



PhoneFX Installation & Admin 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 TM or [®] trademarks of their respective owners. Windows is a trademark of Microsoft Corporation.

Document authored by Mohamed Aquib

Document revision: 7.1

Document issued: March 2020

Copyright © UnifiedFX Limited, 2020.

All rights reserved.

Contents

Overview	5
Document Conventions.....	5
Requirements.....	6
System.....	6
Unified Communications Manager	6
Network Connectivity	6
AutomationFX Installation	7
CUCM Integration	10
Cluster Setup in AutomationFX.....	10
Automatic Cluster Setup.....	10
Manual Cluster Setup.....	12
CUCM Setup.....	13
Enabling web access on entire phone estate	13
Changing CUCM phone Authentication (Optional).....	13
AutomationFX Web Interface Login	15
Requirements.....	15
Cluster credentials reset/recovery	16
PhoneFX (Phone Remote Control).....	17
Phone Filters	19
Creating & Saving a Filter.....	19
Editing & Deleting a Filter.....	19
Creating a Custom Group / Category	19

Overview

PhoneFX is an efficient and accurate way for CUCM professionals of all skills and experience levels to perform their jobs with an overall improvement in workflow and productivity. This guide introduces you to some of the most useful features of PhoneFX.

PhoneFX is built using AutomationFX hence most of this document makes reference to AutomationFX as technically that is the application that is being installed. PhoneFX is the functionality enabled within the AutomationFX platform for controlling Cisco IP Phones. AutomationFX (and therefore PhoneFX) leverages existing technology from PhoneView, PhoneView is the premier Cisco Endpoint Management product from UnifiedFX and has been used by over 10,000 Cisco UC Engineers worldwide.

Document Conventions

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



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



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



The exclamation mark 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].

Requirements

System

- Windows 8 (or above) / Windows Server 2012 (or above)
- Microsoft .NET Framework 4.5.2
- Dual Core CPU 2+ GHz / 4GB RAM (or above)
- 1GB free hard drive space
- VMWare Supported
- Modern web browser *i.e.* Chrome, Edge, Firefox, Safari, IE 10+
- Free TCP port (8181 by default)

Unified Communications Manager

- CUCM Version 8.0 (or above)
- Phone Web Server enabled (for getting screenshots)

Network Connectivity

The following tables describe the TCP Port connectivity requirements of PhoneFX:

TCP Ports between AutomationFX(PhoneFX) and CUCM

From	To	Port	Purpose
AutomationFX	CUCM	80/TCP	HTTP API Interface
AutomationFX	CUCM	8080/TCP	HTTP API Interface
AutomationFX	CUCM	443/TCP	HTTPS API Interface
AutomationFX	CUCM	8443/TCP	HTTPS API Interface
AutomationFX	CUCM	6970/TCP	HTTP API Interface
AutomationFX	CUCM	2748/TCP	CTI API Interface
AutomationFX	CUCM	2789/TCP	CTI API Interface

TCP Ports between AutomationFX and IP Phones

From	To	Port	Purpose
AutomationFX	IP Phone	80/TCP	HTTP API Interface
AutomationFX	IP Phone	443/TCP	HTTPS API Interface
IP Phone	AutomationFX	8181/TCP (Editable)	HTTP API Interface

AutomationFX Installation

Open the MSI Installer file and click **Next** on the Welcome page

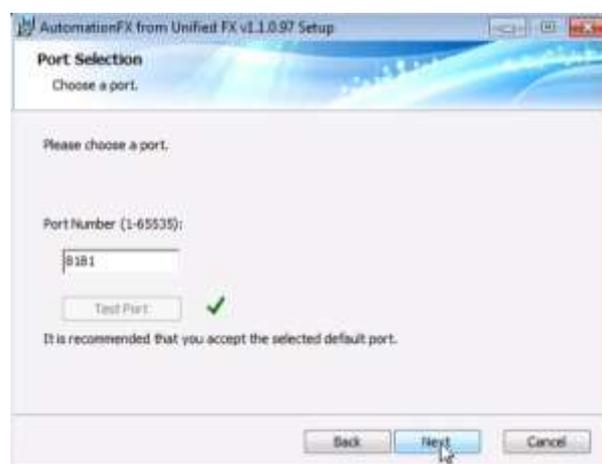


Review and accept the End-User License Agreement then click **Next**



Choose a local TCP port to host the *AutomationFX Web Application Platform*.

