



Collaboration Performance Management  
Technical Deployment Guide  
for  
CPM Analytics & CPM Monitoring

Last Updated: January 14, 2019

Document Version: 3.7.1



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS DOCUMENT ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENT ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE ARE PROVIDED "AS IS" WITH ALL FAULTS. VYOPTA DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL VYOPTA BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF VYOPTA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Other company and product names mentioned herein may be trademarks of their respective companies. Mention of third-party products is for informational purposes only and constitutes neither an endorsement nor a recommendation. Vyopta assumes no responsibility with regard to the performance or use of these products. All understandings, agreements, or warranties, if any, take place directly between the vendors and the prospective users. Every effort has been made to ensure that the information in this document is accurate. Vyopta is not responsible for printing or clerical errors.

Copyright © 2019 Vyopta Incorporated. All rights reserved.  
Vyopta® is a registered trademark of Vyopta Incorporated. Reg. USPTO.



## 1 Table of Contents

1	Table of Contents .....	3
2	Getting Started - Preparing Your Environment .....	6
2.1	Overview .....	6
2.2	Sign Up for a Vyopta Applications Management Portal User Account.....	6
2.3	Obtain Administrator Access for your User Account.....	6
2.4	Configure Service Account.....	7
2.5	Prepare a Vyopta Data Collector server instance .....	8
2.6	Test Connection to the Vyopta Cloud.....	9
2.7	Download and Install the Vyopta Data Collector.....	9
2.8	Launch the vAnalytics™ Configuration Utility Setup.....	10
2.9	Operational Prerequisites.....	11
2.10	Coverage and Compatibility .....	11
3	Cisco Expressway-E/C (formerly VCS Control & VCS Expressway).....	12
3.1	Set up a Service Account for Cisco Expressway-E/C or VCS.....	12
3.2	Add Expressway-E/C or VCS .....	13
3.3	Cisco Video Communications Server Control (VCS-C) & Expressway (VCS-E) Reference Table .....	14
4	Cisco Telepresence Multipoint Control Unit (MCU), Telepresence Server (TPS), or Telepresence Integrated Services Digital Network (ISDN) Gateway .....	15
4.1	Set up a Service Account for Cisco Multipoint Control Unit (MCU), Telepresence Server (TPS), or Integrated Services Digital Network (ISDN) Gateway .....	15
4.2	Enable CDR Permanent Storage on Cisco Codian (MCU) & ISDN Gateway .....	17
4.3	Add MCU, TP Server, or ISDN Gateway .....	17
4.4	Cisco TelePresence Multipoint Control Unit (MCU) Reference Table .....	19
4.5	Cisco TelePresence Server (TPS) Reference Table .....	19
4.6	Cisco TelePresence ISDN Gateway Reference Table .....	19
5	Cisco Telepresence Management Suite (TMS) SQL Server Database .....	20



5.1	Set up a Service Account for Cisco Telepresence Management Suite (TMS) SQL Server Database .....	20
5.2	Add a TMS and TMS Provisioning Extension Connector .....	21
5.3	Cisco TelePresence Management Suite (TMS) Reference Table .....	22
6	Cisco Unified Communications Manager (CUCM) .....	23
6.1	Enable the AXL API User Role for Cisco Unified Communications Manager (CUCM) .....	23
6.2	Set up a Service Account for CUCM .....	24
6.3	Add CUCM Connectors for the Publisher .....	28
6.4	Cisco Unified Communications Manager (CUCM) Reference Table .....	29
7	Cisco Meeting Server (CMS; formerly Acano Server) .....	31
7.1	Set up a Service Account for Cisco Meeting Server (CMS) .....	31
7.2	Add a CMS Connector .....	32
7.3	Cisco Meeting Server (CMS) Reference Table .....	34
8	Cisco WebEx .....	35
8.1	Set up a Service Account for Cisco WebEx .....	35
8.2	Add a WebEx Connector .....	36
8.3	Cisco WebEx (Cloud only) Reference Table .....	37
9	Pexip Infinity .....	38
9.1	Validate the Service Account for Pexip Infinity .....	38
9.2	Add a Pexip Connector .....	39
9.3	Pexip Infinity Reference Table .....	40
10	Skype for Business (SfB) .....	41
10.1	Set up a Service Account for Skype for Business (SfB) .....	41
10.2	Setup Microsoft Skype for Business Realtime (only required for real-time monitoring) .....	43
10.3	Add a Microsoft Skype for Business Connector .....	45
10.4	Microsoft Skype for Business .....	46
11	Polycom RealPresence Distributed Media Application (DMA) .....	47
11.1	Set up Service Account for Polycom RealPresence Distributed Media Application (DMA) .....	47
11.2	Add a Polycom DMA Connector .....	48



11.3	Polycom RealPresence Distributed Media Application (DMA) Reference Table .....	50
12	Polycom RealPresence Collaboration server (RMX) .....	51
12.1	Set up a Service Account for Polycom RealPresence Collaboration server (RMX) .....	51
12.2	Add a Polycom RMX Connector .....	52
12.3	Polycom RealPresence Collaboration server (RMX) Reference Table .....	53
13	Polycom RealPresence Resource Manager (RPRM).....	54
13.1	Set up a Service Account for Polycom RealPresence Resource Manager (RPRM).....	54
13.2	Add a Polycom RPRM Connector.....	54
13.3	Polycom RealPresence Resource Manager (RPRM) Reference Table.....	56
14	Vidyo Management Portal .....	57
14.1	Enable CDR Access in the Vidyo Management Portal.....	57
14.2	Configure a User Account in the Vidyo Management Portal.....	58
14.3	Verify that API Access is enabled.....	58
14.4	Add a Vidyo Management Portal Connector .....	59
14.5	Vidyo Management Portal Reference Table.....	60
15	Zoom Server .....	61
15.1	Create API Key and API Secret .....	61
15.2	Add a Zoom Connector .....	62
15.3	Zoom Server Reference Table .....	63
16	BlueJeans .....	64
16.1	Create App Key and App Secret .....	64
16.2	Add a BlueJeans Connector .....	65
16.3	BlueJeans Server Reference Table.....	66
17	Saving the configuration and starting the service .....	67
17.1	Troubleshooting a Failed Connection.....	68



## 2 Getting Started - Preparing Your Environment

### 2.1 Overview

Vyopta's Collaboration Performance Management application provides an immersive view into your organization's investment in video & unified communications infrastructure, with insights on utilization, capacity and adoption as well as real-time monitoring capabilities. This guide is designed to help you prepare your environment for the installation. Please follow the subsequent steps in order to complete your installation.

### 2.2 Sign Up for a Vyopta Applications Management Portal User Account

To get started, you will need to create a user account in Vyopta's Applications Management Portal. To log into Vyopta's Applications Management Portal:

1. Open a web browser and navigate to the Vyopta website ([www.vyopta.com](http://www.vyopta.com)).
2. Select login, in the upper right corner of the screen.
3. Select Create an Account and enter your company email address.
4. You will receive an email containing a link to sign up for a Vyopta Applications Management Portal user account. Fill out the form linked in the email to set up your user account.

*Note: your email **must** be tied to the domain of your organization.*

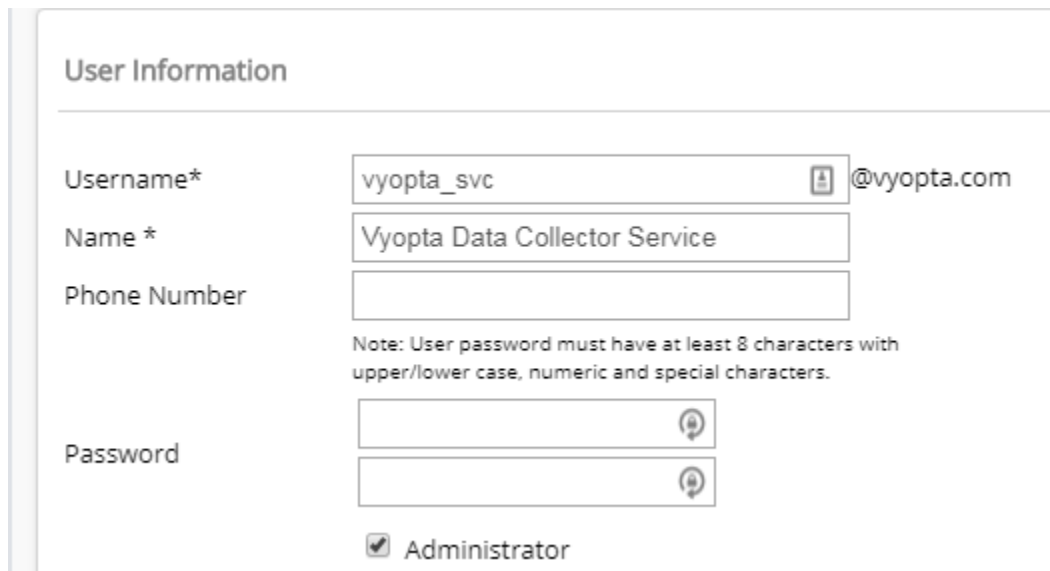
### 2.3 Obtain Administrator Access for your User Account

Your user account must have Administrator privileges for you to complete the remainder of the steps for the deployment. If you are the first account to register for your organization, you will automatically have Administrator privileges. If you only have access to the Profile menu, you do not have Administrator privileges and will need to request Administrator access. To request Administrator access, please contact your organization's current administrators. The list of administrators for your organization can be found on the Organization Profile page.

## 2.4 Configure Service Account

Once you have successfully configured your user account and obtained Administrator privileges, you are ready to provision a service account. The service account is used to manage the Vyopta Data Collector deployed within your environment.

To create the service account, log into the Applications Management Portal and navigate to the Admin > Users Page. Select the icon in the upper-right corner of the screen to add a new user. Fill out the information for the service account (see figure below). Be sure to give the service account administrator privileges which is required.



User Information

Username\*  @vyopta.com

Name \*

Phone Number

Note: User password must have at least 8 characters with upper/lower case, numeric and special characters.

Password

Administrator

Figure 2-1: Vyopta Service Account Setup

The service account does not require an active email address for the username or email address fields but requires your domain to be included in the email address, i.e. `vyopta_svc@<yourdomain>.com`.

When you have entered the information for the service account, click the save button and note the password you assigned so it can be used later.



## 2.5 Prepare a Vyopta Data Collector server instance

A server must be provisioned on which the Vyopta Data Collector will be installed and configured. The Data Collector is used to communicate with your video infrastructure in your internal, and in some cases, external environment. The server can be either a virtual or physical appliance. The server will need network access to your video infrastructure and will always be running.

Please see the table below for the recommended specifications:

<b>CPU</b>	Dual 2.4GHz or Higher
<b>Memory</b>	8GB RAM Recommended
<b>Disk Space</b>	160 GB OS and Data
<b>Network</b>	Single NIC
<b>Operating System</b>	Microsoft Windows Server 2016, or 2012
<b>System Software</b>	.NET Framework Version 4.5 or higher





## 2.6 Test Connection to the Vyopta Cloud

It is important to test the connection to Vyopta's Cloud on the VM or server provisioned for CPM. To test the connection to the Vyopta Cloud, the Administrator must ensure https connectivity to the following Vyopta Cloud Servers: [login.vyopta.com](https://login.vyopta.com), [apps.vyopta.com](https://apps.vyopta.com), [rtadr.vyopta.com](https://rtadr.vyopta.com), [adr.vyopta.com](https://adr.vyopta.com) and [vanalytics.vyopta.com](https://vanalytics.vyopta.com).

Please perform the following tests from Remote Desktop (RDP) on the Vyopta Data Collector Server:

1. Navigate to [login.vyopta.com](https://login.vyopta.com) and confirm that you see an API response.
2. Navigate to [apps.vyopta.com](https://apps.vyopta.com) and confirm that you see the login screen.
3. Navigate to [rtadr.vyopta.com](https://rtadr.vyopta.com) and confirm that you see the login screen.
4. Navigate to [adr.vyopta.com](https://adr.vyopta.com) and confirm that you see the login screen.
5. Finally, navigate to [vanalytics.vyopta.com](https://vanalytics.vyopta.com) and confirm that you see the login screen.

## 2.7 Download and Install the Vyopta Data Collector

To download and install the Vyopta Data Collector, please do the following:

1. Download the Vyopta Data Collector Installer (EXE) from the following URL:  
<http://www.vyopta.com/support/documentation#collector>
2. Once the application has downloaded, open and run the installer as a local administrator on the Data Collector Server provisioned in your environment.
3. Follow the installer's instructions to complete the simple installation process.

## 2.8 Launch the vAnalytics™ Configuration Utility Setup

Once the vAnalytics Configuration Utility is installed, you are almost ready to begin adding your infrastructure to the Data Collector. To complete the setup:

1. Go to Start > All Programs > Vyopta > vAnalytics and open the vAnalytics System Configuration Utility.
2. Once the Vyopta Data Collector application has opened, click on “Get Started” to begin.
3. When ready, click the Proceed button and enter the previously created service account [vyopta\\_svc@<yourdomain>.com](mailto:vyopta_svc@<yourdomain>.com) and your password.
4. Click “Next” to test your connection to the Vyopta Cloud.

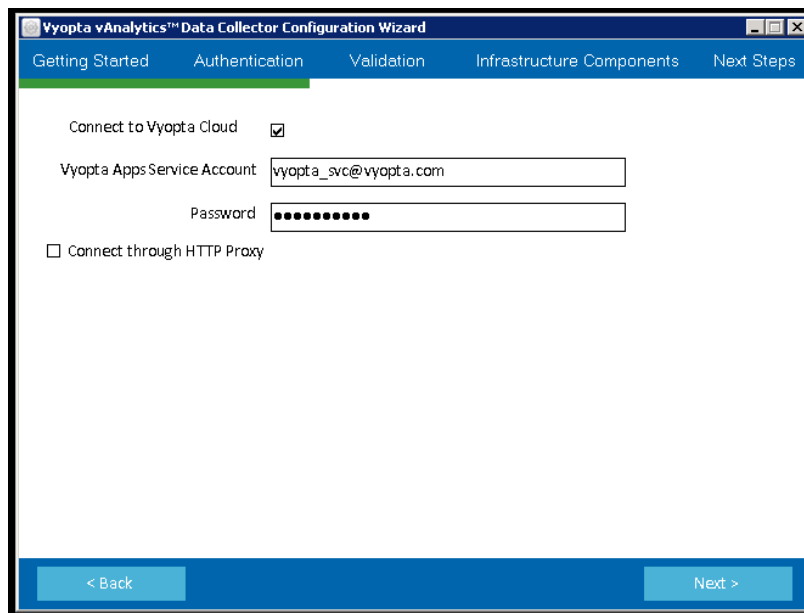


Figure 2-3: Configuration Utility

5. Once the connection is validated click “Next” and the utility will then bring you to the Add Infrastructure page. Click on “Add Infrastructure” to add a component of your video infrastructure.

*Note: If you forget your organization’s service account username or password, you can log into Vyopta’s Applications Management Portal at [apps.vyopta.com](https://apps.vyopta.com) to view the name of the account and/or to change the password.*



## 2.9 Operational Prerequisites

**The following prerequisites must be met to successfully configure and operate the Vyopta Data Collector service for CPM:**

1. Network communication over specific ports between the Vyopta Data Collector and all video infrastructure components within your video environment.
2. Service accounts with the sufficient privileges (typically read-only administrative access) on each component of your video infrastructure.

For a complete list of all network ports and account requirements review the Account and Port Requirement Guide online @ <http://www.vyopta.com/support/documentation#deployment-guides>

The remainder of this guide is devoted to taking you through the steps necessary to configure each of the supported video infrastructure components, detailed in Section 2.10 – Coverage and Compatibility.

## 2.10 Coverage and Compatibility

**The following video infrastructure components are compatible with CPM:**

- Cisco Expressway formerly Video Communications Server (VCS) Control and Expressway
- Cisco Multipoint Control Unit (MCU)
- Cisco ISDN Gateway (ISDN)
- Cisco Telepresence Server (TPS)
- Cisco Telepresence Management Suite & Provisioning Extension (TMS & TMSPE)
- Cisco Unified Communications Manager (CUCM)
- Cisco WebEx
- Cisco Meeting Server (CMS; formerly Acano Server)
- Microsoft Skype for Business (SfB)
- Pexip Management Node
- Polycom DMA with API License
- Polycom RMX
- Polycom RPRM with API License
- Vidyo Management Portal
- Zoom
- BlueJeans

### 3 Cisco Expressway-E/C (formerly VCS Control & VCS Expressway)

#### 3.1 Set up a Service Account for Cisco Expressway-E/C or VCS

To create a service account on the device, perform the following:

1. Log into the device with the proper administrator account.
2. Navigate to the Users > Administrator Accounts tab.

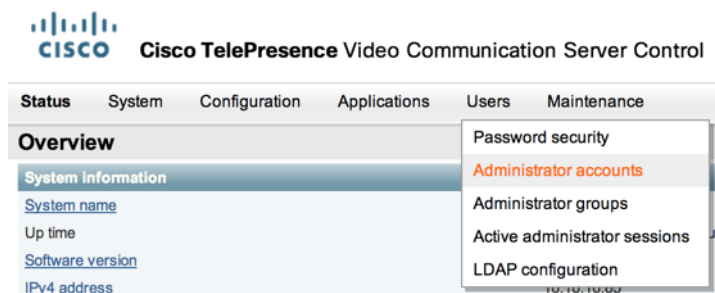


Figure 3-1: Administrator Accounts Tab

3. Select New.
4. Enter the following name for the service account: `vyopta_svc`
5. Set the Access level to *Read-only*.
6. Enter the service account password and confirm this password.
7. Set Web Access and API Access to *Yes* and State to *Enabled*.
8. Click Save.

