



CONVERGENCE™ Enterprise AV Manager

Software Version: 3.0

Notices

Document: DOC-0480-001v1.2 May 2022

© 2022 ClearOne, Inc. All rights reserved.

Information in this document is subject to change without notice.

Contents

Notices	i
1. Introduction	1
2. System Requirements	3
3. Known Issues	4
4. Network Ports	4
5. Un-install Before You Update.....	5
6. Installation	8
7. Appendix.....	16
7.1 Important Folders.....	16
7.2 ClearOne Contacts	16
7.3 How to Add Network Port Firewall Rules in Windows	16

1. Introduction

CONVERGENCE Enterprise AV Manager is single tenant software for an organization to centrally monitor, audit, and control their ClearOne Pro Audio and Video devices worldwide.

Related documents that help you set up and use this application, based on your user role, are found in the Web application's Help view.

1.1 Product Features

Enterprise Special Features

- Self-maintained and hosted on-premises or privately in the cloud by an organization, for complete control and security.
- License any Internet-accessible server, or for an isolated network, license a specific machine.
- Provide better online availability and performance by using multiple server instances for redundancy.
- The Enterprise portal shows the name of your organization as “Branding”.

Unified Software Platform

- Available as a Cloud AV Manager service, or Enterprise AV Manager software, either supported by Local Agent AV Manager servers.
- Scales to support organizations of any size – large or small.
- Organize AV devices and user permissions by any location hierarchy, such as city, building, and room.
- Assign access rights by organization, location, user, and customized roles.
- Communicate using integrated video, audio, and chat tools.
- Convenient single-sign-on access through LDAP connectivity.
- End-to-end security with HTTPS, encrypted cloud servers, and 256-bit encrypted password management for both users and devices.
- Access from any device, desktop to mobile, with a powerful and elegant browser interface.
- Integrates with third-party management systems via a RESTful web interface.

Monitor

- Remote real-time access provides at-a-glance and all-inclusive powerful dashboard views.
- Stay informed with email and SMS text alerts.

Control

- Remotely configure, backup, restore, and update CONVERGE® DSP Mixers and P-Link peripherals systemwide – and simultaneously.
- Provision CONVERGE Pro 2 VoIP lines and view VoIP registration status.

Audit

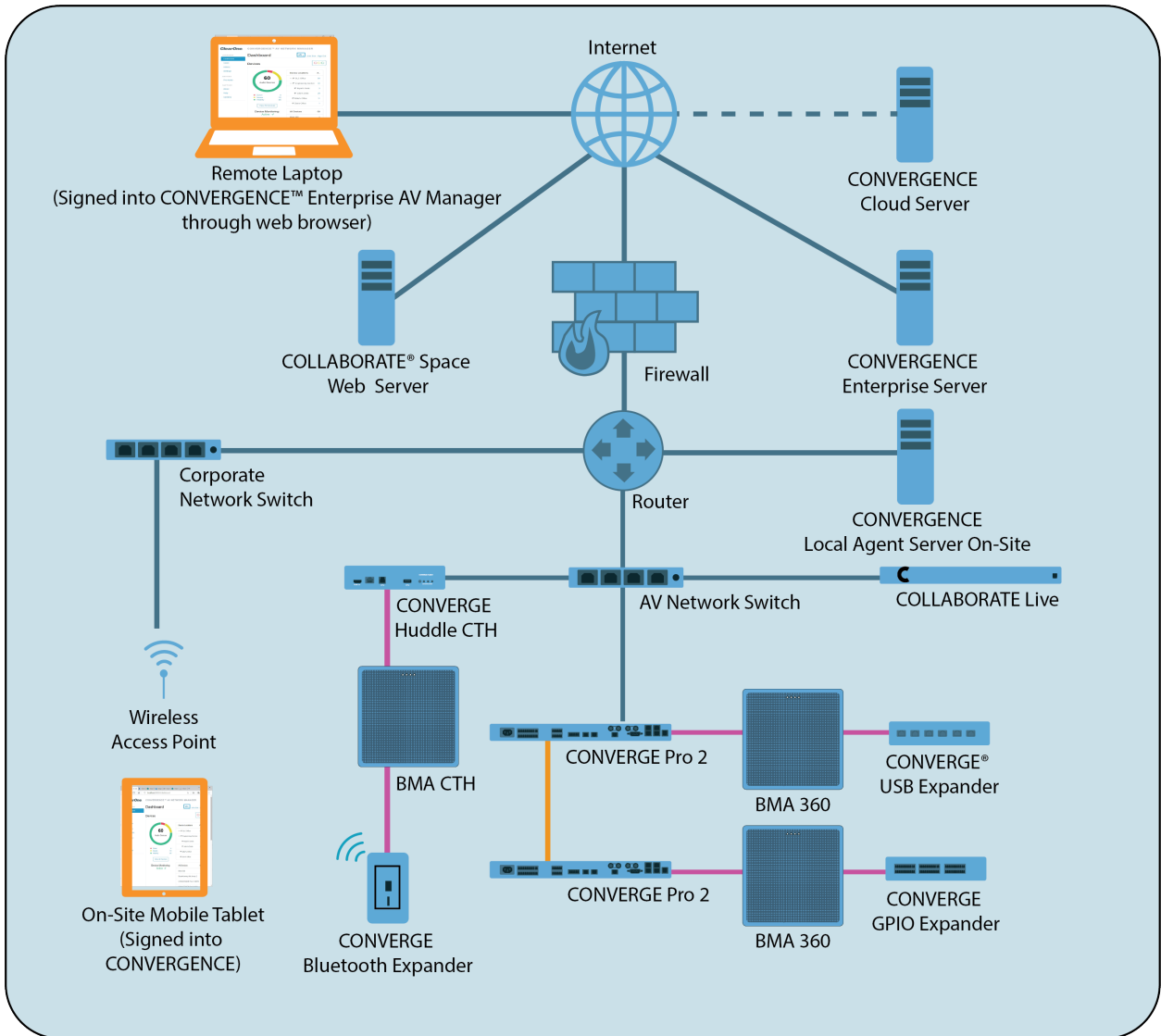
- Get up and running quickly with auto discovery of Pro Audio devices.
- Download device logs and data for troubleshooting, auditing, and reports.

1.2 Supported ClearOne Products

- CONVERGE® Pro 2 DSP Mixers and associated peripheral devices (minimum firmware: 5.0.x)
- CONVERGE Huddle DSP Mixer and associated peripheral devices (minimum firmware: 1.0.x)
- COLLABORATE® Live video codecs (minimum firmware: 249.0.0.77)
- COLLABORATE Space (collaboratespace.net and up-to-date, on-premise versions)

1.3 Example Deployment

Install an instance of CONVERGENCE™ Enterprise AV Manager on a Windows server on premises or on an Infrastructure as a Service. The server must be accessible by the remote CONVERGENCE Local Agent AV Managers and by supporting users, such as over the Internet. Install using HTTPS with a keystore file made from a security certificate.



