Crestron® PinPoint™ App

Deployment Guide

Crestron Electronics, Inc.

This document was written by the Technical Publications department at Crestron.

Contents

Crestron® PinPoint™ App User Guide

Introduction

The Crestron® PinPoint™ app works with Crestron Fusion® software and PP-100 proximity detection beacons to manage meetings, to locate available meeting spaces, to share presentations over an AirMedia® presentation gateway, and more, all from a mobile device.

Infrastructure

The PinPoint app and the Crestron Beacon Setup Pro installer app must run on a device connected to a network with access to the Crestron Fusion server.

Using the PinPoint App with a Wi-Fi® Connection

The PinPoint app can connect to the same network as the Crestron Fusion server using a Wi-Fi or a VPN connection. Many enterprises limit network access for mobile devices. To use the PinPoint app, ensure that the mobile device VLAN has a path to the Crestron Fusion server.

Using the PinPoint App Over a Cellular Data Connection

For an on-premises or a privately hosted Crestron Fusion installation, mobile devices that run the PinPoint app using cellular data must achieve IP connectivity with the Crestron Fusion server. To achieve IP connectivity with the Crestron Fusion server, one or more of the following requirements may be necessary:

- An inbound connection to the Crestron Fusion server from the Internet through the firewall on a static IP address, with port 443 (SSL) connections allowed
- A primary (or secondary) Crestron Fusion server installed in the network DMZ
- Server hardening and other security considerations, such as excluding nonessential IIS directories that could widen the attack surface of the server

  For example, disable access to the Crestron Fusion web client by removing “/fusion/webclient” files from the IIS directory.

NOTE: Crestron-hosted Crestron Fusion installations are configured to be accessible publicly and do not need any special considerations.

DNS Considerations

The PinPoint app and the Crestron Beacon Setup Pro app must know the location of the associated Crestron Fusion server.

The apps first check the Crestron-hosted directory service for the location of the Crestron Fusion server. If the server is not found, the apps then try to connect to *fusion-mobile.company.tld*, where *company.tld* matches the domain name of the email address used to log in to the PinPoint app. For example, the user *joe@xyzcorp.com* would default to a server reachable at *fusion-mobile.xyzcorp.com*.

For on-premises deployments not using the Crestron Directory service, a DNS entry for *fusion-mobile.company.tld* must be added.

If this DNS entry is not found, the user needs to specify a domain name or an IP address of the server directly in the app settings. On iOS® devices, this process is done by entering the address in Settings > PinPoint > Domain or Settings > PinPoint > IP Address, respectively.

If the company uses a different authoritative DNS internally than it does externally (from the Internet), then both DNS records need to be modified to point at the appropriate private (internal) and public (external) hosts.

Multiple *company.tld* user email domains are supported only if those domains are federated together in one Active Directory. If this is not the case, only one of the multiple *company.tld* user domains is supported.

Authentication and Authorization

Active Directory® software is used to authenticate PinPoint app users and Crestron Beacon Setup Pro app users. Authentication is performed via on-premises Active Directory or Azure® Active Directory software (Azure AD) via Crestron Fusion, depending on where Crestron Fusion is deployed.

Use the following guidelines to authenticate users using on-premises Active Directory or Azure AD:

- Create an Active Directory group for PinPoint app users (for example, "PinPointUsers").
- Identify the PinPoint app users, and add them to the Active Directory group created for these users.
- Create an Active Directory group for installers using the Crestron Beacon Setup Pro app to set up the beacons, photos, and floorplans for rooms (for example, "PinPointInstallers").
- Identify the installers using the Crestron Beacon Setup Pro app, and add them to the Active Directory group created for these users.

SSO and Federation

If Azure AD is federated, the PinPoint app receives two tokens directly from the on-premises Active Directory: one for Azure AD and one for Office 365® software, if Office 365 is the scheduling provider. Office 365 must be authorized in the native app registered in Azure AD. Refer to “Additional Steps for a Federated Environment with Office 365” on page 14 for more information.

Certificates

Proper certificates on the device and on the Crestron Fusion web server are necessary for the PinPoint app to successfully communicate with the Crestron Fusion server.

In many enterprise environments, the Mobile Device Management (MDM) environment dictates how to distribute certificates to end user devices. If no MDM environment is in place, send the certificate as an attachment via email to the mailbox provisioned on the mobile device, and then open the attachment in the mail application. Follow the prompts to install the certificate. This process is needed for both the root certificate and any subordinate certificates used.

Custom CA certificates on iOS are stored in **Settings** > **General** > **Profiles & Device Management**.

PinPoint Apps

The PinPoint app can be downloaded from the respective app store for iOS or Android™ devices. The Crestron Beacon Setup Pro app is currently available only in the app store for iOS devices.

The PinPoint apps are supported on the following iOS devices:

- An iPhone® 4S device (or later) is required for the PinPoint app.
- An iPhone 5/5S (or later) is required for the Crestron Beacon Setup Pro app.

The following prerequisites are necessary for using the PinPoint apps:

- A cellular data network (for iPhone and cellular-equipped devices only) or a Wi-Fi network that is connected to the Internet
- An Apple® software ID (if using an iPhone)
- Bluetooth® communications that are enabled on the iOS or Android device

Application Downloads

Use the following procedure to download the PinPoint app or the Crestron Beacon Setup Pro app (iOS only) on a mobile device:

1. On the device’s home screen, tap the Apple App Store® application icon (for iOS devices) or the Google Play™ store application icon (for Android devices).
2. Search for the app:
   a. Tap **Search**.
   b. Tap the search field, and enter the search term “Crestron.”
   c. Tap **Search** again. The Crestron apps are listed.
3. Tap the PinPoint app icon or the Crestron Beacon Setup Pro app icon, and then follow the prompts.

   The device downloads the app. The app’s icon appears on the home screen and displays the download and installation status.

Corporate Deployments

Many corporate enterprises have an MDM process to deploy apps to corporate iPhones and other mobile devices. There are different options and requirements for MDM integration, so Crestron engineering must be engaged to build the best option for an individual customer deployment.

Configuring Crestron Fusion

The Crestron Fusion Configuration web client includes parameters to define the Active Directory groups, to add Client IDs and Keys from Azure AD, to set up PinPoint app notifications, and to confirm licensing.

PinPoint Licensing

The PinPoint apps are free to download; the licensing is priced per user and is set and managed in Crestron Fusion. The PinPoint license comes with a license key, a user count, and a license expiration date.

Installations of Crestron Fusion that do not have a paid license for PinPoint include five free PinPoint user seats for testing purposes. For a licensed copy, the count of the PinPoint users in the system is checked against the licensed user count. New users are allowed to log in even if they exceed the license count; however, the overage information is logged and provided for audit.

License checks are performed using the license expiration date, and all users are denied access if the PinPoint license has expired.

For informational purposes, PinPoint users can be identified in the Crestron Fusion Setup web client by navigating to Objects > People and then viewing the "PinPoint User" column in the "People" table.

In installations with a paid PinPoint license, the Crestron Fusion Configuration web client has a button to sync PinPoint users. This feature compares the PinPoint users in Crestron Fusion with those allowed in Active Directory and sends an email notification to the address set using the License Notification Email field (which can be found by navigating to Configuration > PinPoint) when the number of users using the system exceeds the licensed user count.

Settings in Crestron Fusion Configuration

The properties listed in this section can be set using the Crestron Fusion Configuration web client. Use the following procedure to configure these properties:

1. Navigate to Configuration > PinPoint in the Crestron Fusion Configuration web client.
2. Type the company name in the Company Name text field in the "Settings: PinPoint" table.