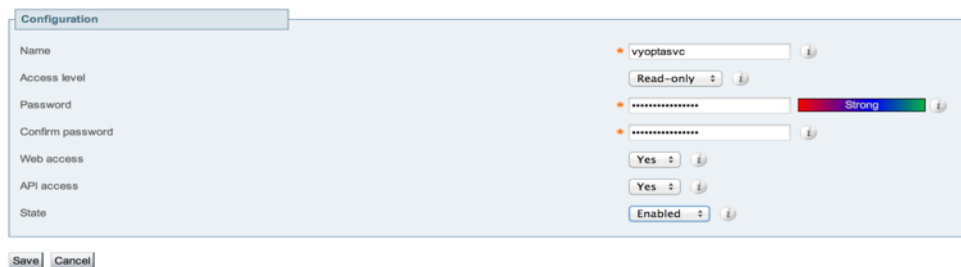


Figure 3-2: New Service Account

The Vyopta Service account is now added to the device. The service account must be added to each VCS Control and Expressway within the video environment.

*Note: VCS Active Directory (AD) accounts are not supported. The account must be a local administrator.*



### 3.2 Add Expressway-E/C or VCS

To add a Cisco Expressway-E/C or VCS requires the following:

- Access to the FQDN/IP address of the video device from the Vyopta Data Collector
- Previously created user service account credentials on each video device

*Note: If you have multiple VCS-C or VCS-E devices you must add a connector for each individual device including all peers and slaves.*

Please follow the instructions below to add each video infrastructure device:

1. Select the correct VCS type in the Infrastructure Type drop-down menu.
2. Enter the infrastructure name. This will be the name displayed for the video device in the Configuration Utility and within Vyopta's Applications Management Portal.

*Note: We recommend using hostname rather than IP as IP addresses are subject to change. It is also helpful to name the infrastructure in a 'friendly' or easily understood way.*

1. Enter the description of the video device. This can include the device type, location, and other unique identifiers.
2. Enter the infrastructure hostname or IP address.
3. Enter the username and password created on the video device.
4. Click Validate to ensure that the data collector application can connect to the video device.
5. If the connection to the video component succeeded, click the Save button.

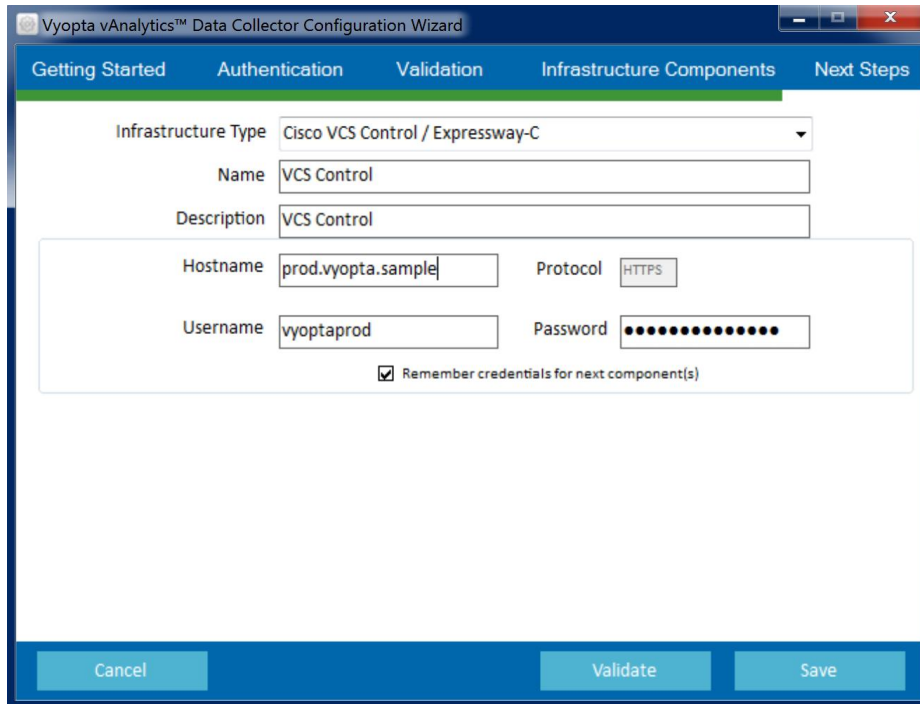


Figure 3-3: VCS Configuration Example

*Note: In a clustered VCS environment, please only add the primary/secondary devices. Please do not add the clustered, named environment.*

### 3.3 Cisco Video Communications Server Control (VCS-C) & Expressway (VCS-E) Reference

#### Table

Cisco Expressway- E/C or Video Communications Server (VCS)	
Version	Expressway x8.5 or above / VCS version x7.2 or above
Device Access	Server IP/FQDN ; Add all VCS cluster devices if applicable.
User/Service Account	Local Administrator read-only account with API access. <i>Note: AD integrated accounts are not supported.</i>
TCP Ports	Vyopta Data Collector outbound to the Expressway / VCS device(s) TCP 443 (https)

## 4 Cisco Telepresence Multipoint Control Unit (MCU), Telepresence Server (TPS), or Telepresence Integrated Services Digital Network (ISDN) Gateway

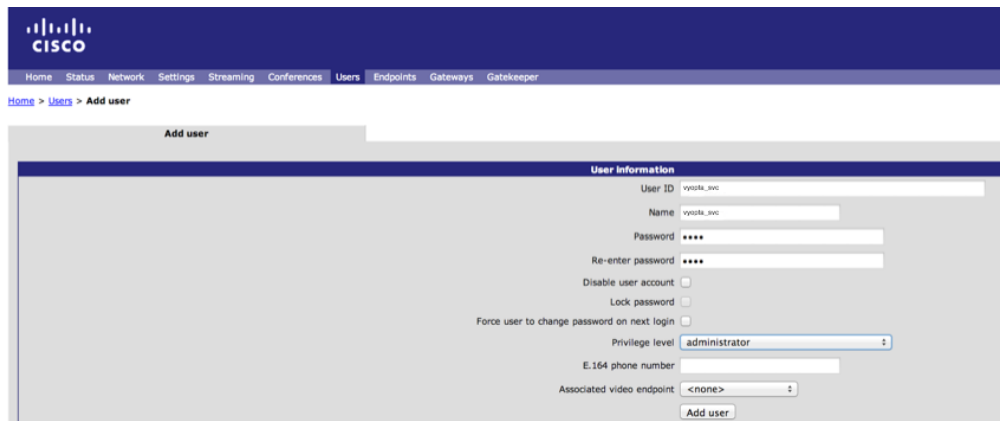
### 4.1 Set up a Service Account for Cisco Multipoint Control Unit (MCU), Telepresence Server (TPS), or Integrated Services Digital Network (ISDN) Gateway

The instructions below are separated by device type. Please follow the relevant instructions to create a service account on the component being added:

*Note: MCU supervisor blades and slave blades in an MCU cluster do not need to be added.*

For Cisco Multipoint Control Units (Codian MCUs) or ISDN Gateways:

1. Log into the infrastructure with any Administrator account.
2. Click on the User tab.
3. Select Add New User.
4. Enter the User ID as `vyopta_svc` and Account Name as `vyopta_svc`
5. Enter and Re-enter the password.
6. Uncheck the box for Force user to change password on next login.
7. Set the Privilege level to *administrator*.
8. Leave the E.164 phone number blank.
9. When finished, add the User.



The screenshot shows the Cisco Telepresence User Management interface. The breadcrumb navigation is [Home](#) > [Users](#) > [Add user](#). The form is titled "Add user" and contains the following fields and options:

- User information**
  - User ID:
  - Name:
  - Password:
  - Re-enter password:
  - Disable user account:
  - Lock password:
  - Force user to change password on next login:
  - Privilege level:
  - E.164 phone number:
  - Associated video endpoint:
- 

Figure 4-1: Add MCU User Service Account

For Cisco TelePresence Servers (TPS) perform the following:

1. Log into the infrastructure with any Administrator account.
2. Click on the User tab.
3. Select Add New User.
4. Enter in the User ID as `vyopta_svc` and Account Name as `vyopta_svc`.
5. Enter and re-enter the password.
6. Set the privilege level to *API access*.
7. When finished, select Add User.



Figure 4-2: Add TPS User Service Account

*Note: Please ensure that **http is enabled** for your TP Server. If it is not enabled, call quality will not be reported for TP Server in Real Time/Historical.*

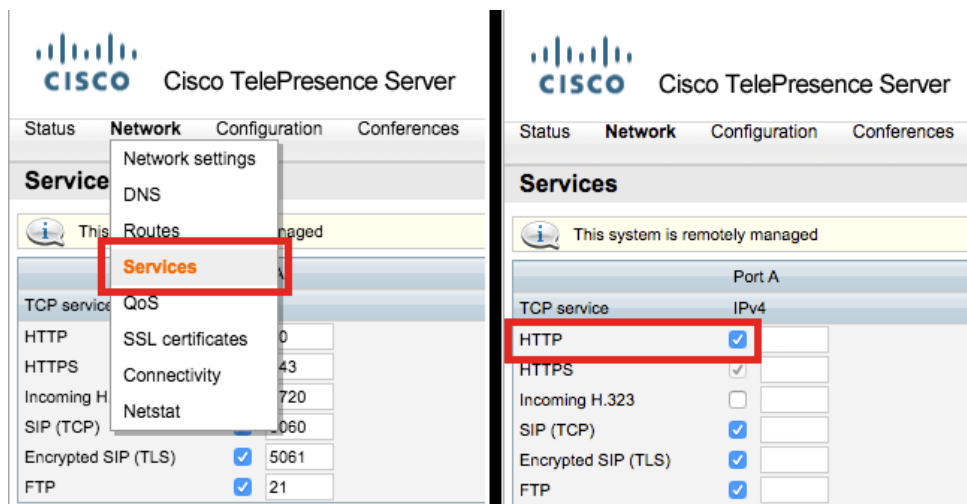


Figure 4-3: HTTP can be enabled within your TP Server under Network → Services → HTTP



## 4.2 Enable CDR Permanent Storage on Cisco Codian (MCU) & ISDN Gateway

In order to maximize the number of call detail records stored on the MCU and ISDN Gateway you must enable CDR permanent storage by performing the following:

1. Log into the device with an administrator account.
2. Navigate to Logs -> CDR logs.
3. Click on the Enable CDR permanent storage button.

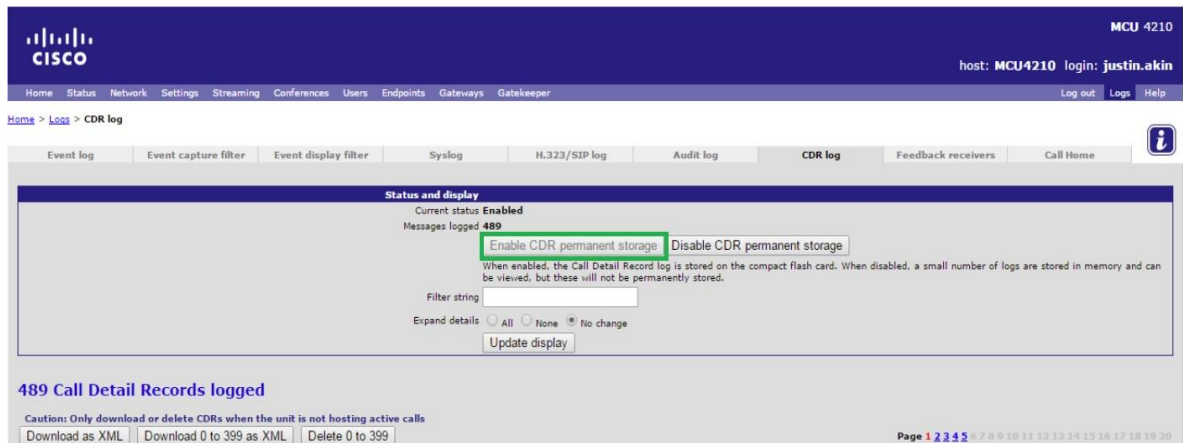


Figure 4-4: Click to enable CDR permanent storage

## 4.3 Add MCU, TP Server, or ISDN Gateway

To add a Cisco MCU, Telepresence Server, or ISDN Gateway requires the following:

- Access to the FQDN/ IP address of the video device from the Vyopta Data Collector
- Previously created user service account credentials on each video device

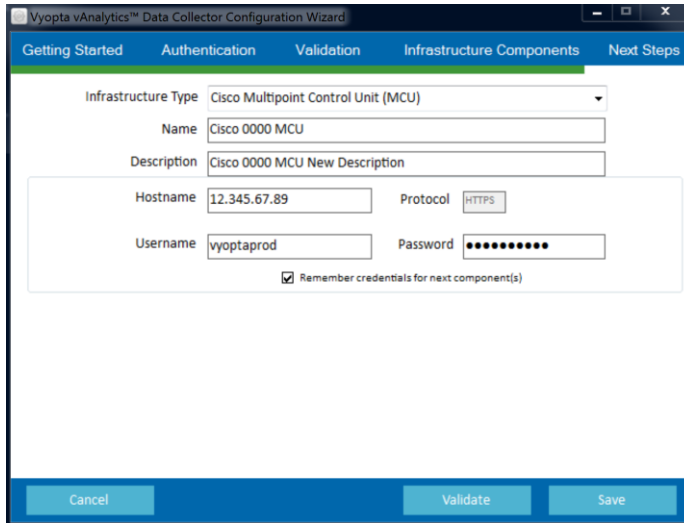
*Note: If you have multiple MCUs, TPS peers, or clusters you must add a connector for each individual device or blade. Do not add slave MCUs as all information is obtained from the Master MCU.*

Please follow the instructions below to add each video infrastructure device:

1. Select the correct device type in the Infrastructure Type drop-down menu.
2. Enter the infrastructure name. This will be the name displayed for the video device in the Configuration Utility and within Vyopta's Applications Management Portal.

*Note: We recommend using hostname rather than IP as IP addresses are subject to change. It is also helpful to name the infrastructure in a 'friendly' or easily understood way.*

3. Enter the description of the video device. This can include the device type, location, and other unique identifiers.
4. Enter the infrastructure hostname or IP address.
5. Enter the username and password created on the video device.
6. Click Validate to ensure that the Vyopta Data Collector application can connect to the video device.
7. If the connection to the video component succeeded, click the Save button.



The screenshot shows the 'Infrastructure Components' step of the 'Vyopta vAnalytics Data Collector Configuration Wizard'. The form contains the following fields and values:

- Infrastructure Type: Cisco Multipoint Control Unit (MCU)
- Name: Cisco 0000 MCU
- Description: Cisco 0000 MCU New Description
- Hostname: 12.345.67.89
- Protocol: HTTPS
- Username: vyoptaprod
- Password: [masked]
- Remember credentials for next component(s)

Buttons at the bottom: Cancel, Validate, Save.

Figure 4-5: MCU Configuration Example



#### 4.4 Cisco TelePresence Multipoint Control Unit (MCU) Reference Table

Cisco TelePresence MCU	
Version	MCU version 4.1 or above
Device Access	Server IP/FQDN
User/Service Account	Local account with Administrator privileges
TCP Ports	Vyopta Data Collector outbound to the MCU device(s) TCP 443 (https)  If MCU is in a cluster only the Master needs to be added

#### 4.5 Cisco TelePresence Server (TPS) Reference Table

Cisco TelePresence Server (TPS)	
Version	TPS 3.1 or above
Device Access	Server IP/FQDN
User/Service Account	Local account with API Access (or Administrator privileges)
TCP Ports	Vyopta Data Collector outbound to the TPS device(s) TCP 443 (https)  TPS device(s) outbound to the Vyopta Data Collector TCP 22280

#### 4.6 Cisco TelePresence ISDN Gateway Reference Table

Cisco TelePresence ISDN Gateway	
Version	Version 2.1 or above
Device Access	Server IP/FQDN
User/Service Account	Local account with Administrator privileges
TCP Ports	Vyopta Data Collector outbound to the ISDN device(s) TCP 443 (https)



## 5 Cisco Telepresence Management Suite (TMS) SQL Server Database

### 5.1 Set up a Service Account for Cisco Telepresence Management Suite (TMS) SQL Server Database

The service account required will be added to the appliance's SQL Database with read-only privileges. You must determine where the appliance's SQL Server Database is located in your environment; whether it is on the TMS appliance or located on a separate SQL server. Once this has been identified, you will require an Administrator account to the server to add the required service account. This may require the assistance of a SQL Server Administrator in your organization to provide server access or to add the account manually.

