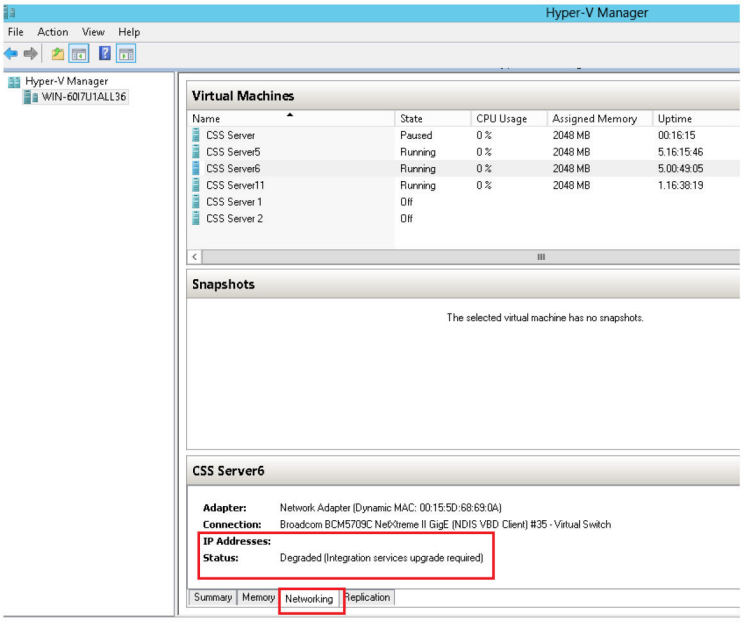
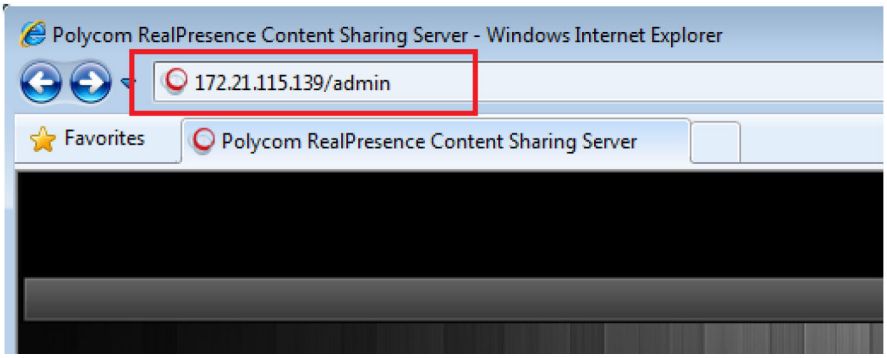


Figure 4: Networking screen showing the ContentConnect Server's IP address

1 Launch a web browser from your PC and enter <IP address of the ContentConnect Server>/admin in the browser's address bar (as shown next).
For example, enter 172.21.115.139/admin, where 172.21.115.139 is the IP address of the ContentConnect Server.



2 Press Enter.
The ContentConnect server Web Configuration Tool Log In screen is displayed.

3 Enter your User ID and Password, and click Log In.
The default login credential for both User ID and Password is admin.

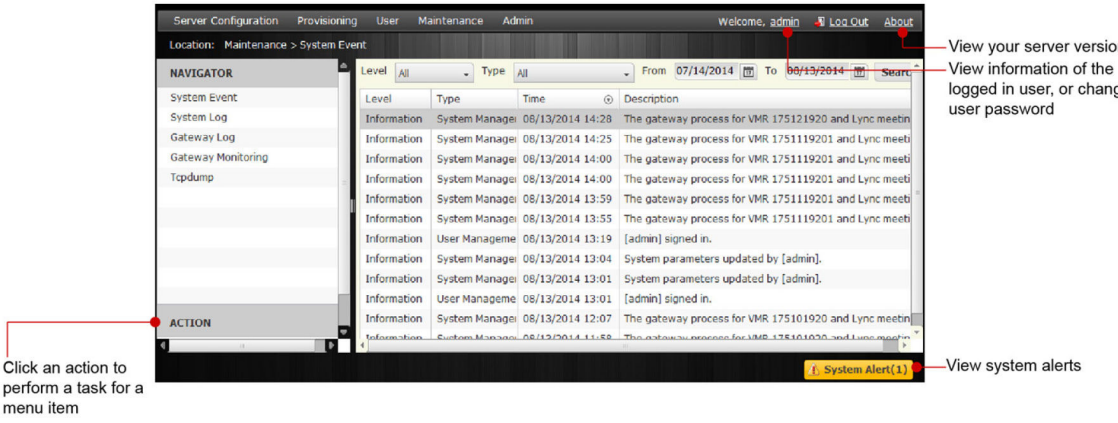
The ContentConnect server Web Configuration Tool screen appears.

Note: If you are accessing the Web Configuration Tool using Google Chrome and are prompted to install Adobe Flash Player constantly, you can go to Settings > Content Settings > Manage exceptions, then add the ContentConnect server IP address to the Allow list.

About the ContentConnect Server Web Configuration Tool

The ContentConnect server Web Configuration Tool has a primary menu bar with five main menus: Server, Provisioning, User, Maintenance, and Admin.

Selecting a menu reveals additional menus that you can click, as shown next. Under the primary menu bar is additional navigation information, to let you know which menu item you're currently configuring.



Each page of the ContentConnect server Web Configuration Tool also displays the following items:

- On the top-right, your user ID, Log Out, and About display. Click them to do the following:
- Click the user's ID to view information about the currently logged-in user (in this case, admin', and to change the user's password.

- Click Log out to log out of the ContentConnect server Web Configuration Tool and return to the Log In screen.
- Click About to display the version of the ContentConnect Server.
- At the bottom-right of the screen is an alert to let you know if there are any important messages you should know about. Click System Alert to view these messages.
- On the far-left of the screen, a list of actions display that enable you to perform specific tasks. For example, depending on the menu item you're configuring, you may be able to create, refresh, edit, export, clear, import, delete, or update items or settings.

Configuring the ContentConnect Server Using the ContentConnect Server Web Configuration Tool

To configure the ContentConnect Server, you need to configure SIP Server, RealPresence Access Director, Active Directory, and provisioning information.

To use the ContentConnect server Web Configuration Tool to perform administrative and maintenance tasks, see Administration and Maintenance Tasks.

Configure ContentConnect Server Running Mode

Polycom ContentConnect server can work in two modes:

- Gateway Mode: Lync clients don't need to install the Polycom ContentConnect Add-on for Microsoft Lync Service for content sharing.

  ContentConnect server works as a RDP-BFCP content gateway, providing full transcoding between RDP and BFCP H264 content streams.
- Add-On Mode: All Lync clients must installing the Polycom ContentConnect Add-on for Microsoft Lync Service for content sharing.

  The Add-on handles content sharing when there is legacy participant with BFCP content supported in the conference.

  In the Add-On Mode, the content media will be only BFCP H264 video stream and go through RealPresence Collaboration Server (RMX) directly from ContentConnect plugin.

1. From the ContentConnect server Web Configuration Tool, select Server Configuration > Running Mode.
2. Select a running mode:
   - Gateway ModeIf you select this option and you have the Polycom ContentConnect Add-on for Microsoft Lync Service installed already, it will be disabled.
   - Add-On ModeIf you select this option and there is a gateway instance running, the gateways will be disabled.
3. Click Save.

Note: In this release, only H.264 content is supported in the Gateway mode. If non-H.264 format content is sent from a Polycom endpoint, the ContentConnect gateway instance cannot transcode it correctly.

Related Concepts

Installing the Polycom ContentConnect Add-on for Microsoft Lync on page 41

You must install RealPresence Content Add-on only if you choose to run your ContentConnect server under Add-On mode.

Configure Server Information

You can configure a SIP server and load balancer server to work with the ContentConnect server.

1. Log in to the ContentConnect server Web Configuration Tool.
2. Select Server Configuration > Server.
3. Enter the following information:
   - SIP Server Address The IP address or host name of Polycom DMA.
   - SIP Server Administrator User The user name of a DMA administrator.
   - SIP Server Administrator Password The password of a DMA administrator.
   - SIP Proxy Port The Polycom DMA port number.
   - SIP Registrar Port The Polycom DMA registrar port.
   - SIP Domain Suffix The domain suffix of the DMA server.
   - SIP Authorization Name, SIP Password SIP authentication credentials created in Polycom DMA (if DMA needs to authenticate ContentConnect Gateway).
   - Call Rate The call rate for the SIP call with Polycom RealPresence Collaboration Server (RMX).
   - SIP Transport Protocol The transport protocol to be used for the SIP call.
   - Media Encryption Whether to enable media encryption. If you select Auto, the SIP server decides whether or not to enable media encryption.
   - Media Transport Port Range The port range allocated for media transmission.
   - Load Balancer Server Address Enter 127.0.0.1 to use the Polycom DMA as your load balancer, or enter an F5 Load Balancer virtual server address.
4. Click Save.

   Note: You must ensure the following before using Polycom DMA as your load balancer:

   - Your RealPresence DMA system is version 9.0.1 or later.
   - Enable the Integrations > Polycom ContentConnect > Load-balance multiple Content Connect systems option in the RealPresence DMA system.
   - Set 127.0.0.1 as the Load Balancer Server Address in the Polycom ContentConnect system.
   - Your ContentConnect must work in the Gateway mode.

   Note: Not all options are available in the Add-On mode.

Configure QoS

You can enable the QoS for Polycom ContentConnect.

The QoS feature allows the Polycom ContentConnect to mark transmitted media traffic with the appropriate QoS value, enhancing the potential of Polycom ContentConnect to improve the user experience.

1. From the ContentConnect server Web Configuration Tool, select Admin > Server Configuration > QoS Status.
2. Check the Enable QoS check box.
3. Select one QoS Type from the drop-down list.
4. Set the QoS Value.

QoS Type	QoS Value
DSCP (DIFFSERV)	The value range from 0-63
IP-PRECEDENCE (TOS)	The value range from 0-7.

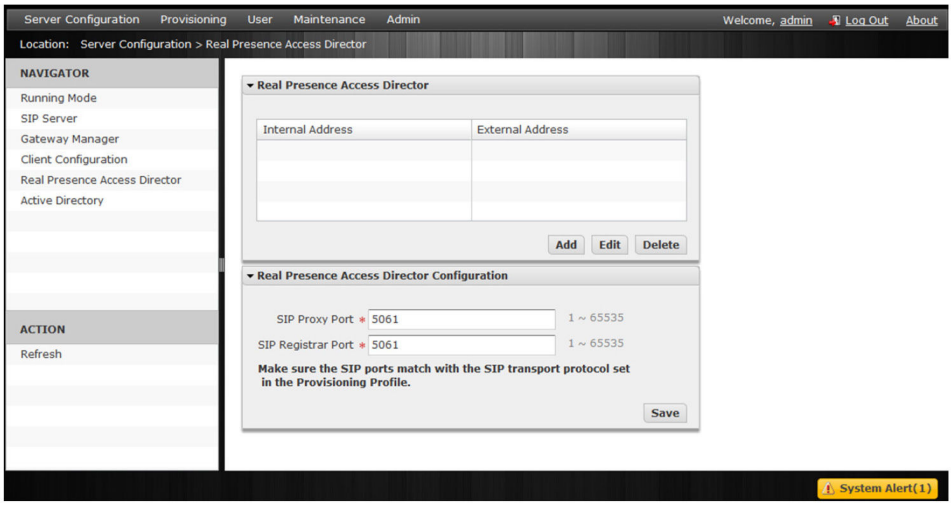
5 Click Save.

Configure RealPresence Access Director Settings

If your deployment uses RealPresence Access Director, configure its settings.

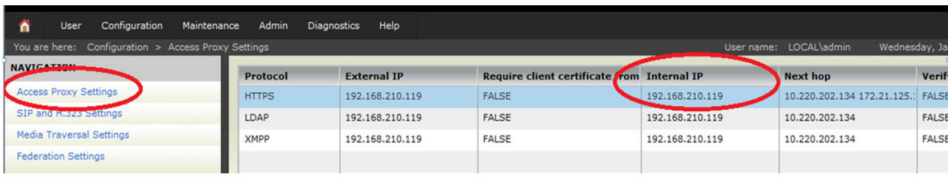
1 Log in to the ContentConnect server Web Configuration Tool.

2 Select ServerConfiguration > RealPresence Access Director.
The RealPresence Access Director and RealPresence Access Director Configuration windows display, as shown next.

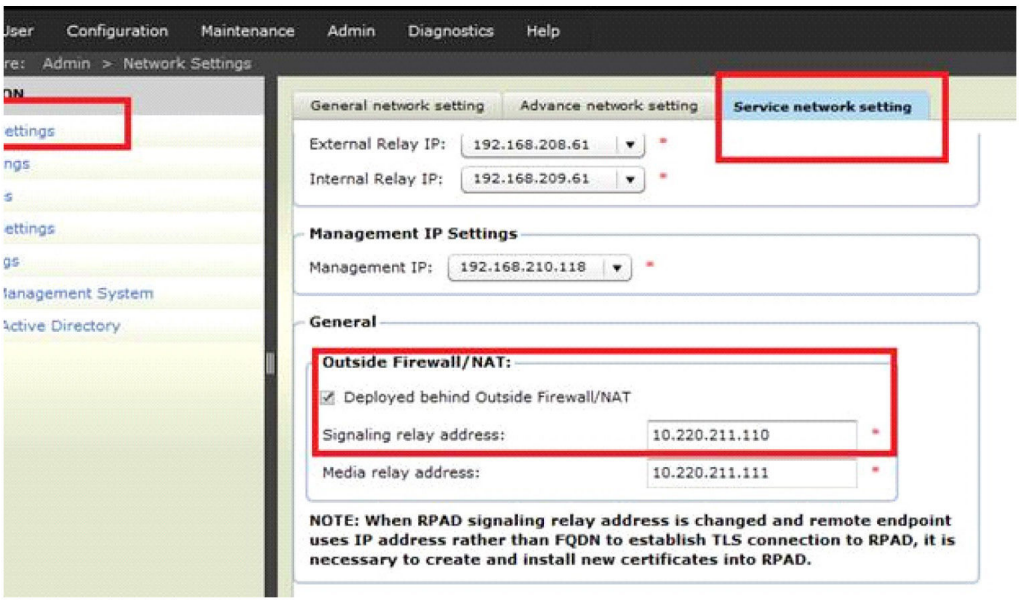


3 In the RealPresence Access Director window, click Add, enter the internal and external IP addresses of RealPresence Access Director, and click Save.

- Internal Address The internal IP address for RealPresence Access Director's Access Proxy Settings. To obtain this address, navigate to Configuration > Access Proxy Settings from RealPresence Access Director (as shown next).

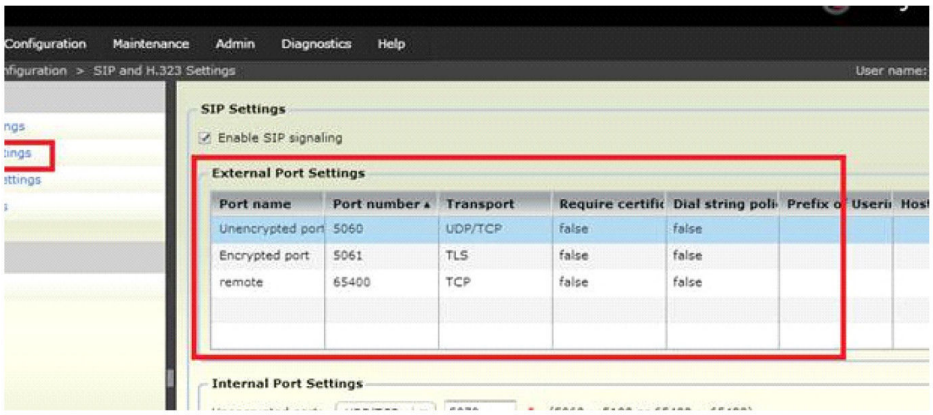


- External Address RealPresence Access Director's Signaling relay address. The ContentConnect server will replace the SIP server address with the external address if a requestor's source address matches the internal address. To obtain RealPresence Access Director's Signaling relay address, navigate to Signaling relay addressSignaling relay address from RealPresence Access Director (as shown next).



4 In the RealPresence Access Director Configuration window, enter the Signaling relay address and SIP Registrar Port, and click Save.
The ports should match RealPresence Access Director. (The ports will be used by the client to communicate with RealPresence Access Director.)

To obtain RealPresence Access Director's SIP proxy and SIP Registrar ports, navigate to Configuration > SIP and H.323 Settings from RealPresence Access Director (as shown next). The following figure displays the listening port of RealPresence Access Director for the client request.



Configuring Active Directory Settings

You need to configure communications with Active Directory server.

Before you do this, set up a machine account in Active Directory, and make sure you add the DNS server record through the ContentConnect server Web Configuration Tool.

Set up a Machine Account in Active Directory

You can set up a machine account in Active Directory.

1. On the Microsoft Active Directory system, open the Active Directory Users and Computers module (Start > Programs > Administrative Tools > Active Directory Users and Computers).
2. Select the node for your domain, right-click the OU folder in which to add the computer account, and select New > Computer.
3. For Computer name, type PolycomCSS or an appropriate name for your environment, and click Next and Finish (or simply click OK depending on your version of Active Directory).
4. Ensure that the Active Directory Users and Computers console will show all available computer options necessary for the remaining steps by enabling View > Advanced Features.
5. Right-click the computer account, select Properties, and open the Security tab.
6. In the Group or user names section of the Security tab, select the SELF object.
7. In the Permissions for SELF section, select Change password, and click OK.
8. Login to the domain controller where the computer account was created and set the password using the following command:

   ```
   net user <
   computername
   >$ <
   password
   >
   ```

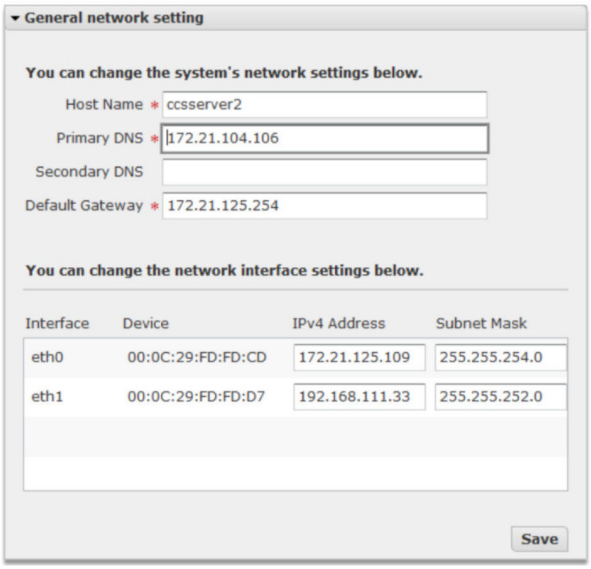
   For example: net user polycomcss$ p@ssw0rd

Add the DNS Server Record

You can add the DNS server record.

1. Log in to the ContentConnect server Web Configuration Tool.
2. Select Admin > Network Configuration.

3 In the General network setting window (shown next), update the DNS settings.

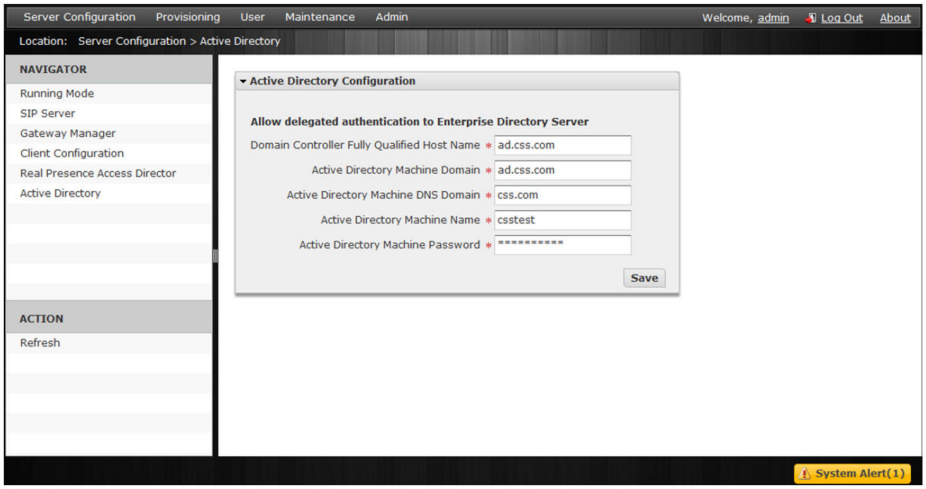


Configure Active Directory Settings

You can configure Active Directory settings.

1 Log in to the ContentConnect server Web Configuration Tool.

2 Select Server Configuration > Active Directory.
The Active Directory Configuration window displays, as shown next.



3 Enter the following information:

- Domain Controller Fully Qualified Host Name The Fully Qualified Domain Name (FQDN) of Active Directory.
- Active Directory Machine Domain The name of the current domain.
- Active Directory Machine DNS Domain The full name of the domain.
- Active Directory Machine Name The machine name, which must match the Machine Name created in Active Directory.
- Active Directory Machine Password The machine password, which is configured in Active Directory.

4 Click Save.

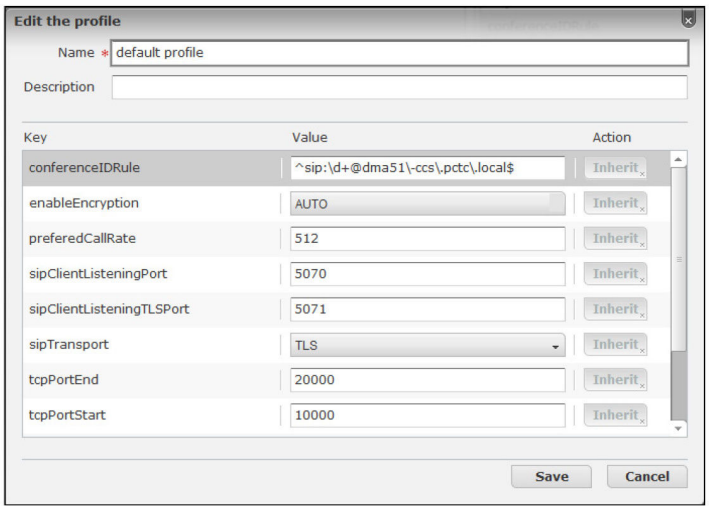
Configure Provisioning Information

If you want to update provisioning information, you can update the settings in the ContentConnect Server's default Provisioning Profile.

The default profile contains 12 settings that you can update. The ContentConnect server can only have one provisioning profile.

The ContentConnect Server's provisioning profile defines a preferred call rate for the SIP call with Polycom RealPresence Collaboration Server (RMX). To share content, the call rate must be equal to or higher than 128K.

1. Log in to the ContentConnect server Web Configuration Tool.
2. Select Provisioning > Provisioning Profile.
3. Under Action, select Edit.
   The Edit the profile window displays, as shown next.



4. From the Edit the profile window, update one or more of the following:

- Name The name of the provisioning profile.
- Description A description of the provisioning profile.
- conferenceIDRule Defines whether a call is a Lync-only call, or a RealPresence Collaboration Server (RMX) bridge call that will use ContentConnect. You need to configure the rule with JS regular expression to match the DMA conference room ID format, which is dialed from the Lync client. (For example, for 123456@dma51-ccs.pctc.local, the route dma51-ccs.pctc.local has been created in Lync.) A valid conference ID must start with ^sip:. For example, to configure a rule that allows any combination of digits as a meeting room ID, create the following rule: ^sip:\d+@dma51\-ccs\.pctc\.local$ (Note: dma51-ccs.pctc.local is the FQDN of DMA.) If the rule is defined, any combination of digits that is used as a meeting ID created in DMA can be used to join a meeting and share content with a Lync client.
- enableEncryption Determines whether encryption should be enabled for the SIP call.
- preferredCallRate The preferred call rate for the client for the SIP call with RealPresence Collaboration Server (RMX). Note that to share content, you need to set a call rate equal to or higher than 128K.
- sipClientListeningPort The client listening port (UDP/TCP).
- sipClientListeningTLSPort The client listening port (TLS).
- sipTransport The SIP transport for the SIP call.
- tcpPortEnd / tcpPortEnd / tcpPortStart / udpPortEnd / udpPortStart If the port configured for sipClientListeningPort is occupied, the new listening port will be chosen during tcp/udpPortStart and tcp/udpPortStop.
- verifyCert Determines if the client will verify the server's CA.

