



Crestron® Room Scheduling Panels for TSW-60 Series

Operations 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.

Crestron product development software is licensed to Crestron dealers and Crestron Service Providers (CSPs) under a limited nonexclusive, nontransferable Software Development Tools License Agreement. Crestron product operating system software is licensed to Crestron dealers, CSPs, and end-users under a separate End-User License Agreement. Both of these Agreements can be found on the Crestron website at www.crestron.com/legal/software_license_agreement.

The product warranty can be found at www.crestron.com/warranty.

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/opensource.

Crestron, the Crestron logo, Crestron Fusion, Crestron Toolbox, RoomView, and XiO Cloud are either trademarks or registered trademarks of Crestron Electronics, Inc. in the United States and/or other countries. Ad Astra is either a trademark or a registered trademark of Ad Astra Information Systems, LLC in the United States and/or other countries. CollegeNET and 25Live are either trademarks or registered trademarks of CollegeNET, Inc. in the United States and/or other countries. Google and Google Calendar are either trademarks or registered trademarks of Google, Inc. in the United States and/or other countries. Active Directory, Microsoft, Microsoft Entra, and Office 365 are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Other trademarks, registered trademarks, and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Crestron disclaims any proprietary interest in the marks and names of others. Crestron is not responsible for errors in typography or photography. Other trademarks, registered trademarks, and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Crestron disclaims any proprietary interest in the marks and names of others. Crestron is not responsible for errors in typography or photography.

©2023 Crestron Electronics, Inc.

Contents

| | |
|---|-----------|
| Introduction | 1 |
| Setup | 2 |
| Access the Web Configuration Interface | 2 |
| Set the Time Zone | 3 |
| Select the Scheduling App (Non-TSS Only) | 4 |
| Connect to a Scheduling Calendar | 6 |
| Connect to Crestron Fusion | 6 |
| Connect to Microsoft Exchange Using EWS | 7 |
| Connect to Office 365 Using Microsoft Graph | 9 |
| Connect to Google Calendar | 10 |
| Connect to Ad Astra | 12 |
| Connect to CollegeNet 25 Live | 12 |
| Web Configuration | 14 |
| Actions Menu | 15 |
| Reboot | 15 |
| Restore | 15 |
| Firmware Upgrade | 16 |
| Download Logs | 16 |
| Manage Certificates | 16 |
| Enter Setup | 16 |
| Enter Standby | 16 |
| Save Changes | 17 |
| Revert | 17 |
| Upload Scheduling Project | 17 |
| Status | 18 |
| Device | 18 |
| Network | 19 |
| USB | 20 |
| Room Scheduling | 20 |
| Display | 20 |
| Schedule | 21 |
| Settings | 24 |
| System Setup | 25 |
| Network Proxy Settings | 29 |
| Audio | 30 |
| Cloud Settings | 31 |
| Configure Date/Time | 31 |
| Authentication Management | 32 |
| 802.1x Configuration | 41 |
| Auto Update | 43 |

| | |
|---|-----------|
| Applications | 44 |
| Device Pairing | 45 |
| Schedule | 45 |
| Reservation | 52 |
| UI Settings | 54 |
| Display | 56 |
| Room | 58 |
| Automation | 59 |
| Work Hours | 62 |
| Broadcast Messages | 63 |
| Crestron Fusion Configuration | 64 |
| Add Custom Properties to a Room | 64 |
| Set Custom Properties for the Scheduling Application | 65 |
| Scheduling Application Custom Properties | 66 |
| Work Hours Settings | 66 |
| Display Settings | 67 |
| Broadcast Message Settings | 67 |
| UI Settings | 68 |
| Automation Settings | 69 |
| Room Settings | 69 |
| Reservation Settings | 71 |
| Schedule Settings | 72 |
| All Scheduling Application Custom Properties | 73 |
| Appendix A: Configure Modern Authentication for EWS | 75 |
| Configure the Crestron Room Scheduling EWS App | 75 |
| Create the Crestron Room Scheduling App | 75 |
| Obtain Authentication IDs | 77 |
| Configure Additional Settings | 78 |
| Connect the Scheduling App to EWS | 86 |
| Appendix B: Configure Microsoft Graph for Crestron Room Scheduling | 90 |
| Configure the Crestron Room Scheduling App | 90 |
| Create the Crestron Room Scheduling App | 91 |
| Create a Client Secret | 95 |
| Add API Permissions | 97 |
| Obtain Authentication IDs | 102 |
| Connect the Scheduling App to Microsoft Graph | 104 |

Introduction

The Crestron® room scheduling application provides a complete room scheduling solution for the Crestron [TSS-7](#) and [TSS-10](#) room scheduling touch screens and the [TSW-560](#), [TSW-560P](#), [TSW-760](#), and [TSW-1060](#) touch screens. When the scheduling application is enabled on a touch screen installed outside of a meeting space, users may view the room's availability, check the status of nearby rooms, and book an ad hoc meeting directly through the touch screen.

The scheduling application integrates with Crestron Fusion® software, Microsoft® Exchange and Microsoft Office 365® software, the Google Calendar™ calendaring application (via a Google® software account), Ad Astra™ software, or CollegeNet® 25Live® software to provide real-time notifications and to monitor the meeting space intelligently.

NOTE: The scheduling application comes preinstalled on supported touch screens. Ensure that the touch screen is running the latest firmware version that includes the scheduling application. For more information, refer to the firmware release notes.

The following documents are also provided for the scheduling application:

- For more information about scheduling application functionality and the user interface, refer to the [Crestron Room Scheduling Panels User Guide](#).
- For more information about customizing the scheduling application, refer to the [Crestron Room Scheduling Panels Programming Guide](#).

Setup

Use the following procedures to select the room scheduling application mode on the touch screen (for touch screens not dedicated to room scheduling) and to set up a connection to a supported scheduling calendar.

NOTE: Ensure that the latest touch screen firmware that includes the scheduling application is installed on the touch screen. If older firmware is installed on the touch screen, download and install the most recent firmware from www.crestron.com/Support/Resource-Library.

Access the Web Configuration Interface

Turn on the room scheduling application via the included web configuration interface. The web configuration interface is accessible from a web browser if the IP address of the touch screen is known. A similar interface is also accessible using the XiO Cloud® service.

To access the web configuration interface:

1. Use the **Device Discovery** tool in Crestron Toolbox™ software to discover the touch screen and its IP address on the network
2. Open a web browser.
3. Enter the touch screen IP address into the browser URL field. The configuration interface is displayed.

NOTE: If authentication is turned on for the touch screen, an administrator username and password must be entered prior to accessing the web configuration interface. For more information on configuring authentication settings, refer to [Authentication Management on page 32](#).



Set the Time Zone

If Microsoft Exchange or Crestron Fusion will be used as the scheduling calendar provider, set the time zone on the touch screen prior to enabling the scheduling application.

NOTE: If Google Calendar will be used as the scheduling panel provider, the scheduling application uses the time zone set in the Google Calendar settings.

To set the time zone from the configuration interface:

1. Navigate to **Settings > Configure Date/Time**.

Settings Tab - Configure Date/Time

2. Turn on the **Enable Time Synchronization** toggle to use time synchronization via SNTP (Simple Network Time Protocol).
3. Turn on the **Time Synchronization** toggle to use time synchronization via SNTP (Simple Network Time Protocol).
4. Enter the necessary information in the **TimeServers** table and the **Time Zone**, **Time(24hr Format)**, and **Date** fields. For more information, refer to [Configure Date/Time on page 31](#).
5. Select **Synchronize Now**. The touch screen may take up to two minutes to synchronize with the SNTP server.

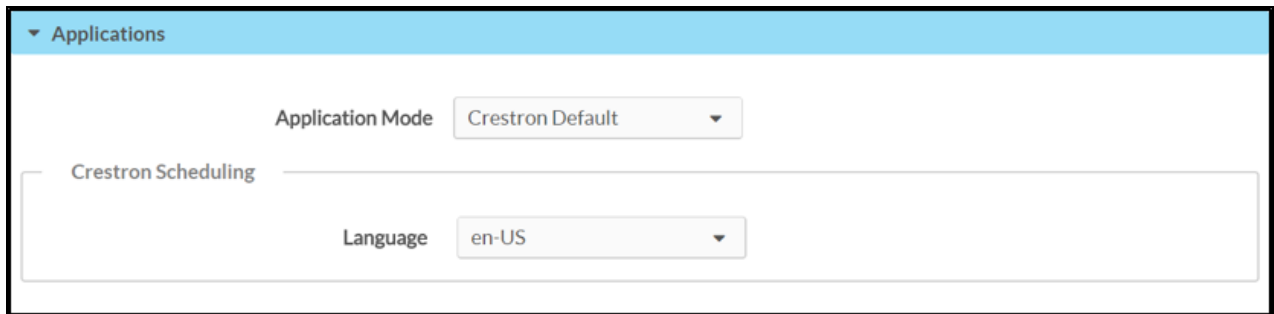
Select the Scheduling App (Non-TSS Only)

To select the scheduling application from the configuration interface if using a TSW-60 series touch screen not dedicated exclusively to room scheduling:

NOTE: The Crestron scheduling application is selected by default on TSS-7 and TSS-10 touch screens.

1. Navigate to **Settings > Applications**.
2. Select **Crestron Default** from the **Application Mode** drop-down menu.

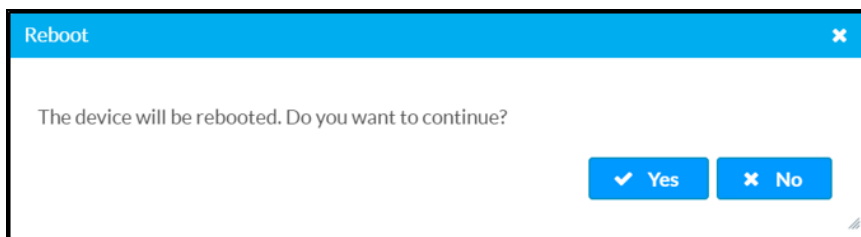
Settings Tab - Applications (Crestron Default)



The screenshot shows the 'Applications' settings screen. At the top, there is a blue header bar with a dropdown arrow and the text 'Applications'. Below this, the 'Application Mode' is set to 'Crestron Default' in a dropdown menu. Underneath, there is a section titled 'Crestron Scheduling' which contains a 'Language' dropdown menu set to 'en-US'.

3. Use the **Language** drop-down menu to select the language that will be displayed by the scheduling application.
4. Select **Save Changes** from the **Action** menu. A pop-up window stating that the touch screen will be rebooted displays.

Reboot Window



The screenshot shows a 'Reboot' confirmation window. It has a blue header bar with the text 'Reboot' and a close button (X). The main text asks, 'The device will be rebooted. Do you want to continue?'. At the bottom right, there are two buttons: 'Yes' with a checkmark icon and 'No' with an X icon.