For all instances where the TMS/TMSPE SQL databases are hosted on a separate SQL Server please consult with your organization's SQL Server DBA to create the required database read-only account.

***There are two ways to identify where your TMS & TMSPE databases are located:***

1. RDP to the TMS server as an administrator and run the '**TMS Tools**' application configuration utility from Start > Programs > Cisco TelePresence Management Suite. **Please note that this is the recommended option as it highlights the connection port.**
2. Log in to the TMS Web UI as an administrator and navigate to Administrative Tools > TMS Server Maintenance. Click on 'Database Files and Size Info' to view the database server in use. If the database server is '(local)\SQLTMS' then your database resides on the actual TMS server. Your database could also use the name of the actual server, e.g. 'TMSPROD\SQLTMS'. If the server name matches your TMS server then your database resides on the TMS server.

The read-only database account should be titled `vyopta_svc` which has the 'db\_datareader' and 'public' roles as well as access to the 'tmsng' and 'tmspe' databases. For SQL databases residing on the TMS server (atypical), please contact [support@vyopta.com](mailto:support@vyopta.com) for assistance with the TMS Preparation Installer.

*Note: You will need to make sure that you obtain the assigned password and also the appropriate TCP/IP port for database access. The default for this is 1433 but other ports can be configured.*



## 5.2 Add a TMS and TMS Provisioning Extension Connector

To add a connector for Telepresence Management Suite (TMS) and/or Telepresence Management Suite Provisioning Extension (TMSPE) you will need to prepare by completing the following prerequisites:

- Confirm access to the FQDN/IP address of the server hosting the SQL Database from the Vyopta Data Collector.
- Obtain credentials for the Microsoft SQL Server Database Read-only Account.
- Identify whether a static or dynamic SQL port is used. (If dynamic, please identify and record the dynamic port value within Microsoft SQL Configuration Manager.)
- Verify that TCP/IP is enabled for the SQL Server within SQL Configuration Manager.

Please follow the instructions below to add TMS and repeat for TMSPE:

1. Select the correct TMS product type in the Infrastructure Type drop-down menu.
2. Enter the infrastructure name and description of TMS. This will be the name displayed for the video device in CPM. This can include the device type, location, and other unique identifiers.

*Note: We recommend using hostname rather than IP as IP addresses are subject to change. It is also helpful to name the infrastructure in a 'friendly' or easily understood way.*

3. Enter the SQL Server hostname or IP address. If the SQL Server Instance Name is not the default name MSSQLSERVER, you will have to add the SQL Server Instance Name as a suffix to the Hostname or IP address as per below or specify the instance name in the field below.

<Device Hostname>\<SQL Server Instance Name>

4. Enter the username and password created on the SQL Server.
5. Leave the Port Number and Database Name blank, it will use the default port numbers. If you have verified that the default port or database is not used, enter in the custom port number or database name.
6. Click Validate to ensure connectivity to the video device.
7. If the connection to the video component succeeded, click the Save button.

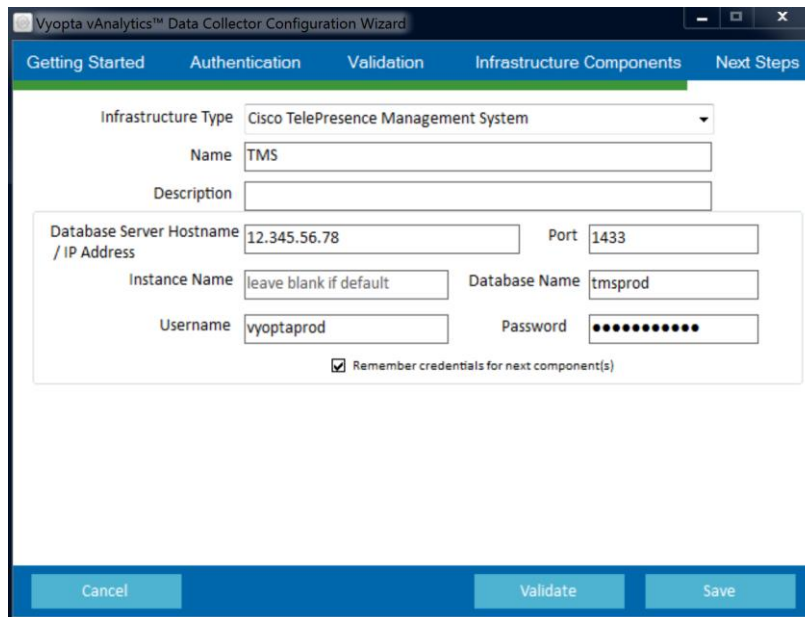


Figure 5-1: TMS Configuration Example

*Note: You must repeat the procedure above to add the TMSPE database.*

### 5.3 Cisco TelePresence Management Suite (TMS) Reference Table

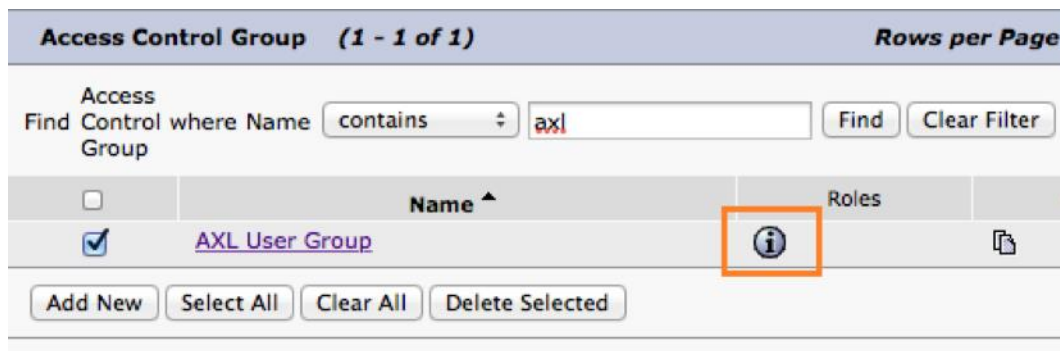
Cisco TelePresence Management Suite (TMS)	
Version	TMS version 13.2 or above
Device Access	Server IP/FQDN that hosts the SQL 'tmsng' and 'tmspe' databases  While the TMS application server can host the SQL database this is typically not implemented in an enterprise environment. Please consult with your organization's DBA for more information.
User/Service Account	Local DBA read-only user account that has access to the 'tmsng' and 'tmspe' databases
TCP Ports	Vyopta Data Collector outbound to the SQL databases TCP 1433  Note: Your SQL DBA may have set a separate TCP port other than the default. Please consult with your organization's DBA for more information.

## 6 Cisco Unified Communications Manager (CUCM)

### 6.1 Enable the AXL API User Role for Cisco Unified Communications Manager (CUCM)

The Vyopta Data Collector leverages the AXL API for gaining access to CUCM registered endpoints. The AXL API User role is not enabled by default. The following steps will guide you in creating this required user role:

1. Log into the Cisco UCM with an Administrator Account.
2. Navigate to the Cisco Unified CM Administration tab.
3. Go to User Management > User Settings > Role and search for AXL User Group.
4. If the role already exists, then proceed to the next section, otherwise click Add New.
5. Under Application, select *Cisco Call Manager AXL Database*, and click Next.
6. Enter *Standard AXL API Access* as the name and *Allow AXL APIs* as the description.
7. Check the Allow to use API check box and click Save.
8. Go to User Management > User Settings > Access Control Group and select Add New.
9. Name the group *AXL User Group* and click Save.
10. Return to the Access Control Group page and search for *AXL User Group* once again.
11. Find the AXL User Group from the List, and select the 'i' button as shown below:



**Figure 6-1: Add Role to AXL User Group**

12. Select Assign Role to Group and find the *Standard AXL API Access* role.
13. Select the role, click the "Add Selected" button, and click the save button. The role will now be listed in this User Group.

## 6.2 Set up a Service Account for CUCM

Next, you will create an application user service account on your Call Manager publisher:

1. Log into the CUCM publisher with the Administrator account.
2. Go to User Management > Application User > Add User.
3. Enter `vyopta_svc` for the Username.
4. Set a password for the account.
5. Assign the following groups to the user account:
  - AXL User Group
  - Standard CCM Read-Only
  - Standard CCM Server Monitoring
  - Standard CTI Enabled
  - Standard CTI Allow Control of Phones supporting Connected Xfer and conf
6. Endpoints that you will be monitoring in real time should be moved from the 'Available Devices' to the 'Controlled Devices' list under the Device Information section. You can use the 'Device Association' or 'Find more phones' button to better navigate the endpoints in your CUCM environment.

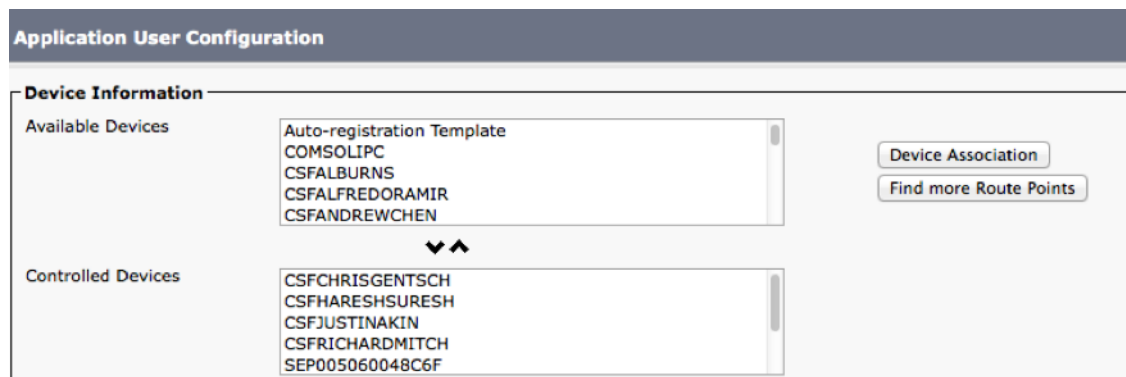


Figure 6-2: CUCM Application User Configuration

7. Save the user account.



8. Once you have added the account, ensure that the following services are enabled by navigating to Cisco Unified Serviceability > Tools > Service Activation on each CUCM Publisher:

- **Cisco Call Manager** (note: If CallManager service is not activated then you will be unable to verify and enable the data collector service for CUCM. Please contact [support@vyopta.com](mailto:support@vyopta.com).)
- **Cisco CTI Manager**
- **Cisco SOAP – CDRonDemand Service**
- **Cisco CAR Web Service**
- **Cisco AXL Web Service**

CM Services		
	Service Name	Activation Status
<input checked="" type="checkbox"/>	Cisco CallManager	Activated
<input type="checkbox"/>	Cisco Messaging Interface	Deactivated
<input type="checkbox"/>	Cisco Unified Mobile Voice Access Service	Deactivated
<input type="checkbox"/>	Cisco IP Voice Media Streaming App	Deactivated
<input checked="" type="checkbox"/>	Cisco CTIManager	Activated
<input type="checkbox"/>	Cisco Extension Mobility	Deactivated
<input type="checkbox"/>	Cisco Extended Functions	Deactivated
<input type="checkbox"/>	Cisco DHCP Monitor Service	Deactivated
<input type="checkbox"/>	Cisco Intercluster Lookup Service	Deactivated
<input type="checkbox"/>	Cisco Location Bandwidth Manager	Activated
<input type="checkbox"/>	Cisco Dialed Number Analyzer Server	Deactivated
<input type="checkbox"/>	Cisco Dialed Number Analyzer	Deactivated
<input type="checkbox"/>	Cisco Tftp	Activated

CTI Services		
	Service Name	Activation Status
<input type="checkbox"/>	Cisco IP Manager Assistant	Deactivated
<input type="checkbox"/>	Cisco WebDialer Web Service	Deactivated

CDR Services		
	Service Name	Activation Status
<input checked="" type="checkbox"/>	Cisco SOAP - CDRonDemand Service	Activated
<input checked="" type="checkbox"/>	Cisco CAR Web Service	Activated

Database and Admin Services		
	Service Name	Activation Status
<input type="checkbox"/>	Cisco Bulk Provisioning Service	Deactivated
<input checked="" type="checkbox"/>	Cisco AXL Web Service	Activated
<input type="checkbox"/>	Cisco UXL Web Service	Deactivated
<input type="checkbox"/>	Cisco TAPS Service	Deactivated

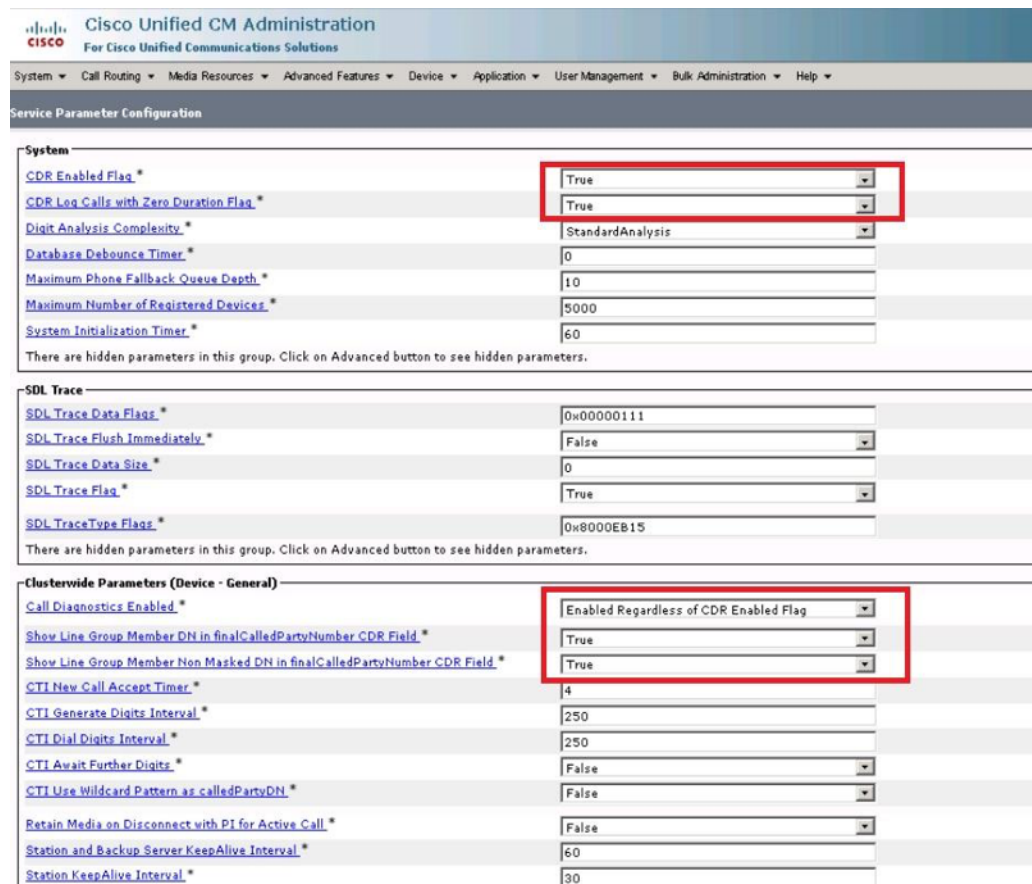
Performance and Monitoring Services		
	Service Name	Activation Status
<input type="checkbox"/>	Cisco Serviceability Reporter	Deactivated
<input type="checkbox"/>	Cisco CallManager SNMP Service	Deactivated

Figure 6-3: CUCM Unified Serviceability Service Activation

9. Make sure parameters are correctly enabled under Cisco Unified CM Administration for Active Publishers:
  - a. Navigate to Cisco Unified CM Administration -> System -> Service Parameters.
  - b. Select Active Publishing Server(s).
  - c. Select the Cisco Call Manager Service.
  - d. Under System section set CDR Enabled Flag and CDR Log Calls with Zero Duration Flag to *True*.

*Note: The CDR Enabled Flag and CDR Log Calls with Zero Duration Flag **must** be set to True on **every Publisher and Subscriber** – Subscribers do not inherit these values from Publishers, and these values are not set by default. If not set correctly, CDRs will not be transmitted and data loss is likely.*

- e. Under Cluster Wide parameters (Device - General) set Call Diagnostic Enabled to *Enabled Regardless of CDR Enabled Flag* and the two Show Line Group Member parameters to *True*.



