UnifiedFX

PhoneView Administration Guide

Disclaimer
The information in this document is subject to change without notice and does not represent a commitment on the part of UnifiedFX Limited. The software described in this document is subject to a License Agreement and may not be copied to other media except as specifically allowed in the License Agreement.
All product and company names are ™ or ® trademarks of their respective owners. Windows is a trademark of Microsoft Corporation.

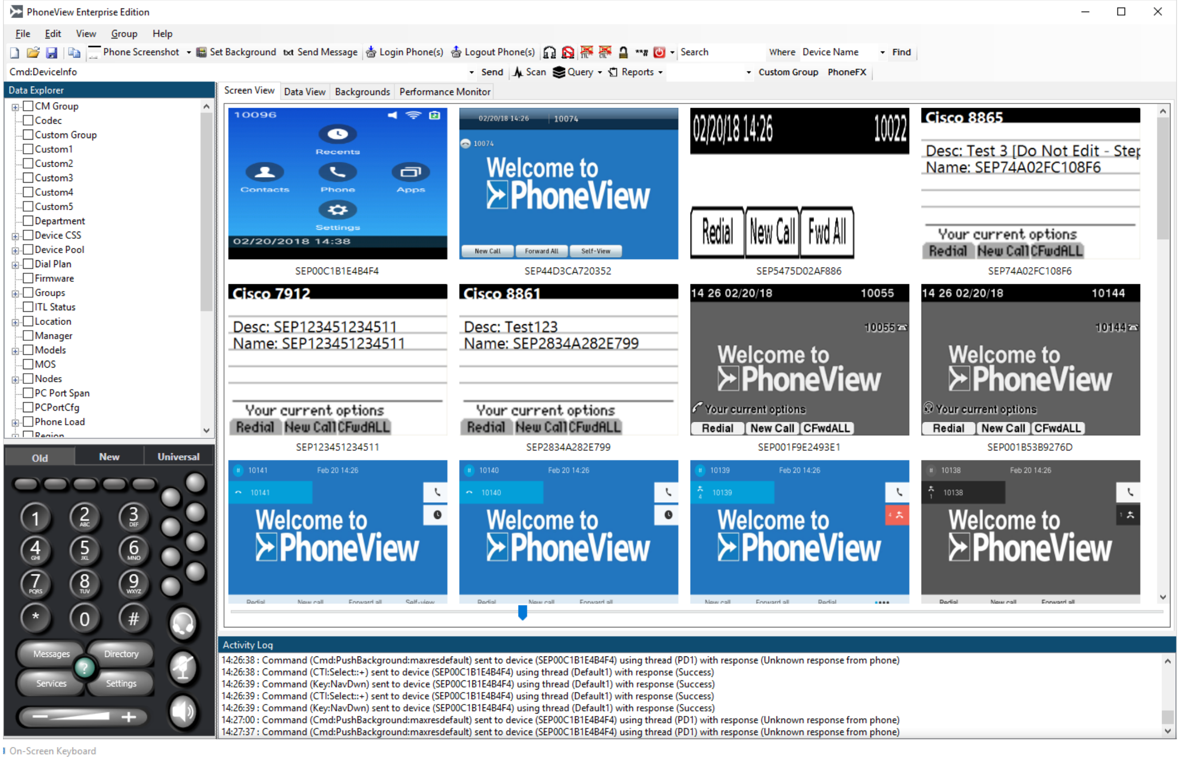
Document authored by Jim Paton
Document revision: 7.1
Document issued: September 2020

Cover image modified and used under the terms of the Pixabay License. Original image by Peggy und Marco Lachmann-Anke from Pixabay.

Table of Contents

Welcome to PhoneView!

Congratulations on choosing PhoneView!
Whether you have the **Free Lab**, **Free Trial**, **Engineer**, or **Enterprise** Edition, with PhoneView you now have at your fingertips the only fully-featured, certified Cisco Compatible IP phone endpoint management solution.



```
14:26:38 : Command (Cmd:PushBackground:maxresdefault) sent to device (SEP00C1B1E4B4F4) using thread (PD1) with response (Unknown response from phone)
14:26:38 : Command (CTI:Select::+) sent to device (SEP00C1B1E4B4F4) using thread (Default1) with response (Success)
14:26:39 : Command (Key:NavDwn) sent to device (SEP00C1B1E4B4F4) using thread (Default1) with response (Success)
14:26:39 : Command (CTI:Select::+) sent to device (SEP00C1B1E4B4F4) using thread (Default1) with response (Success)
14:26:39 : Command (Key:NavDwn) sent to device (SEP00C1B1E4B4F4) using thread (Default1) with response (Success)
14:27:00 : Command (Cmd:PushBackground:maxresdefault) sent to device (SEP00C1B1E4B4F4) using thread (PD1) with response (Unknown response from phone)
14:27:37 : Command (Cmd:PushBackground:maxresdefault) sent to device (SEP00C1B1E4B4F4) using thread (PD1) with response (Unknown response from phone)
```

Figure 1-1 – PhoneView Main Window

With its powerful real-time monitoring features, PhoneView provides the means to visualise all of your IP phones within a single intuitive, industry-leading user interface, scaling effortlessly from a few hundred phones on a single cluster to massive enterprise-level telephony installations comprising hundreds of thousands of devices connected over multiple clusters.
PhoneView makes it trivial for you to remotely manage and control multiple Cisco IP phones from a single location. The powerful search, filter and group facilities make it easy to target specific devices based on model, firmware, location, pool, group *etc.* - right down to a single device, allowing you to focus on the task at hand whether that's logging a user in or out of the phone, deleting ITL/CTL files, setting phone backgrounds or even updating firmware.

The real-time monitoring and remote management features included in PhoneView mean that most phone-related issues (other than physical phone faults) that would previously have required a site visit can now be handled remotely, eliminating around 90% of site call-outs and therefore providing unparalleled return on investment (ROI).

Who Should Read This Guide

This guide is primarily intended for system administrators and engineers who need to know how to install and configure PhoneView.

It outlines the system requirements for the PhoneView software, and describes the procedure for installing the software and registering your license key. It contains detailed instructions on configuring your Cisco environment for compatibility with PhoneView, including enabling and starting essential services, setting up required user accounts and setting configuration options to enable specific PhoneView features and functionality. It also features guidance on how to add your first cluster to PhoneView.

If you're an engineer installing and configuring PhoneView for your own use, or a system administrator managing a multi-user PhoneView Enterprise Edition installation, you'll find the information you need to get up and running with PhoneView in this guide.

Conventions Used in This Guide

This guide uses specific formatting to point out special facts and to warn you of potential issues:

The lightbulb symbol indicates a tip or additional piece of information that may be useful for more advanced users.

The information symbol highlights important information that is essential for the given context.

The warning symbol warns you of potential issues and information that requires your full attention.

Furthermore, the following formatting is used:

- Paths and locations on your hard drive or other storage devices are printed in *italics*;
- Important names and concepts are highlighted in **bold**;
- Square brackets are used to reference keys on a computer keyboard, *e.g.* Press [Shift] + [Enter].

Online Resources

Although this guide is intended to be the primary reference for PhoneView, UnifiedFX have a number of online resources to provide additional support and assistance when you need it:

- **UnifiedFX Support Portal**
  The UnifiedFX Support Portal features a knowledge base containing articles where you can find out more about the features and functionality of PhoneView and other UnifiedFX products.

- **UnifiedFX Video Tutorials**
  UnifiedFX also produces regular videos covering PhoneView-related topics. A selection of these videos is featured on the UnifiedFX website, but the best way to watch is to head over to our YouTube channel at https://www.youtube.com/user/UnifiedFX and click the subscribe button.

- **UnifiedFX Webex Webinars**
  UnifiedFX host regular Webex sessions on how to get the most out of PhoneView. These sessions are a great way to learn about PhoneView in an interactive setting where you can ask questions and get answers direct from the UnifiedFX engineers.

How to Contact Us

If you encounter a problem with PhoneView or have a question that isn't covered in this guide or in any of the online PhoneView content in the support portal, you can contact the UnifiedFX support team for additional assistance either by sending an email to the support team at support@unifiedfx.com or submitting a support request through the support portal at https://support.unifiedfx.com/hc/en-gb/requests/new.

Alternatively, if you're looking to upgrade to a different edition of PhoneView, add additional phones to your license, or you want to find out more about the other products in the UnifiedFX range, you can contact the sales team by sending an email to sales@unifiedfx.com or by filling out the form on the website **Contact Us** page at https://www.unifiedfx.com/about-us/get-in-touch.

For enquiries on any other topic, the Contact Us page has a full list of contact details.

We look forward to hearing from you!

System Requirements

System Requirements

PhoneView is a desktop application that runs on the Microsoft Windows operating system. The minimum recommended requirements to run PhoneView are:

- Microsoft Windows 8/8.1/10 -or- Microsoft Windows Server 2012/2012R2/2016/2019;
- Microsoft .NET Framework 4.5.2 (or above);
- 2.0GHz CPU (dual core) or greater;
- 4GB RAM or greater
- 2GB free hard disk space

> The exact memory requirements for PhoneView will depend on the size of the phone estate being managed.
> PhoneView will run on a system with as little as 2GB RAM, however this is not recommended or supported. The guideline requirement of 4GB will be adequate for the most common usage scenarios, for example phone estates of up to approximately 10,000 phones.
> For phone estates larger than 10,000 phones, contact the UnifiedFX support team who can advise with more detailed requirements.

Infrastructure Requirements

PhoneView is certified Cisco Compatible and works with the widest range of Cisco Unified Communication Manager (CUCM) or Cisco Call Manager versions and Cisco IP phone models. The table below shows the list of software versions and phone models that have been tested for compatibility:

Feature	Supported Models / Versions
Cisco Unified Communication Manager	5.x, 6.x, 7.x, 8.x, 9.x, 10.x, 11.x, 12.x
Phones	6921, 6941, 6945, 6961, 7821, 7841, 7861, 7905, 7906, 7911, 7912, 7925, 7926, 7937, 7940, 7941, 7942, 7945, 7960, 7961, 7962, 7965, 7970, 7971, 7975, 8811, 8821, 8831, 8841, 8845, 8851, 8861, 8865, 8941, 8945, 8961, 9951, 9971, IP Communicator, Cisco CIUS

Feature	Supported Models / Versions
Background Updates using personalization method	UCM6.1 or above, and the following phone models: 7906, 7911, 7925, 7926, 7941, 7942, 7945, 7961, 7962, 7965, 7970, 7971, 7975 8811, 8821, 8841, 8845, 8851, 8861, 8865, 8961, 9951, 9971
Remote deletion of ITL certificates	6921, 6941, 6945, 6961, 7821, 7841, 7861, 7906, 7911, 7941, 7942, 7945, 7961, 7962, 7965, 7970, 7971, 7975, 8811, 8821, 8831, 8841, 8845, 8851, 8861, 8865, 8941, 8945, 8961, 9951, 9971
Remote deletion of CTL certificates	6921, 6941, 6945, 6961, 7821, 7841, 7861, 7906, 7911,7940, 7941, 7942, 7945, 7960, 7961, 7962, 7965, 7970, 7971, 7975, 8811, 8821, 8831, 8841, 8845, 8851, 8861, 8865, 8941, 8945, 8961, 9951, 9971

Under certain circumstances a CUCM update or device pack may be required support new phone models.

Network Requirements

PhoneView needs to interact with both the Cisco Unified Communications Manager (Cisco Call Manager) and also the embedded web server built-in to every Cisco IP Phone, so network connectivity from the client PC to these devices is required.

PhoneView will attempt to automatically create and configure any necessary Windows Firewall rules on your system.

From	To	Destination Port	Purpose
PhoneView	UCM	80/TCP	HTTP API Interface
PhoneView	UCM	8080/TCP	HTTP API Interface
PhoneView	UCM	443/TCP	HTTP API Interface
PhoneView	UCM	8443/TCP	HTTP API Interface
PhoneView	UCM	6970/TCP	HTTP API Interface
PhoneView	UCM	2748/TCP	CTI API Interface
PhoneView	UCM	2789/TCP	CTI API Interface

PhoneView also requires the following for direct connectivity to IP phones:

From	To	Destination Port	Purpose
PhoneView	IP Phone	80/TCP	HTTP Web Interface
PhoneView	IP Phone	443/TCP	HTTP Web Interface
PhoneView	IP Phone	16384-32768/ UDP	RTP Stream
IP Phone	PhoneView	9090/TCP	HTTP Web Interface

Although the PhoneView web server runs on port 9090 by default, this can be changed by selecting Help » Set WebServer from the PhoneView main menu.

SYSTEM CONFIGURATION

Configuring the Cisco Unified Communications Manager for PhoneView

Before running PhoneView for the first time, there are a number of configuration settings that need to be made in the Cisco Unified Communications Manager (CUCM) to enable the full range of PhoneView features. The sections in this chapter will take you through the steps necessary to make these configuration changes.