5. Select **Yes** to retart the touch screen in scheduling mode.

Connect to a Scheduling Calendar

Use the following procedures to connect to one of the supported scheduling calendars (Crestron Fusion, Microsoft Exchange/Office 365, Google Calendar, Ad Astra, or CollegeNet 25Live).

NOTE: The scheduling application must be selected before a connection to a scheduling calendar can be established.

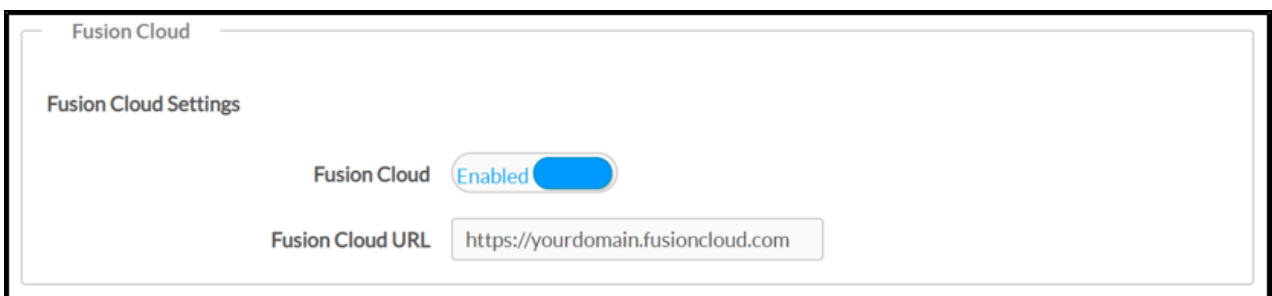
Connect to Crestron Fusion

To connect to a Crestron Fusion scheduling calendar:

NOTE: The touch screen must be added to a room in Crestron Fusion before the scheduling calendar shows as online. For more information, refer to the [Adding Devices to Crestron Fusion Getting Started Guide](#).

1. Navigate to **Settings > System Setup (Crestron Fusion Cloud)**
2. Turn on the **Crestron Fusion Cloud** toggle.

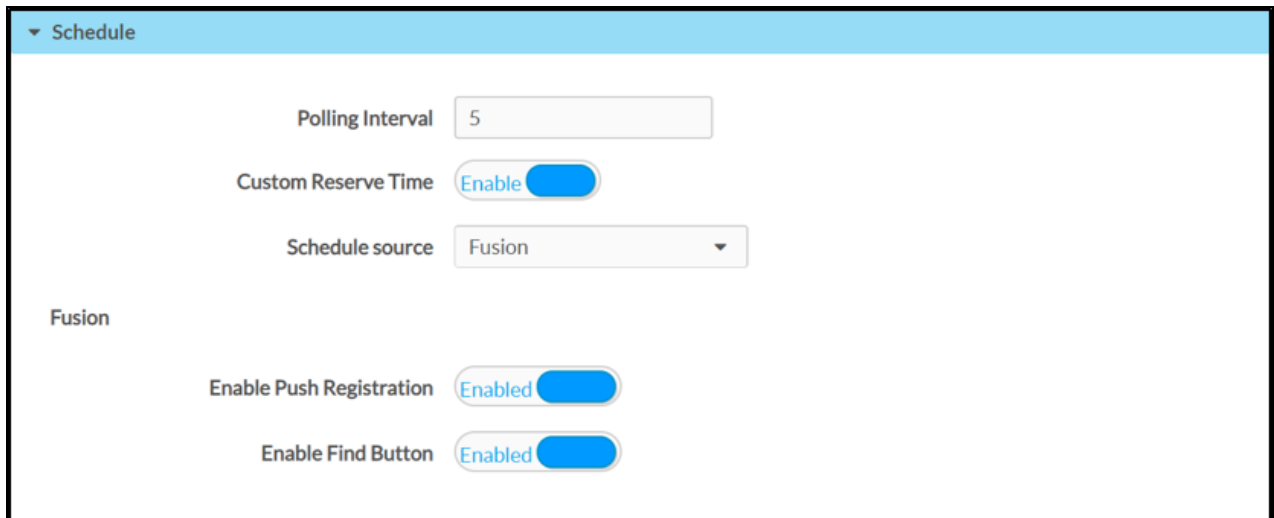
Settings Tab - System Setup (Crestron Fusion Cloud)



3. Enter the Crestron Fusion cloud URL that contains the desired scheduling calendar in the **Crestron Fusion Cloud URL** field.
4. Navigate to **Settings > Schedule**.
5. Configure the desired **Polling Interval** and **Custom Reserve Time** settings. For more information, refer to [Schedule on page 45](#).

6. Select **Crestron Fusion** from the **Schedule Source** drop-down menu.

Settings Tab - Schedule (Crestron Fusion)

The screenshot shows the 'Schedule' settings tab for Crestron Fusion. It features a light blue header with a dropdown arrow and the text 'Schedule'. Below this, there are five settings: 'Polling Interval' with a text input field containing the number '5'; 'Custom Reserve Time' with a toggle switch labeled 'Enable' that is turned on; 'Schedule source' with a dropdown menu showing 'Fusion'; a section header 'Fusion'; 'Enable Push Registration' with a toggle switch labeled 'Enabled' that is turned on; and 'Enable Find Button' with a toggle switch labeled 'Enabled' that is turned on.

7. Configure the following Crestron Fusion settings:
 - Turn on the **Enable Push Registration** toggle to have Crestron Fusion push scheduling calendar data to the scheduling application.
 - Turn on the **Enable Find Button** toggle to display a find button on the scheduling application so a user may look up nearby rooms available for meetings.
8. Select **Save Changes** from the **Action** menu. The Crestron Fusion scheduling calendar connects to the scheduling application without requiring a restart.

Connect to Microsoft Exchange Using EWS

To connect to a Microsoft Exchange scheduling calendar using EWS (Exchange Web Services):

NOTE: The Microsoft Exchange account and scheduling calendar must be fully configured before the scheduling calendar shows as online.

1. Navigate to **Settings > Schedule**.
2. Configure the desired **Polling Interval** and **Custom Reserve Time** settings. For more information, refer to [Schedule on page 45](#).

3. Select **Exchange EWS** from the **Schedule Source** drop-down menu.

Settings Tab - Schedule (Exchange EWS)

▼ Schedule

Polling Interval

Custom Reserve Time ☐ Disable

Schedule source

Exchange EWS

Enable Modern Authorization ☐ Disabled

Exchange Calendar Email Address This field is required.

Exchange Account Username This field is required.

Exchange Account Password This field is required.

Exchange Domain

Exchange Web Services URL This field is required.

4. Enter the following Microsoft Exchange account information:

- Turn on the **Enable Modern Authentication** toggle to use Modern Authentication for the EWS account. For instructions on configuring Modern Authentication for use with the Crestron Room Scheduling application, refer to [Appendix A: Configure Modern Authentication for EWS on page 75](#).
- Enter the email address associated with the Microsoft Exchange scheduling calendar in the **Exchange Calendar Email Address** text field.
- Enter the username for the Microsoft Exchange account in the **Exchange Account Username** text field.

NOTE: The username must include the ".com" suffix similar to the email address entered in the **Exchange Calendar Email Address** text field.

- Enter the password for the Microsoft Exchange account in the **Exchange Account Password** text field.
- Enter the domain name associated with the Microsoft Exchange account in the **Exchange Domain** text field.

NOTE: The **Exchange Domain** text field must be left blank if using Office 365 software.

- Enter the Microsoft EWS (Exchange Web Services) server URL that the scheduling calendar uses to access Microsoft Exchange scheduling data in the **Exchange Web Services URL** text field.
5. Select **Save Changes** from the **Action** menu. The Microsoft Exchange scheduling calendar connects to the scheduling application without requiring a restart.

Additional registration steps are required if Enable Modern Authentication is set to enabled. Refer to [Appendix A: Configure Modern Authentication for EWS on page 75](#) for more information.

Connect to Office 365 Using Microsoft Graph

To connect to an Office 365 scheduling calendar using Microsoft Graph:

NOTES:

- The Office 365 account and scheduling calendar must be fully configured before the scheduling calendar shows as online.
- Additional registration steps are required in the Microsoft Entra® portal. Refer to [Appendix B: Configure Microsoft Graph for Crestron Room Scheduling on page 90](#) for more information.

1. Navigate to **Settings > Schedule**.
2. Configure the desired **Polling Interval** and **Custom Reserve Time** settings. For more information, refer to [Schedule on page 45](#).
3. Select **O365** from the **Schedule Source** drop-down menu.

Settings Tab - Schedule (O365)

▼ Schedule

Polling Interval

Custom Reserve Time ☐ Disable

Schedule source

O365

Exchange Calendar Email Address This field is required.

O365 Tenant ID This field is required.

Client ID (Application ID) This field is required.

Client Secret

4. Enter the following Office 365 account information:

NOTE: The **Client ID (Application ID)**, **O365 Tenant ID**, and **Client Secret** values are generated within the Microsoft Entra portal for the Microsoft Entra app. For more information, refer to [Appendix B: Configure Microsoft Graph for Crestron Room Scheduling on page 90](#).

- Enter the email address associated with the Office 365 scheduling calendar in the **Exchange Calendar Email Address** text field.
- Enter the client (application) ID generated for the Microsoft Entra app in the **Client ID (Application ID)** text field.
- Enter the directory (tenant) ID generated for the Microsoft Entra app in the **O365 Tenant ID** text field.

- Enter the client secret generated for the Microsoft Entra app in the **Client Secret** text field.
5. Select **Save Changes** from the **Action** menu. The Office 365 scheduling calendar connects to the scheduling application without requiring a restart.

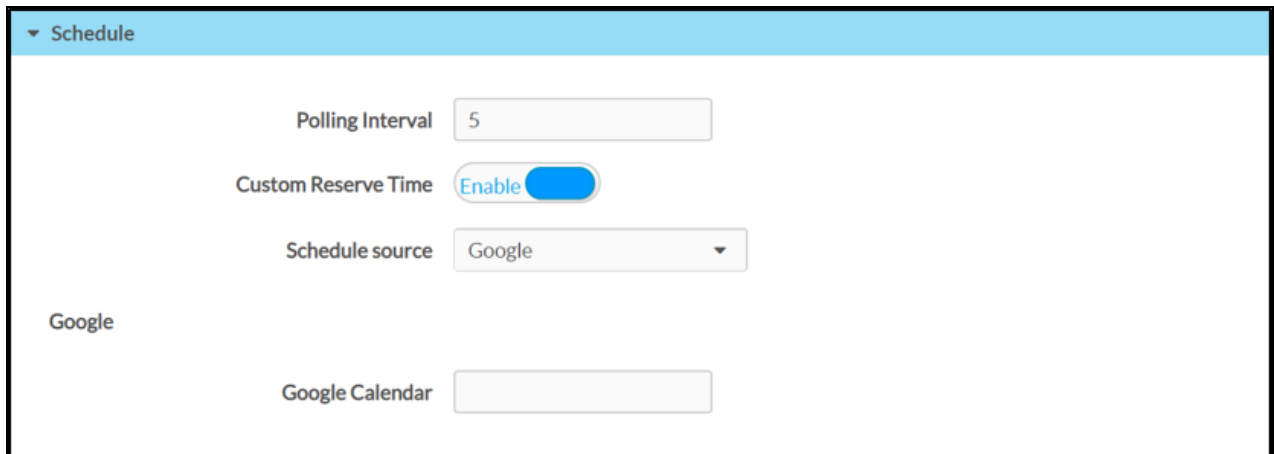
Connect to Google Calendar

To connect to a Google scheduling calendar:

NOTE: The Google account and scheduling calendar must be fully configured before the scheduling calendar shows as online.