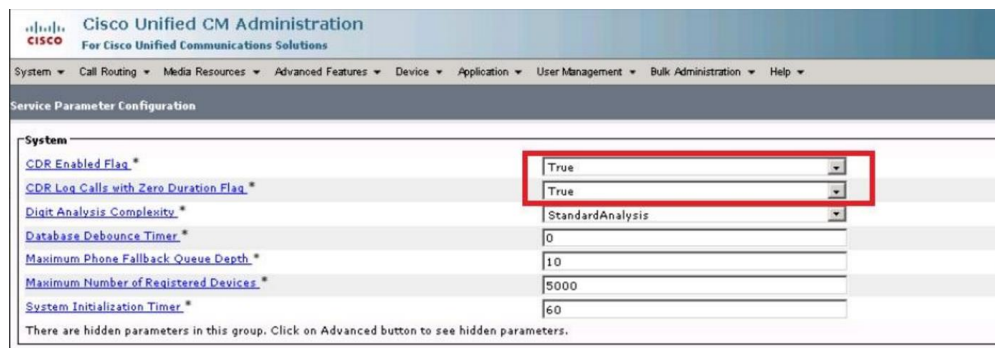
Cisco Unified CM Administration	
For Cisco Unified Communications Solutions	
System > Call Routing > Media Resources > Advanced Features > Device > Application > User Management > Bulk Administration > Help	
Service Parameter Configuration	
<b>System</b>	
CDR Enabled Flag *	True
CDR Log Calls with Zero Duration Flag *	True
Digit Analysis Complexity *	StandardAnalysis
Database Debounce Timer *	0
Maximum Phone Fallback Queue Depth *	10
Maximum Number of Registered Devices *	5000
System Initialization Timer *	60
There are hidden parameters in this group. Click on Advanced button to see hidden parameters.	
<b>SDL Trace</b>	
SDL Trace Data Flags *	0x00000111
SDL Trace Flush Immediately *	False
SDL Trace Data Size *	0
SDL Trace Flag *	True
SDL TraceType Flags *	0x8000EB15
There are hidden parameters in this group. Click on Advanced button to see hidden parameters.	
<b>Clusterwide Parameters (Device - General)</b>	
Call Diagnostics Enabled *	Enabled Regardless of CDR Enabled Flag
Show Line Group Member DN in finalCalledPartyNumber CDR Field *	True
Show Line Group Member Non Masked DN in finalCalledPartyNumber CDR Field *	True
CTI New Call Accept Timer *	4
CTI Generate Digits Interval *	250
CTI Dial Digits Interval *	250
CTI Await Further Digits *	False
CTI Use Wildcard Pattern as calledPartyDN *	False
Retain Media on Disconnect with PI for Active Call *	False
Station and Backup Server KeepAlive Interval *	60
Station KeepAlive Interval *	30

Figure 6-4: Cisco Unified CM Administration Service Parameters

10. Make sure the following parameters are enabled under Cisco Unified CM Administration for Subscribers (if applicable)

- a. Navigate to Cisco Unified CM Administration -> System -> Service Parameters.
- b. Select Subscribers.
- c. Select the Cisco Call Manager Service
- d. Under System section set CDR Enabled Flag and CDR Log Calls with Zero Duration Flag to True.

*Note: The CDR Enabled Flag and CDR Log Calls with Zero Duration Flag **must** be set to True on every Publisher and Subscriber – Subscribers do not inherit these values from Publishers, and these values are not set by default. If not set correctly, CDRs will not be transmitted and data loss is likely.*



**Figure 6-5:** Cisco Unified CM Administration Service Parameters for Subscribers

11. For large Call Manager deployments (i.e., More than 5 nodes or with multiple clusters) it is recommended to adjust the following parameters under Cisco Unified CM Administration > System > Enterprise Parameters from their default values in order to facilitate timely CDR collection:

- a. CDR File Time Interval: By increasing this value from the default of 1 minute to 5 minutes, the number of CDR files will be reduced by a factor of 5 with no impact on CUCM performance. Please ensure that any other CDR reporting / billing solutions will not be adversely affected by changing this parameter.
- b. Allowed CDRonDemand get\_file Queries per Minute: For larger Call Manager deployments (greater than 20 total nodes) it is recommended to increase this value from the default value of 10 to 20, which will assist in CDR collection with no impact on CUCM performance.



### 6.3 Add CUCM Connectors for the Publisher

To add a CUCM Connector requires the following:

- Access to the FQDN/ IP address of the video device from the Vyopta Data Collector
- Previously created user service account credentials on each video device

*Note: **Only Publishers should be added.** (No Subscribers should be added.) If Publisher fails to verify and cannot be enabled, please contact [support@vyopta.com](mailto:support@vyopta.com).*

Please follow the instructions below to add each CUCM Publisher:

1. Select Cisco Unified Communications Manager (CUCM) from the Infrastructure Type menu.
2. Enter the infrastructure name. This will be the name displayed for the video device in the Configuration Utility and within Vyopta's Applications Management Portal.

*Note: We recommend using hostname rather than IP as IP addresses are subject to change. It is also helpful to name the infrastructure in a 'friendly' or easily understood way.*

3. Enter the description. This can include the device type, location, and other unique identifiers. In the description always add Publisher or Subscriber for Vyopta Support purposes, for example 'CUCM01' – Pub, etc.
4. Enter the infrastructure hostname or IP address.
5. Enter the username and password created on the video device.
6. Click Validate to ensure that the Vyopta Data Collector application can connect to the video device.
7. If the connection to the video component succeeded, click the Save button.

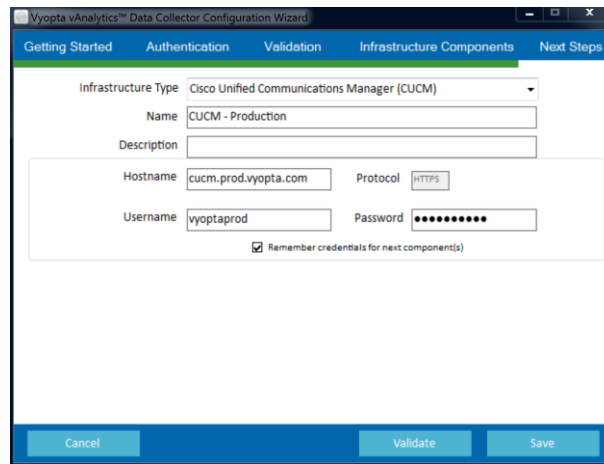


Figure 6-6: CUCM Configuration Example

#### 6.4 Cisco Unified Communications Manager (CUCM) Reference Table

Cisco Unified Communications Manager (CUCM)	
Version	CUCM version 10.0 or above
Device Access	Call Manager Publisher(s) IP/FQDN; Subscribers not required.
User/Service Account	CUCM Application User with AXL User Group, Standard CCM Read-only, Standard CCM Server Monitoring, Standard CTI Enabled, and Standard CTI Allow Control of Phones supporting Connected Xfer and conf
TCP Ports	<p>Vyopta Data Collector to CUCM TCP 443, 8443, 2748, 2749, 2789</p> <p>CUCM to Vyopta Data Collector Passive FTP (21) or SFTP*</p> <p>*FTP requires that passive FTP be open and allowed from CUCM to the Vyopta Data Collector. If SFTP is selected then only port 22 must be open. SFTP requires using a third party SFTP client on the Vyopta Data Collector.</p>



Call Manager Service Requirements	Cisco Call Manager CISCO CTI Manager Cisco SOAP – CDRonDemand Service CISCO CAR Web Service Cisco AXL Web Service
Call Manager Service Parameters	'CDR Enabled Flag' and 'CDR Log Calls with Zero duration' to True  'Call Diagnostic Enabled' to Enabled Regardless and 'Show Line Group Member' parameters to true



## 7 Cisco Meeting Server (CMS; formerly Acano Server)

### 7.1 Set up a Service Account for Cisco Meeting Server (CMS)

To utilize CMS meeting and user reporting APIs, a service account with read-only administrator access must be created:

1. SSH into the CMS box using any convenient command line utility.
2. Login with the Administrator account (e.g. [admin@10.10.10.200](mailto:admin@10.10.10.200)).
3. Enter the following command: `user add vyopta_svc api`
4. Type in the `vyopta_svc` user account password.

*Note: By default, CMS provisions new account passwords with a 180-day duration, meaning that you will need to update the password on the service account twice yearly. If your corporate service account policies permit, you may want to extend this default duration **before** adding the `vyopta_svc` account.*

*To change the default user account password duration, after logging into the CMS command line interface with your administrator account, **but before adding the `vyopta_svc` account**, enter the following command:*

```
user rule password_age NNNN
```

*where NNNN is the number of days before a password expires. So to set the default expiration to yearly, enter:*

```
user rule password_age 1825
```

*If you have already added the Vyopta service account but want to extend its expiration duration, you still enter the above command, followed by:*

```
passwd vyopta_svc
```

*You'll then be prompted to confirm your administrator password to allow you to do this, then simply reenter the existing password on the `vyopta_svc` account. It does not need to be refreshed -- and if you do change it, you will need to update it on the Vyopta apps management portal.*

5. To verify that the API role is set (and the password expiration, if changed), enter the following command: `user list`
6. Close the SSH session.

```

acano> user add vyoptasvc api
Please enter new password:
Please enter new password again:
Success
acano> user list
  USERNAME      ROLE      PASSWORD EXPIRY      LOGGED IN
  -----      -
  admin         admin     2015-Oct-01          yes
  vyoptasvc     api       2016-Mar-29          no
acano>

```

**Figure 7-1: CMS User Account Information**

## 7.2 Add a CMS Connector

To add a CMS Connector requires the following:

- Access to your organization’s CMS Webpage from the Vyopta Data Collector
- Credentials for the CMS read-only API service account established in the previous step (*Section 7.1, Set up a Service Account for Cisco Meeting Server (CMS)*)

Please follow the instructions below to add the CMS instance:

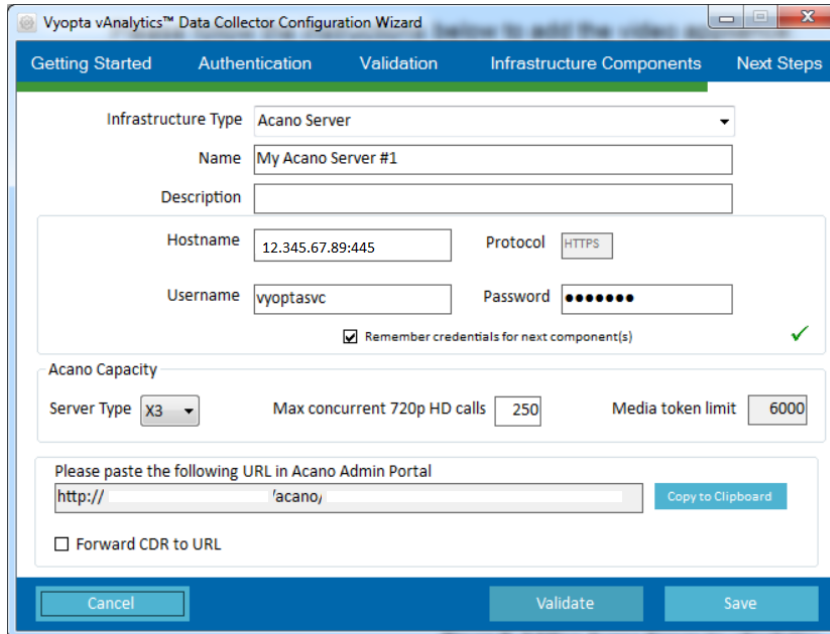
1. Select either *Cisco Meeting Server (CMS)* or *Acano Server*, depending upon your version of the Vyopta Data Collector, in the Infrastructure Type drop-down menu. (Only one of those two choices will be available.)
2. Enter the server name.
3. Enter the CMS URL into the Hostname.

*Note: Please include any non-standard port number in the URL. For example: 10.200.30.24:445 (where 445 is the port number).*

4. Enter an optional description of the video device in the Description field.
5. Enter the username and password of the service account established in the prior section.
6. Select Server Type (X2, X3 or VM). If VM, enter the number of ports for which your CMS is licensed in the ‘Max concurrent 720p calls’ field.



*Note: If you are on a fractionally licensed X2 / X3 then please add as a VM instead and specify your max concurrent HD calls.*



**Figure 7-2: Adding CMS**

7. Click Validate to ensure that the Vyopta Data Collector can connect to your CMS.
8. If the connection to the video component succeeded, click the 'Copy to Clipboard' button in order to capture the CDR URL which needs to be entered in CMS and then click the Save button.
9. Login to the CMS configuration portal using administrator credentials.
10. Navigate to Configuration > CDR Settings tab
  - a. If the Receiver URI 1 field is blank then paste the URL that you copied in step 8 into the 'URI 1' field. Otherwise paste the value into the 'URI 2' field.
  - b. Click Submit.
11. For Acano versions prior to 1.8 or for deployments which require more than 2 CDR streams, please contact [support@vyopta.com](mailto:support@vyopta.com)

*Note: Port 22280 is the default port over which the Vyopta Data Collector will listen for inbound CMS CDR data. **If this port is not open in your network environment then please reach out to [support@vyopta.com](mailto:support@vyopta.com) for further assistance.***



### 7.3 Cisco Meeting Server (CMS) Reference Table

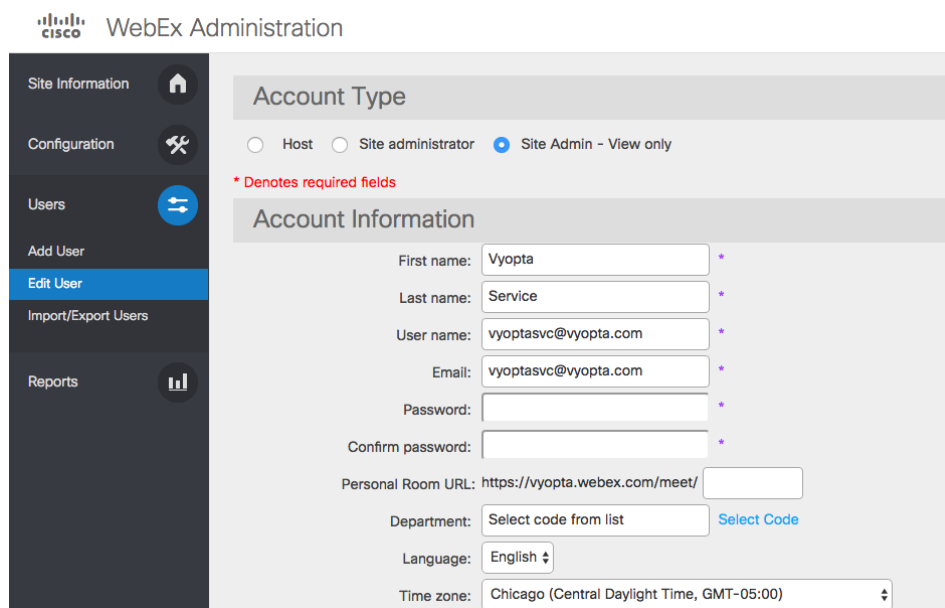
CMS	
Version	Acano 1.7 or above, CMS 2.0.0 or above
Device Access	Server IP/FQDN of CMS device(s)
User/Service Account	Local account with read-only API access enabled.
TCP Ports	<p>Vyopta Data Collector to CMS TCP 443*</p> <p>CMS CDR forward push to Vyopta Data Collector TCP 22280</p> <p>Note: the management port can be set to a separate port such as TCP 445 so please confirm the correct port with your CMS administrator.</p>

## 8 Cisco WebEx

### 8.1 Set up a Service Account for Cisco WebEx

To create a service account for Cisco WebEx, perform the following:

1. Log into the WebEx Web Portal using an existing site administrator account.
2. Select Site Administrator tab to open the Administration page.
3. Use the appropriate tab under Manage Users to create a new WebEx account:
  - a. Select the *Site Admin – View only* privilege.
  - b. Enter *Vyopta* for the First name.
  - c. Enter *Service* for the Last name.
  - d. Enter *vyoptasvc* for the User name.
  - e. Enter [vyoptasvc@vyopta.com](mailto:vyoptasvc@vyopta.com) for the Email address.
  - f. Set and confirm the password for the service account.
4. Select Update to save the service account information.



