Federated Single Sign-On for Crestron Fusion® Software

Configuration Guide

Crestron Electronics, Inc.

Original Instructions
The U.S. English version of this document is the original instructions.
All other languages are a translation of the original instructions.

The product warranty can be found at www.crestron.com/legal/sales-terms-conditions-warranties.

The specific patents that cover Crestron products are listed at www.crestron.com/legal/patents.

Certain Crestron products contain open source software. For specific information, visit www.crestron.com/legal/open-source-software.

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

Contents

Federated Single Sign-On for Crestron Fusion® Software

Introduction

This document describes the procedures required to configure federated single sign-on for Crestron Fusion® software via the Azure® Active Directory® service.

NOTE: The procedures and web page images provided in this document are subject to change at any time but are accurate as of Crestron Fusion version 11.1.8000.

Configure Azure Active Directory

Prior to configuring Crestron Fusion, Azure Active Directory must be configured to support federated single sign-on via the Azure portal.

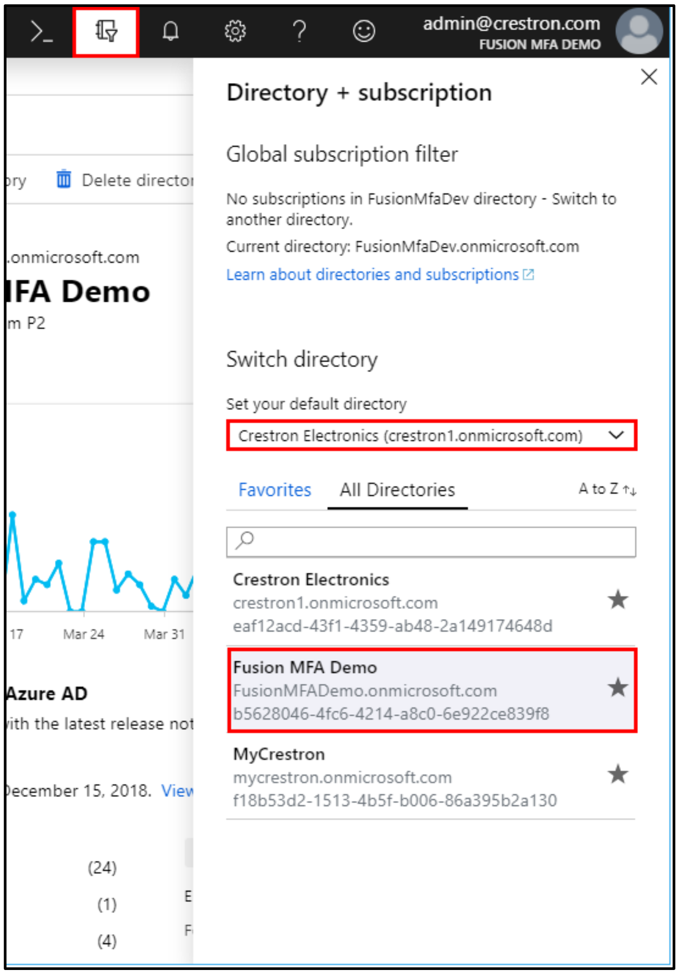
Register a New Azure Application

To register a new Crestron Fusion application in Azure Active Directory:

1. Sign into the Azure portal (https://portal.azure.com/#home).

2. Select the correct directory and subscription using the top navigation menu. Refer to the following image.

Directory + subscription Page



Directory + subscription

Global subscription filter

No subscriptions in FusionMfaDev directory - Switch to another directory.

Current directory: FusionMfaDev.onmicrosoft.com

Learn about directories and subscriptions

Switch directory

Set your default directory: Crestron Electronics (crestron1.onmicrosoft.com)

Favorites | All Directories | A to Z ↑↓

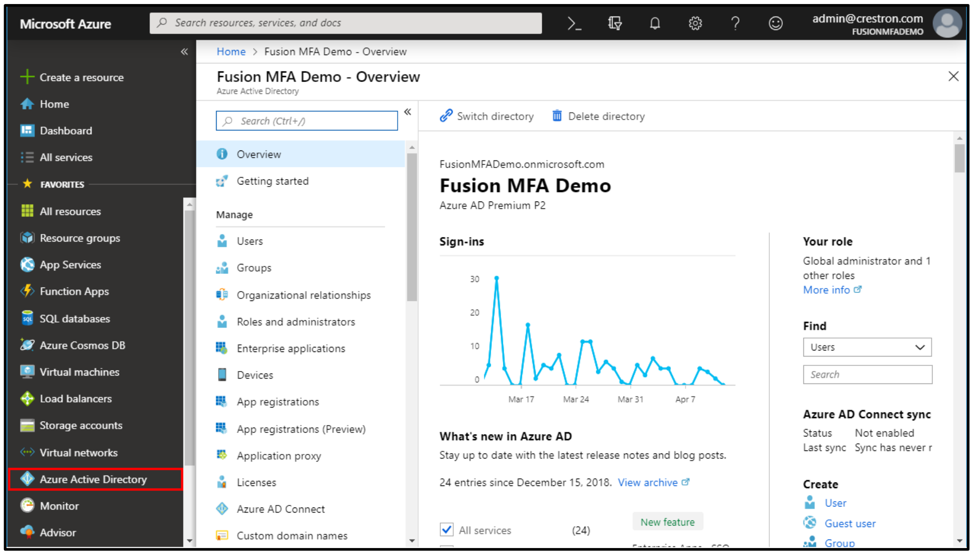
Crestron Electronics
crestron1.onmicrosoft.com
eaf12acd-43f1-4359-ab48-2a149174648d

Fusion MFA Demo
FusionMFADemo.onmicrosoft.com
b5628046-4fc6-4214-a8c0-6e922ce839f8

MyCrestron
mycrestron.onmicrosoft.com
f18b53d2-1513-4b5f-b006-86a395b2a130

3. Select **Azure Active Directory** from the left navigation menu.

Azure Active Directory Page – Overview



FusionMFADemo.onmicrosoft.com

Fusion MFA Demo

Azure AD Premium P2

Your role

Global administrator and 1 other roles

More info

What's new in Azure AD

Stay up to date with the latest release notes and blog posts.

24 entries since December 15, 2018. View archive

☑ All services (24)

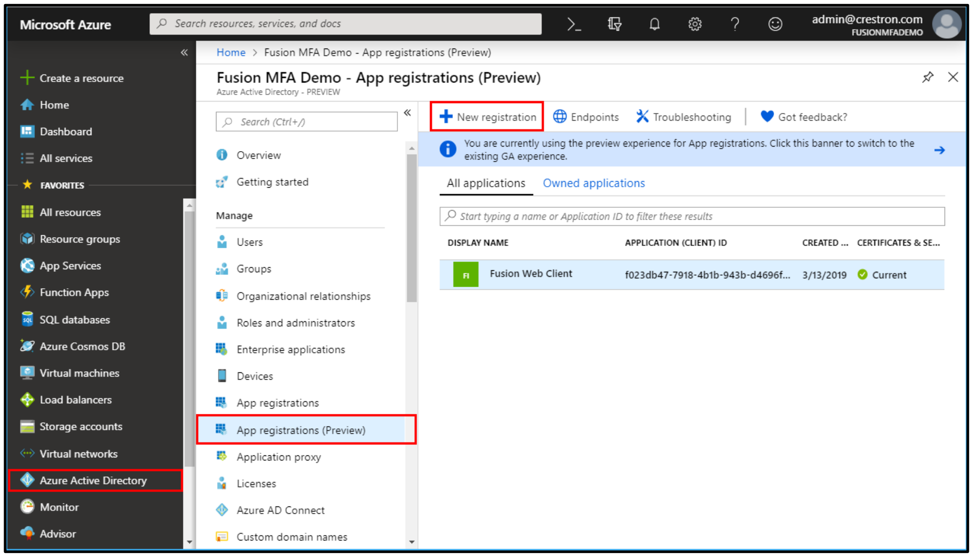
Azure AD Connect sync

Status	Not enabled
Last sync	Sync has never r

4. Select **App registrations (Preview)** from the Azure widget menu.

5. Click + **New registration**.

Azure Active Directory Page – App registrations (Preview)



You are currently using the preview experience for App registrations. Click this banner to switch to the existing GA experience.

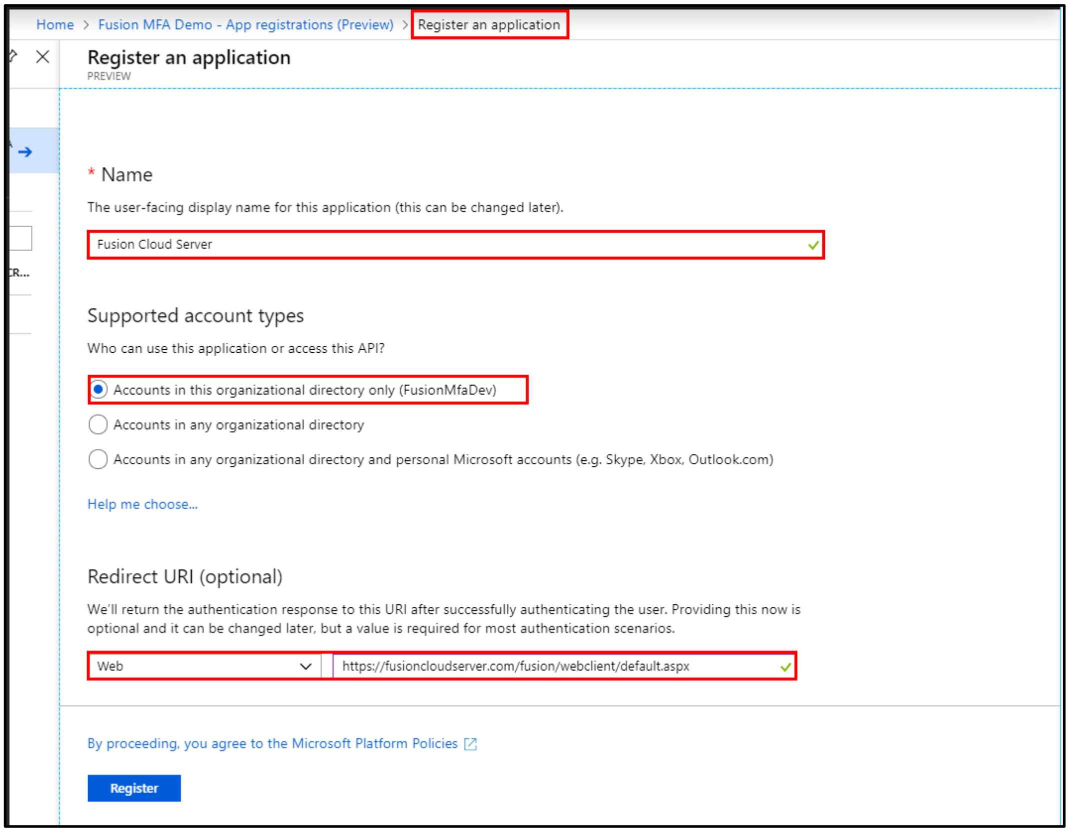
DISPLAY NAME	APPLICATION (CLIENT) ID	CREATED ...	CERTIFICATES & SE...
FI Fusion Web Client	f023db47-7918-4b1b-943b-d4696f...	3/13/2019	Current

6. Enter the following information in the **Register an application** page:

   - **Name:** Enter a name for the application.
   - **Supported account types:** Click the **Accounts in this organizational directory only** radio button.
   - **Redirect URI (optional)**: Set a redirection URI for the application:
     - Select **Web** from the drop-down menu.
     - Enter the URL for the Crestron Fusion Cloud login page in the text box (such as "https://fusioncloudserver.com/fusion/webclient/default.aspx").

     NOTE: The URL must be entered in all lowercase characters.

Register an Application Page



Home > Fusion MFA Demo - App registrations (Preview) > Register an application

Register an application
PREVIEW

* Name

The user-facing display name for this application (this can be changed later).

Fusion Cloud Server ✓

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (FusionMfaDev)

○ Accounts in any organizational directory

○ Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

Help me choose...

Redirect URI (optional)

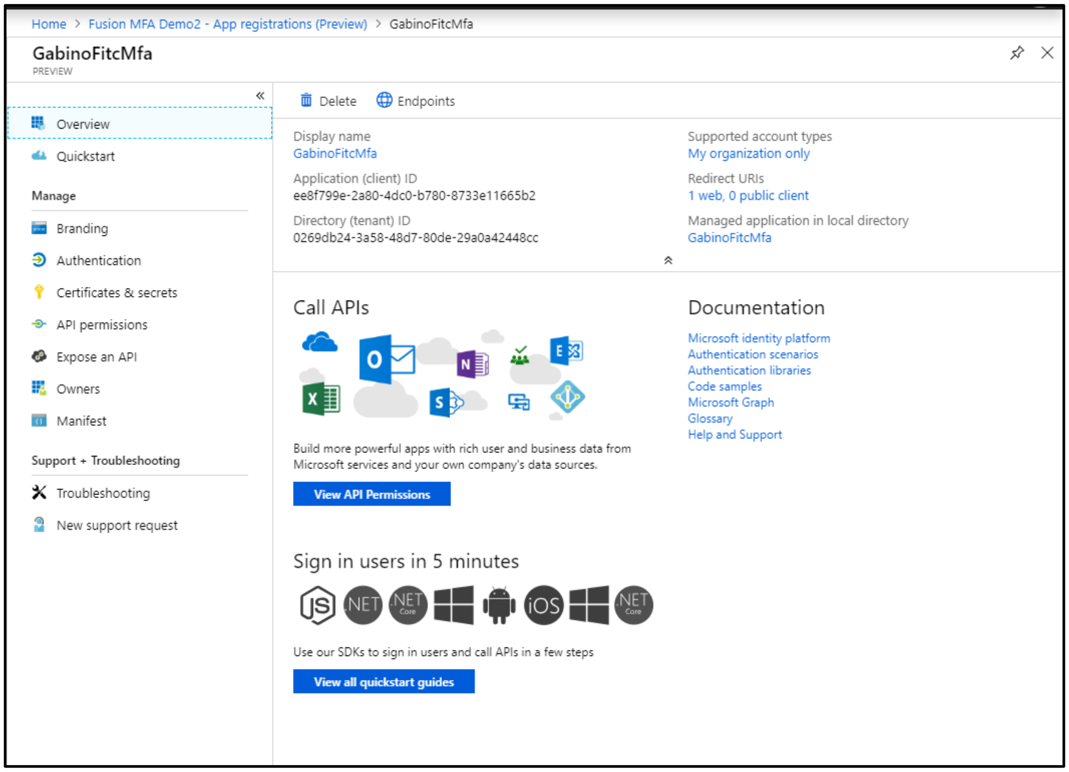
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web | https://fusioncloudserver.com/fusion/webclient/default.aspx ✓