1. Navigate to **Settings > Schedule**.
2. Configure the desired **Polling Interval** and **Custom Reserve Time** settings. For more information, refer to [Schedule on page 45](#).
3. Select **Google** from the **Schedule Source** drop-down menu.

Settings Tab - Schedule (Google)



The screenshot shows the 'Schedule' settings interface for Google. At the top, there is a blue header bar with a dropdown arrow and the text 'Schedule'. Below this, the settings are organized into sections. The first section contains 'Polling Interval' with a text input field containing the number '5'. The second section contains 'Custom Reserve Time' with a blue toggle switch labeled 'Enable'. The third section contains 'Schedule source' with a dropdown menu showing 'Google'. Below these settings, there is a section labeled 'Google' which contains a 'Google Calendar' text input field.

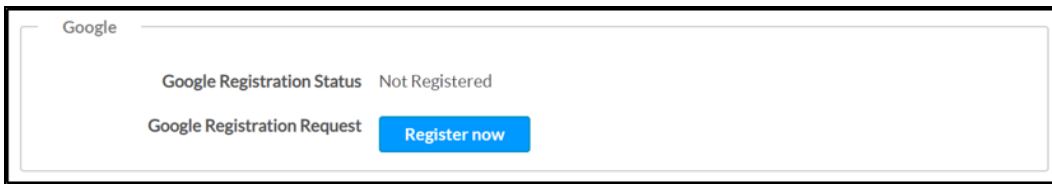
4. Enter the calendar account name or ID in the **Google Calendar** text field if more than one calendar is available for the Google account. If this field is left empty, the scheduling application uses the primary calendar set for the Google account.

NOTE: To switch to a different calendar on the same Google account, enter the new calendar account name or ID in the **Google Calendar** text field.

5. Select **Save Changes** from the **Action** menu.

6. Navigate to **Status > Schedule**. The **Google** subsection displays a **Register now** button.

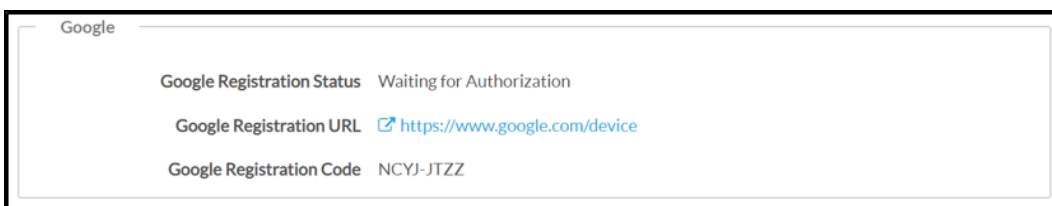
Status Tab - Schedule (Register now Button)



7. Select **Register Now**.

When the web configuration interface refreshes, the **Google** subsection displays a **Google Registration URL** and a **Google Registration Code**, and the **Google Registration Status** updates to "Waiting for Authorization."

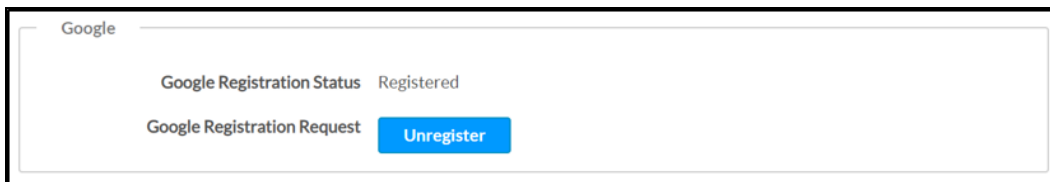
Status Tab - Schedule (Registration URL and Code)



8. Select the provided registration URL. The **Google Connect a device page** is displayed.
9. Enter the provided Google registration code in the **Enter code** field and select **Next**. The **Choose an account** page is displayed.
10. Select the Google account that contains the desired scheduling calendar and enter the account password if prompted. A message window is displayed asking whether Crestron Scheduling Panels is allowed access to manage the Google Calendar account.
11. Select **Allow**. A success message displays if the connection is successful.

When the web configuration interface refreshes, the **Google Registration Status** updates to **Registered**. The Google scheduling calendar connects to the scheduling application without requiring a restart.

Status Tab - Schedule (Registered)



NOTE: Google currently has a token refresh limit of 50. If the limit is reached, it will invalidate the oldest refresh token. For example, if a deployment has 50 touch screens under one account, and if an admin reregisters one of the panels with Google, the touch screen with the oldest refresh token from the remaining 49 will go offline. It is recommended that only 15 or 20 calendars/touch screens are used for one user account. This limit does not apply to service accounts.

Connect to Ad Astra

To connect to an Ad Astra scheduling calendar:

NOTE: The Ad Astra account and scheduling calendar must be fully configured before the scheduling calendar shows as online. Additionally, Ad Astra software does not support scheduling ad hoc meetings from the touch screen.

1. Navigate to **Settings > Schedule**.
2. Configure the desired **Polling Interval** and **Custom Reserve Time** settings. For more information, refer to [Schedule on page 45](#).
3. Select **Ad Astra** from the **Schedule Source** drop-down menu.

Settings Tab - Schedule (Ad Astra)

The screenshot shows the 'Schedule' configuration screen for Ad Astra. It features a light blue header with a dropdown arrow and the text 'Schedule'. Below the header, there are four settings: 'Polling Interval' with a text input field containing the number '5'; 'Custom Reserve Time' with a toggle switch set to 'Disable'; 'Schedule source' with a dropdown menu showing 'Ad Astra'; and 'Ad Astra' as a section header. Under the 'Ad Astra' section, there are four text input fields: 'Username', 'Password', 'Room ID', and 'Server URL'. To the right of each of these four fields is a red error message that reads 'This field is required.'

4. Enter the following Ad Astra account information:
 - Enter the username for the Ad Astra account in the **Username** text field.
 - Enter the password for the Ad Astra account in the **Password** text field.
 - Enter the room ID associated with the Ad Astra scheduling calendar in the **Room ID** text field.
 - Enter the URL of the Ad Astra scheduling calendar server in the **Server URL** text field.
5. Select **Save Changes** from the **Action** menu. The Ad Astra scheduling calendar connects to the scheduling application without requiring a restart.

Connect to CollegeNet 25 Live

To connect to an CollegeNet 25Live scheduling calendar:

NOTE: The CollegeNet 25Live account and scheduling calendar must be fully configured before the scheduling calendar shows as online. Additionally, CollegeNet 25 Live software does not support scheduling ad hoc meetings from the touch screen.

1. Navigate to **Settings > Schedule**.
2. Configure the desired **Polling Interval** and **Custom Reserve Time** settings. For more information, refer to [Schedule on page 45](#).
3. Select **25Live** from the **Schedule Source** drop-down menu.

Settings Tab - Schedule (25Live)

The screenshot shows the 'Schedule' settings tab for the 25Live integration. At the top, there is a blue header bar with a dropdown arrow and the text 'Schedule'. Below this, the 'Polling Interval' is set to '5' in a text input field. The 'Custom Reserve Time' is set to 'Disable' with a toggle switch. The 'Schedule source' is set to '25Live' in a dropdown menu. Below these settings, the '25Live' section is expanded, showing four required fields: 'Username', 'Password', 'Space ID', and 'Server URL'. Each field has a red error message to its right that reads 'This field is required.'.

| Field | Value | Requirement |
|---------------------|---------|-------------------------|
| Polling Interval | 5 | |
| Custom Reserve Time | Disable | |
| Schedule source | 25Live | |
| 25Live Username | | This field is required. |
| 25Live Password | | This field is required. |
| 25Live Space ID | | This field is required. |
| 25Live Server URL | | This field is required. |

4. Enter the following CollegeNet 25Live account information:
 - Enter the username for the CollegeNet 25Live account in the **Username** text field.
 - Enter the password for the CollegeNet 25Live account in the **Password** text field.
 - Enter the space ID associated with the CollegeNet 25Live scheduling calendar in the **Space ID** text field.
 - Enter the URL of the CollegeNet 25Live scheduling calendar server in the **Server URL** text field.
5. Select **Save Changes** from the **Action** menu. The CollegeNet 25Live scheduling calendar connects to the scheduling application without requiring a restart.

Web Configuration

Once the scheduling application is enabled on the touch screen, scheduling application settings may be monitored and configured using the included web configuration interface. This interface is also accessible using the XiO Cloud® service.

NOTE: The scheduling application must be enabled to view and configure scheduling application settings.

If Crestron Fusion will be used to configure the scheduling application, skip ahead to [Crestron Fusion Configuration on page 64](#).

To access the configuration interface, refer to the procedure described in [Access the Web Configuration Interface on page 2](#). The **Status** tab is opened by default.

Web Configuration Interface

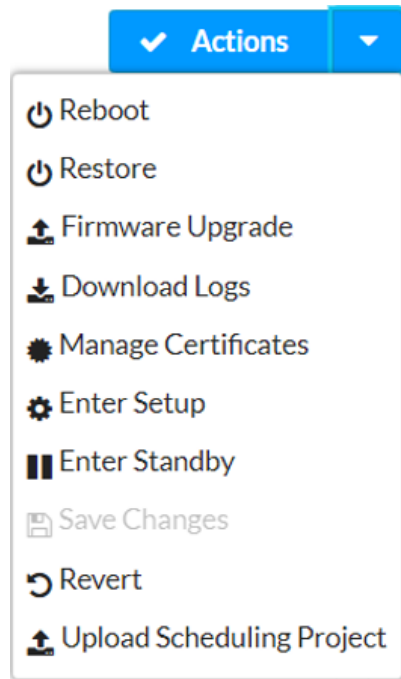


The configuration interface provides a **Status** tab for monitoring scheduling application settings and a **Settings** tab for configuring scheduling application settings. The device host name is displayed at the top left of the page.

Actions Menu

The configuration interface provides an **Actions** drop-down menu on the top right of the page. The **Actions** menu may be accessed at any time.

Actions Menu



Once any changes have been made to the touch screen configuration, the **Actions** button changes to a **Save Changes** button. Select **Save Changes** to save changes to the configuration settings.

If a restart is required after changes have been saved, a dialog box is displayed asking whether the restart should be performed. Select **Yes** to restart the device or **No** to cancel the restart.