The screenshot shows the Cisco WebEx Administration interface. The left sidebar contains navigation options: Site Information, Configuration, Users, Add User, Edit User (highlighted), Import/Export Users, and Reports. The main content area is titled 'WebEx Administration' and shows the 'Account Type' section with radio buttons for 'Host', 'Site administrator', and 'Site Admin - View only' (selected). Below this is the 'Account Information' section with the following fields:

- First name: Vyopta \*
- Last name: Service \*
- User name: vyoptasvc@vyopta.com \*
- Email: vyoptasvc@vyopta.com \*
- Password: \*
- Confirm password: \*
- Personal Room URL: https://vyopta.webex.com/meet/ [ ]
- Department: Select code from list [Select Code]
- Language: English [v]
- Time zone: Chicago (Central Daylight Time, GMT-05:00) [v]

\* Denotes required fields

Figure 8-1: WebEx User Account Information

## 8.2 Add a WebEx Connector

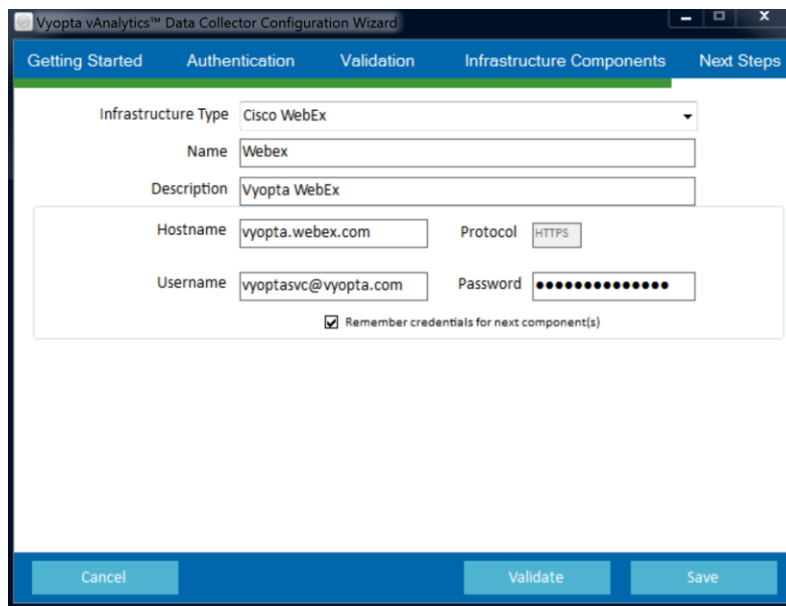
**Note:** If you have a next-gen Webex Site integrated with Cisco Control Hub and use Common Identity please reach out to [support@vyopta.com](mailto:support@vyopta.com) for getting started information.

To add a WebEx Connector requires the following:

- Access to your organization's WebEx Site URL from the Vyopta Data Collector
- Credentials for the WebEx Site Admin - View only account

Please follow the instructions below to add your WebEx site:

1. Select *Cisco WebEx* in the Infrastructure Type drop-down menu.
2. Enter the WebEx site name.
3. Enter *WebEx* into the Description field; you may also add the WebEx type, location, or other unique identifiers.
4. Enter the WebEx Site URL in the Hostname field.
5. Enter the username and password of the Site Admin - View only account.
6. Click *Validate* to ensure that the Vyopta Data Collector application can connect.
7. If the connection succeeded, click the *Save* button.
8. You must repeat for each Webex site needed



The screenshot shows a configuration wizard window titled "Vyopta vAnalytics™ Data Collector Configuration Wizard". The "Infrastructure Components" tab is active. The form contains the following fields and values:

- Infrastructure Type: Cisco WebEx (dropdown menu)
- Name: Webex
- Description: Vyopta WebEx
- Hostname: vyopta.webex.com
- Protocol: HTTPS
- Username: vyoptasvc@vyopta.com
- Password: [masked with dots]
- Remember credentials for next component(s)

At the bottom of the window, there are three buttons: "Cancel", "Validate", and "Save".

Figure 8-2: Adding a WebEx Site



### 8.3 Cisco WebEx (Cloud only) Reference Table

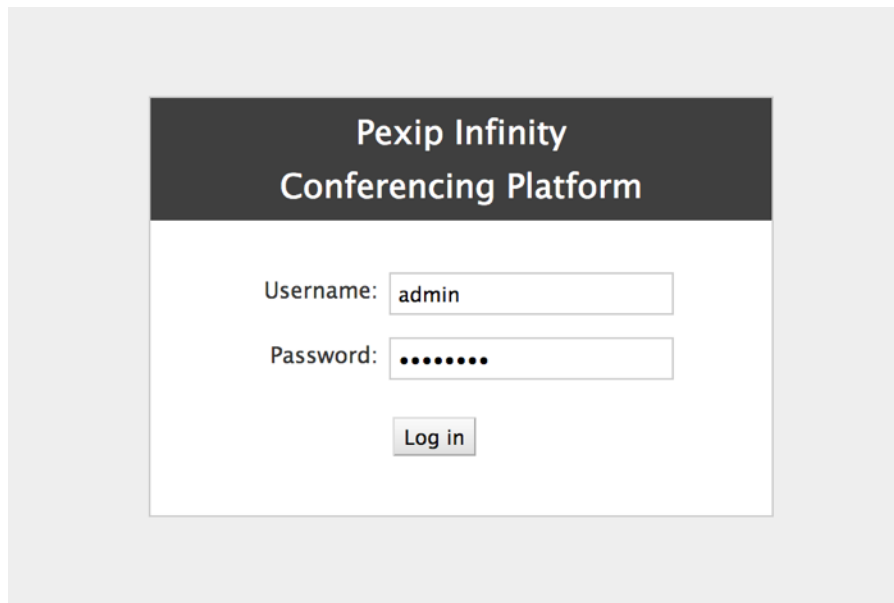
Cisco WebEx (Cloud only)	
Version	Version T28 or above
Device Access	FQDN of WebEx sites
User/Service Account	Local Site Admin - View-only WebEx account
TCP Ports	Vyopta Data Collector outbound to the WebEx Cloud TCP 443 (https)

## 9 Pexip Infinity

### 9.1 Validate the Service Account for Pexip Infinity

The account used by the Vyopta Data Collector for connection to Pexip Infinity is the Pexip Management Node admin account that is used to log into the Pexip Management Web Portal. To verify the credentials for the Pexip Management Node, please follow these steps:

1. Open a web browser and navigate to the domain name or IP address of the Pexip Management Node.
2. Enter the admin username and password for the Pexip Management Node.
3. Ensure you can successfully log into the Pexip Management Node.



**Figure 9-1:** Pexip Management Node Login Page

*Note: If the Pexip Management Node is LDAP-integrated, **only a local admin account can be used** for the Pexip Connector. If the User Authentication Source is set to LDAP database only, **the Pexip admin account must be used.***

## 9.2 Add a Pexip Connector

To add a Pexip Connector requires the following:

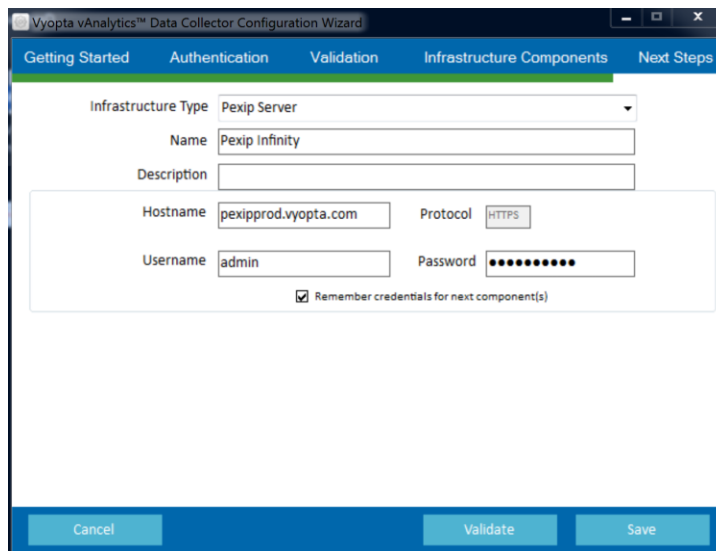
- Access through a web browser to the Pexip Node from the Vyopta Data Collector
- Credentials for the admin account on the Pexip Management Node from the previous section

Please follow the instructions below to add a Pexip Infinity device:

1. Select *Pexip Server* in the Infrastructure Type drop-down menu.
2. Enter the infrastructure name. This will be the name displayed for the video device in the Configuration Utility and within Vyopta's Applications Management Portal.

*Note: We recommend using hostname rather than IP as IP addresses are subject to change. It is also helpful to name the infrastructure in a 'friendly' or easily understood way.*

3. Enter the description of the video device. This can include the device type, location, and other unique identifiers.
4. Enter the Pexip Management Node hostname or IP address.
5. Enter the username and password for the administrator account.
6. Click Validate to confirm that Vyopta Data Collector can connect to the Pexip Management Node.
7. If the connection to the Pexip Node succeeded, click the Save button.



The screenshot shows the 'Vyopta vAnalytics™ Data Collector Configuration Wizard' window. The 'Infrastructure Components' tab is active. The form contains the following fields and options:

- Infrastructure Type: Pexip Server (dropdown menu)
- Name: Pexip Infinity (text input)
- Description: (empty text input)
- Hostname: pexipprod.vyopta.com (text input)
- Protocol: HTTPS (dropdown menu)
- Username: admin (text input)
- Password: (password input field with masked characters)
- Remember credentials for next component(s)

At the bottom of the wizard, there are three buttons: Cancel, Validate, and Save.

**Figure 9-2:** Adding Pexip infrastructure



### 9.3 Pexip Infinity Reference Table

Pexip Infinity	
Version	Pexip Infinity 10 or above
Device Access	Server IP/FQDN of Pexip Management Node(s)
User/Service Account	Local account with full Administrator access
TCP Ports	Vyopta Data Collector to Pexip Management Node(s) TCP 443*



## 10 Skype for Business (SfB)

### 10.1 Set up a Service Account for Skype for Business (SfB)

*Note: Requires (at least) version [3.4.6](#) of the Vyopta Data Collector.*

The service account for this component will be added to three (3) SfB SQL Server databases, with read-only privileges. You must determine where the SfB SQL Server databases are located within your environment. Check with your SfB administrator or SQL DBA for more information.

*Note: For setup instructions using Windows Authentication for Skype for Business, please contact Vyopta support at [support@vyopta.com](mailto:support@vyopta.com). This requires (at least) version [3.4.6](#) of the Vyopta Data Collector.*

Once you have identified where the SQL Server is located, you must verify that the server has Microsoft SQL Server Management Studio or download the software application to your local computer. To create a service account on the SfB SQL Server, perform the following:

1. Using SQL Server Management Studio, connect to the database used by SfB.
2. Log in with a SQL Server Administrator account or Local Administrator account.

*Note: The administrator account must have write privileges to create a service account.*

3. Navigate to the Security > Logins folder.
4. Right click on the Logins folder and choose *New Login*, which should display the following:

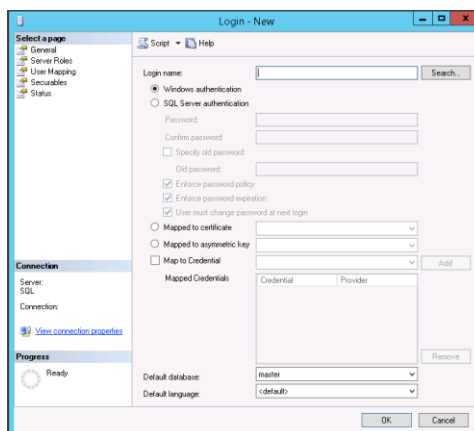


Figure 10-1: SQL User Creation Screen

5. Create a local database user account with the following information:
6. Fill in the Login Name. We recommend using a descriptive name like *vyopta\_svc*, as has been done in this example.
7. Select *SQL Server Authentication*.
8. Assign a Password and confirm the password.
9. Uncheck *Enforce Password Policy*.
10. Select *User Mapping* in the left-hand column.
11. Select the *LcsCDR* database to provide the account access to the database.
12. Once the database has been selected, you must identify the role membership. Select the *db\_datareader* and *public* roles.
13. Repeat steps 12 and 13 for the *QoEMetrics* & *xds* databases in the database List.
14. Click OK to create the user.

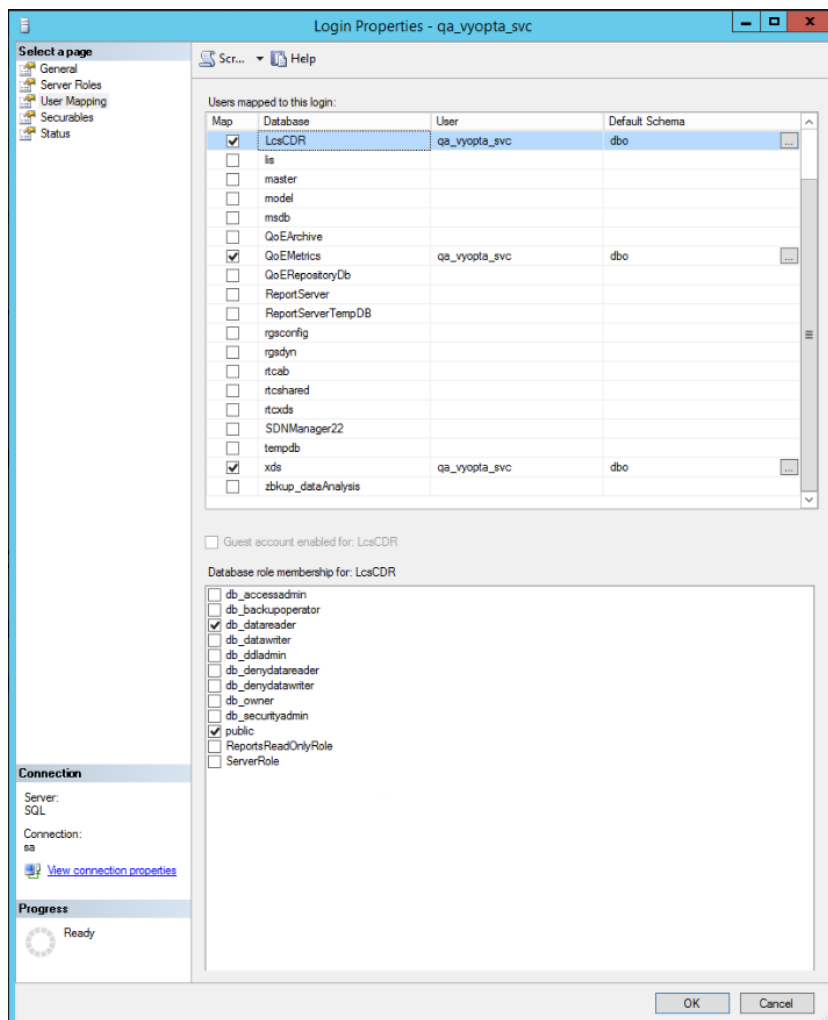


Figure 10-2: SQL User Role Mapping Screen

15. You will need to identify the Instance Name of the SQL Server hosting the Skype for Business database that will be the target of the Vyopta Data Collector. Your database administrator may be able to provide this information directly, or you can perform the following:
  - a. Open the Microsoft SQL Server Configuration Manager application and select the SQL Server Services tab as displayed below:

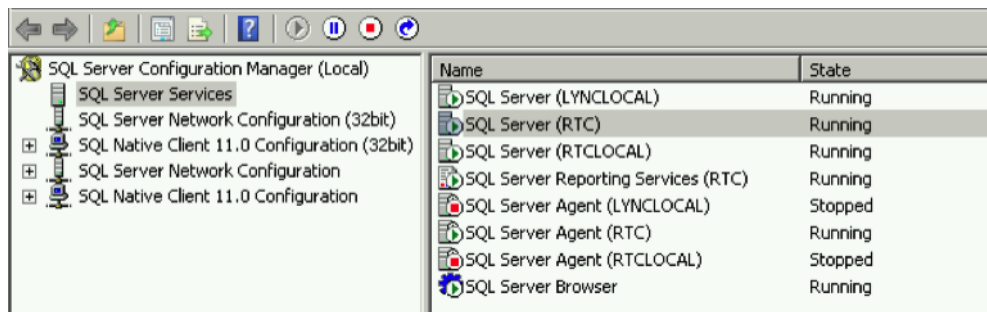


Figure 10-3: SQL Server Configuration Manager

- b. Identify the Instance Name of the SQL Server hosting the SfB Database. In the example above the SQL Server Instance Name is RTC.
  - c. Document this information to use in adding the SfB Connector.