> Further information on configuring CUCM can be found in the **Administration Guide for Cisco Unified Communications Manager**. The correct documentation for your version of CUCM can be found on the web at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

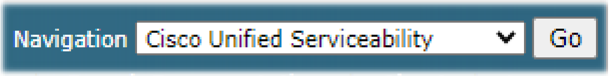
Ensuring Required Services are Running

Several services need to be activated and running within CUCM in order for certain PhoneView features to operate properly:

- **Cisco AXL Web Service**
  This service is required to retrieve the list of devices and their properties from the cluster.
- **Cisco Extension Mobility**
  This service is required to log users in and out of their phone without the need for their password.
- **Cisco CTIManager**
  This service is required if using CTI for remote control or Remote Audio Monitoring.
- **Cisco RIS Data Collector**
  This service is required to get information on phones when performing a Group Update in PhoneView.

Cisco AXL Web Service, Cisco Extension Mobility and Cisco CTIManager are feature services and must be activated before they can be started. To activate these services please follow the steps listed below:

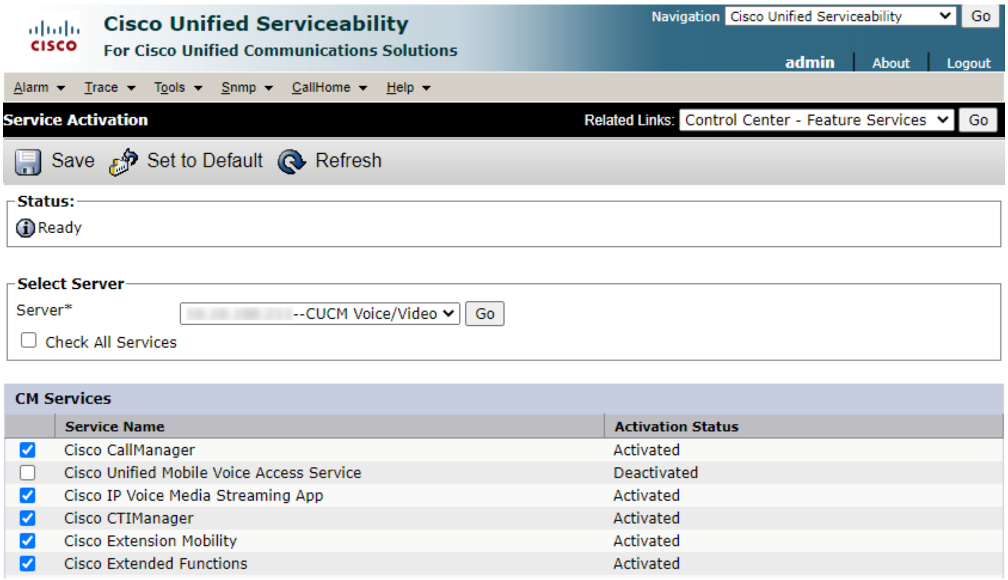
1. **Navigate to Cisco Unified Serviceability:**
   Select Cisco Unified Serviceability from the Navigation drop down list in the top-right of the page and click the Go button.



Navigation: Cisco Unified Serviceability

Figure 3-1 - Navigation

2. **Open the Service Activation page:**
   Select Tools » Service Activation on the main menu to open the **Service Activation** page, which will allow you to view all the services and their activation statuses.


Cisco Unified Serviceability
For Cisco Unified Communications Solutions
Navigation
Cisco Unified Serviceability
Go
admin
About
Logout
Alarm
Trace
Tools
Snmp
CallHome
Help
Service Activation
Related Links:
Control Center - Feature Services
Go
Save
Set to Default
Refresh

Status:
Ready

Select Server
Server* [redacted]--CUCM Voice/Video Go
□ Check All Services

CM Services

	Service Name	Activation Status
☑	Cisco CallManager	Activated
□	Cisco Unified Mobile Voice Access Service	Deactivated
☑	Cisco IP Voice Media Streaming App	Activated
☑	Cisco CTIManager	Activated
☑	Cisco Extension Mobility	Activated
☑	Cisco Extended Functions	Activated

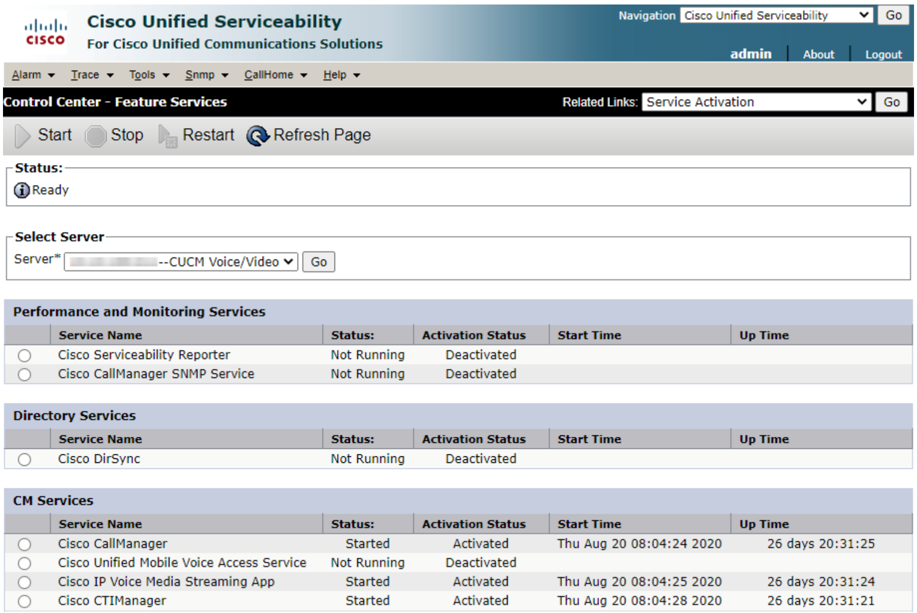
Figure 3-2 - Service Activation

3. **Enable the required services:**
   Find the required services in the list and activate them by checking the check box beside each service.

The **Cisco CTIManager** and **Cisco Extension Mobility** services can be found in the **CM Services** category and the **Cisco AXL Web Service** in the **Database and Admin Services** category.

4. **Save the changes:**
   Click the Save button.

Once the feature services have been activated, you can check that their activation status is **Activated** and status is **Started** by selecting Tools » Control Center – Feature Services from the main menu to display the Feature Services page:


Cisco Unified Serviceability
For Cisco Unified Communications Solutions
Navigation Cisco Unified Serviceability Go
admin | About | Logout
Alarm Trace Tools Snmp CallHome Help
Related Links: Service Activation Go
Start Stop Restart Refresh Page

Control Center - Feature Services

Status:
Ready

Select Server
Server* [redacted]--CUCM Voice/Video Go

Performance and Monitoring Services

	Service Name	Status:	Activation Status	Start Time	Up Time
○	Cisco Serviceability Reporter	Not Running	Deactivated		
○	Cisco CallManager SNMP Service	Not Running	Deactivated		

Directory Services

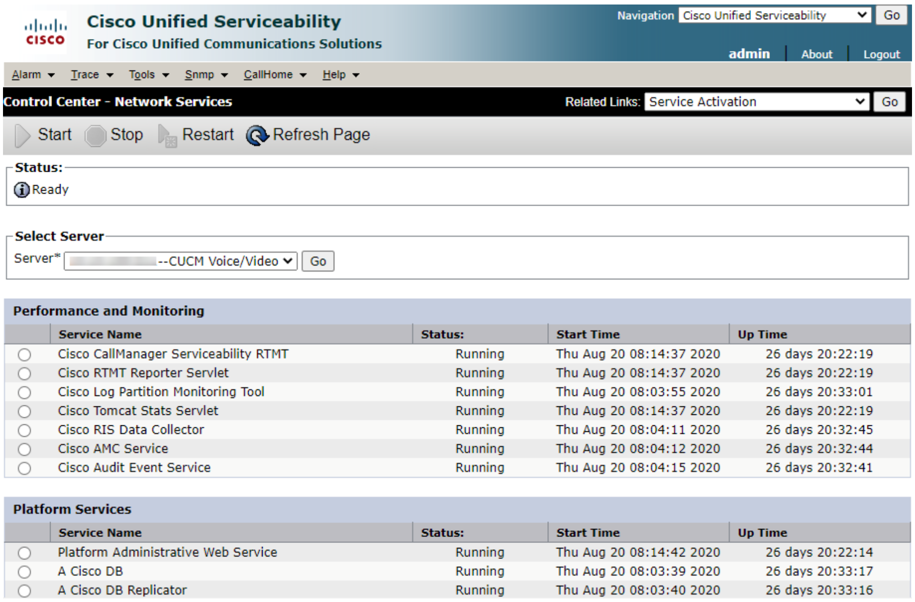
	Service Name	Status:	Activation Status	Start Time	Up Time
○	Cisco DirSync	Not Running	Deactivated		

CM Services

	Service Name	Status:	Activation Status	Start Time	Up Time
○	Cisco CallManager	Started	Activated	Thu Aug 20 08:04:24 2020	26 days 20:31:25
○	Cisco Unified Mobile Voice Access Service	Not Running	Deactivated		
○	Cisco IP Voice Media Streaming App	Started	Activated	Thu Aug 20 08:04:25 2020	26 days 20:31:24
○	Cisco CTIManager	Started	Activated	Thu Aug 20 08:04:28 2020	26 days 20:31:21

Figure 3-3 - Control Center - Feature Services

You can check the status of the Cisco RIS Data Collector service on the Network Services page by selecting Tools » Control Center – Network Services from the main menu:


Cisco Unified Serviceability
For Cisco Unified Communications Solutions
Navigation Cisco Unified Serviceability Go
admin | About | Logout
Alarm Trace Tools Snmp CallHome Help
Related Links: Service Activation Go
Start Stop Restart Refresh Page

Control Center - Network Services

Status:
Ready

Select Server
Server* [redacted]--CUCM Voice/Video Go

Performance and Monitoring

	Service Name	Status:	Start Time	Up Time
○	Cisco CallManager Serviceability RTMT	Running	Thu Aug 20 08:14:37 2020	26 days 20:22:19
○	Cisco RTMT Reporter Servlet	Running	Thu Aug 20 08:14:37 2020	26 days 20:22:19
○	Cisco Log Partition Monitoring Tool	Running	Thu Aug 20 08:03:55 2020	26 days 20:33:01
○	Cisco Tomcat Stats Servlet	Running	Thu Aug 20 08:14:37 2020	26 days 20:22:19
○	Cisco RIS Data Collector	Running	Thu Aug 20 08:04:11 2020	26 days 20:32:45
○	Cisco AMC Service	Running	Thu Aug 20 08:04:12 2020	26 days 20:32:44
○	Cisco Audit Event Service	Running	Thu Aug 20 08:04:15 2020	26 days 20:32:41

Platform Services

	Service Name	Status:	Start Time	Up Time
○	Platform Administrative Web Service	Running	Thu Aug 20 08:14:42 2020	26 days 20:22:14
○	A Cisco DB	Running	Thu Aug 20 08:03:39 2020	26 days 20:33:17
○	A Cisco DB Replicator	Running	Thu Aug 20 08:03:40 2020	26 days 20:33:16

Figure 3-4 - Control Center - Network Services

The service status should be **Running**.

Adding Required Users and Setting Permissions

PhoneView requires two types of user account to be configured in the CUCM, one for access to administrative functions and another to interact with the individual phones. Although you can configure existing accounts with the correct options, we recommend creating at least one dedicated user account of each type to use with PhoneView.

Administrative User

The PhoneView administrative user is used to extract a list of phones from the CUCM system along with some basic information for each phone such as the phone's IP Address, and for logging users in and out using the Extension Mobility service. We recommended you create the administrative user as an **Application User** and add them to the following Access Control Groups:

- Standard TabSync User
- Standard CCM Server Monitoring
- Standard EM Authentication Proxy Rights
- Standard CTI Enabled
- Standard CTI Allow Control of All Devices
- Standard CTI Allow Control of Phones supporting Connected Xfer and conf
- Standard CTI Allow Control of Phones supporting Rollover Mode

> If you plan on using the Remote Audio feature of PhoneView you'll need to add the administrative user to the **Standard CTI Allow Call Monitoring** Access Control Group as well.