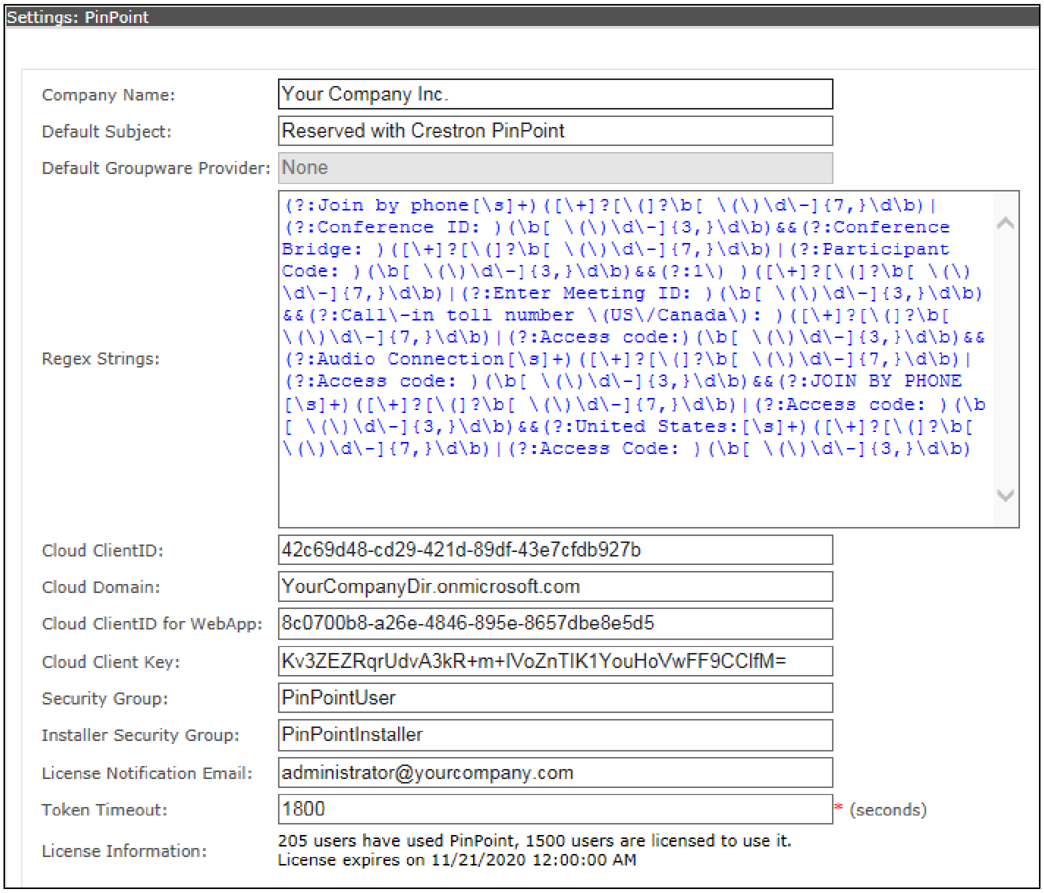
The table on the following page describes the subsequent fields that can be configured:

Crestron Fusion Configuration Settings

FIELD	DESCRIPTION
Default Subject	This field is used to automatically populate the meeting subject field with text when booking a meeting from the PinPoint app.
Default Groupware Provider	This read-only field is populated by the **DefaultGroupwareProvider** property in the **Settings: All** page in the Configuration web client.
Regex Strings	This text box is a prepopulated regular expression used by the PinPoint app to parse meeting details from the body of the meeting invite for one-touch connections. The included example string may need to be modified if the company uses custom meeting invitation sections in the body of messages sent by users. The default strings support the formatting for the following programs: the Lync® application or the Skype® application for business, the WebEx® application, and the BlueJeans application.
Cloud Client ID Cloud Domain Cloud Client ID for Web App Cloud Client Key	These fields are used for Azure AD implementations only. Obtain these settings from the Active Directory administrator. If Crestron Fusion is used with the PinPoint app on-premises, these fields are not necessary.
Security Group	Configure an Active Directory or Azure AD group that includes the end users authorized to use the PinPoint app, and enter the group name in this field. Do not specify this field in domain format; use the group name only.
Installer Security Group	Configure an Active Directory or Azure AD group that includes the end users authorized to use the Crestron Beacon Setup Pro app, and enter the group name in this field. Do not specify this field in domain format; use the group name only.
License Notification Email	Enter the email address that should receive email notifications about license information in this field.
Token Timeout	Enter the duration that it takes for a token to time out. The recommended default is 1800 seconds, or 30 minutes. This information is used for security purposes and logs out a user who is no longer authorized.

Simple Mail Transfer Protocol (SMTP) settings are required in Crestron Fusion in order for PinPoint licensing notifications to be sent. From the Crestron Fusion Configuration web client, click the **Configuration** tab, and select the **SMTP** folder. Enter the parameters for the SMTP server and the email address.

Example Settings for Crestron Fusion Configuration



Settings: PinPoint

Company Name:	Your Company Inc.
Default Subject:	Reserved with Crestron PinPoint
Default Groupware Provider:	None

Regex Strings:

```
(?:Join by phone[\s]+)([\+]?[\(]?\b[ \(\)\d\-]{7,}\d\b)|
(?:Conference ID: )(\b[ \(\)\d\-]{3,}\d\b)&&(?:Conference
Bridge: )([\+]?[\(]?\b[ \(\)\d\-]{7,}\d\b)|(?:Participant
Code: )(\b[ \(\)\d\-]{3,}\d\b)&&(?:1\) )([\+]?[\(]?\b[ \(\)
\d\-]{7,}\d\b)|(?:Enter Meeting ID: )(\b[ \(\)\d\-]{3,}\d\b)
&&(?:Call\-in toll number \(US\/Canada\): )([\+]?[\(]?\b[
\(\)\d\-]{7,}\d\b)|(?:Access code:)(\b[ \(\)\d\-]{3,}\d\b)&&
(?:Audio Connection[\s]+)([\+]?[\(]?\b[ \(\)\d\-]{7,}\d\b)|
(?:Access code: )(\b[ \(\)\d\-]{3,}\d\b)&&(?:JOIN BY PHONE
[\s]+)([\+]?[\(]?\b[ \(\)\d\-]{7,}\d\b)|(?:Access code: )(\b
[ \(\)\d\-]{3,}\d\b)&&(?:United States:[\s]+)([\+]?[\(]?\b[
\(\)\d\-]{7,}\d\b)|(?:Access Code: )(\b[ \(\)\d\-]{3,}\d\b)
```

Cloud ClientID:	42c69d48-cd29-421d-89df-43e7cfdb927b
Cloud Domain:	YourCompanyDir.onmicrosoft.com
Cloud ClientID for WebApp:	8c0700b8-a26e-4846-895e-8657dbe8e5d5
Cloud Client Key:	Kv3ZEZRqrUdvA3kR+m+lVoZnTlK1YouHoVwFF9CClfM=
Security Group:	PinPointUser
Installer Security Group:	PinPointInstaller
License Notification Email:	administrator@yourcompany.com
Token Timeout:	1800 * (seconds)
License Information:	205 users have used PinPoint, 1500 users are licensed to use it. License expires on 11/21/2020 12:00:00 AM

Crestron Fusion All Configuration Parameter Guide

The PinPoint app parameters highlighted in yellow can be configured by navigating to Configuration > All in the Crestron Fusion Configuration web client. Refer to "Settings in Crestron Fusion Configuration" on page 4 for more information.

Crestron Fusion All Configuration Parameters

Parameter	On-Prem	FITC	FITC - Federated
CEMAAllowedAppsFITC	AppStore|Enterprise	AppStore|Enterprise	AppStore|Enterprise
CEMAAllowedAppsOnPrem	AppStore|Enterprise	AppStore|Enterprise	AppStore|Enterprise
CEMAClientKey	*not used*	*from Azure*	*from Azure*
CEMACloudClientID	*not used*	*from Azure*	*from Azure*
CEMACloudClientIDWebApp	*not used*	*from Azure*	*from Azure*
CEMACloudDomain	*not used*	*from Azure*	*from Azure*
CEMACompanyName	*end user provided*	*end user provided*	*end user provided*
CEMADefaultSubject	Reserved with Crestron PinPoint	Reserved with Crestron PinPoint	Reserved with Crestron PinPoint
CEMALicenseNotificationEMail	*administrator*	*crestron administrator*	*crestron administrator*
CEMALicenseSubject	%Company%	%Company%	%Company%
CEMAOffice365ResourceURL	*not used*	*not used*	https://outlook.office365.com/
CEMASecurityGroup	*end user provided*	*end user provided*	*end user provided*
CEMASecurityGroupInstaller	*end user provided*	*end user provided*	*end user provided*
CEMASMTPHostAddress	*android only*	*android only*	*android only*
CEMASSLValidation	True	True	True
CEMATokenTimeout	1800	1800	1800
isFITC	False	True	True
CEMAFederated	False	False	True
FITCSSLCertSubject	*match cert*	*.crestronfusion.com	*.crestronfusion.com
UseSSLFITC	True	True	True

Proximity Data Setup in Crestron Fusion

The PinPoint app uses GPS data, Geographical Region Information, Beacon detection, Location, and Adjacent Location fields to locate and provide a list of available, nearby rooms.

When the end user searches for rooms using the PinPoint app, an HTTPS request is sent to the PinPoint web service (CEMA). The sequence below describes how the web service builds the room results.