If the CONVERGENCE Enterprise license is not tied to the MAC address of its server, it must have access to ClearOne’s CONVERGENCE Cloud server at cx.clearone.com on the Internet. A CONVERGENCE Local Agent server must be able to access ClearOne Pro Audio devices on premises over an IP network and sign into the CONVERGENCE Enterprise server whether it is also on premises or on a private cloud infrastructure as a service (IaaS). Supported ClearOne video devices may also be accessed over the Internet through Enterprise.

After you set up a Local Agent Server Account for your organization on CONVERGENCE Enterprise AV Manager, you can connect your CONVERGENCE Local Agent servers to it. Then users of your organization can remotely and securely monitor and control the ClearOne CONVERGE® audio devices behind your firewall through Enterprise AV Manager without the need of VPN. Users sign in through the web browser on their laptops or other computing devices.

You can connect multiple Local Agent servers of your organization to Enterprise AV Manager, aggregating all of them together into a single dashboard, device list, and alert.

Through your user account settings, you can also sign into your COLLABORATE Space account in the cloud. Then you can monitor or administer your organization's COLLABORATE Space account users and COLLABORATE Live video codecs, together with your accessible supported CONVERGE audio devices.

2. System Requirements

- Disk space: 3 GB free
- Processor: 1 GHz Intel Pentium processor (dual core or more recommended)
- RAM: 1 GB RAM free (to serve over 2,000 devices)
- Operating System: Windows 7 and above, or Windows Server 2012 R2 and above (Windows 10 Pro or Windows Server 2019 recommended)
- A CONVERGENCE Enterprise server must reach the Internet to connect to:
 - ClearOne's update server
 - CONVERGENCE Cloud for license verification (unless licensed with a specific machine's MAC address)
 - COLLABORATE Space Administrator (collaboratespace.net)
- Supported browsers:
 - Firefox
 - Chrome
 - Edge
 - Safari
 - Internet Explorer works for the most part, but may have a few minor issues.
- The Web server, database, and application are 100% pure Java (8 and above). Installations are currently available for the following operating systems:
 - Microsoft Windows 7, 8, and 10
 - Microsoft Windows Server 2012 R2 and above

3. Known Issues

- User interface translations of CONVERGENCE have been temporarily disabled.
- To update CONVERGENCE Enterprise AV Manager, you must first uninstall the previous version and restart the server machine.
- The Help documentation is in English only.
- CONVERGENCE only changes live values of DSP audio mixers and cannot save them to CONSOLE AI project files, or read them.
- Unless all CP2s of the stack are already in the database, CONVERGENCE does **not** correctly identify an incomplete stack.
- CONVERGENCE does not recognize when a CONVERGE Pro 2 supporting VoIP is registered to Skype for Business.
- COLLABORATE Live device firmware needs to be up-to-date to download its logs, see accurate device time, or see its serial number.
- If CONVERGENCE reports COLLABORATE Live devices are down, but they are up and running, you may need to reaccept the device's GDPR in Settings > Advanced > Space.
- The Windows service "Clearone Convergence Dashboard" may not restart on Windows Server without restarting the host machine.
- Video Collaboration devices may not update older firmware from Convergence. You may need to update them from the COLLABORATE Live device screen or its web page.

4. Network Ports

Required Network Ports

The following network ports are required for your machine to act like a Web server, or for CONVERGENCE Enterprise to have access to updates:

Ports that should not be used by other applications (such as other Web applications; depends on protocol and port chosen during installation):

- HTTP: 80 or 8080, 9990 for database
- HTTPS: 443 or 8443, 9993 for database

Open server firewall inbound ports (depends on protocol and port chosen during installation):

- HTTP (not secure): 80 or 8080
- HTTPS (secure, but requires a keystore certificate): 443 or 8443
- FTP: 21
- CFS (Configuration File Service access - new): 8888

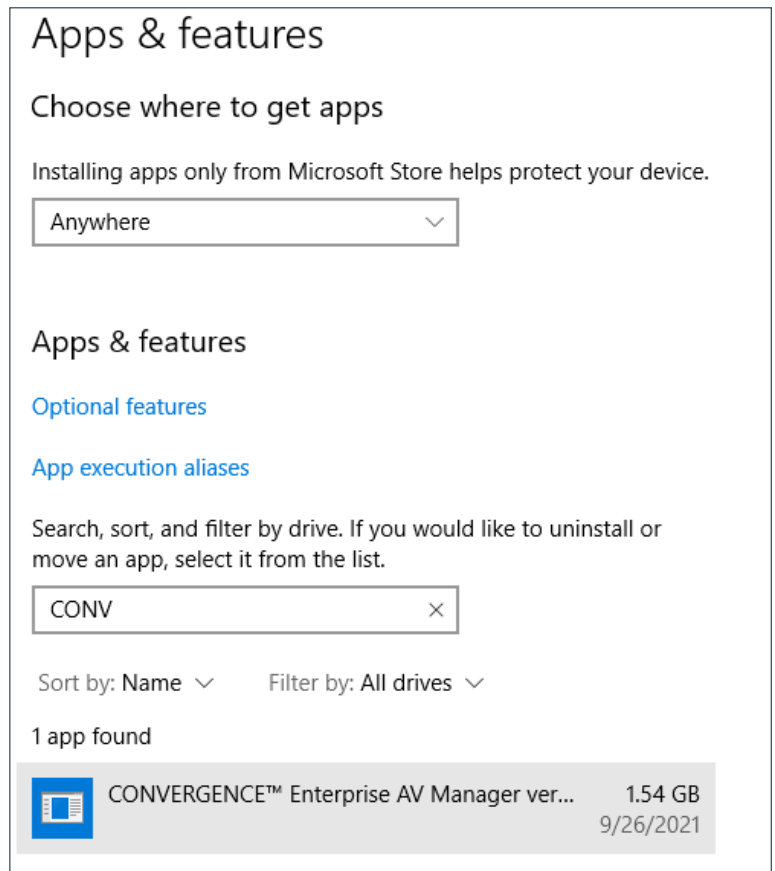


Note: Needed firewall rules are now added and removed automatically as part of installation and uninstallation respectively. ([See Appendix section 7.3](#) on how to manually inspect, add, or change network ports on Windows.) However, if using an IaaS (Infrastructure as a Service) for Enterprise AV Manager, such as AWS, then with the exception of FTP, you will need to add the HTTPS and CFS ports manually to the security group inbound rules applied to the server instance (EC2 in AWS).

5. Un-install Before You Update

If you have a previously installed version of CONVERGENCE on your machine, you must complete the steps in this section. If not, proceed to [section 6. Installation](#).

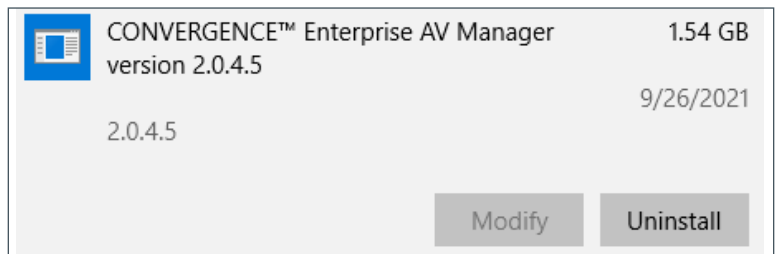
5.1 From your Windows menu, **navigate to Settings > Apps > Apps & Features**.