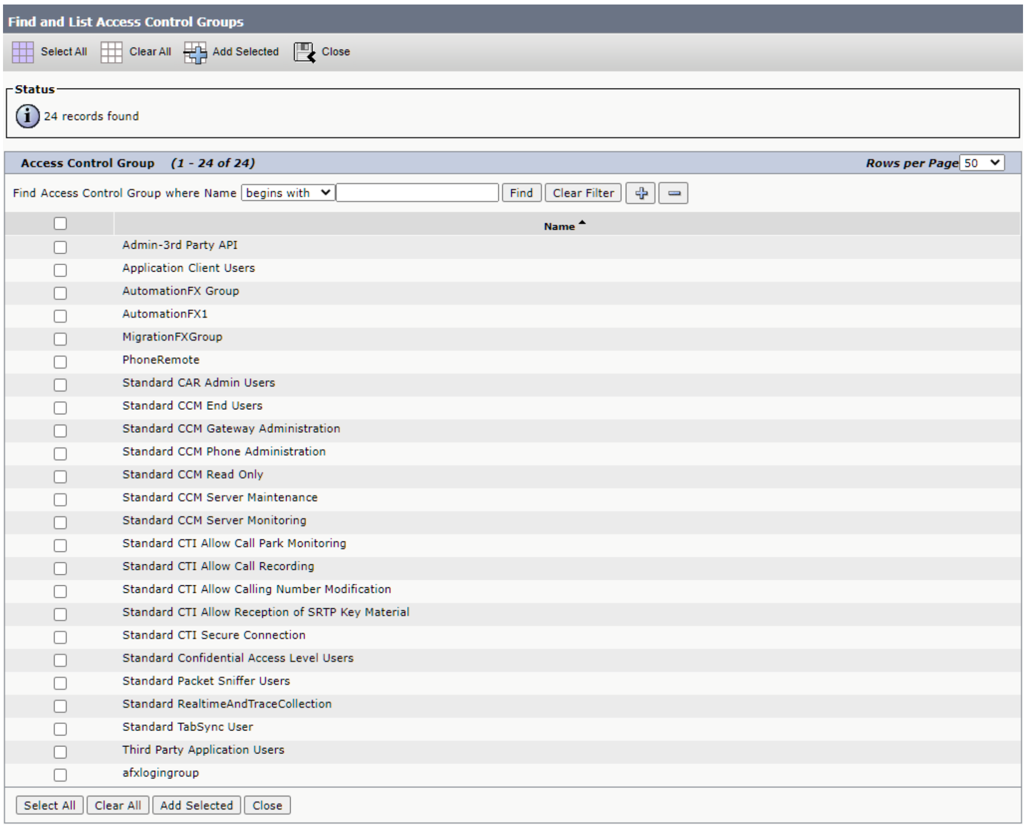
To configure the administrative user, please follow the steps below:

1. **Open the Find and List Application Users page:**
   Select User Management » Application Users from the main menu in the CUCM Administration interface to open the Find and List Application Users page. This page displays a list of the Application Users registered on the system. If the list is initially empty, click the Find button to populate the list.

2. **Create a new or select an existing user to use:**
   If you are planning to use an existing user as the PhoneView administrative user, find the user in the list and select to open the Application User Configuration page. Alternatively, click the Add New button to create a new Application User.

> If you are creating a new user to use as the PhoneView administrative user, you will need to supply credentials for the user by entering a password in the **Password** and **Confirm Password** fields on the page.

3. **Add the user to the required Access Control Groups:**
   In the **Permissions Information** section of the page, click the Add to Access Control Group button. This will open a new window containing the **Find and List Access Control Groups** page. If you do not see any Access Control Groups in the list, click the Find button to populate the list.



24 records found

Access Control Group (1 - 24 of 24) — Rows per Page 50

Find Access Control Group where Name begins with [ ] Find Clear Filter

☐	Name
☐	Admin-3rd Party API
☐	Application Client Users
☐	AutomationFX Group
☐	AutomationFX1
☐	MigrationFXGroup
☐	PhoneRemote
☐	Standard CAR Admin Users
☐	Standard CCM End Users
☐	Standard CCM Gateway Administration
☐	Standard CCM Phone Administration
☐	Standard CCM Read Only
☐	Standard CCM Server Maintenance
☐	Standard CCM Server Monitoring
☐	Standard CTI Allow Call Park Monitoring
☐	Standard CTI Allow Call Recording
☐	Standard CTI Allow Calling Number Modification
☐	Standard CTI Allow Reception of SRTP Key Material
☐	Standard CTI Secure Connection
☐	Standard Confidential Access Level Users
☐	Standard Packet Sniffer Users
☐	Standard RealtimeAndTraceCollection
☐	Standard TabSync User
☐	Third Party Application Users
☐	afxlogingroup

Figure 3-5 - Find and List Access Control Groups

   Check the checkbox next to the Access Control Groups that you want to add and then click the Add Selected button when you're done. If the Access Control Groups were added successfully to the user account they should appear in the **Groups** list box under **Permissions Information** on the **Application User Configuration** page.

4. **Save the changes:**
   Click the Save button to save the changes.

Phone User

The PhoneView phone user is used to remotely control phones and take phone screenshots. The phone user should be created as an **End User** and should be added to the following Access Control Group:

- Standard CTI Enabled

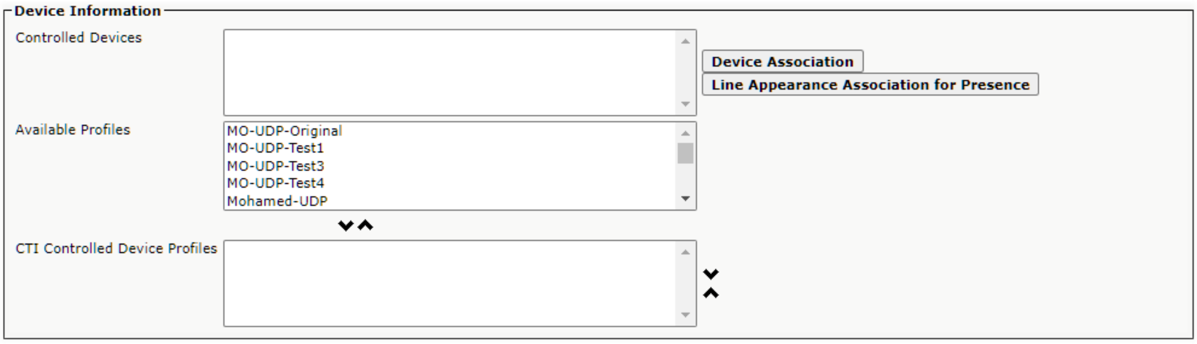
The phone user also needs a Device Association with all physical phones in the cluster.
The process to create an End User and configure the Access Control Group membership is essentially the same as for an Application User, as described in the previous section. The **Find**

and List Users page for End Users is accessed by selecting User Management » End User from the main menu.

> The Permissions Information panel is not displayed on the page used to add a new End User, so you will need to supply the basic user information then click Save to save the new user. The page will then refresh and the Permissions Information panel will now be available, and you can go ahead and add the required Access Control Group.

The devices associated with the End User are configured from the **Device Information** section of the End User Configuration page. Any phone that you want to view screenshots from or control from PhoneView must be present in the list of controlled devices, so you will need to add any phones that are not currently in the Controlled Devices list using the procedure below:

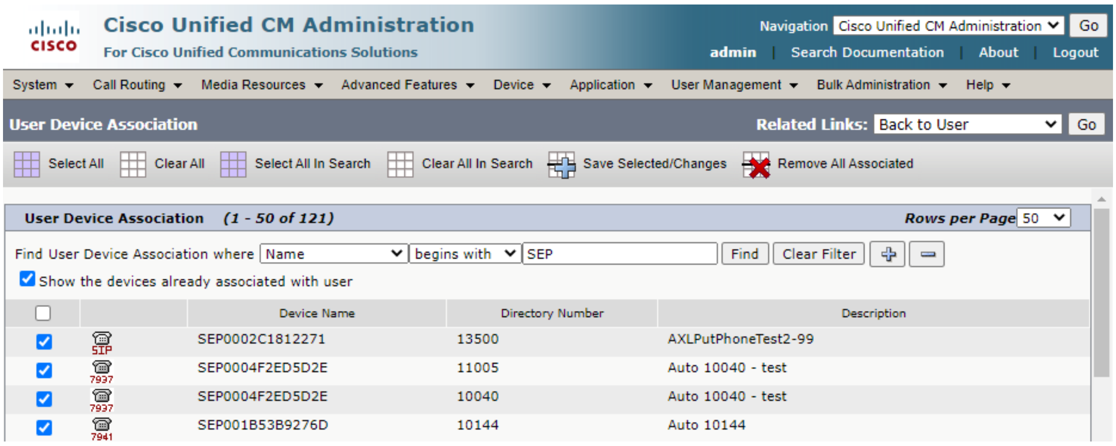
1. **Open the Device Association page:**
   Click the Device Association button on the right of the Controlled Devices list in the Device Information section. This will open the User Device Association page.



Available Profiles:
MO-UDP-Original
MO-UDP-Test1
MO-UDP-Test3
MO-UDP-Test4
Mohamed-UDP

Figure 3-6 - Device Information

2. **Select the devices to associate:**
   You can search for a specific device by entering a value in the search box, or you can list all devices by simply clicking the Find button. Select each device that you want to add by checking the checkbox next to the device in the list and save your selection by clicking the Save Selected/Changes button.


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
admin | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
User Device Association
Related Links: Back to User Go
Select All
Clear All
Select All In Search
Clear All In Search
Save Selected/Changes
Remove All Associated
Find
Clear Filter

User Device Association (1 - 50 of 121) Rows per Page 50

Find User Device Association where Name begins with SEP

☑ Show the devices already associated with user

□		Device Name	Directory Number	Description
☑	☎ SIP	SEP0002C1812271	13500	AXLPutPhoneTest2-99
☑	☎ 7937	SEP0004F2ED5D2E	11005	Auto 10040 - test
☑	☎ 7937	SEP0004F2ED5D2E	10040	Auto 10040 - test
☑	☎ 7941	SEP001B53B9276D	10144	Auto 10144

Figure 3-7 - User Device Association

We recommend only adding phones starting with “SEP” - this will ensure you only have physical phones associated and not softphones.

You can change the number of phones returned on a page of results by selecting a value from the **Rows per Page** drop down list at the top right of the results. You can also add all of the phones on a page of the list of devices by checking the checkbox in the column header of the list.

If you have added or removed an device association and there are multiple pages of devices in your list, make sure you remember to click the Save Selected/Changes button before navigating to a different page otherwise your changes will be lost.

If you have a large number of search results, it is impractical to add them one page of results at a time. You can add all phones that match your search condition (irrespective of whether they appear on the current page of results) by clicking the Select All In Search button on the toolbar and then clicking Save Selected/Changes.

3. Return to the User Configuration page and check the device associations.

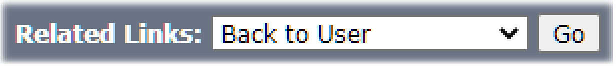


Figure 3-8 - Related Links

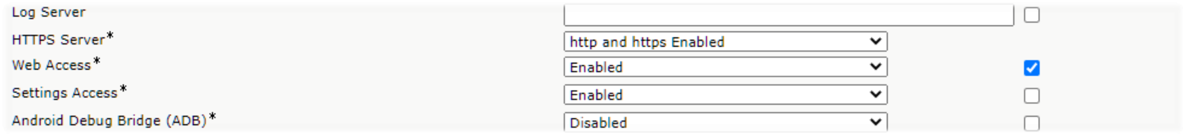
Ensure that **Back to User** is selected in the **Related Links** dropdown list and click the Go button to return to the End User Configuration page and confirm that the correct device associations are shown in the Controlled Devices list.

Enabling Phone Web Server Access

PhoneView requires access to a phone's internal web server to obtain screenshots. The Web Access setting can be enabled on an entire phone estate using the **Enterprise Phone Configuration** feature in CUCM.

1. **Open the Enterprise Phone Configuration page:**
   Select System » Enterprise Phone Configuration from the main menu in the CUCM Administration interface to open the Enterprise Phone Configuration page.

2. **Enable the Web Access setting:**
   Find the **Web Access** property in the list of configuration settings and set the value in the dropdown to **Enabled**. Check the **Override Common Settings** check box for the same property.



Log Server		□
HTTPS Server*	http and https Enabled	
Web Access*	Enabled	☑
Settings Access*	Enabled	□
Android Debug Bridge (ADB)*	Disabled	□

Figure 3-9 - Enterprise Phone Configuration

3. **Save the changes:**
   Click the Save button.

> Changing Enterprise Phone Configuration settings can cause phones to reboot or you may need to reboot the phones manually for the changes to take effect.

Setting Authentication URL Parameters

Remote control requests and pushing background images to phones require authentication. The **URL Authentication** and / or **Secured Authentication URL** Enterprise Parameters need to be configured with a URL that uses an IP Address or hostname that can be successfully resolved from the IP Phone. The value of these Enterprise Parameters can be changed by following the steps listed below:

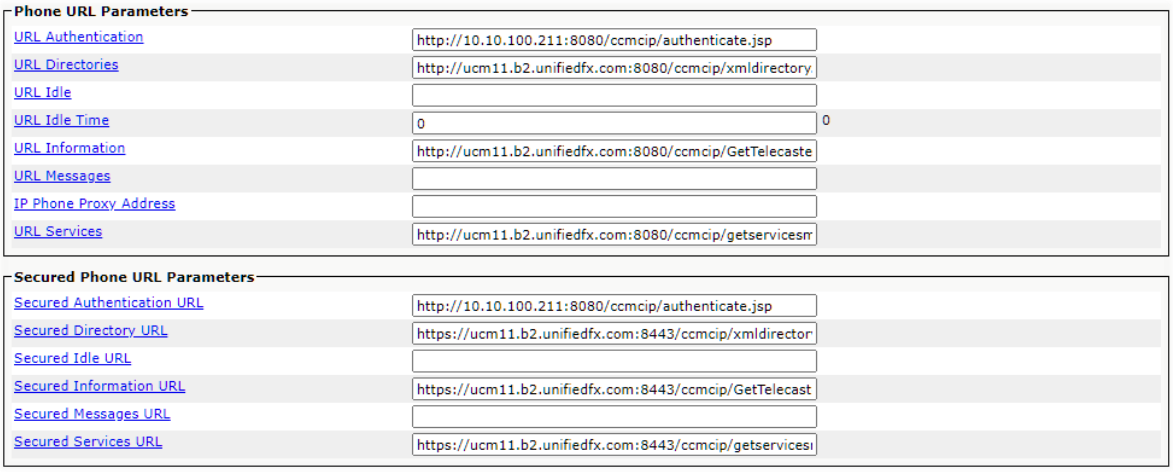
1. **Open the Enterprise Parameters Configuration page:**
   Select System » Enterprise Parameters from the main menu in the CUCM Administration interface. This will open the Enterprise Parameters Configuration page.