**You have now created a new database read-only user account on the SfB database. This account is configured to be a service account for use in the Configuration Utility to set up the connection to the appropriate service.**

## 10.2 Setup Microsoft Skype for Business Realtime (only required for real-time monitoring)

*Note: Skype for Business Realtime Monitoring **requires (at least) version 3.5** of the Vyopta Data Collector and **version 2.4.1** of Microsoft Skype for Business SDN. For more information about SDN see the [Deploying Skype for Business SDN Interface](#) documentation published by Microsoft.*

*If your organization meets these requirements above, please contact [support@vyopta.com](mailto:support@vyopta.com) or your dedicated Sales Account Manager for more information.*

### Microsoft Skype for Business SDN Interface Online Resources

- [Deploying Skype for Business SDN Interface](#)
- [Installing Skype for Business SDN Interface](#)



- [Configuring Skype for Business SDN Interface](#)

To add a Microsoft Skype for Business Realtime Monitoring requires the following:

1. Microsoft Skype for Business SDN Interface must be installed, configured and deployed you're your existing production SfB environment.
2. If SDN is operational, please ensure that QoS is operational by running the following command on the Skype for Business server:

```
PS C:> Get-CsMediaConfiguration
```

... which should return a set of values where it can be verified that:

```
EnableInCallQoS : True
```

3. After verifying the QoS, please ensure that QoE is operational by running the following command on the Skype for Business server:

```
PS C:> Get-CsQoEConfiguration
```

... which should return a set of values where it can be verified that:

```
EnableQoE : True
```

4. If either of these values are 'false' then set to 'true' by running the following:

```
Set-CsMediaConfiguration -EnableQoS $true -EnableInCallQoS $True
```

5. Log into the SDN Manager and run the following commands from command line:

- a. Set 'hidepii' to False:

```
SDNManager.exe /p m hidepii=False
```

- b. Configure the SDN manager to send SDN logs to Vyopta Subscriber:



**SDNManager.exe /p s Vyopta submituri=http://<datacollector\_ip\_or\_fqdn>:22280/adr/skype**

**c. Add additional SDN manager commands for Vyopta Subscriber:**

**SDNManager.exe /p s Vyopta signaling=True**

**SDNManager.exe /p s Vyopta sendrawsdp=True**

- 6. Additionally, verify that the XDS database has the same permissions as the QoE and LcsCDR databases as noted in steps 1-14 of section 10.1.**

### **10.3 Add a Microsoft Skype for Business Connector**

*Note: For setup instructions using Windows Authentication for Skype for Business, please contact Vyopta support at [support@vyopta.com](mailto:support@vyopta.com). This requires (at least) version [3.4.6](#) of the Vyopta Data Collector.*

**To add a Microsoft Skype for Business Server Connector requires the following:**

- Access to the FQDN/IP address of the Server hosting the Skype for Business SQL Databases from the Vyopta Data Collector
- Credentials for the Microsoft SQL Server service account created in the previous section
- Knowledge of the SQL port type (static or dynamic) and if dynamic, the port value defined within Microsoft SQL Configuration Manager
- TCP/IP Connectivity enabled for the SQL Server within SQL Configuration Manager

**Please follow the instructions below to add Microsoft Skype for Business:**

1. Open the Vyopta System Config Utility and continue to the Infrastructure screen
2. Click the "Add Infrastructure" button to begin adding Skype for Business
3. Select *Microsoft Skype for Business* in the Infrastructure Type drop-down menu.
4. Enter the infrastructure name. This will be the name displayed for the video device in CPM.
5. Enter the description. This can include the device type, location, and other unique identifiers.
6. Click Next.
7. Enter the SQL Server Database Server hostname (or IP address).

*Note: We recommend using hostname rather than IP as IP addresses are subject to change. It is also helpful to name the infrastructure in a 'friendly' or easily understood way.*



8. Leave the Port Number of the SQL Server blank (unless changed from default value).
9. Click Validate to ensure that the Vyopta Data Collector application can connect to the host.
10. Click Next.
11. Add the **LcsCDR** SQL Server Instance Name and Database Name.
12. Enter the username and password of the Microsoft SQL Server service account created previously.
13. Click Validate to ensure that the Vyopta Data Collector application can connect to the **LcsCDR** database.
14. If the connection to the **LcsCDR** database succeeds, click the Next button.
15. Repeat steps 11 through 14 for the **QoEMetrics** database (Note: the QoE Metrics database may reside on a separate SQL server instance. Check with your SfB Admin or SQL DBA as needed.)
16. If the connection to the **QoEMetrics** database succeeds, click the Next button.
17. Repeat steps 11 through 14 for the **xds** database.
18. If the connection to the **xds** database succeeds, click the Save button.

#### 10.4 Microsoft Skype for Business

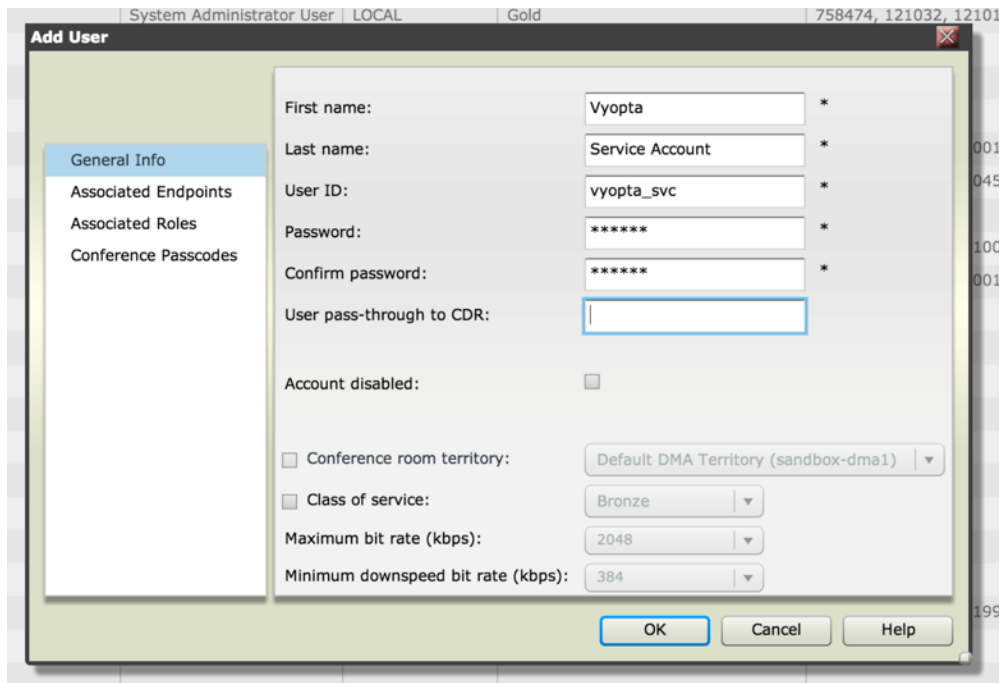
Skype for Business	
Version	Version 2015 or above
Device Access	Server IP/FQDN of S4B/Skype for Business database server/cluster responsible for reporting
User/Service Account	Local read-only database account that has access to the 'LcsCDR', 'QoEMetrics' and 'xds' databases.
SDN (required for Realtime support only)	Microsoft Skype for Business SDN 2.4.1
TCP Ports	<p>* Vyopta Data Collector to SQL database server/cluster TCP 1433*</p> <p>* Port can vary depending on customer environment; Exact port to be provided by Customer Skype for Business DBA team</p> <p>Inbound from SDN Manager to TCP 22280 on the Vyopta Data Collector server which listens for incoming SfB real-time data</p>

## 11 Polycom RealPresence Distributed Media Application (DMA)

### 11.1 Set up Service Account for Polycom RealPresence Distributed Media Application (DMA)

Create a service account on DMA which requires setting up a local account with administrator credentials. To add and verify the credentials for Polycom DMA, complete the following:

1. Open a web browser and navigate to the domain or IP address of the Polycom DMA.
2. Log in as an administrator using your username and password.
3. Navigate to the User > Users tab to open up the User Administration Panel.
4. Select Add to add the required user service account.
5. Enter the Name, User ID, and Password for the service account.
6. Select the Associated Roles tab and add the Administrator role.
7. Click OK to add the user account.
8. Log out of the Polycom DMA and verify that you can successfully log in using the service account credentials.



The screenshot shows the 'Add User' dialog box in the Polycom DMA administration interface. The window title bar includes 'System Administrator User | LOCAL | Gold | 758474, 121032, 12101'. The dialog has a sidebar with tabs: 'General Info' (selected), 'Associated Endpoints', 'Associated Roles', and 'Conference Passcodes'. The main form contains the following fields and options:

- First name: Vyopta \*
- Last name: Service Account \*
- User ID: vyopta\_svc \*
- Password: \*\*\*\*\* \*
- Confirm password: \*\*\*\*\* \*
- User pass-through to CDR: [Empty text box]
- Account disabled:
- Conference room territory:  Default DMA Territory (sandbox-dma1) [Dropdown]
- Class of service:  Bronze [Dropdown]
- Maximum bit rate (kbps): 2048 [Dropdown]
- Minimum downspeed bit rate (kbps): 384 [Dropdown]

Buttons at the bottom: OK, Cancel, Help.

Figure 11-2: Polycom DMA Add User Menu



## 11.2 Add a Polycom DMA Connector

To add a Polycom DMA Connector requires the following:

- Access to the FQDN/IP address of the DMA from the Vyopta Data Collector
- Port 8443 must be open between the Vyopta Data Collector and the Polycom DMA
- Credentials for the user service account on the Polycom DMA

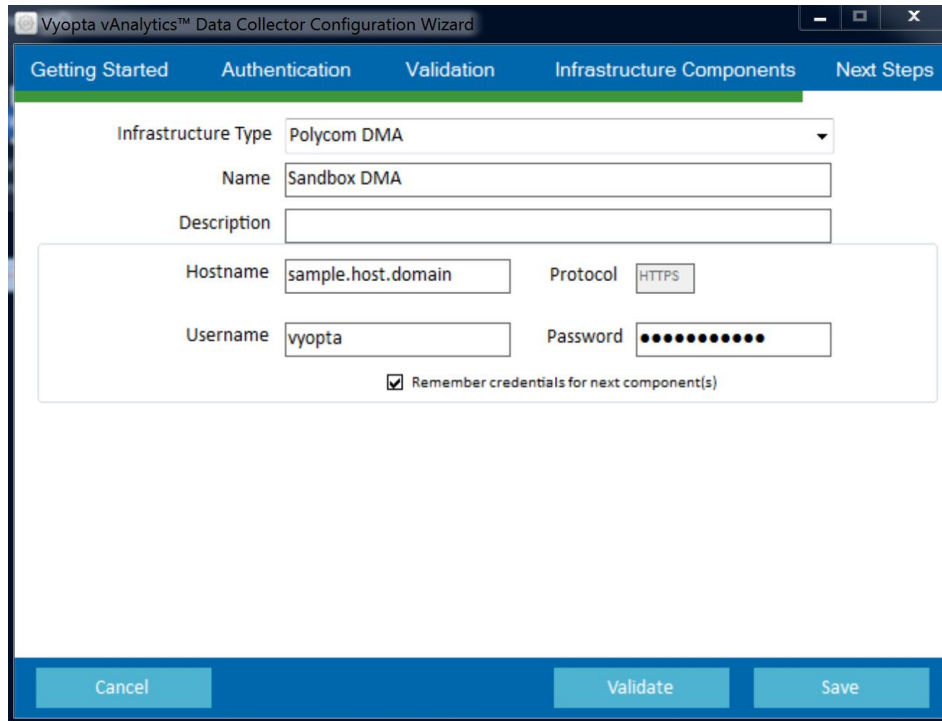
Please follow the instructions below to add each DMA instance:

1. Select *Polycom DMA* from the Infrastructure Type drop-down menu.
2. Enter the infrastructure name. This will be the name displayed for the video device in the Configuration Utility and within Vyopta's Applications Management Portal.

***Note: We recommend using hostname rather than IP as IP addresses are subject to change. It is also helpful to name the infrastructure in a 'friendly' or easily understood way.***

3. Enter the description of the device. This can include the device type, location, and other unique identifiers.
4. Enter the hostname or IP address followed by : 8443
5. Enter the username and password for the user service account.
6. Click Validate to ensure that the Vyopta Data Collector application can connect.
7. If the connection to the Polycom device succeeds, click the Save button.





The screenshot shows the 'Vyopta vAnalytics™ Data Collector Configuration Wizard' window. The 'Infrastructure Components' step is active, indicated by a green bar under the tab. The form contains the following fields and options:

- Infrastructure Type:** Polycom DMA (dropdown menu)
- Name:** Sandbox DMA (text input)
- Description:** (empty text input)
- Hostname:** sample.host.domain (text input)
- Protocol:** HTTPS (dropdown menu)
- Username:** vyopta (text input)
- Password:** (password input field with 10 dots)
- Remember credentials for next component(s)

At the bottom of the window, there are three buttons: 'Cancel', 'Validate', and 'Save'.

**Figure 11-3:** Polycom DMA Configuration Example



### 11.3 Polycom RealPresence Distributed Media Application (DMA) Reference Table

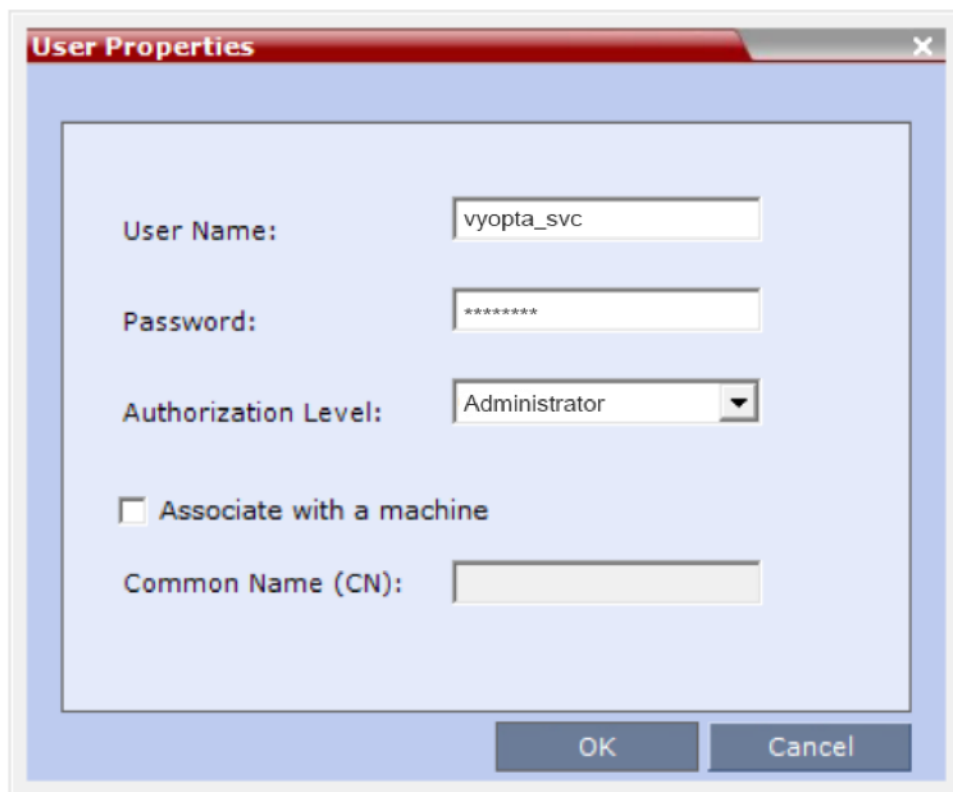
Polycom RealPresence Distributed Media Application (DMA)	
Version	DMA version 6.2 or above
Device Access	Server IP/FQDN
User/Service Account	Local account with full Administrator read/write or Provisioner privileges.
TCP Ports	Vyopta Data Collector outbound to the DMA device(s) TCP 8443

## 12 Polycom RealPresence Collaboration server (RMX)

### 12.1 Set up a Service Account for Polycom RealPresence Collaboration server (RMX)

The required service account must be an account with full read/write administrator credentials. The Polycom API will not allow an administrator account with read-only privileges to retrieve CDR data. To add and verify the credentials for the Polycom RMX, complete the following:

1. In the Polycom RMX Manager application click Users.
2. Click New User to open the User Properties dialog box.
3. Enter the username `vyopta_svc` in the User Name field for the user service account.
4. Enter the password in the Password field.
5. Select *Administrator* in the Authorization Level drop-down field.
6. Click OK to add the user account.
7. Log out of the Polycom RMX Manager application and verify that you can successfully log in using the service account credentials.



The screenshot shows a 'User Properties' dialog box with the following fields and values:

- User Name: `vyopta_svc`
- Password: `*****`
- Authorization Level: `Administrator`
- Associate with a machine
- Common Name (CN):

Figure 12-1: Polycom RMX Add User Menu



## 12.2 Add a Polycom RMX Connector

To add a Polycom RMX Connector requires the following:

- Access to the FQDN/IP address of the RMX from the Vyopta Data Collector
- Port 80/443 must be open between the Vyopta Data Collector and the Polycom RMX
- Credentials for the user service account on the Polycom RMX

Please follow the instructions below to add each RMX instance:

1. Select *Polycom RMX* from the Infrastructure Type drop-down menu.
2. Enter the infrastructure name. This will be the name displayed for the video device in the Configuration Utility and within Vyopta's Applications Management Portal.