By proceeding, you agree to the Microsoft Platform Policies

7. Click **Register**. The application is created and the following panel is displayed.

Application Page



Home > Fusion MFA Demo2 - App registrations (Preview) > GabinoFitcMfa

GabinoFitcMfa
PREVIEW

Display name
GabinoFitcMfa

Application (client) ID
ee8f799e-2a80-4dc0-b780-8733e11665b2

Directory (tenant) ID
0269db24-3a58-48d7-80de-29a0a42448cc

Supported account types
My organization only

Redirect URIs
1 web, 0 public client

Managed application in local directory
GabinoFitcMfa

Call APIs

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

Sign in users in 5 minutes

Use our SDKs to sign in users and call APIs in a few steps

Documentation

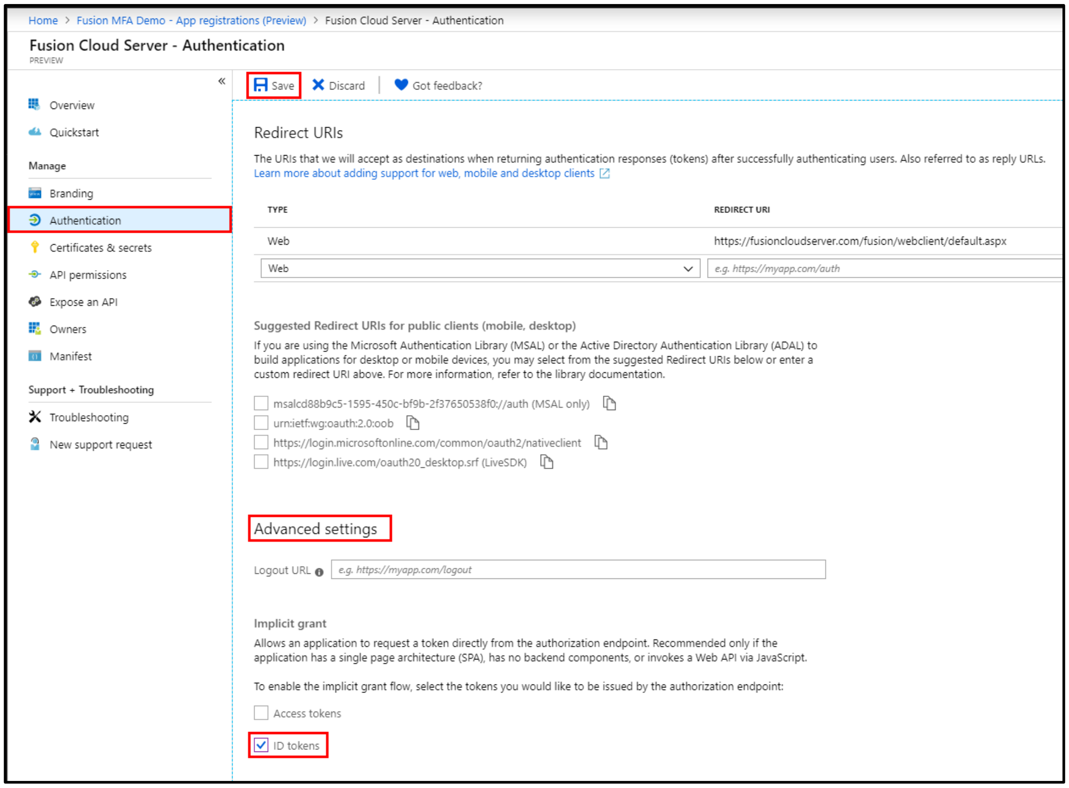
Configure Authentication

To configure authentication settings for the application:

1. On the application page, select **Authentication** from the left navigation menu.
2. Under **Advanced settings**, click the check box next to **ID tokens** to enable this feature. A filled check box indicates that the feature is enabled.

3. Click **Save** at the top of the page.

Application Page – Authentication



Home > Fusion MFA Demo - App registrations (Preview) > Fusion Cloud Server - Authentication

Fusion Cloud Server - Authentication

PREVIEW

Redirect URIs

The URIs that we will accept as destinations when returning authentication responses (tokens) after successfully authenticating users. Also referred to as reply URLs.
Learn more about adding support for web, mobile and desktop clients

TYPE	REDIRECT URI
Web	https://fusioncloudserver.com/fusion/webclient/default.aspx
Web	e.g. https://myapp.com/auth

Suggested Redirect URIs for public clients (mobile, desktop)

If you are using the Microsoft Authentication Library (MSAL) or the Active Directory Authentication Library (ADAL) to build applications for desktop or mobile devices, you may select from the suggested Redirect URIs below or enter a custom redirect URI above. For more information, refer to the library documentation.

- □ msalcd88b9c5-1595-450c-bf9b-2f37650538f0://auth (MSAL only)
- □ urn:ietf:wg:oauth:2.0:oob
- □ https://login.microsoftonline.com/common/oauth2/nativeclient
- □ https://login.live.com/oauth20_desktop.srf (LiveSDK)

Advanced settings

Logout URL: e.g. https://myapp.com/logout

Implicit grant

Allows an application to request a token directly from the authorization endpoint. Recommended only if the application has a single page architecture (SPA), has no backend components, or invokes a Web API via JavaScript.

To enable the implicit grant flow, select the tokens you would like to be issued by the authorization endpoint:

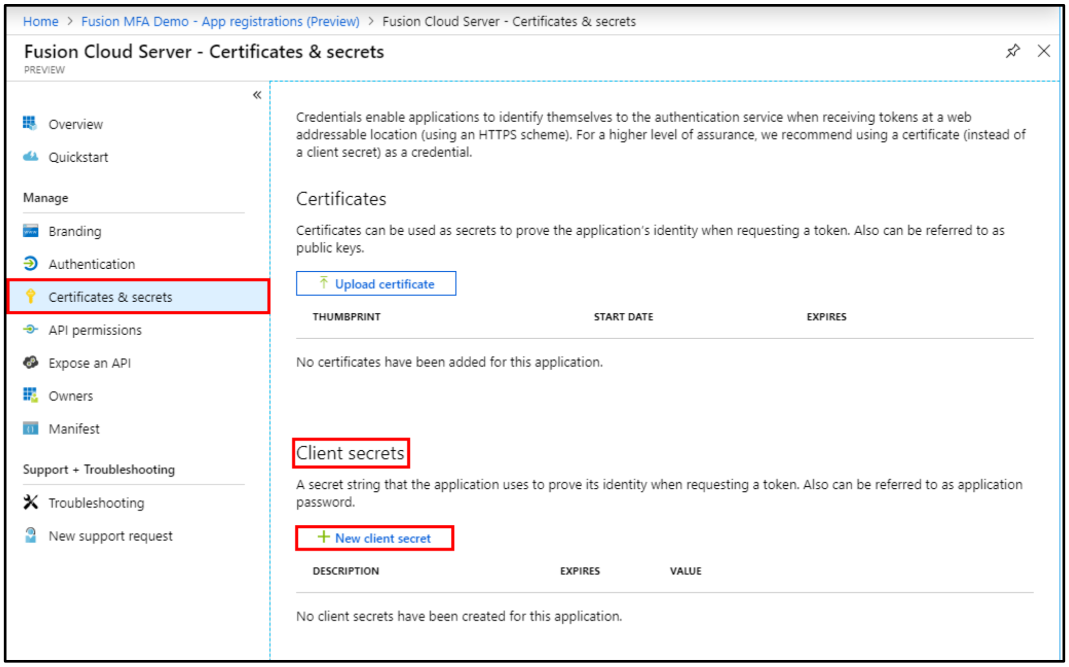
- □ Access tokens
- ☑ ID tokens

Configure Certificates and Secrets

To configure certificates and secrets settings for the application:

1. On the application page, select **Certificates & secrets** from the left navigation menu.
2. Under **Client secrets**, click **+ New client secret**.

Application Page – Certificates & secrets



Credentials enable applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

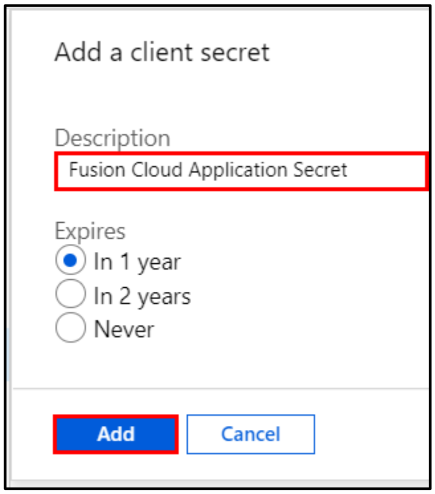
No certificates have been added for this application.

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

No client secrets have been created for this application.

An **Add a client secret** dialog box is displayed.

Add a client secret Dialog Box



Description: Fusion Cloud Application Secret

Expires

● In 1 year
○ In 2 years
○ Never

3. Enter a description for the client secret in the **Description** text field.

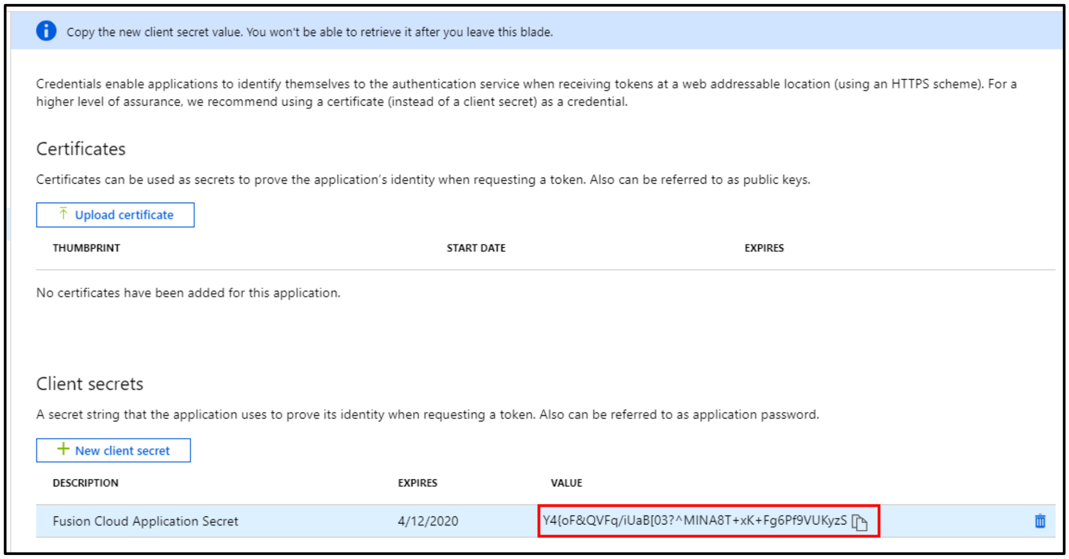
4. Select **In 1 year**, **In 2 years**, or **Never** from the **Expires** selections.

5. Click **Add**. A new client secret value for the application is displayed on the **Certificates & secrets** page.

6. Copy the client secret value and save it to a secure location. This value will be entered later in the Crestron Fusion Configuration Manager.

NOTE: The client secret value cannot be retrieved after leaving the **Certificates & Secrets** page. Ensure the value is copied to a secure location prior to leaving the page.

Application Page – Certificates & secrets (Client Secret Value)



Copy the new client secret value. You won't be able to retrieve it after you leave this blade.

Credentials enable applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

THUMBPRINT	START DATE	EXPIRES

No certificates have been added for this application.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

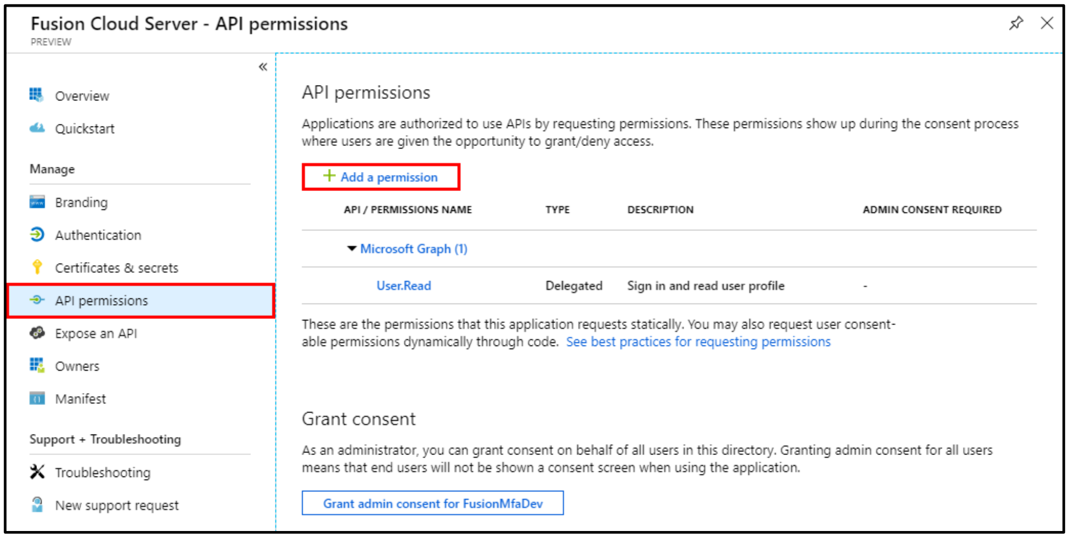
DESCRIPTION	EXPIRES	VALUE
Fusion Cloud Application Secret	4/12/2020	Y4{oF&QVFq/iUaB[03?^MINA8T+xK+Fg6Pf9VUKyzS

Add Microsoft® Graph Software Permissions

To configure Microsoft® Graph software permissions for the application:

1. On the application page, select **API permissions** from the left navigation menu.
2. Under **API permissions**, click **+ Add a permission**.

Application Page – API permissions



Fusion Cloud Server - API permissions
PREVIEW

API permissions

Applications are authorized to use APIs by requesting permissions. These permissions show up during the consent process where users are given the opportunity to grant/deny access.

+ Add a permission

API / PERMISSIONS NAME	TYPE	DESCRIPTION	ADMIN CONSENT REQUIRED
▾ Microsoft Graph (1)			
User.Read	Delegated	Sign in and read user profile	-

These are the permissions that this application requests statically. You may also request user consent-able permissions dynamically through code. See best practices for requesting permissions

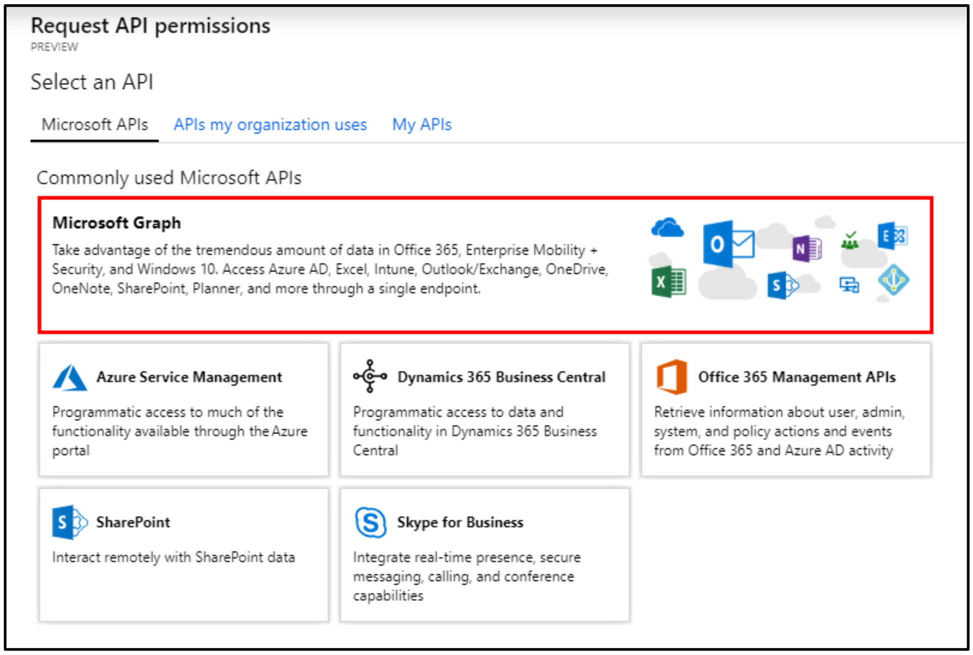
Grant consent

As an administrator, you can grant consent on behalf of all users in this directory. Granting admin consent for all users means that end users will not be shown a consent screen when using the application.