1. The web service receives the request and processes results based on the following conditions.
    a. The web service attempts to identify the closest room to the handheld device, which is the Origin Room.
        i. If the GPS location is sent in the request from the device, then the web service finds the room with the closest GPS location.
        ii. If the Bluetooth beacon ID is sent in the request from the device, then the web service finds the room with the matching Bluetooth beacon ID.
        iii. If no room is located using the GPS location or Bluetooth beacon ID, then an error is returned to the device.
    b. If the Origin Room has regional data associated with it, then web service does the following:
        i. Loads rooms from the parent region of the Origin Room
        ii. Groups rooms with matching regional information into the Nearby group
        iii. Groups rooms without matching regional information into the Other Rooms group
        iv. Sorts the Nearby group by GPS proximity to the Origin Room
        v. Sorts the Other Rooms group by GPS proximity to the Origin Room
        vi. Joins the Nearby and the Other Rooms groups into a single list
    c. Else If the Origin Room has GPS data associated with it, then the web service does the following:
        i. Loads all of the rooms
        ii. Groups rooms with the matching GPS location into the Nearby group
        iii. Groups rooms without the matching GPS location (including no GPS) into the Other Rooms group
        iv. Sorts the Nearby group by GPS proximity to the Origin Room
        v. Sorts the Other Rooms group by GPS proximity to the Origin Room
        vi. Joins the Nearby and the Other Rooms groups into a single list
    d. Else If the Origin Room has the Location field set, then the web service does the following:
        i. Loads all of the rooms
        ii. Groups rooms with a matching Location field into the Nearby group

        iii. Groups rooms without a matching Location field into the Other Rooms group

        iv. (Skip sorting)

        v. (Skip sorting)

        vi. Joins the Nearby and the Other Rooms groups into single list

    e. **Else If** the Origin Room has the Adjacent Location field set, then the web service does the following:

        i. Loads all of the rooms

        ii. Groups rooms with a matching Adjacent Location field into the Nearby group

        iii. Groups rooms without a matching Adjacent Location field into the Other Rooms group

        iv. (Skip sorting)

        v. (Skip sorting)

        vi. Joins the Nearby and the Other Rooms groups into a single list

2. The list is built, and the web service moves the Origin Room to top of the list.
3. If the **CEMASuppressNonReservableRooms** parameter is set to "True" in All Configuration, then the web service removes all rooms with GroupwareID="NonReservable" from the list.
4. If the phone sends asset type IDs in the search request from the PinPoint client app, then the web service removes all rooms with the NO asset matching any asset type ID sent in the request.
5. The web service returns the room list to the PinPoint app.

Geographical Region Information

- Add or remove geographic region fields as necessary to best describe the room layouts of the organization by navigating to **Objects** > **Geographic Regions** in the Crestron Fusion Setup web client. The default fields are **Country**, **State**, **City**, and **Street**.
- Edit each node and enter geographic information by selecting the **Address** tab in the **Edit - Room** window for a particular room. Each Crestron Fusion node should reflect the geographic hierarchy of the organization.
- For each room, complete the geographic information if the values inherited from the node are not complete. If necessary, the fields can be left blank.

GPS Locations of Rooms and Nodes

- Enter the GPS coordinates of any nodes that may reflect a particular area of the geographic hierarchy of the organization.
- For each room, enter the GPS coordinates at the highest available resolution if the inherited value is not granular enough.

Location and Adjacent Location Fields

- Logically group the rooms together using associating terms (for example, 2nd Floor East Wing, Demo Area South Building).
- Enter the associating term for each room.

Room Configuration

Geographical Coordinates, **Room Type**, **Capacity**, **Adjacent Location**, and **Air Media Info** are properties of the room in Crestron Fusion that support the PinPoint app. Select the **Room Details** tab in the **Edit - Room** window for a particular room to configure these properties.

- **Geographical Coordinates** are the latitude and longitude of the room in degrees and minutes.
- **Room Type** defines the type of a room, including **Small**, **Medium**, **Large**, or **Boardroom**. Room Types may be defined by following these steps:
    a. Open the Crestron Fusion Setup web client.
    b. Navigate to **Objects** > **Room Types**.
    c. Add, edit, and delete room types as necessary using the buttons above the "Room Type" table.
- **Capacity** is an integer defining the seating capacity of the room.
- **Adjacent Location** assists with room searches. The PinPoint app performs room searches by using GPS, region data, location, and the adjacent location. The PinPoint app returns the rooms closest to the beacon at the top of the list. Any room with an **Adjacent Location** field matching the closest room is placed next in the search results.
- **Air Media Info** contains the AirMedia AM-100 or AM-101 IP address and security code if the room includes an AirMedia device. The PinPoint app uses this field to operate one-button presentations via AirMedia. The security code should be set to static. Rotating keys work only if the AirMedia device is directly connected to Crestron Fusion.

Crestron Beacon Setup Pro App

For more information about setting up Crestron Beacon, refer to the Crestron Beacon Setup Pro App User Guide (Doc. 7896) at www.crestron.com/manuals.

Functions

The Crestron Beacon Setup Pro app assigns PP-100 beacons to spaces and configures the strength of each beacon.

The Crestron Beacon Setup Pro app performs the following tasks:

- Associates a PP-100 beacon with an existing room in Crestron Fusion
- Configures the Bluetooth signal strength of the beacon
- Determines coverage for the beacon signal and any overlapping signals

- Adds photos that reference the space for wayfinding, including the following:
    - A floor plan highlighting the room
    - The room entryway
    - A beauty shot showing features and configurations

Prerequisites

The following prerequisites are necessary for using the Crestron Beacon Setup Pro app:

- An iPhone 4S (or later); an iPad® device in iPhone mode, 3rd generation (or later); an iPad mini™ device (or later); an iPod touch® device, 5th generation (or later); an iOS 7 based device (or later, iOS 9 preferred)

  NOTE: iPad devices must have at least 1 GB of RAM for reliable performance.

- A mobile device that is Bluetooth enabled
- A mobile broadband or Wi-Fi network (required for connection to the Crestron Fusion server)
- A Crestron Fusion server configured with a valid SSL certificate and HTTPS

Beacon Placement Best Practices

The following are best practices for placing a beacon:

- Place the beacon in the center of the room.
- Do not install the beacon in a sealed, metal enclosure.
- Install the beacon in an easily accessible location.
- Install the beacon in a location that is out of sight.
- If installing the beacon in the center of the room is not possible, do the following:
    - Install the beacon in a wall outlet on the farthest wall from other rooms containing beacons to reduce overlap.
    - Install the beacon in outlets with built-in USB connectors (if possible).

Provisioning Active Directory

There are several different methods for handling identity information for logging into the PinPoint app using Active Directory (AD):

- Crestron Fusion with On-Premises AD
- Azure AD synchronized with On-Premises AD

  Refer to "Azure AD" on page 11 for more information.

- Azure AD with Office 365 (no on-premises AD)

  The customer's Active Directory exists in Azure. Follow the application registration process “Register the Crestron Fusion Server as a Native Client Application” on page 13 and “Register the Crestron Fusion Server as a Web Application” on page 13.

- Federated Identity Provider, Azure AD with Office 365

  Follow the procedure in “Additional Steps for a Federated Environment with Office 365” on page 14 with additional settings for federated deployments.

Crestron Directory Service

On startup, the PinPoint app automatically contacts the Crestron directory service, which supplies the domain hostname information used to contact the Crestron Fusion server. For all Crestron Fusion hosted PinPoint app deployments, this directory entry is maintained by Crestron and is set to the hostname of the Crestron Fusion server.

If the Directory Service is not configured, the PinPoint app tries to connect to *fusion-mobile.company.tld*, where *company.tld* matches the domain name of the email address used to log in to the PinPoint app.

For an on-premises deployment, the end user should add a DNS entry for *fusion-mobile.company.tld*.

The app startup workflow is described below.

- Query the Crestron directory service at https://fitclookup.crestronfusion.com/fitc/sitelinks?val=@*company.tld* using a hashed version of the user’s login domain.
- If the web service returns a FITC domain and the FITC domain is DNS resolvable, then the FITC domain is stored and used for further connections.
- If the web service does not return a FITC domain or the FITC domain is not DNS resolvable, an FQDN (fully qualified domain name) is created by concatenating “fusion-mobile” with the domain from the user login (for example, *fusion-mobile.xyzcorp.com*), and the FQDN is stored if it resolves.
- If the above request fails, the app tries to resolve using the previously stored hostname, if any.

Azure AD

The majority of the PinPoint app or Crestron Fusion configuration revolves around authenticating users to the company Active Directory.

The PinPoint app automatically contacts a Directory Service for Crestron Fusion, which supplies the domain hostname information necessary for contacting the server that is servicing the account based on the domain name of the email address used to log in to the PinPoint app. For Crestron Fusion Cloud hosted deployments, this directory entry is maintained by Crestron and is set to the hostname of the Crestron Fusion cloud server. Refer to “Crestron Directory Service” above.

For Crestron Fusion Cloud deployments, the customer must have Azure AD configured. Typically, Azure AD is already configured for companies supporting Office 365, and there is an existing *azurename.onmicrosoft.com* directory account.

For those companies not already supporting this configuration, one or more system on the enterprise network needs to be configured with Microsoft® Azure Active Directory Connect to synchronize the company directory with the cloud. A user with Enterprise Admin access to the on-premises Active Directory is required to install this software

Azure AD Setup

The four basic steps for the Azure AD setup are summarized below. The sections following these steps describe them in more detail.