5.2 **Scroll down** to “CONVERGENCE™ Enterprise AV Manager” or type part of it in the Search field. Then **click** the **CONVERGENCE™ Enterprise AV Manager** entry.

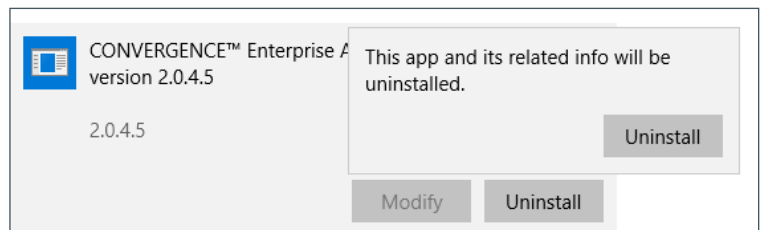
The icon expands to show Modify and Uninstall options.

5.3 **Click Uninstall**.



A popup dialog box appears.

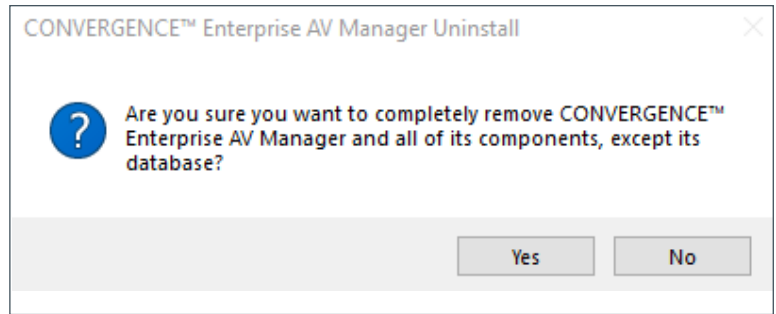
5.4 On the popup dialog box, **click Uninstall**.



The system displays a window to make sure you want to completely remove CONVERGENCE.

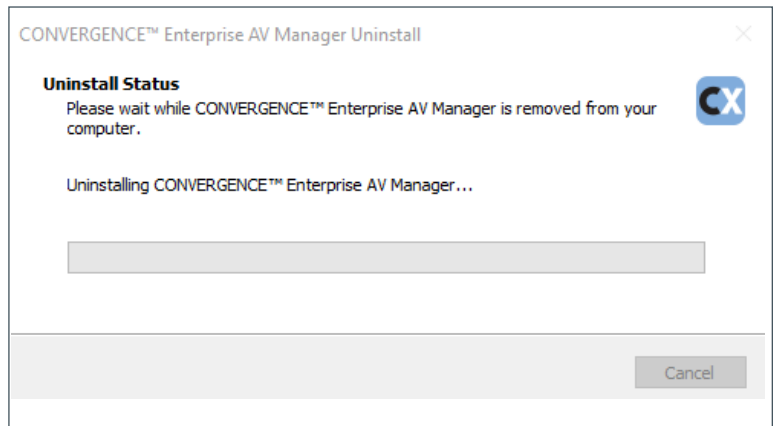
5.5 **Click Yes.**

Windows presents a dialog window (not shown here) that asks for permission to alter your computer.



5.6 **Click Yes** to allow Windows to remove CONVERGENCE Enterprise AV Manager.

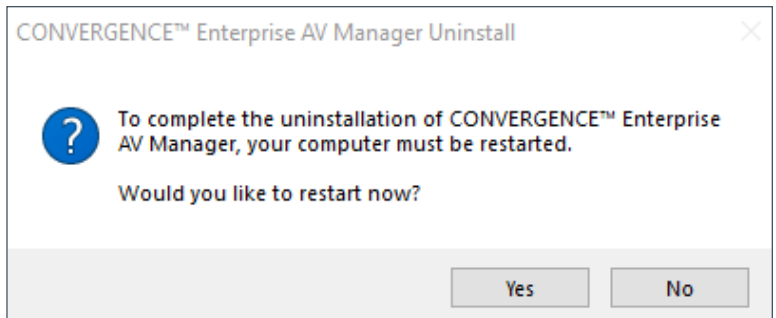
Windows begins the process to uninstall CONVERGENCE Enterprise AV Manager.



After the uninstall process is complete, a pop-up window appears that asks if you want to restart your computer.

5.7 **Click Yes.**

Your computer restarts.

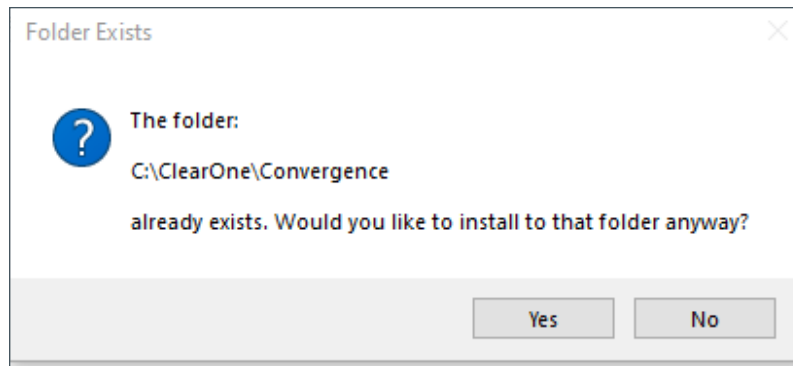


5.8 **Navigate to the folder** where you downloaded the most recent version of the CONVERGENCE Enterprise AV Manager installer.

5.9 **Open the CONVERGENCE installer (.exe) file.**

 **Note the following:**

- The uninstall process does not delete all folders and files that the install process loaded onto your computer.
- During reinstall, when you select a destination location ([see step 6.5](#)), if you select the same location for CONVERGENCE, the installer displays the following dialog window:



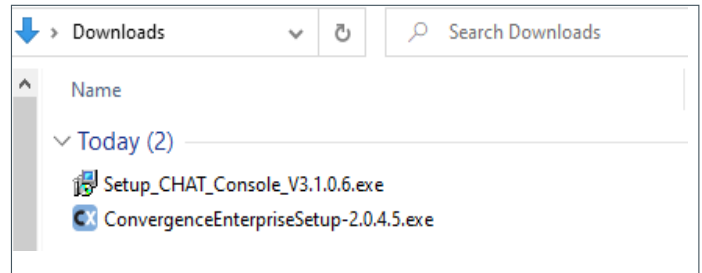
- You may click **Yes**.