Grant admin consent for FusionMfaDev

3. On the **Request API permissions** page, select the **Microsoft APIs** tab, and then click the **Microsoft Graph** tile.

Request API permissions Page



Request API permissions
PREVIEW

Select an API

Commonly used Microsoft APIs

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Service Management
Programmatic access to much of the functionality available through the Azure portal

Dynamics 365 Business Central
Programmatic access to data and functionality in Dynamics 365 Business Central

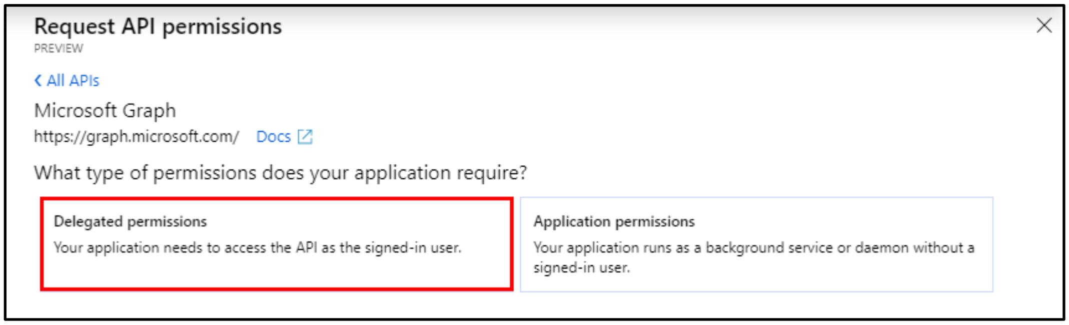
Office 365 Management APIs
Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity

SharePoint
Interact remotely with SharePoint data

Skype for Business
Integrate real-time presence, secure messaging, calling, and conference capabilities

4. Click the **Delegated permissions** tile.

Request API permissions Page – Microsoft Graph



Request API permissions

PREVIEW

‹ All APIs

Microsoft Graph

https://graph.microsoft.com/ Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

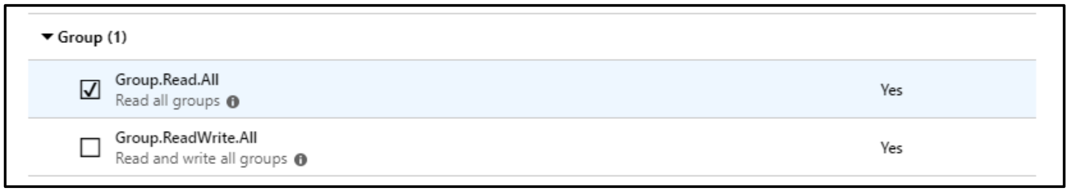
Application permissions
Your application runs as a background service or daemon without a signed-in user.

5. Click the check boxes next to the following permissions to select them:

- offline_access
- openid
- profile

6. Scroll down to and expand the **Group** accordion, and then click the check box next to **Group.Read.All**.

Request API permissions Page – Group

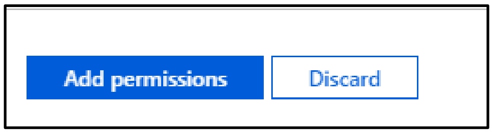


▾ Group (1)

☑	Group.Read.All Read all groups	Yes
□	Group.ReadWrite.All Read and write all groups	Yes

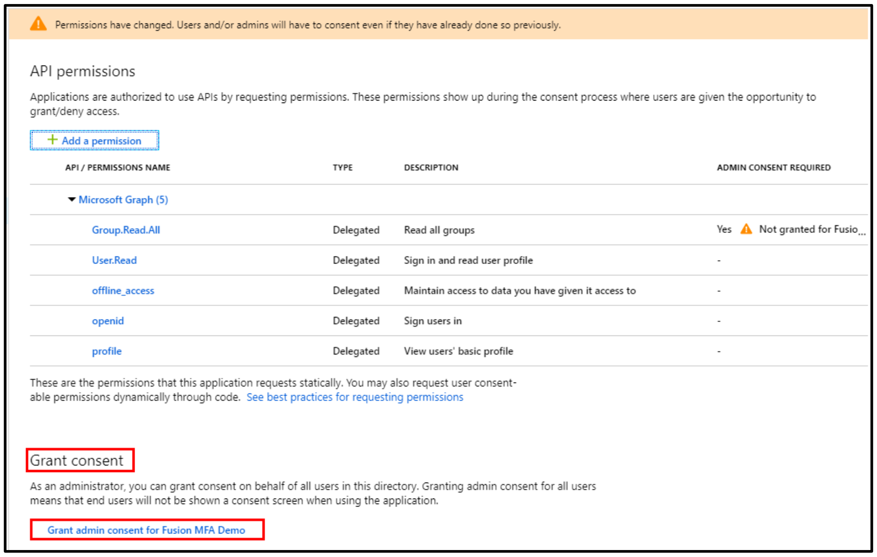
7. Click **Add permissions**.

Request API permissions – Add permissions Button



8. Under **Grant consent**, click **Grant admin consent for [Directory Name]**.

API permissions Page – Grant Admin Consent



Permissions have changed. Users and/or admins will have to consent even if they have already done so previously.

API permissions

Applications are authorized to use APIs by requesting permissions. These permissions show up during the consent process where users are given the opportunity to grant/deny access.

API / PERMISSIONS NAME	TYPE	DESCRIPTION	ADMIN CONSENT REQUIRED
▾ Microsoft Graph (5)			
Group.Read.All	Delegated	Read all groups	Yes ⚠ Not granted for Fusio...
User.Read	Delegated	Sign in and read user profile	-
offline_access	Delegated	Maintain access to data you have given it access to	-
openid	Delegated	Sign users in	-
profile	Delegated	View users' basic profile	-

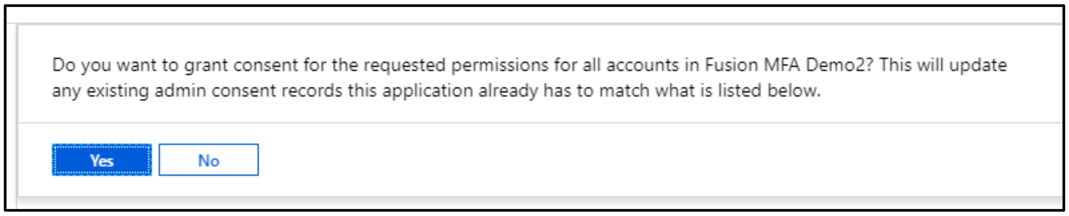
These are the permissions that this application requests statically. You may also request user consent-able permissions dynamically through code. See best practices for requesting permissions

Grant consent

As an administrator, you can grant consent on behalf of all users in this directory. Granting admin consent for all users means that end users will not be shown a consent screen when using the application.

9. A message window confirming the changes is displayed. Click **Yes** to confirm.

Grant Permissions Message Window



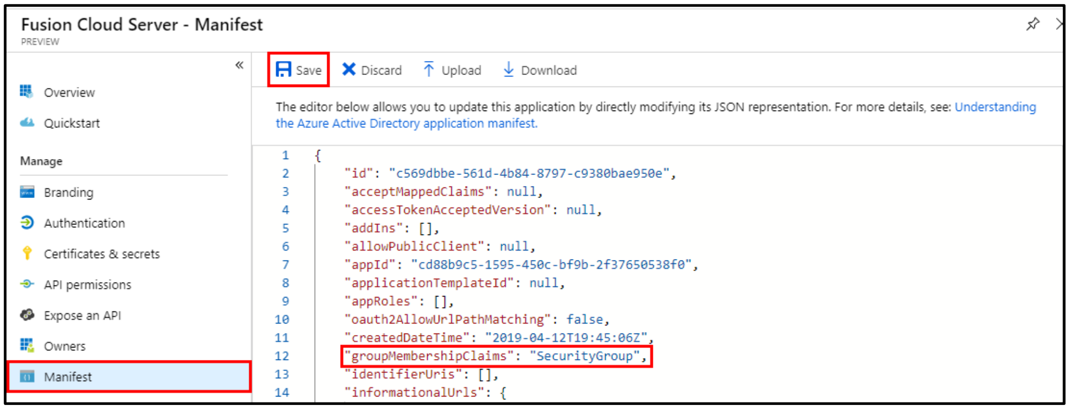
Do you want to grant consent for the requested permissions for all accounts in Fusion MFA Demo2? This will update any existing admin consent records this application already has to match what is listed below.

Update the Manifest

To update the manifest file for the application:

1. On the application page, select **Manifest** from the left navigation menu.
2. In the manifest JSON object, change the value of "`groupMembershipClaims`" from `null` to "`SecurityGroup`".
3. Click **Save**.

Application Page – Edit Manifest



The editor below allows you to update this application by directly modifying its JSON representation. For more details, see: Understanding the Azure Active Directory application manifest.

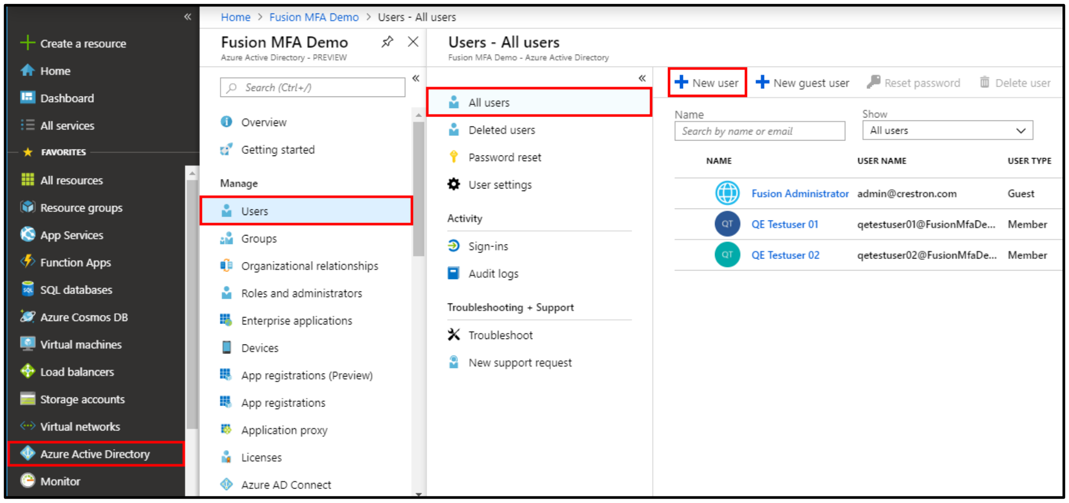
```
{
    "id": "c569dbbe-561d-4b84-8797-c9380bae950e",
    "acceptMappedClaims": null,
    "accessTokenAcceptedVersion": null,
    "addIns": [],
    "allowPublicClient": null,
    "appId": "cd88b9c5-1595-450c-bf9b-2f37650538f0",
    "applicationTemplateId": null,
    "appRoles": [],
    "oauth2AllowUrlPathMatching": false,
    "createdDateTime": "2019-04-12T19:45:06Z",
    "groupMembershipClaims": "SecurityGroup",
    "identifierUris": [],
    "informationalUrls": {
```

Create an Administrator User

To create a new administrator user in Azure Active Directory:

1. Select **Azure Active Directory** from the left navigation menu in the Azure portal.
2. Navigate to **Users** > **All users**.
3. Click **+ New user**.

Users Page – All users

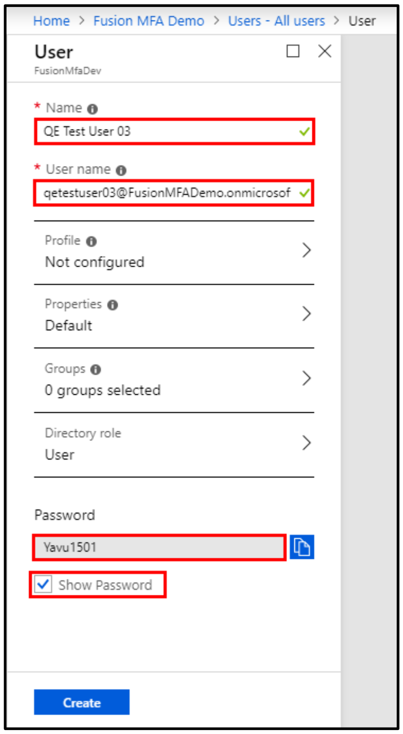


NAME	USER NAME	USER TYPE
Fusion Administrator	admin@crestron.com	Guest
QE Testuser 01	qetestuser01@FusionMfaDe...	Member
QE Testuser 02	qetestuser02@FusionMfaDe...	Member

4. Enter the following information for the new user in the page that is displayed:

   - **Name**: Enter the first and last name of the user.
   - **User name**: Enter the user's email from the directory domain. In the example image below, the directory used is "FusionMfaDemo2.onmicrosoft.com", so a valid username would be "username@FusionMfaDemo2.onmicrosoft.com".
   - **Password**: A temporary password is provided in this field after a name and username are entered.
   - Click the **Show Password** check box under the **Password** field, and then copy the password to a secure location.