The **Actions** menu provides the following selections.

Reboot

Select **Reboot** to restart the touch screen.

After **Reboot** is selected, a dialog box is displayed asking whether the touch screen should be restarted. Select **Yes** to restart the device or **No** to cancel the restart.

Restore

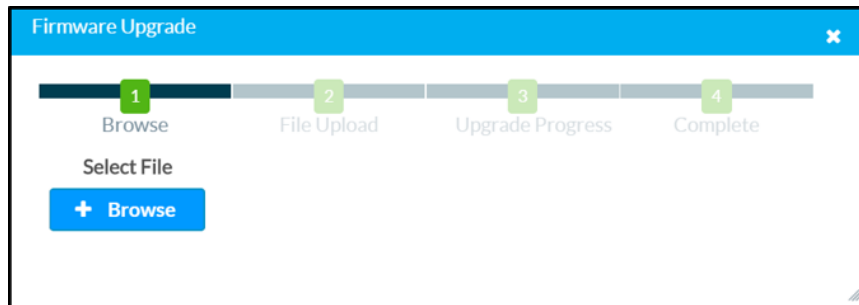
Select **Restore** to restore the touch screen configuration settings to their default values.

After **Restore** is selected a dialog box is displayed asking whether the device settings should be restored. Select **Yes** to restore the settings or **No** to cancel the restore.

Firmware Upgrade

Select **Firmware Upgrade** to upgrade the touch screen firmware manually with a downloaded PUF (package update file). The **Firmware Upgrade** dialog box opens.

Firmware Upgrade Dialog Box



To upload a firmware PUF through the web configuration interface:

NOTE: Visit the appropriate device product page or www.crestron.com/Support/Resource-Library to download the latest firmware PUF.

1. Select **Browse**, and then navigate to the firmware PUF on the host computer.
2. Select the firmware PUF, and then select **Open**.
3. Select **Load** to load the PUF to the touch screen. The upload progress is shown in the dialog box.
4. Once the touch screen has completed the firmware upgrade, select **OK**.

Select the **x** button to close the **Firmware Upgrade** dialog box at any time during the upgrade process. Selecting the **x** button before the PUF is uploaded to the touch screen cancels the upgrade.

Download Logs

Select **Download Logs** to download the touch screen message logs for diagnostic purposes. The message files download as a compressed .tgz file. Once the compressed file is downloaded, extract the message log files to view them.

Manage Certificates

Select **Manage Certificates** to manage any certificates that are installed on the touch screen. For more information on certificate management, refer to [802.1x Configuration on page 41](#).

Enter Setup

Select **Enter Setup** to force the touch screen to enter its built-in setup interface.

Enter Standby

Select **Enter Standby** to force the touch screen to enter standby mode.

Save Changes

Select **Save Changes** to save any changes made to the configuration settings.

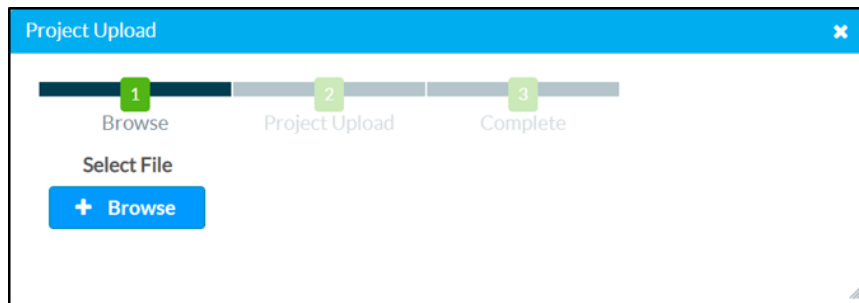
Revert

Select **Revert** to revert the touch screen back to the last saved configuration settings.

Upload Scheduling Project

Select **Upload Scheduling Project** to upload a custom scheduling project to the touch screen. A **Project Upload** dialog box opens.

Project Upload Dialog Box



To upload a custom scheduling project:

1. Select **Browse**, and then navigate to the project .vtz file on the host computer.
2. Select the project .vtz file, and then select **Open**.
3. Select **Load** to load the project .vtz file to the touch screen. The upload progress is shown in the dialog box.
4. Once the touch screen has completed the project upload, select **OK**.

Select the **x** button to close the **Project Upload** dialog box at any time during the upgrade process. Selecting the **x** button before the project file is uploaded to the touch screen cancels the upload.

Status

Select the **Status** tab on the top left of the configuration interface to display selections for viewing the status of device, network, and application settings.

Select a selection name to expand the selection. If the selection is expanded, select the selection name again to collapse the section.

Status Tab Selections

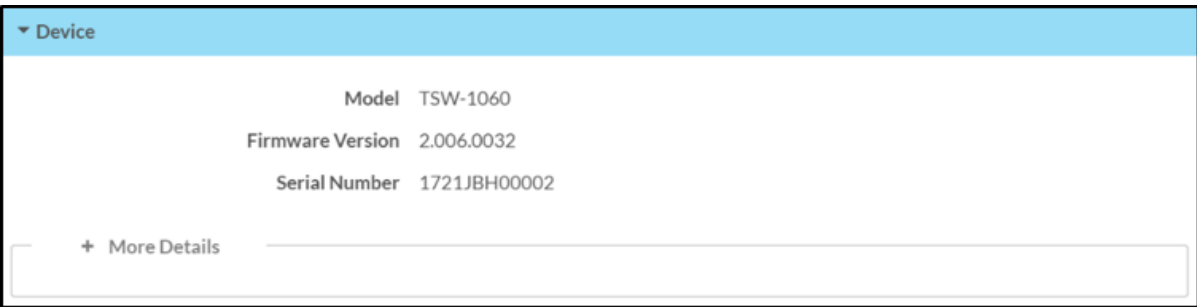


Each selection is described in the sections that follow

Device

Select **Device** to view general device information.

Status Tab - Device



The following **Device** information is displayed:

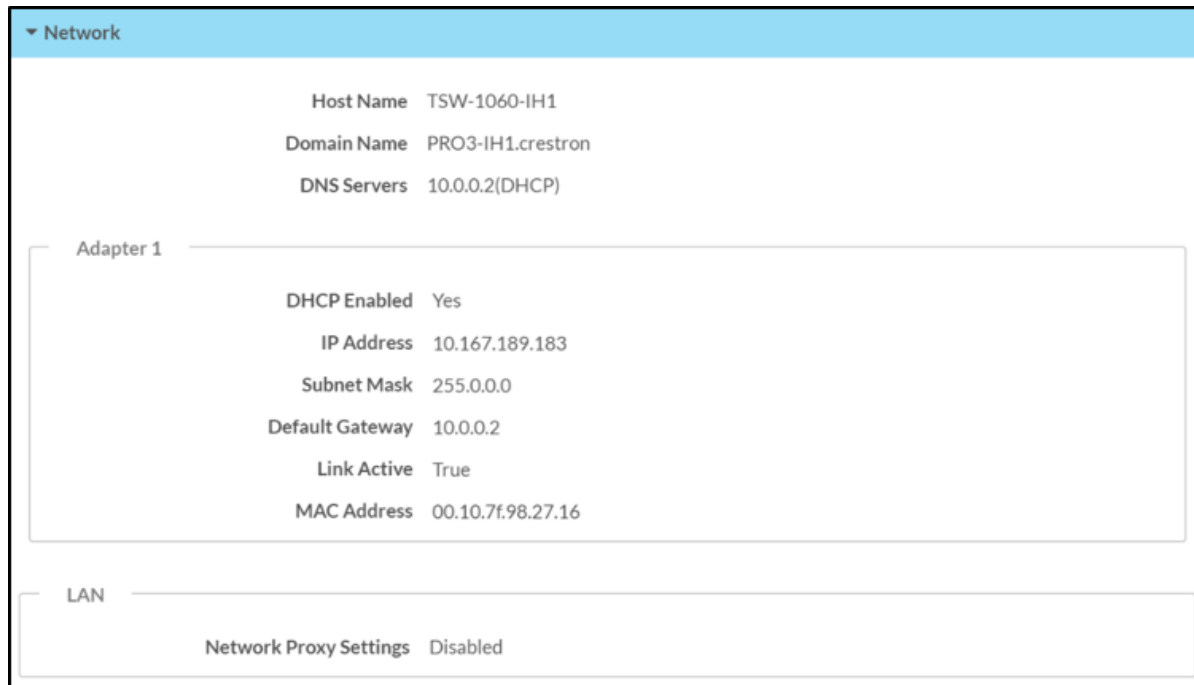
- **Model:** The touch screen model name
- **Firmware Version:** The firmware version loaded onto the touch screen
- **Serial Number:** The touch screen serial number

Select **+ More details** at the bottom of the **Device** tab to display an expanded section that shows additional touch screen information. If **+ More Details** is selected, select **- Less** details to collapse the section.

Network

Select **Network** to view the status of the network settings for the touch screen.

Status Tab - Network



The screenshot displays the Network status interface. At the top, a blue header bar contains a dropdown menu labeled 'Network'. Below this, the settings are organized into sections. The first section lists general network information: Host Name (TSW-1060-IH1), Domain Name (PRO3-IH1.crestron), and DNS Servers (10.0.0.2(DHCP)). The second section, titled 'Adapter 1', contains details for the primary network interface: DHCP Enabled (Yes), IP Address (10.167.189.183), Subnet Mask (255.0.0.0), Default Gateway (10.0.0.2), Link Active (True), and MAC Address (00.10.7f.98.27.16). The third section, titled 'LAN', shows Network Proxy Settings (Disabled).

| | |
|------------------------|-------------------|
| Host Name | TSW-1060-IH1 |
| Domain Name | PRO3-IH1.crestron |
| DNS Servers | 10.0.0.2(DHCP) |
| Adapter 1 | |
| DHCP Enabled | Yes |
| IP Address | 10.167.189.183 |
| Subnet Mask | 255.0.0.0 |
| Default Gateway | 10.0.0.2 |
| Link Active | True |
| MAC Address | 00.10.7f.98.27.16 |
| LAN | |
| Network Proxy Settings | Disabled |

The following **Network** information is displayed:

- **Host Name:** The touch screen host name
- **Domain Name:** The touch screen domain name
- **DNS Servers:** The DNS (domain name server) addresses used to resolve the touch screen domain to an IP address
- **DHCP Enabled:** Reports whether the IP address is static (Yes) or dynamic (No)
- **IP Address:** The touch screen IP address
- **Subnet Mask:** The touch screen subnet mask address
- **Default Gateway:** The gateway router address
- **Link Active:** Reports the status of the Ethernet connection (A true message indicates that the Ethernet connection is active, while a false message indicates that the Ethernet connection is inactive.)
- **MAC Address:** The unique touch screen MAC (media access control) address
- **Network Proxy Settings:** Reports whether network proxy settings are enabled or disabled for the touch screen

For more information on configuring network settings, refer to [System Setup on page 25](#).