*Note: We recommend using hostname rather than IP as IP addresses are subject to change. It is also helpful to name the infrastructure in a 'friendly' or easily understood way.*

3. Enter the description of the device. This can include the device type, location, and other unique identifiers.
4. Enter the hostname or IP address.
5. Enter the username and password for the user service account.
6. Click Validate to ensure that the Vyopta Data Collector application can connect.
7. If the connection to the Polycom RMX device succeeds, click the Save button.

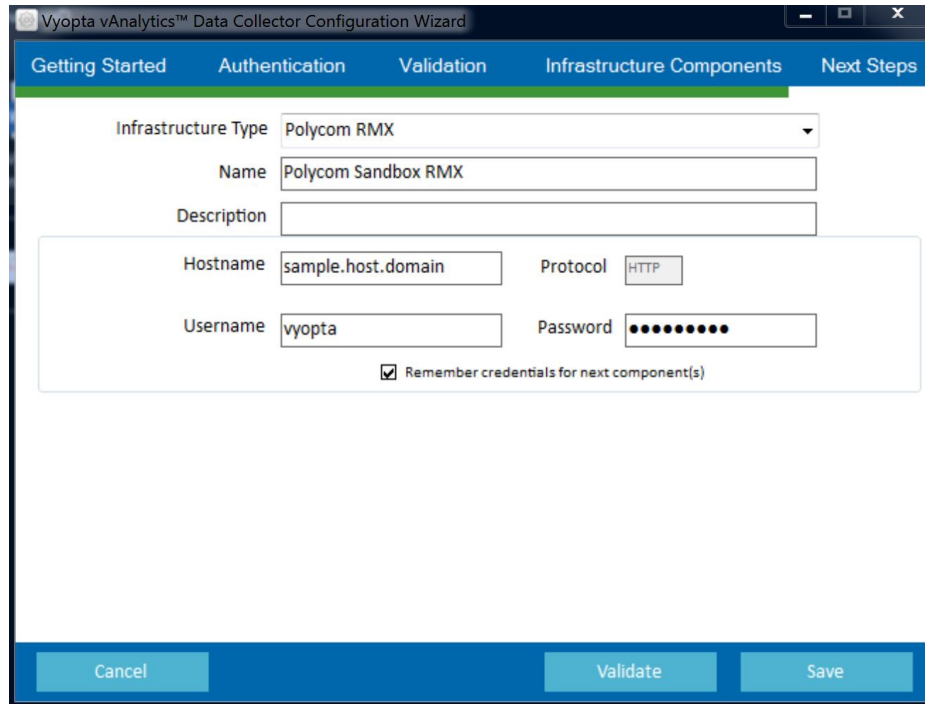


Figure 12-2: Polycom RMX Configuration Example

### 12.3 Polycom RealPresence Collaboration server (RMX) Reference Table

Polycom RealPresence Collaboration server (RMX)	
Version	RMX 8.5 or above
Device Access	Server IP/FQDN
User/Service Account	Local account with full Administrator read/write or privileges. Note: unable to use RMX read-only administrator due to limitation with API for CDR access.
TCP Ports	Vyopta Data Collector outbound to the RMX device(s) TCP 80/443

## 13 Polycom RealPresence Resource Manager (RPRM)

### 13.1 Set up a Service Account for Polycom RealPresence Resource Manager (RPRM)

Create a service account on DMA which requires setting up a local account with administrator credentials. To add and verify the credentials for Polycom RPRM complete the following:

1. Open a web browser and navigate to the domain or IP address of the Polycom RPRM.
2. Log in as an administrator using your username and password.
3. Navigate to the User > Users tab to open up the User Administration Panel.
4. Select Add to add the required user service account.
5. Enter the Name, User ID, and Password for the service account.
6. Select the Associated Roles tab and add the Administrator role.
7. Click OK to add the user account.
8. Log out of the Polycom RPRM and verify that you can successfully log in using the service account credentials.

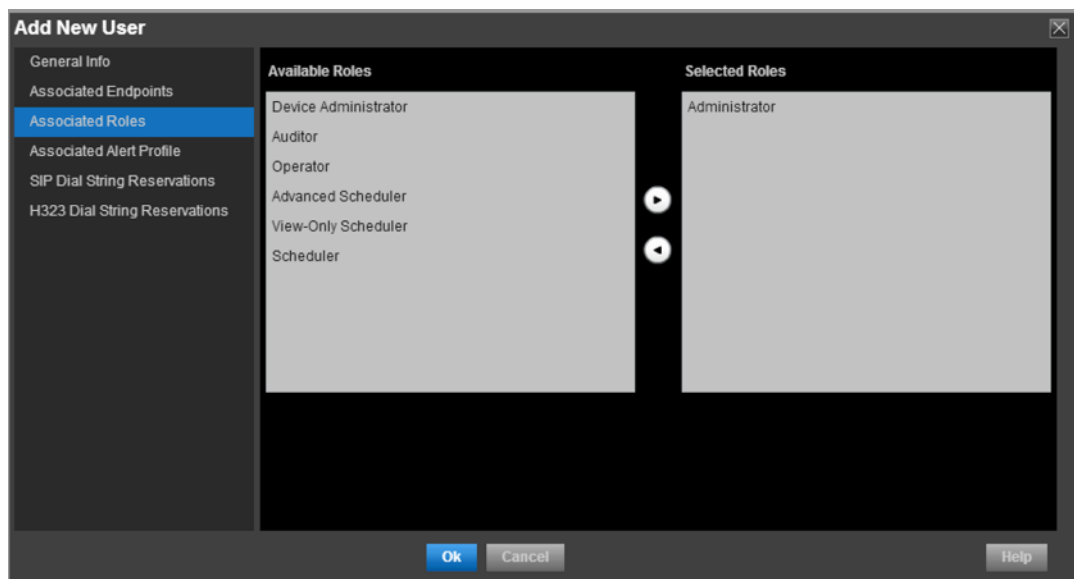


Figure 13-1: Polycom RPRM Add User Associated Roles Menu

### 13.2 Add a Polycom RPRM Connector

To add a Polycom RPRM Connector requires the following:

- Access to the FQDN/IP address of the RPRM from the Vyopta Data Collector

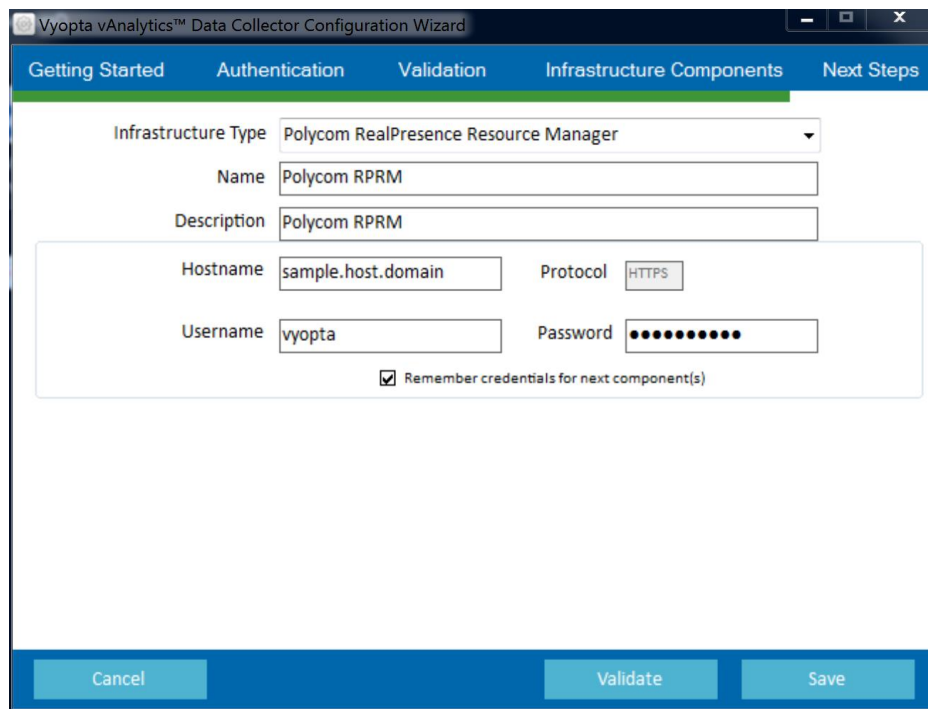
- Port 8443 must be open between the Vyopta Data Collector and the Polycom RPRM
- Credentials for the user service account on the Polycom RPRM

**Please follow the instructions below to add each RPRM instance:**

1. Select *Polycom RealPresence Resource Manager* from the Infrastructure Type drop-down menu.
2. Enter the infrastructure name. This will be the name displayed for the video device in the Configuration Utility and within Vyopta’s Applications Management Portal.

*Note: We recommend using hostname rather than IP as IP addresses are subject to change. It is also helpful to name the infrastructure in a 'friendly' or easily understood way.*

3. Enter the description of the device. This can include the device type, location, and other unique identifiers.
4. Enter the hostname or IP address followed by : 8443
5. Enter the username and password for the user service account.
6. Click Validate to ensure that the Vyopta Data Collector application can connect.
7. If the connection to the Polycom device succeeds, click the Save button.



**Figure 13-2:** Polycom RPRM Configuration Example



### 13.3 Polycom RealPresence Resource Manager (RPRM) Reference Table

Polycom RealPresence Resource Manager (RPRM)	
Version	RPRM version 8.2 or above
Device Access	Server IP/FQDN
User/Service Account	Local account with full Administrator read/write, device administrator or Operator privileges
TCP Ports	Vyopta Data Collector to RPRM TCP 8443

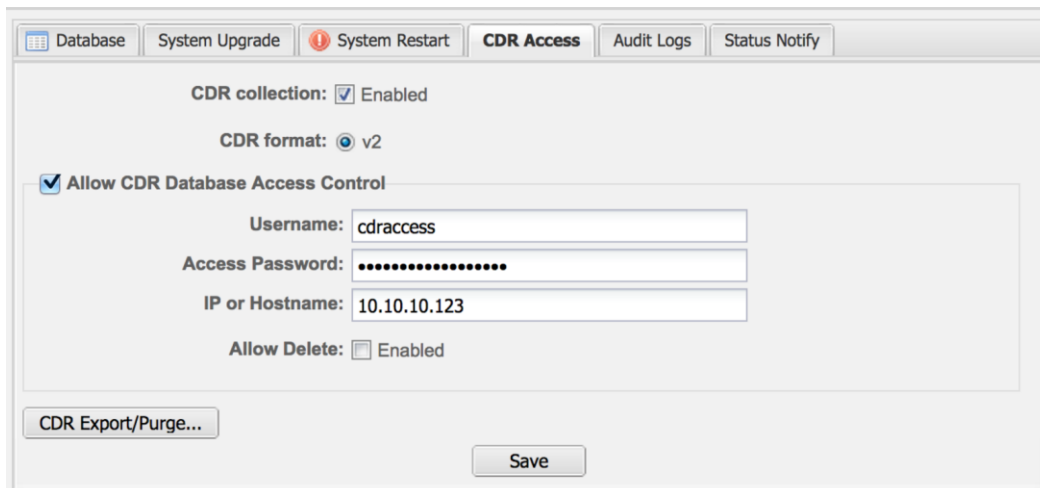


## 14 Vidyo Management Portal

### 14.1 Enable CDR Access in the Vidyo Management Portal

**CDR Access for the Vyopta Data Collector must be enabled using a Super Admin account as outlined below:**

1. Open a web browser and navigate to the domain or IP address of the Vidyo Router Super Admin portal.
2. Log in with a Super Admin account.
3. Select Settings > Maintenance > CDR Access.
4. Perform the following to configure the **cdaccess** account for CDR collection:
  - a. Ensure the CDR Collection is *Enabled*.
  - b. Set the Access Password to the cdaccess account.
  - c. Enter the IP address or Hostname of the Vyopta Data Collector in your environment.
  - d. Verify that the “Allow Delete” is not Enabled (i.e., the checkbox is unchecked).
5. Select Save to finish the CDR Account configuration.
6. Log out of the Vidyo Management Portal.



**Figure 14-1:** CDR Account Configuration Settings

## 14.2 Configure a User Account in the Vidyo Management Portal

1. Navigate to the Standard Vidyo Admin Portal
2. Log in with an Admin Account
3. Under *Manage Users* select *Add User* and fill in the following information:
  - a. Select *Admin* for *User Type*.
  - b. Enter in *cdraccess* for the *User Name*, this must match the DB service account username.
  - c. Enter in the same *Password* used above for the DB service account password above.
  - d. Enter in *cdraccess* for the *Display Name*.
  - e. The E-mail Address must be entered, but does not need to be a live email address. It is recommended *cdraccess@domain.com* be used.
  - f. The Extension must also be entered, but does not need to follow any dial-plan. It is recommended *1000* or *9999* be used.
  - g. All other fields can be set to the default value.
  - h. Verify that the Status and Allowed to log in to user portal are both *Enabled*.
4. Once the User has been created, select *Save* to finish the User Account configuration.
5. Log out of the Vidyo Admin Portal.

## 14.3 Verify that API Access is enabled

Please ensure that the following licenses are enabled for Vidyo. The API licenses (User & Admin) feature keys are required to support third-party software integration. These are not enabled by default and you will have to reach out to Vidyo to enable them.

1. Log into the Vidyo Super Portal and go to Settings > System License.
2. Scroll down to Admin API Access on the System License page.
3. Confirm that the Admin API is enabled (as shown below).

System License <small>[Lines License Model]</small>	
Feature	License
User API Access	Enable
Admin API Access	Enable
Encryption	None
MultiTenant	Disable
Allow UC Clients	Disable

Figure 14-2: Verifying if Admin and User API Access is enabled

## 14.4 Add a Vidyo Management Portal Connector

To add a Vidyo Management Portal Connector requires the following:

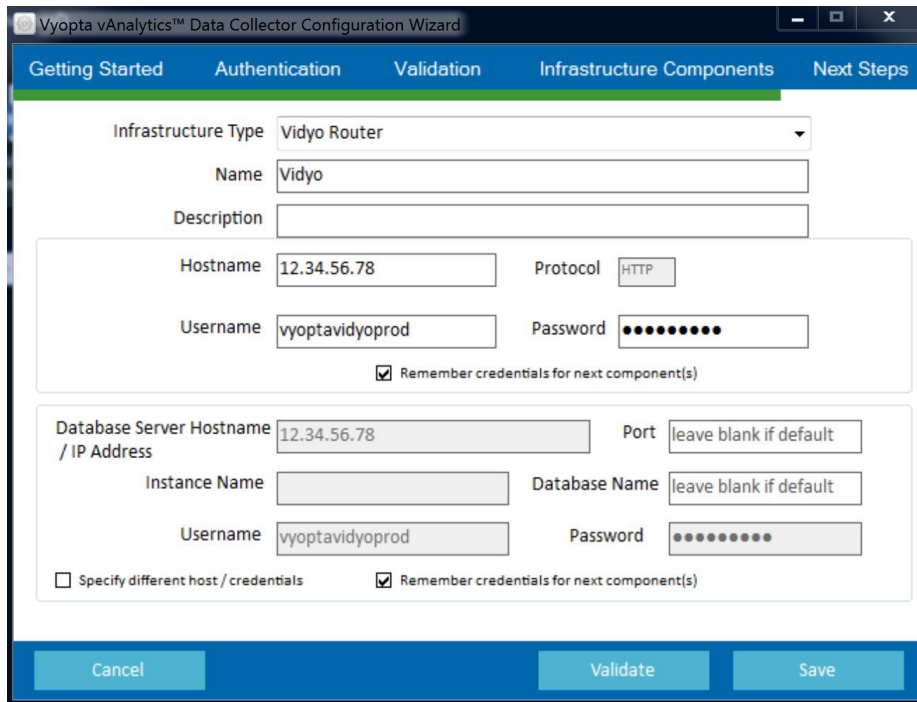
- Access to the Vidyo Management Portal and database from the Vyopta Data Collector
- Credentials for the cdraccess account on the Vidyo Management Portal

Please follow the instructions below to add the video appliance:

1. Select *Vidyo Router* in the Infrastructure Type drop-down menu.
2. Enter a suitable name and description into the appropriate fields.

*Note: We recommend using hostname rather than IP as IP addresses are subject to change. It is also helpful to name the infrastructure in a 'friendly' or easily understood way.*

3. Enter the Vidyo Management Portal IP address or Hostname.
4. Enter `cdraccess` for the Username and the appropriate Password for the Account.
5. Click **Validate** to ensure that the Vyopta Data Collector application can connect.
6. If the connection to the video component succeeded, click the **Save** button.