New User Page



Home > Fusion MFA Demo > Users - All users > User

User

FusionMfaDev

* Name

QE Test User 03

* User name

qetestuser03@FusionMFADemo.onmicrosof

Profile

Not configured

Properties

Default

Groups

0 groups selected

Directory role

User

Password

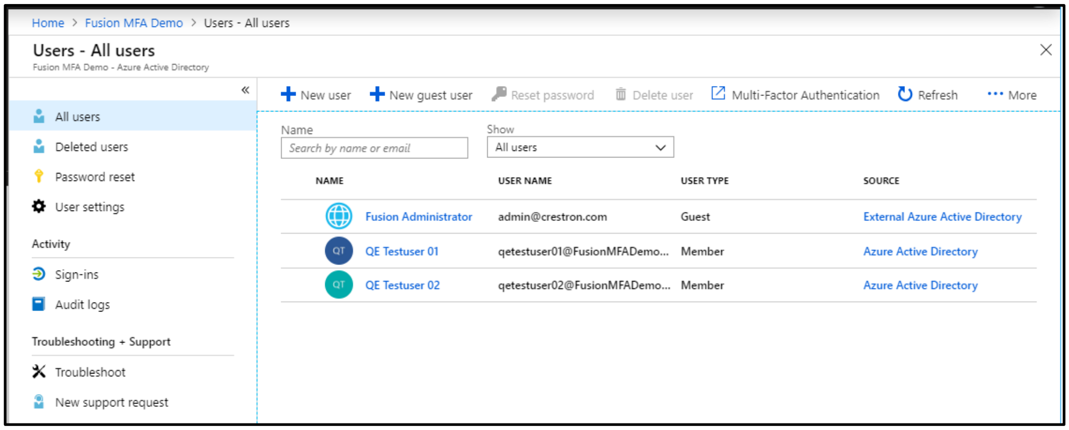
Yavu1501

☑ Show Password

Create

5. Click **Create**. The new user is added to the **All users** window.

Users Page – All users



NAME	USER NAME	USER TYPE	SOURCE
Fusion Administrator	admin@crestron.com	Guest	External Azure Active Directory
QT QE Testuser 01	qetestuser01@FusionMFADemo...	Member	Azure Active Directory
QT QE Testuser 02	qetestuser02@FusionMFADemo...	Member	Azure Active Directory

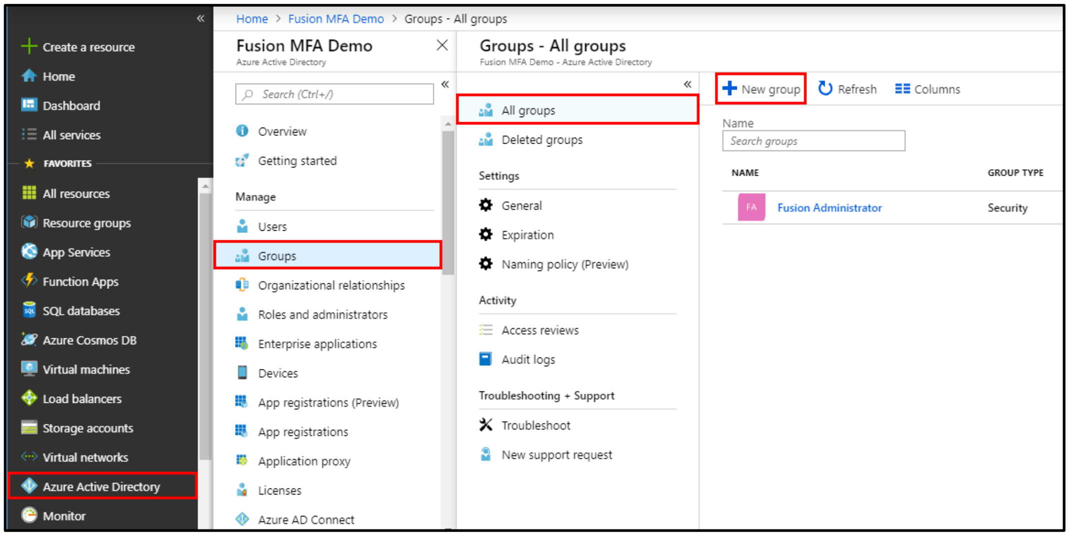
Repeat this procedure for each additional user that will have administrator privileges in Crestron Fusion.

Create an Administrator Group

To create a new administrator group in Azure Active Directory:

1. Select **Azure Active Directory** from the left navigation menu in the Azure portal.
2. Navigate to **Groups** > **All groups**.
3. Click **+ New group**.

Groups Page– All groups

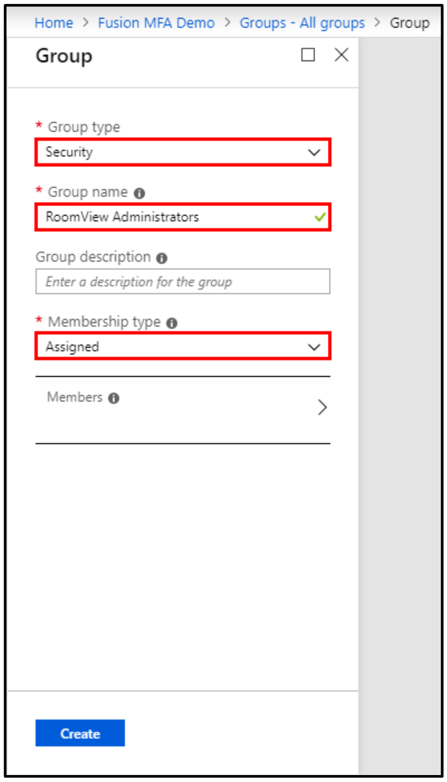


NAME	GROUP TYPE
FA Fusion Administrator	Security

4. Enter the following information for the new user in the page that is displayed:

    - **Group type**: Select **Security** from the drop-down menu.
    - **Group name**: Enter a group name in the text field.
    - **Membership type**: Select **Assigned** from the drop-down menu.

New Group Page



Home > Fusion MFA Demo > Groups - All groups > Group

Group

* Group type: Security

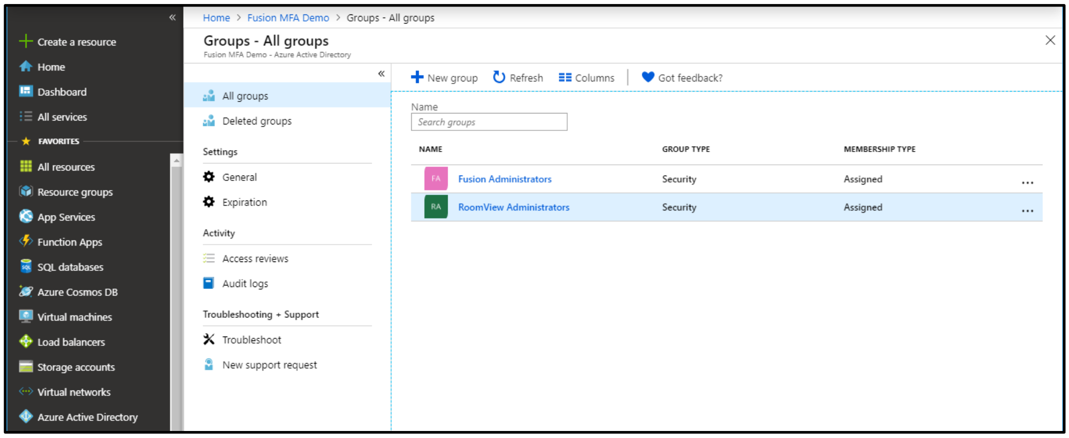
* Group name: RoomView Administrators

Group description: *Enter a description for the group*

* Membership type: Assigned

5. Click **Create**. The new group is added to the **All groups** window.

Groups Page – All groups



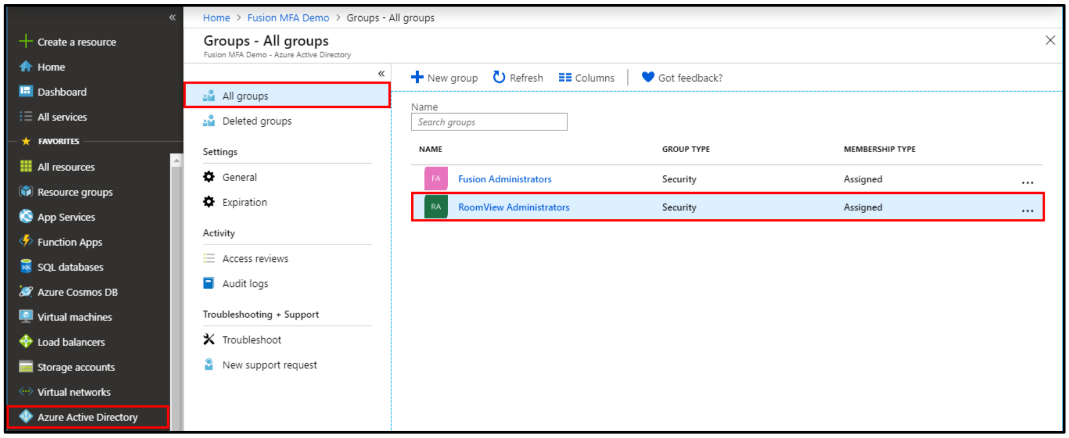
NAME	GROUP TYPE	MEMBERSHIP TYPE
FA Fusion Administrators	Security	Assigned
RA RoomView Administrators	Security	Assigned

Add Users to the Administrator Group

Use the following procedure to add Azure Active Directory users to a group that will be designated as the Crestron Fusion Administrators group in the Crestron Fusion Configuration Manager. Users in this group will have full administrative rights in Crestron Fusion.

1. Select **Azure Active Directory** from the left navigation menu in the Azure portal.
2. Navigate to **Groups** > **All groups**.
3. Click on the group that will be designated as the Crestron Fusion Administrator group.

Groups Page – All groups

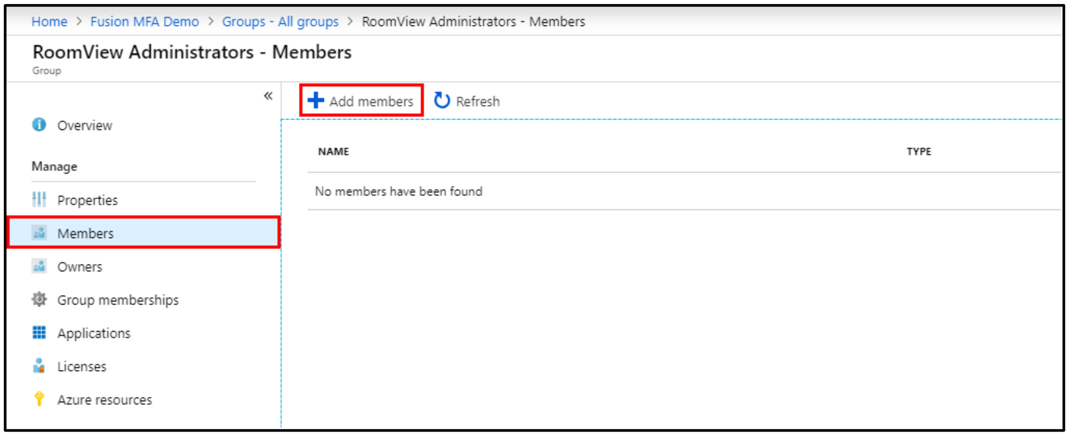


NAME	GROUP TYPE	MEMBERSHIP TYPE
FA Fusion Administrators	Security	Assigned
RA RoomView Administrators	Security	Assigned

4. Select **Members** from the left navigation menu.

5. Click **+ Add members**.

Members Page – Add members

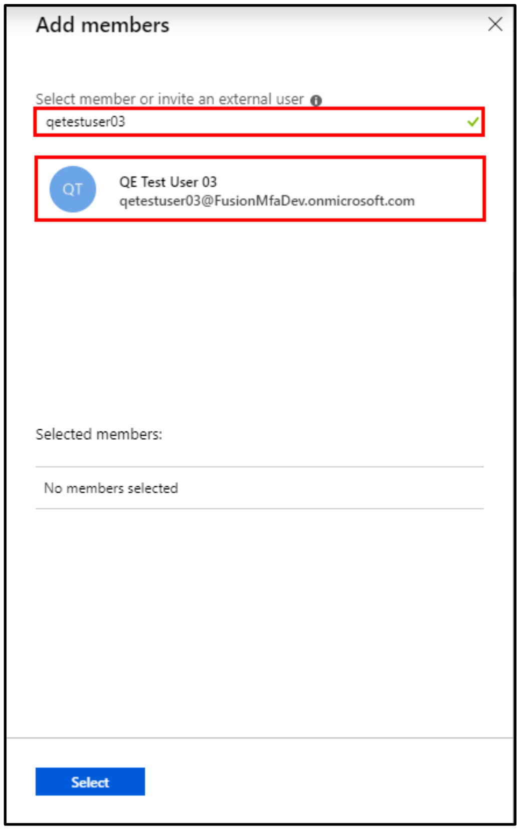


No members have been found

6. Select the user in the **Add members** page:

- Type the desired username in the text field.
- Select the corresponding user from the results list.

Add members Page



Select member or invite an external user

qetestuser03

QE Test User 03
qetestuser03@FusionMfaDev.onmicrosoft.com

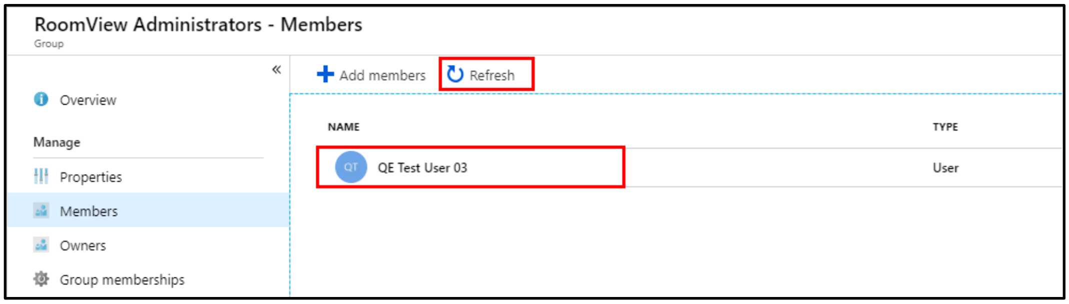
Selected members:

No members selected

7. Click **Select**.

8. Click **Refresh** in the **Members** page. The new user will be added to the list underneath.

Members Page – User Added



RoomView Administrators - Members

Group

NAME	TYPE
QT QE Test User 03	User

Configure Crestron Fusion

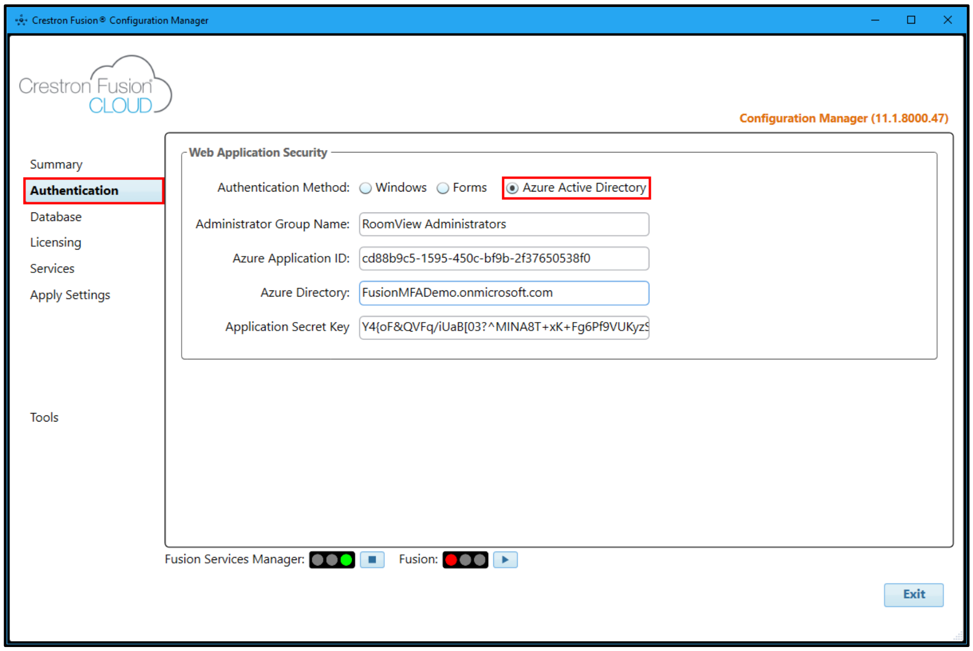
Once Azure Active Directory has been configured for single sign-on, Crestron Fusion can be configured to support this authentication method.

Configuration is accomplished by entering the administrator group name and other values from Azure Active Directory into the Crestron Fusion Configuration Manager. Once Crestron Fusion is running, additional Azure Active Directory groups can be specified in the Crestron Fusion setup web client to allow for different levels of user access and authorization. These optional groups are added to the Functional and Object security policies (refer to the Crestron Fusion help files and online documentation for more information).