5 Click Save.

Configuring an Optional Load Balancer

You can deploy a load balancer with your ContentConnect solution.

You can use Polycom DMA as your load balancer, or an F5 BIG-IP LTM Load Balancer.

Note: To ensure successful load balancing, it's recommended to include only ContentConnect VMs with the same configurations in a load balancing pool.

Using Polycom® RealPresence® DMA as a Load Balancer

If you are using multiple ContentConnect servers, you can configure the RealPresence DMA to load balance them.

Only RealPresence DMA system 9.0.1 or higher supports this feature.

Note: Don't modify the ContentConnect networking settings from the Web Configuration Tool. Otherwise, the DMA load balancing feature will not work.

Ensure That the ContentConnect and RealPresence DMA Are Accessible via DNS

You need to ensure that both systems are accessible via DNS.

1 In the Reverse Lookup Zones, create one FQDN entry for your ContentConnect server in your DNS server, with the option Create Associated Pointer (PTR) Record enabled.

2 Ensure one FQDN entry exists for your RealPresence DMA server in the DNS server, with the option Create Associated Pointer (PTR) Record enabled.

Enable ContentConnect Load-Balancing within the RealPresence DMA

From the RealPresence DMA system user interface, you enable the load balancer for multiple Polycom ContentConnect systems.

You can also disable load balancing when necessary.

Note: When you enable the RealPresence DMA system as a load balancer, the system creates a user named contentbalanceuser in the user interface. While the system is enabled as a load balancer, do not delete this user.

1. In the RealPresence DMA system, go to Integrations > Polycom ContentConnect.
2. Select the Load-balance multiple ContentConnect systems check box.
   The Available ContentConnect systems table includes the following information about each ContentConnect system connected to the RealPresence DMA system load balancer:
   - IP address
   - Current usage
   - Maximum capacity
   - Last heartbeat received
3. Select Update.

Configure Each ContentConnect Server for Load Balancing

You need to re-deplpoy and configure each ContentConnect server to use the RealPresence DMA for load balancing.

You do this in the VMware or HyperV console of the respective ContentConnect server.

1. Deploy the ContentConnect using the OVA(VMWare) or VHD(Hyper-V) files.
2. Power on the ContentConnect and log in from the VMware or HyperV console.
   The default user name and password is polycom/polycom.
3. Configure the ContentConnect from the console:
   - Change Host Name: Enter the ContentConnect FQDN.
   - Configure Network: Enter network information for your ContentConnect FQDN in eth0 > Static address setup.
   - Configure DNS: Enter your DNS server information.
4. Select Reboot Server.
   After the ContentConnect powers up, log in to the ContentConnect Web Configuration Tool.
5. Select Server Configuration > Server and configure the following:
   - SIP Server Address: Enter the FQDN of your RealPresence DMA system.

     Note: If you have a Supercluster with a primary and backup DMA configured in your territory, you can specify the Embedded DNS FQDN of the DMA in the SIP Server Address field under Server Configuration > Server. If the primary DMA experiences a failover, the backup will continue to use the same pool of ContentConnect devices for future conferences until the primary DMA is back online. For more information on the Embedded DNS, refer to the Polycom® RealPresence® Distributed Media Application™ (DMA®) System Operations Guide available on BARhttps://support.polycom.com.
   - Load Balancing Virtual Server: 127.0.0.1
6. Reboot the ContentConnect server.
7. Repeat these steps for each ContentConnect server.

8 Verify that the RealPresence DMA is now load balancing the servers.
9 Within the RealPresence DMA system, go to Integrations > Polycom ContentConnect.
10 Verify that your ContentConnect instances display in the
11 Available ContentConnect systems table.

Note: To use a RealPresence DMA as a load balancer, ensure all ContentConnect servers in your network set the Load Balancing Virtual Server as 127.0.0.1.

Note: Don't modify ContentConnect networking settings from the Web Configuration Tool. Otherwise, the DMA load balancing feature will not work.

Deploying ContentConnect with an F5 BIG-IP LTM Load Balancer

To deploy ContentConnect with an F5 BIG-IP LTM load balancer, complete the following steps:

1 Create Nodes to Identify Resources
2 Create a Load Balancing Pool
3 Add Members to the Load Balancing Pool
4 Add a New OneConnect Profile
5 Add a New HTTP Profile
6 Adding a New XML Profile, iRule, and Persistence Profile
7 Create and Configure a Virtual Server to Use the Configured Pool and HTTP Profile

Note: After you successfully configured a Load Balance, ContentConnect sessions are routed to different ContentConnect Servers in the resource pool per your specified load balancing method. You can log in to a ContentConnect Servers from its Web Configuration Tool and select Maintenance > Gateway Monitoring to check the gateway instance status.

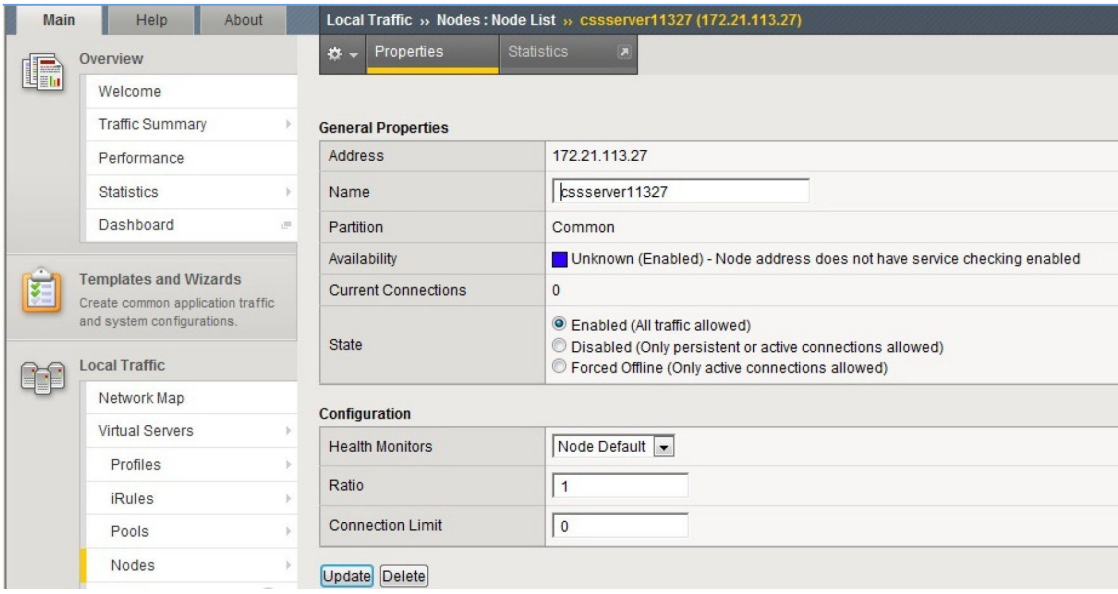
Note: For specific information and instructions on how to configure an F5 BIG-IP LTM, see the F5 Knowledge Base.

Create Nodes to Identify Resources

Before you can create a ContentConnect server resource pool, you need to identify available ContentConnect server s as nodes.

1 Log in to the BIG-IP Configuration Utility.
2 From the Main tab of the navigation pane, expand Local Traffic and click Nodes.
3 From the top-right of the screen, click Create.
The New Node screen displays.
4 For the Address setting, type the IP address of the ContentConnect server.
5 Click Finished.

The following figure shows a sample node configuration page.

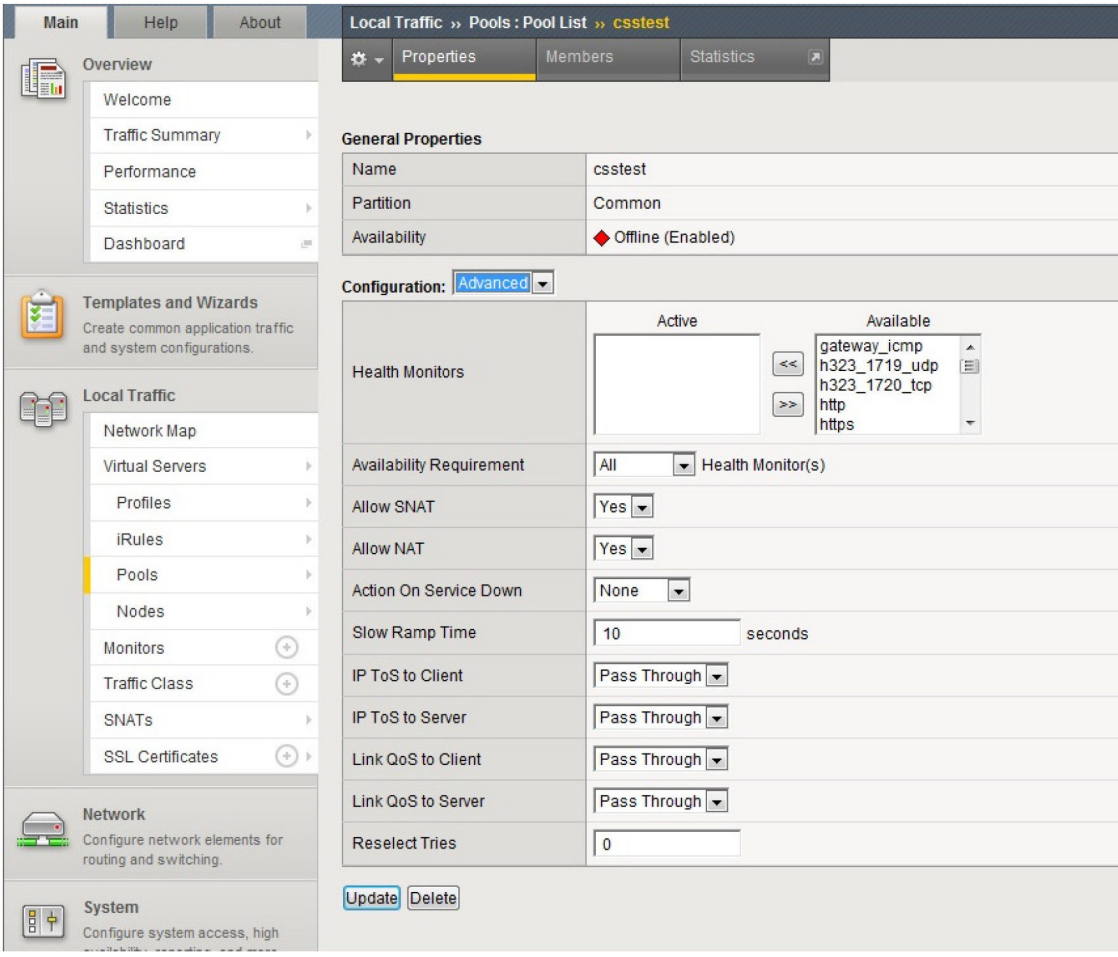


Create a Load Balancing Pool

You must create a ContentConnect server resource pool for load balancing.

1. Log in to the BIG-IP Configuration Utility.
2. From the Main tab of the navigation pane, expand Local Traffic and click Pools.
   The Pools screen displays.
3. From the top-right of the screen, click Create.
   The New Pool screen displays.
4. From the Configuration list, select Advanced.
5. For the Name setting, type a name for the pool.
6. Click Finished.

The following figure shows a sample pool configuration page.

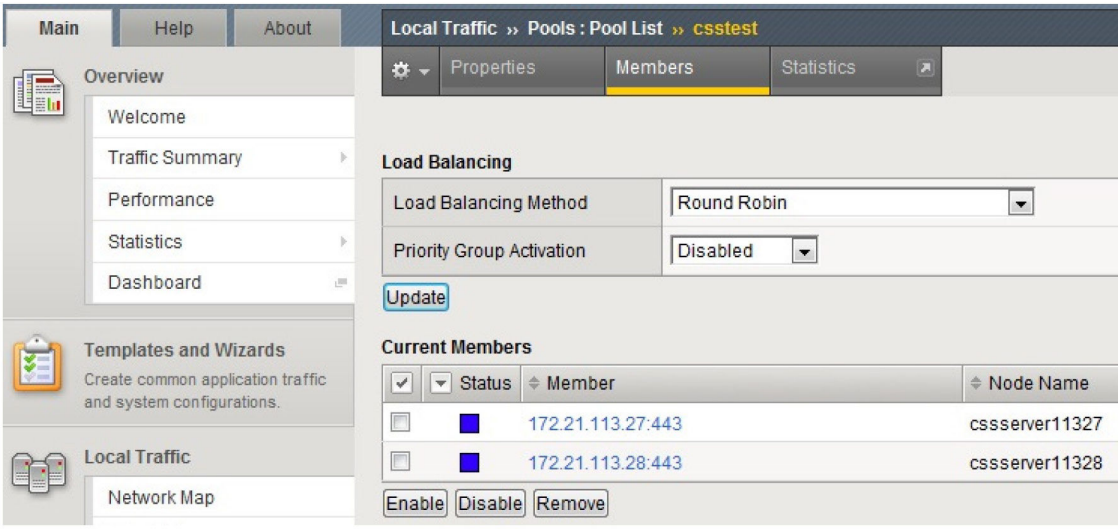


Add Members to the Load Balancing Pool

You need to add at least two ContentConnect server s to your load balancing pool.

1. Log in to the BIG-IP Configuration Utility.
2. From the Main tab of the navigation pane, expand Local Traffic and click Pools.
   The Pools screen displays.
3. From the pool list, select your pool.
4. From the Members tab, click the number shown to list the existing pool members.
5. From the far-right of the screen, click Add.
   The New Pool Member screen displays.
6. In the Address box, select Node List and select an IP address.
7. In the Service Port box, type the port number on which the corresponding proxy server is listening.
8. Click Finished.

The following figure shows an example of pool members.

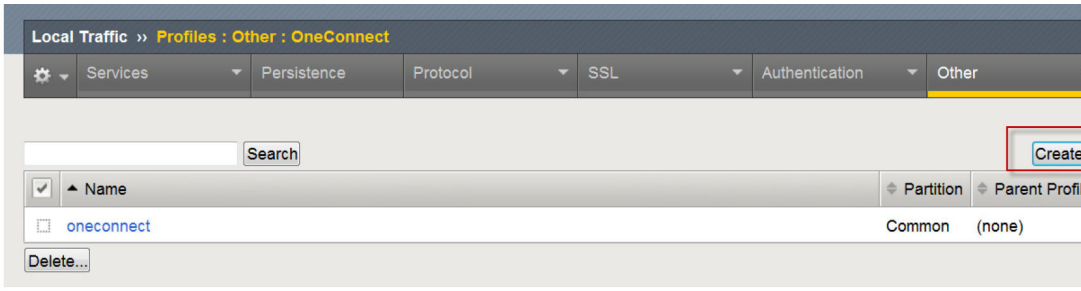


Add a New OneConnect Profile

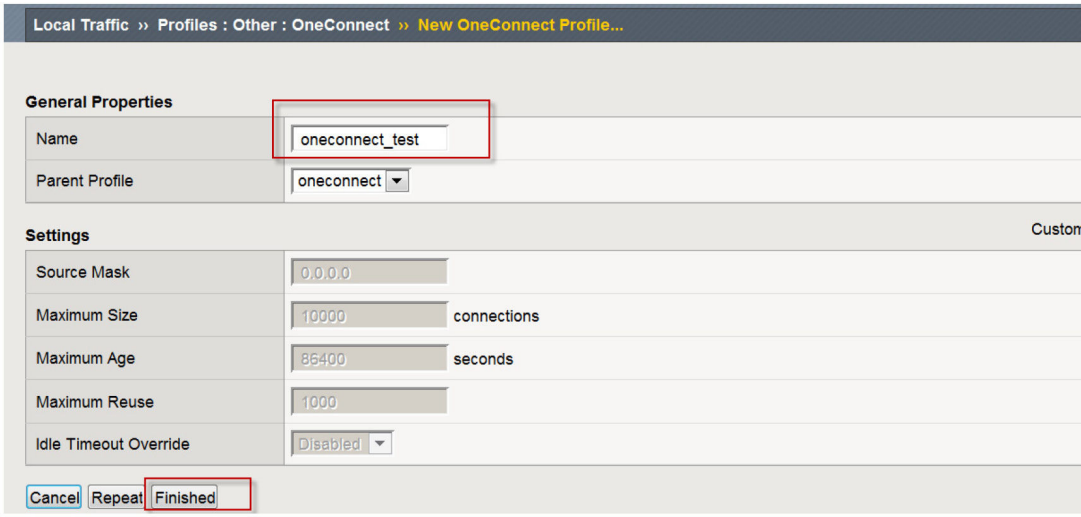
To balance the ContentConnect server workload, you must configure a OneConnect profile to let the DMA system forward different VMR cascading messages to different ContentConnect server s.

Note: OneConnect profile is needed only in the Gateway Mode

1. Log in to the BIG-IP Configuration Utility.
2. From the Main tab of the navigation screen, expand Local Traffic and click Profiles > Other > OneConnect.
3. Click Create.



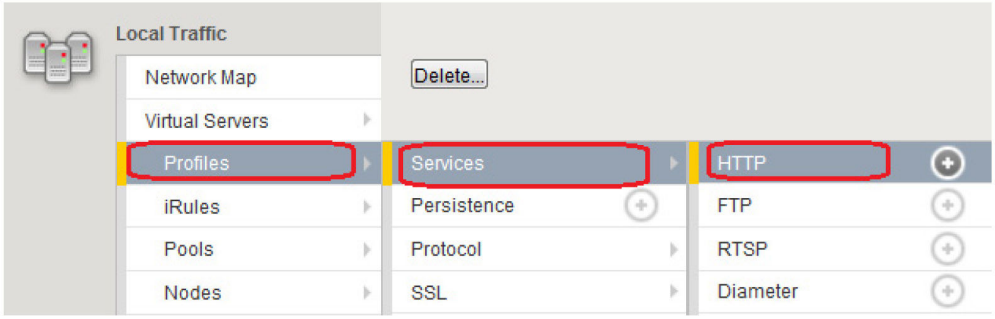
4. Enter a name for the new profile and click Finished.



Add a New HTTP Profile

You need to enable the X-Forwarded-For header in HTTP profiles so the virtual server can forward ContentConnect client requests to your ContentConnect server resource pool.

1. Log in to the BIG-IP Configuration Utility.
2. From the Main tab of the navigation screen, expand Local Traffic and click Profiles > Services > HTTP.



3. From the top-right of the screen, click Create.
   The New HTTP Profile screen displays
4. Enter a name for your profile.
5. Select http as Parent Profile.
6. Select the option Insert-X-Forward-For, and then select Enabled.

7. Click Finished.

Adding a New XML Profile, iRule, and Persistence Profile

To work with the Gateway mode, you must also configure an XML profile, an iRule, and a persistence profile to let the F5 Load Balancer route cascade messages of the same VMR to the same ContentConnect server.

Create a New XML Profile for Working with the Gateway Mode

You can create a new XML profile for working with the gateway mode.

1. Log in to the BIG-IP Configuration Utility.
2. From the Main tab of the navigation screen, expand Local Traffic and click Profiles > Services > XML.
3. From the top-right of the screen, click Create.
   The New XML Profile screen displays.
4. Enter a name for your profile.
5. Select xml as Parent Profile.
6. For Namespace Mappings, select Specify.
   Enter the following settings and then click Add.

   ```
   Prefix: ns5
   Namespace: urn:com:polycom:api:rest:plcm-conference-v3
   ```

7. In XPath Queries, select Specify.
   Enter the following settings and then click Add:

   ```
   XPath: //ns5:dial-in-number
   ```

8. Click Finish.

Create an iRule for Use with the Gateway Mode

You can create an iRule for use with the Gateway Mode.

1. Log in to the BIG-IP Configuration Utility.
2. From the Main tab of the navigation screen, expand Local Traffic and click iRules.
   The iRule List screen displays.
3. From the top-right of the screen, click Create.
   The New iRule screen displays.
4. In the Name box, type a name for the iRule.
5. In the Definition box, enter the following rules and click Update.

- For F5 Load Balancer versions earlier than 11.2, use the following rules:

```
when HTTP_REQUEST
{
if { !( [HTTP::uri] contains "api/rest" )} {
persist source_addr 255.255.255.255 7200
}
}
when XML_CONTENT_BASED_ROUTING
{
log local0. "XML Detected"
for {set i 0} { $i < $XML::count } {incr i} {
log local0. $XML::queries($i)
log local0. $XML::values($i)
if {($XML::queries($i) contains "dial-in-number")} {
persist uni $XML::values($i)
}
}
}
```

- For F5 Load Balancer versions later than 11.2, use the following rules:

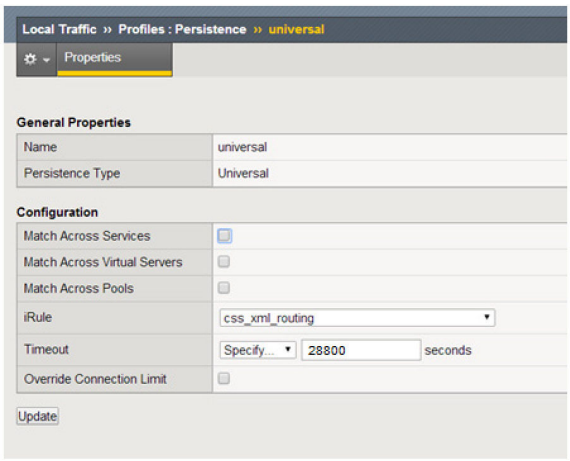
```
when HTTP_REQUEST
{
if { !( [HTTP::uri] contains "api/rest" )} {
persist source_addr 255.255.255.255 3600
}
}
when XML_CONTENT_BASED_ROUTING
{
log local0. "XML Detected"
for {set i 0} { $i < $XML_count } {incr i} {
log local0. $XML_queries($i)
log local0. $XML_values($i)
if {($XML_queries($i) contains "dial-in-number")} {
persist uni $XML_values($i)
}
}
}
```

6 Click Finish.

Create a Persistence Profile for Use with the iRule

You can create a persistence profile for use with the iRule.

1 Log in to the BIG-IP Configuration Utility.
2 From the Main tab of the navigation screen, expand Local Traffic and click Profiles > Persistence.
3 From the top-right of the screen, click Create.
The New Persistence Profile screen displays.
4 In the Name box, type a name for the persistence profile.
5 For Persistence Type, select Universal.
6 For iRule, select the iRule you have created for working with the Gateway Mode.
7 For Timeout, specify a time length that is longer than your conference duration. Setting a time much longer than your actual meeting duration may cause the load balancing to fail. Within the time out duration, calls to the same VMR are always routed to the same ContentConnect server.
8 The following is an example configuration of the persistence profile.



9 Click Finish.

Create and Configure a Virtual Server to Use the Configured Pool and HTTP Profile

You need to create a virtual server and configure it to use your load balancing pool.

1 Log in to the BIG-IP Configuration Utility.

2 From the Main tab of the navigation screen, expand Local Traffic and click Virtual Servers.
The Virtual Servers screen displays.