1. Set up the Azure Active Directory synchronization. The end user must complete this task to synchronize Azure AD with the on-premises AD.
2. In Azure AD, register Crestron Fusion server as a native client application. Then, add the generated Cloud Client ID to the Crestron Fusion Configuration web client.
3. In Azure AD, register Crestron Fusion server as a web application. This task is used to synchronize users between Crestron Fusion and Azure AD. Then, add the generated Cloud Client ID for WebApp to the Crestron Fusion Configuration web client.
4. In Azure AD, generate the Client Key for the Web Application. Then, add the generated Key to the Crestron Fusion Configuration web client.

Set up the Azure Active Directory Synchronization

This task is typically already completed by the end user. A user with Global Admin access to the Azure Active Directory is needed to set up the Azure Active Directory synchronization.

1. Log in to the Azure Management Portal for the company.
2. Create an Azure Active Directory domain. A DNS record with the domain name registrar is required to confirm ownership of the domain. Use the instructions below to create either a TXT or MX record type for a domain that is registered at the registrar. For more information, refer to https://azure.microsoft.com/en-us/documentation/articles/active-directory-add-domain/.
3. Assign a user Global Admin privileges in Azure AD.
4. Install the AD synchronization tool, Azure AD Connect, on an on-premises system (typically a file server), and then sync the on-premises directory to the cloud using an account that has Enterprise Admin access in the on-premises environment.

   Typically, synchronization is scheduled for every three hours, and user changes take up to three hours to propagate to the cloud.

   NOTE: If synchronizing multiple on-premises Active Directory forests, specify a custom installation when installing, and specify how to match or how to merge user identities that exist across multiple directories.

   Once the synchronization completes, the users and groups from the on-premises directory are visible in the Azure Active Directory.
5. Record the name of the directory domain in the Crestron Fusion Configuration web client by navigating to **Configuration** > **PinPoint**, and then record the domain name using the form *domainName.onmicrosoft.com* in the **Cloud Domain** field.

Register the Crestron Fusion Server as a Native Client Application

Follow this procedure for registering the Crestron Fusion server as a native client application. For more information, refer to “Appendix E: Azure AD Detailed Configuration” on page 26.

1. Log in to the Azure Management Portal for the company.
2. Under **Applications**, add an application to authorize Crestron Fusion to authenticate PinPoint app users in the Azure AD domain.
    a. Name the application. The name must be unique.

    b. Select **Native Client Application**.

    c. Provide the Redirect URI, a unique identifier name for *fusionserver.company.tld*.

    d. Under the **Configure** tab, grant the new application read directory data permission.
3. Record the generated Client ID in the Crestron Fusion Configuration web client by navigating to **Configuration** > **PinPoint**, and then enter the generated ID in the **Cloud ClientID** field.

Register the Crestron Fusion Server as a Web Application

This function synchronizes users between Crestron Fusion and Azure AD and is used to true-up the licensed users for the PinPoint app with Azure AD. For more information, refer to “Appendix E: Azure AD Detailed Configuration” on page 26.

1. Log in to the Azure Management Portal for the company.
2. Under **Application**s, add an application to authorize Crestron Fusion to authenticate the PinPoint app users in the Azure AD domain.
    a. Name the application. The name must be unique.

    b. Select **Web Application**.

    c. Provide the sign-on URL. This URL can be the directory domain name, recorded as above, *domainName.onmicrosoft.com*, or *fusionserver.company.tld*.

    d. Provide the App ID URI. This URI is a unique identifier name for *appID.onmicrosoft.com* or *fusionserver.company.tld*.

    e. Under the **Configure** tab, grant the new web application read directory data permission.

    f. Select a duration and record the "expires on date" in a calendar with a reminder to renew this key in the future.
3. Record the generated Client Key as the Cloud Client Key in the Crestron Fusion Configuration web client by navigating to **Configuration** > **PinPoint**, and then enter the generated key in the **Cloud Client Key** field. Copy this key immediately after it is generated or it will not be retrievable.

NOTE: One or more *company.tld* user email domains are supported for all PinPoint app users if those domains are federated together in one on-premises Active Directory or are consolidated into a single Azure Active Directory; otherwise, a single *company.tld* user domain is supported.

Additional Steps for a Federated Environment with Office 365

Customers in a federated environment use the on-premises identity provider for authentication.

When the PinPoint app detects that the customer has federation enabled, it redirects the users to an on-premises login page for authentication. Upon successful authentication, the PinPoint app requests two tokens:

- Token for Azure AD: This token is needed by the PinPoint app for authentication and to verify that the user is part of the PinPoint app user security group.
- Token for Office 365: This token is needed to retrieve meetings and to book meetings.

The device makes requests with these tokens to the Crestron Fusion CEMA web service.

Configuration Settings in Crestron Fusion for Federated Environments

In a federated environment, set the following configuration variables:

- CEMAFederated: True
- CEMARedirectURI: Provided by the customer upon registration of the native application in Azure AD. Example: *https://companyuri.onmicrosoft.com*
- CEMAOffice365ResourceURL: *https://outlook.office365.com/*

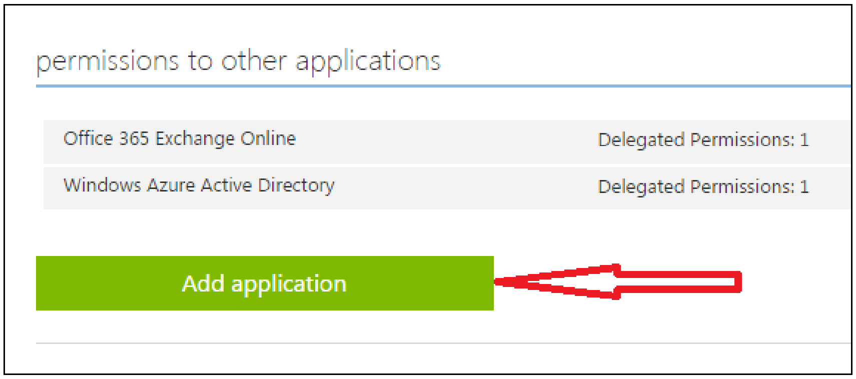
Changes to Azure AD for Federated Environments

The native application registered in Azure AD must have access to Office 365.

Follow this procedure to enable the application in Azure AD to access Office 365:

1. Open the native application, select the **Configure** tab, and scroll down to **permissions to other applications**. Select **Add application**.

   Configure Tab - permissions to other applications

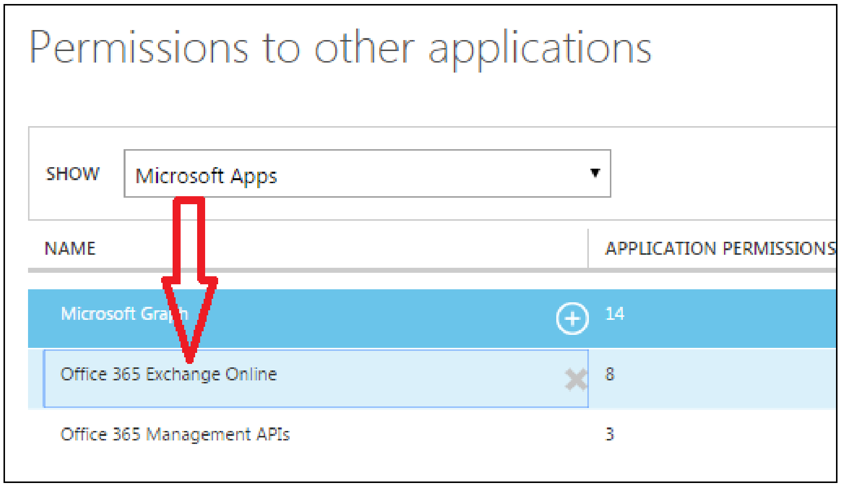


permissions to other applications

Office 365 Exchange Online	Delegated Permissions: 1
Windows Azure Active Directory	Delegated Permissions: 1

2. Select **Office 365 Exchange Online**.

Permissions to other applications



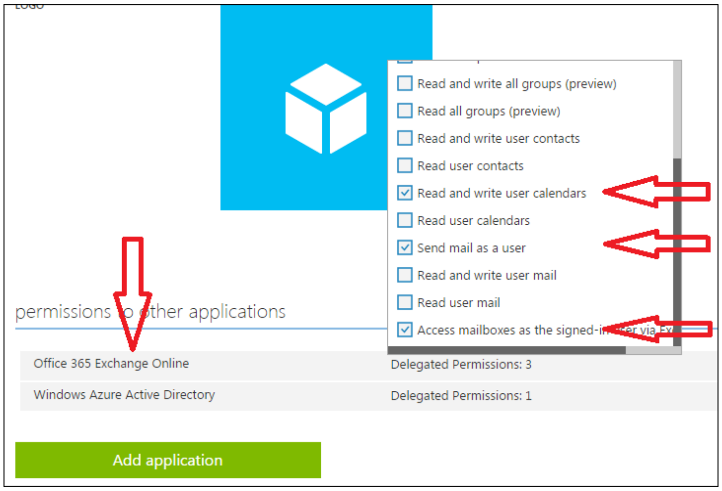
Permissions to other applications

SHOW: Microsoft Apps ▾

NAME	APPLICATION PERMISSIONS
Microsoft Graph	14
Office 365 Exchange Online	8
Office 365 Management APIs	3

3. Select the delegated permissions.

Selecting the Delegated Permissions



- ☐ Read and write all groups (preview)
- ☐ Read all groups (preview)
- ☐ Read and write user contacts
- ☐ Read user contacts
- ☑ Read and write user calendars
- ☐ Read user calendars
- ☑ Send mail as a user
- ☐ Read and write user mail
- ☐ Read user mail
- ☑ Access mailboxes as the signed-in user via Ex

permissions to other applications

Office 365 Exchange Online	Delegated Permissions: 3
Windows Azure Active Directory	Delegated Permissions: 1

a. Select the following delegated permissions: **Read and write user calendars**, **Send mail as a user**, and **Access mailboxes as the signed-in user via Exchange.** (Refer to the above image.)

b. Select the following application permissions: **Read Active Directory Groups in the Web App AD setup** (not shown in the above image).