- Click **Test Port** to check that the chosen port is available on the local machine.
- Click **Next** to continue





The default port is **8181**, this can be changed to port 80 as long as there are no other applications hosted on port 80 on the local machine.



The value is saved to the following registry entry:

HKLM\Software\UnifiedFX\AutomationFX\PortNumber

Once all the required information has been captured, click **Install** to start the installation.



All necessary files will then be copied to the local machine and the AutomationFX Windows Service will be installed and started.

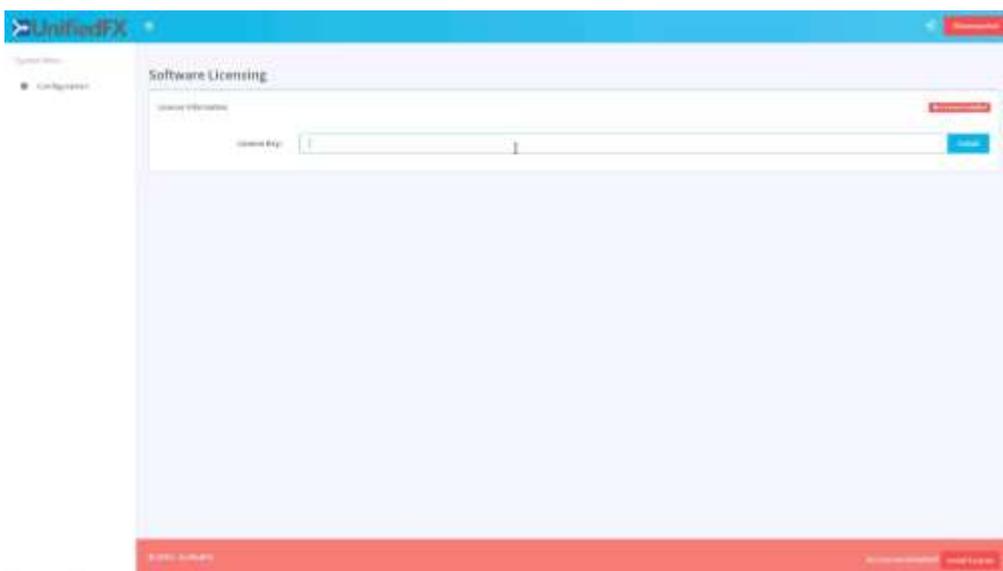


Once the installation is complete click **Finish** to close the installer



After the MSI installation is complete the application web interface is opened automatically (<http://127.0.0.1:8181>).

The first step for a new installation is to install the license key. Enter the License Key and click **Install**. Once installed, you will see the license parameters on this page.



CUCM Integration

This section provides information on CUCM cluster integration for PhoneFX phone control and configuring the phones to use AutomationFX authentication service.

Cluster Setup in AutomationFX

Once AutomationFX is installed and licensed, the first task is to add one or more CUCM clusters. Click **Configuration** and then **Clusters** - this will navigate to the cluster page.

There are two methods you can use to add a cluster to AutomationFX: **Automatic Cluster Setup** and **Manual Cluster Setup**.

Automatic Cluster Setup

When Automatic Cluster Setup is used, the application will automatically create an application user **AutomationFXUser** in CUCM with appropriate permissions for AutomationFX. Once the user account is created successfully, AutomationFX will use this credential to integrate with CUCM.