2. **Update the required parameter values:**
   Find the **URL Authentication** parameter on the page and change the host name part of the URL from the cluster host name to the cluster IP address.

> The default authentication URL is created when the CUCM cluster is installed, and will look something like this:
> **http:// ucm11.com:8080/ccmcip/authenticate.jsp**

Repeat this process for the **Secured Authentication URL** parameter.

The **URL Authentication** parameter can be found in the **Phone URL Parameters** section of the Enterprise Parameters Configuration page and the **Secured Authentication URL** setting in the **Secured Phone URL Parameters** section.



Phone URL Parameters

URL Authentication	http://10.10.100.211:8080/ccmcip/authenticate.jsp	
URL Directories	http://ucm11.b2.unifiedfx.com:8080/ccmcip/xmldirectory.	
URL Idle		
URL Idle Time	0	0
URL Information	http://ucm11.b2.unifiedfx.com:8080/ccmcip/GetTelecaste	
URL Messages		
IP Phone Proxy Address		
URL Services	http://ucm11.b2.unifiedfx.com:8080/ccmcip/getservicesm	

Secured Phone URL Parameters

Secured Authentication URL	http://10.10.100.211:8080/ccmcip/authenticate.jsp
Secured Directory URL	https://ucm11.b2.unifiedfx.com:8443/ccmcip/xmldirector
Secured Idle URL	
Secured Information URL	https://ucm11.b2.unifiedfx.com:8443/ccmcip/GetTelecast
Secured Messages URL	
Secured Services URL	https://ucm11.b2.unifiedfx.com:8443/ccmcip/getservicesı

Figure 3-10 - Enterprise Parameters

The values in the **Secured Phone URL Parameters** section are usually all **https://** addresses, however non-secure **http://** addresses will be accepted as valid so the value used for the **URL Authentication** parameter can simply be copied and pasted into the **Secured Authentication URL** parameter if a secure URL is not available.

3. **Save the changes:**
   Click the Save button to save the updated values.

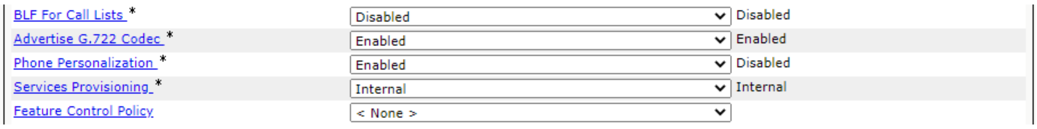
Changing Enterprise Parameters can cause phones to reboot or you may need to reboot the phones manually for the changes to take effect.

You can check whether authentication / secure authentication is working by navigating to the URL in a browser and verify that you get an **unauthorized** message.

Enabling Phone Personalization

PhoneView requires Phone Personalization to be enabled to allow background images to be pushed to phones. The parameter can be changed by following the instructions below:

1. **Open the Enterprise Parameters Configuration page:**
   Select System » Enterprise Parameters from the main menu in the CUCM Administration interface. This will open the Enterprise Parameters Configuration page.
2. **Set the Phone Personalization parameter value:**
   Find the Phone Personalization parameter and change the value to Enabled.



BLF For Call Lists *	Disabled	Disabled
Advertise G.722 Codec *	Enabled	Enabled
Phone Personalization *	Enabled	Disabled
Services Provisioning *	Internal	Internal
Feature Control Policy	< None >	

Figure 3-11 - Phone Personalization

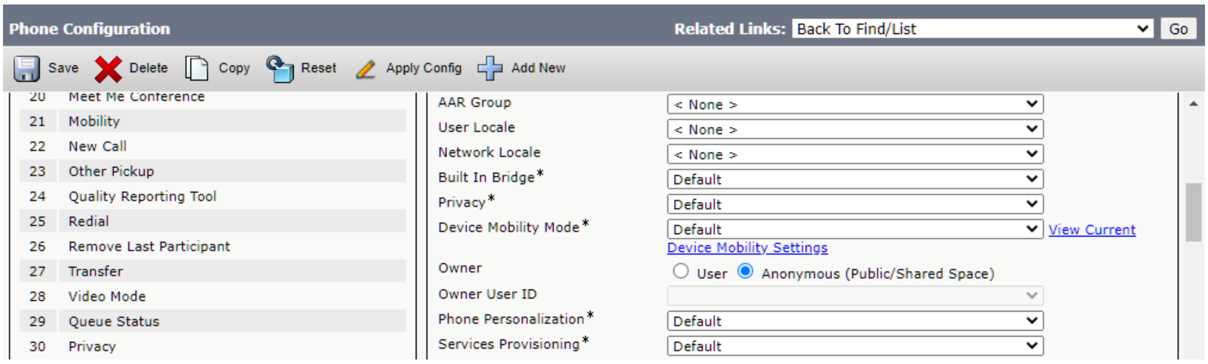
3. **Save the changes**
   Click the Save button to save the changes.

Changing Enterprise Parameters can cause phones to reboot or you may need to reboot the phones manually for the changes to take effect.

Changing Settings Per-Device

In addition to being configured at Enterprise level, the Web Access, Phone Personalization and Built-In Bridge settings can also be enabled on a per-phone basis from the Phone Configuration page for the phone - see **Turning on the Built-In Bridge** on page 23 for more information on the Built-In Bridge.
To configure the settings for a specific phone, follow the instructions below:

1. **Open the Find and List Phones page:**
   Select Device » Phone from the main menu in the CUCM Administration interface. This will open the **Find and List Phones** page.
2. **Open the Phone Configuration page:**
   Click the Find button to display the list of all available phones and find the desired phone, or search for the phone directly. Select the phone that you want to configure by clicking the Device Name hyperlink. This will open the Phone Configuration page.
3. **Enable the desired setting:**
   Find the setting that you want to change in the Device Information panel and change the value of the setting from Default to Enable.



20	Meet Me Conference
21	Mobility
22	New Call
23	Other Pickup
24	Quality Reporting Tool
25	Redial
26	Remove Last Participant
27	Transfer
28	Video Mode
29	Queue Status
30	Privacy

AAR Group	< None >
User Locale	< None >
Network Locale	< None >
Built In Bridge*	Default
Privacy*	Default
Device Mobility Mode*	Default View Current Device Mobility Settings
Owner	○ User ● Anonymous (Public/Shared Space)
Owner User ID	
Phone Personalization*	Default
Services Provisioning*	Default

Figure 3-12 - Phone Configuration

4. **Save the changes**
   Click the Save button at the top left of the page.

If you can’t find the option for Phone Personalization it may be because the selected phone model doesn’t support this feature. Check the list of supported phone models in the section on infrastructure requirements on page 7 for the selected model.

You can use the **Bulk Administration** tool to do this on multiple phones.

Configuring Remote Audio

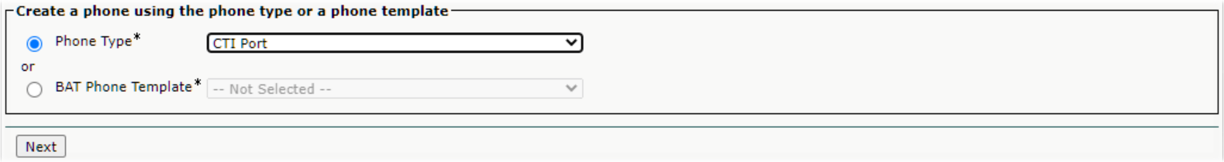
Some additional configuration is required if you have licensed and are intending to use the Remote Audio feature within PhoneView.

Creating a CTI Port

Follow the steps below to create a unique CTI port for Remote Audio monitoring:

1. **Open the Find and List Phones page:**
   Select Device » Phone from the main menu in the CUCM Administration interface. This will open the Find and List Phones page.

2. **Add a new phone:**
   Click the Add New button to open the .Add a New Phone Page. Ensure **Phone Type** is selected and select **CTI Port** from the dropdown list of values. Click Next to continue to the Phone Configuration page.



Create a phone using the phone type or a phone template

● Phone Type* CTI Port

or

○ BAT Phone Template* -- Not Selected --

Figure 3-13 - Add a New Phone

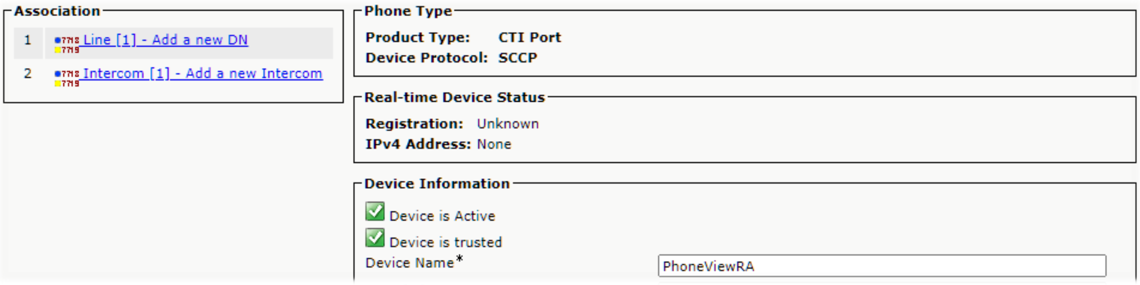
3. **Set the phone configuration options:**
   You will need to provide values for the following required parameters:
   - **Device Name**;
   - **Device Pool** – the default value is Default; you can leave this value selected or choose a different value;
   - **Owner User ID**;
   - **Device Security Profile** – set to **Cisco CTI Port – Standard SCCP Non-Secure Profile**.
4. **Save the changes:**
   Click the Save button to save the changes.

> If you intend to use multiple instances of PhoneView for Remote Audio Monitoring on the same cluster then a unique CTI Port will be required per instance of PhoneView.

Adding a DN

Follow the steps below to add a new Directory Number:

1. **Open the Find and List Phones page:**
   Select Device » Phone from the main menu in the CUCM Administration interface. This will open the Find and List Phones page.
2. **Open the Phone Configuration page for the new CTI Port device:**
   Find the CTI Port device that you just added in the list and click the **Device Name** hyperlink to open the **Phone Configuration** page for the device.



Association

1 Line [1] - Add a new DN

2 Intercom [1] - Add a new Intercom

Phone Type

Product Type: CTI Port

Device Protocol: SCCP

Real-time Device Status

Registration: Unknown

IPv4 Address: None

Device Information

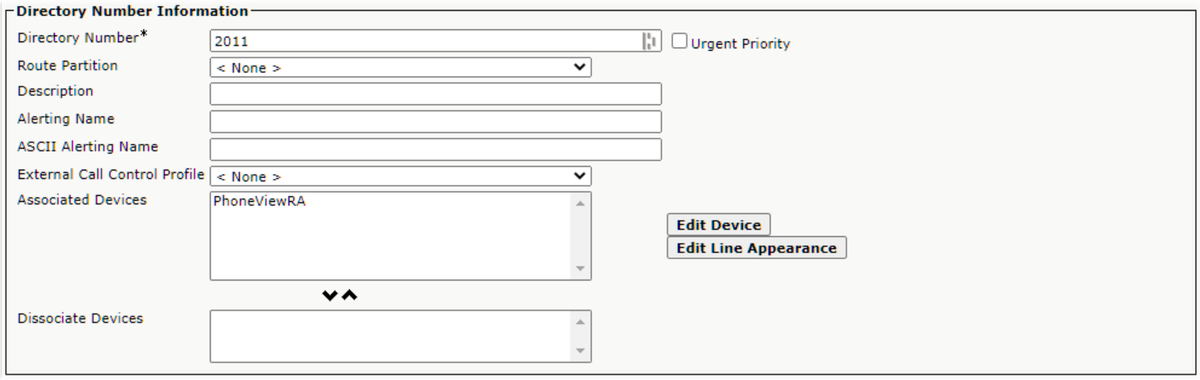
☑ Device is Active

☑ Device is trusted

Device Name* PhoneViewRA

Figure 3-14 - Phone Configuration

3. **Add a new DN:**
   In the **Association** panel on the left-hand side of the **Phone Configuration** page, click the Add a new DN hyperlink to open the **Directory Number Configuration** page.