Troubleshooting

The following sections provide information for possible trouble situations.

Verify Connectivity

The PinPoint app must, at a minimum, achieve IP connectivity with the Crestron Fusion server. In an on-premises installation, this connection must be available from the Wi-Fi network, from a VPN connection, or directly from the cellular data network.

Perform the following procedure to confirm that a mobile device can reach the Crestron Fusion server:

1. On the mobile device running the app, open a web browser, and connect to the Crestron Fusion server using the address below.
   Example: *http(s)://<Fusion server IP* or *hostname>/fusion/webclient/*

   If the connection resolves and returns a login screen, the DNS is working.

   If the connection does not resolve, try connecting by the IP address to rule out any DNS problems. Verify that the DNS includes a record for the Crestron Fusion Server name being used.

2. Verify that the user account is in the optional Crestron Directory Service. Try the following link with the encoded user name:

   https://fitclookup.crestronfusion.com/fitc/sitelinks?val=7c9d872cf15acecabb4e1bd2e04f51023948877b2ad80c10a9f772065abcb83d<*@company.tld*>

   - The user name is hashed using SHA-256. Universal Encoding Tool. A tool that can create the hash for a particular user can be found at https://unenc.com.
   - If the entire organization is listed in the Crestron Directory Service, use the below URL without the hash:

     https://fitclookup.crestronfusion.com/fitc/sitelinks?val=<*@company.tld*>

3. Test the connection to the CEMA web service running on the Crestron Fusion server using the following address, .

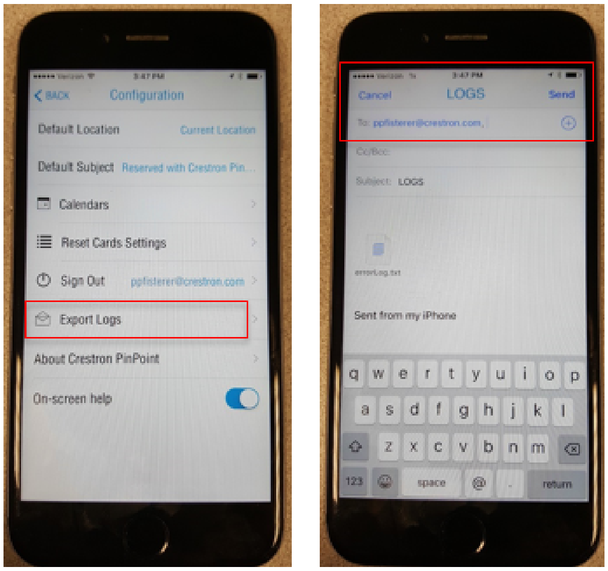
   https://<*yourserver*>/Fusion/CEMA/Versions?PinPointMinAPIVersion=1&PinPointMaxAPIVersion=1&AppVersion=1.2.2.298&AppPlatform=iOS&AppName=PinPoint&AppType=AppStore

PinPoint App Log

Check the logs on the phone or device running the PinPoint app using the following procedure.

1. Launch the PinPoint app.
2. Click the **Configuration** gear icon.
3. Select **Export Logs**.
4. Enter a recipient email address.
5. Press **Send**.

Configuration - Export Logs



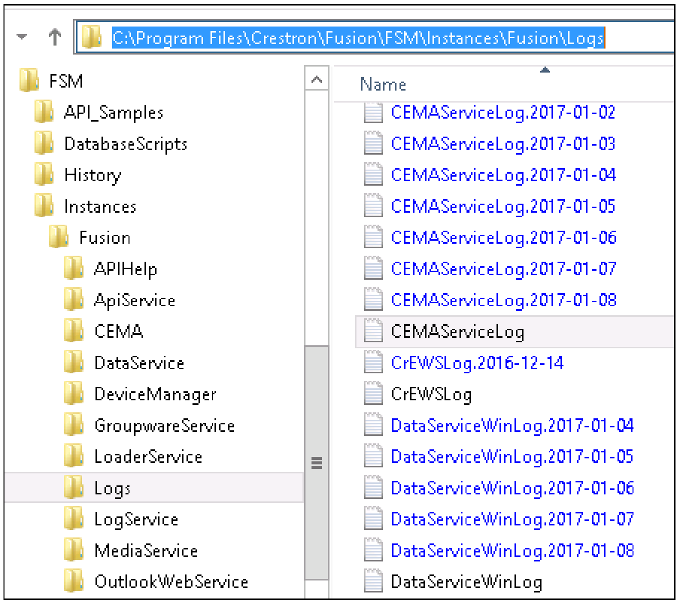
CEMA Web Service Log

The CEMAServiceLog is located with the other Crestron Fusion logs. The log is created after a successful login from PinPoint app has occurred.

The log includes the following:

- User login audits
- Licensing audits

Crestron Fusion Logs - CEMA Web Service Log



C:\Program Files\Crestron\Fusion\FSM\Instances\Fusion\Logs

FSM
API_Samples
DatabaseScripts
History
Instances
Fusion
APIHelp
ApiService
CEMA
DataService
DeviceManager
GroupwareService
LoaderService
Logs
LogService
MediaService
OutlookWebService

Name
CEMAServiceLog.2017-01-02
CEMAServiceLog.2017-01-03
CEMAServiceLog.2017-01-04
CEMAServiceLog.2017-01-05
CEMAServiceLog.2017-01-06
CEMAServiceLog.2017-01-07
CEMAServiceLog.2017-01-08
CEMAServiceLog
CrEWSLog.2016-12-14
CrEWSLog
DataServiceWinLog.2017-01-04
DataServiceWinLog.2017-01-05
DataServiceWinLog.2017-01-06
DataServiceWinLog.2017-01-07
DataServiceWinLog.2017-01-08
DataServiceWinLog

General Troubleshooting Notes

Refer to the following notes for general troubleshooting information:

- Do not use spaces in group names when creating Active Directory groups. For example, use "PPUsers" and not "PP Users."
- Active Directory groups cannot be nested inside other groups.
- Use the following entries for the below All Configuration parameters:
    - CEMAAllowedAppsOnPrem should be set to "Enterprise|AppStore."
    - ISFITC should be set to "True" for AzureAD, and "False" for On Prem AD.
    - CEMAFederated should be set to "True" if Azure AD is federated.
- The CEMA log appears only when a user is able to successfully log in to the Crestron Fusion server.

Error Message Reference

The following table describes common error messages that may appear when using the Crestron Fusion app.

Crestron Fusion App Error Messages

ERROR MESSAGE	EXPLANATION
There was a problem with this action. Please try again later.	This message is a general error message for a network request failure.
Authentication failed.	The username or password provided failed authentication.
Search did not return any results.	The search for rooms did not return any results.
Could not complete the action at this time. Please try again later.	A network request to Crestron Fusion reached the server, but the server returned a failure response.
There was a problem connecting to the server.	The DNS resolution failed for the domain trying to connect to a Crestron Fusion server.
There was a problem trying to validate the server SSL certificate. Please contact your administrator.	The Crestron Fusion server SSL certificate was not valid, or in case of a self-signed certificate, the certificate authority has not been installed on the phone.
Login failed, number of users exceeds maximum. Please contact your administrator.	The server user license has been exceeded.
License expired. Please contact your administrator.	The server user license has expired.
Login failed.	The credentials provided are incorrect, or there is some other problem authenticating the user.
Login failed. User not authorized in the security group. Please contact your administrator.	The login user credential provided is not a member of the security group authorizing users.
Login failed. Bad security group. Please contact your administrator.	The security group configured in Crestron Fusion is invalid for the domain.
This version of Crestron Fusion is no longer supported.	The app is too new for the Crestron Fusion server. The server version needs to be updated in order to work with the version of the client application.
This version of Crestron PinPoint is no longer supported.	The app needs to be updated in order to work with the version of Crestron Fusion installed.
This version of Crestron PinPoint is no longer supported (200VT).	The application type in the Crestron Fusion server indicates that the application downloaded is disallowed by the server. Contact the company IT department to determine how to download the PinPoint app.