To configure Crestron Fusion for single sign-on:

1. Log in to the Microsoft Windows® operating system server hosting the Crestron Fusion application.
2. Open the Crestron Fusion Configuration Manager.
3. Select **Authentication** from the left navigation menu.
4. Click the **Azure Active Directory** radio button.

Crestron Fusion Configuration Manager – Authentication



Web Application Security

Authentication Method: ○ Windows ○ Forms ● Azure Active Directory

Administrator Group Name: RoomView Administrators

Azure Application ID: cd88b9c5-1595-450c-bf9b-2f37650538f0

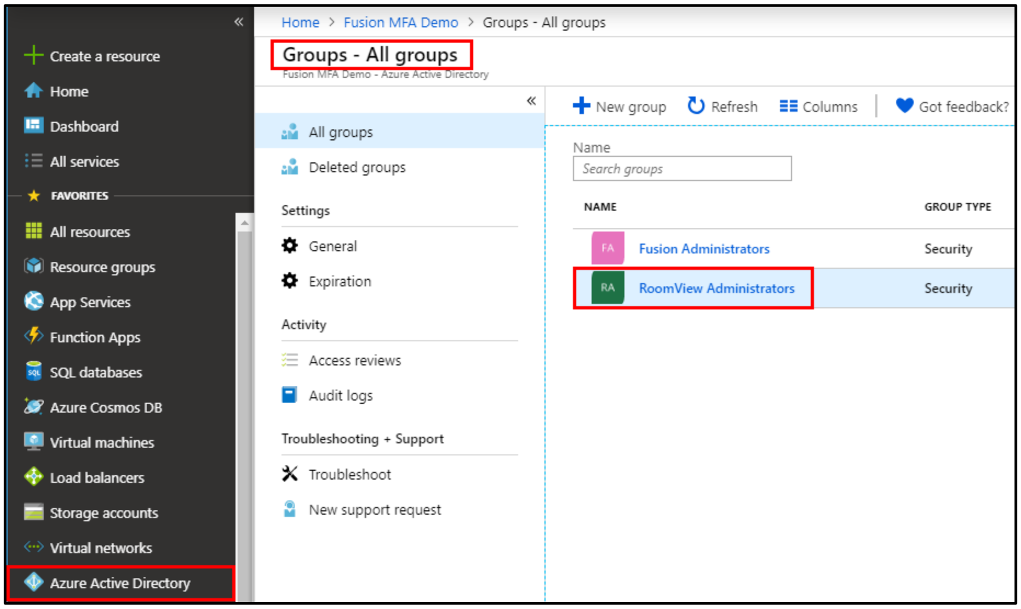
Azure Directory: FusionMFADemo.onmicrosoft.com

Application Secret Key Y4{oF&QVFq/iUaB[03?^MINA8T+xK+Fg6Pf9VUKyz

5. Enter the administrator group name created in Azure Active Directory in the **Administrator Group Name** text field. This group should include all members that will have full administrator access to the Crestron Fusion application. For more information, refer to “Create an Administrator Group” on page 14.

   To locate the administrator group name, navigate to **Azure Active Directory** > **Groups** > **All groups** in the Azure portal, and then copy the appropriate group name.

Groups Page – All groups

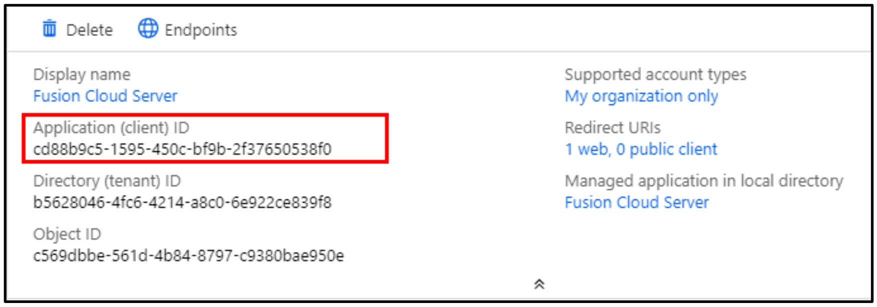


NAME	GROUP TYPE
FA Fusion Administrators	Security
RA RoomView Administrators	Security

6. Enter the Azure application ID for the Crestron Fusion application in the **Azure Application ID** text field.

   To locate the Azure application ID, navigate to **Azure Active Directory** > **Select Application** > **App registrations (Preview)** in the Azure portal, and then copy the value shown under **Application (client) ID**.

Azure Application ID



Display name
Fusion Cloud Server

Application (client) ID
cd88b9c5-1595-450c-bf9b-2f37650538f0

Directory (tenant) ID
b5628046-4fc6-4214-a8c0-6e922ce839f8

Object ID
c569dbbe-561d-4b84-8797-c9380bae950e

Supported account types
My organization only

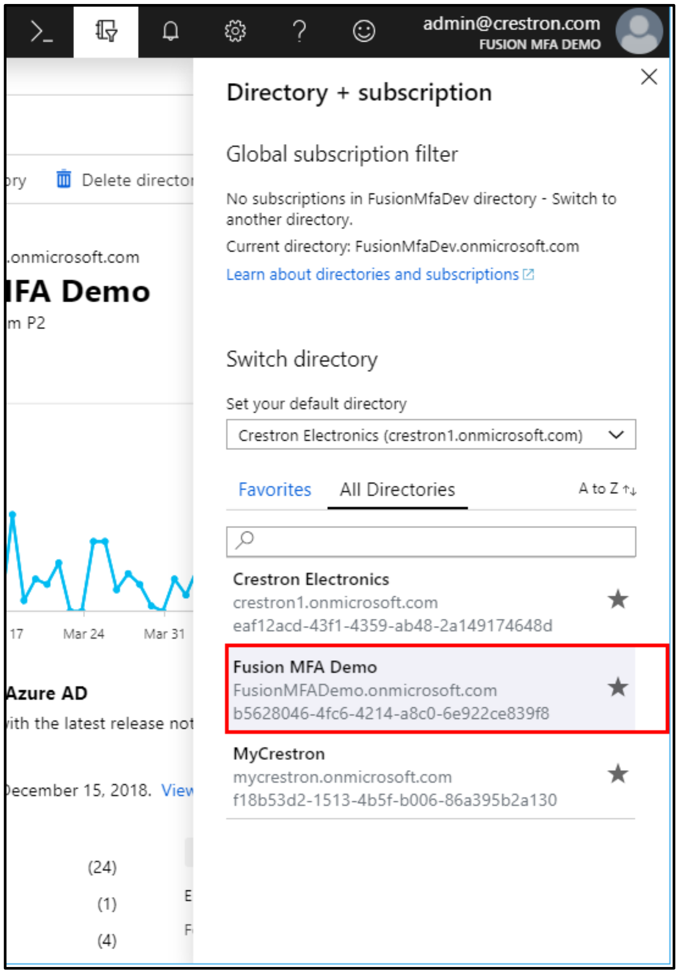
Redirect URIs
1 web, 0 public client

Managed application in local directory
Fusion Cloud Server

7. Enter the Azure directory name in the **Azure Directory** text field.

   To locate the Azure directory name, navigate to **Directory + subscription** in the Azure portal, and then copy the appropriate directory name.

   Directory + subscription Page

   Directory + subscription

   Global subscription filter

   No subscriptions in FusionMfaDev directory - Switch to another directory.

   Current directory: FusionMfaDev.onmicrosoft.com

   Learn about directories and subscriptions

   Switch directory

   Set your default directory

   Crestron Electronics (crestron1.onmicrosoft.com)

   Favorites | All Directories | A to Z ↑↓

   Crestron Electronics
   crestron1.onmicrosoft.com
   eaf12acd-43f1-4359-ab48-2a149174648d ★

   Fusion MFA Demo
   FusionMFADemo.onmicrosoft.com
   b5628046-4fc6-4214-a8c0-6e922ce839f8 ★

   MyCrestron
   mycrestron.onmicrosoft.com
   f18b53d2-1513-4b5f-b006-86a395b2a130 ★

8. Enter the secret key created for the Crestron Fusion application in the **Application Secret Key** text field. For more information on the secret key, refer to "Configure Certificates and Secrets" on page 7.

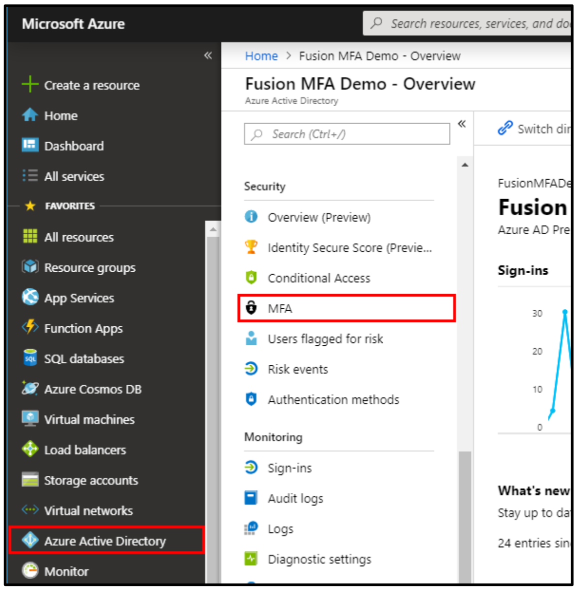
Enable Multifactor Authentication

Multifactor authentication can also be enabled for Azure Active Directory users on an individual basis. This authentication method is optional.

To enable multifactor authentication:

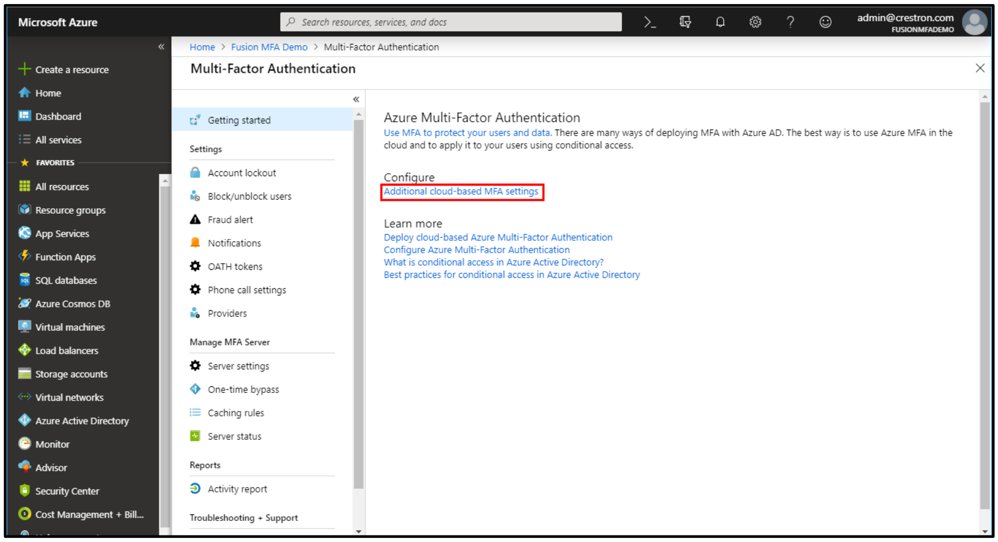
1. Log in to the Azure Active Directory portal.
2. Navigate to **Azure Active Directory** > **MFA**.

Azure Active Directory Page – MFA



3. Under **Configure**, click **Additional cloud-based MFA settings**.

Multi-factor Authentication Page



Azure Multi-Factor Authentication

Use MFA to protect your users and data. There are many ways of deploying MFA with Azure AD. The best way is to use Azure MFA in the cloud and to apply it to your users using conditional access.

Configure

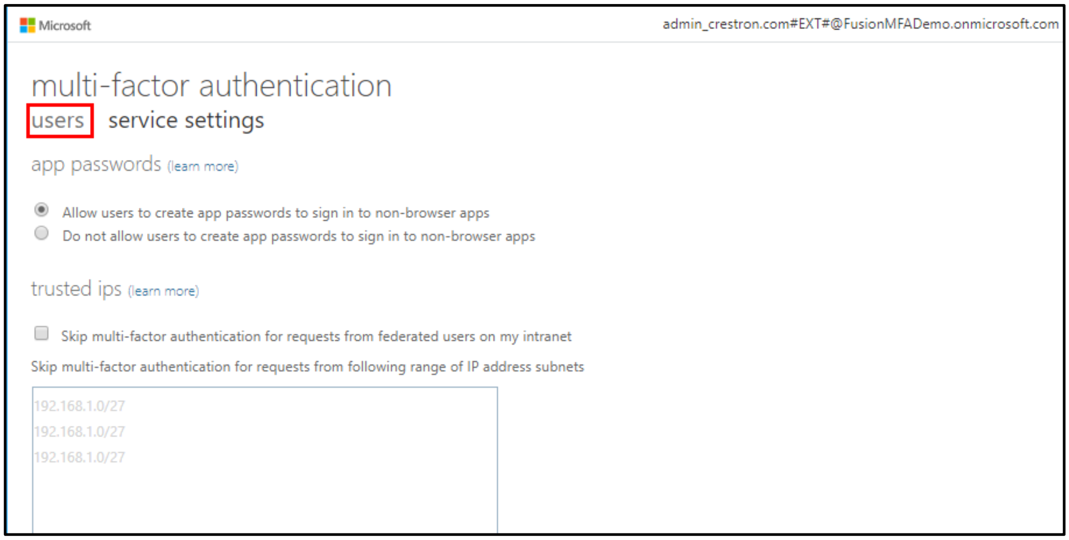
Additional cloud-based MFA settings

Learn more

Deploy cloud-based Azure Multi-Factor Authentication
Configure Azure Multi-Factor Authentication
What is conditional access in Azure Active Directory?
Best practices for conditional access in Azure Active Directory

4. Click **users** in the **multi-factor authentication** dialog box that is displayed.

multi-factor authentication Dialog Box



Microsoft admin_crestron.com#EXT#@FusionMFADemo.onmicrosoft.com

multi-factor authentication

users service settings

app passwords (learn more)

● Allow users to create app passwords to sign in to non-browser apps

○ Do not allow users to create app passwords to sign in to non-browser apps

trusted ips (learn more)

□ Skip multi-factor authentication for requests from federated users on my intranet

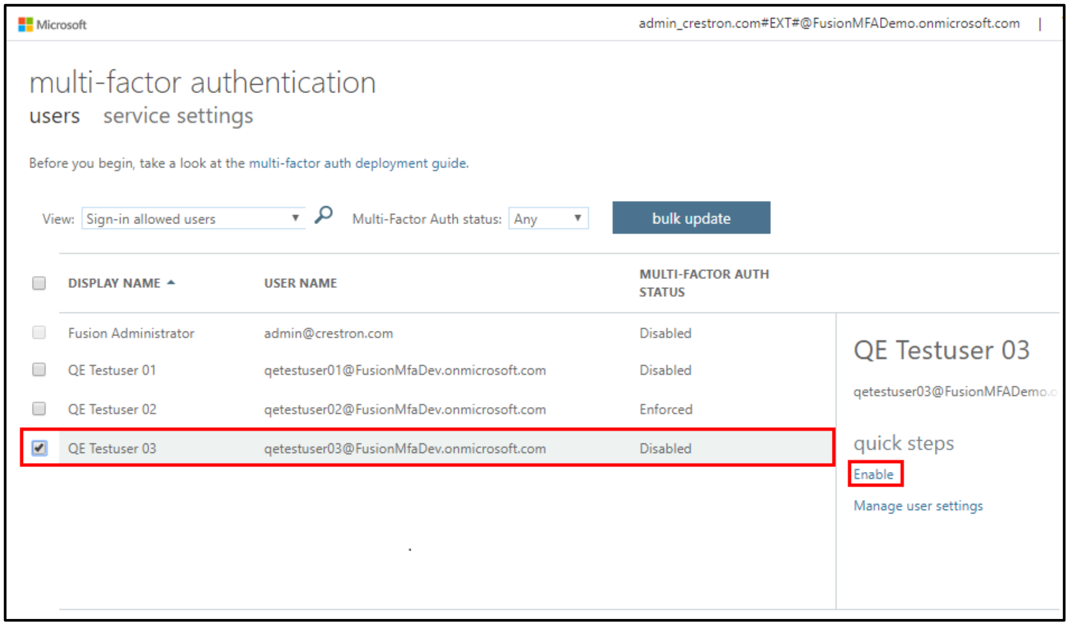
Skip multi-factor authentication for requests from following range of IP address subnets

```
192.168.1.0/27
192.168.1.0/27
192.168.1.0/27
```

5. Click the check box next to the user(s) that require multifactor authentication.

6. Click **Enable**.

multi-factor authentication – users Dialog Box



Microsoft admin_crestron.com#EXT#@FusionMFADemo.onmicrosoft.com |

multi-factor authentication

users service settings

Before you begin, take a look at the multi-factor auth deployment guide.