USB

Select **USB** to view the status of a connected USB accessory, such as a room scheduling hallway sign or light bar.

Status Tab - USB

| ▼ USB | |
|---------------------|---------|
| Accessory Connected | Unknown |
| Accessory Type | Unknown |

The following **USB** information is displayed:

- **Accessory Connected:** The name of the connected accessory
- **Accessory Type:** The type of connected accessory

Room Scheduling

Select **Room Scheduling** to view the status of the room if using a room scheduling application.

Status Tab - Room Scheduling

| ▼ Room Scheduling | |
|----------------------|---------|
| Room Status | Unknown |
| Calendar Sync | Unknown |
| Fusion Online Status | Unknown |

The following **Room Scheduling** information is displayed:

- **Room Status:** The status of the connected room (available or reserved)
- **Calendar Sync:** The status of the sync between the touch screen and the room scheduling calendar
- **Crestron Fusion Online Status:** The status of the Crestron Fusion connection (if applicable)

Display

Select **Display** to view the display status.

Status Tab - Display

| ▼ Display | |
|----------------|----|
| Display Status | On |

The **Display Status** field indicates the display status (on, standby, or screensaver).

Schedule

Select **Schedule** to view the status of the connected scheduling calendar and the current meeting information.

Status Tab - Schedule

| | |
|---------------------------|---------------------------|
| ▼ Schedule | |
| Connection Status | Connected |
| Connection Status Message | Successfully connected |
| Occupancy Status | Vacant |
| Occupancy Source | Fusion |
| Push Registration Status | Not Supported |
| Current Meeting | |
| Meeting Info | |
| Scheduled | true |
| Subject | Walk up meeting |
| Start Time | 3:05 PM - October 2, 2019 |
| End Time | 3:35 PM - October 2, 2019 |
| Recurring | false |
| Organizer | Walk up organizer |
| Check In Status | Yes |
| Meeting Privacy Level | Public |

The following **Schedule** information is displayed:

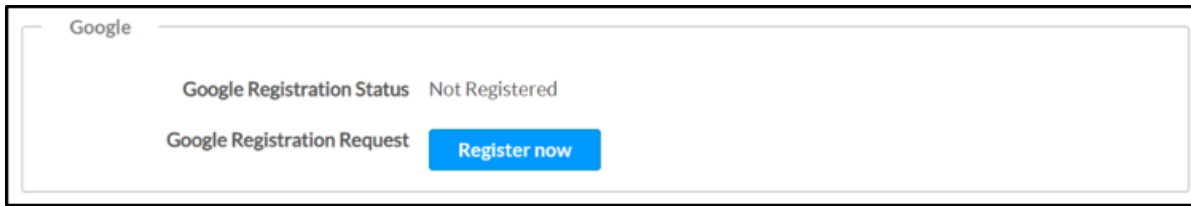
- **Connection Status:** Indicates the status of the scheduling calendar connection
- **Connection Status Message:** Displays any applicable information about the scheduling calendar connection status
- **Occupancy Status:** Indicates whether the connected room is occupied (if the room is equipped with an occupancy sensor)
- **Occupancy Source:** Displays occupancy sensor information for the connected room (if the room has occupancy-detecting equipment)
- **Push Registration Status:** The status of the scheduling calendar registration (if applicable)

The **Schedule** section also includes the following subsections.

Google

The **Google** subsection is used to register the touch screen with Google Calendar and to view the registration status of the Google Calendar account.

Status Tab - Schedule (Google)



Depending on the status of the Google Calendar registration, the following Google information may be displayed. For more information on connecting to a Google scheduling calendar, refer to [Connect to Google Calendar on page 10](#).

- **Google Registration Status:** Indicates the registration status between the touch screen and Google Calendar
- **Google Registration Request:** If the touch screen is not registered with Google Calendar, displays a **Register Now** button for requesting a connection to Google Calendar

NOTE: If the touch screen is registered with Google Calendar, an **Unregister** button is displayed instead. Select this button to unregister the touch screen with Google Calendar.

- **Google Registration URL:** If a Google Calendar registration has been requested, displays a URL used to register the touch screen with Google Calendar
- **Google Registration Code:** If a Google Calendar registration has been requested, displays a unique code used to register the touch screen with Google Calendar

Exchange

The **Exchange** subsection is used to register the touch screen with EWS via Modern Authentication and to view the registration status of the EWS account.

Status Tab - Schedule (Exchange)



Depending on the status of the EWS registration, the following registration information may be displayed. For more information on connecting to EWS via Modern Authentication, refer to [Appendix A: Configure Modern Authentication for EWS on page 75](#).

- **Exchange Registration Status:** Indicates the registration status between the touch screen and EWS
- **Exchange Registration Request:** If the touch screen is not registered with EWS, displays a **Register Now** button for requesting a connection to EWS

NOTE: If the touch screen is registered with EWS, an **Unregister** button is displayed instead. Select this button to unregister the touch screen with Google Calendar.

- **Exchange Registration Code:** If an EWS registration has been requested, displays a unique code used to register the touch screen with EWS

Current Meeting

The **Current Meeting** subsection is used to view details about an in-progress meeting. If no meeting is currently scheduled, no meeting details are displayed.

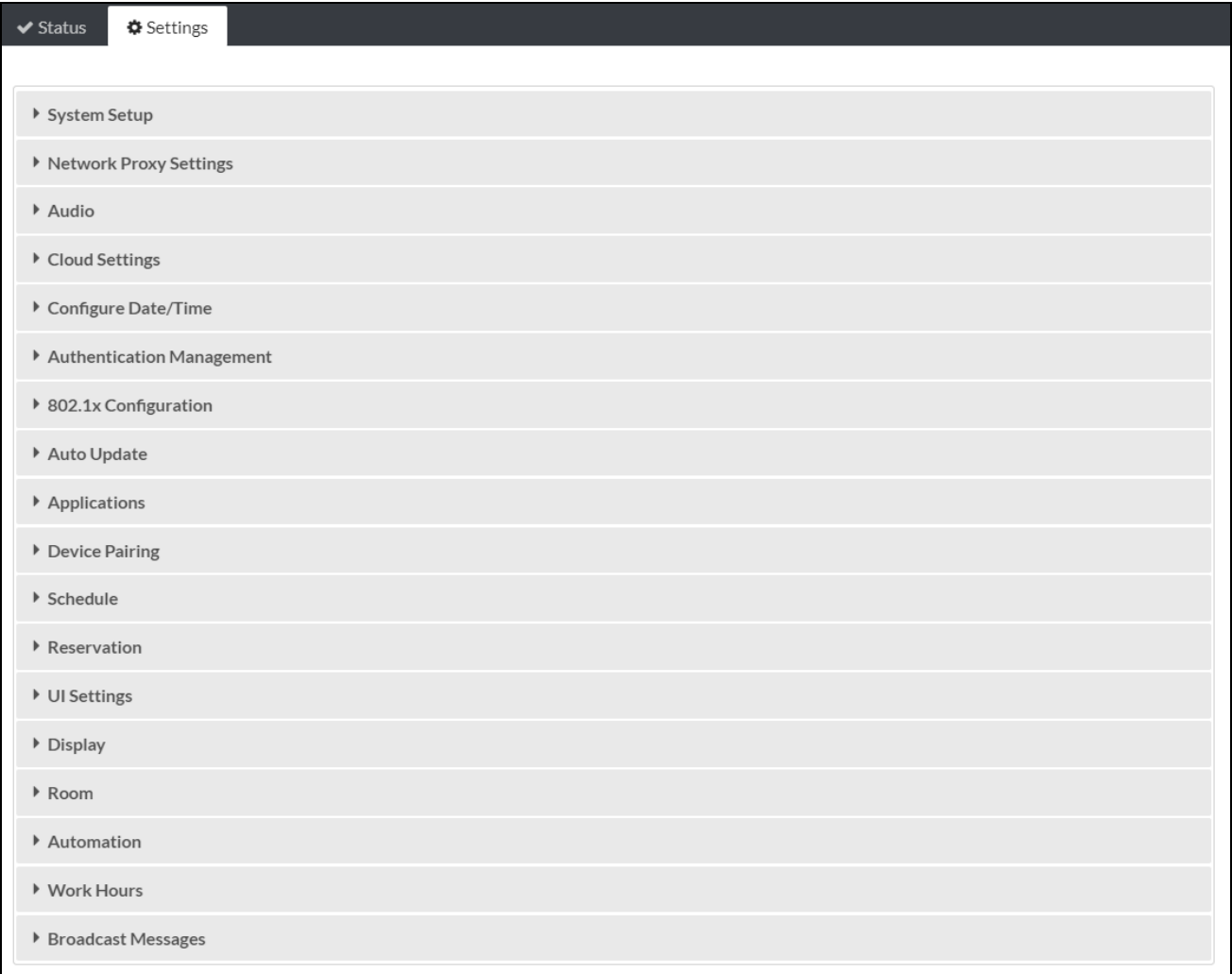
The following **Current Meeting** information is displayed:

- **Scheduled:** Indicates whether the connected room is currently reserved (A **true** message indicates that the room is reserved, while a **false** message indicates that the room is available.)
- **Subject:** The subject of the current reservation
- **Start Time:** The start time of the current reservation
- **End Time:** The scheduled end time of the current reservation
- **Recurring:** Indicates whether the current meeting is set to recur on the scheduling calendar (A **true** message indicates that the meeting is set to recur, while a **false** message indicates that the meeting is not set to recur.)
- **Organizer:** The name of the current reservation organizer (if this information is not set to private)
- **Check In Status:** Indicates whether the current reservation has been checked in (if required)
- **Meeting Privacy Level:** The privacy level of the current reservation

Settings

Select the **Settings** tab on the top left of the configuration interface to display selections for configuring various touch screen settings and to select a touch screen application.

Settings Selections



Each selection is described in the sections that follow.

System Setup

Select **System Settings** to configure general network and touch screen settings.

Settings Tab - System Setup

▼ System Setup

Network

Host Name

TSW-1060-IH1

Domain Name

PRO3-IH1.crestron

Primary Static DNS

Secondary Static DNS

Adapter 1

DHCP

Enabled

IP Address

10.167.189.183

Subnet Mask

255.0.0.0

Default Gateway

10.0.0.2

Device Display

LCD

Auto Brightness

Off

ALS Threshold Value

50

Brightness

100

Brightness High Preset

80

Brightness Medium Preset

40

Brightness Low Preset

10

LED

Enable LEDs

On

Custom LED Colors

On

'Available' Brightness

0% Red

100% Green

0% Blue

'Reserved' Brightness

100% Red

0% Green

0% Blue

(Continued on following page)

Settings Tab - System Setup (continued)

Hard Key

Backlight

Disabled

Backlight Brightness

80

Backlight Auto Brightness

Off

ALS Threshold Value

50

Backlight High Preset

80

Backlight Medium Preset

40

Backlight Low Preset

10

Wakes LCD

On

Screensaver and Standby

Standby Timeout

60

Enable Screensaver

Disabled

Enable 24 Hour Digital Clock

Disabled

Brightness

50

Local Setup Sequence

Enabled

Camera

Camera

Enabled

Fusion Cloud

Fusion Cloud Settings

Fusion Cloud

Enabled

Fusion Cloud URL

https://yourdomain.fusioncloud.com

Network

NOTE: The **IP Address**, **Subnet Mask**, and **Default Gateway** fields are required only if DHCP is turned off.