Directory Number Information

Directory Number*	2011
Route Partition	< None >
Description	
Alerting Name	
ASCII Alerting Name	
External Call Control Profile	< None >
Associated Devices	PhoneViewRA
Dissociate Devices	

Figure 3-15 - Directory Number Configuration

4. **Set the Directory Number:**
   Enter a value for the Directory Number.

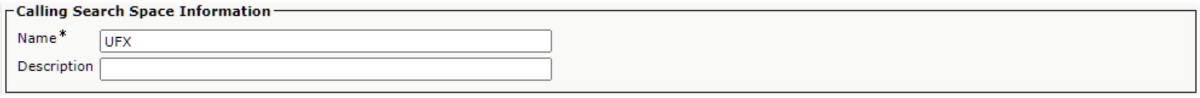
5. **Save the changes:**
   Click the Save button to save the changes.

Adding a Calling Search Space

Follow the steps below to add a new Calling Search Space:

1. **Open the Find and List Calling Search Spaces page:**
   Select Call Routing » Class of Control » Calling Search Space from the main menu in the CUCM Administration interface. This will open the Find and List Calling Search Spaces page.

2. **Add a new Calling Search Space:**
   Click the Add New button to open the Calling Search Space Configuration page and enter the required information.



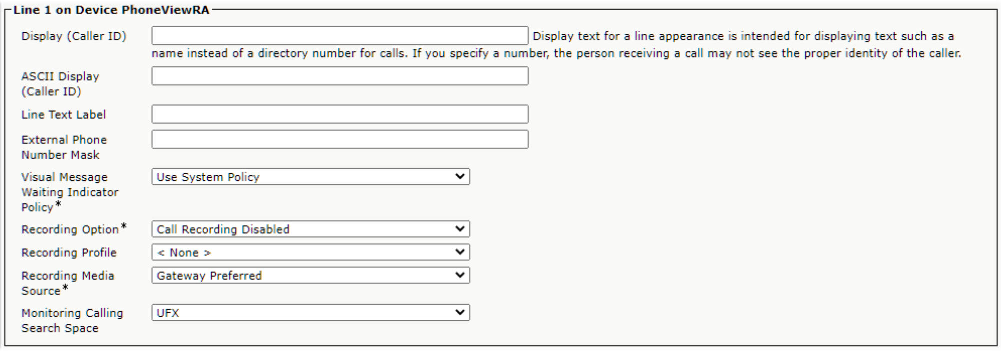
Calling Search Space Information

Name*	UFX
Description	

Figure 3-16 - Calling Search Space Configuration

3. **Save the changes:**
   Click the Save button to save the new Calling Search Space.

4. **Update the Directory Number configuration with the new Calling Search Space:**
   Navigate back to the Directory Number Configuration page of the CTI port and find the **Line <*n*> on Device <*Device Name*>** panel. Select the new Calling Search Space that you just created from the dropdown list of values for Monitoring Calling Search Space.



Line 1 on Device PhoneViewRA

Display (Caller ID)	Display text for a line appearance is intended for displaying text such as a name instead of a directory number for calls. If you specify a number, the person receiving a call may not see the proper identity of the caller.
ASCII Display (Caller ID)	
Line Text Label	
External Phone Number Mask	
Visual Message Waiting Indicator Policy*	Use System Policy
Recording Option*	Call Recording Disabled
Recording Profile	< None >
Recording Media Source*	Gateway Preferred
Monitoring Calling Search Space	UFX

Figure 3-17 - Directory Number Configuration

5. **Save the changes:**
   Click the Save button to save the changes.

Associating the CTI Port with an Administrative User

The newly created CTI Port needs to be associated with a PhoneView Administrative user.

For more information about PhoneView Administrative users, see **Adding Required Users and Setting Permissions - Administrative User** on page 12.

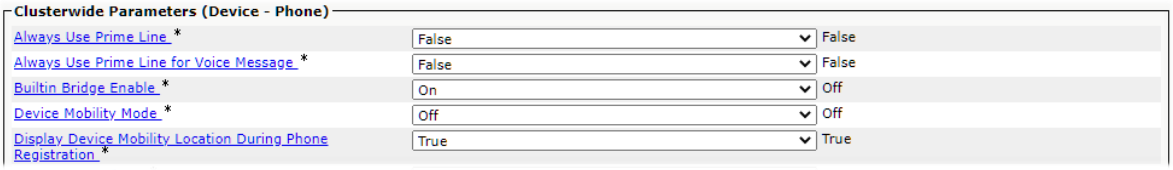
To create the Device Association, follow the steps below:

1. **Open the Find and List Application Users page:**
   Select User Management » Application Users from the main menu in the CUCM Administration interface to open the Find and List Application Users page. This page displays a list of the Application Users registered on the system. If the list is initially empty, click the Find button to populate the list.
2. **Open the Application User Configuration page for the desired user:**
   Find the Application User that you want to associate with the CTI port in the list and click on the name hyperlink to open the Application User Configuration page for the user.
3. **Open the Device Association page:**
   In the Device Information section, click the Device Association button to open the User Device Association page. Use the Find User Device Association controls to search for and display a list of results containing the new CTI Port.
4. **Select the CTI Port device to associate:**
   Select the CTI Port device by checking the checkbox next to the device in the list. Save the selection by clicking the Save Selected/Changes button.
5. **Return to the User Configuration page and save the changes:**
   Ensure that **Back to User** is selected in the **Related Links** dropdown list and click the Go button to return to the End User Configuration page. Click the Save button to save the updated user configuration.

Turning on the Built-In Bridge

The final configuration step for Remote Audio Monitoring is to set the Built-In Bridge Enable setting to On. You can do this by following the steps below:

1. **Open the Service Parameter Configuration page:**
   Select System » Service Parameters from the main menu in the CUCM Administration interface. This will open the Service Parameter Configuration page.
2. **Select the required Server and Service:**
   Select the server that you want to work with from the dropdown list of servers, and then select **Cisco Call Manager** from the dropdown list of services.
3. **Enable the Built-In Bridge**
   Find the **Clusterwide Parameters (Device - Phone)** section on the page and set the **Built-In Bridge Enable** parameter value to **On**.



Clusterwide Parameters (Device - Phone)

Always Use Prime Line *	False	False
Always Use Prime Line for Voice Message *	False	False
Builtin Bridge Enable *	On	Off
Device Mobility Mode *	Off	Off
Display Device Mobility Location During Phone Registration *	True	True

Figure 3-18 - Service Parameter Configuration - Clusterwide Parameters (Device – Phone)

4. **Save the changes:**
   Click Save to save the changes.

Changing Service Parameters can cause phones to reboot or you may need to reboot the phones manually for the changes to take effect.

The Built-In Bridge can also be enabled on a per-device basis. See **Changing Settings Per-Device** on page 18 for more details.

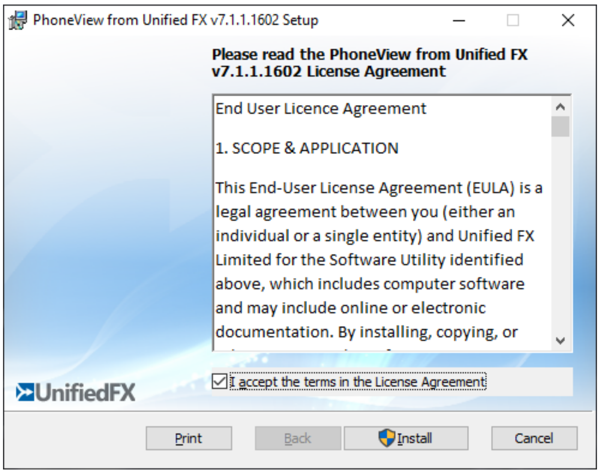
Downloading and Installing PhoneView

PhoneView is distributed as a Windows Installer package that installs the application components on your Window system. Follow the steps below to download and install PhoneView on your system. If you have already downloaded the Windows Installer .msi file, you can skip steps 1 & 2.

1. **Sign in to the UnifiedFX website**
   Go to the UnifiedFX website at https://www.unifiedfx.com/ and sign in using your UnifiedFX username and password.

2. **Download the latest PhoneView installer package**
   Navigate to the PhoneView Download page and use the button to download the latest installer package.

3. **Start the PhoneView Installer**
   Locate the downloaded .msi file and double-click it to run the installer.



Please read the PhoneView from Unified FX v7.1.1.1602 License Agreement

End User Licence Agreement

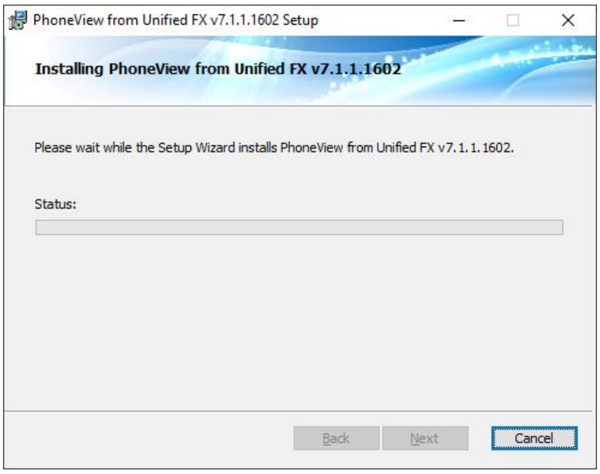
1. SCOPE & APPLICATION

This End-User License Agreement (EULA) is a legal agreement between you (either an individual or a single entity) and Unified FX Limited for the Software Utility identified above, which includes computer software and may include online or electronic documentation. By installing, copying, or

☑ I accept the terms in the License Agreement

Figure 4-1 PhoneView Installer – EULA

4. **Accept the End User License Agreement (EULA)**
   Read the EULA and click the checkbox to indicate that you accept the terms of the agreement. Click the Install button to start the installation process.



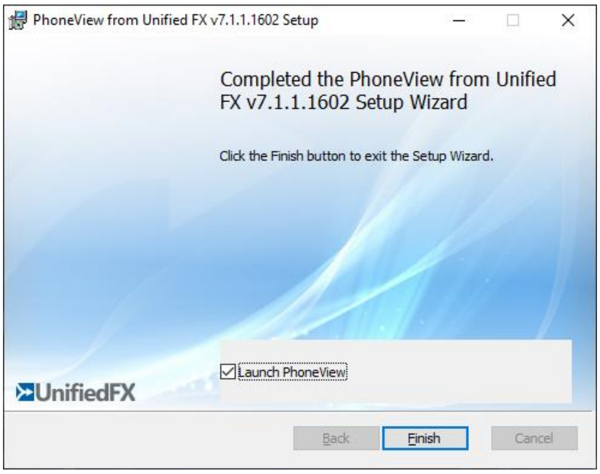
Installing PhoneView from Unified FX v7.1.1.1602

Please wait while the Setup Wizard installs PhoneView from Unified FX v7.1.1.1602.

Status:

Figure 4-2 PhoneView Installer - Installation Progress

While the installation is in progress, the installer window will provide feedback.



Completed the PhoneView from Unified FX v7.1.1.1602 Setup Wizard

Click the Finish button to exit the Setup Wizard.

☑ Launch PhoneView

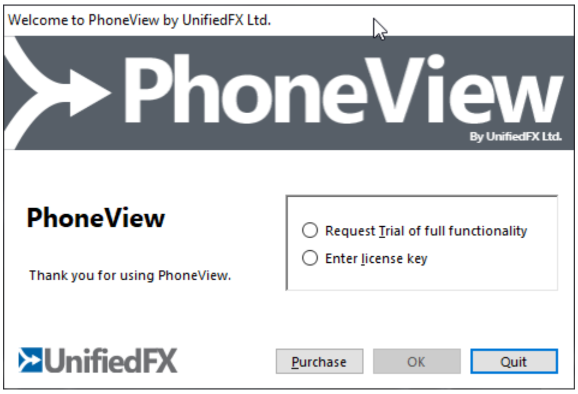
Figure 4-3 PhoneView Installer - Finish

5. **Finish the installation**
   Once the installation is complete, click Finish to close the installer.

You can start PhoneView right after the installer is closed by selecting the Launch PhoneView checkbox before you click the Finish button.

Activating PhoneView

Before you can start using PhoneView, the software must be activated by installing a valid license. If PhoneView detects that no valid license is installed, a Welcome dialog box will be displayed that will allow you to request a trial, arrange to purchase a license key or enter an existing key.


Welcome to PhoneView by UnifiedFX Ltd.