Enter the following and press the **Setup** button:

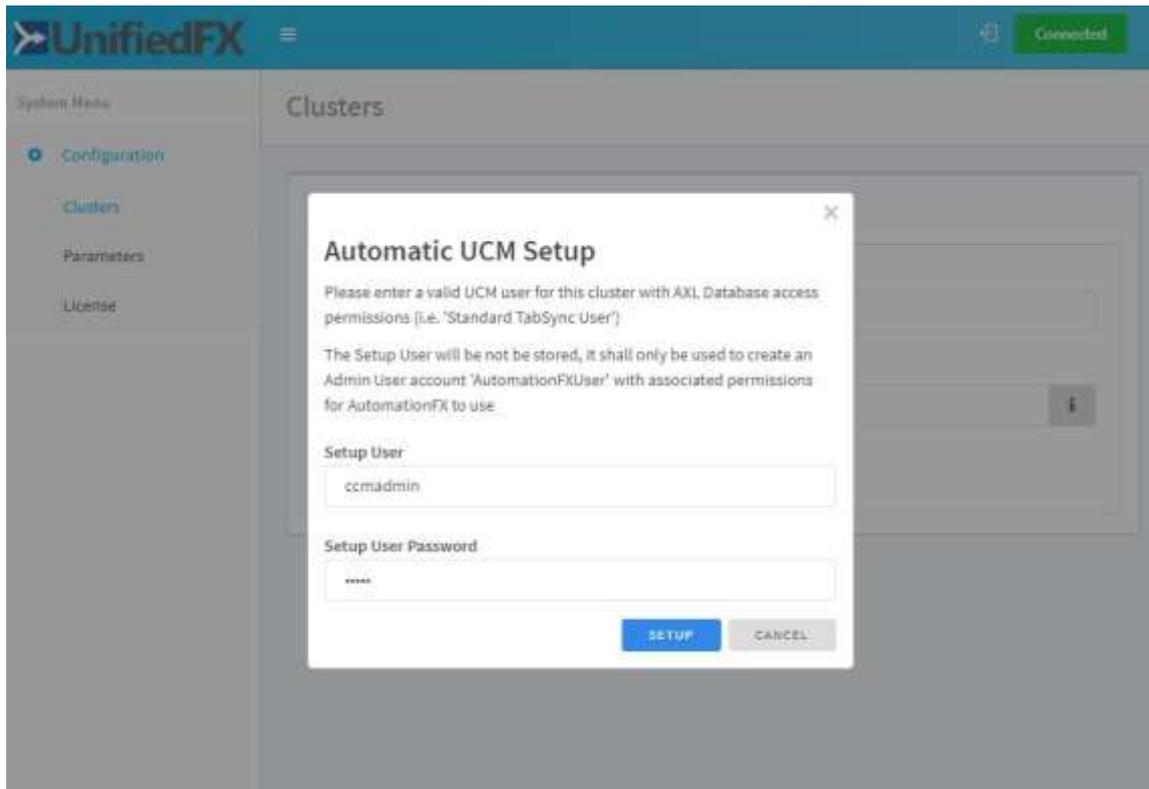
- Friendly Name
- Publisher IP Address



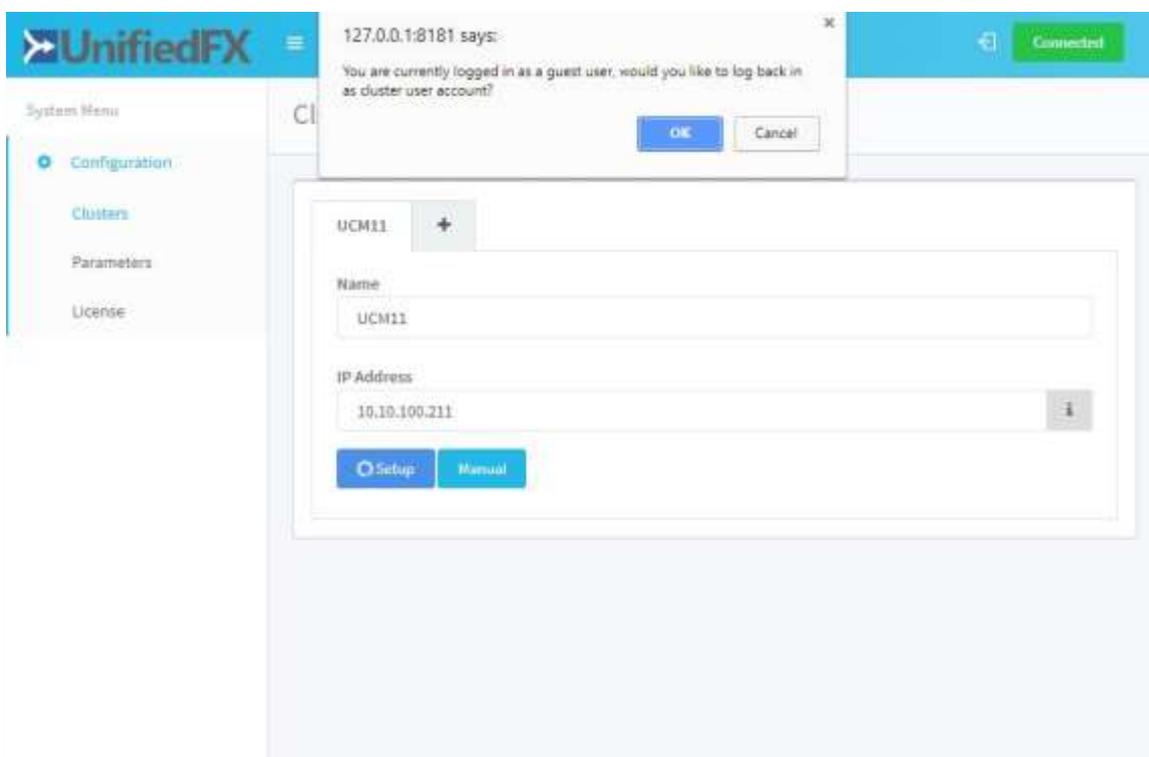
Enter a valid UCM user for this cluster with AXL Database access permissions (*i.e.* **Standard TabSync User**).



The Setup User will not be stored, it will only be used to create an Admin User account **AutomationFXUser** with appropriate permissions and a Phone User **UFXPhoneUser**.



After adding the first cluster you are prompted to login with a CUCM user account from the newly added cluster. This is required in order to gain access to all menu items within the web admin interface.