6. Installation

! **Important:** If CONVERGENCE Enterprise is already on your machine and you are re-installing, you must first **uninstall it.**

To download and install CONVERGENCE, complete the following steps:

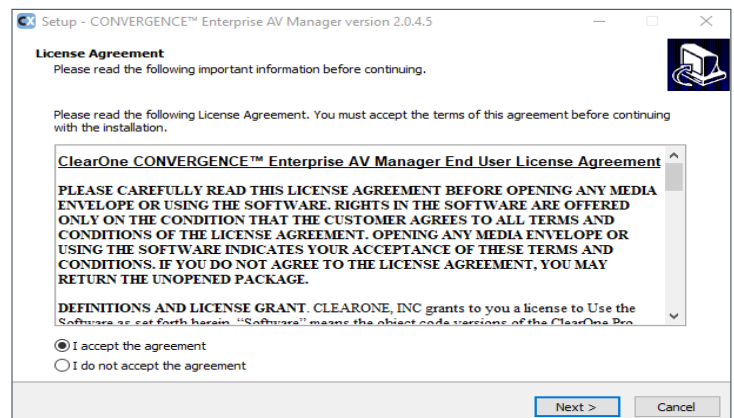
- 6.1 **Navigate to the folder** where you downloaded the **CONVERGENCE Enterprise installer (.exe).**
Open the installer.



- 6.2 If your system displays a window that asks if you want to allow this app to make changes to your device, click Yes.

The License Agreement window opens.

- 6.3 **Carefully read** the license agreement. Then click the **I accept the agreement** radio button.



The Next button activates.

- 6.4 **Click Next.**

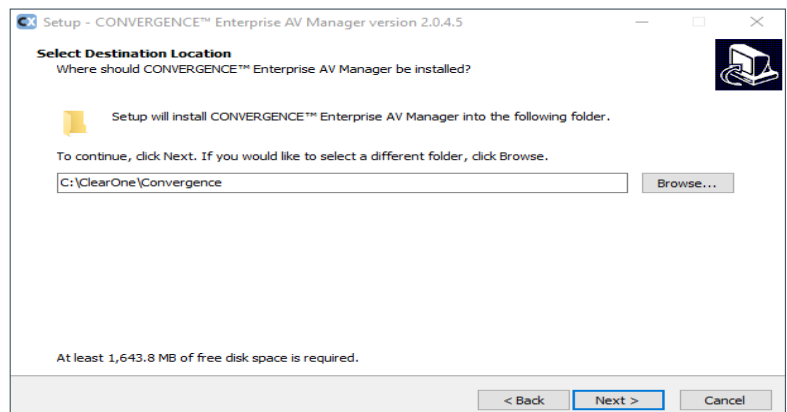
The installer displays the Select Destination Location window.

- 6.5 If you want the installer to use the folder location indicated, **click Next.**

or

To use a different folder:

Click Browse, navigate to the folder, **select it,** then on the Browse for folder window, **click OK.**



! **Caution:** If you select an existing folder, the installer overwrites the folder's contents.

The target directory path must **not** contain a blank space.

On the installer's destination location window, **click Next.**

The installer displays the Select Convergence Web server protocol window.

6.6 From the dropdown, **select** either **HTTP protocol** or **HTTPS protocol**.

Then **click Next**.

Do either **a** or **b** below:

- a. If you selected **HTTP** protocol:
CONVERGENCE displays the Custom HTTP port dialog window.

Replace “localhost” with the **network address or domain name** to be accessed from the machine on which you are installing.

Click Next.

The system displays the Custom HTTP port dialog window.

Enter the port number.

Now **go to Step 6.12**.

- b. If you selected **HTTPS** protocol (recommended):
CONVERGENCE displays the Custom HTTPS port dialog window.

Proceed to step 6.7.

6.7 8443 is the default HTTPS port.

To change, **enter another port number**.

The recommended ports for HTTPS are 443 or 8443.

Click Next.

The system displays the Server keystore information dialog window.

6.8 **Do** either **a** or **b** below:

- a. To Import an existing keystore, **click that radio button**, then **click Next**.

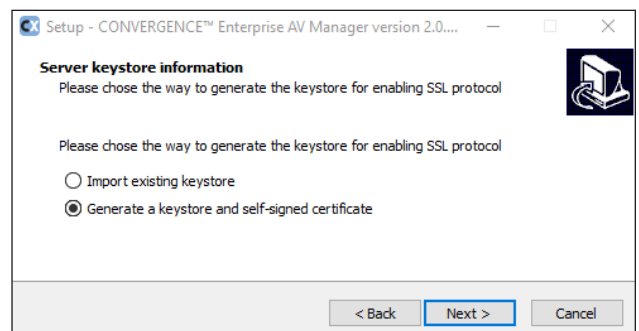
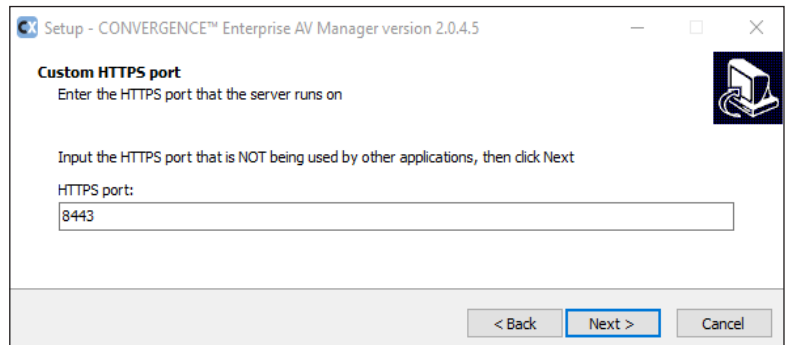
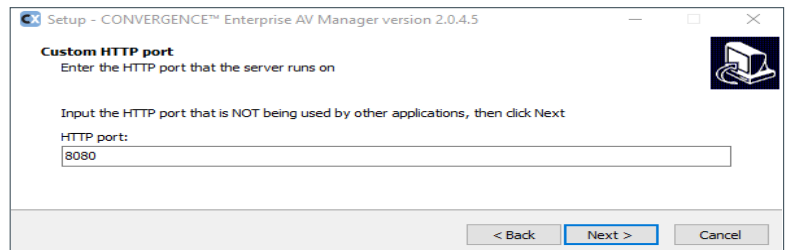
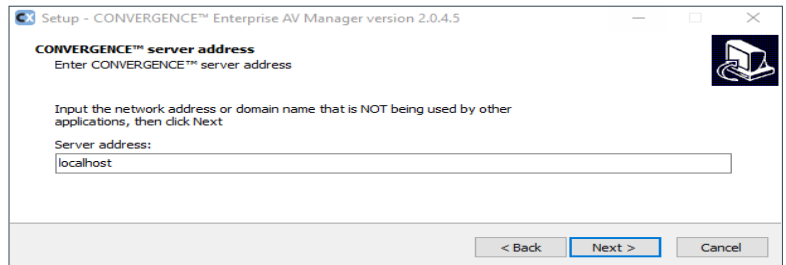
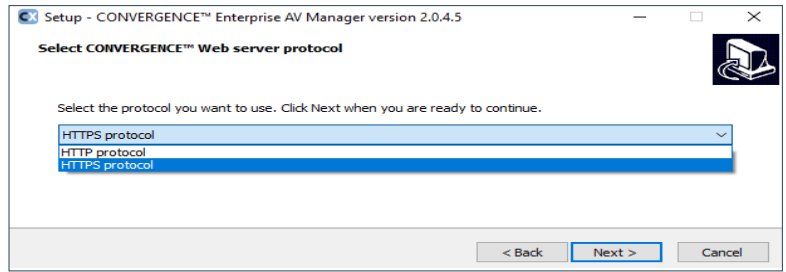
CONVERGENCE displays the Select Keystore Location dialog window.