PhoneView

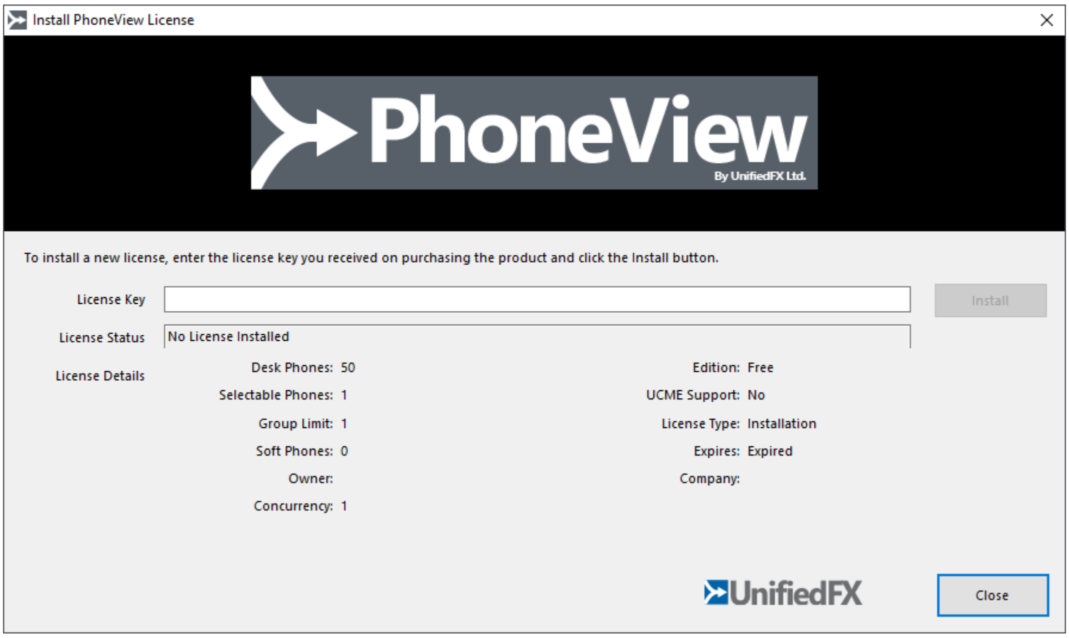
Thank you for using PhoneView.

○ Request Trial of full functionality
○ Enter license key

Figure 4-4 - License Selection Dialog

If you already have a valid license key, select the Enter license key option and click the OK button to continue.

Online Activation


Install PhoneView License

To install a new license, enter the license key you received on purchasing the product and click the Install button.

License Key

License Status: No License Installed

License Details

Desk Phones:	50	Edition:	Free
Selectable Phones:	1	UCME Support:	No
Group Limit:	1	License Type:	Installation
Soft Phones:	0	Expires:	Expired
Owner:		Company:	
Concurrency:	1		

Figure 4-5 - License Details Dialog

If you already have a license key for PhoneView and your PC is connected to the Internet, you can activate the software by simply entering the license key in the box and clicking the Install button. PhoneView will contact the UnifiedFX licensing servers on the Internet to verify the license key, retrieve your license details, and display them.

PhoneView requires both inbound and outbound access to the following addresses and ports for automatic license activation to succeed:

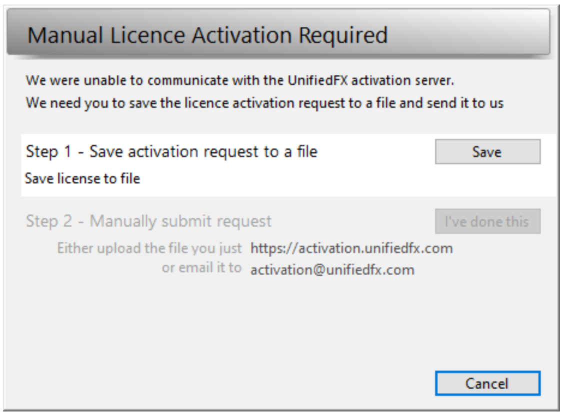
- **wyday.com** (80 & 443), and;
- **licensing.unifiedfx.com** (80 & 443).

Once your license key has been installed and validated, you can close the dialog by clicking the Close button.

Offline Activation

If the computer that you intend to use to run PhoneView does not have an active connection to the Internet or access to the license servers is blocked by your firewall, the license key will not be able to be validated automatically and you will need to follow an alternative process to activate your license manually.

1. **Create an activation request**



Manual Licence Activation Required

We were unable to communicate with the UnifiedFX activation server.
We need you to save the licence activation request to a file and send it to us

Step 1 - Save activation request to a file

Save license to file

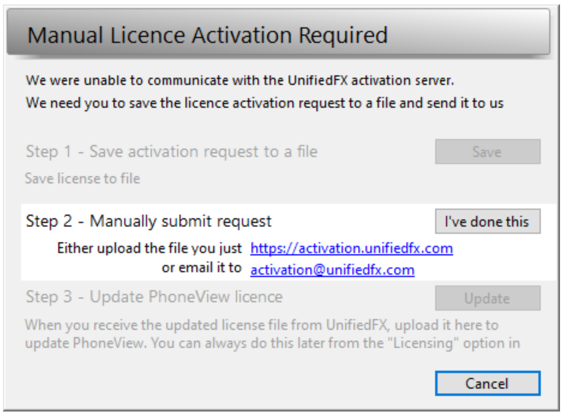
Step 2 - Manually submit request

Either upload the file you just https://activation.unifiedfx.com
or email it to activation@unifiedfx.com

Figure 4-6 - Manual License Activation Dialog - Step 1

Click on the Save button to generate a manual license activation request file *ActivationRequest.xml* and save it to a location on your device. Ensure you note where you save the file as you will need the file for the next step.

2. **Submit the activation request for authorisation.**
Open your web browser and navigate to the UnifiedFX Offline License Activation page at the URL displayed in the dialog. Follow the instructions on the page to upload the file created in the previous step for authorisation. Once the activation request file has been uploaded, the page will automatically create and download a license activation file *ActivationRequest_Activated.xml*. Note where this file is saved as you will need the file for the next step.



Manual Licence Activation Required

We were unable to communicate with the UnifiedFX activation server.
We need you to save the licence activation request to a file and send it to us

Step 1 - Save activation request to a file
Save license to file

Step 2 - Manually submit request
Either upload the file you just https://activation.unifiedfx.com
or email it to activation@unifiedfx.com

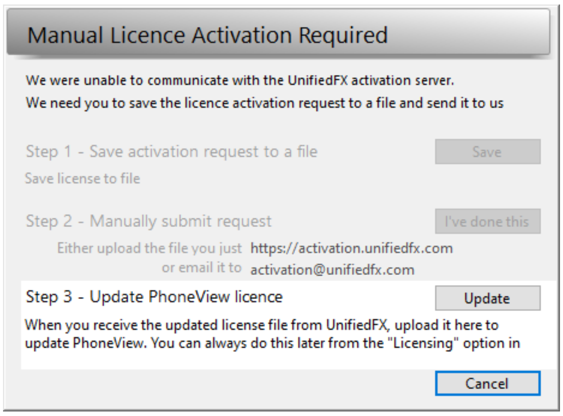
Step 3 - Update PhoneView licence
When you receive the updated license file from UnifiedFX, upload it here to update PhoneView. You can always do this later from the "Licensing" option in

Figure 4-7 - Manual License Activation Dialog - Step 2

If for any reason you can't access the UnifiedFX Offline License Activation page, the license key owner can also email the *ActivationRequest.xml* file created in step 1 from their registered email address to activation@unifiedfx.com and the activation file will be sent back to the registered address.

When you have a license activation file, click on the I've done this button to move on to the next step.

3. **Import the validated PhoneView license.**



Manual Licence Activation Required

We were unable to communicate with the UnifiedFX activation server.
We need you to save the licence activation request to a file and send it to us

Step 1 - Save activation request to a file
Save license to file

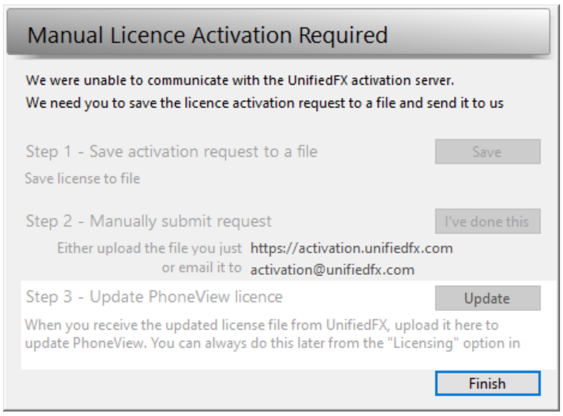
Step 2 - Manually submit request
Either upload the file you just https://activation.unifiedfx.com
or email it to activation@unifiedfx.com

Step 3 - Update PhoneView licence
When you receive the updated license file from UnifiedFX, upload it here to update PhoneView. You can always do this later from the "Licensing" option in

Figure 4-8 - Manual License Activation Dialog - Step 3

Click on the Update button and select the license activation file you obtained in step 2 to import it and update the stored PhoneView license details.

4. Close the dialog.



Manual Licence Activation Required

We were unable to communicate with the UnifiedFX activation server.
We need you to save the licence activation request to a file and send it to us

Step 1 - Save activation request to a file

Save license to file

Step 2 - Manually submit request

Either upload the file you just https://activation.unifiedfx.com
or email it to activation@unifiedfx.com

Step 3 - Update PhoneView licence

When you receive the updated license file from UnifiedFX, upload it here to update PhoneView. You can always do this later from the "Licensing" option in

Figure 4-9 - Manual License Activation Dialog – Completed

Click the Finish button to close the dialog.

Your license information may not show up immediately in the License Details dialog – if this happens, simply close any open dialogs and exit PhoneView. When you restart PhoneView, your license should be installed. You can check the status and details of your license at any time by selecting Help » Licensing from the main PhoneView menu.

Cluster Configuration

Overview

Before you can start working with PhoneView, you need to set up and configure your cluster details so that PhoneView can access your devices.

PhoneView stores cluster configuration information in its own proprietary file format with a *.pvd* file extension.

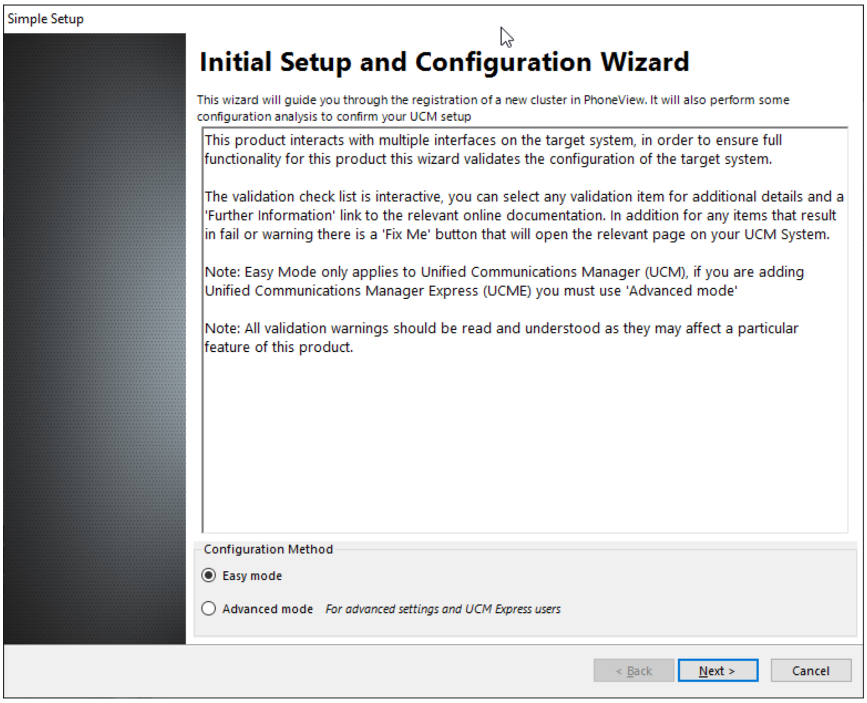
PhoneView has a step-by-step wizard-based Easy configuration mode to simplify the initial set up, although an Advanced Mode that gives you access to all the settings is also available.

The Easy Mode setup wizard can only be used if the cluster that you're adding is on Cisco Unified Communications Manager (CUCM). If the cluster is Unified Communications Manager Express (UCME), you will need to use Advanced Mode.

Adding a Cluster in Easy Mode

Follow the steps below

1. **Start the Configuration Wizard:**
   Select File » New... from the PhoneView main menu to start the Initial Setup / Configuration Wizard.



Initial Setup and Configuration Wizard

This wizard will guide you through the registration of a new cluster in PhoneView. It will also perform some configuration analysis to confirm your UCM setup

This product interacts with multiple interfaces on the target system, in order to ensure full functionality for this product this wizard validates the configuration of the target system.

The validation check list is interactive, you can select any validation item for additional details and a 'Further Information' link to the relevant online documentation. In addition for any items that result in fail or warning there is a 'Fix Me' button that will open the relevant page on your UCM System.

Note: Easy Mode only applies to Unified Communications Manager (UCM), if you are adding Unified Communications Manager Express (UCME) you must use 'Advanced mode'

Note: All validation warnings should be read and understood as they may affect a particular feature of this product.