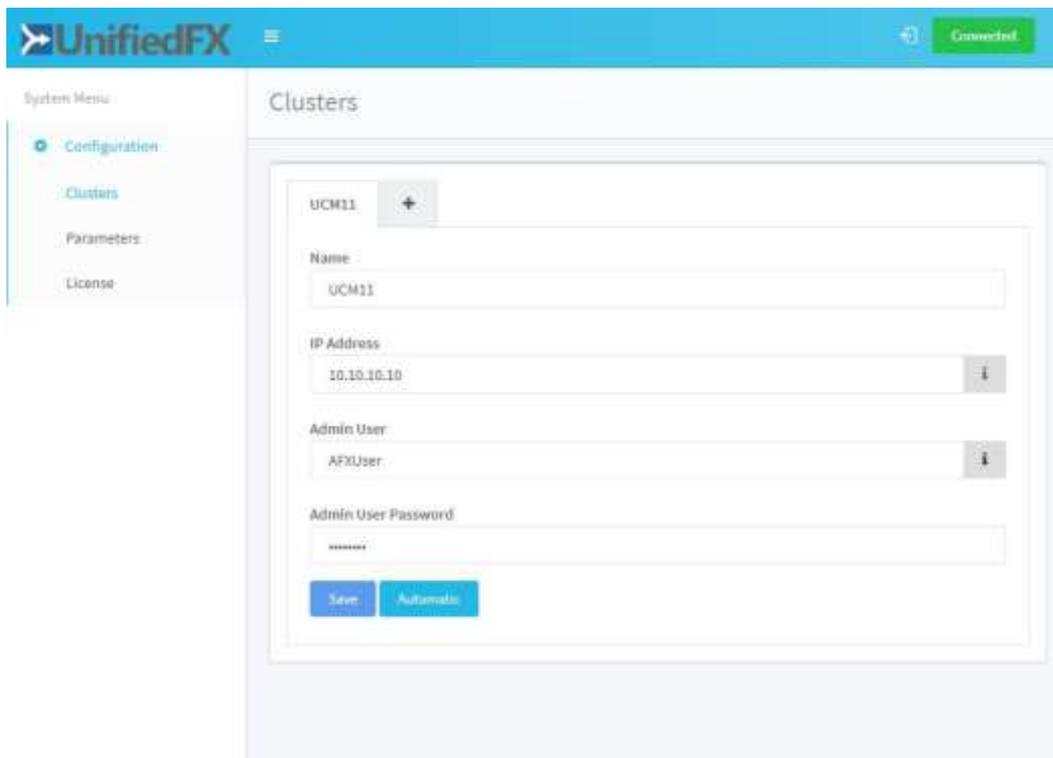
Manual Cluster Setup

AutomationFX requires a CUCM Application User account to access the relevant CUCM APIs and perform the required functionality. This Admin User account requires the following permissions:

- Standard TabSync User
- Standard CCM Server Monitoring
- Standard CCM Phone Administration
- 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 EM Authentication Proxy Rights
- AutomationFX Group (Custom Access Control Group)
 - AutomationFX Role (Custom Cisco Call Manager Administration Role)
 - Phone Migration (Resource - Read & Update)
 - Super Copy Info (Resource - Read & Update)]
 - Phone web pages (Resource - Read & Update)

Once the user is account is created in CUCM, click the **Manual** button on the cluster page and enter the following:

- Friendly Name
- Publisher IP Address
- Username
- Password



The screenshot displays the 'UnifiedFX' interface with a 'Clusters' section. A sidebar on the left shows 'System Menu' with options for 'Configuration', 'Clusters', 'Parameters', and 'License'. The main content area shows a form for adding a new cluster. The form has a title 'UCM11' with a plus sign. Below the title are four input fields: 'Name' (containing 'UCM11'), 'IP Address' (containing '10.10.10.10'), 'Admin User' (containing 'AFXUser'), and 'Admin User Password' (masked with asterisks). At the bottom of the form are two buttons: 'Save' and 'Automatic'.

CUCM Setup

This section provides information on CUCM changes required for Zero Touch Migration and eliminating device association for PhoneFX.

Enabling web access on entire phone estate



This change is required for PhoneFX Screenshots.



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.

Browse to the **CUCM Admin Interface » System » Enterprise Phone Configuration** page:

The screenshot shows the 'Enterprise Phone Configuration' page in the Cisco Unified CM Administration interface. The 'Web Access' property is set to 'Enabled' and the 'Override Common Settings' checkbox is checked. The 'Save' button is highlighted with a red box.

Property	Value	Override Common Settings
Allow User-Defined VPN Profiles	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Require Screen Lock*	User Controlled	<input type="checkbox"/>
Maximum Screen Lock Timeout*	600	<input type="checkbox"/>
Enforce Screen Lock During Display-On Time	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Lock Device During Audio Call*	Disabled	<input type="checkbox"/>
Kerberos Server		<input type="checkbox"/>
Kerberos Realm		<input type="checkbox"/>
TLS Resumption Timer*	3600	<input type="checkbox"/>
User Credentials Persistent for Expressway Sign in*	Disabled	<input type="checkbox"/>
WLAN SCEP Server		<input type="checkbox"/>
WLAN Root CA Fingerprint (SHA256 or SHA1)		<input type="checkbox"/>
Outbound Rollover*	Disabled	<input type="checkbox"/>
Detect Unified CM Connection Failure*	Normal	<input type="checkbox"/>
Time to Wait for Seamless Reconnect After TCP Drop or Roaming (seconds)	5	<input type="checkbox"/>
Load Server		<input type="checkbox"/>
IPv6 Load Server		<input type="checkbox"/>
Peer Firmware Sharing*	Enabled	<input type="checkbox"/>
Log Server		<input type="checkbox"/>
HTTPS Server*	http and https Enabled	<input type="checkbox"/>
Web Access*	Enabled	<input checked="" type="checkbox"/>
Settings Access*	Enabled	<input type="checkbox"/>
Android Debug Bridge (ADB)*	Disabled	<input type="checkbox"/>
Customer support upload URL		<input type="checkbox"/>

Enable the **Web Access** property and check the **Override Common Settings** check box for the same property, then click **Save** to save the changes.