Go to step 6.10.


- b. To have the installer generate a keystore and self-signed certificate, **ensure that the radio button is selected**, then **click Next**.

CONVERGENCE displays the Server keystore self signed certificate generation dialog window.

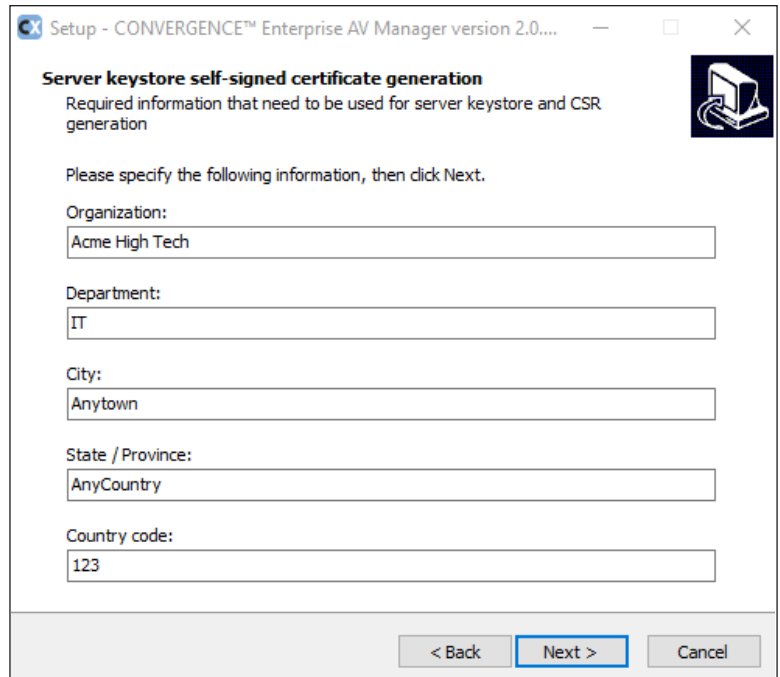
Proceed to step 6.9.



- 6.9 For each of the input boxes, **enter information**.
Then **click Next**.

 **Note:** To proceed with the install, you must enter information in every input box

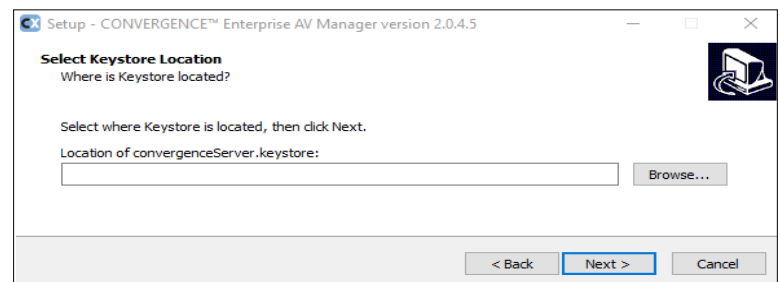
[Go to step 6.12.](#)



If you selected **Import** on step 6.8, then complete steps 6.10 and 6.11.

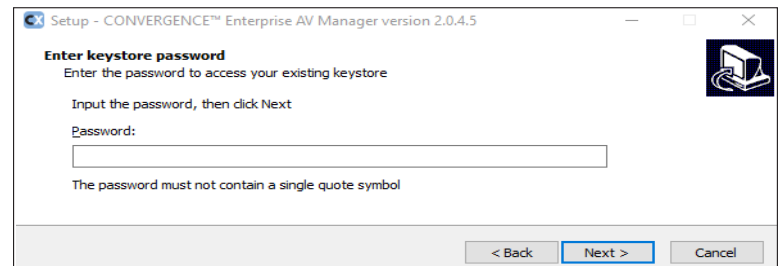
- 6.10 On the Select Keystore Location dialog window, **enter the location** of the keystore file, or **click Browse**, navigate to the keystore file, and **click OK**.
Then **click Next**.

CONVERGENCE displays the Enter keystore password dialog window.



- 6.11 **Enter the password**, then **click Next**.

CONVERGENCE displays the Select Database Type for CONVERGENCE Application dialog window.

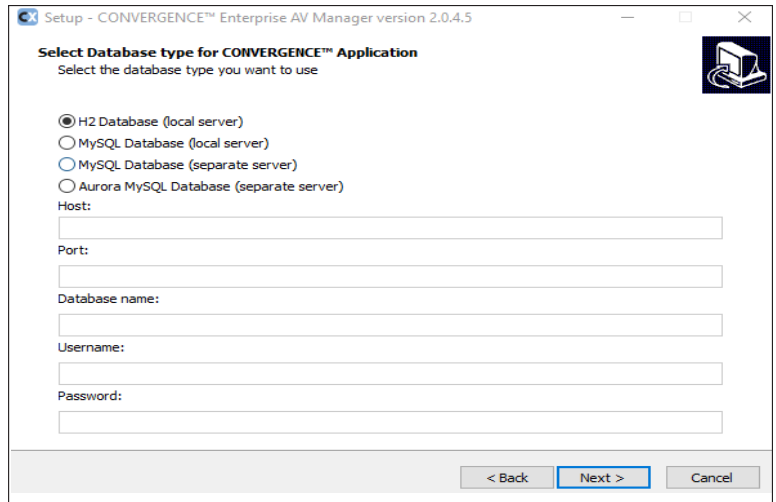


6.12 Click the appropriate radio button.


If needed, enter information in the displayed entry boxes.

Then click Next.

CONVERGENCE displays the Add FTP port to server firewall rules dialog window.