- **Host Name:** Enter the touch screen host name.
- **Domain Name:** Enter the fully qualified domain name on the network.
- **Primary Static DNS:** Enter the primary DNS address.
- **Secondary Static DNS:** Enter the secondary DNS address.
- **DHCP:** Turn on the toggle to use DHCP for the Ethernet connection.

NOTE: If DHCP is turned on, IP does not function until a reply has been received from the server. The touch screen broadcasts requests for an IP address periodically.

- **IP Address:** Enter the touch screen IP address on the network.
- **Subnet Mask:** Enter the touch screen subnet mask address on the network.
- **Default Gateway:** Enter the gateway router address on the network.

Device Display

- **LCD**
 - **Auto Brightness:** Turn on the toggle to use automatic brightness control for the touch screen LCD display.
 - **ALS Threshold Value:** If **Auto Brightness** is turned on, enter a value (1–100) for the ALS (ambient light sensor) threshold, which is used for switching between high and low autobrightness presets.
 - **Brightness:** If **Auto Brightness** is turned off, enter a value (1–100) for the LCD display brightness.
 - **Brightness High Preset:** Enter a value (1–100) for the LCD display high brightness preset.
 - **Brightness Medium Preset:** Enter a value (1–100) for the LCD display medium brightness preset.
 - **Brightness Low Preset:** Enter a value (1–100) for the LCD display low brightness preset.
- **LED**
 - **Enable LEDs:** Turn on the toggle to use LED lighting when using the touch screen with a room availability accessory (such as the TSW series light bar or the SSC/SSW/SIW series hallway signs).

If turned on, the LEDs on the room scheduling accessory light green to indicate that the room is available or red to indicate that the room is reserved. These default colors can be changed using the **Custom LED Colors** setting.
 - **Custom LED Colors:** Turn on the toggle to use custom LED color mixing for the available and reserved scheduling states.

- **'Available' Brightness:** If **Custom LED Colors** is turned on, use the **Red, Green, and Blue** sliders to create a custom LED color for the available scheduling state. Color values can be adjusted from 0–100% in 10% increments.
- **'Reserved' Brightness:** If **Custom LED Colors** is turned on, use the **Red, Green, and Blue** sliders to create a custom LED color for the reserved scheduling state. Color values can be adjusted from 0–100% in 10% increments.
- **Hard Key**
 - **Backlight:** Turn on the toggle to use the hard key backlight.
 - **Backlight Brightness:** If **Backlight** is turned on, enter a value (1–100) for the key backlight brightness.
 - **Backlight Auto Brightness:** If **Backlight** is turned on, turn on the toggle to use automatic brightness control for the key backlight.
 - **ALS Threshold Value:** If **Backlight** and **Backlight Auto Brightness** are both turned on, enter a value (1–100) for the backlight button ALS threshold, which is used for switching between high and low autobrightness presets.
 - **Backlight High Preset:** Enter a value (1–100) for the key backlight high brightness preset.
 - **Backlight Medium Preset:** Enter a value (1–100) for the key backlight medium brightness preset.
 - **Backlight Low Preset:** Enter a value (1–100) for the key backlight low brightness preset.
 - **Wakes LCD:** Turn on the toggle to wake the LCD display by tapping the hard keys on or off.
- **Screensaver and Standby**
 - **Standby Timeout:** Enter a standby timeout duration (1–120 seconds) for the touch screen.
 - **Enable Screensaver:** Turn on the toggle to display a screensaver on the touch screen during standby timeout.
 - **Enable 24 Hour Digital Clock:** Turn on the toggle to display a 24-hour digital clock on the touch screen during standby timeout.
 - **Brightness:** Enter a value (1–100) for the LCD display brightness during standby timeout.
 - **Local Setup Sequence:** Turn on the toggle to allow local access to the setup screens using the five-finger press or 1-2-3-4 button sequence.

Camera Settings

Turn on the **Camera** toggle to use the touch screen camera. This setting is not available for the TSW-x60-NC and TSW-560P models.

Crestron Fusion Cloud Settings

NOTE: If connecting to a Crestron Fusion® software on-premises server, connections are made using either traditional (outbound) or inbound communications. For more information, refer to the [Crestron Fusion 10 On-Premises Software Getting Started Guide](#).

- **Crestron Fusion Cloud:** Turn on the toggle to allow a connection to a Crestron Fusion Cloud server. This connection is only applicable when the scheduling mode is set to Crestron Default or User Project.

- **Crestron Fusion Cloud URL:** Enter the URL used to connect the touch screen to the desired Crestron Fusion Cloud server.

Network Proxy Settings

Select **Network Proxy Settings** to configure network proxy settings for the touch screen.

Settings Tab – Network Proxy Settings

▼ Network Proxy Settings

Proxy ☐ Disabled

HTTP Settings

HTTP Proxy ☐ Disabled

HTTP Proxy Address

HTTP Proxy Port

Username

Password

HTTPS Settings

HTTPS Proxy ☐ Disabled

HTTPS Proxy Address

HTTPS Proxy Port

Username

Password

- **Proxy:** Turn on the toggle to configure the touch screen for use with a proxy server.
- **HTTP Settings**
 - **HTTP Proxy:** Turn on the toggle to use an HTTP proxy server.
 - **HTTP Proxy Address:** Enter the IP address of the HTTP proxy server.
 - **HTTP Proxy Port:** Enter the port number of the HTTP proxy server.
 - **Username:** Enter the username required for the HTTP proxy server.
 - **Password:** Enter the password required for the HTTP proxy server.
- **HTTPS Settings**
 - **HTTPS Proxy:** Turn on the toggle to use an HTTPS proxy server.
 - **HTTPS Proxy Address:** Enter the IP address of the HTTPS proxy server.
 - **HTTPS Proxy Port:** Enter the port number of the HTTPS proxy server.
 - **Username:** Enter the username required for the HTTPS proxy server.
 - **Password:** Enter the password required for the HTTPS proxy server.

Audio

Select **Audio** to configure various audio settings for the touch screen.

Settings Tab – Audio Settings

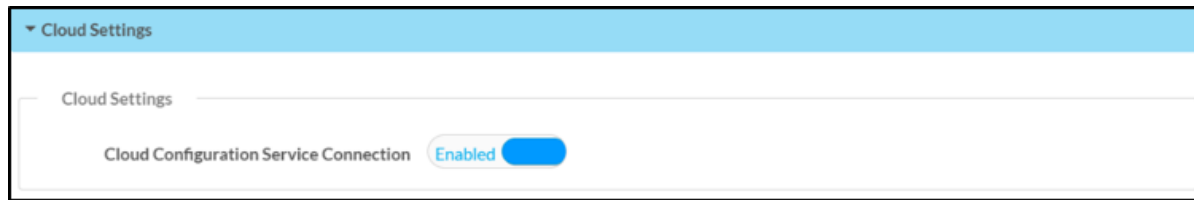
NOTE: The **Media Volume** setting adjusts the H.264 streaming media level in relation to the **Panel Volume** setting.

- **Panel Mute:** Turn on the toggle to mute the touch screen volume.
- **Panel Volume:** Enter a value (1–100) for the touch screen main volume level.
- **Media Mute:** Turn on the toggle to mute the touch screen media volume.
- **Media Volume:** Enter a value (1–100) for the touch screen media volume level.
- **Beep Enabled:** Turn on the toggle to mute the touch screen beep volume.
- **Beep Volume:** Enter a value (1–100) for the touch screen beep volume.

Cloud Settings

Select **Cloud Settings** to enable or disable a connection between the touch screen and an XiO Cloud® service account. A connection to the XiO Cloud service is enabled by default.

Settings Tab – Cloud Settings



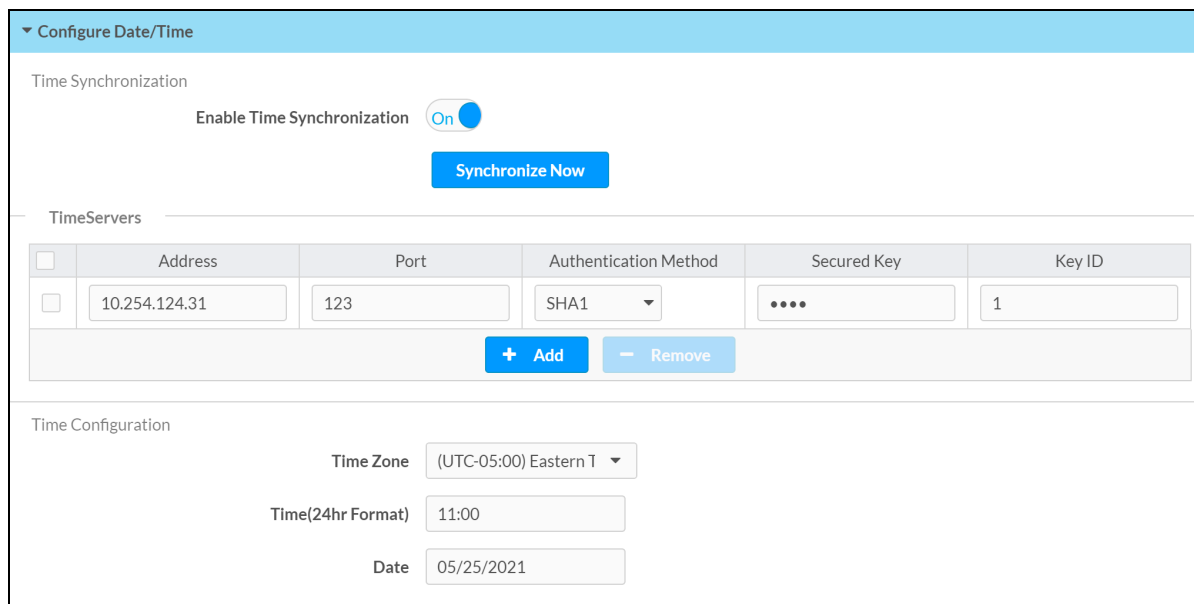
Turn on the **Cloud Configuration Service Connection** toggle to allow a connection between the touch screen and an XiO Cloud account. This setting is turned on by default.

For more information on connecting to the XiO Cloud service, refer to "Connect to XiO Cloud Service" in the [TSW-560, TSW-760, and TSW-1060 Supplemental Guide](#) or the [TSS-7 and TSS-10 Supplemental Guide](#).

Configure Date/Time

Select **Configure Date/Time** to configure date and time settings for the touch screen.