Changing CUCM phone Authentication (Optional)

Using this configuration AutomationFX will provides an authentication service to IP Phones. This eliminates the need to associate phones with a user account in CUCM as would previously be required for PhoneView. The AutomationFX authentication service will check if the credentials match the Phone User / Password configured for the cluster - if they do not

match the request will be forwarded to the publisher to complete the authentication request as normal.

To use the AutomationFX based authenticate service with CUCM, you need to update **URL Authentication** and **Secured Authentication URL** within **Enterprise Parameters** with the following URL:

- `http://[AutomationFX_IP]:8181/ccmcp/authenticate.jsp`



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.

The screenshot shows the Cisco Unified CM Administration interface for Enterprise Parameters Configuration. The 'URL Authentication' field is set to `http://10.10.10.10:8080/ccmcp/authenticate.jsp` and the 'Secured Authentication URL' field is set to `http://10.10.10.10:8080/ccmcp/authenticate.jsp`. Both fields are highlighted with red boxes. Other parameters include 'Enable Caching' (True), 'Certificate Validity Check' (Disabled), and 'Prepare Cluster for Rollback' (False).

Parameter	Value	Default
Enable Caching	True	True
TLS Ciphers	AES-256, AES-128 ciphers RSA preferred	AES-256, AES-128 ciphers RSA preferred
SRTP Ciphers	All supported AES-256, AES-128 ciphers	All supported AES-256, AES-128 ciphers
Certificate Validity Check	Disabled	Disabled
Validity Check Frequency (hours)	24	24
Prepare Cluster for Rollback to pre 8.0	False	False
URL Authentication	http://10.10.10.10:8080/ccmcp/authenticate.jsp	
URL Directories	http://UCM11:8080/ccmcp/xmldirectory.jsp	
URL Idle		
URL Idle Time	0	0
URL Information	http://UCM11:8080/ccmcp/GetTelecasterHelpText.jsp	
URL Messages		
IP Phone Proxy Address		
URL Services	http://UCM11:8080/ccmcp/getservicesmenu.jsp	
Secured Authentication URL	http://10.10.10.10:8080/ccmcp/authenticate.jsp	
Secured Directory URL	https://UCM11:8443/ccmcp/xmldirectory.jsp	
Secured Idle URL		
Secured Information URL	https://UCM11:8443/ccmcp/GetTelecasterHelpText.jsp	
Secured Messages URL		

AutomationFX Web Interface Login

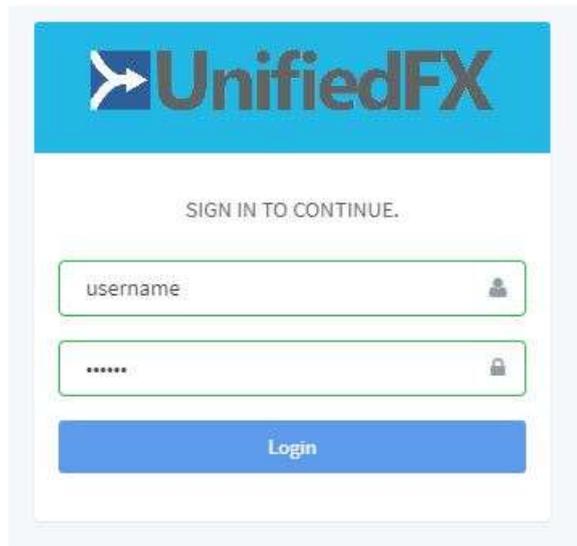
This section provides information on AutomationFX web interface login requirements, customising the login permissions and updating / recovering CUCM cluster credentials.

Requirements

The web interface for AutomationFX requires authentication once the first CUCM cluster has been added. AutomationFX uses the existing Application and End User accounts on CUCM to provide authenticated access to the AutomationFX web interface, hence the requirement for at least one CUCM cluster to be added before CUCM authentication is possible.