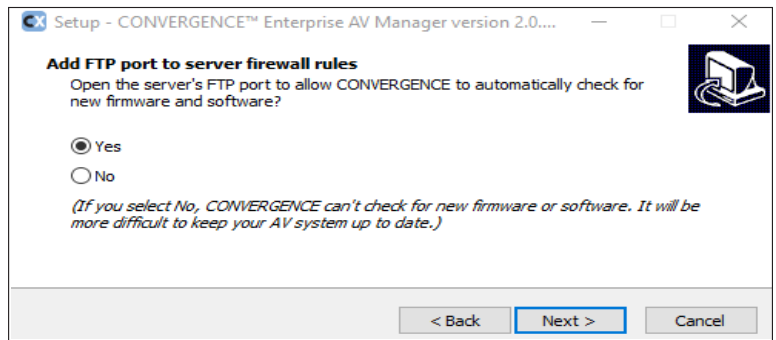


6.13 To change from the default (Yes), click the No radio button.

 **Note:** ClearOne recommends that you select Yes.

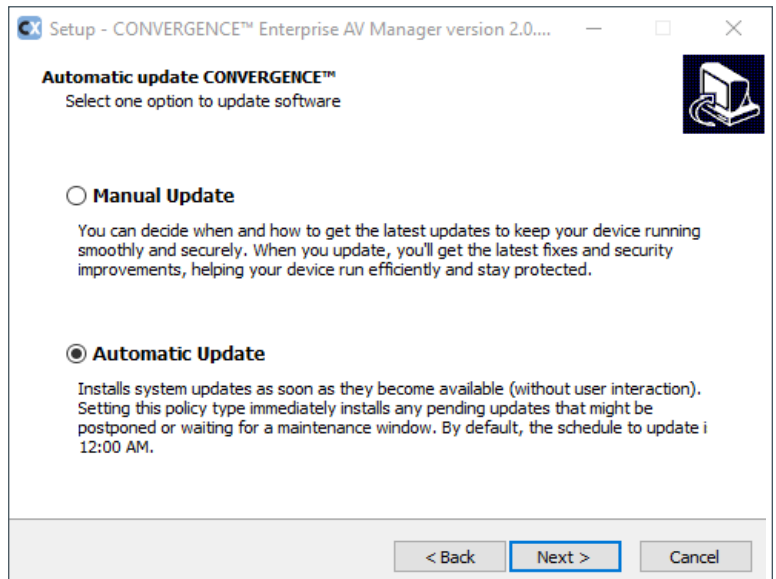
Click Next.

CONVERGENCE displays the Automatic update CONVERGENCE dialog window.



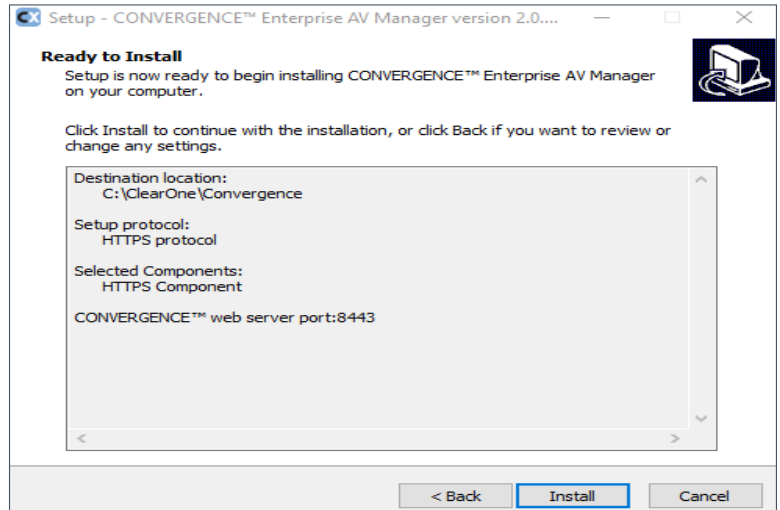
6.14 Click the radio button of your preferred method to update software.

CONVERGENCE displays the Ready to Install dialog window.

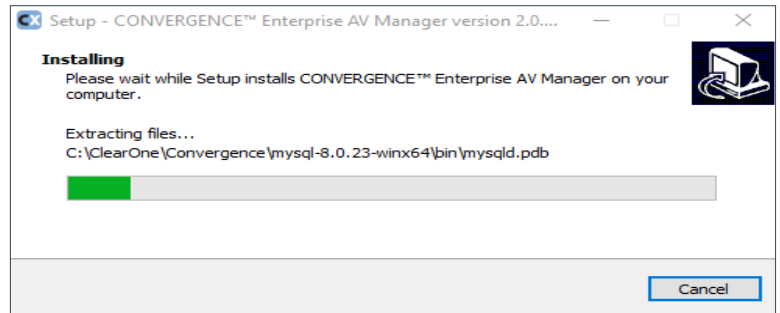


6.15 Click Install.

The installer displays the Installing window.



After the installation is complete, the installer displays the Information window which includes release notes and usage notes.



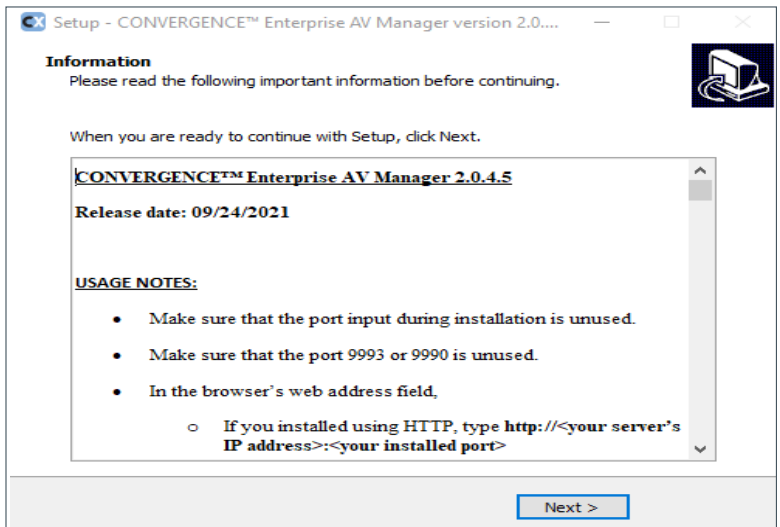
6.16 Read the release and usage notes.

Then Click Next.

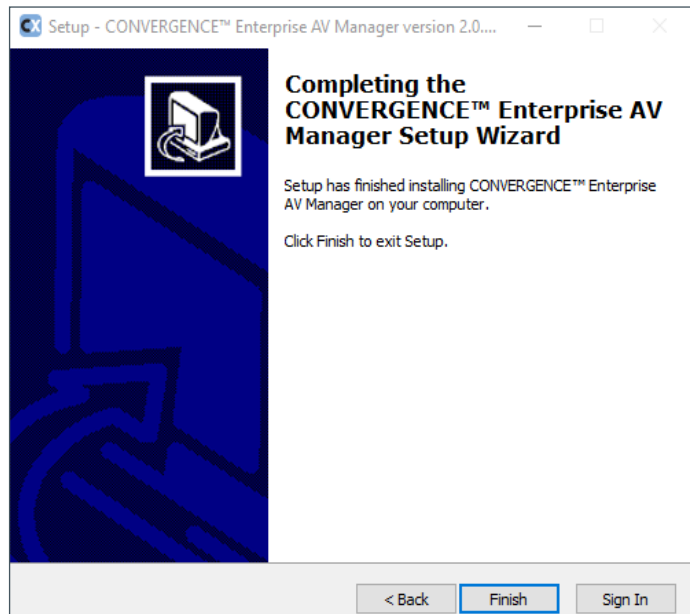
The installer displays a different window based on whether or not this is the first installation or a reinstallation.