Appendix A: On Premises Pre-Installation Checklist

The following list describes the steps that should be taken prior to installing the PinPoint apps for use within an on-premises Crestron Fusion installation.

- Verify that Crestron Fusion 10.2 (or later) is installed and running.
- Determine whether Crestron hosts the organization pointers in the Crestron Directory.

  If the pointers are not Crestron hosted, add *fusion-mobile.company.tld* to the DNS server, where *company.tld* matches the domain name of the email address used to log in to the PinPoint app.
- Create an Active Directory group for PinPoint app users (for example, "PinPointUsers").
- Identify the PinPoint app users, and add them to the Active Directory group created for these users.
- Create an Active Directory group for installers using the Crestron Beacon Setup Pro app to set up the beacons, photos, and floor plans for rooms (for example, "PinPointInstallers").
- Identify the installers using the Crestron Beacon Setup Pro app, and add them to the Active Directory group created for these users.
- Identify any MDM processes needed to deploy apps to corporate mobile devices; otherwise, download the PinPoint apps from the appropriate app store to the mobile devices. Understand the MDM permissions that may affect installing and using the PinPoint apps.
- Obtain Crestron PP-100 beacons and power supplies.
- Install the beacons in the designated conference rooms.
- Obtain a floor plan image for each room location for wayfinding.
- Install any required certificates on the mobile devices using the PinPoint apps and on the Crestron Fusion server.

Appendix B: Creating an SSL Certificate Using OpenSSL

For some development or Proof-of-Concept installations, it may be difficult to get the proper organizational certificates deployed. In order to test the PinPoint app without organizational certificates, use self-signed certificates instead.

OpenSSL provides tools for using self-signed certificates. OpenSSL can be acquired at https://www.openssl.org/.

Instead of paying a commercial Certificate Authority (CA) to create SSL certificates for the organization, use OpenSSL to act as the CA. The new custom CA certificate must be installed on each device. The devices then automatically trust any certificates issued based on the new OpenSSL root CA certificate.

Use the following procedures to create a CA root certificate with OpenSSL and to create certificates based on the root certificate.

Creating the CA Root Certificate

1. Create a private key file.

   ```
   openssl genrsa -out myCA.key 2048
   ```

2. Create the certificate.

   Set the days parameter to several years if it is not necessary to repeat this process immediately.

   ```
   openssl req -x509 -sha256 -new -key myCA.key -out myCA.cer -days 730 -subj /CN="My Custom CA"
   ```

The certificate file (myCA.cer) can be publicly shared and installed on iOS or other operating systems to act as a built-in, trusted root CA.

The private key file (myCA.key) is used only for creating new SSL certificates.

Creating Additional Certificates Based on This CA Root Certificate

A Client Signing Request (CSR) is required before a new subordinate certificate can be issued, similar to purchasing a commercial SSL certificate.

1. Create a private key.

   ```
   openssl genrsa -out mycert1.key 2048
   ```

2. Create the CSR.

   Ensure that the Common Name (CN) matches the server domain where the self-signed certificate will be installed:

   ```
   openssl req -new -out mycert1.req -key mycert1.key -subj /CN=www2.mysite.com
   ```

3. Use the CSR to create the certificate.

   ```
   openssl x509 -req -sha256 -in mycert1.req -out mycert1.cer -CAkey myCA.key-CA myCA.cer -days 365 -CAcreateserial -CAserial serial
   ```

The certificate file (mycert1.cer) can be installed on a web server and accessed from any iOS device that already has the CA certificate installed.

Installing the Certificate in IIS

To install the certificate in IIS, first convert the certificate to .pfx format:

```
openssl pkcs12 -inkey mycert1.key -in mycert1.cer -export -out mycert1.pfx
```

If IIS reports that the certificate is missing the root authority, export the custom ROOT CA as a .pfx file and install it in the server as described in “Creating the CA Root Certificate” on page 21.

For more information about installing the certificate in IIS, refer to "Appendix C: Installing Certificates in IIS" on page 23.

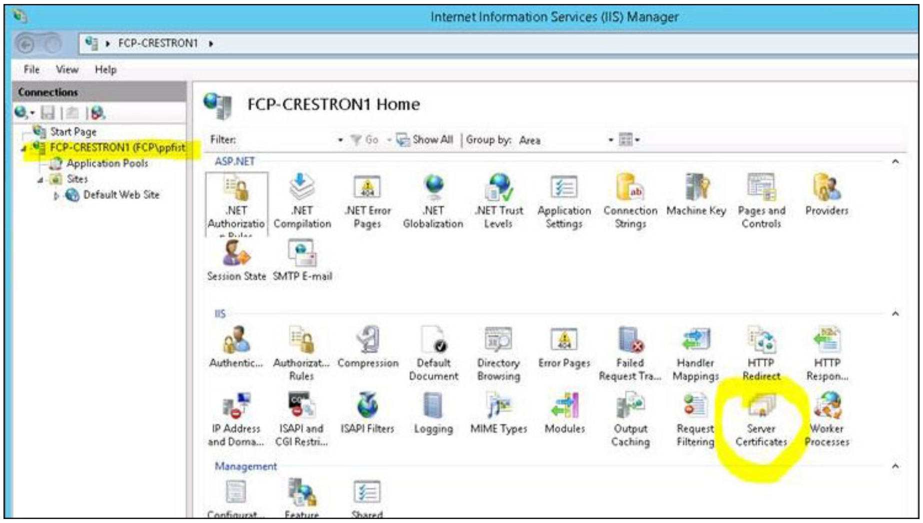
Appendix C: Installing Certificates in IIS

Use the following procedures to add a certificate to the Crestron Fusion IIS web server and to set the HTTPS bindings on the server to use that certificate.

If necessary, use OpenSSL to test created certificates. Refer to “Appendix B: Creating an SSL Certificate Using OpenSSL” on page 21.

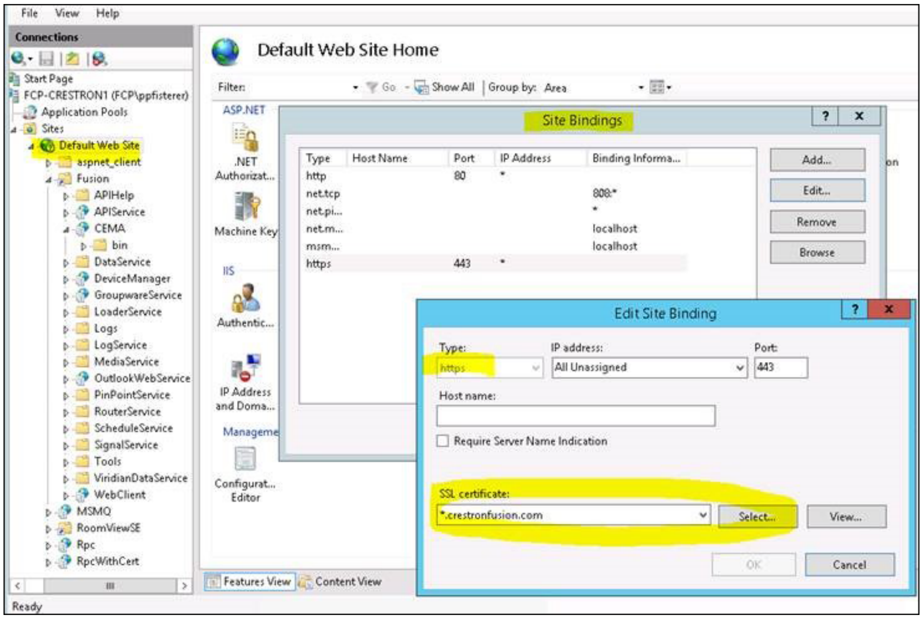
1. At the server level, select **Server Certificates**. The certificate is imported to this location.

Internet Information Services (IIS Manager)



2. At the default site, add the HTTPS type to the bindings, and select the certificate to be used.

Site Bindings - Edit Site Bindings



Type	Host Name	Port	IP Address	Binding Informa...
http		80	*	
net.tcp				808:*
net.pi...				*
net.m...				localhost
msm...				localhost
https		443	*	

Type: https

IP address: All Unassigned

Port: 443

Host name:

☐ Require Server Name Indication

SSL certificate: *.crestronfusion.com

Appendix D: Crestron Fusion All Configuration Properties

The following table describes the Crestron Fusion All Configuration properties for the PinPoint app.