The screenshot shows the 'Infrastructure Components' tab of the 'Vyopta vAnalytics™ Data Collector Configuration Wizard'. The form is filled with the following information:

- Infrastructure Type:** Vidyo Router
- Name:** Vidyo
- Description:** (empty)
- Hostname:** 12.34.56.78
- Protocol:** HTTP
- Username:** vyoptavidyoprod
- Password:** (masked with dots)
- Remember credentials for next component(s)
- Database Server Hostname / IP Address:** 12.34.56.78
- Port:** leave blank if default
- Instance Name:** (empty)
- Database Name:** leave blank if default
- Username:** vyoptavidyoprod
- Password:** (masked with dots)
- Specify different host / credentials
- Remember credentials for next component(s)

At the bottom of the wizard, there are three buttons: **Cancel**, **Validate**, and **Save**.

Figure 14-3: Vidyo Infrastructure Information Example



## 14.5 Vidyo Management Portal Reference Table

VIDYO Management Portal	
Version	Vidyo version 3.1 or above
Device Access	Server IP/FQDN of Vidyo Management Portal
User/Service Account	Local read-only account named 'cdraccess'
TCP Ports	Vyopta Data Collector to Vidyo Management Portal TCP 443  Vyopta Data Collector to Vidyo database TCP 3306

## 15 Zoom Server

### 15.1 Create API Key and API Secret

To create an API Key and API secret for Zoom, login as an administrator and perform the following:

1. Login to Zoom using an existing administrator account (must be an admin account).
2. Select 'Zoom for Developers' under the 'Advanced' heading.
3. In the new window that opens (Zoom for Developers), select your name in the upper right and click **Developer Account**.
4. Fill out the Details Tab and check the Web / API checkbox under platforms and click save.
5. On the API Tab generate and copy the API Key and the API Secret.

### Developer Account

Welcome to the Zoom Developers Account page. You can find below details about the app you're building, credentials for the API, settings for webhooks, and credentials for Zoom SDK (Windows, Mac, iOS, Android).

Details **API** Webhook SDK OAuth

### API Credentials

Use your API Key and Secret to access the Zoom APIs. [View Docs](#)

API Key	<input type="text"/>	Copy
API Secret	<input type="text"/>	Copy
IM Chat History Token	<input type="text"/>	Copy

[Disable](#) [Regenerate Secret](#) [Regenerate Access Token](#) [View Call Logs](#)

**Figure 15-1: Enabling API Integration for Zoom**

That's it! You should now have your API Key and API Secret, with which Zoom can be added to the Vyopta Data Collector.

**Note: Make sure to record your API Key and API Secret as they will be used to connect Zoom via API.**

## 15.2 Add a Zoom Connector

To add a Zoom Connector requires the following:

- Access to your organization’s Zoom API URL
- Credentials for your API Key and API Secret
- Vyopta Data Collector version 3.4.1 or higher

Please follow the instructions below to add your Zoom instance to Data Collection:

1. Select *Zoom Server* in the Infrastructure Type drop-down menu.
2. Enter the Zoom name and description as desired.
3. Next, enter the default API URL and make sure SSL is checked.
4. Click Validate and Next if the API URL passes validation.

**Note: The default Zoom API URL is “api.zoom.us”, however this should reflect the URL of the Zoom infrastructure and may vary for on-premise deployment.**

5. After that, enter the API Key and API Secret.
6. Click Validate to ensure that the Vyopta Data Collector application can connect.
7. If the connection succeeded, click the Save button.

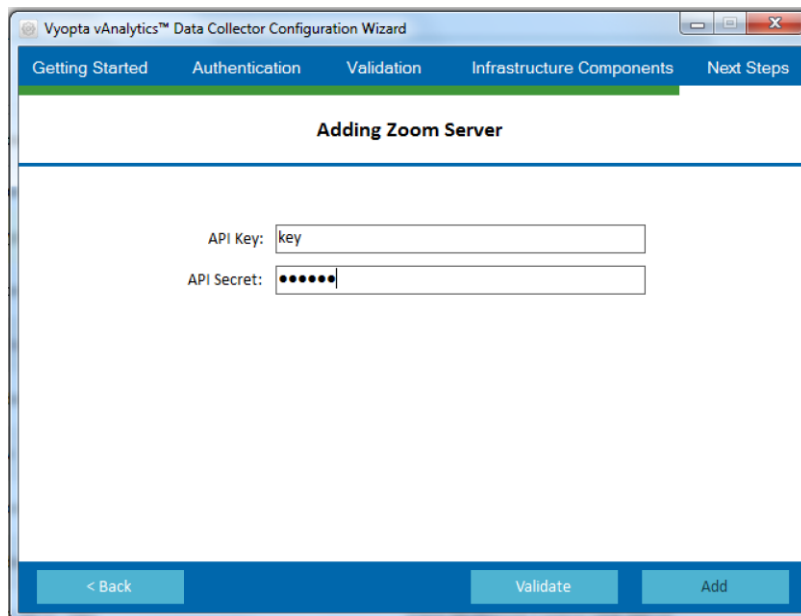
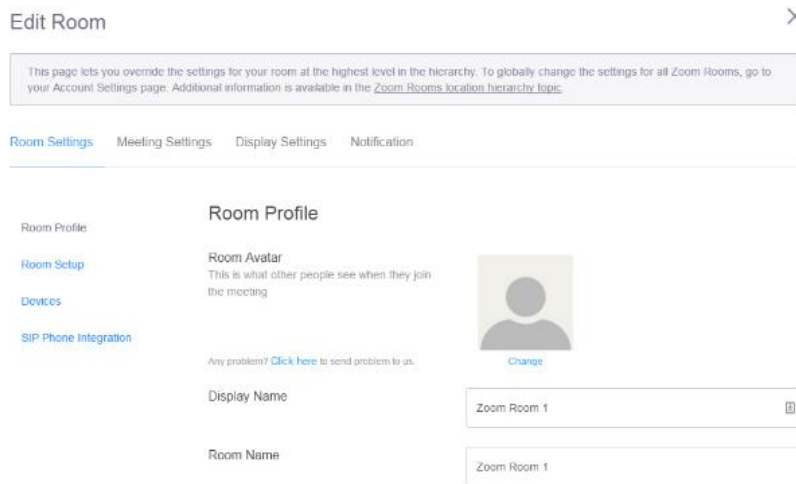


Figure 15-2: Adding a Zoom Server

*Note: Enabling Zoom Rooms for data collection may require adjustments in the Zoom Room name and display name used by your organization. **To enable Zoom Room tracking and matching, please note that all Zoom Room names and display names must be identical.** Additionally, all Room Names must be unique.*



The screenshot shows the 'Edit Room' interface with a 'Room Profile' section. The 'Display Name' and 'Room Name' fields are both set to 'Zoom Room 1'. There is also a 'Room Avatar' section with a 'Change' button.

**Figure 15-3:** Setting up matching Zoom Room name and display name

### 15.3 Zoom Server Reference Table

Zoom Server	
Data Collector	Vyopta Data Collector 3.4.1 or higher
User/Service Account	Zoom admin account with full Administrator privileges. Please note that admin rights are required to generate API key and shared secret.
TCP Ports	Vyopta Data Collector outbound to the Zoom Server TCP 443 (https)

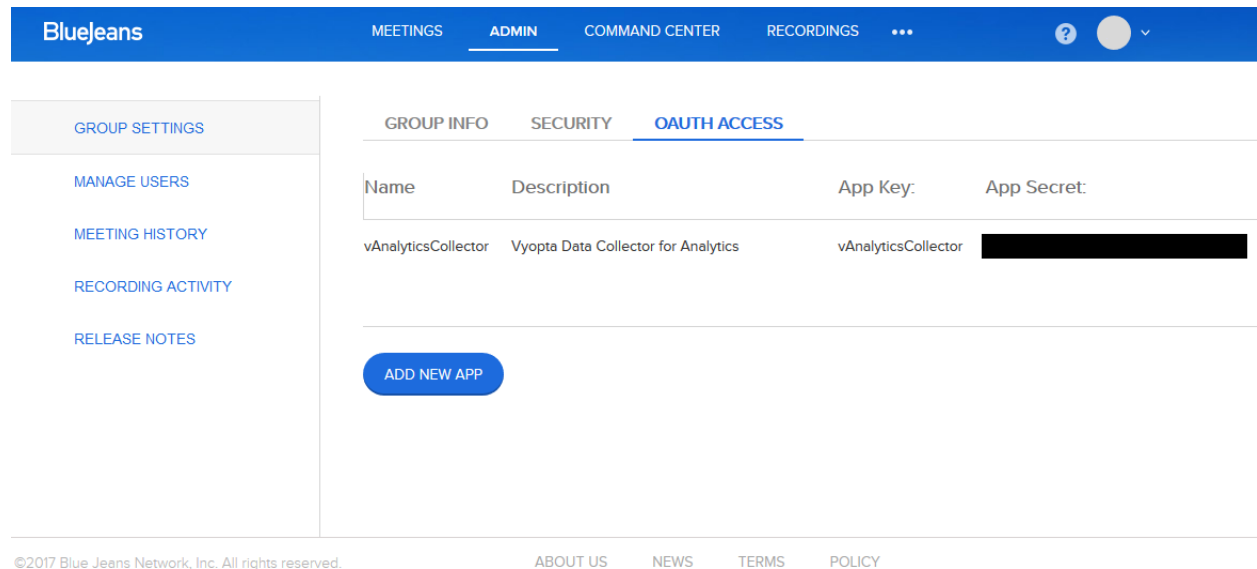
## 16 BlueJeans

### 16.1 Create App Key and App Secret

To begin, a BlueJeans administrator will need to create an App Key and App Secret, in the BlueJeans admin console, by perform the following:

1. Login to BlueJeans using an existing administrator account (must be an admin account).
2. Select 'Group Settings' under the 'Admin' heading.
3. Create the App Key and App Secret by selecting 'Add New App'.
4. Save the new App Key and App Secret.

*Note: When adding a new BlueJeans environment to the Vyopta Data Collector, please generate a new App Key and App Secret for each environment.*



**Figure 16-1:** Enabling App Key and Secret for BlueJeans

That's it! You should now have your App Key and App Secret, with which BlueJeans can be added to the Vyopta Data Collector.

*Note: **Make sure to record your App Key and App Secret** as they will be used to connect BlueJeans to Vyopta via API.*



## 16.2 Add a BlueJeans Connector

To add a BlueJeans Connector requires the following:

- Access to your organization’s BlueJeans Admin portal.
- Credentials for your BlueJeans App Key and App Secret
- Vyopta Data Collector version 3.4.5 or higher

Please follow the instructions below to add your BlueJeans instance to Data Collection:

1. Select *BlueJeans* in the Infrastructure Type drop-down menu.
2. Enter the BlueJeans name and description as desired.
3. Next, accept the default API URL (auto-populated) and make sure SSL is checked.
4. Click Validate and Next if the API URL passes validation.

*Note: The default BlueJeans API URL is “api.bluejeans.com”*

5. After that, enter the App Key and App Secret.
6. Click Validate to ensure that the Vyopta Data Collector application can connect.
7. If the connection succeeded, click the Save button.

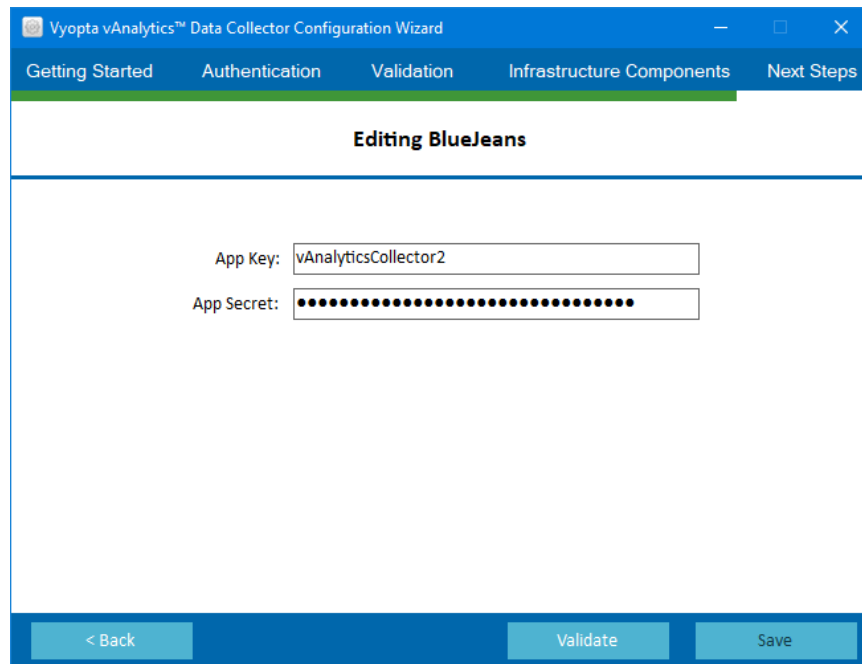


Figure 16-2: Adding BlueJeans to Data Collection

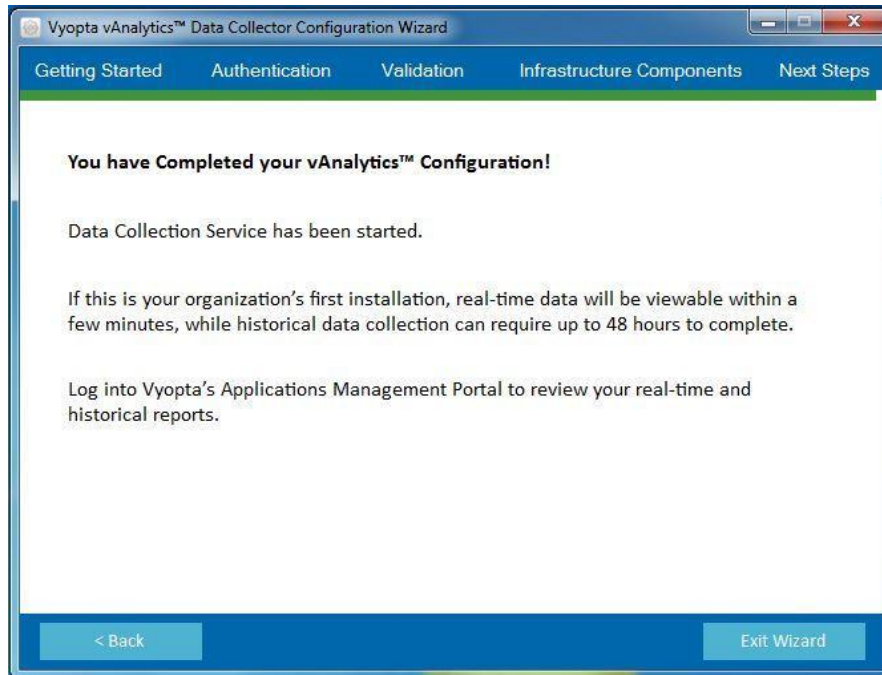


### 16.3 BlueJeans Server Reference Table

BlueJeans	
Data Collector	Vyopta Data Collector 3.4.5 or higher
User/Service Account	BlueJeans admin account with full Administrator privileges. Please note that admin rights are required to generate App Key and App Secret.
TCP Ports	Vyopta Data Collector outbound to the BlueJeans API TCP 443 (https)

## 17 Saving the configuration and starting the service

After you have successfully added all of your video devices into the vAnalytics Configuration Utility, click the Next button and you will see the wizard starting the vAnalytics Service.



**Figure 16-1: Vyopta Configuration Wizard**

*Congratulations! You have now installed and configured Vyopta's Data Collector within your video collaboration environment.*

*Please note: It will take approximately 2 days to populate historical data in CPM Analytics, but you should be able to start seeing real-time data immediately in CPM Monitoring by logging into <https://vanalytics.vyopta.com>.*

*If you have any questions or require assistance, please contact [support@vyopta.com](mailto:support@vyopta.com).*



## 17.1 Troubleshooting a Failed Connection

If you receive an error while adding a video infrastructure device, there are many reasons that could be the result of the issue. Depending on your IT Organization, this typically requires involvement from your Network Administrator. There are, however, steps that you can use to troubleshoot your network connection.

Attempting to connect to the video device from a web browser will determine if the issue is with the connection to the infrastructure, a problem with the account on the video device, or information entered while adding the video device to the Configuration Utility. Please try the following steps to resolve these issues:

1. Open a web browser such as Chrome, Firefox, or Internet Explorer.
2. In your browser, type in the host name or IP address of the video device, then press enter. Wait for the webpage to load.
3. If you are unable to connect to the video device through a web browser, please verify that you are using the proper protocol (HTTP or HTTPS).
4. If you can connect to the video device through a web browser, verify that the web protocol matches the protocol used while adding the infrastructure.
5. Log into the video device using the configured username and password on the video device that was set up as part of the configuration process.
6. If you are unable to log in, ensure that you have the proper credentials for the account on the video device.
7. If you can log into the video device with the account credentials, ensure that the account is properly configured on the device.

If you continue to have issues connecting to the video device, you may have a network configuration issue or network proxy in place that needs to be addressed in the for your configuration. Please reach out to your network administrator to troubleshoot the network connection or contact [support@vyopta.com](mailto:support@vyopta.com) for further assistance.