Configuration Method

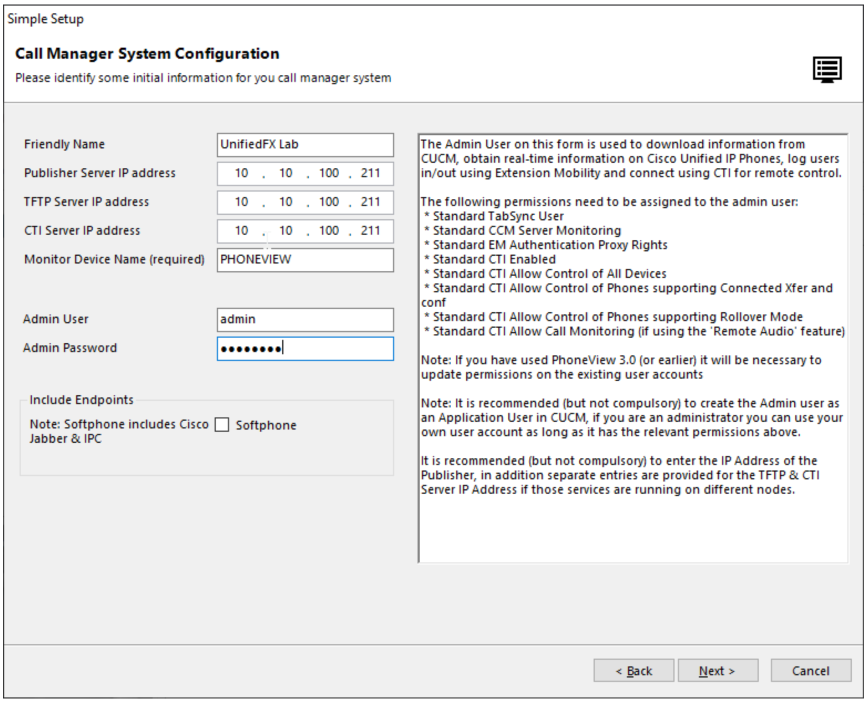
● Easy mode

○ Advanced mode *For advanced settings and UCM Express users*

Figure 5-1 - Initial Setup and Configuration Wizard

2. **Choose between Easy or Advanced mode:**
   Select the Easy mode option and click the Next > button to advance to the main Call Manager Configuration page.

3. **Enter the CUCM configuration information:**



Call Manager System Configuration

Please identify some initial information for you call manager system

Friendly Name: UnifiedFX Lab

Publisher Server IP address: 10 . 10 . 100 . 211

TFTP Server IP address: 10 . 10 . 100 . 211

CTI Server IP address: 10 . 10 . 100 . 211

Monitor Device Name (required): PHONEVIEW

Admin User: admin

Admin Password: ••••••••

Include Endpoints

Note: Softphone includes Cisco Jabber & IPC □ Softphone

The Admin User on this form is used to download information from CUCM, obtain real-time information on Cisco Unified IP Phones, log users in/out using Extension Mobility and connect using CTI for remote control.

The following permissions need to be assigned to the admin user:
* Standard TabSync User
* Standard CCM Server Monitoring
* Standard EM Authentication Proxy Rights
* Standard CTI Enabled
* Standard CTI Allow Control of All Devices
* Standard CTI Allow Control of Phones supporting Connected Xfer and conf
* Standard CTI Allow Control of Phones supporting Rollover Mode
* Standard CTI Allow Call Monitoring (if using the 'Remote Audio' feature)

Note: If you have used PhoneView 3.0 (or earlier) it will be necessary to update permissions on the existing user accounts

Note: It is recommended (but not compulsory) to create the Admin user as an Application User in CUCM, if you are an administrator you can use your own user account as long as it has the relevant permissions above.

It is recommended (but not compulsory) to enter the IP Address of the Publisher, in addition separate entries are provided for the TFTP & CTI Server IP Address if those services are running on different nodes.

Figure 5-2 - Call Manager System Configuration

Some of the options displayed on this page of the wizard may vary depending on the particular edition of PhoneView that you have installed and on the specifics of your license.

You will need to supply values for the following configuration settings on the cluster configuration page:

- **Friendly Name**
  This will be the name that PhoneView uses to identify your cluster.
- **Publisher Server IP Address**
  The IP Address of the CUCM server.

If you don't supply values for the TFTP Server IP Address and CTI Server IP Address settings, these values will be automatically set to be the same as the Publisher Server IP Address.

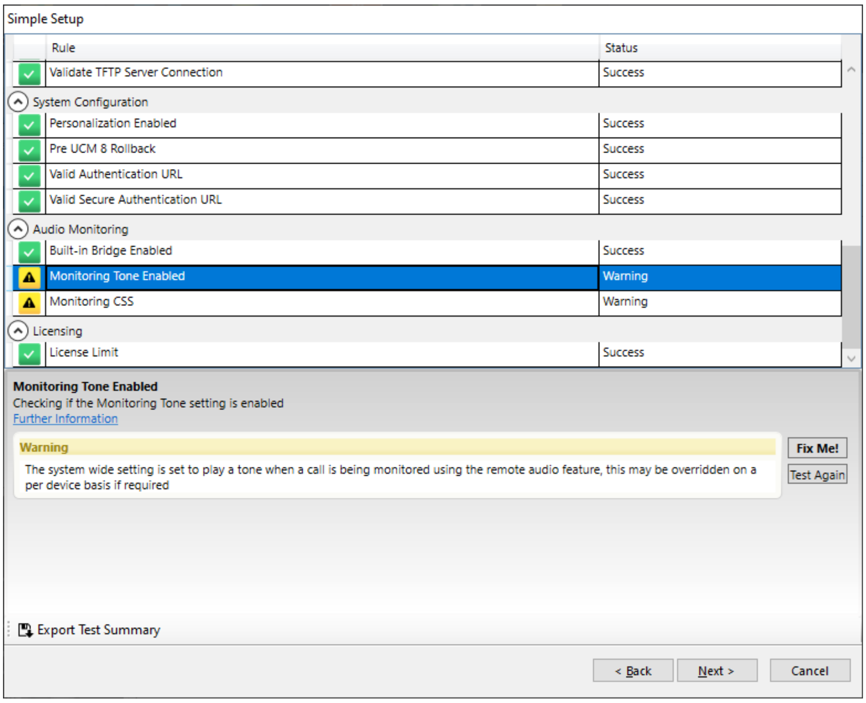
- **Administrative User Credentials**
  The username and password of the PhoneView administrative user.

The panel on the right of the wizard describes the permissions required by the Administrative User – see **Adding Required Users and Setting Permissions - Administrative User** on page 12 for further information.

When all the required information has been entered click the Next > button to validate the configuration and advance to the next page of the wizard.

Adding a completely new cluster updates the details in your PhoneView license, so access to the UnifiedFX licensing servers is required – see the information box in **Activating PhoneView - Online Activation** on page 26 for the addresses and ports required.
If you don't have access to the internet or access to the license servers is blocked by your firewall, you will need to activate the cluster manually using the offline activation procedure – see **Offline Cluster Activation** on page 36 for more information.

4. **Review the setup validation checklist:**



Simple Setup

	Rule	Status
✓	Validate TFTP Server Connection	Success
System Configuration		
✓	Personalization Enabled	Success
✓	Pre UCM 8 Rollback	Success
✓	Valid Authentication URL	Success
✓	Valid Secure Authentication URL	Success
Audio Monitoring		
✓	Built-in Bridge Enabled	Success
⚠	Monitoring Tone Enabled	Warning
⚠	Monitoring CSS	Warning
Licensing		
✓	License Limit	Success

Monitoring Tone Enabled
Checking if the Monitoring Tone setting is enabled
Further Information

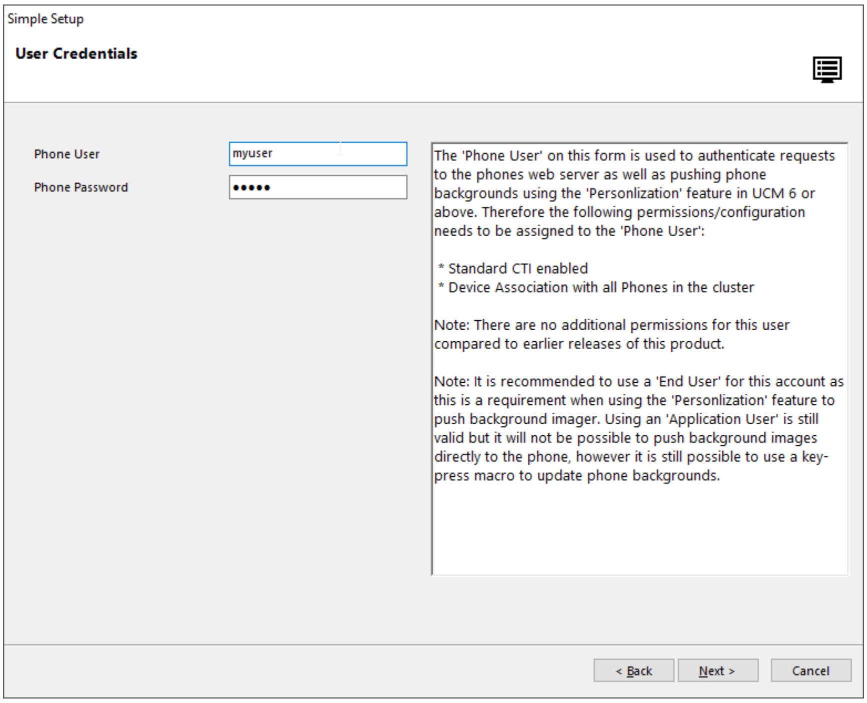
Warning
The system wide setting is set to play a tone when a call is being monitored using the remote audio feature, this may be overridden on a per device basis if required

Figure 5-3 - Simple Setup Validation Checklist

The wizard will now perform a series of rule-based checks and tests to verify the configuration and authenticate the credentials entered with the CUCM. The name of each validation rule is displayed in the checklist along with the status of the test.
The validation checklist is interactive - you can select any validation rule item from the checklist and additional details about the rule will be displayed in the pane below the checklist, along with a link to get further information about the Rule.
If for any reason the check fails, or there is a problem communicating with the CUCM, a warning / error message will be displayed. You can click the Fix Me! button to attempt to rectify the problem and / or click the Test Again button to re-execute the validation rule.
If you are happy with the results of the validation checklist, click the Next > button to advance to the next page of the wizard.

5. **Set up the Phone User credentials:**
Enter the username and password for the PhoneView Phone User.

The panel on the right of the wizard describes the permissions required by the Phone User - see **Adding Required Users and Setting Permissions - Phone User** on page 13 for further information.



Simple Setup

User Credentials

Phone User: myuser

Phone Password: •••••

The 'Phone User' on this form is used to authenticate requests to the phones web server as well as pushing phone backgrounds using the 'Personlization' feature in UCM 6 or above. Therefore the following permissions/configuration needs to be assigned to the 'Phone User':

* Standard CTI enabled
* Device Association with all Phones in the cluster

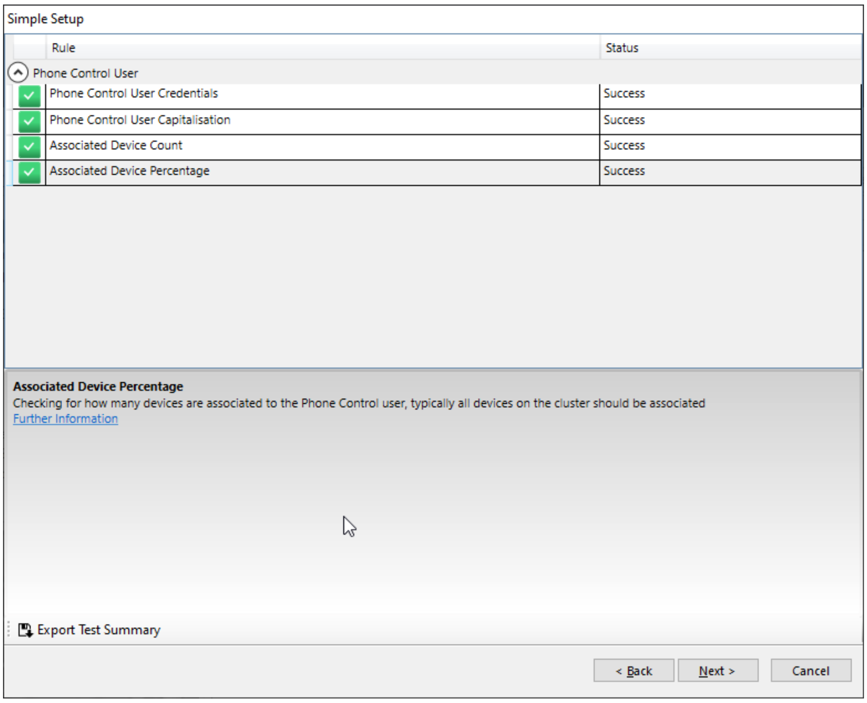
Note: There are no additional permissions for this user compared to earlier releases of this product.