View: Sign-in allowed users ▾ Multi-Factor Auth status: Any ▾ bulk update

□	DISPLAY NAME ▴	USER NAME	MULTI-FACTOR AUTH STATUS
□	Fusion Administrator	admin@crestron.com	Disabled
□	QE Testuser 01	qetestuser01@FusionMfaDev.onmicrosoft.com	Disabled
□	QE Testuser 02	qetestuser02@FusionMfaDev.onmicrosoft.com	Enforced
☑	QE Testuser 03	qetestuser03@FusionMfaDev.onmicrosoft.com	Disabled

QE Testuser 03

qetestuser03@FusionMFADemo.

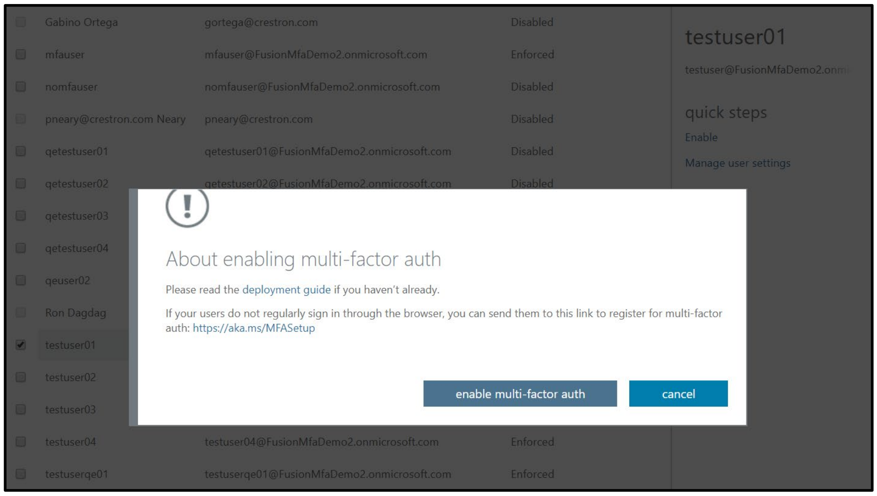
quick steps

Enable

Manage user settings

7. Click **enable multi-factor auth** in the message window that is displayed.

Enable Multifactor Authentication Message Window



□	Gabino Ortega	gortega@crestron.com	Disabled
□	mfauser	mfauser@FusionMfaDemo2.onmicrosoft.com	Enforced
□	nomfauser	nomfauser@FusionMfaDemo2.onmicrosoft.com	Disabled
□	pneary@crestron.com Neary	pneary@crestron.com	Disabled
□	qetestuser01	qetestuser01@FusionMfaDemo2.onmicrosoft.com	Disabled
□	qetestuser02	qetestuser02@FusionMfaDemo2.onmicrosoft.com	Disabled
□	qetestuser03		
□	qetestuser04		
□	qeuser02		
□	Ron Dagdag		
☑	testuser01		
□	testuser02		
□	testuser03		
□	testuser04	testuser04@FusionMfaDemo2.onmicrosoft.com	Enforced
□	testuserqe01	testuserqe01@FusionMfaDemo2.onmicrosoft.com	Enforced

testuser01

testuser@FusionMfaDemo2.onm

quick steps

Enable

Manage user settings

About enabling multi-factor auth

Please read the deployment guide if you haven't already.

If your users do not regularly sign in through the browser, you can send them to this link to register for multi-factor auth: https://aka.ms/MFASetup

8. A success message is displayed. Click **Close** to exit the message window.

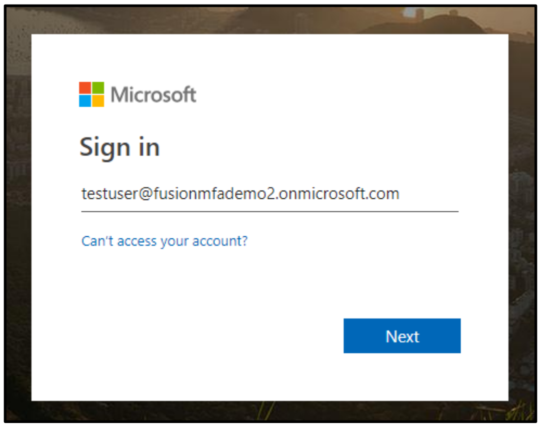
Sign in with Multifactor Authentication

Once multifactor authentication is enabled for an Azure Active Directory user, the user must use the following procedure to log on to the Crestron Fusion server.

1. Navigate to the organization's Crestron Fusion server address (for example, "https://yourserver.crestronfusion.com/Fusion/WebClient/default.aspx"). The user is redirected to a Microsoft login page.

2. Enter a username in the **Sign in** text field.

Microsoft Login Page – Sign in



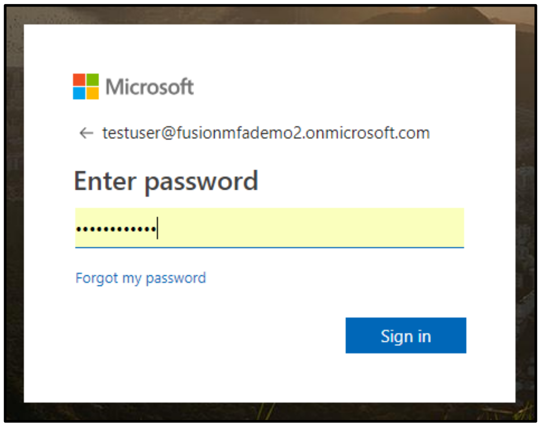
Microsoft

Sign in

testuser@fusionmfademo2.onmicrosoft.com

3. Enter the user's password in the **Enter password** text field.

Microsoft Login Page – Sign in



Microsoft

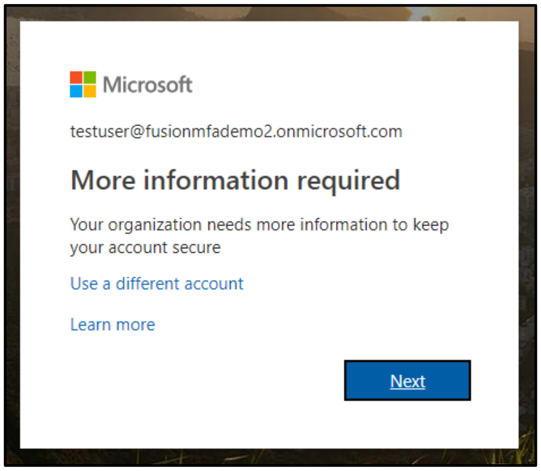
← testuser@fusionmfademo2.onmicrosoft.com

Enter password

•••••••••••

4. Click **Sign in**. A message window stating that more information is required is displayed.

More information required Message Window



Microsoft

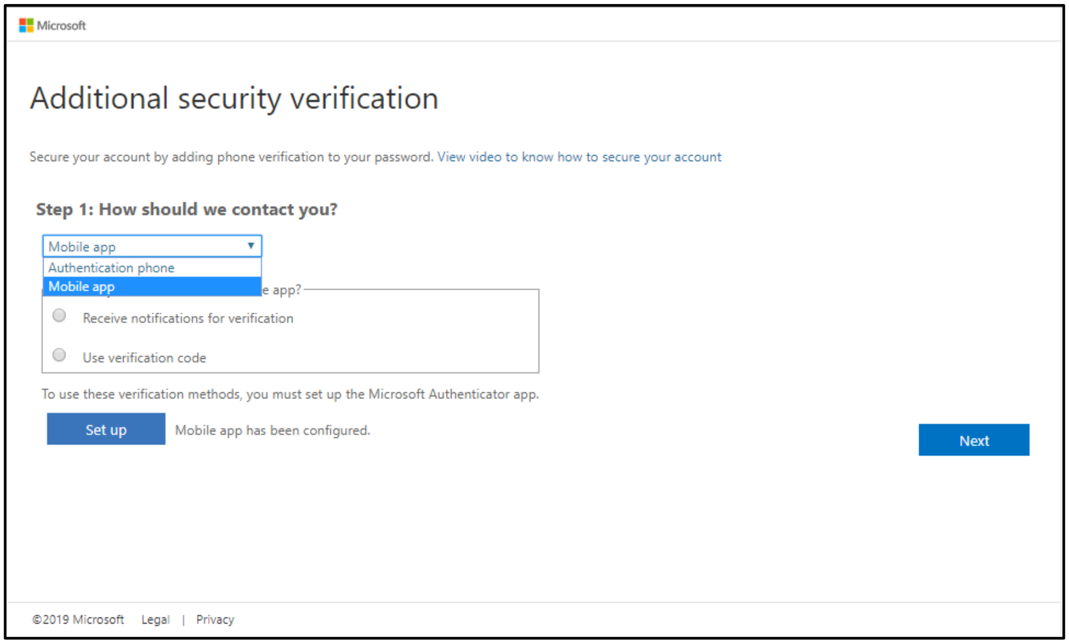
testuser@fusionmfademo2.onmicrosoft.com

More information required

Your organization needs more information to keep your account secure

5. Click **Next**. An **Additional security verification** page is displayed.

Additional security verification Page



Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account

Step 1: How should we contact you?

○ Receive notifications for verification

○ Use verification code

To use these verification methods, you must set up the Microsoft Authenticator app.

Mobile app has been configured.

To complete multifactor authentication, users can choose to provide additional verification via phone or the Microsoft Authenticator app.

Phone Verification

To verify user credentials via phone:

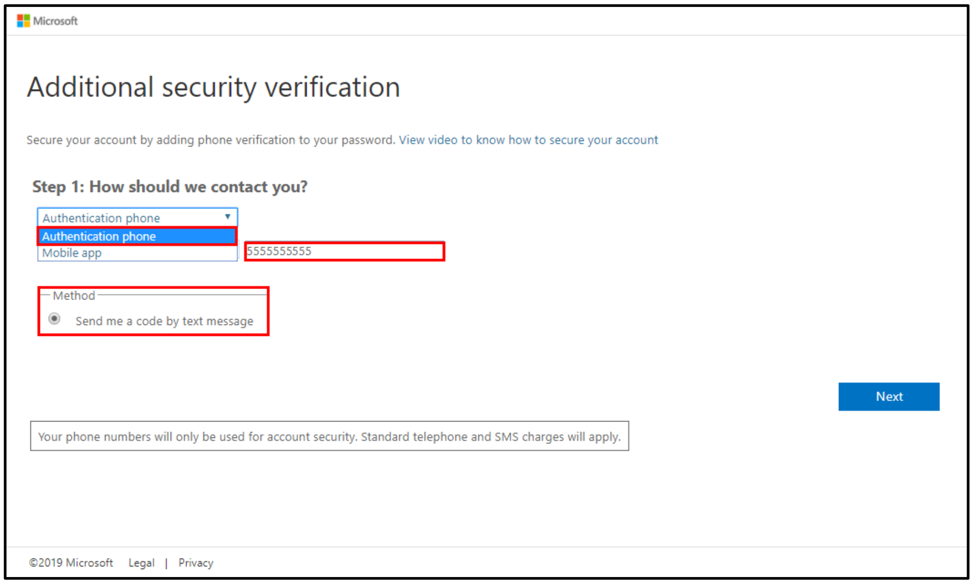
1. Choose the **Authentication phone** contact method:

   a. Select **Authentication phone** from the drop-down menu.

   b. Enter the user's mobile phone number in the text field next to the drop-down menu.

   c. Click the **Send me a code by text message** radio button.

Additional security verification Page



Microsoft

Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account

Step 1: How should we contact you?

Authentication phone ▾
Authentication phone
Mobile app

5555555555

Method

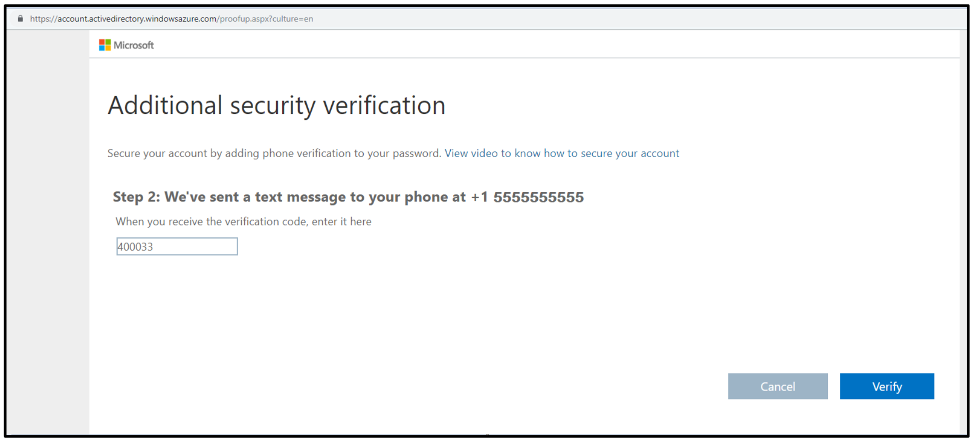
● Send me a code by text message

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

©2019 Microsoft Legal | Privacy

2. Click **Next**. A message is displayed stating that a verification code has been sent to the mobile phone number provided.

Additional security verification Page – Verification Code



https://account.activedirectory.windowsazure.com/proofup.aspx?culture=en

Microsoft

Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account

Step 2: We've sent a text message to your phone at +1 5555555555

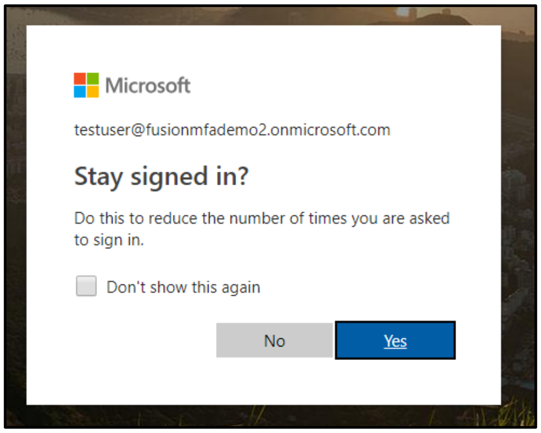
When you receive the verification code, enter it here

400033

3. Enter the verification code in the text field, and then click **Verify**.

4. Once the code is verified, click **Done**. A message window asking whether the user account should stay signed into the Crestron Fusion server is displayed.