The CUCM Application or End User account requires one of the following permissions:

- Standard CCM Admin
- Standard Phone Administration



Before the first CUCM cluster has been added you can access the AutomationFX admin interface in *guest mode* automatically from the local machine (*i.e.* <http://127.0.0.1:8181>). However, if you need to access the AutomationFX web interface remotely before the first CUCM cluster has been added, you can use the following hard-coded guest account credentials:

- Username: **guest**
- Password: **ufx12345**



The guest login is disabled when one or more CUCM clusters have been configured, from that point onward only a valid CUCM login can be used to login.

Cluster credentials reset/recovery

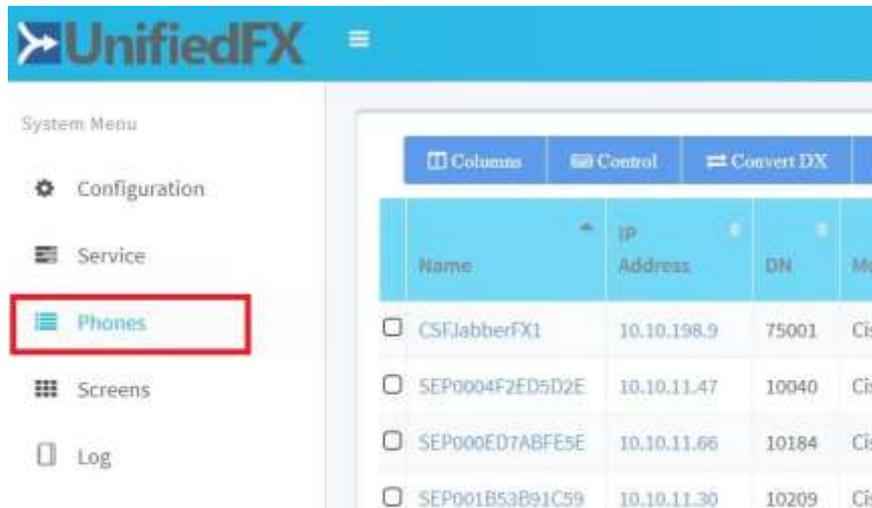
There may be a scenario where the credentials used to integrate CUCM cluster with AutomationFX have been changed. In this case users with appropriate permissions can login to the admin interface and update the cluster password.

By default, the admin login permission will stay the same as web interface login mentioned in the previous sections, however if the permissions were customised, user will require the custom permission/group configured in AutomationFX.

PhoneFX (Phone Remote Control)

This section provides information on how to control Cisco IP phones from the AutomationFX admin interface.

Click on the **Phones** menu from the navigation panel:



Find a specific phone from the search bar on the top right corner:



The **Search** feature is a wildcard multi-field search, so you can find a device by any of the following values:

- Device Name
- Description
- Directory Number
- IP Address *etc.*

Select the check box for the desired phone, then click on the **Control** button above the table to launch PhoneFX. A new browser popup window will be opened with the PhoneFX remote-control interface.



Phone Filters

The Filter menu is shown at the bottom of the AutomationFX navigation sidebar section when you navigate to the **Phones** page. You can create filters to group devices using built in summary options or custom grouping / tagging.



Creating & Saving a Filter

To create a filter tick / apply the appropriate filter rules.

Type an appropriate name and press [Enter] or click on the name typed. If the provided name is added to the filter list, the **Save** button will be highlighted with a red overlay to indicate that there is a save operation pending.

Click the **Save** button to persist the created filter.

Editing & Deleting a Filter

To edit a filter, load the appropriate filter and click the **Edit** icon . You can change the filter rules if desired or enter an appropriate description.

Click **Save** to save the changes or **Delete** to delete the filter.

Creating a Custom Group / Category

In most cases the built-in summary filters will be sufficient, however there may be scenarios where a custom group (subset of phones) is required for more granular control. You can tag phones to a category (custom group) by browsing to the **Phones** page and selecting the desired phones. [Ctrl] + Click and [Ctrl] + [Shift] + Click options are available for multiple selection.