Note: It is recommended to use a 'End User' for this account as this is a requirement when using the 'Personlization' feature to push background imager. Using an 'Application User' is still valid but it will not be possible to push background images directly to the phone, however it is still possible to use a key-press macro to update phone backgrounds.

Figure 5-4 - Phone User Credentials

Click the Next > button to continue.

6. **Review the Phone User setup checklist:**



Simple Setup

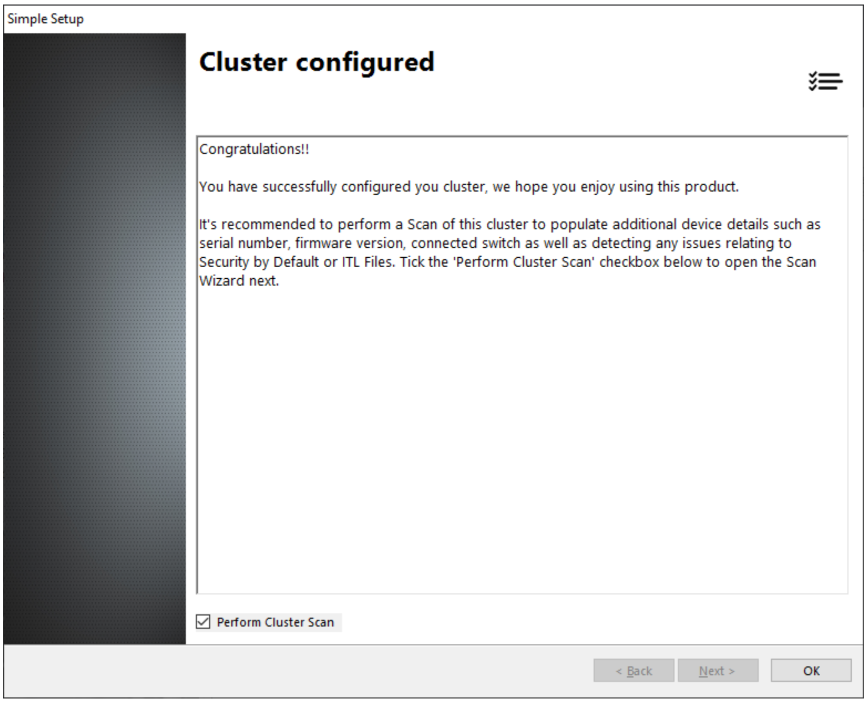
	Rule	Status
	Phone Control User	
✓	Phone Control User Credentials	Success
✓	Phone Control User Capitalisation	Success
✓	Associated Device Count	Success
✓	Associated Device Percentage	Success

Associated Device Percentage
Checking for how many devices are associated to the Phone Control user, typically all devices on the cluster should be associated
Further Information

Figure 5-5 - Phone Control User Validation Checklist

Review the validation rule results. If you are content with the results of the validation checklist, click the Next > button to advance to the final page of the wizard.

7. **Complete the setup wizard:**



Cluster configured

Congratulations!!

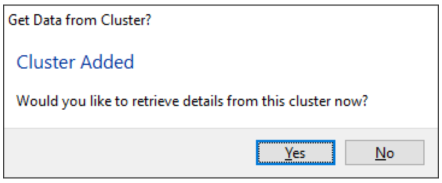
You have successfully configured you cluster, we hope you enjoy using this product.

It's recommended to perform a Scan of this cluster to populate additional device details such as serial number, firmware version, connected switch as well as detecting any issues relating to Security by Default or ITL Files. Tick the 'Perform Cluster Scan' checkbox below to open the Scan Wizard next.

☑ Perform Cluster Scan

Figure 5-6 - Simple Setup Wizard Final Page

Uncheck the Perform Cluster Scan check box and click the OK button to complete the wizard. PhoneView will prompt you to get the cluster data – click Yes to retrieve the data and populate the list of devices.



Cluster Added

Would you like to retrieve details from this cluster now?

Figure 5-7 - Cluster Data Confirmation Message Box

You should now be able to see all of the devices in the cluster in the PhoneView interface.

Whenever you add or make changes to a cluster, we recommend doing a group update by selecting Group » Update » [Cluster] from the main menu.

Ensure that there are no actions currently executing in the activity log before you attempt a Group Update otherwise the update will not succeed.

To enable viewing of actual phone screens in the Screen View, click the Phone Screenshot toolbar button and select Automatic Screenshot from the dropdown menu.

Offline Cluster Activation

Cluster activation is effectively making a change to your PhoneView license, so the offline process for cluster activation is essentially the same as that described in **Activating PhoneView - Offline Activation** on page 27, with a few key differences:

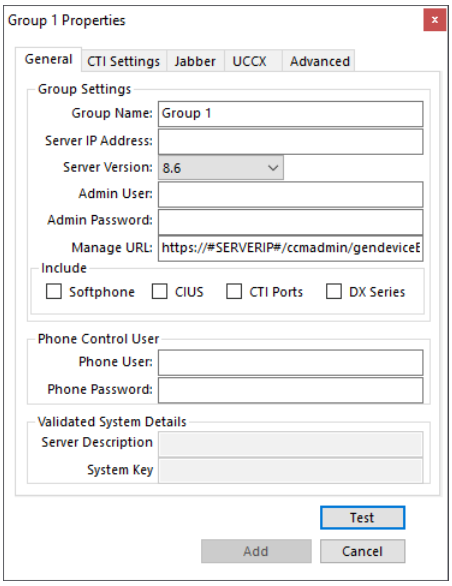
- The activation request file created is a cluster activation request, *ClusterActivationRequest.xml*;
- When you upload the file on the UnifiedFX Offline License Activation page, you will be required to enter the Cluster PIN to activate the changes to the license; and
- The response file will be created as *ClusterActivationRequest_Activated.xml*.

If you don't have the Cluster PIN, you should be able to obtain it from the registered license key owner – it will have been provided to them when they received the initial email containing their license key.
If the original email has been lost or misplaced, the registered license key owner can submit a request to the UnifiedFX support team to have it re-issued.

Advanced Mode

Unlike the Easy Mode for cluster configuration, in Advanced Mode there is little or no guidance as to what is required to configure a cluster. Instead of the step-by-step wizard, the cluster properties are presented in a simple, tabbed property page dialog interface similar to that used for file or folder properties in Windows. A Test button is provided on the dialog, however in contrast to the extensive set of validation rules executed in Easy Mode, only a simple connectivity check is carried out.
The dialog consists of five pages: **General**, **CTI Settings**, **Jabber**, **UCCX** and **Advanced**.

Cluster Properties - General Tab



Group Settings

Group Name: Group 1

Server IP Address:

Server Version: 8.6

Admin User:

Admin Password:

Manage URL: https://#SERVERIP#/ccmadmin/gendeviceE

Include

□ Softphone □ CIUS □ CTI Ports □ DX Series

Phone Control User

Phone User:

Phone Password:

Validated System Details

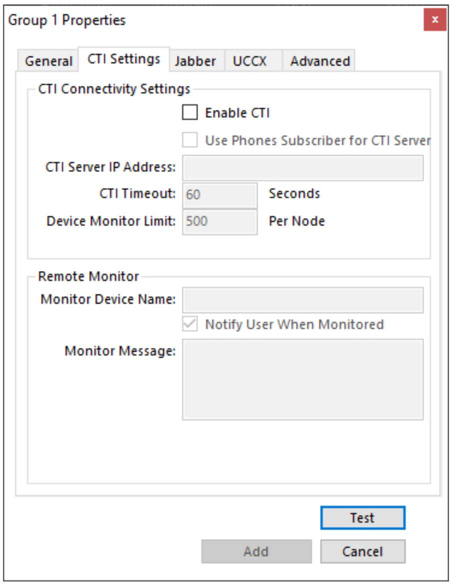
Server Description

System Key

Figure 5-8 - Cluster Properties - General

The **General** property page contains the main cluster configuration information: the Group Name (called the Friendly Name in the Easy Mode wizard), the CUCM server address and the credential information for the PhoneView Administrative and Phone users.

Cluster Properties – CTI Settings Tab



CTI Connectivity Settings

□ Enable CTI

□ Use Phones Subscriber for CTI Server

CTI Server IP Address:

CTI Timeout: 60 Seconds

Device Monitor Limit: 500 Per Node

Remote Monitor

Monitor Device Name:

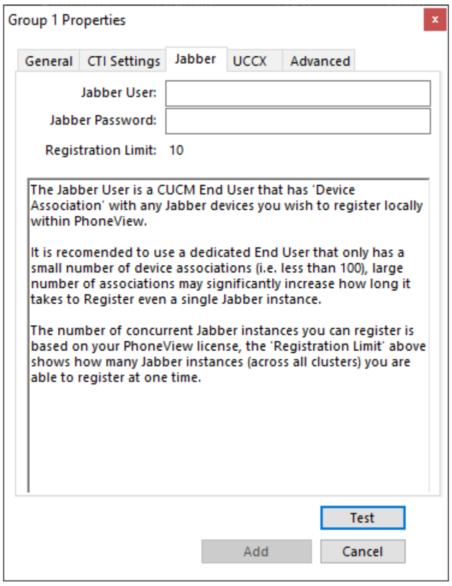
☑ Notify User When Monitored

Monitor Message:

Figure 5-9 - Cluster Properties - CTI Settings

The CTI Settings property page contains the settings to configure CTI connectivity, including additional settings for Remote Monitoring that are not available when using the Easy Mode.

Cluster Properties – Jabber Tab



Jabber User:

Jabber Password:

Registration Limit: 10

The Jabber User is a CUCM End User that has 'Device Association' with any Jabber devices you wish to register locally within PhoneView.

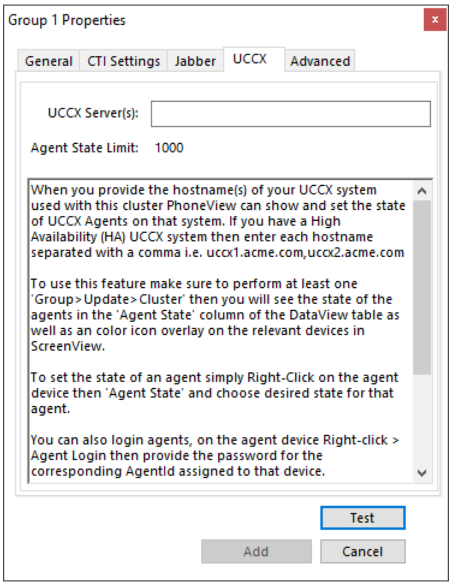
It is recomended to use a dedicated End User that only has a small number of device associations (i.e. less than 100), large number of associations may significantly increase how long it takes to Register even a single Jabber instance.

The number of concurrent Jabber instances you can register is based on your PhoneView license, the 'Registration Limit' above shows how many Jabber instances (across all clusters) you are able to register at one time.

Figure 5-10 - Cluster Properties - Jabber

The **Jabber** property page allows you to specify the CUCM End User associated with any Jabber devices that you intend to register within PhoneView.

Cluster Properties – UCCX Tab



UCCX Server(s):

Agent State Limit: 1000

When you provide the hostname(s) of your UCCX system used with this cluster PhoneView can show and set the state of UCCX Agents on that system. If you have a High Availability (HA) UCCX system then enter each hostname separated with a comma i.e. uccx1.acme.com,uccx2.acme.com

To use this feature make sure to perform at least one 'Group>Update>Cluster' then you will see the state of the agents in the 'Agent State' column of the DataView table as well as an color icon overlay on the relevant devices in ScreenView.

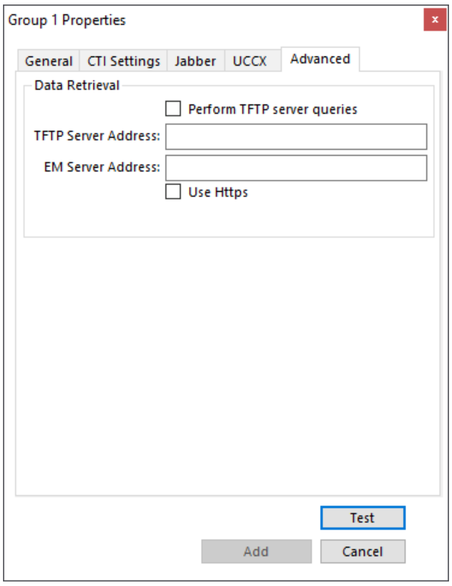
To set the state of an agent simply Right-Click on the agent device then 'Agent State' and choose desired state for that agent.

You can also login agents, on the agent device Right-click > Agent Login then provide the password for the corresponding AgentId assigned to that device.

Figure 5-11 - Cluster Properties - UCCX

The UCCX property page allows you to link your UCCX system with PhoneView, enabling the ability to display and change the Agent State against an associated device and log agents in and / or out from within the PhoneView user interface.

Cluster Properties – Advanced Tab



Group 1 Properties

□ Perform TFTP server queries

TFTP Server Address:

EM Server Address:

□ Use Https

Figure 5-12 - Cluster Properties - Advanced

The Advanced property page allows you to specify server addresses used for retrieving additional data, *e.g.* .TFTP Server.