If this is a reinstallation, [go to step 6.21](#).

If this is the first installation, **proceed to step 6.17**.



6.17 On the Setup Wizard window, **click Sign In.**



CONVERGENCE Enterprise displays the Register Initial Owner Account window.

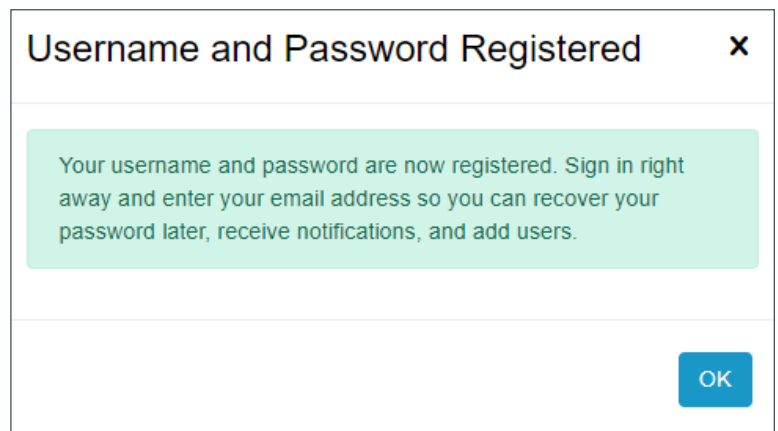
6.18 **Enter the information requested** in the input boxes.

Take note of your username and password.

Then **click Register.**

CONVERGENCE Enterprise displays a Username and Password Registered window.

6.19 **Click OK.**

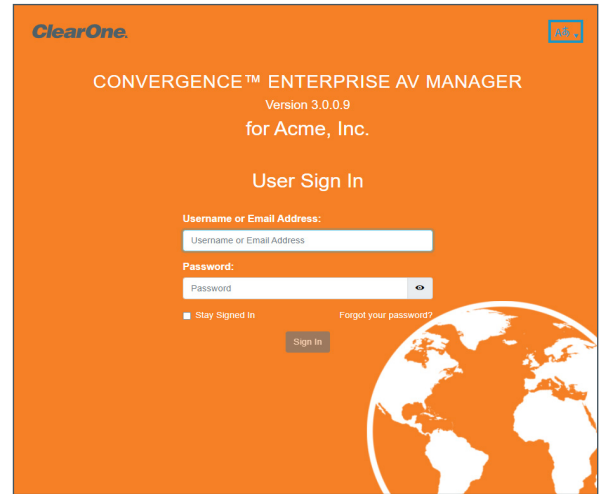


CONVERGENCE Enterprise displays the User Sign In portal.

6.20 Enter your CONVERGENCE Enterprise username or email address, and your password.

Then click Sign In.

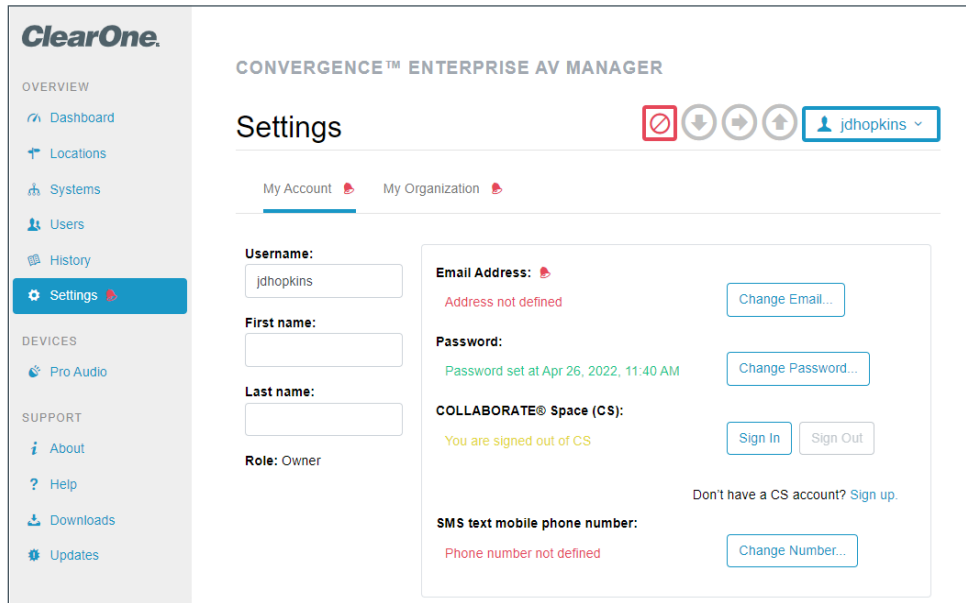
CONVERGENCE Enterprise displays the Settings > My Account view.



Notice any red alarm symbols .

They indicate areas where you may need to take further action.

For detailed instructions about Settings see the online Help, available when you sign in. Under the navigation bar's SUPPORT section, click Help. The Help page appears. In the navigation bar under OWNER, click Setting Up the Enterprise Organization.



 Note the following:

- If after an update your browser displays a blank web page, click your browser's refresh icon.
- If the browser is running on the server, you can type "localhost" for your server's IP address.
- If during the installation process you selected **HTTPS** and you did **not** use a valid certificate, your browser displays a security warning page. Regardless, you can "push through" to the server's webpage.

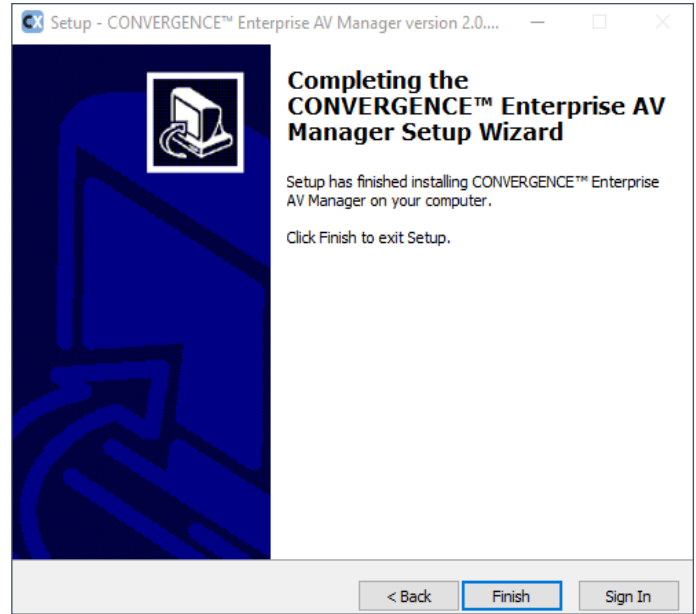
6.21 *If this is a reinstallation:* **Click Finish or Sign In.**

*If you click **Sign In**, the Setup Wizard window closes.*

The system then displays the User Sign In window.

*If you click **Finish**, the Setup Wizard closes.*

When you want to sign in to CONVERGENCE Enterprise, **complete step 6.22.**



6.22 **Open an HTML browser**, such as Edge, Safari, or Chrome.