All Configuration Properties

PROPERTY	DESCRIPTION	DEFAULT VALUE
Top of Form________________ CEMAAllowedAppsFITCBottom of Form	CEMAAllowedAppsFITC	AppStore|Enterprise
CEMAAllowedAppsOnPrem	CEMAAllowedAppsOnPrem	Enterprise
CEMAAPIVersion	API Version of server for PinPoint	1
CEMAClientKey		Ku3ZEZRqrUdvA3kR+m+IVoZmSHK1YoaHoVwEE9BBIfM=
CEMAClientURLForInstallerIOS	Installer client URL	
CEMAClientURLForPinPointIOS	PinPoint Client URL	
CEMACloudClientID		
CEMACloudClientIDWebApp		8c0700b8-a26e-4846-895e-7546cad8e4c4
CEMACloudDomain		CrestronDir.onmicrosoft.com
CEMACompanyName		Crestron Electronics Inc.
CEMADefaultSubject		Reserved with Crestron PinPoint
CEMAGraphResourceURL		https://graph.windows.net/me?api-version=1.6
CEMALicenseMessage		Licensed Users[%LicenseCount%], PinPoint Users[%PinPointCount%]
CEMALicenseNotificationEMail		bdonlan@crestron.com
CEMALicenseSubject		Crestron PinPoint Licensing Notification - %Company%
CEMAOffice365ResourceURL		https://outlook.office365.com/
CEMAPasscode		Crestron123

(Continued on the following page)

All Configuration Properties (Continued)

<table>
<tr><th>PROPERTY</th><th>DESCRIPTION</th><th>DEFAULT VALUE</th></tr>
<tr><td>CEMARegex</td><td></td><td>(?:Join by phone[\s]+)([\+]?[\(]?\b[\(\)\d\-]{7,}\d\b)|(?:Conference ID:)(\b[\(\)\d\-]{3,}\d\b)&&(?:Conference Bridge:)([\+]?[\(]?\b[\(\)\d\-]{7,}\d\b)|(?:Participant Code:)(\b[\(\)\d\-]{3,}\d\b)&&(?:1\))([\+]?[\(]?\b[\(\)\d\-]{7,}\d\b)|(?:Enter Meeting ID:)(\b[\(\)\d\-]{3,}\d\b)&&(?:Call\-in toll number \(US\/Canada\):)([\+]?[\(]?\b[\(\)\d\-]{7,}\d\b)|(?:Access code:)(\b[\(\)\d\-]{3,}\d\b)&&(?:Audio Connection[\s]+)([\+]?[\(]?\b[\(\)\d\-]{7,}\d\b)|(?:Access code:)(\b[\(\)\d\-]{3,}\d\b)&&(?:JOIN BY PHONE[\s]+)([\+]?[\(]?\b[\(\)\d\-]{7,}\d\b)|(?:Access code:)(\b[\(\)\d\-]{3,}\d\b)&&(?:United States:[\s]+)([\+]?[\(]?\b[\(\)\d\-]{7,}\d\b)|(?:Access Code:)(\b[\(\)\d\-]{3,}\d\b)</td></tr>
<tr><td>CEMASecurityGroup</td><td></td><td></td></tr>
<tr><td>CEMASecurityGroupInstaller</td><td></td><td></td></tr>
<tr><td>CEMASMTPHostAddress</td><td>CEMASMTPHostAddress</td><td></td></tr>
<tr><td>CEMASSLValidation</td><td></td><td></td></tr>
<tr><td>CEMATokenTimeout</td><td></td><td>1800</td></tr>
</table>

Appendix E: Azure AD Detailed Configuration

The following sections describe how to register the Crestron Fusion application on the Azure Management Portal for user authentication and for client authentication.

For User Authentication

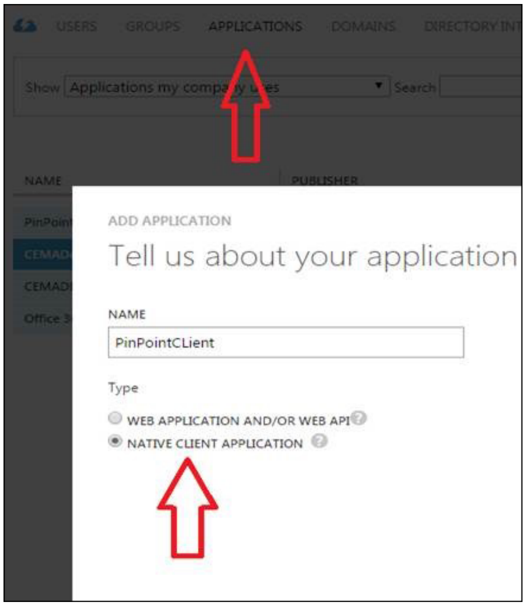
1. Register Crestron Fusion or the PinPoint app as a Native Client Application in the Azure Active Directory. This registration generates a Client ID, which is needed by the Crestron Fusion and PinPoint app to authenticate users. After adding the application, enter the following information in the Add Application window:

    - Name: Enter the name of the application. This name must be unique.
    - Type: Select Native Client Application.
    - Redirect URI: Enter a unique identifier of your application. This should point to the Crestron Fusion server.

      Example: https://*yourcompany*.crestronfusion.com

      In the case of a native application, the Redirect URI is a unique identifier to which Azure AD redirects the user-agent in an OAuth 2.0 request.

    Add Application Window

    ADD APPLICATION

    Tell us about your application

    NAME

    PinPointCLient

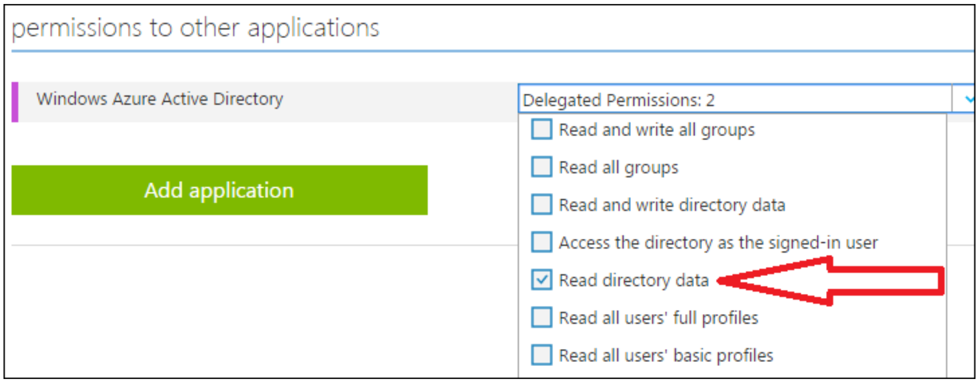
    Type

    ○ WEB APPLICATION AND/OR WEB API

    ● NATIVE CLIENT APPLICATION

2. From the Configure tab, grant Crestron Fusion and the PinPoint app permission to read user information from the Azure Active Directory by selecting the Read directory data option from the Delegated Permissions: 2 drop-down list.

Configure Tab - Permissions to other applications


permissions to other applications
Windows Azure Active Directory
Add application

Delegated Permissions: 2

- ☐ Read and write all groups
- ☐ Read all groups
- ☐ Read and write directory data
- ☐ Access the directory as the signed-in user
- ☑ Read directory data
- ☐ Read all users' full profiles
- ☐ Read all users' basic profiles

3. Enter values for the following fields, which can be accessed by navigating to Configuration > PinPoint in the Crestron Fusion Configuration web client.

    - Cloud ClientID is listed on the Configure tab of the Azure portal.
    - Cloud Domain is listed on the Domains tab of the Azure portal.
    - Security Group is the Active Directory group used for authenticating PinPoint app users.

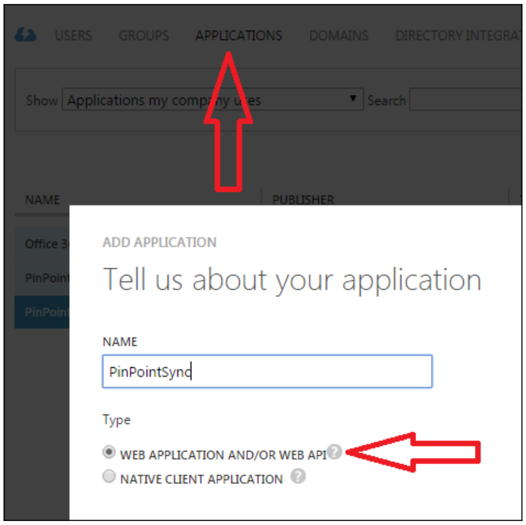
For Client Authentication

This procedure is used to synchronize the Azure Active Directory group for PinPoint app users with Crestron Fusion.