3 From the top-right of the screen, click Create.
The New Virtual Server screen displays.

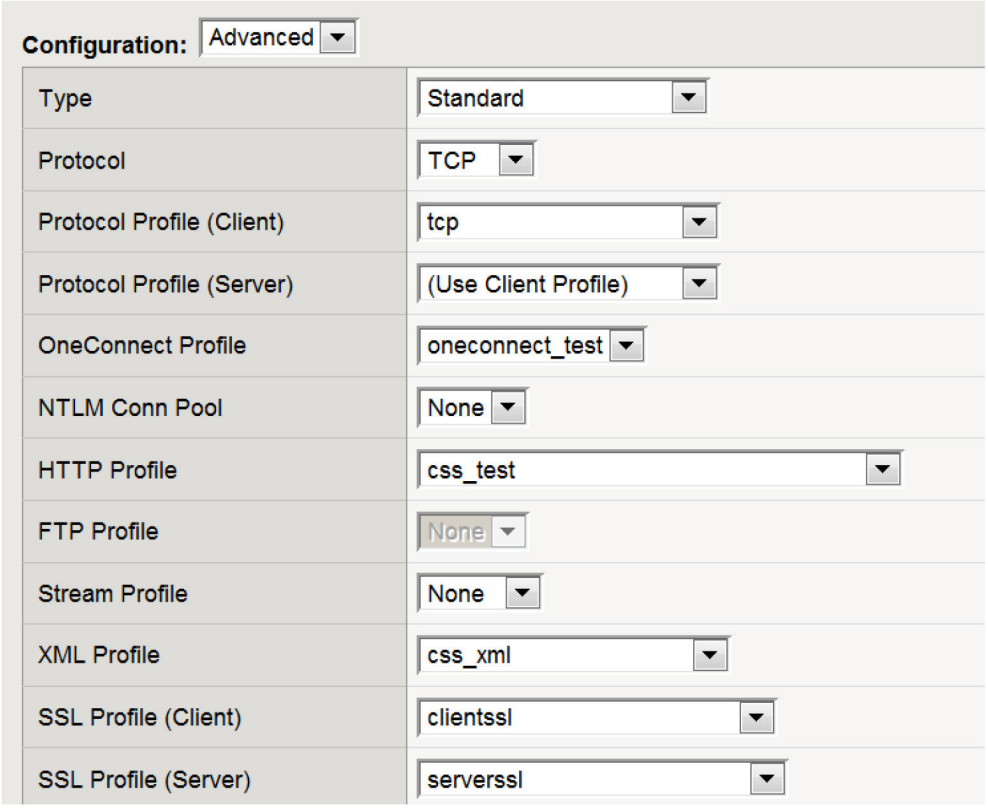
4 In the Name box, type a name for the virtual server.

5 In the Destination box, enter the IP address you will use as the virtual IP for the ContentConnect Virtual Server in the Address field.

6 In the Service Port box, specify a listen port.
This is the IP address and port to which ContentConnect clients connect.

7 For Configuration, select Advanced.
Then configure the following:

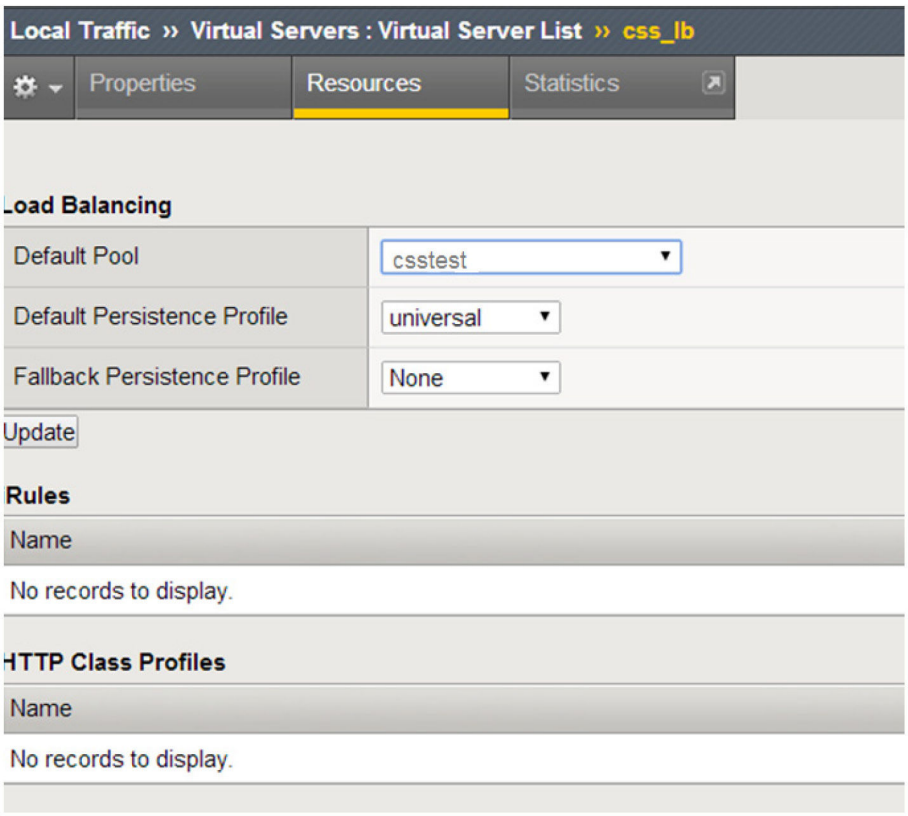
- OneConnect Profile: Select the OneConnect profile you created.
- HTTP Profile: Select the HTTP profile you created.
- SSL Profile (client): Select clientssl.
- SSL Profile (server): Select serverssl.
- XML Profile: Select the XML profile you created for working with the Gateway Mode.
- SSL Profile (client): Select clientssl.
- SSL Profile (server): Select serverssl.
- SNAT Pool: Select Auto Map.The following figure shows a sample advanced configuration for a virtual server.



8 Click Apply to save your settings.

9 Click the Resource tab and select the pool you created under Load Balancing section.

10 For Default Persistence Profile, select the persistence profile you have created for use with the Gateway Mode.



11 Click Update.

Administration and Maintenance Tasks

Administration and maintenance tasks for the ContentConnect server include managing users and administrators, upgrading, restarting, and shutting down the system, enabling Hot Standby, and activating the ContentConnect server license.

For the ContentConnect Client, you can access a tool that collects and packages log files so you can diagnose ContentConnect Client issues.

ContentConnect Server Tasks

You can perform several ContentConnect server maintenance and administrative tasks from the ContentConnect server Web Configuration Tool.

Activating the ContentConnect Server Licenses

From version 1.3 and onwards, ContentConnect adopts Flexera licensing technology to provide subscription-based license management.

You can now purchase licenses for individual features; activate, or deactivate your licenses anytime you want.

Activation Modes

You can activate your licenses in two ways:

- Standalone mode: Activate your licenses from Polycom Licensing Center online or offline with your activation keys.

  We recommend you choose standalone online activation.
- Solution mode: Connect to the Polycom RealPresence Platform Director or Polycom RealPresence Resource Manager to get your licensing information. RealPresence Platform Director or Polycom RealPresence Resource Manager controls and provides ContentConnect licensing information.

  If you have a Polycom RealPresence Resource Manager system version 10.0 or later, you must use the RealPresence Resource Manager system to license your ContentConnect system. If you have not deployed a RealPresence Resource Manager system or if you have not upgraded your RealPresence Resource Manager system to version 10.0 or later, you must license your product using the RealPresence Platform Director system.

  In this release, ContentConnect cannot be deployed nor configured by the RealPresence Platform Director.

  Note: Both VMware and Hyper-V are supported in standalone mode. However, only VMware is supported in solution mode. For solution mode, you must deploy the Polycom RealPresence Director on a VMware server.

  Note: ContentConnect versions earlier than 1.3 use another licensing mechanism. Please request your Polycom Support team to upgrade it to the new licensing mechanism.

Activating Licenses in Standalone Mode

You can activation your licenses from Polycom Licensing Center in two ways:

- Online mode ContentConnect server sends your activation keys to Polycom Licensing Center for activation or deactivation.

  You must have Internet access for this operation.

- Offline mode Log in to the Polycom Licensing Center yourself and activate licenses with activation request and response files. You need the following steps to activate a license offline:

  1 Generate an activation request with your activation key.
  2 Upload the activation request to Polycom Licensing Center.
  3 Obtain an activation response from Polycom Licensing Center.
  4 Upload the activation response to the ContentConnect Web Configuration Tool to activate or deactivate the ContentConnect product or feature.

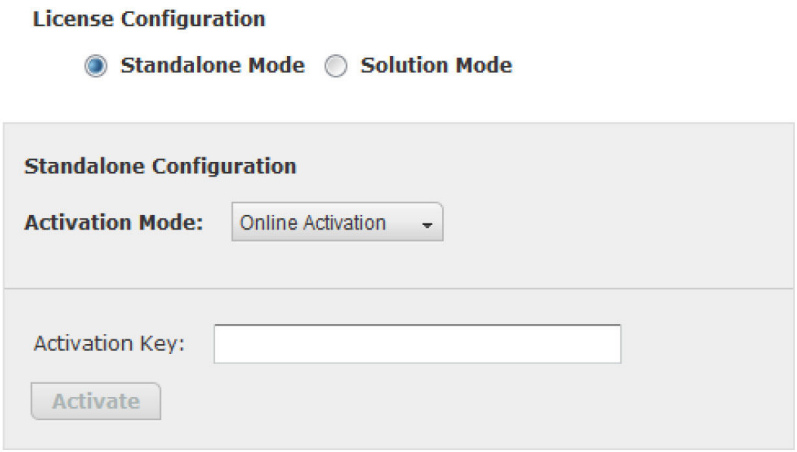
Note: ContentConnect licenses come into two types: product license (primary license) and feature licenses. The product license activates the ContentConnect application itself while feature licenses activate features such as call encryptions and HA. You must activate the product license before you can activate and use other features.

Activate the ContentConnect Server Product License Online in Standalone Mode

You can activate the ContentConnect server product license online in standalone mode.

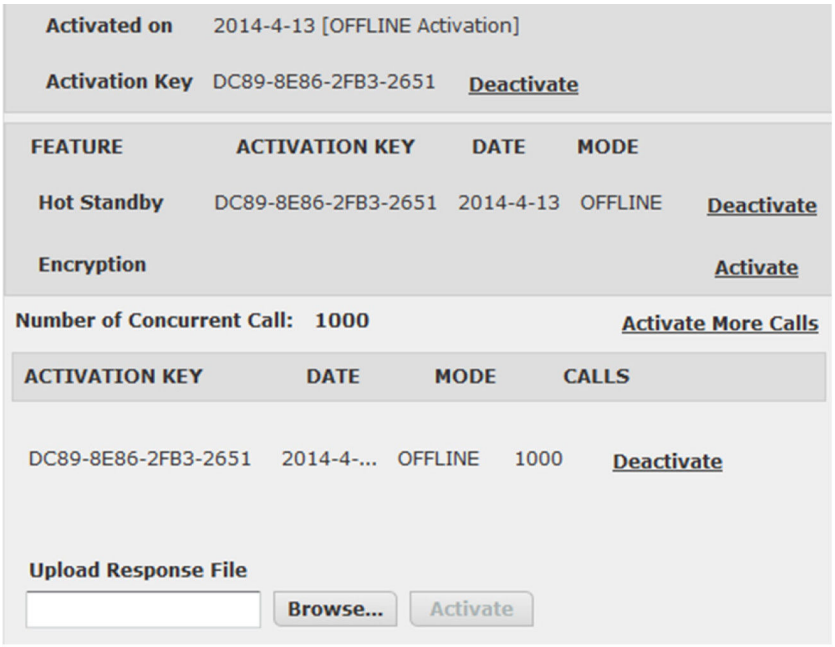
1 From the ContentConnect server Web Configuration Tool, select Admin > Licenses to view the license configuration options.

2 Click Standalone Mode to view the standalone configuration options.



3 For Activation Mode, select Online Activation.
This is the default option.

4 Enter your ContentConnect product activation key, and then click Activate.
The screen refreshes. A message indicates the license activation is successful, and a list of activated licenses displays. The entitled features vary with your license.



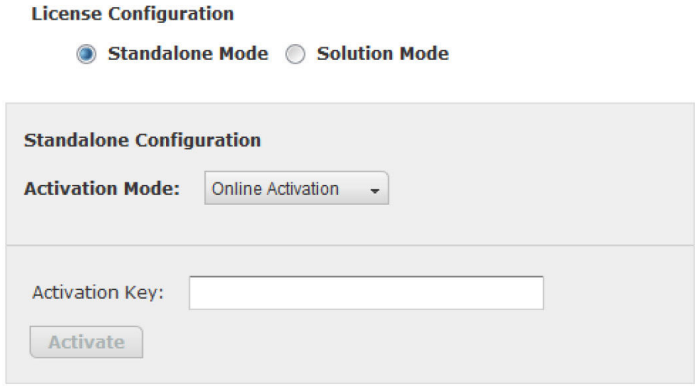
You can click the Activate options next to a feature to active it online using its activation key (if available).

Activate the ContentConnect Server Product License Offline in Standalone Mode

You can activate the ContentConnect server product license offline in standalone mode.

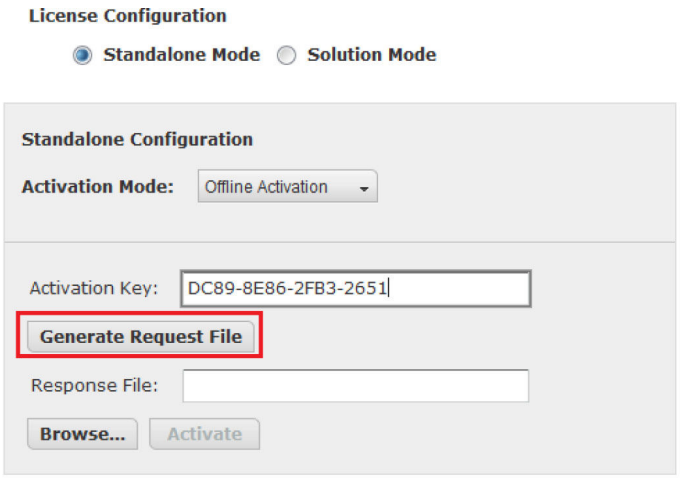
1 From the ContentConnect server Web Configuration Tool, select Admin > Licenses.
The License Configuration options appear.

2 Click Standalone Mode.
The Standalone Configuration options appear.



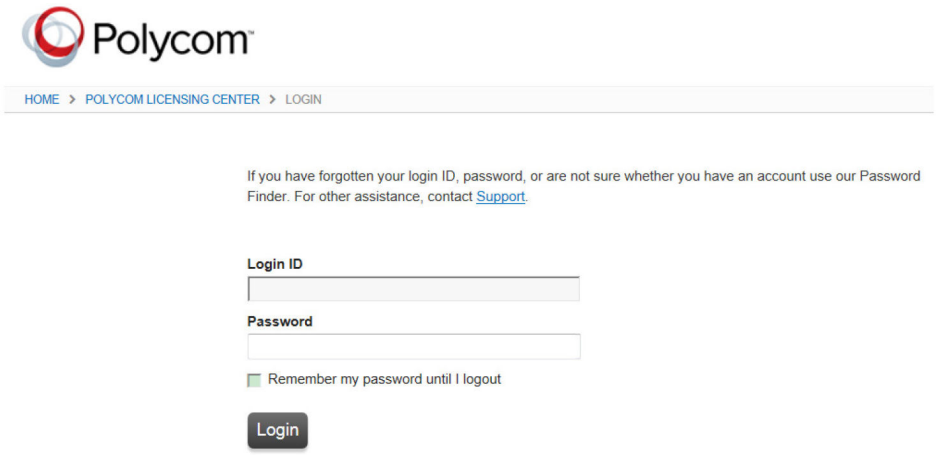
3 For Activation Mode, select Offline Activation.
Enter your Activation Key, and then click Generate Request File.

You can find the activation key in the Welcome email you received from Polycom Customer Support after purchasing the ContentConnect product.



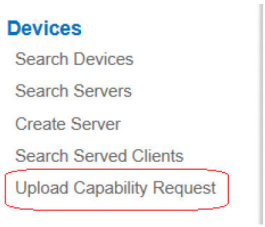
4 A dialog appears prompting that a request.bin file is generated.
Save the generated file to your computer. You can change the file name (but not its extension).

5 Log in to Polycom Licensing Center with your credentials.

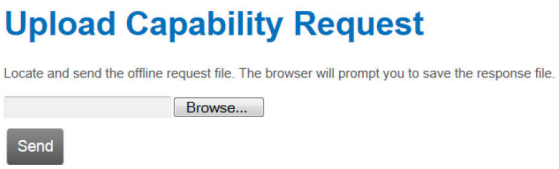


You can find the log in credentials in the Welcome email you received from Polycom Customer Support after purchasing the ContentConnect product.

6 On the left of your screen, select Upload Capability Request.



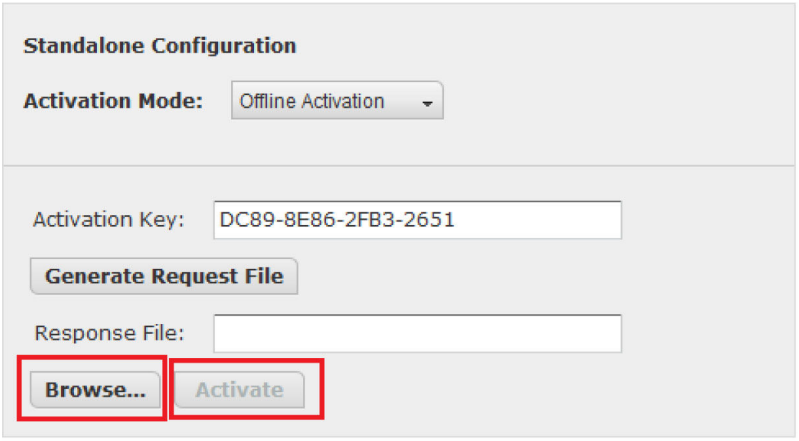
7 Click Browse to upload the request.bin file you get in step 4, and click Upload Capability Request.



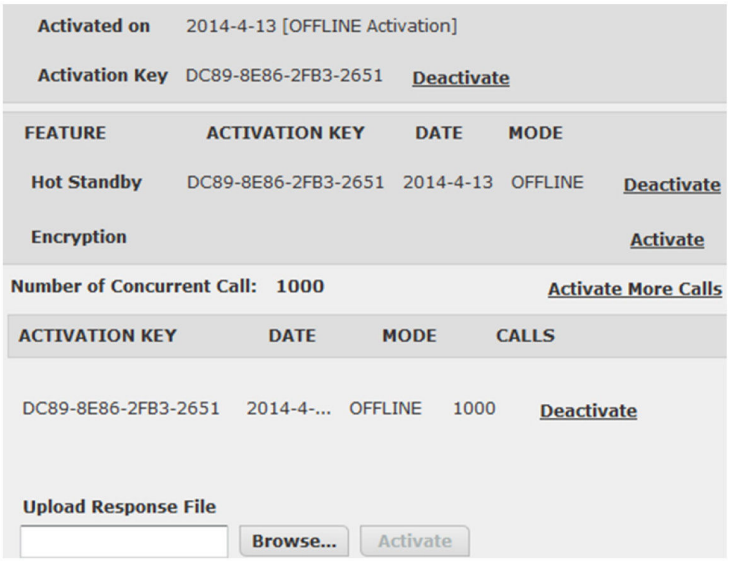
8 A dialog prompting that a response.bin file is generated.

Save the file to your computer. You can change the file name (but not its extension).

9 From ContentConnect Web Configuration Tool, from Admin > Licenses, click Browse to upload the response.bin file you get from step 10, and click Activate.



The Web Configuration Tool web page refreshes. You can see the activation time, activation code, and activated features (if entitled in this license).



On the right of the window, License Detail pane refreshes.

Note: Follow the steps 3-12 to activate features offline in standalone mode, such as call encryption, or adding more concurrent calls.

Related Concepts

Viewing License Details on page 94

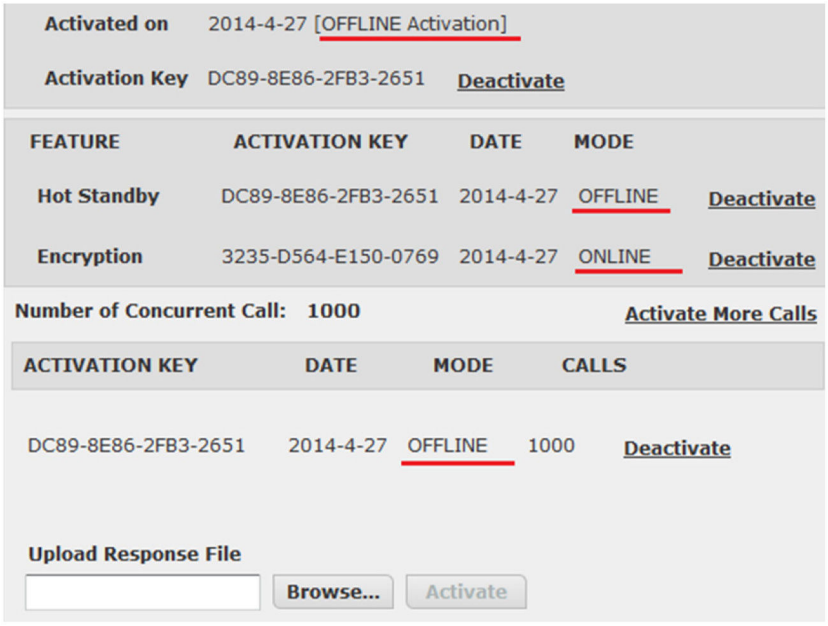
You can find your license details in the License Detail window.

Deactivating ContentConnect Product or Features in Standalone Mode

If you re-install your ContentConnect system, or if you want to use a license on another instance of ContentConnect system, you need to deactivate your ContentConnect product or feature licenses first.

You can do the deactivation online or offline.

If a license is activated online, the default deactivation method is also online. The same goes to offline activation and deactivation. You can find the activation mode in the Admin > Licenses web page.



Note: It is recommended that you deactivate ContentConnect features first. If you deactivate features, you can still use the ContentConnect product. However, If you deactivate the ContentConnect product first, the application and all features become unavailable.

Deactivate the ContentConnect Product or Services Online in Standalone Mode

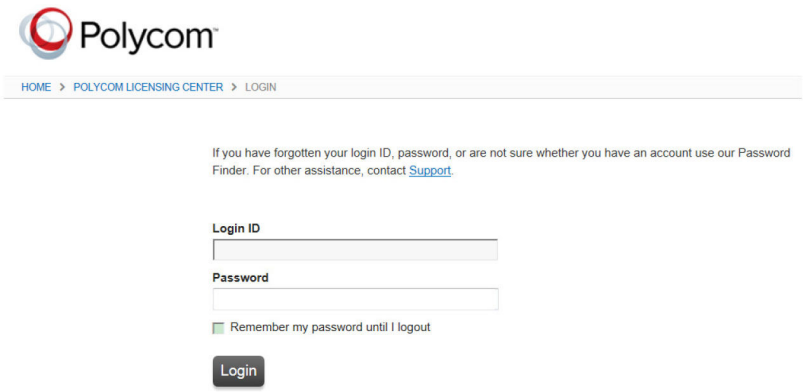
You can deactivate the ContentConnect product or services online in standalone mode.

1. From the ContentConnect server Web Configuration Tool, select Admin > Licenses.
2. Click the Deactivate next to the desired item.