In the browser’s web address field, **do** either **a** or **b** below.

a. If you selected HTTP, type the following:

http://<your server’s IP address or domain name>:<port number>

b. If you selected HTTPS, type the following:

https://<your server’s IP address or domain name>:<port number>

Use the port number you entered in the previous steps.

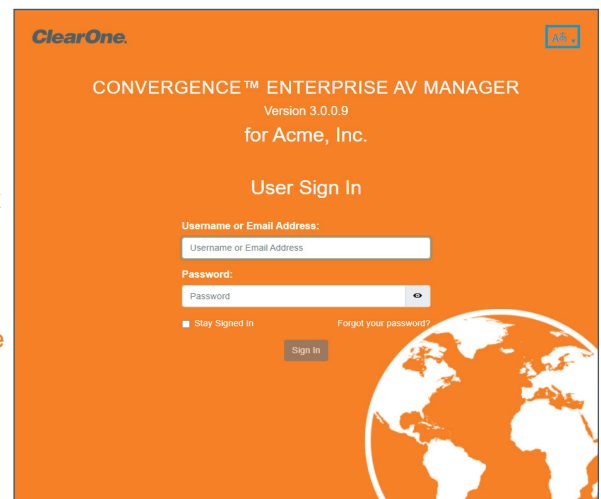
 **Note:** You do **not** need to type the colon and port number if you chose the default ports 80 or 443.

Press Enter.

Your browser displays the User Sign In portal.

 **Note the following:**

- If you forgot the password, and you configured an email address for your account, you can click “Forgot your password?” to reset it.
- Otherwise you will have to delete or move out the files in the database folder identified in the Appendix at the end of this guide, and restart the server.
- Then you can enter a new username and password as an initial owner. All previously entered data will be lost.



7. Appendix

7.1 Important Folders

Here are some folders used by CONVERGENCE that you, as a system administrator, might find useful:

Folder	Location
H2 Database	C:\Windows\System32\config\systemprofile\h2
MySQL Database	<INSTALL_FOLDER>\Convergence\mysql-8.0.23-winx64\data
Server's log	<INSTALL_FOLDER>\Convergence\wildfly-x.x.x.x\standalone\log
Configuration backup	C:\Windows\System32\config\systemprofile\Convergence\ConfigurationBackup
Downloaded firmware	C:\Windows\System32\config\systemprofile\Convergence\Firmwares

7.2 ClearOne Contacts

Headquarters

5225 Wiley Post Way Suite 500
Salt Lake City, UT 84116

Sales

Tel: +1.801.975.7200
sales@clearone.com

Headquarters

Tel: +1.801.975-7200

Technical Support

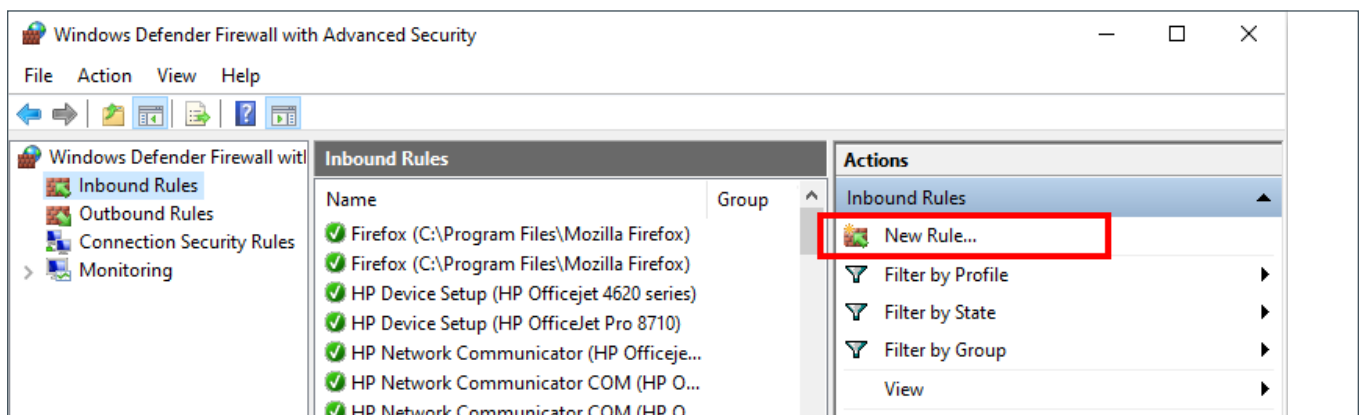
Tel: +1.801.974.3760
audiotechsupport@clearone.com

7.3 How to Add Network Port Firewall Rules in Windows

To open needed Web and FTP ports on the server's firewall (Windows), complete the following steps:

1. **Open the following location:**

- Windows Control Panel >
- System and Security >
- Windows Defender Firewall >
- Advanced Settings >
- Inbound Rules



2. Under Actions, **click New Rule.**

A New Inbound Rule Wizard window opens.

3. **Select Port.** Then **click Next.**

The Protocol and Ports window opens.

What type of rule would you like to create?

- Program**
Rule that controls connections for a program.
- Port**
Rule that controls connections for a TCP or UDP port.
- Predefined:**
@FirewallAPI.dll,-80200
Rule that controls connections for a Windows experience.
- Custom**
Custom rule.

< Back **Next >** Cancel

4. Do the following:

- a. Under “Does this rule apply to TCP or UDP?” **select TCP.**
- b. Under “Does this rule apply to all local ports or specific local ports?” **click the Specific local ports radio button.**
- c. In the Specific local ports field, **type one or more** of the following that apply to the rule:

- 80 (optional - access as default HTTP web server)
- 443 (optional - access as default HTTPS web server)
- 8080 (optional - access as an HTTP web server, must enter port)
- 8443 (optional - access as an HTTP web server, must enter port)
- 21 (FTP - required for firmware and software downloads)
- 9001-65000 (Pro Audio device port range - required for operation)

d. **Click Next.**

The Actions window opens.

Does this rule apply to TCP or UDP?

- TCP**
- UDP**

Does this rule apply to all local ports or specific local ports?

- All local ports**
- Specific local ports:**
Example: 80, 443, 5000-5010

< Back **Next >** Cancel

5. **Click the Allow the connection radio button.**

Then **click Next.**

The Profile window opens.

What action should be taken when a connection matches the specified conditions?

- Allow the connection**
This includes connections that are protected with IPsec as well as those are not.
- Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
Customize...
- Block the connection**

< Back **Next >** Cancel

- If the Web server is not to be exposed to the Internet, **click the Public check box** to remove the check mark.

Leave the Domain and Private check boxes selected.

Then **click Next**.

The Name window opens.

- Type a Name and Description** (optional).

Then **click Finish**.

When does this rule apply?

Domain
Applies when a computer is connected to its corporate domain.

Private
Applies when a computer is connected to a private network location, such as a home or work place.

Public
Applies when a computer is connected to a public network location.

Name:

Description (optional):