1. Register the PinPoint app as a Web Application in Azure Active Directory. This registration generates a ClientID and a ClientKey, which are required to synchronize users between Crestron Fusion and the Azure AD PinPoint app users group. After adding the application, enter the following information in the Add Application window:

    - Name: Enter the name of the application. This name must be unique.
    - Type: Select Web Application and Web API.
    - Sign-On URL: This is the URL where users can sign-in and use the app. Enter the Crestron Fusion URL.
    - Example: https://*yourcompany*.crestronfusion.com
    - App ID URI: Enter a unique URI for the application.
    - Example: https://*yourcompany*.crestronfusion.com

Add Application Window



Show Applications my company uses

ADD APPLICATION

Tell us about your application

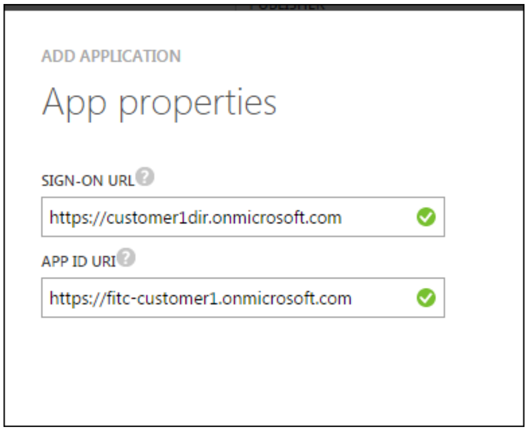
NAME: PinPointSync

Type

● WEB APPLICATION AND/OR WEB API

○ NATIVE CLIENT APPLICATION

Add Application Window - App properties



ADD APPLICATION

App properties

SIGN-ON URL: https://customer1dir.onmicrosoft.com

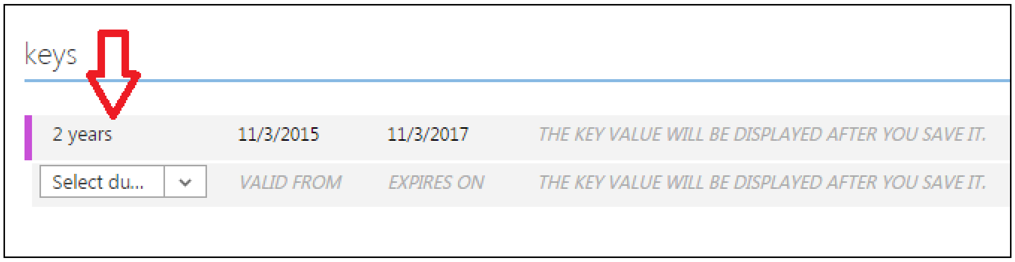
APP ID URI: https://fitc-customer1.onmicrosoft.com

2. From the **Configure** tab, generate the key for the web application. This key is commonly referred to as "client secret."

3. Use the **Select duration** drop-down menu to select a one-year key or two-year key. Notice that the value does not display immediately. Click **Save** to display the key.

NOTE: This key displays only once after **Save** is clicked. Be sure to record the key immediately once it displays, as it cannot be retrieved later and will have to be regenerated.

Configure Tab - keys

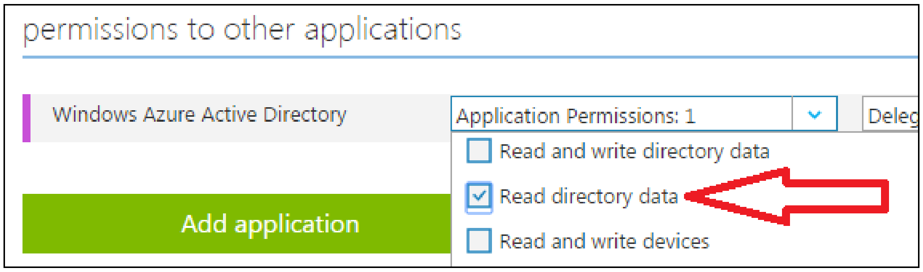


keys

2 years	11/3/2015	11/3/2017	THE KEY VALUE WILL BE DISPLAYED AFTER YOU SAVE IT.
Select du...	VALID FROM	EXPIRES ON	THE KEY VALUE WILL BE DISPLAYED AFTER YOU SAVE IT.

4. From the **Configure** tab, grant the PinPoint app permission to read user information from the Azure Active Directory by selecting the **Read directory data** option in the **Application Permissions: 1** drop-down list.

Configure Tab - permissions to other applications



permissions to other applications

Windows Azure Active Directory

Application Permissions: 1

☐ Read and write directory data

☑ Read directory data

☐ Read and write devices

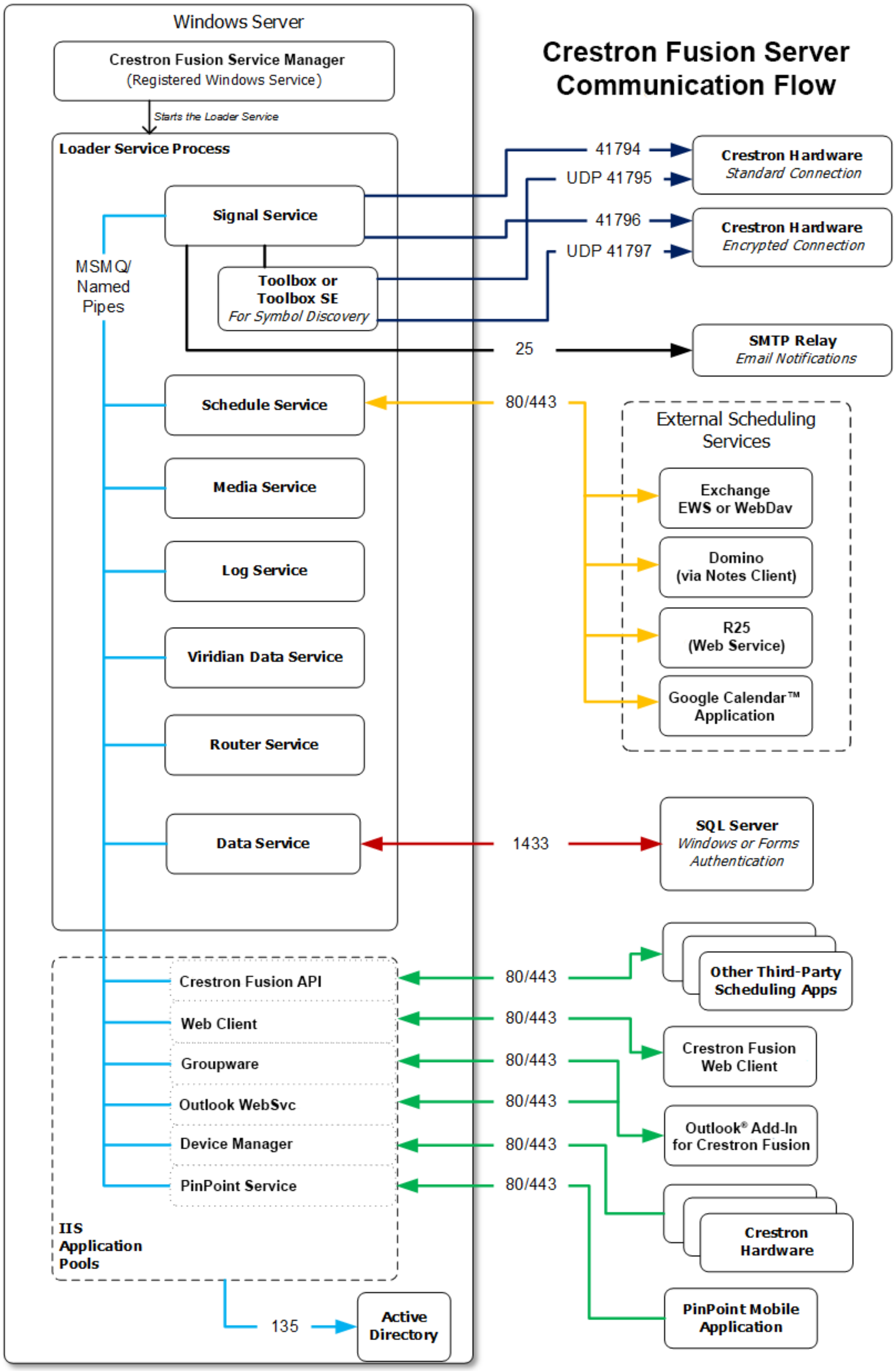
5. Enter values for the following fields, which can be accessed by navigating to **Configuration** > **PinPoint** in the Crestron Fusion Configuration web client.

    - **Cloud ClientID** is listed on the **Configure** tab of the Azure portal.
    - **Cloud Client Key** is listed on the **Configure** tab of the Azure portal.
    - **Cloud Domain** is listed on the **Domains** tab of the Azure portal.
    - **Security Group** is the Active Directory group used for authenticating PinPoint app users.

Appendix F: Network Communication Flow

The following diagram explains the network communication flow.

Crestron Fusion Server Communication Flow



Unless otherwise noted, all external ports utilize TCP.

This page is intentionally left blank.

Crestron Electronics, Inc.
15 Volvo Drive   Rockleigh, NJ 07647
Tel: 888.CRESTRON
Fax: 201.767.7576
www.crestron.com

Deployment Guide – DOC. 7976A
(2048386)
05.17
Specifications subject to
change without notice.