Deactivate the ContentConnect Product or Service License Offline in Standalone Mode

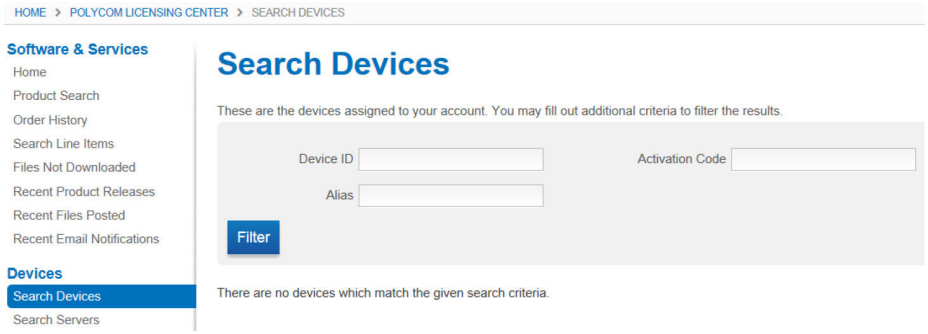
You can deactivate the ContentConnect product or service license offline in standalone mode.

1. Log in to Polycom Licensing Center with your credentials.
   You can also access the Polycom Licensing Center from Polycom support web site, LICENSING AND PRODUCT REGISTRATION > Activation/upgrade > RealPresence ContentConnect.



You can find the log in credentials in the Welcome email you received from Polycom Customer Support after purchasing the ContentConnect product.

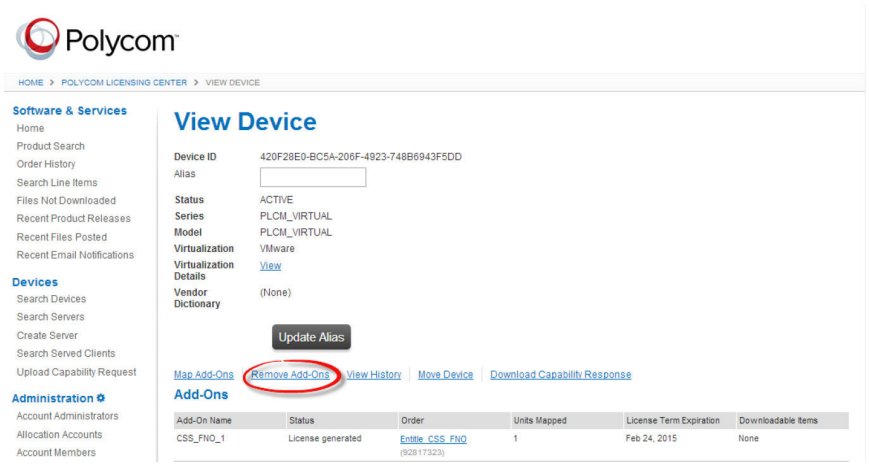
2 On the left of your window, under Devices, select Search Devices.



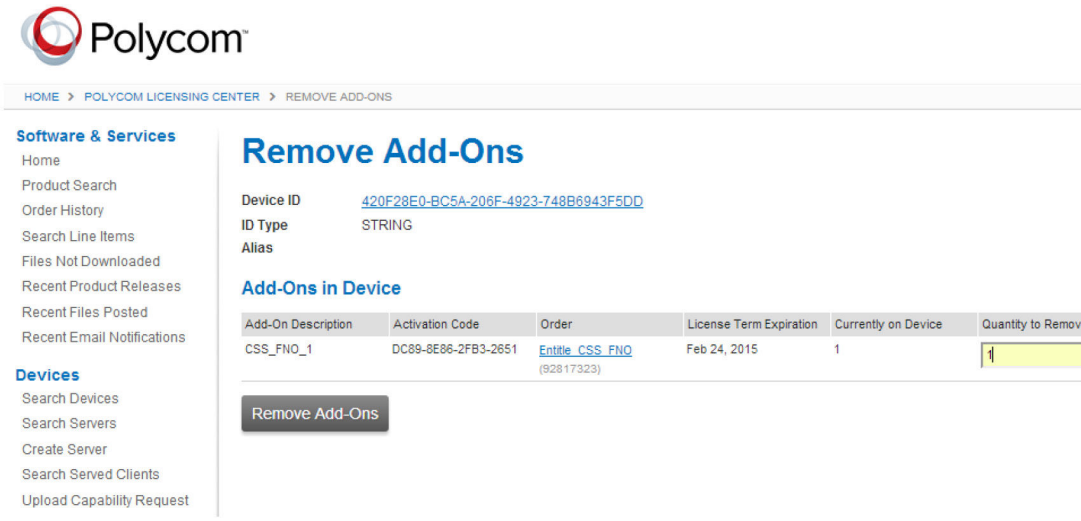
3 Type your ContentConnect product Host ID for Device ID, and click Filter.
You can use wildcard * in the Device ID search.

The Device ID is available either from the Welcome email you received, or from Admin > Licenses of your ContentConnect Web Configuration Tool, in License Details window.

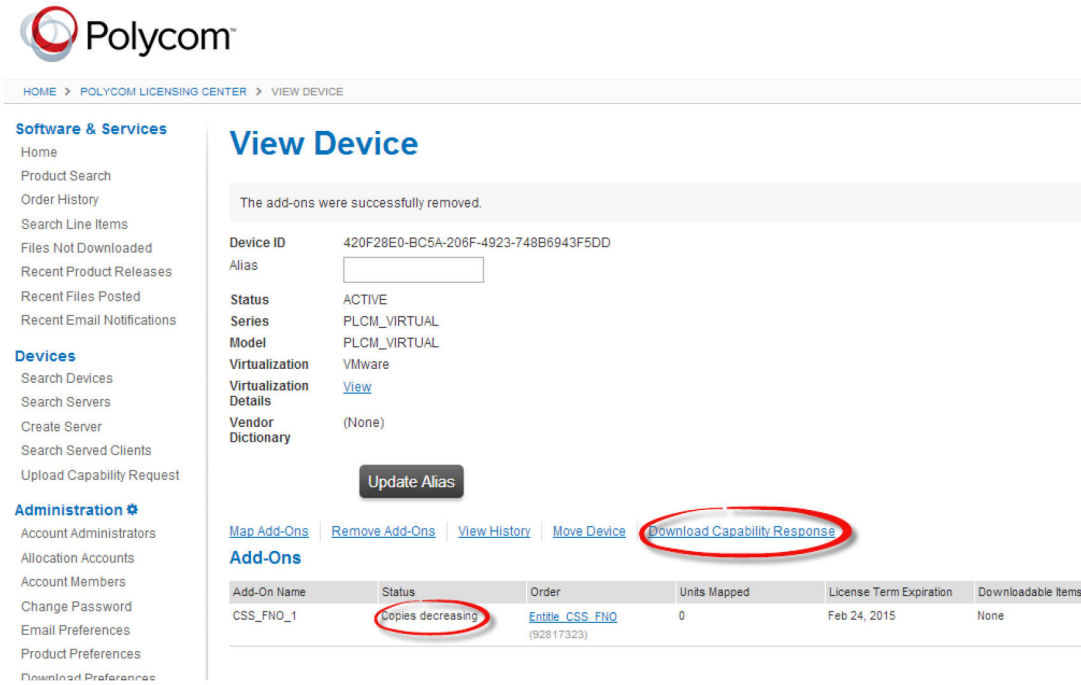
4 Click the Device ID in the result list to view device details.
In the View Device window, click Remove Add-Ons.



5 Enter the quantity of the license you want to delete and click Remove Add-Ons.
For example, to remove one copy of the license, type 1.



6 The screen refreshes to reflect the changes.
Click Download Capability Response.

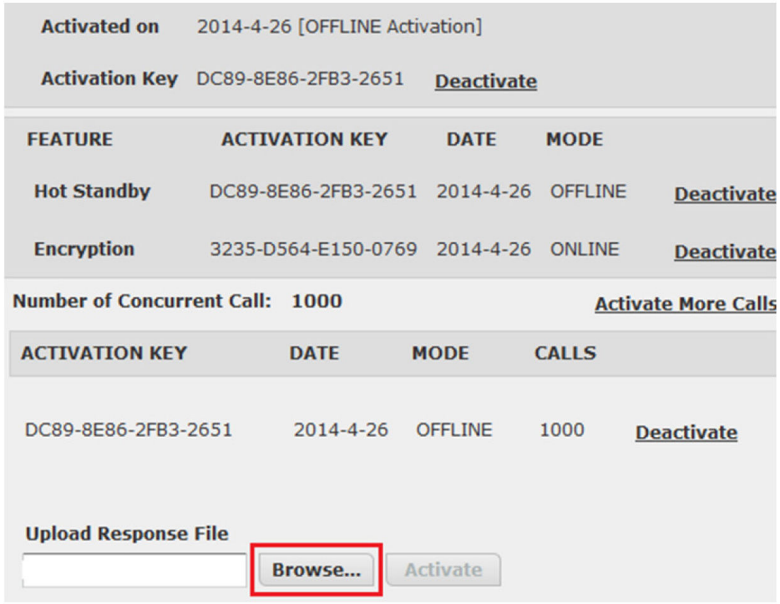


7 A dialog appears prompting you that a file response.bin is generated.
Save the file to your computer. You can change the file name (but not its extension).

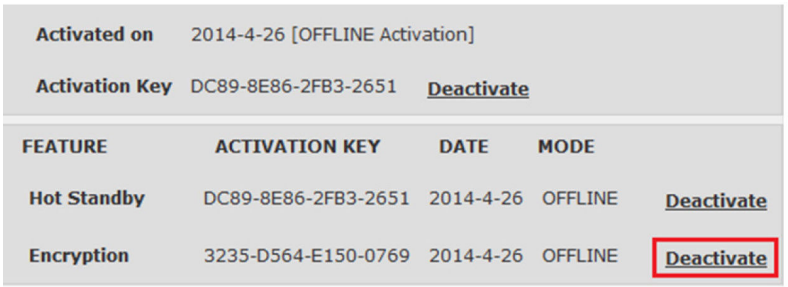
8 From the ContentConnect server Web Configuration Tool, select Admin > Licenses.

9 Do one of the following:

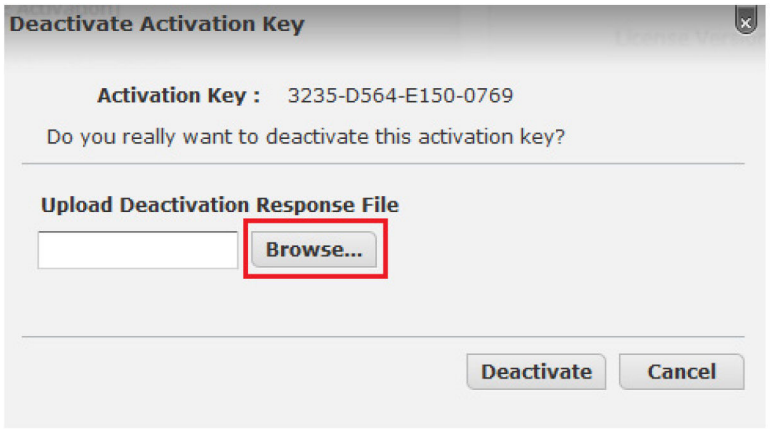
- Click Browse at the bottom of your window, and navigate to upload the response.bin file you got in step 7, and then click Activate.



- Click the Deactivate next to the desired license.



A dialog opens. Click Browse to select the response.bin file you saved in step 4, and then click Deactivate.



Activating the ContentConnect Server in Solution Mode

In solution mode, Polycom RealPresence Platform Director or Polycom RealPresence Resource Manager works as ContentConnect license server.

It controls and provides ContentConnect licensing information.

Licensing Your System with RealPresence Resource Manager

The RealPresence Resource Manager system must communicate with your system so it can be licensed and monitored.

After you install your system using your virtual environment tools, you need to add your system instance to the RealPresence Resource Manager system to establish communication.

For complete instructions on how to use the RealPresence Resource Manager system, see the *RealPresence Resource Manager System Operations Guide*.

License Your System with RealPresence Platform Director

The RealPresence Platform Director system must communicate with your system so it can be licensed and monitored.

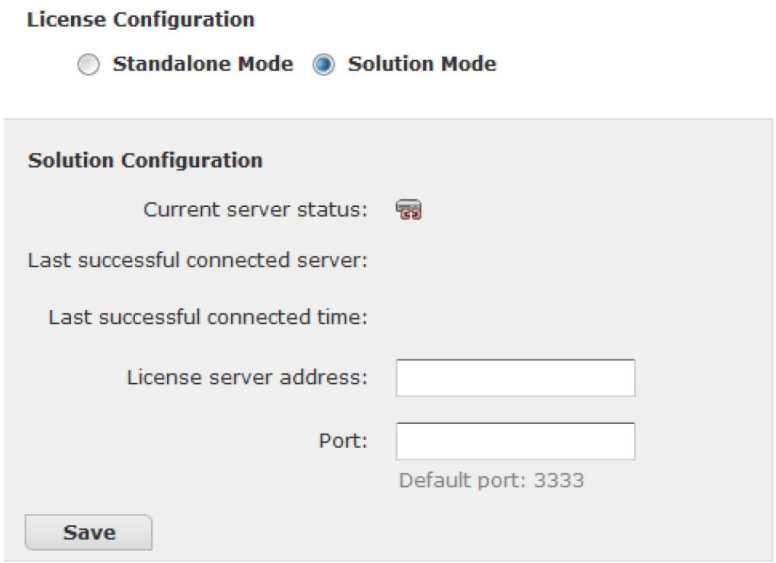
- If you used the RealPresence Platform Director system to deploy your system, communication is established automatically.
- If you used your virtual environment tools to install the system, you need to add your system instance to the RealPresence Platform Director if you have not done so already.
  For complete instructions on how to use the RealPresence Platform Director system, see the *RealPresence Platform Director System Administrator Guide*.

  Note: If your deployment includes a RealPresence Resource Manager system version 10.0 or later, you cannot use the RealPresence Platform Director system to license your product.

Activate the ContentConnect Server Product in Solution Mode

You can activate the ContentConnect server product in solution mode.

1. From the ContentConnect server Web Configuration Tool and select Admin > Licenses.
2. Click Solution Mode.
   The Solution configuration pane appears.



3. Enter your RealPresence Platform Director or Polycom RealPresence Resource Manager IP address and port in License server address and Port, then click Save.
4. When asked to confirm this action, click Yes.

If the activation is successful, your Current server status shows Online  ;

If the activation fails, you see Offline  instead. You can find more information in System Alert, which is on the lower-right of your window.

Related Concepts

Viewing License Details on page 94

You can find your license details in the License Detail window.

Deactivate Your Server License

You can deactivate your server license.

1. From the ContentConnect server Web Configuration Tool, select Admin > Licenses.
2. Click Deactivate.
3. When asked to confirm this action, click Yes.

Viewing License Details

You can find your license details in the License Detail window.

The available options are shown in the following table.

License Details

Attribute	Description
Host ID	The ContentConnect server device ID. This ID is generated by vSphere after you install the ContentConnect package. If you re-install the ContentConnect package, the ID changes also.
License version	License version.
License status	Valid: This license is valid. Expired: This license is expired and cannot be used.
Support media encryption	True: Media encryption is available for configuration. False: Media encryption is unavailable.
Support hot standby	True: Hot Standby is available for configuration. In case of master server failure, the slave server takes over its functionalities. False: Hot Standby is unavailable.
Licensed call number	The maximum number of concurrent calls you can make using this license. When your License mode is Package, the maximum call number is decided by Polycom DMA.
Used	Number of calls already used on this ContentConnect server.
Left	Number of calls available to make on this ContentConnect server.
Max used number of history	Maximum used call number in history on this ContentConnect server.
Expire time	Expiration date of this license.

Related Tasks

[Activate the ContentConnect Server Product License Offline in Standalone Mode](#) on page 86

You can activate the ContentConnect server product license offline in standalone mode.

[Activate the ContentConnect Server Product in Solution Mode](#) on page 93

You can activate the ContentConnect server product in solution mode.

Configure Video-based Screen Sharing (VbSS)

You can enable or disable Microsoft® Video-based Screen Sharing (VbSS) feature.

1. From the ContentConnect server Web Configuration Tool, select Admin > Server Configuration > VBSS Status.
2. Select an option and then select OK.

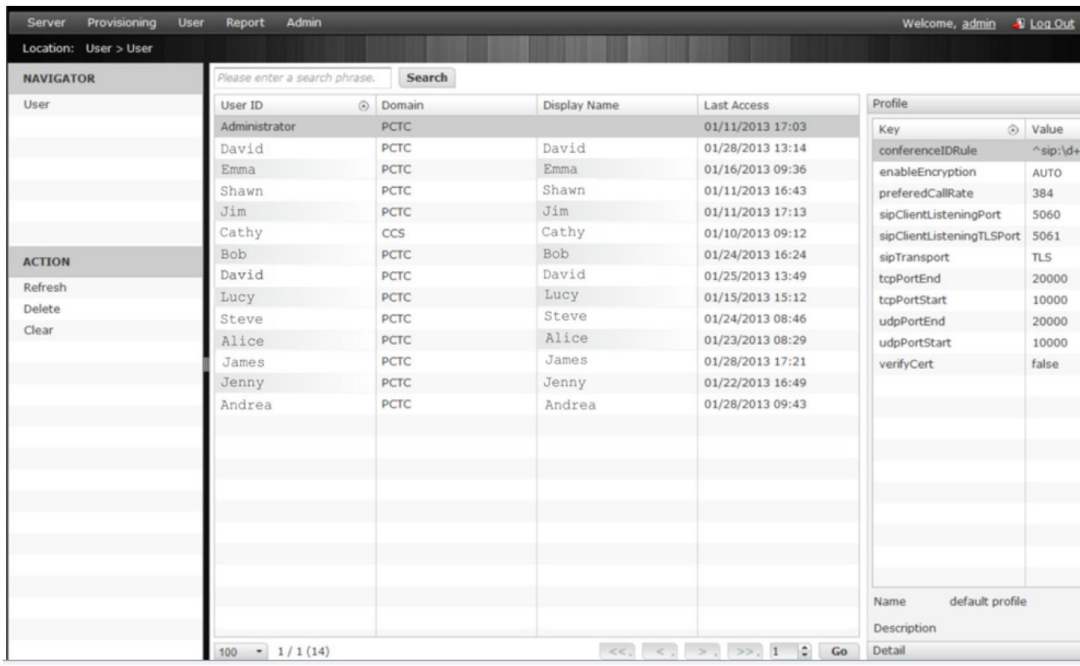
Manage Users

From the ContentConnect server Web Configuration Tool, you can view the server administrator, and all the Active Directory users who can join meetings using the ContentConnect Client.

Note: The User list is a list of all users who have ever registered to the ContentConnect server. The User list is not a live count of active users.

Log in to the ContentConnect server Web Configuration Tool and select User > User. From the User screen (shown next), you can do the following:

- Display the most up-to-date user information by clicking Refresh.
- Delete a user by selecting a user and clicking Delete.
- Delete all the users on a page by clicking Clear.
- Display a specific user when enter a user name in the Search box, and click on Search.
- Select the number of users to display on a page.
- Select a page to display by selecting a page number and clicking Go.



System Maintenance

The ContentConnect server maintains a list of system events and logs.

You can view certain events and logs, monitor gateway information, run the command tcpdump to download TCP packets for further analysis, or download logs to your local disk.

The ContentConnect server produces the following logs:

- System Event records activities related to system management and user management.
- System Log
- CCS.log records activities related to the ContentConnect process.

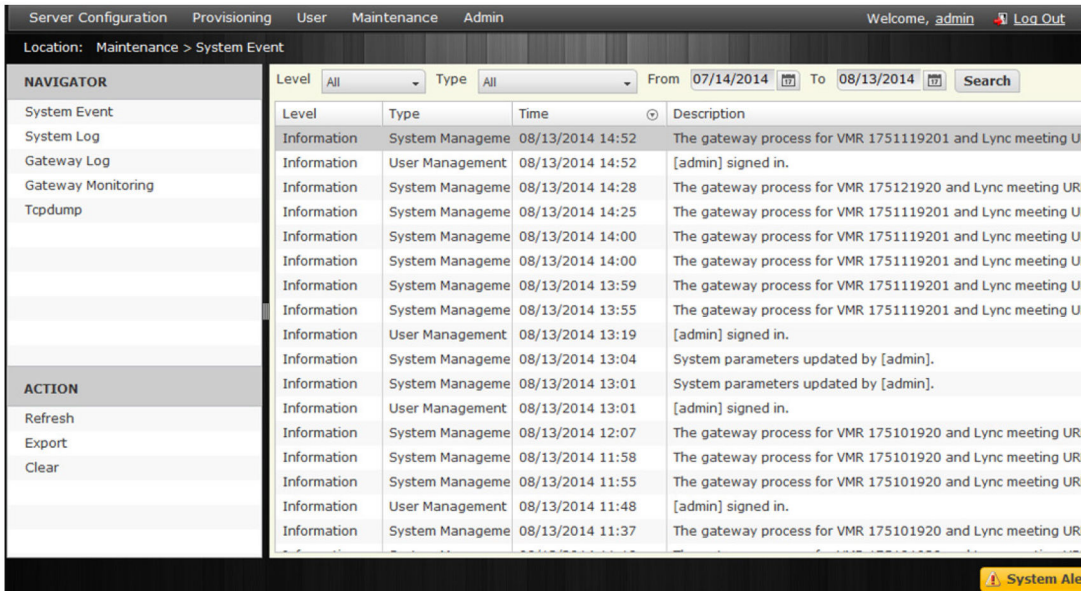
- catalina.log and localhost.log records activities related to the Apache Tomcat process.
- ccs-upgrade.log records activities related to upgrading the ContentConnect server.
- dhbs.log records activities related to HA.
- Gateway Log records activities related to Gateway instances.
- Gateway Monitoring records activities related to ContentConnect Gateway status.
- Traffic Capture provides the function to capture TCP packets sent from or received by your ContentConnect server.

Manage System Events

You can manage system events.

1. Log in to the ContentConnect server Web Configuration Tool and select Maintenance > System Event.
2. Filter the results you want to see by Level, Type, and date range.
   After you select filter criteria, click Search.
3. From the Action panel on the lower-left of the screen, you can do the following:
   - Delete the filtered results by clicking Clear.
   - Display the most up-to-date event information by clicking Refresh.
   - Open or save filtered results by clicking

- Export.



Manage System Logs

You can manage system logs.

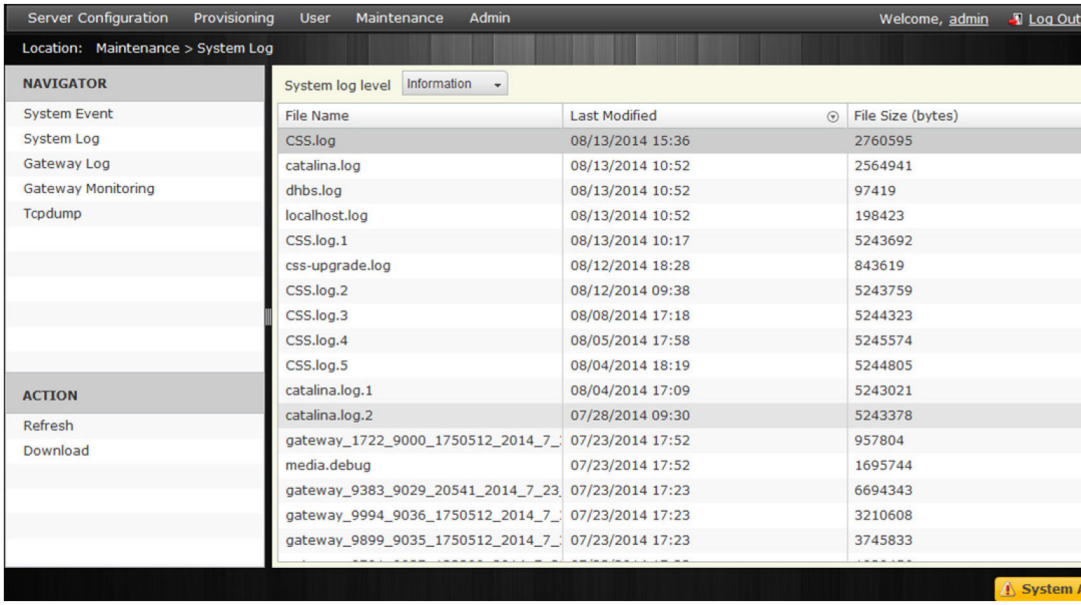
1. Log in to the ContentConnect server Web Configuration Tool and select Maintenance > System Log.
2. From the System Log screen you can do the following:

- Select what type of information to record in system logs by selecting a log level from the System log level list:
  - Information The system will include information for all log levels in system logs.
  - Warning The system will ignore information-level logs and include only warning- and error-level logs.