Stay signed in? Message Window



Microsoft

testuser@fusionmfademo2.onmicrosoft.com

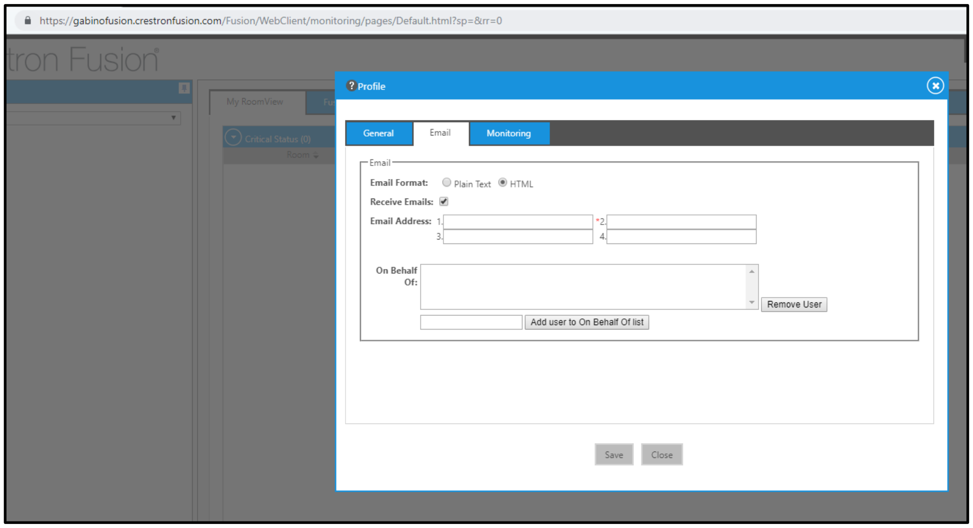
Stay signed in?

Do this to reduce the number of times you are asked to sign in.

□ Don't show this again

5. Select **Yes** or **No**. The user is now redirected to the main Crestron Fusion page.

Crestron Fusion Page



https://gabinofusion.crestronfusion.com/Fusion/WebClient/monitoring/pages/Default.html?sp=&rr=0

Email

Email Format: ○ Plain Text ● HTML

Receive Emails: ☑

Email Address: 1. *2. 3. 4.

On Behalf Of:

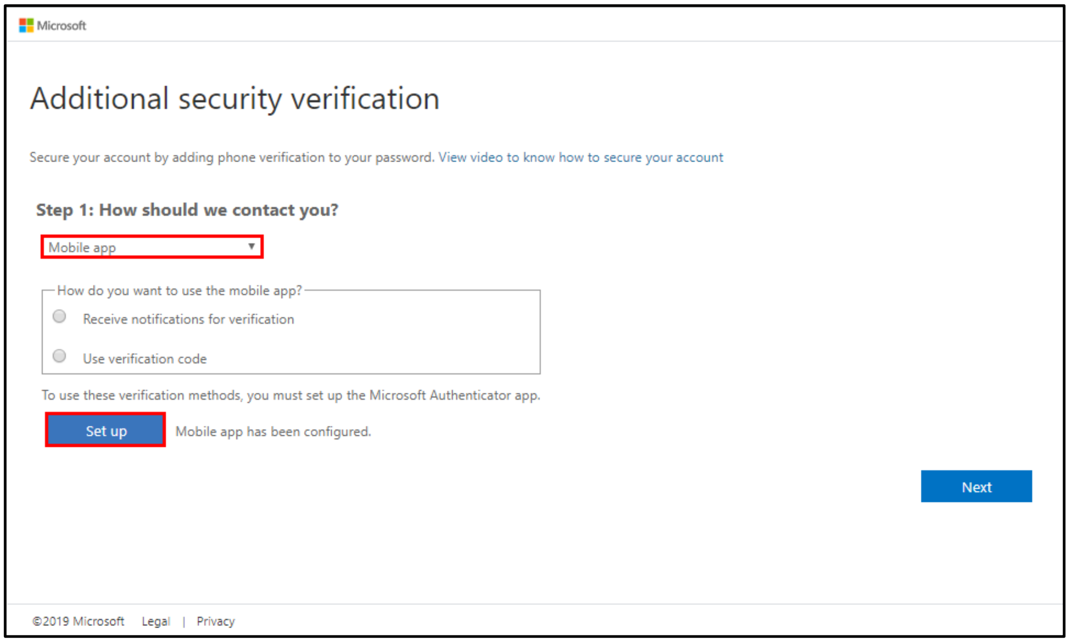
Mobile App Verification

To verify user credentials via the Microsoft Authenticator app:

NOTE: This procedure requires the Microsoft Authenticator app to be installed on a mobile device. Download the Microsoft Authenticator app from the Google Play® online store (for Android® OS devices) or from the App Store® online store (for iOS® devices)

1. Choose the **Mobile app** contact method.
2. Click **Set Up**.

Additional security verification Page – Mobile App



Microsoft

Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account

Step 1: How should we contact you?

Mobile app ▾

How do you want to use the mobile app?

○ Receive notifications for verification

○ Use verification code

To use these verification methods, you must set up the Microsoft Authenticator app.

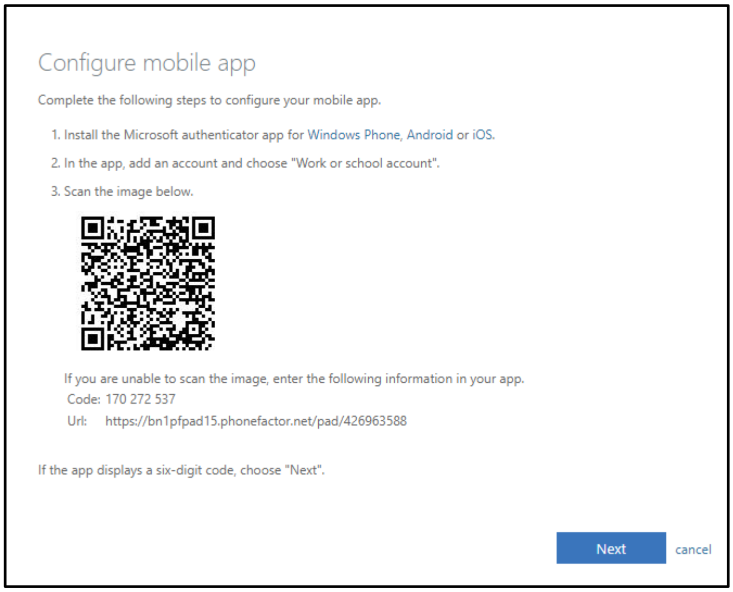
Set up   Mobile app has been configured.

Next

©2019 Microsoft   Legal | Privacy

After the Azure portal retrieves the information necessary for configuration, a **Configure Mobile App** dialog box is displayed.

Crestron mobile app Dialog Box



Configure mobile app

Complete the following steps to configure your mobile app.

1. Install the Microsoft authenticator app for Windows Phone, Android or iOS.
2. In the app, add an account and choose "Work or school account".
3. Scan the image below.

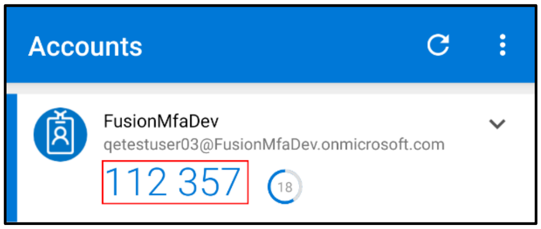
If you are unable to scan the image, enter the following information in your app.
Code: 170 272 537
Url: https://bn1pfpad15.phonefactor.net/pad/426963588

If the app displays a six-digit code, choose "Next".

3. Follow the instructions presented in the dialog box to add the user account to the Microsoft Authenticator app.

   If the user is added successfully, the app displays a six-digit code underneath the user account.

Microsoft Authenticator App – Accounts

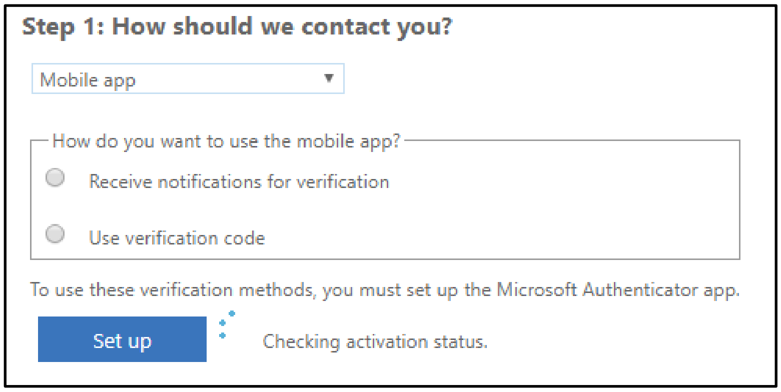


Accounts

FusionMfaDev
qetestuser03@FusionMfaDev.onmicrosoft.com
112 357

4. Click **Next**. The **Additional security verification** page displays a “Checking Activation” status next to the **Set up** button.

Microsoft Authenticator App – Accounts



Step 1: How should we contact you?

Mobile app ▾

How do you want to use the mobile app?

○ Receive notifications for verification

○ Use verification code

To use these verification methods, you must set up the Microsoft Authenticator app.

Checking activation status.

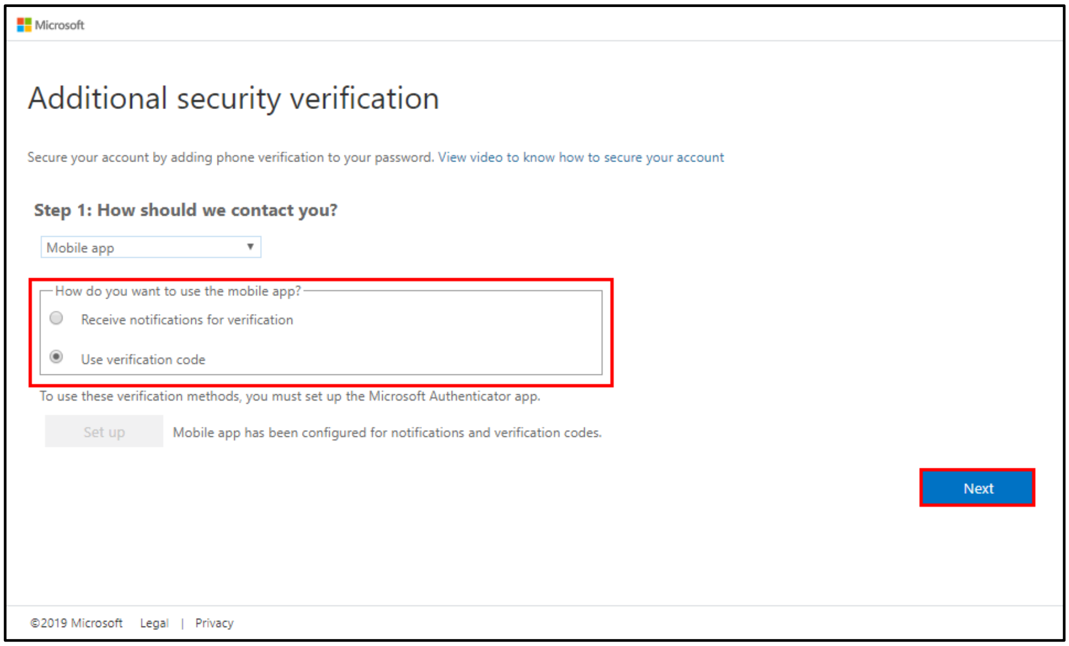
The account is successfully set up once a "Mobile app has been configured for notifications and verification codes" message is displayed and the **Set up** button becomes greyed out.

5. Select one of the following verification methods to use for the mobile app:

   - Click **Receive notifications for verification** to receive notifications in the Microsoft Authenticator app to verify login.

   - Click **Use verification code** to use a verification code for login.

Microsoft Authenticator App – Accounts



Microsoft

Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account

Step 1: How should we contact you?

Mobile app ▼

How do you want to use the mobile app?

○ Receive notifications for verification

● Use verification code

To use these verification methods, you must set up the Microsoft Authenticator app.

Mobile app has been configured for notifications and verification codes.

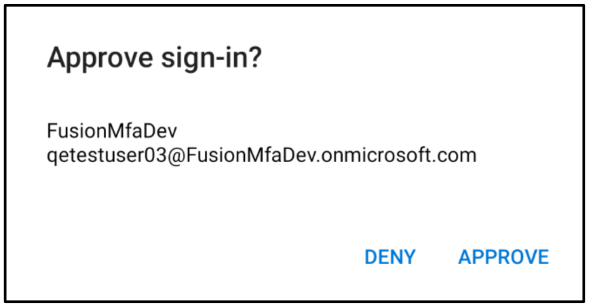
©2019 Microsoft Legal | Privacy

6. Click **Next.** The remaining procedures differ depending on the selected verification method.

Receive Notifications for Verification

If **Receive notifications for verification** was selected, an **Approve sign-in?** notification is sent to the Microsoft Authenticator app.

Approve sign-in? Notification



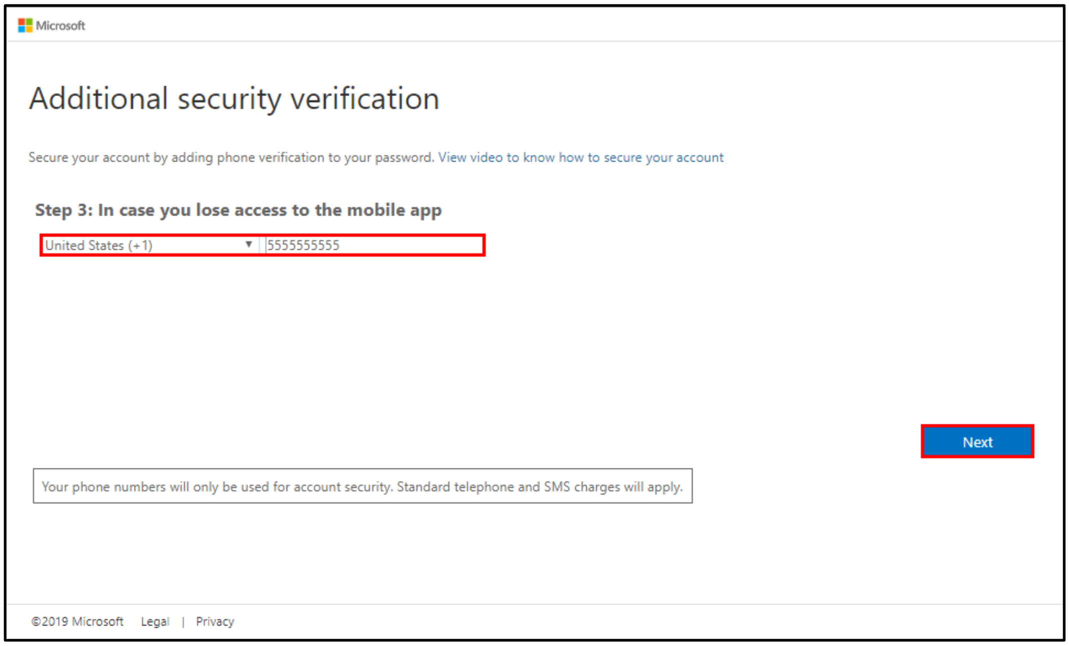
Approve sign-in?