Settings Tab – Configure Date/Time



| | Address | Port | Authentication Method | Secured Key | Key ID |
|--------------------------|---------------|------|-----------------------|-------------|--------|
| <input type="checkbox"/> | 10.254.124.31 | 123 | SHA1 | | 1 |

- **Time Synchronization**

- **Enable Time Synchronization:** Turn on the toggle to use time synchronization via SNTP (Simple Network Time Protocol).
- **Synchronize Now:** With **Enable Time Synchronization** turned on, select **Synchronize Now** to synchronize the touch screen with the SNTP server(s) entered in the **TimeServers** table.

- **TimeServers:** With **Enable Time Synchronization** turned on, use the provided table to enter information regarding the SNTP server(s) used to synchronize the date and time for the touch screen.
 - Select **Add** to add a new SNTP server entry into the table.
 - Enter the following information for each entry:
 - Enter the SNTP server address into the **Address** text field.
 - Enter the SNTP server port into the **Port** text field.
 - Use the **Authentication Method** drop-down menu to select the authentication method used to access the SNTP server (if one exists).
 - If an authentication method is selected, enter the key used to authenticate against the SNTP server into the **Authentication Key** text field.
 - If an authentication method is selected, enter the ID for the key used to authenticate against the SNTP server into the **Key ID** text field.
 - To remove an entry, fill the checkbox to the left of the table entry, and then select **Delete**.
- **Time Configuration**
 - **Time Zone:** Select a time zone for the touch screen using the drop-down menu.
 - **Time(24hr Format):** Select the time for the touch screen (in 24-hour format) using the pop-up menu that is displayed.
 - **Date:** Select the date for the touch screen using the pop-up calendar that is displayed.

Authentication Management

Select **Authentication Management** to configure authentication management for touch screen users and groups and to set different access levels.

Settings Tab - Authentication Management

Turn on the **Enable Authentication** toggle to use authentication for the touch screen. Authentication is turned on by default.

When authentication is turned on, the web configuration interface prompts the user to enter a new administrator username and password. After restarting the touch screen, this username and password

must be entered to access the web configuration utility or to connect to the touch screen through Crestron Toolbox™ software.

CAUTION: Do not lose the administrator username and password, as the touch screen settings must be restored to factory defaults to reset the username and password.

Use the following **Authentication Management** settings to add, delete, and edit touch screen users and groups.

Current User

Select the **Current User** tab to view and edit information for the current touch screen user.

Authentication Management - Current User Tab

| Current User | Users | Groups |
|-----------------------|----------------|--------|
| Name | jsmith | |
| Access Level | Administrator | |
| Active Directory User | No | |
| Groups | Administrators | |

Change Current User Password

The following settings are displayed for the current user:

- **Name:** The chosen username
- **Access Level:** The access level granted to the user (Administrator, Programmer, Operator, User, or Connect)
- **Active Directory User:** Reports whether the current user is (**Yes**) or is not (**No**) authenticated through Active Directory® software

NOTE: A user must be added to an Active Directory group before the user may be selected as an active directory user. For more information, refer to [Groups on page 38](#).

- **Groups:** Any groups of which the current user is a member

Select **Change Current User Password** to change the password for the current user. The **Change Password** dialog box is displayed.

Change Password Dialog Box

Change Password

Password

Password field cannot be empty

Confirm Password

Confirm Password field cannot be empty

OK

Cancel

Enter a new password in the **Password** field, and then reenter the password in the **Confirm Password** field.

Select **OK** to save the new password, or select **Cancel** to cancel the change.

Users

Select the **Users** tab to view and edit information for the touch screen users.

Authentication Management - Users Tab

Current UserUsersGroups

Search Users

| Username | AD User | Actions |
|---------------|---------|--|
| connectaccess | No | <div><div></div><div></div><div></div></div> |
| jsmith | No | <div><div></div><div></div><div></div></div> |

1

10

Create User

Enter text in to the **Search Users** field to search for and display users that match the search term(s).

Touch screen users are listed in table format. The following information is displayed for each touch screen user:


- **Username:** The chosen username
- **AD User:** Reports whether the user is (**Yes**) or is not (**No**) authenticated through Active Directory

NOTE: A user must be added to an Active Directory group before the user may be selected as an active directory user. For more information, refer to [Groups on page 38](#).

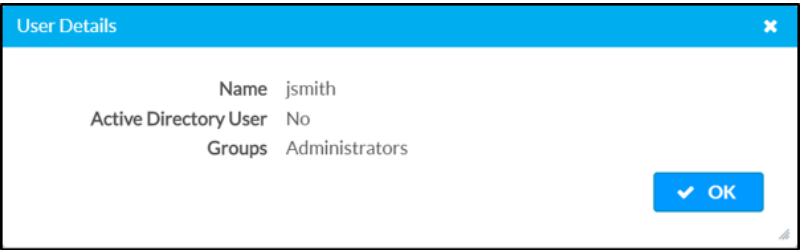
If the touch screen users span multiple pages, use the navigation arrows on the bottom of the page to move forward or backward through the pages, or select a page number to navigate to that page. Additionally, the number of users displayed on each page may be set to 5, 10, or 20 users.

An **Actions** column is also provided for each user that allows various actions to be performed. The following selections may be selected from the **Actions** column.

User Details

Select the information button  in the **Actions** column to view information for the selected user. The **User Details** pop-up dialog box is displayed.

User Details Dialog Box




The following settings are displayed for the current user:

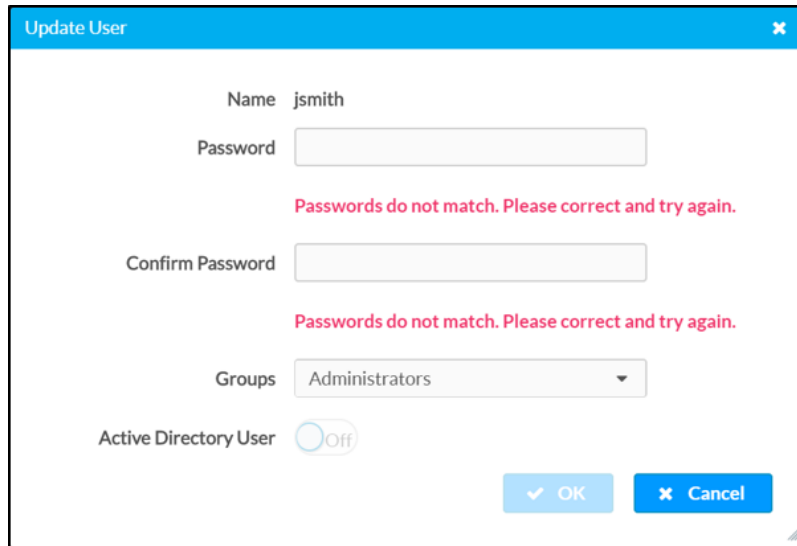
- **Name:** The chosen username
- **Active Directory User:** Reports whether the user is (**Yes**) or is not (**No**) authenticated through Active Directory
- **Groups:** Lists any groups that contain the user

Select **OK** to return to the **Authentication Management > Users** page.

Update User

Select the editing button  in the **Actions** column to edit settings for the selected user. The **Update User** dialog box is displayed.

Update User Dialog Box



The 'Update User' dialog box is shown with a blue header and a close button. It contains the following fields and controls:

- Name:** A text field containing 'jsmith'.
- Password:** A text field.
- Confirm Password:** A text field.
- Groups:** A dropdown menu with 'Administrators' selected.
- Active Directory User:** A toggle switch currently set to 'Off'.
- Buttons:** 'OK' (with a checkmark) and 'Cancel' (with an X).

Red error messages are displayed below the Password and Confirm Password fields: 'Passwords do not match. Please correct and try again.'

The following **Update User** settings may be viewed or configured:

- **Name:** The chosen username
- **Password:** Enter a new password for the selected user.
- **Confirm Password:** Reenter the password provided in the **Password** field.
- **Groups:** Add the user to one or more groups. For more information, refer to [Groups on page 38](#).
- **Active Directory User:** Turn on the toggle to use authentication via Active Directory for the selected user.

NOTE: A user must be added to an Active Directory group to be selected as an Active Directory user.

Select **OK** to save any changes and to return to the **Authentication Management > Users** page. Select **Cancel** to cancel any changes.

Delete User

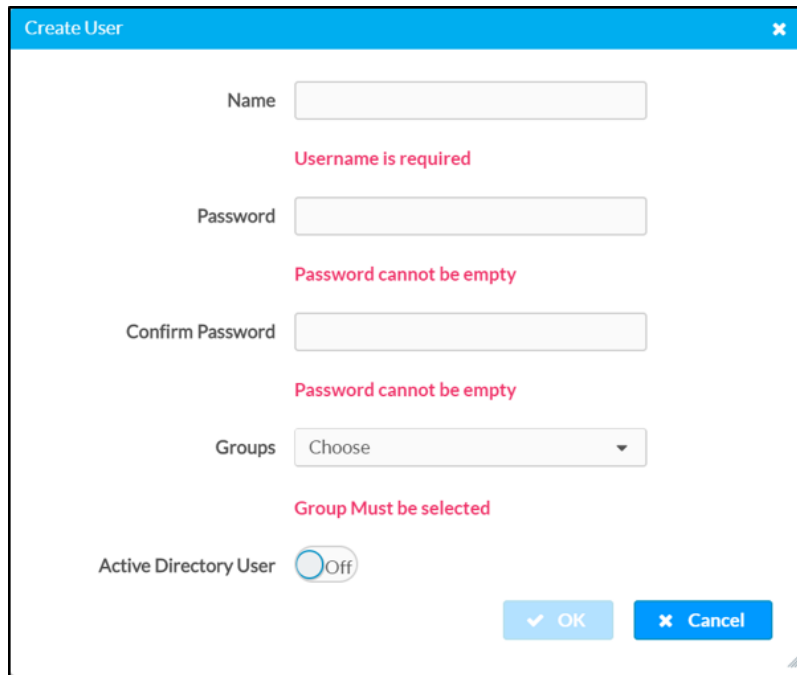
Select the trashcan icon  in the **Actions** column to delete the user.

A pop-up dialog box is displayed asking whether the user should be deleted. Select **Yes** to delete the user or **No** to cancel deleting the user.

Create User

Select **Create User** at the bottom of the page to create a new touch screen user. The **Create User** dialog box is displayed.

Create User Dialog Box

A screenshot of the 'Create User' dialog box. It has a blue header bar with the title 'Create User' and a close button (X). The form contains four input fields: 'Name' (with a red error message 'Username is required'), 'Password' (with a red error message 'Password cannot be empty'), 'Confirm Password' (with a red error message 'Password cannot be empty'), and 'Groups' (a dropdown menu with 'Choose' selected and a red error message 'Group Must be selected'). At the bottom left is a toggle switch for 'Active Directory User' which is currently 'Off'. At the bottom right are two buttons: 'OK' (light blue) and 'Cancel' (blue).