- Error The system will record only error-level logs.
- Off The system won't record any information in logs.

From the Action panel on the lower-left of the screen, you can do the following:

- Display the most up-to-date log information by clicking Refresh.
- Open or save filtered results by clicking Download.



Note: ContentConnect logs can be saved into maximum 10 files, with each file up to 5 MB. In case of more logs, the oldest log file is overwritten with new log info.

Manage Gateway Logs

You can manage gateway logs.

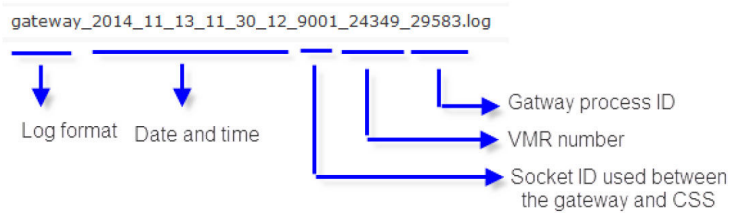
Following rules govern gateway logs:

- Gateway-formatted logs (gateway_xxxx.log) can be saved into maximum five files, with each file up to 10 MB. In case of more logs, the oldest log file is overwritten with new log info.
- Log files from the same gateway instance share the same date, time, and VMR info in their file names.

Following rules govern gateway logs archiving:

- Log files modified during the last 10 minutes are skipped in the archiving.
- The ContentConnect server archives gateway logs daily at 12:00:00 am automatically. However, archiving will be skipped in case of system upgrades.
- Both manual and automatic archiving will be skipped if the ContentConnect server CPU usage reaches 50% or above. You can find the server CPU usage from Maintenance > Gateway Monitoring.

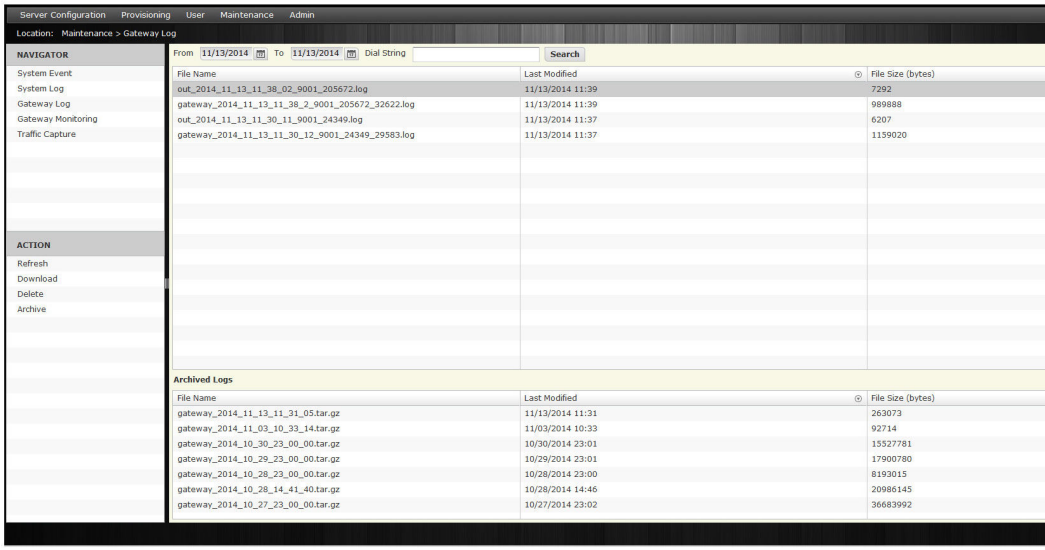
1 Log in to the ContentConnect server Web Configuration Tool and select Maintenance > Gateway Log.
Two log files (out_xxxx.log for standard console log output, and gateway_xxxx.log for Polycom gateway log output) are generated for each gateway instance. Log names consist these info:



2 Filter logs by the time range of the conference, by the dial string (VMR number) of the conference, or by both.

3 From the Action panel on the lower-left of the screen, you can do the following:

- Display the most up-to-date log information by clicking Refresh.
- Open or save filtered results by clicking Download.
- Delete a selected log or log archive by clicking Delete.
- Archive all log files into a compressed package by clicking Archive.



Monitor Gateway Information

You can monitor gateway information.

1 Log in to the ContentConnect server Web Configuration Tool and select Maintenance > Gateway Monitoring.

2 The following information is available:

Item	Description
CPU Count	Number of CPU cores of your ContentConnect server host.
CPU Usage	ContentConnect server host CPU resource usage by percentage.
Physical Memory Size	Physical memory of your ContentConnect server host.
Free Memory Size	Available memory size in the ContentConnect server host.
Total Disk Size	Total disk space in the ContentConnect server host.
Free Disk Size	Available disk space in the ContentConnect server host.
Total Gateway Resource	Maximum number of low quality content sharing (720 p15 or lower) sessions supported by your ContentConnect server.
Used Gateway Resource	Used gateway resource measured against resource needed for a low quality content sharing (720 p15 or lower) session.
Dial String	VMR number used to dial in to the conference.
Lync Meeting URL	Lync meeting URL used to dial in to the conference.
Content Quality	High: content of resolution 720 p30, 1080 p5 or higher.
	Low: content of resolution 720 p15 or lower.
CPU (%) Per Core	CPU resource usage by percentage for a CPU core.
Memory	Used system memory.

3. To display the most up-to-date log information, click Refresh.
4. To terminate a gateway instance, click Terminate.
   You can terminate active content sharing sessions to release CPU resource or memory.

Capture TCP Packets

You can capture TCP packets sent from or received by your ContentConnect server.

You can download the captured packets content for further analysis.

1. Log in to the ContentConnect server Web Configuration Tool and select Maintenance > Traffic Capture.
2. Click Capture to start packets capturing.
3. To stop the capturing, click Stop.
4. From the Action panel on the lower-left of the screen, you can do the following:

- Display the most up-to-date package list by clicking Refresh.
- Open or save filtered results by clicking Download.
- Delete a package by clicking Delete.
- Delete all packages by clicking Delete All.

Manage Administrators

From the ContentConnect server Web Configuration Tool, you can view a list of administrators that can manage the ContentConnect system.

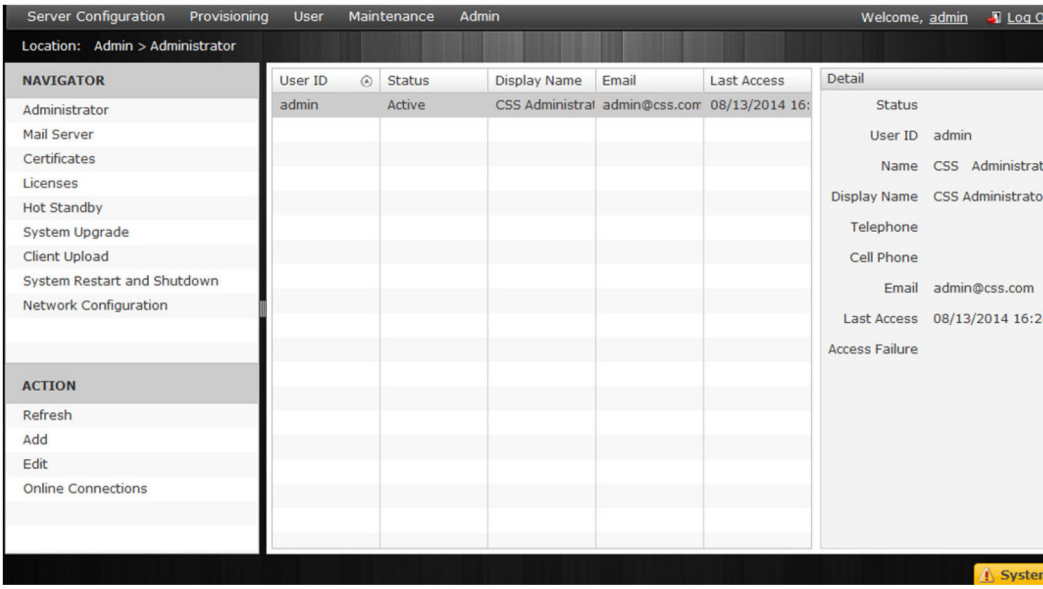
You can add new administrators, as well as edit existing ones.

1 Log in to the ContentConnect server Web Configuration Tool and select Admin > Administrator.

2 From the Administrator screen (shown next), you can do the following:

- Display the most up-to-date information (for example, an administrator's most current activity), by clicking Refresh.
- Add an administrator by clicking Add.
- Update an administrator's information (for example, the password, display name, telephone number, or status) by clicking Edit.
- Automatically log out an administrator who's currently signed in by clicking Online Connections, selecting a login session, and clicking Kick Out.

  Note: If you are using a Polycom RealPresence DMA system as your load balancer, the system adds 'matchmaker-agent' to the Administrator list automatically. Don't delete this account. Otherwise, the load balancer doesn't work. You cannot add this account back manually after the deletion, unless you re-deploy the ContentConnect application.



Managing the Database

You can back up or restore the ContentConnect server database, as well as view a list of previously backed up database files and delete old files.

When you restore a database, you update the ContentConnect server with a previously backed up file that you saved on your computer.

Note: You can back up and restore the database only for servers of the same version. For example, you can't back up the database of a ContentConnect version 1.5 server and restore it on a 1.6 one.

You can back up the ContentConnect server database.

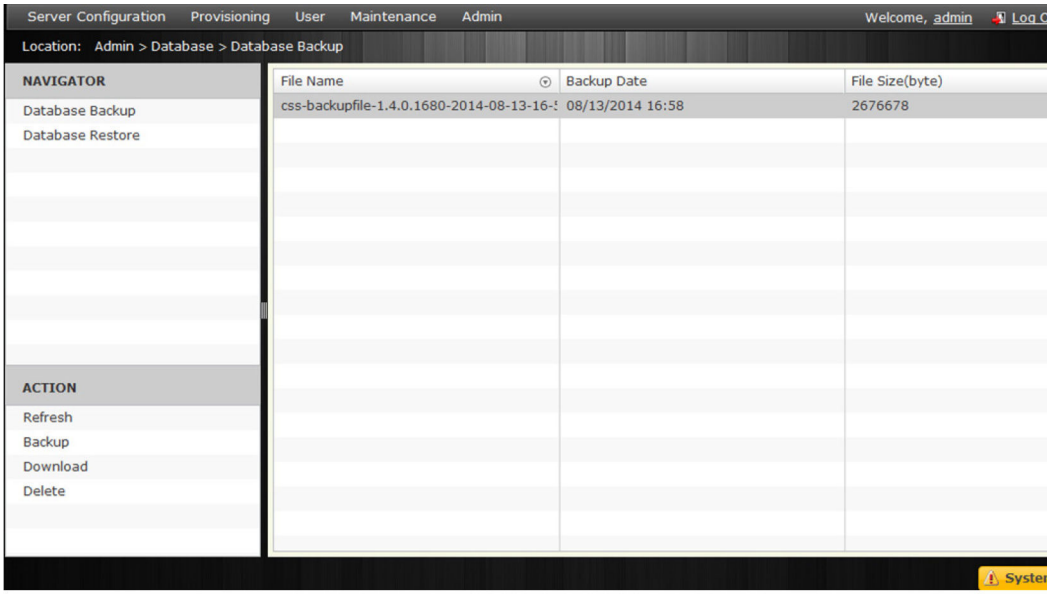
Managing the Database

You can back up or restore the ContentConnect server database, as well as view a list of previously backed up database files and delete old files.

When you restore a database, you update the ContentConnect server with a previously backed up file that you saved on your computer.

Note: You can back up and restore the database only for servers of the same version. For example, you can't back up the database of a ContentConnect version 1.5 server and restore it on a 1.6 one.

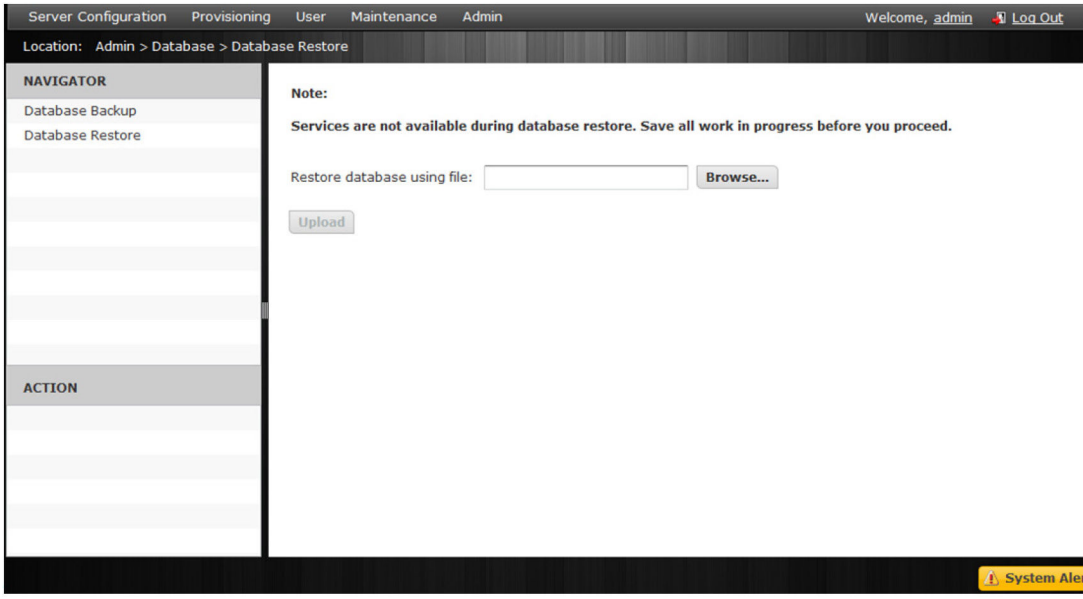
1. Log in to the ContentConnect server Web Configuration Tool and select Admin > Database > Database Backup.
2. From the Database Backup screen (shown next), you can do the following:
   - View a list of previously backed up files.
   - Display the most up-to-date information by clicking Refresh.
   - Create a backup file by selecting Backup.
   - Save a backup file to a central location by selecting a file, and clicking Download.
   - Delete a backup file by selecting a file, and clicking Delete.



Restore the ContentConnect Server Database

You can restore the ContentConnect server database.

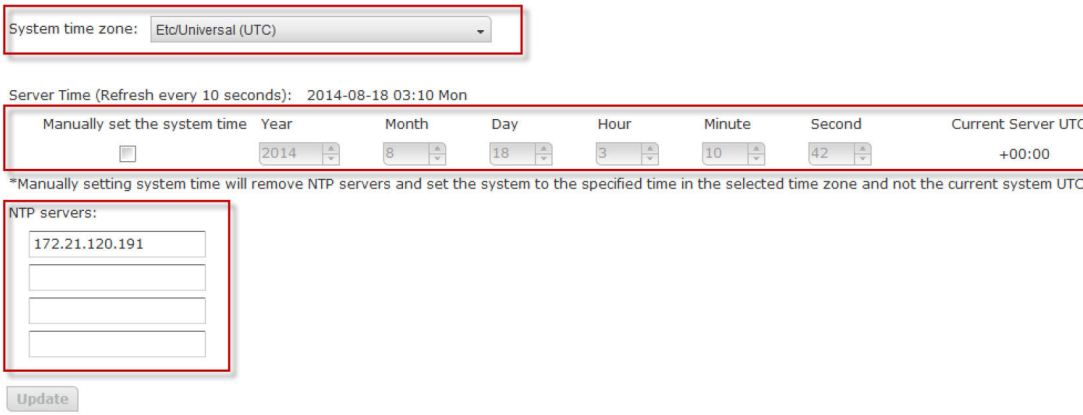
1. Log in to the ContentConnect server Web Configuration Tool and select Admin > Database > Database Restore.
2. From the Database Restore screen (shown next), click Browse to navigate to the backup file you want to use to restore the database, and click Upload.



Configure Your ContentConnect Server System Time

You can configure an NTP server to obtain time automatically, or set your system time manually.

1 Log in to the ContentConnect server Web Configuration Tool and select Admin > Time Configuration.



2 To set the time zone for the ContentConnect server, select a time zone from System time zone dropdown list.

3 To set your system time, do one of the following:

- To receive time from an NTP server, enter one or several NTP server addresses.
- To set your system time manually, select Manually set the system time, and then enter the time.

4 Click Update to save your changes.

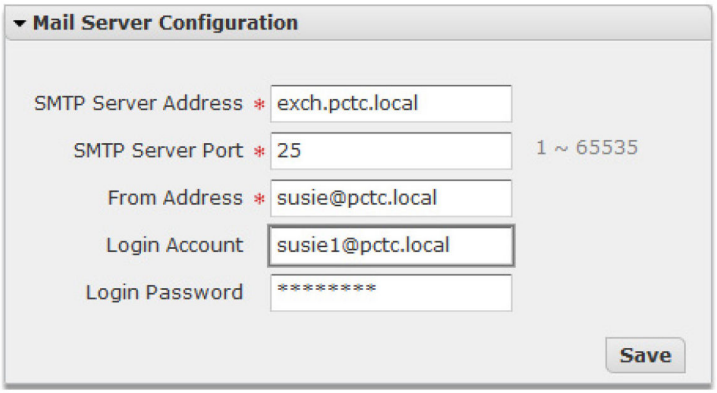
Note: When you enter multiple NTP server addresses, ContentConnect server will synchronize the time with the first NTP server. If the first NTP connection fails; the ContentConnect server connects to the next one available.

Configure a Mail Server for Administrators

Users who attempt to log in to the ContentConnect server Web Configuration Tool, but forget the login password, can click Forget Password to request the forgotten password.

You need to configure a mail server in order to receive these requests.

1 Log in to the ContentConnect server Web Configuration Tool and select Admin > Mail Server.
The Mail Server Configuration screen displays, as shown next.



2 Enter the administrator's mail server details and click Save.

Managing Certificates

By default, to support encrypted communications and establish a minimum level of trust, the ContentConnect system presents a self-signed digital certificate (without private key) to its clients.

You are recommended to get a certificate from a trusted certificate authority (CA) and update this self-signed certificate after you purchased the ContentConnect system.

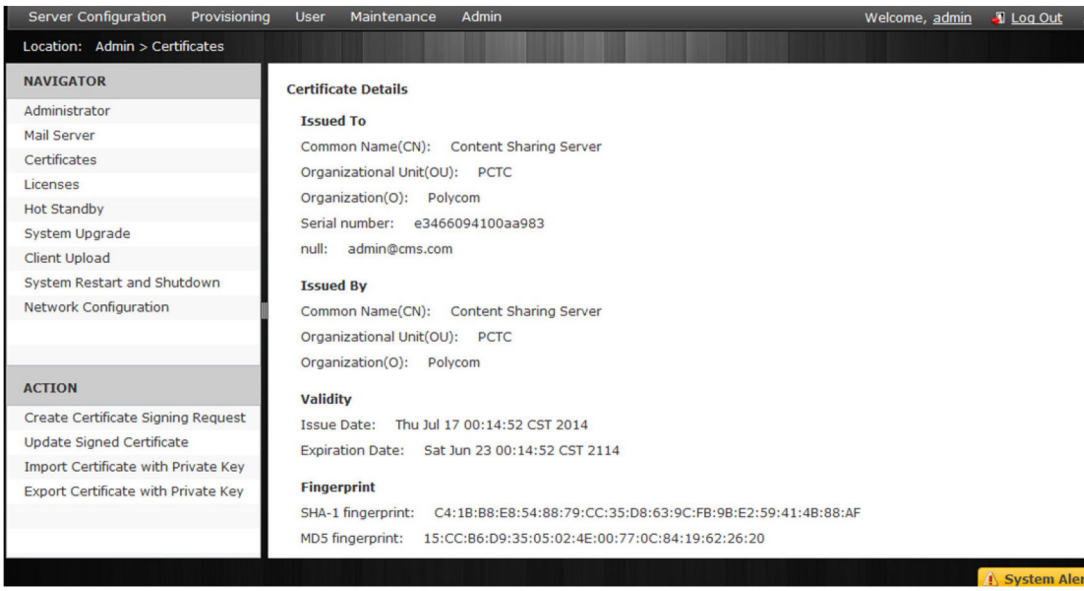
You can also export your ContentConnect certificate (with its private key) so that you can use it on another ContentConnect instance, or import a certificate (including the private key) generated from another ContentConnect system and use it on your ContentConnect system.

View Your Current Certificate

You can view your current certificate.

1 Log in to the ContentConnect server Web Configuration Tool.

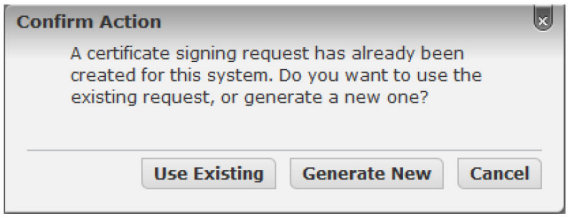
2 Select Admin > Certificates.
The Certificates Details window displays, as shown next.



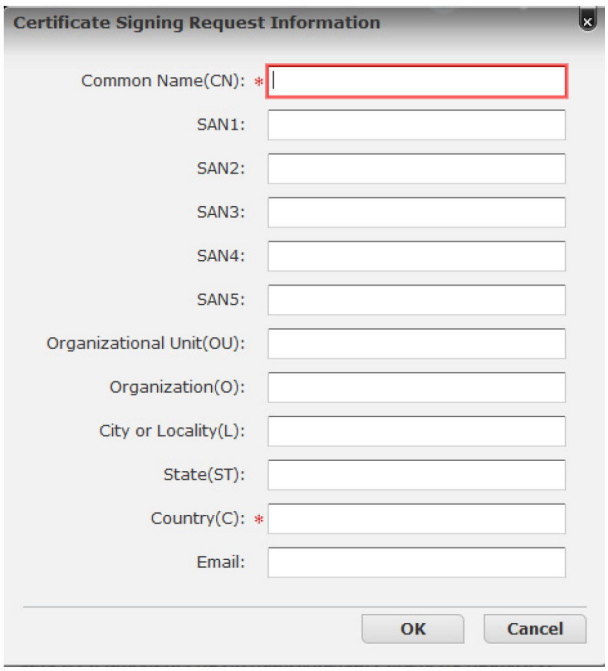
Create a Certificate Signing Request

You can create a certificate signing request.

1 Click Create Certificate Signing Request.
If a signing request has already been created, the server asks if you want to use the existing request or generate a new one (shown next). Click Use Existing to view the existing request, click Generate New to generate a new request.