FusionMfaDev
qetestuser03@FusionMfaDev.onmicrosoft.com

1. Tap **APPROVE** in the app.

2. On the **Additional security verification** page, enter a security phone number.

Additional security verification Page – Phone Verification



Microsoft

Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account

Step 3: In case you lose access to the mobile app

United States (+1) ▾ | 5555555555

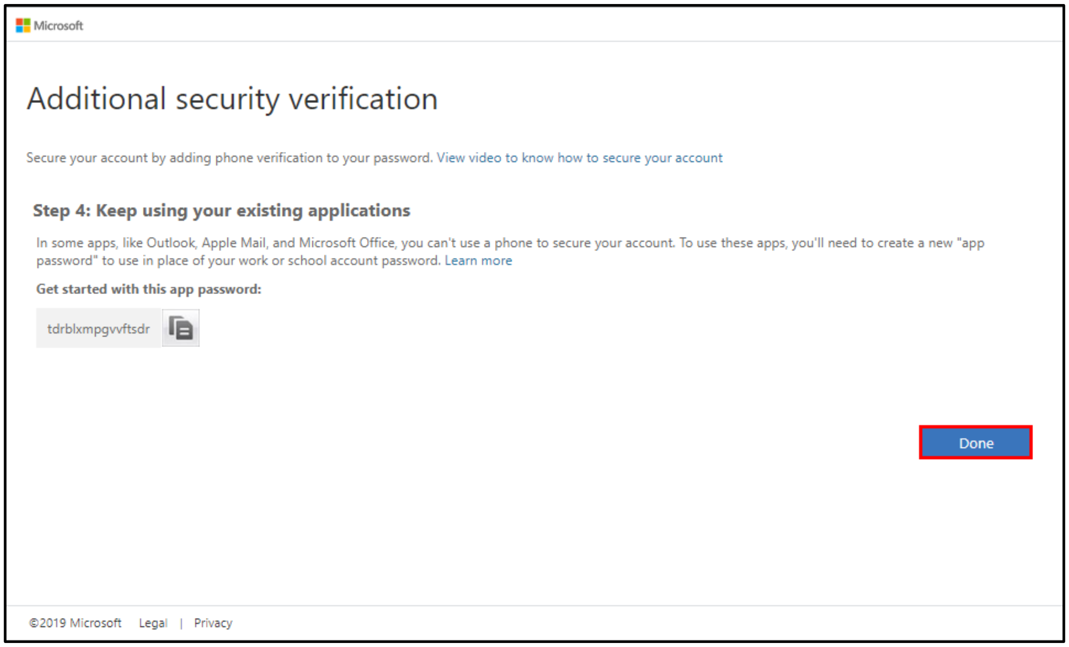
Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

©2019 Microsoft Legal | Privacy

3. Click **Next**.

4. Click **Done** on the next page.

Additional security verification Page – Existing Applications



Microsoft

Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account

Step 4: Keep using your existing applications

In some apps, like Outlook, Apple Mail, and Microsoft Office, you can't use a phone to secure your account. To use these apps, you'll need to create a new "app password" to use in place of your work or school account password. Learn more

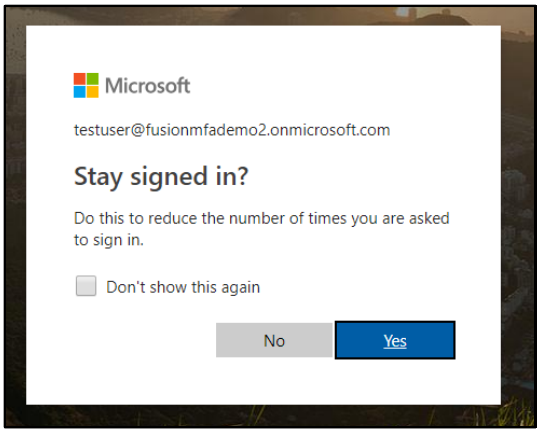
Get started with this app password:

tdrblxmpgvvftsdr

©2019 Microsoft Legal | Privacy

5. Once the account is verified, a message window asking whether the user account should stay signed into the Crestron Fusion server is displayed.

Stay signed in? Message Window



testuser@fusionmfademo2.onmicrosoft.com

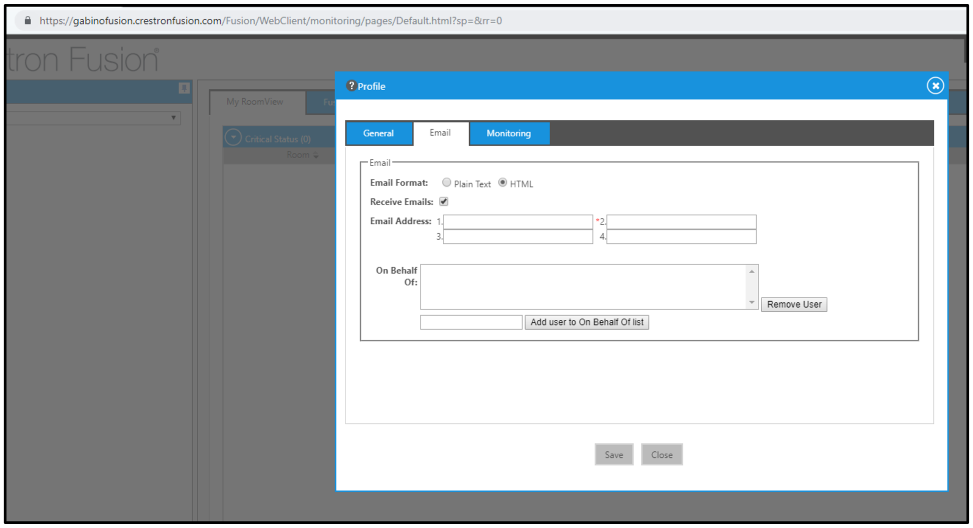
Stay signed in?

Do this to reduce the number of times you are asked to sign in.

□ Don't show this again

6. Select **Yes** or **No**. The user is now redirected to the main Crestron Fusion page.

Crestron Fusion Page


https://gabinofusion.crestronfusion.com/Fusion/WebClient/monitoring/pages/Default.html?sp=&rr=0

Email

Email Format: ○ Plain Text ● HTML

Receive Emails: ☑

Email Address: 1. *2. 3. 4.

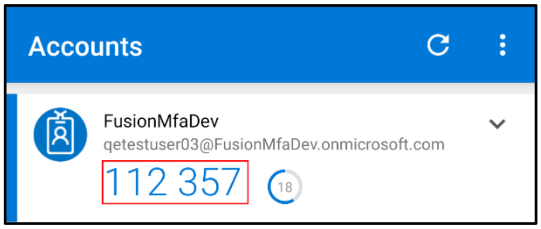
On Behalf Of:

Use Verification Code

If **Use verification code** was selected, the six-digit verification code created in step 3 of "Mobile App Verification" is used for authentication.

1. Navigate to the **Accounts** tab in the Microsoft Authenticator app.
2. Copy the six-digit code listed underneath the appropriate user account.

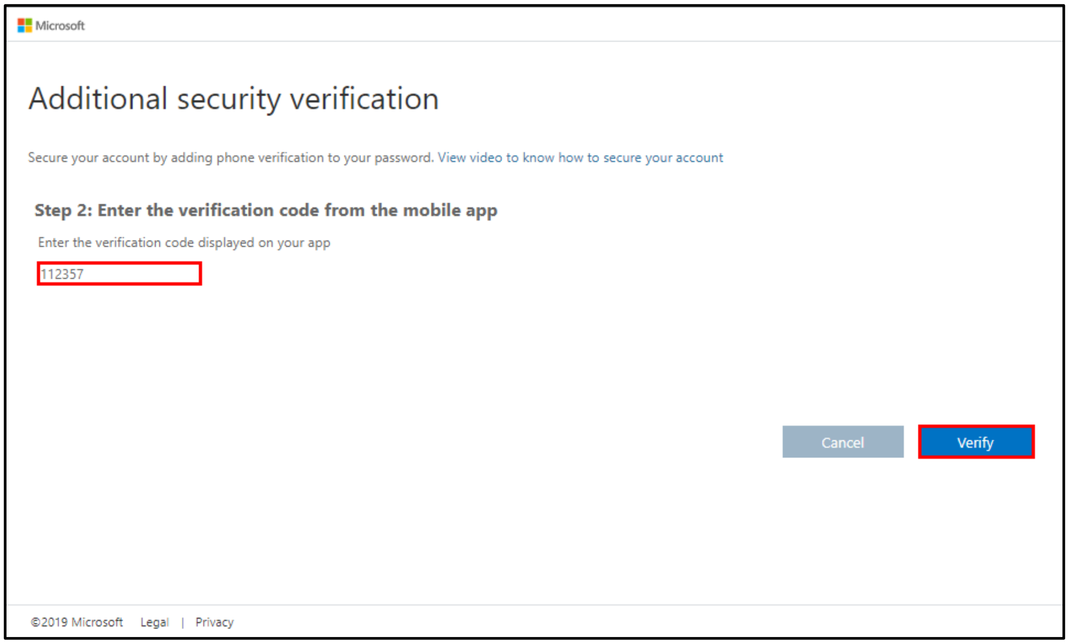
Microsoft Authenticator App – Accounts



FusionMfaDev
qetestuser03@FusionMfaDev.onmicrosoft.com
112 357

3. On the **Additional security verification** page, enter the verification code from the app in the provided text field.

Additional security verification Page – Verification Code



Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account

Step 2: Enter the verification code from the mobile app

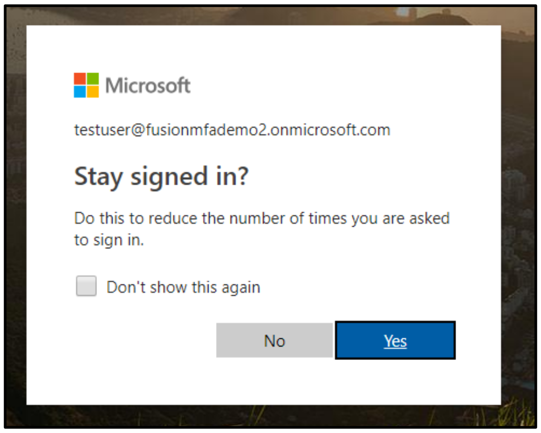
Enter the verification code displayed on your app

112357

©2019 Microsoft Legal | Privacy

4. Once the account is verified, click **Done**. A message window asking whether the user account should stay signed into the Crestron Fusion server is displayed.

Stay signed in? Message Window



Microsoft

testuser@fusionmfademo2.onmicrosoft.com

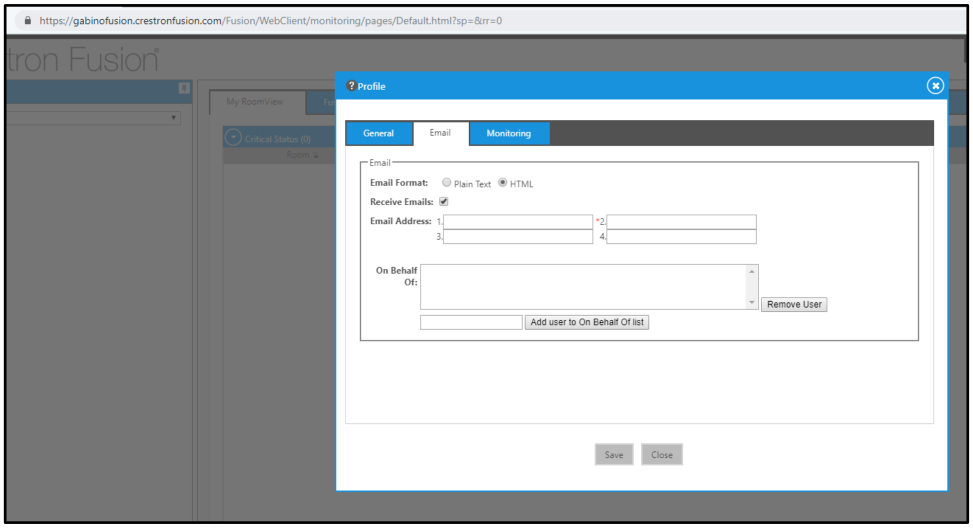
Stay signed in?

Do this to reduce the number of times you are asked to sign in.

□ Don't show this again

5. Select **Yes** or **No**. The user is now redirected to the main Crestron Fusion page.

Crestron Fusion Page



https://gabinofusion.crestronfusion.com/Fusion/WebClient/monitoring/pages/Default.html?sp=&rr=0

Profile

Email

Email Format: ○ Plain Text ● HTML

Receive Emails: ☑

Email Address: 1. *2. 3. 4.

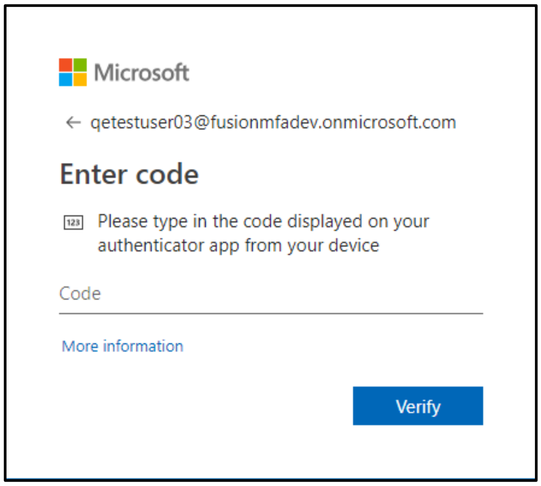
On Behalf Of:

Subsequent Logins

Depending on the verification method selected, the following information is required for subsequent logins into the Crestron Fusion server through Azure Active Directory.

- If a verification code was selected, enter the verification code shown under the user account in the Microsoft Authenticator app into the provided text field, and then click **Verify**.

Enter Code Message Window



Microsoft

← qetestuser03@fusionmfadev.onmicrosoft.com

Enter code

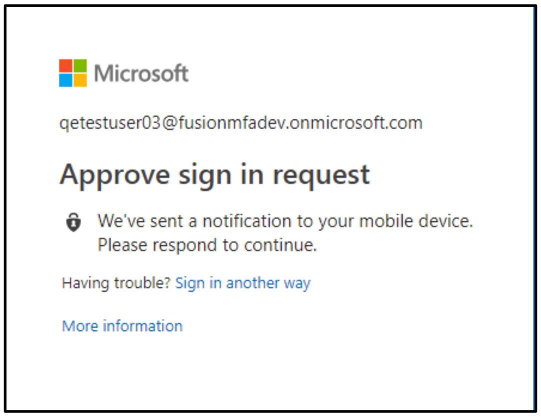
Please type in the code displayed on your authenticator app from your device

Code

More information

- If receiving notifications for verification was selected, respond to the notification in the Microsoft Authenticator app to continue to log in.

Enter Code Message Window



Microsoft

qetestuser03@fusionmfadev.onmicrosoft.com

Approve sign in request

We've sent a notification to your mobile device. Please respond to continue.

Having trouble? Sign in another way

More information

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

Configuration Guide – DOC. 8459A
(2053719)
04.19
Specifications subject to
change without notice.