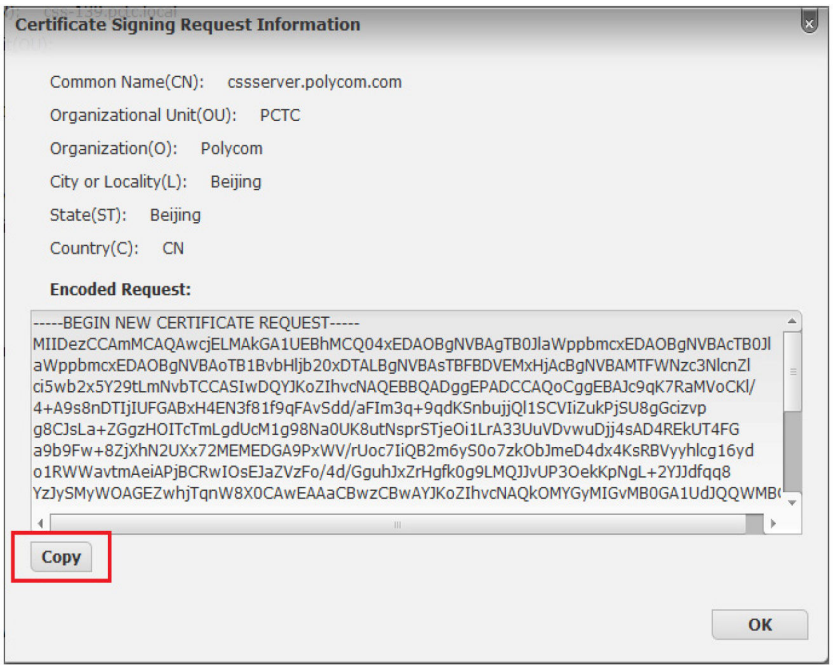
2 In the Certificate Signing Request Information window (shown next), enter the following information.



- Common Name (CN) Required. The Fully Qualified Domain Name (FQDN) or a human-friendly string.
- SANx Optional. The Subject Alternative Names. It should be a hostname or an IP address.
- Organizational unit (OU) Optional. The subdivision of your organization, such as Human Resources or IT that is handling the certificate.
- Organization (O) Optional. Usually the legal name of your enterprise.
- City or locality (L) Optional.
- State (ST) Optional.
- Country (C) Required. Two-character ISO code for the country in which your enterprise is located.
- Email Optional. An email address to contact your enterprise (usually the email address of the certificate administrator or IT department).

3 Click OK.

4 In the Certificate Signing Request Information window (shown next), click Copy to copy the entire contents of the Encoded Request to clipboard, you can save it to file or send to CA to apply certificate.



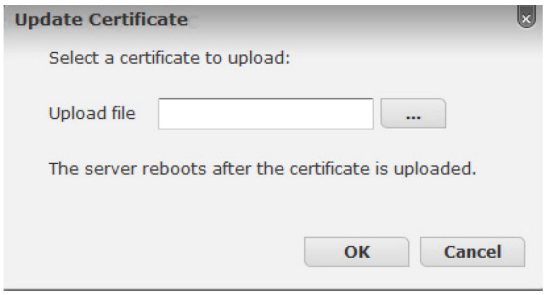
5 Click OK.

Update the Certificate

You can update the certificate.

1 Click Update Signed Certificate.

2 In Update Certificate dialog, browse to the location that contains the certificate file, and click OK.
If it's valid, server will validate the selected certificate and restart automatically.

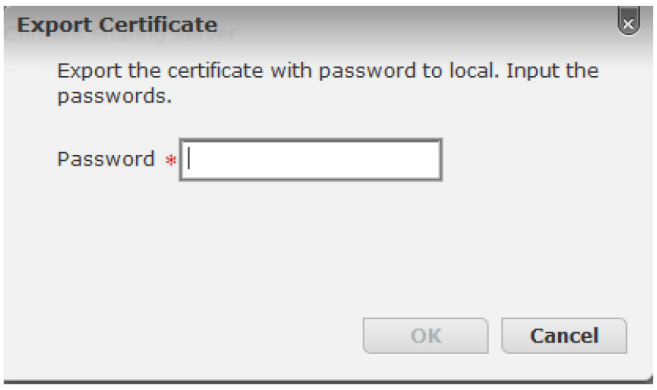


When the server restarts, log in and navigate to Certificate page. The new certificate details will display.

Export a Certificate with Private Key

You can export a certificate with private key.

1 Click Export Certificate with Private Key.

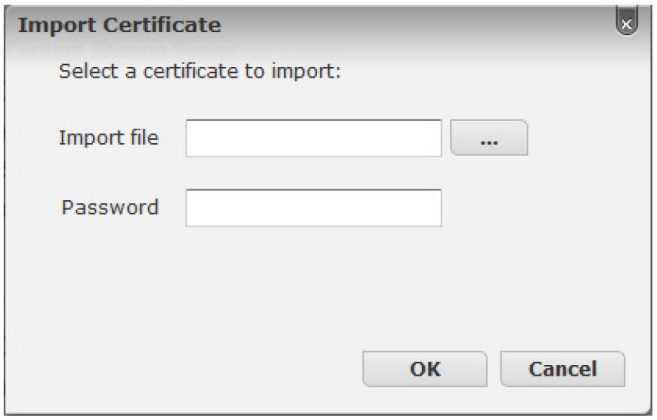


2 Enter a password to protect your certificate and click OK.
The same password must be provided when someone wants to import this certificate.

Import a Certificate with Private Key

You can import a certificate with private key.

1 Click Import Certificate with Private Key.



2 Click the button next to the Import file field to select your desired certificate.
3 Type the certificate password and click OK.
Contact the person who has exported the certificate to get the password.
4 When the server restarts, log in and navigate to Certificate page.
The new certificate details will display.

Enabling High Availability (Hot Standby)

Before you enable High Availability (Hot Standby), make sure you've installed and set up two ContentConnect servers with the same configurations.

You must activate the master ContentConnect server product license and HA license before you configure the HA.

In a High Availability (Hot Standby) environment, a master and slave server communicate using private network heartbeats. To enable High Availability (Hot Standby), you need to configure a new, virtual IP address as the Public IP address - which is different from the master and slave IP addresses - that the master and slave servers can share.

For example, your master/slave server configuration may look like this:

Master server configuration:

- Eth0 IP:172.21.125.145/23
- Eth1 IP:192.168.1.102/24 (used for private network heartbeats)

Slave server configuration:

- Eth0 IP:172.21.125.140/23
- Eth1 IP:192.168.1.101/24 (used for private network heartbeats)

Public IP address that you configured for both master and slave to share:

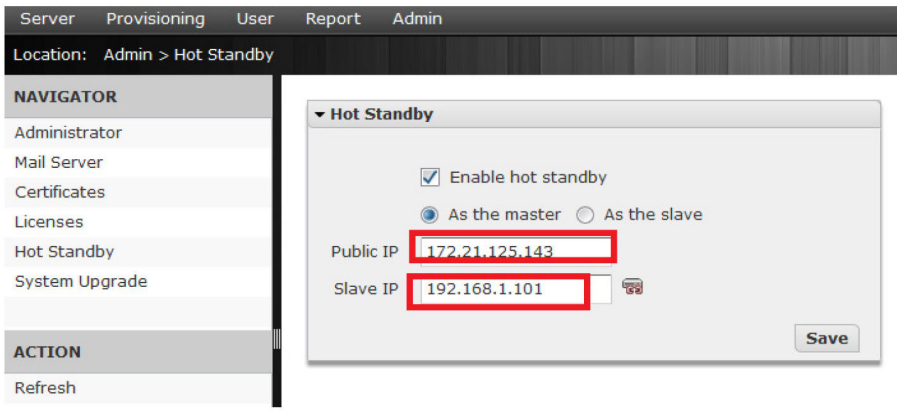
- 172.21.125.143

Note: To ensure successful hot standby, it's recommended to deploy two identical ContentConnect server s in an HA environment.

Enable Hot Standby Master Server

You can enable hot standby master server.

1. Log in to the ContentConnect server Web Configuration Utility and select Admin > Hot Standby.
2. From the Hot Standby screen (shown next), do the following:
3. Select the Enable hot standby option.
4. Enable the As the master option.
5. In the Public IP box, enter the virtual IP address you configured.
6. In the Slave IP box, enter the slave's heartbeat IP address.
7. Click Save.
   An icon displays next to the Slave IP box to verify the connection between the master and slave.



Note: Before you can configure a ContentConnect server as an HA master, you must activate both its product license and HA license.

Enable Hot Standby Slave Server

You can enable hot standby slave server.

1. Log in to the ContentConnect server Web Configuration Utility and select Admin > Hot Standby.
2. Do one of the following:
   - If the ContentConnect server has an activated HA license, select Enable hot standby and then select As the slave.
   - If the ContentConnect server has no HA license, select Set this server to be slave.

3 Click Save.

Note: When High Availability (Hot Standby) is setting up, the slave server will be in standby status and cannot be accessed by the ContentConnect server Web Configuration Tool.

Update Network Settings

You can update the system's network settings from the Network Configuration screen.

1 Log in to the ContentConnect server Web Configuration Tool and select Admin > Network Configuration.
2 From the Network Configuration screen (shown next), update the system's network settings.
3 Click Save.

Upgrade the ContentConnect Server

Before you can upgrade the ContentConnect server, you need to know the file path to the upgrade file.

Note: When you upgrade ContentConnect, make sure you enable the Client Version Compatible option on the administrator's web interface, or upgrade both the ContentConnect server and the Polycom ContentConnect Add-on for Microsoft Lync to the same version. For example, if you install version 1.2 of the Polycom ContentConnect server preconfigured VHD installation package, you need to install version 1.2 of the Polycom ContentConnect Add-on for Microsoft Lync on each Lync Client machine. If the ContentConnect server and Polycom ContentConnect Add-on for Microsoft Lync have different versions, your ContentConnect solution won't work properly.

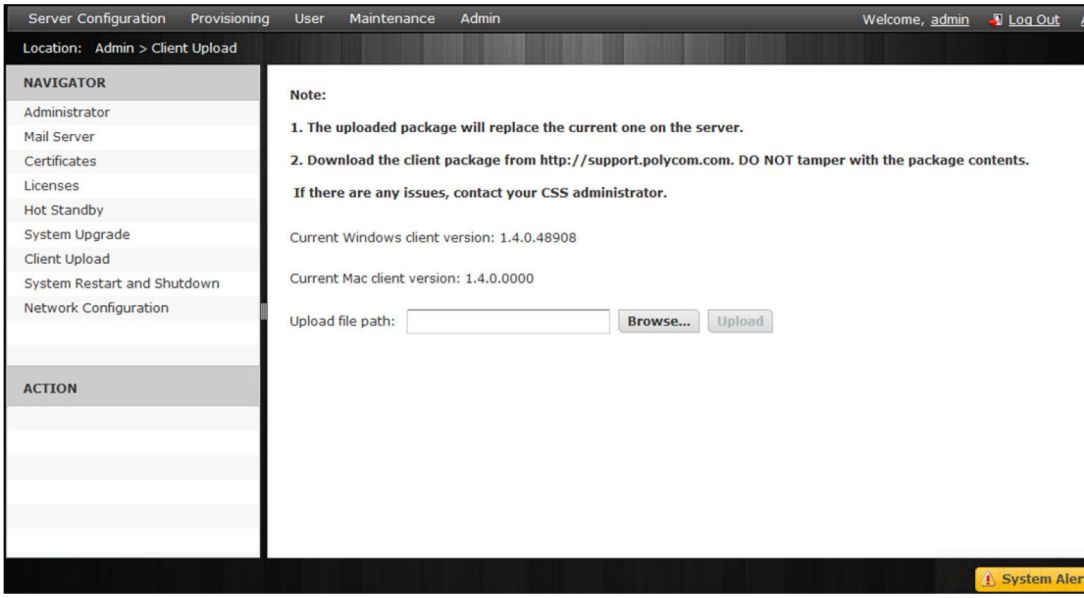
1 Save the upgrade file to a location on the computer.
2 Log in to the ContentConnect server Web Configuration Tool and select Admin > System Upgrade.
3 From the System Upgrade screen (shown next), click Browse, navigate to the location of the upgrade file, and click Upload.
The ContentConnect service restarts.

Update the Client Package

You can upload the Client package to the server on both Windows and Mac platforms.

Before you can update the Client package, you need to know the path of the Client package.

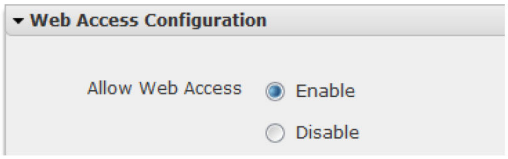
1 Save the Client package to a location on the computer.
2 Log in to the ContentConnect server Web Configuration Tool and select Admin > Client Upload
3 From the Client Upload screen (shown next), click Browse, navigate to the location of the client package, and click Upload.
The client package will update to the new version.



Enable Web Client Access

You can enable/disable the web client access from the Web Configuration Tool.

1. Log in to the ContentConnect server Web Configuration Tool and select Server Configuration > Client Configuration.
2. Click Enable on the right of the option Allow Web Access.

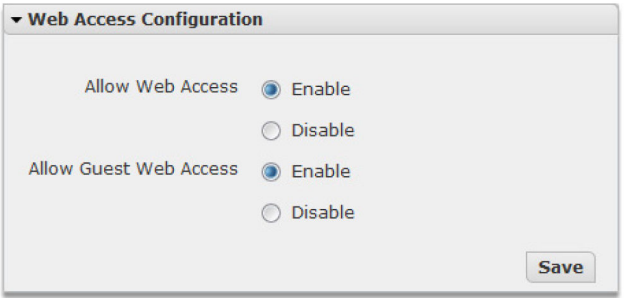


When web access is enabled, you can access the ContentConnect web client from a web browser using https://<your server ip address>/css/.

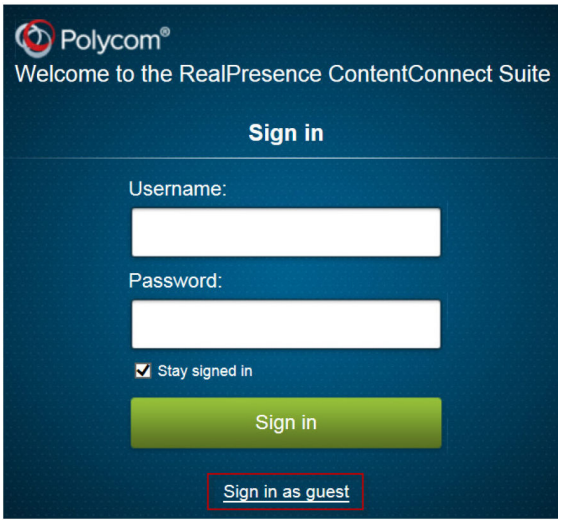
Enable Guest Web Access

You can enable/disable the guest web access from the Web Configuration Tool.

1. Log in to the ContentConnect server Web Configuration Tool and select Server Configuration > Client Configuration.
2. Click Enable on the right of the option Allow Guest Web Access.



When Allow Guest Web Access is enabled, you can log in to the web client as a guest without entering a username or password.



Configure Client Version Compatible Option

You can enable/disable the Client Version Compatible option.

If you select enable, ContentConnect server will set its compatibility with the client between the minimum versions to the current client version on server, or else ContentConnect server will support the current client version only.

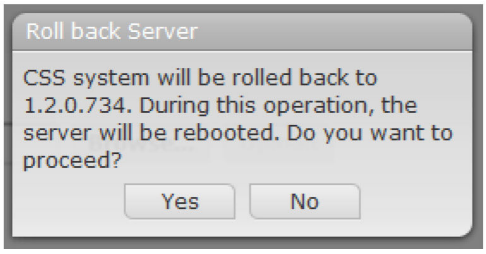
1. Log in to the ContentConnect server Web Configuration Tool and select Server Configuration > Client Configuration.
2. Click Enable for the option Client Version Compatible.
3. Click Save.

Roll Back the ContentConnect Server

After you upgrade the server, you have an option to roll back to its latest previous version from which it was upgraded.

1. Log in to the ContentConnect server Web Configuration Tool and select Admin > System Upgrade.
2. Click Rollback, as shown next.

3. In the dialog, click Yes to roll back the server to previous version.



System Restart or Shutdown

Before you restart or shut down the system, make sure you save any updates you've made using the ContentConnect server Web Configuration Tool.

Any unsaved changes will be lost when you restart or shut down the server.

1. Log in to the ContentConnect server Web Configuration Tool and select Admin > System Restart and Shutdown.
2. To restart the system, click Restart.
3. To shut down the system, click Shut Down.

   Note: Reboot is determined by the Install Shield (which is used for installation) depending on the operating system configuration and software installed on your PC.

ContentConnect Client Tasks

ContentConnect Client tasks include upgrading the Polycom ContentConnect Add-on for Microsoft Lync on the Lync Client's machine, and accessing a tool - the RealPresence ContentConnect Log Collector - that automatically packages ContentConnect Client log files.

Note: The Polycom ContentConnect Add-on for Microsoft Lync is required only when your ContentConnect server runs in the Add-On mode.

Upgrading the Polycom ContentConnect Add-on for Microsoft Lync

When you upgrade ContentConnect, make sure you enable the Client Version Compatible option on the administrator's web interface if you want to work with the already existing version of client on your PC.

You will need to upgrade both the ContentConnect server and the Polycom ContentConnect Add-on for Microsoft Lync to the same version. For example, if you install version 1.2 of the Polycom ContentConnect server installation package, you need to install version 1.2 of the Polycom ContentConnect Add-on for Microsoft Lync on each Lync Client machine. If the ContentConnect server and Polycom ContentConnect Add-on for Microsoft Lync have different versions, your ContentConnect solution won't work properly.

Check the Version of the ContentConnect Server

You can check the version of the ContentConnect server.

1. Log in to the ContentConnect server Web Configuration Tool and select Admin > System Upgrade.
2. From the System Upgrade screen, the current system version displays.

Check the Version of the Content Add-on for Lync

You can check the version of the content add-on for Lync.

1. Open the Lync Client computer's Control Panel.

2 Navigate to Programs and Features, and scroll to Polycom ContentConnect Add-on for Microsoft Lync.
The version displays in the Content Add-on for Lync row.

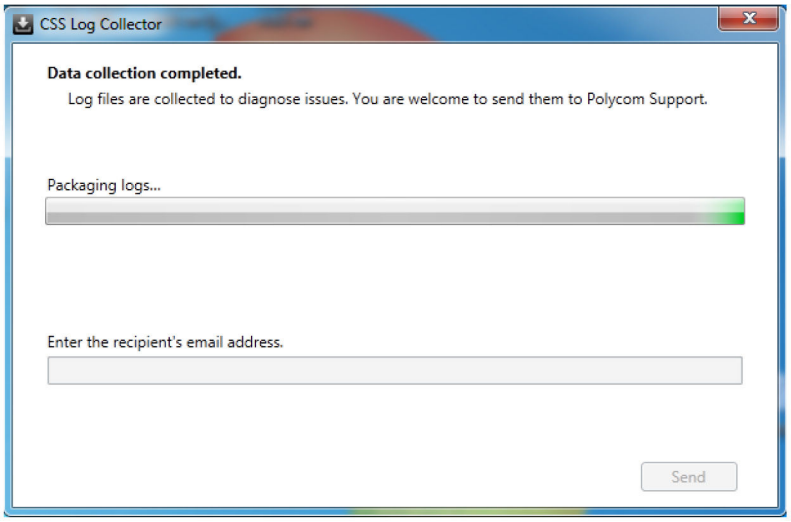
Access ContentConnect Client Logs

When you access the ContentConnect Log Collector, log files are automatically packaged for your convenience.

You can then enter an e-mail address to send the packaged log files to.

1 Close any open e-mail applications, such as Outlook.
(If you don't do this, the Log Collector may not be able to email the logs to the specified email address.)

2 From your computer's Start menu, select All Programs > Polycom > Polycom ContentConnect Add-on for Microsoft Lync > Log Collector.
The Log Collector opens and begins to package the log files, as shown next.



3 When Log Collector finishes packaging the files, the message “Log packaging completed” displays.

4 Enter the e-mail address to send the logs to, and click Send.

View and Share Content

The following information describes how to share and view content when the ContentConnect is deployed.

You can choose to share and view content from Microsoft Lync, or by entering a URL in your browser and accessing content over the Web.

Using Microsoft Lync to Share and View Content

This section describes how to use Microsoft Lync when the ContentConnect is deployed.

After reading this section, you'll understand how to use Lync to view and share content from your Lync client.

You can share your desktop or a program with other Lync endpoints, and video endpoints that receive content from RealPresence Collaboration Server (RMX).

Note: To share content when your ContentConnect server runs in the Add-On mode, the Polycom ContentConnect Add-on for Microsoft Lync on the Client machine must match the version on the server. If the two versions don't match, a dialog will display, prompting you to download and install a newer version of the Add-on. Click Download, and select Run to upgrade the Add-on to the newer version, or select Save to save the installation file and launch it manually to upgrade the Add-on.To check the version of the Polycom ContentConnect Add-on for Microsoft Lync on the ContentConnect server, log in to the ContentConnect server Web Configuration Tool and select Admin > Client Upload.

Viewing and Sharing Content

You can share your desktop or a program with other Lync users and endpoints that receive content from Polycom RealPresence Collaboration Server (RMX).

You have several ways to view and share content:

- As a non-Lync user, dial in using the conference ID included in the Outlook invitation e-mail.

  From ContentConnect version 1.3 and onwards, when you schedule a call from Outlook, the call can be automatically cascaded between Lync Server and Polycom RealPresence Collaboration Server (RMX) system.
- As a Lync user, invites a VMR number as a participant into the call.
- (Add-On mode only) As a Lync user, dial in using a VMR number.

Schedule a Conference from Outlook

You can schedule a conference from Outlook.

1. A Lync user initiates a new Lync meeting from Outlook.
2. Other Lync users dial in using the Lync URL contained in the meeting invitation.
   A meeting URL has this format: https://<FQDN>/<user>/<FocusID>
3. Standard video endpoints dial in using the conference ID contained in the meeting invitation.
   A conference ID may be one of the following formats:
   - 93646351@dmadomain.net
   - 7793646351@dmadomain.net

Invite a VMR Number as Participant into a Lync Call

You can invite a VMR number as participant into a Lync call.

1 When you are in a Lync call, invite more people:

- (Lync 2013) Click Invite More People
- (Lync 2010) Click Invite by Name or Phone Number.

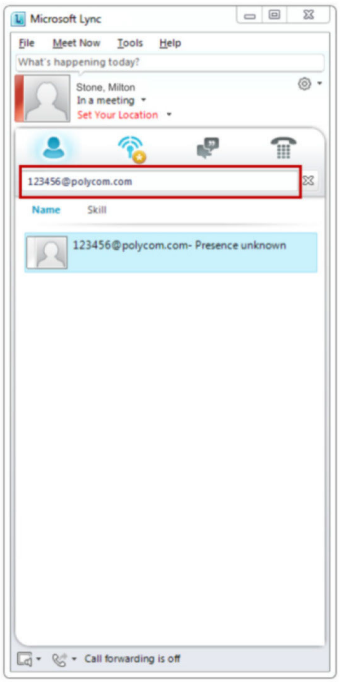
2 Add a VMR number, such as 721234@polycom.com, into your call.

Dial in to a VMR Call

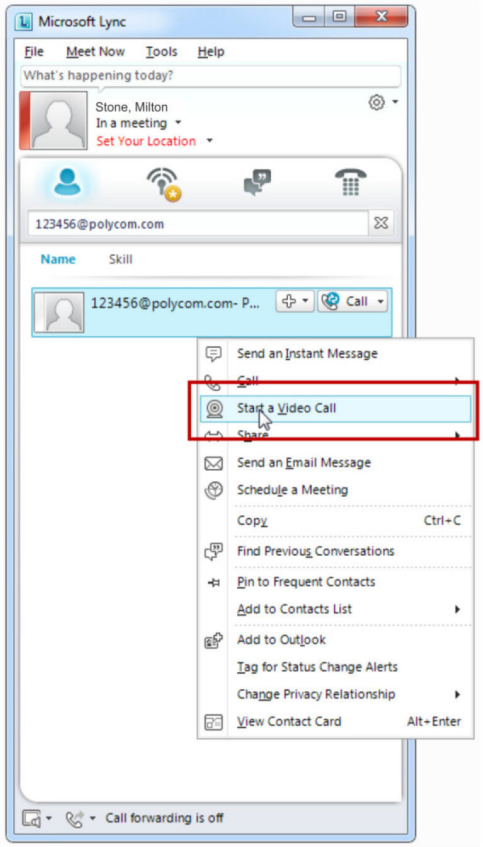
You can dial in to a VMR call.

1 From Microsoft Skype for Business, enter the VMR meeting number in the search box (as shown next).
The number displays in the window below the search box.

2 Enter a VMR meeting number



3 Right-click the number in the window, and select Start a Video Call (as shown next).



4 The call connects.
You can now view and share content with other meeting participants.

Configure Polycom DMA, RealPresence Collaboration Server (RMX), and ContentConnect server for Automatic VMR Call Cascading

For information on versions of compatible components, refer to the Interoperability List in the Release Notes of Polycom® RealPresence® ContentConnect available on support.polycom.com.

Note: Only general configuration steps are given in this book. For detailed information regarding Polycom RealPresence Collaboration Server (RMX) and DMA configuration, refer to their respective documentation from support.polycom.com.

Configure DMA for Auto VMR Cascading

You can configure DMA for auto VMR cascading.

1 Configure your Lync pool as an external SIP peer:
2 Enable combined RealPresence-Lync scheduled conference.
3 Assign a Lync account URI for conference resolution.
4 Enable the dial rule: When users dial in by Lync conference ID, resolve it to Lync Conference ID.
5 (For manual cascading only) Publish contact presence:
6 Enable Microsoft Active Directory Integration.
7 Publish contact presence to Lync pool.
8 Ensure DMA NTP server be the same as the one used by your Lync 2013 server.
9 Set DMA Domain FQDN as that of the Lync Pool.

Configure RealPresence Collaboration Server (RMX) for Auto VMR Cascading

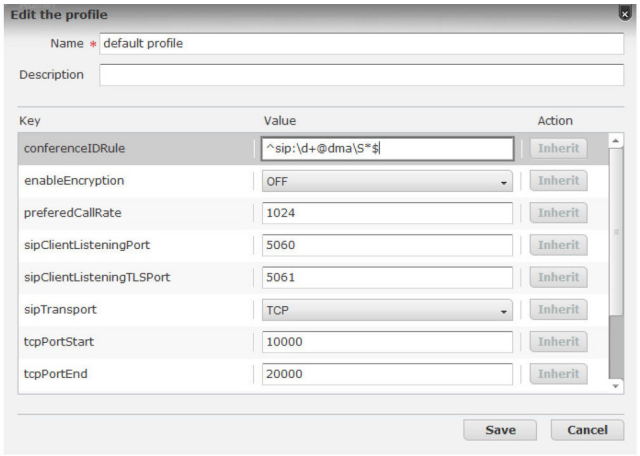
You can configure RealPresence Collaboration Server (RMX) for auto VMR cascading.

Enable support for Lync 2013 cascaded conferences.

Configure ContentConnect Server

You can configure ContentConnect server.

1. Choose Provisioning > Provisioning Profile.
2. Click Edit. The profile editing window opens.
3. Enter a VMR ID rule, for example, ^sip:\d+@dma\S*$, for conferenceIDRule.

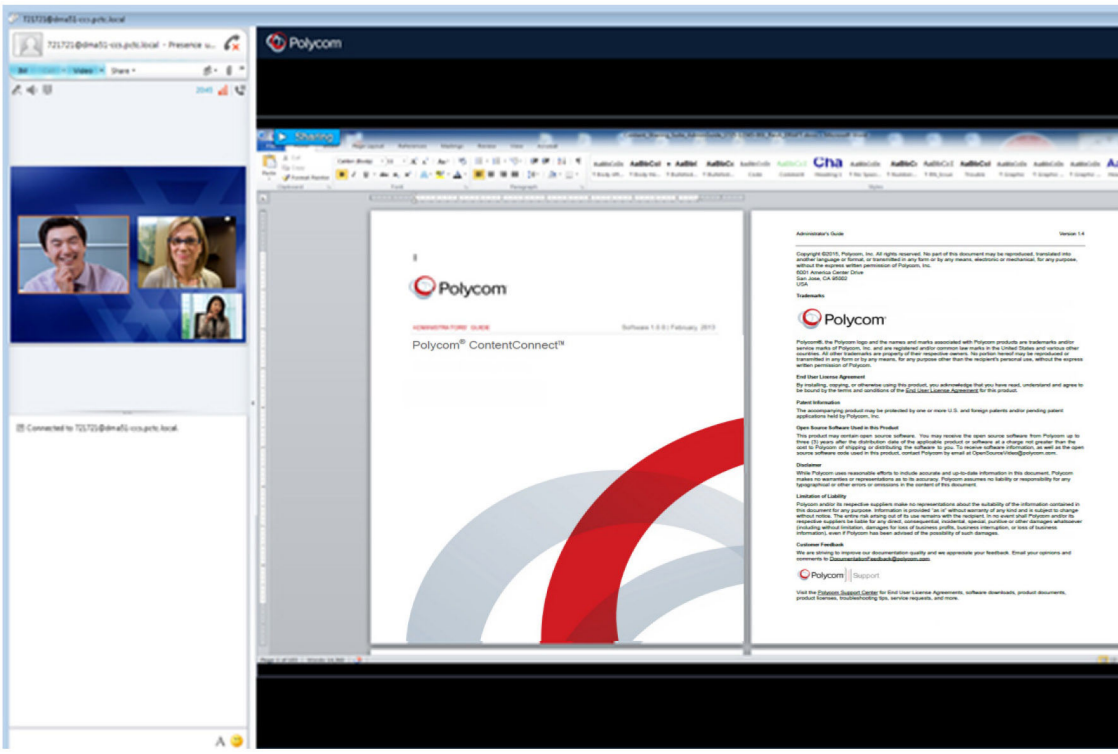


Viewing Content

If you're in a VMR call, another meeting participant can share their desktop or a program, and you'll see the shared content on the Lync content stage.

In the following example, a meeting participant is sharing a program (in this case, a Microsoft Word document). If a meeting participant wants to share content with you, you'll automatically see the content on the Lync stage.

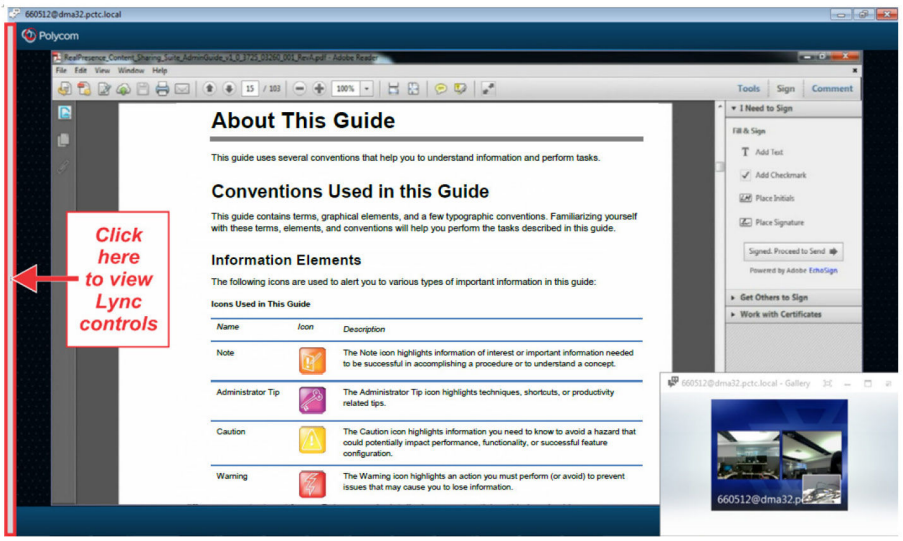
A meeting participant is sharing a program



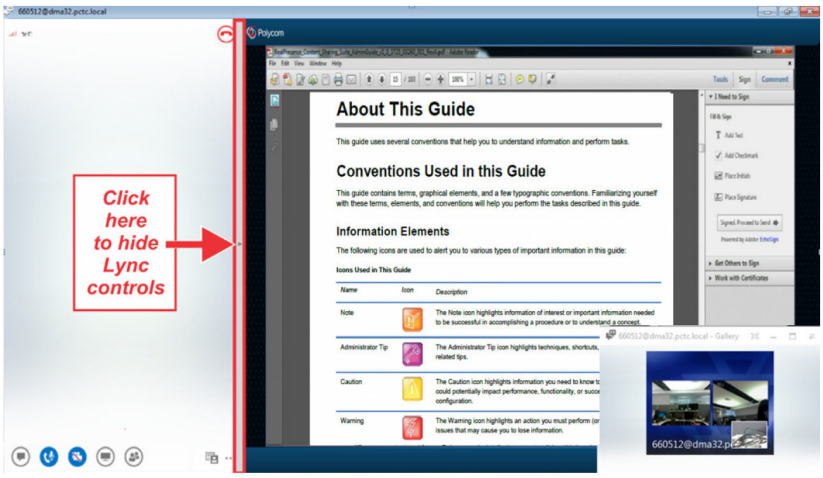
Viewing ContentConnect Content

Note that if you use Lync 2013, and you're viewing ContentConnect content, the Lync window is hidden.

To access Lync controls, click the gray bar that displays at the far-left of the screen, as shown next.



To hide the Lync controls, click the gray bar again, as shown next.

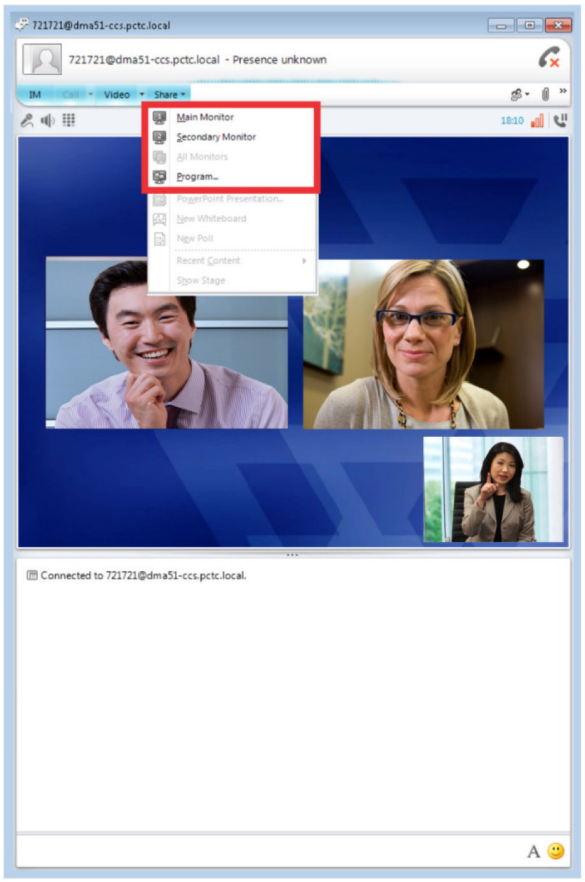


Sharing Content

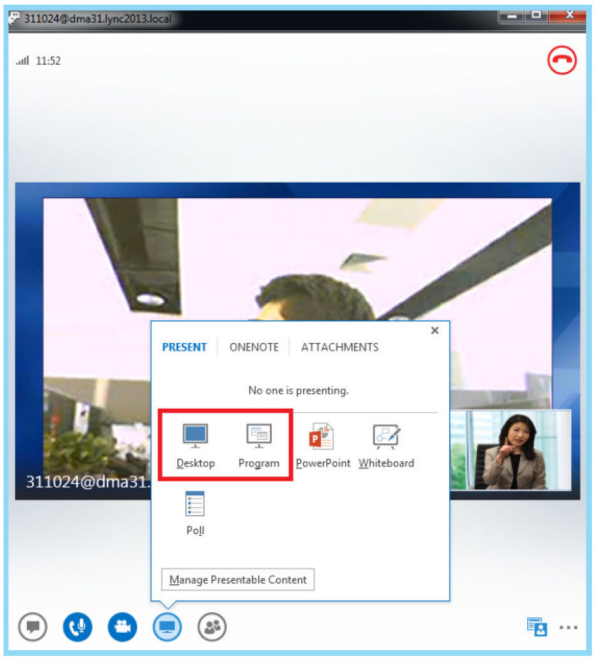
You can easily share content with other meeting participants.

You can easily share content with other meeting participants by navigating to Lync's Share menu (for Lync 2010) or by clicking the Monitor icon (for Lync 2013). After you select the Share menu or click the icon, you can choose to share your desktop or a program on your computer. If you have more than one monitor attached to your computer, you'll have the option to share one of your monitors.

The following figure shows Lync 2010's Share menu. In the example, more than one monitor is attached to the computer. You can choose to share the main monitor, a secondary monitor, or a program.

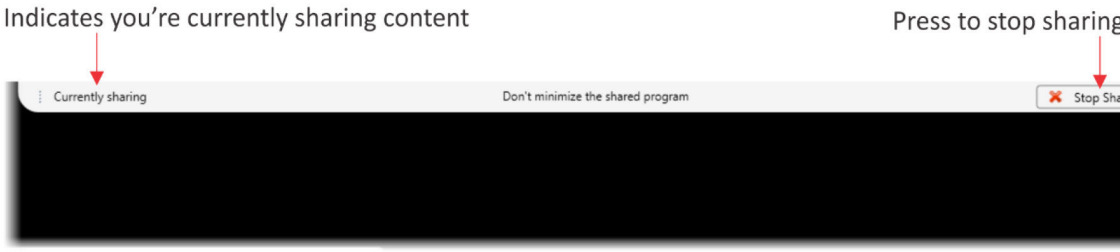


The following figure shows how to access sharing options in Lync 2013. In the example, only one monitor is attached to the computer. You can choose to share the desktop or a program.

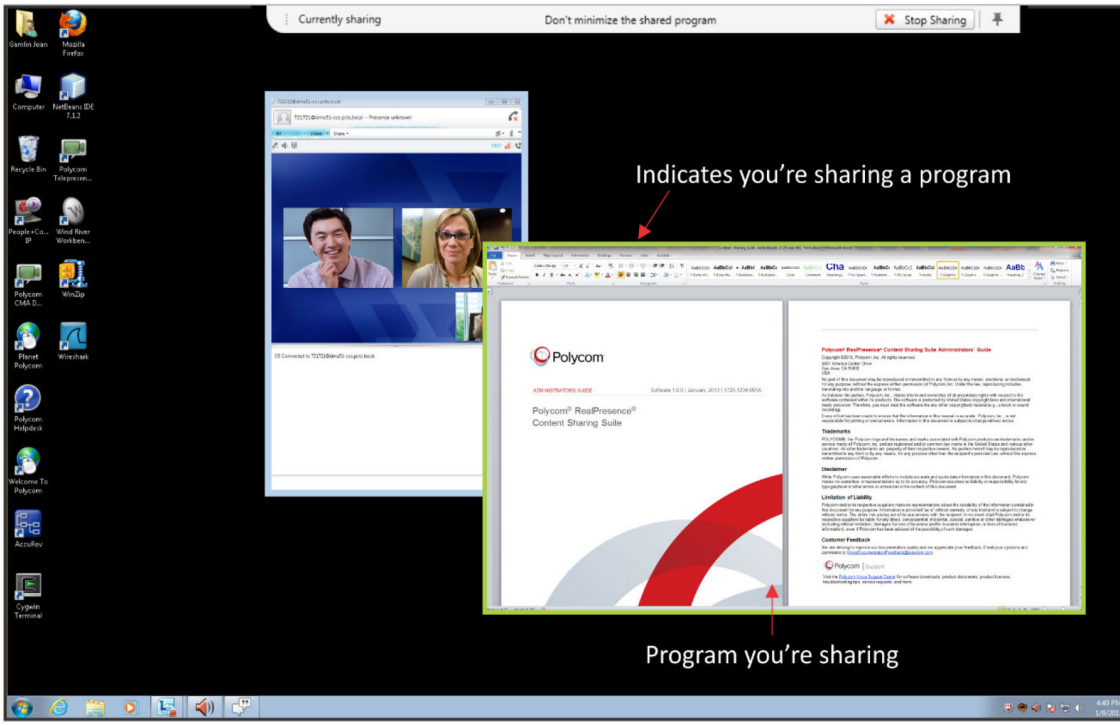


After you select the content you want to share, other meeting participants will automatically see the content.

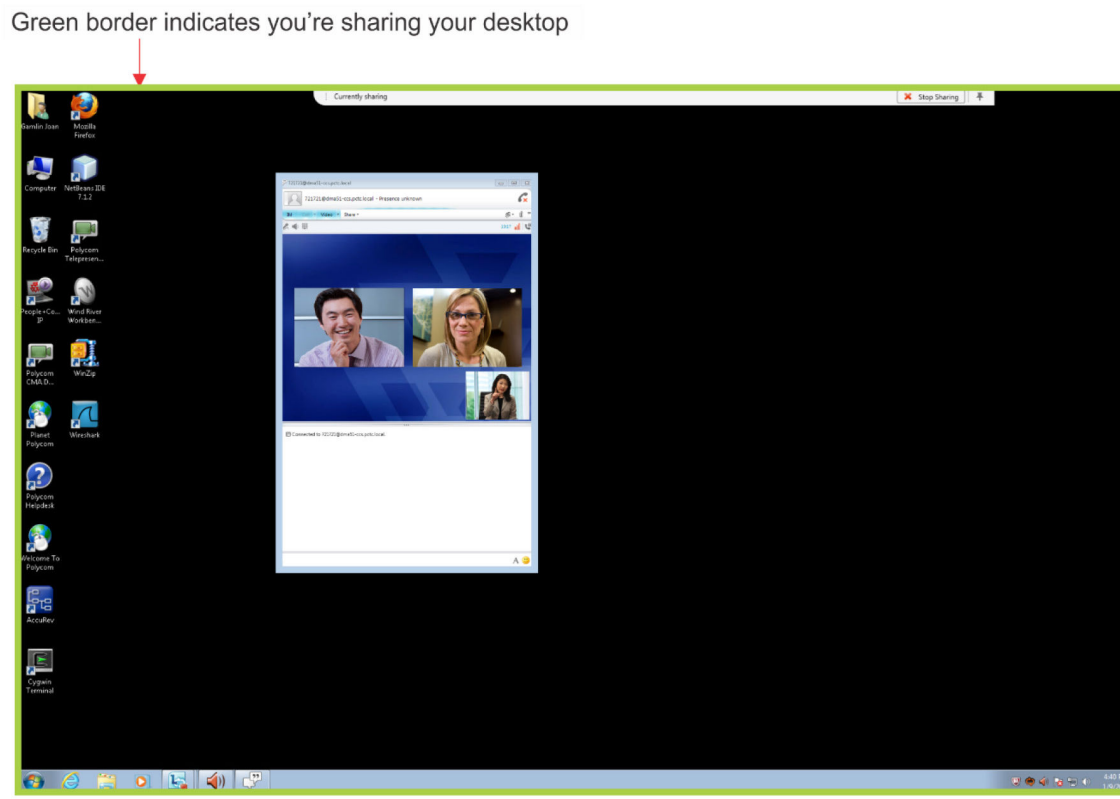
While you share content, a tab displays at the top of your computer indicating that you're currently sharing content, as shown next. To stop sharing content, click Stop Sharing at the far right of the tab.



If you're sharing a program, the program displays a green border, as shown next.



If you're sharing your desktop, a green border displays around your desktop, as shown next.



Share Your Desktop

You can share your desktop.

1. If you have Lync 2010, select Share > Desktop.

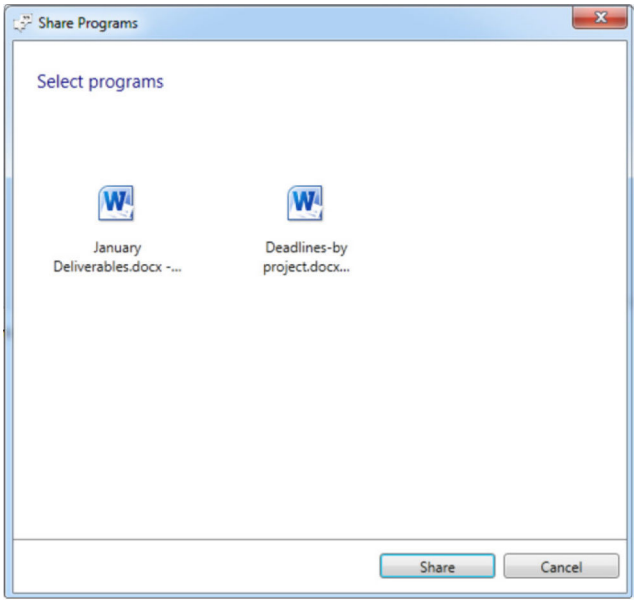
   Or, if you have Lync 2013, click and select Desktop.
2. If you have more than one monitor attached to your computer, choose Main Monitor or Secondary Monitor instead.
   A green border displays around your desktop. Other meeting participants will automatically see your desktop.

Share a Program

You can share a program.

1. Open the program you want to share.
2. If you have Lync 2010, select Share > Program.

   Or, if you have Lync 2013, click and select Program.
3. From the Share Programs window, shown next, select the program you want to share, and click Share.



The program you want to share displays on your desktop, outlined in bright green. Other meeting participants will automatically see the program.

Note: If you minimize a program you're sharing to your taskbar, the people you're sharing the program with will see a black screen. Make sure the program you want to share is maximized and in front of other open programs

View and Share Content over the Web

If you don't have access to Lync, you can access ContentConnect content over the Web by entering a special URL - https://<server IP>/css/ - in a Web browser.

This is helpful for non-Lync users dialing in to a meeting over audio but also wishing to view the shared content, or for external users sharing presentations with meeting participants.

After you enter the URL in your Web browser, you will be prompted to install or upgrade (if required) the BFCP Content-Only Client Plug-in on your machine so you can dial the VMR and view and share content.

When you view and share content over the Web, you won't have access to audio or video.

You can access Web-based content from Windows machines running Windows 7(32-bit and 64-bit) and Windows 8 with Internet Explorer 8 or later; and Mac machines running Mac OS X 10.7 or later with Safari(5.1 or later).

1 From a Web browser, enter the URL specified in the meeting request and press Enter.
The URL will have the following format: https://<server IP>/css/ (for example: https://172.21.125.152/css/).

   For the first access to the ContentConnect content over the Web, or your installed ContentConnect browser plugin is outdated, you are prompted to download and install the updated plugin. After the plugin is installed, restart your web browser, and enter the URL again.

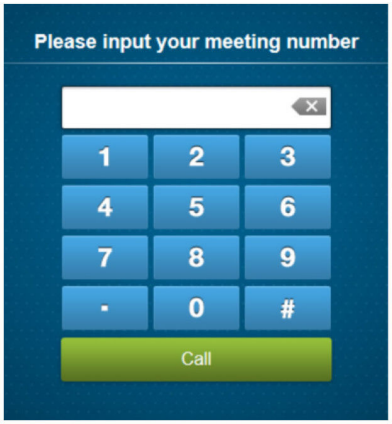
2 A login screen displays, as shown next.
Enter you Active Directory username and password and select Sign In.

You can also Sign in as guest. No user name or password is needed for guest users.

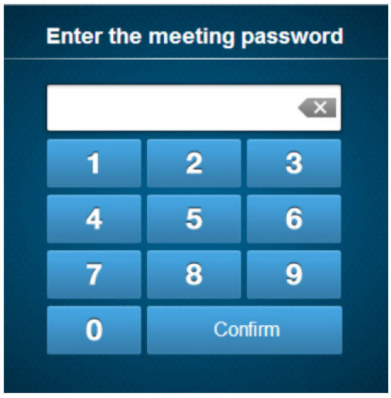
If this option is not available, check whether Allow Guest Web Access is enabled from the ContentConnect server Web Configuration Tool: Admin > Server Configuration.

3 For the first access, you are prompted to download the BFCP Content-Only Client Plug-in.

4 From the dialpad screen, shown next, use the onscreen dialpad to enter the VMR number and select Call to dial into the meeting.

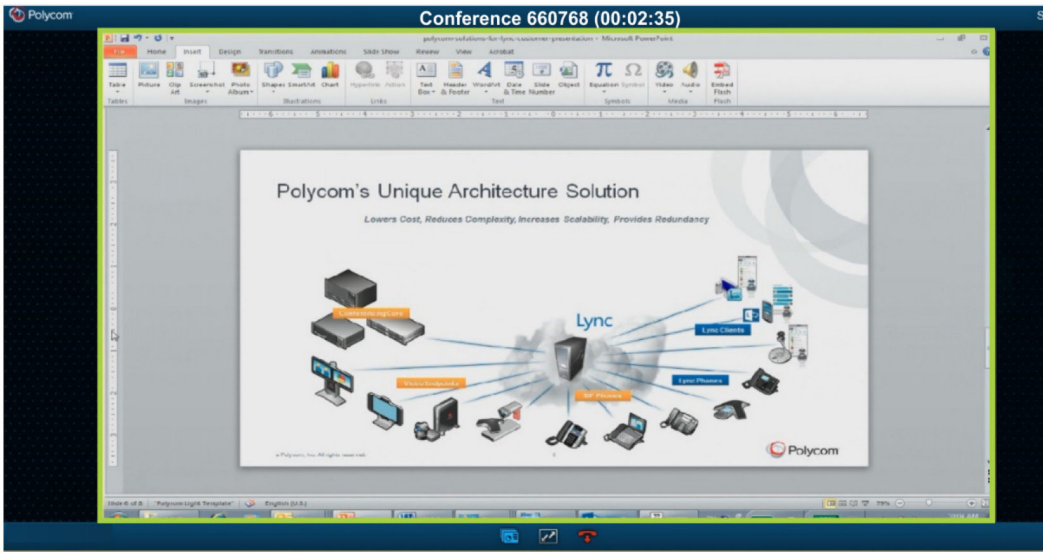


If the meeting requires you to enter a password to join the meeting, a password screen displays, as shown next. Using the online keypad, enter the meeting password (included in the meeting request), and then click Confirm, to join the meeting.

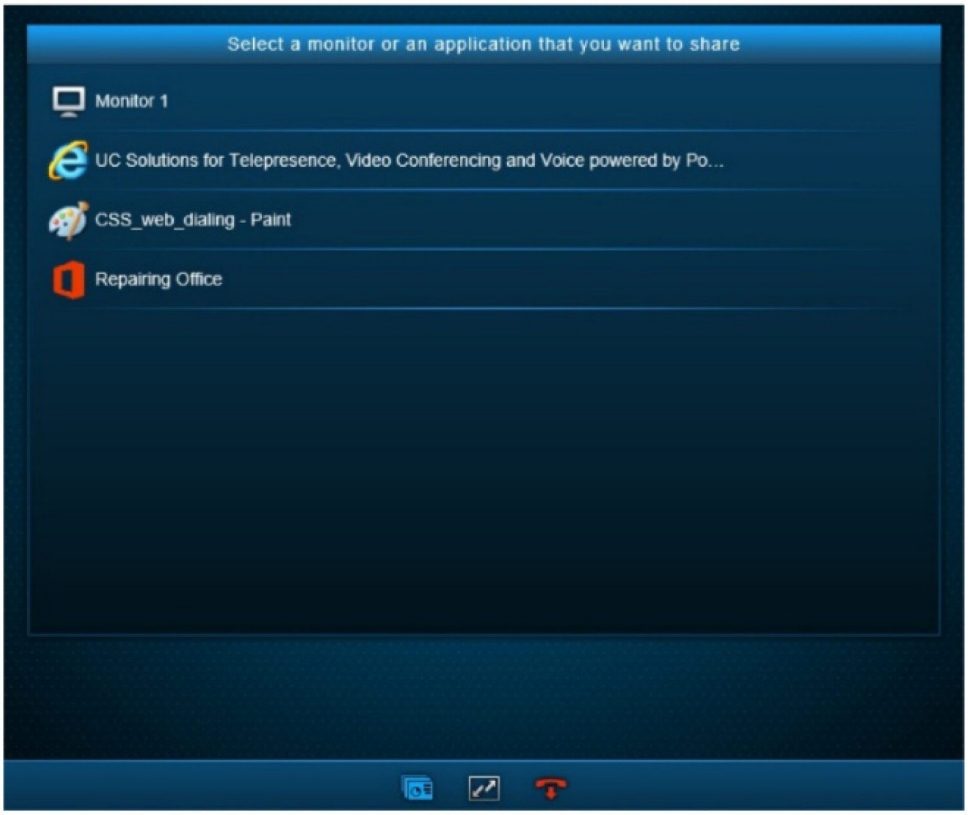


5 After you join the meeting, one of the following happens:

- If a meeting participant is sharing content (as shown next), you'll automatically see the content on the Web page. The shared content is outlined in green.



- If no meeting participants are sending content, the webpage displays a list of content - a monitor or an open application - that you can share (as shown next). To share content, select an item to share.



At the bottom of the Web page is a toolbar with three icons, as shown next.

6 Select an icon to do one of the following:

- To toggle between sharing and not sharing content, select  .
- To toggle between showing content on the full screen, or in a smaller window, select  .
- To exit the meeting, select  .

Note: The meeting request may contain a URL that contains the VMR (for example: https://172.21.115.134/css/?id=661920, where 172.21.115.134 is the server IP address and 661920 is the VMR number). If you enter this URL in your Web browser, you'll dial directly into the VMR (after completing any required steps, such as logging in, installing the plugin, or entering a meeting password) without having to enter a VMR using the dialpad.

Related Concepts

Product Overview of Polycom ContentConnect on page 12

The Polycom ContentConnect is a video collaboration application that enables users on disparate devices and clients, including Lync client, H.323 and SIP video

endpoints, and audio only participants, to participate in the full content sharing session.

ContentConnect Port Usage

The following table shows Add-on mode, the ContentConnect port usage when it is used inside and outside your corporate networks.

ContentConnect Port Usage in Add-on Mode

Source Interface	Source Port	Destination	Destination Port	Protocol	Use
Corporate network ContentConnect web client	Any	ContentConnect server	80	TCP	HTTP Provision (Redirects to HTTPS)
Corporate network ContentConnect web client	Any	ContentConnect server	443	TCP	HTTPS Provision
Corporate network ContentConnect Add-on client	Any	ContentConnect server	443	TCP	HTTPS Provision
External network ContentConnect web client	Any	RealPresence Access Director external interface	443	TCP	HTTPS Provision
External network ContentConnect Add-on client	Any	RealPresence Access Director external interface	443	TCP	HTTPS Provision
Corporate network ContentConnect web + Add-on client	Any	DMA	5060	TCP	Unencrypted SIP Signaling
External network ContentConnect web + Add-on client	Any	RealPresence Access Director external interface	5060	TCP	Unencrypted SIP Signaling
RealPresence Access Director internal interface	5070	DMA	5060	TCP	Unencrypted SIP Signaling
Corporate network ContentConnect web + Add-on client	Any	DMA	5061	TLS	Encrypted SIPS Signaling

Source Interface	Source Port	Destination	Destination Port	Protocol	Use
External network ContentConnect web + Add-on client	Any	RealPresence Access Director external interface	5061	TLS	Encrypted SIPS Signaling
RealPresence Access Director internal interface	5071	DMA	5061	TLS	Encrypted SIP Signaling
Corporate network ContentConnect web + Add-on client	10,000 - 20,000 (Default UDP ports assigned in ContentConnect Provisioning Profile)	RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 and Virtual Edition	49,152 - 59,999	UDP	RTP BFCP Media Traffic
External network ContentConnect web + Add-on client	10,000 - 20,000 (Default UDP ports assigned in ContentConnect provisioning profile)	RealPresence Access Director external media port	20,002 - 20,051 (Default UDP ports assigned in RealPresence Access Director external media port range. Upper range is subject to RealPresence Access Director license)	UDP	RTP BFCP Media Traffic

Source Interface	Source Port	Destination	Destination Port	Protocol	Use
RealPresence Access Director internal media port	40,002 - 40,051 (Default UDP ports assigned in RealPresence Access Director internal media port range. Upper range is subject to RealPresence Access Director license)	RealPresence Collaboration Server (RMX) 1500/1800/2000/ 4000 and Virtual Edition	49,152 - 59,999 (RealPresence Collaboration Server (RMX) default port range)	UDP	RTP BFCP Media Traffic
ContentConnect server	Any	AD Server	445	TCP	SMB
ContentConnect server	Any	AD Server	135	TCP	Netlogon RPC
ContentConnect server	Any	AD Server	139	TCP	NetBIOS Session Service
ContentConnect server	Any	AD Server	137	UDP	NetBIOS Name Resolution
DMA (DMA Integration with AD server is optional)	Any	AD Server	389	TCP	LDAP Integration

The following table shows Gateway mode, the ContentConnect port usage when it is used inside and outside your corporate networks.

ContentConnect Port Usage in Gateway Mode

Source Interface	Source Port	Destination	Destination Port	Protocol	Use
ContentConnect server	Any	Lync Edge Server, DMA, load balance server	443	TCP	ICE
ContentConnect server	Any	Lync Edge Server	443	TCP(STUN/MSTURN)	STUN/TURN negotiation of candidates over TCP on port 443
ContentConnect server	Any	Lync Edge Server	3478	UDP(STUN/MSTURN)	STUN/TURN negotiation of candidates over UDP on port 3478
ContentConnect	33300-43300 (Default media ports assigned in Server Configuration > Server > Media Transport Port Range)	Lync Edge Server	Any	TCP	Media Transport
ContentConnect server	Any	AD Server	445	TCP	SMB
ContentConnect server	Any	AD Server	135	TCP	Netlogon RPC
ContentConnect server	Any	AD Server	139	TCP	NetBIOS Session Service
ContentConnect server	Any	AD Server	137	UDP	NetBIOS Name Resolution
ContentConnect server	Any	NTP Server	123	UDP	Synchronize time
ContentConnect server	Any	DMA Server	8443	TCP	REST API registrar
DMA Server	Any	ContentConnect server	443	TCP	REST API callback

Source Interface	Source Port	Destination	Destination Port	Protocol	Use
ContentConnect server	Any	DMA Server	5060	TCP	Unencrypted SIP Signaling
ContentConnect server	Any	DMA Server	5061	TLS	Encrypted SIPS Signaling
RealPresence Collaboration Server (RMX)	Any	ContentConnect server	33300-43300	UDP	Media transport
ContentConnect server	Any	RealPresence Collaboration Server (RMX)	49152-59151	UDP	Media transport
ASMCU	Any	ContentConnect	33300-43300	UDP	Media transport
ASMCU	Any	ContentConnect	33300-43300	TCP	Media transport
ContentConnect	Any	ASMCU	49152-65535	TCP	Media transport
ContentConnect	Any	Flexera License Server	3333	TCP	License activate

Troubleshooting

Use the following information as a guide to resolve issues, problems, or common difficulties you may encounter while deploying ContentConnect.

Getting System Logs

If you encounter issues with the ContentConnect server, refer to the ContentConnect server's system logs.

To access the logs, see System Maintenance.

If you encounter issues with the ContentConnect Client, refer to the ContentConnect Client logs. To access the logs, see ContentConnect Client Tasks.

Installing and Upgrading Solution Components

When you install ContentConnect components, make sure you install the same versions of the ContentConnect server and the Polycom ContentConnect Add-on for Microsoft Lync.

If you are upgrading ContentConnect, make sure you enable Client Version Compatible option on the administrator's web interface. You will need to upgrade both the ContentConnect server and the Polycom ContentConnect Add-on for Microsoft Lync to the same version. For example, if you install version 1.2 of the Polycom ContentConnect server installation package, you need to install version 1.2 of the Polycom ContentConnect Add-on for Microsoft Lync on each Lync client machine.

Install a Newer Version of the Polycom ContentConnect Add-on

To share content when your ContentConnect server runs in the Add-On mode, the Polycom ContentConnect Add-on for Microsoft Lync on the Client machine must match the version on the server.

If the two versions don't match, a dialog will display, prompting you to download and install a newer version of the Add-on.

Click Download, and select Run to upgrade the Add-on to the newer version, or select Save to save the installation file and launch it manually to upgrade the Add-on.

Check the Version of the Polycom ContentConnect Add-on

You can check the version of the Polycom ContentConnect Add-on for Microsoft Lync on the ContentConnect server.

1. Log in to the ContentConnect server Web Configuration Tool.
2. Go to Admin > Client Upload.

Troubleshoot the ContentConnect Server

The following table lists issues you may encounter with the ContentConnect server.

Troubleshoot the ContentConnect Server

Description/Message	Action
There is an AD server integration failure in the ContentConnect server.	Do the following: Check if the ContentConnect server machine account and password in the AD server is valid. Check if the Netlogon service in the AD server is started.
The ContentConnect server cannot obtain an IP address when it started with DHCP protocol.	Do the following: Check if the DHCP server is working. Check if the DHCP IP address pool has enough available IP addresses.
The ContentConnect server cannot obtain an IP address when it started statically.	Do the following: Check if the IP address is duplicated in the network. Check if the network setting is correct. To update network settings, see Update Network Settings.
The Lync Client menu isn't replaced with the RealPresence Add-on for Lync menu during a VMR call.	Check if the ConferenceIDRule in the ContentConnect server is correct. To update the rule, see Configure Provisioning Information.
“Error: web site—Cannot access Polycom ContentConnect server. Exit and start Lync again.”	If you performed a silent installation without exiting Lync first, this message may display near your Windows taskbar, along with a progress bar which won't go away (as shown next). Close each message box by clicking the red x, and restart Lync.
“Conference ID rule does not match the conference ID.”	Edit the ContentConnect configuration file to reflect your domain. The error message indicates that the conferenceIDRule in the ContentConnect server - that determines if a contact is allowed in the RealPresence Collaboration Server (RMX) call - is incorrect. To update the rule, see Configure Provisioning Information.
I'm unable to share content.	If you're unable to share content, the preferred call rate for the SIP call with RealPresence Collaboration Server (RMX) may be set too low. The ContentConnect server's provisioning profile defines a preferred call rate for the SIP call with RealPresence Collaboration Server (RMX). To assure add-on can work for all conference rate on RealPresence Collaboration Server (RMX), the call rate must be equal to or higher than 512K. To check the call rate, see Configure Provisioning Information.

Description/Message	Action
My content sharing stops.	If the ContentConnect server works in the Gateway mode, the reason could be that the server CPU usage reaches 90% or above and it terminates some gateway instances to release system resource. Check your server log for more information.

Troubleshoot the ContentConnect Client

The following table lists issues you may encounter with the ContentConnect Client.

Troubleshoot the ContentConnect Client

Description/Message	Action
The Polycom ContentConnect Add-on for Microsoft Lync failed to start.	Do the following: Check if the ContentConnect Client - Polycom ContentConnect Add-on for Microsoft Lync and Polycom RealPresence Content Add-on for Web - display in the Control Panel. For more information, see Verify that the Content Add-on for Lync Installed Successfully. Check if the ContentConnect Client service - Polycom ContentConnect Add-on for Microsoft Lync Service - started successfully. For more information, see Upgrading Windows Installer. Check if the Polycom ContentConnect Add-on for Microsoft Lync is blocked by certain security software. If so, add LyncAddonDemon.exe, LyncAddon.exe, and ShareHook.dll to the security software's trusted list.
The Polycom ContentConnect Add-on for Microsoft Lync failed to install or upgrade	Certain security software may not permit the RealPresence Content Add-on to create windows service Polycom ContentConnect Add-on for Microsoft Lync Service. If so, you may need to change the security policy of your security software to allow this operation before you install or upgrade the Add-on.
The Polycom ContentConnect Add-on for Microsoft Lync failed to sign in.	Check your AD account and password, and enter them in the dialog boxes.
The server address cannot be found from the SRV records on the DNS Server. Check the Network status, DNS setting, or SRV configuration.	Check if the DNS address configured in your PC is correct. Check that the ContentConnect SRV record in the DNS server is configured correctly. For more information, see Configure Lync Clients to Auto-Discover the ContentConnect Server Address.
The far end is unreachable.	Do the following: Check if the Polycom ContentConnect Add-on for Microsoft Lync transport type provisioned from the ContentConnect server is consistent with DMA. Check if the DMA address is configured correctly in the ContentConnect server. Check the connection between the Polycom ContentConnect Add-on for Microsoft Lync and DMA. Confirm if DMA is working.

Description/Message	Action
Your user name or password is incorrect.	Do the following: Check if DMA requires authentication. Check if the SIP user and password is configured correctly. For more information, see Configure Server Information.
Cannot dial the unknown host.	Check if the DNS address in your PC is correct.
The server is in maintenance mode. Try again later.	Check if the Polycom ContentConnect Add-on for Microsoft Lync encryption mode provisioned from the ContentConnect server is consistent with RealPresence Collaboration Server (RMX).
The far end is unreachable. (When Polycom ContentConnect Add-on for Microsoft Lync is outside of RealPresence Access Director or the Acme Packet system.)	Do the following: Check if RealPresence Access Director parameters are configured correctly. Check that: The internal address matches the internal access IP in RealPresence Access Director. The external address matches the outer signal address in RealPresence Access Director. Check if the SIP server is working. Check if unsupported-UDP NAT devices are used and if the transport type UDP is set in the ContentConnect server. If so, try to adjust the transport type as TCP or TLS. Check if Acme Packet parameters are configured correctly.
Content sharing has stopped because the far end has ended the call.	Due to a network issue or other reason, the ContentConnect client has disconnected. End the call and dial again.
Sometimes the content you're sharing on a secondary monitor falls outside of the green border, indicating you are not sharing all the content on the monitor.	Stop and restart sharing to show all the content on the secondary monitor.
Sometimes, when you change your PC resolution while receiving content, you see a blue screen.	Resize the window to see the shared content again.
Sharing is not supported with this contact.	Edit the ContentConnect configuration file to reflect your domain. The error message indicates that the conferenceIDRule in the ContentConnect server - that determines if a contact is allowed in the RealPresence Collaboration Server (RMX) call - is incorrect. To update the rule, see Configure Provisioning Information.

Description/Message	Action
ContentConnect server address can't be found from the SRV records on the DNS Server. Please check the Network status, the DNS setting or SRV configuration.	Make sure you created the SRV record correctly. For more details, see Configure Lync Clients to Auto-Discover the ContentConnect Server Address .
Cannot access ContentConnect server, please edit and start Lync again.	You need to configure the Lync Client to find the ContentConnect server. For more details, see Configure Lync Clients to Auto-Discover the ContentConnect Server Address.
Shared content does not display properly.	To successfully view and share content from your machine, the Lync user name and password must match the Polycom ContentConnect Add-on for Microsoft Lync user name and password. If a Polycom ContentConnect Add-on for Microsoft Lync sign-in window displays after you log in to Lync (as shown next), make sure you enter your Lync credentials in the window. To avoid entering your credentials again, select Save my password in the login screen.
I'm unable to share a program, even though I selected it to share.	You're unable to share a program if it is minimized to the taskbar or behind another application. Make sure the program you want to share is maximized and in front of other open programs.
Error: WebPlugin - Polycom ContentConnect Add-on for Microsoft Lync doesn't match the server's version. Contact your administrator.	If the ContentConnect server and Polycom ContentConnect Add-on for Microsoft Lync have different versions, your ContentConnect solution won't work properly. Make sure the ContentConnect server and Polycom ContentConnect Add-on for Microsoft Lync have the same version.
The Polycom ContentConnect Add-on for Microsoft Lync won't start.	Check to make sure that your computer has only Lync 2010 or 2013. The Polycom ContentConnect Add-on for Microsoft Lync won't start if both Lync 2010 and 2013 are installed on the same machine.
Lync client or ContentConnect plug-in disconnects when more Lync user joins the meeting	Do one of the following: Move Lync/ContentConnect client to a better network. Lower the conference rate on RealPresence Collaboration Server (RMX) to fit actual network condition.
The far end is sending content, but I'm not receiving it.	Ask the far end to check if the firewall is blocking the content stream related to the Polycom ContentConnect Add-on for Microsoft Lync process.

Description/Message	Action
The Polycom ContentConnect Add-on for Microsoft Lync won't start automatically after an install or upgrade.	Try to manually start the Polycom ContentConnect Add-on for Microsoft Lync Service. To manually start the service, open your computer's Control Panel, double-click Administrative Tools, and double-click Services. Right-click Polycom ContentConnect Add-on for Microsoft Lync Service, and select Start.
Call InstallHook() from ShareHook64.dll failed after three times. Reboot or contact your administrator.	Restart the computer.
The Polycom ContentConnect Add-on for Microsoft Lync won't start.	Make sure you haven't signed into your computer using multiple accounts simultaneously. If you sign into your computer using multiple accounts simultaneously, the Polycom ContentConnect Add-on for Microsoft Lync may not run in one of the accounts, because it's still running in the other account.
The Polycom ContentConnect Add-on for Microsoft Lync is installed, but I can't receive or share content.	There may be an issue with the size of the text that displays on your computer screen. Open your computer's Control Panel, navigate to the Display settings, and make sure the size of text and other items on your screen is set to 100%.

Troubleshoot the Web Client

The following table lists issues you may encounter with the Web Client.

Troubleshooting the Web Client

Description/Message	Action
I don't see a green border (indicator for an ongoing content sharing) when I share an application using Internet Explorer.	Try the following: Disable Internet Explorer Protected Mode. Add the IP address to the list of Trusted Sites in Internet Explorer.
Cannot upgrade the ContentConnect server using Mozilla Firefox	Use another Web browser, such as Internet Explorer.
Cannot download the log and data-backup files of ContentConnect servers when using Chrome 29.0.1547.62 m version	Use a different browser.

Encryption Information

This table lists Polycom ContentConnect features and functionality that are encrypted, including the protocol used.

Application	Encryption Function	Description	Protocol Used
SIP Media Encryption	Confidentiality Integrity	End to end encryption of SIP videoconferencing media (audio, video) between product and far-end conference peer	SRTP per RFCs 3711, 4568, 6188
SIP Authentication	Authentication	Provides authentication of the product's SIP user agent credentials to the SIP Proxy/Registrar	NTLMv2
SIP Signaling Channel Client	Authentication Integrity Confidentiality	Allows product to register to a SIP registrar/proxy server to access videoconferencing call services over an encrypted TLS channel	TLS 1.2,1.1,1.0
SIP Signaling Channel Server	Authentication Integrity Confidentiality	Allows a SIP proxy server to send videoconferencing call signaling to the product on an encrypted TLS channel	NA

Open Source Attributions and Licenses

The Polycom ContentConnect includes components subject to various open source licenses.

Some of these licenses give you the right to request the source code for the components to which they apply. If you wish to receive the source code for particular components that are subject to such a license, please make a specific request to the following email address: opensourcevideo@polycom.com.

For a complete list of open source attributions and licenses, see the *Polycom Content Sharing Suite Open Source Licenses and Notices* document, available from the Polycom® RealPresence® ContentConnect support page.