Use the following settings to create a new user:

- **Name:** Enter a username.
- **Password:** Enter a password for the user.
- **Confirm Password:** Reenter the password provided in the Password field.
- **Groups:** Add the user to one or more groups. For more information, refer to [Groups on page 38](#).
- **Active Directory User:** Turn on the toggle to use authentication via Active Directory for the user.

NOTE: A user must be added to an Active Directory group to be selected as an Active Directory user.

Select **OK** to save any changes and to return to the **Authentication Management > Users** page. Select **Cancel** to cancel creating a new user.

Groups

Select the **Groups** tab to view and edit settings for touch screen groups. Touch screen groups are used to group users by access level and Active Directory authentication settings.

Authentication Management - Groups Tab

Current UserUsersGroups

Search Groups

| Group Name | AD Group | Access Level | Actions |
|----------------|----------|---------------|-----------------------------------|
| Administrators | No | Administrator | <div><div></div><div></div></div> |
| Connects | No | Connect | <div><div></div><div></div></div> |
| Operators | No | Operator | <div><div></div><div></div></div> |
| Programmers | No | Programmer | <div><div></div><div></div></div> |
| Users | No | User | <div><div></div><div></div></div> |

1

10

Create Group

Enter text in to the **Search Groups** field to search for and display groups that match the search term(s).

Touch screen groups are listed in table format. The following information is displayed for each touch screen group:

- **Group Name:** The chosen group name
- **AD Group:** Reports whether the group is (**Yes**) or is not (**No**) authenticated through Active Directory


NOTE: Active Directory provides an additional layer of authentication for touch screen groups and users. Active directory group and user names are stored in the touch screen console along with a unique SID (security identifier). When an Active Directory user attempts to authenticate against the console, the console first checks the user credentials. If the Active Directory authentication is successful, Active Directory queries the console for the user or group's SID. The user is granted access to the touch screen only if at least one SID match is found.

- **Access Level:** The access level for the selected group (**Administrator, Programmer, Operator, User,** or **Connect**)

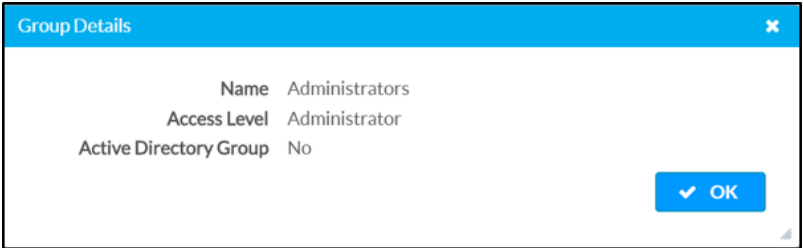
If the touch screen groups span multiple pages, use the navigation arrows on the bottom of the page to move forward or backward through the pages, or select a page number to navigate to that page. Additionally, the number of groups displayed on each page may be set to 5, 10, or 20 users.

An **Actions** column is also provided for each group that allows various actions to be performed. The following selections may be selected from the **Actions** column.

Group Details

Select the information button  in the **Actions** column to view information for the selected group. The **Group Details** dialog box is displayed.

Group Details Dialog Box



The Group Details dialog box displays the following information:

| | |
|------------------------|----------------|
| Name | Administrators |
| Access Level | Administrator |
| Active Directory Group | No |

At the bottom right, there is a blue button with a checkmark and the text "OK".

The following settings are displayed for the current group:

- **Name:** The chosen group name
- **Access Level:** The access level of the group and its users
- **Active Directory User:** Reports whether the group is (**Yes**) or is not (**No**) authenticated through Active Directory

Select **OK** to return to the **Authentication Management > Groups** page.

Delete Group

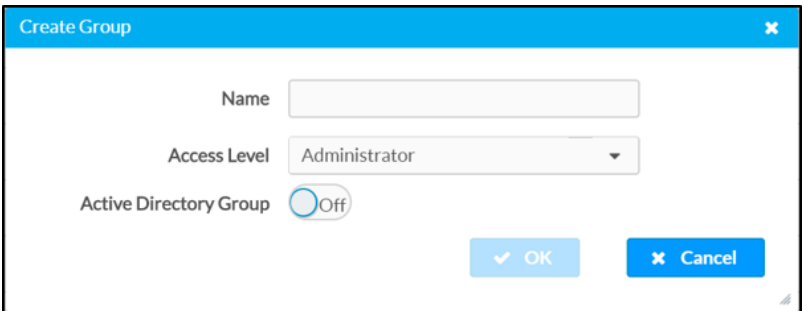
Select the trashcan icon  in the **Actions** column to delete the group.

A pop-up dialog box is displayed asking whether the group should be deleted. Select **Yes** to delete the group or **No** to cancel deleting the group.

Create Group

Select **Create Group** at the bottom of the page to create a new touch screen group. The **Create Group** dialog box is displayed.

Create Group Dialog Box



The Create Group dialog box contains the following fields:

- Name:** A text input field.
- Access Level:** A dropdown menu currently showing "Administrator".
- Active Directory Group:** A toggle switch currently set to "Off".

At the bottom, there are two buttons: a blue button with a checkmark and "OK", and a blue button with an 'X' and "Cancel".

Use the following settings to create a new group:

- **Name:** Enter a group name.

NOTE: If authenticating with Active Directory, do not enter the domain name for the Active Directory group in the **Name** field. If this information is being entered via console commands, omit `domain\local` from the command (for example, `adddomain -n:crestron -L:A` instead of `adddomain -n:domain.local\crestron -L:A`).

- **Access Level:** Select an access level for the group and its users from the drop-down menu.
- **Active Directory Group:** Turn on the toggle to use authentication via Active Directory for the group.

Select **OK** to save any changes and to return to the **Authentication Management > Groups** page. Select **Cancel** to cancel creating a new group.

802.1x Configuration

Select **802.1x Configuration** to configure IEEE 802.1X network authentication for touch screen security.

Settings Tab - 802.1x Configuration

▼ 802.1x Configuration

IEEE 802.1x Authentication **Enabled**

Authentication Method **EAP MSCHAP V2- pas**

Domain

Username

Username cannot be empty

Password

Password cannot be empty

Enable Authentication Server Validation **Disabled**

Select Trusted Certificate Authoritie(s)

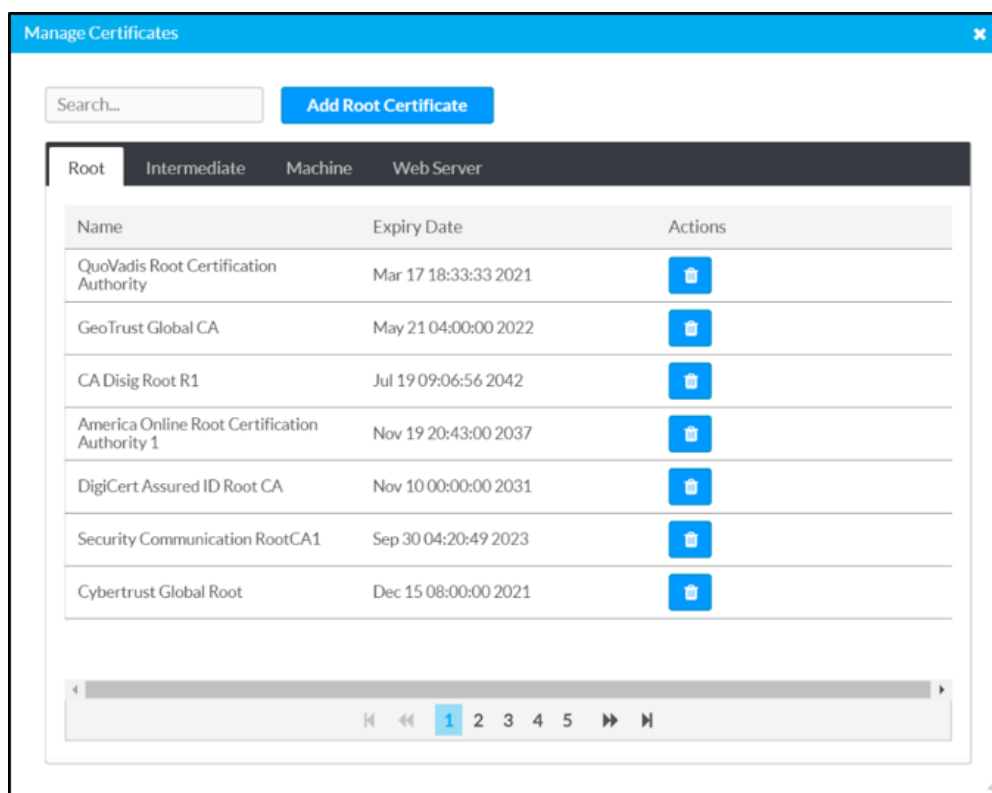
- ☐ Amazon Root CA 4
- ☐ Atos TrustedRoot 2011
- ☐ Autoridad de Certificacion Firmaprofesional CIF A62634068
- ☐ Baltimore CyberTrust Root
- ☐ Buypass Class 2 Root CA
- ☐ Buypass Class 3 Root CA
- ☐ CA Disig Root R2
- ☐ CFCA EV ROOT
- ☐ COMODO Certification Authority
- ☐ COMODO ECC Certification Authority
- ☐ COMODO RSA Certification Authority
- ☐ Certigna
- ☐ Certinomis - Root CA
- ☐ Certum Trusted Network CA 2
- ☐ Certum Trusted Network CA

- **IEEE 802.1x Authentication:** Turn on the toggle to use 802.1X authentication for the touch screen.
- **Authentication Method:** Select an 802.1X authentication method (**EAP-TLS Certificate** or **EAP MSCHAP V2- password**) from the drop-down menu.
- **Domain:** If **EAP MSCHAP V2- password** is selected for **Authentication Method**, enter a domain name that is required for authentication.
- **Username:** If **EAP MSCHAP V2- password** is selected for **Authentication Method**, enter a username that is required for authentication.
- **Password:** If **EAP MSCHAP V2- password** is selected for **Authentication Method**, enter a password that is required for authentication.

- **Enable Authentication Server Validation:** Turn on the toggle to use server validation for increased security.
- **Select Trusted Certificate Authorities:** Select trusted CAs (Certificate Authorities) from the provided CAs to be used for server validation:
 - Select the check box to the left of a CA to select it as a trusted CA.
 - Enter a search term into the text field at the top of the CA menu to search for and display CAs that match the search term.
 - Select the check box to the left of the search field at the top of the CA menu to select all CAs as trusted CAs.

Select **Manage Certificates** to add or remove CAs from the list. The **Manage Certificates** dialog box is displayed with the **Root** tab selected.

Manage Certificates Dialog Box - Root Tab




Select the tabs near the top of the page to switch between the different types of CAs (**Root**, **Intermediate**, **Machine**, or **Web Server**). The same settings are provided for each type of CA.

Type a search term into the **Search...** text field to search for and display CAs that match the search term.

The following information is provided for each type of CA:

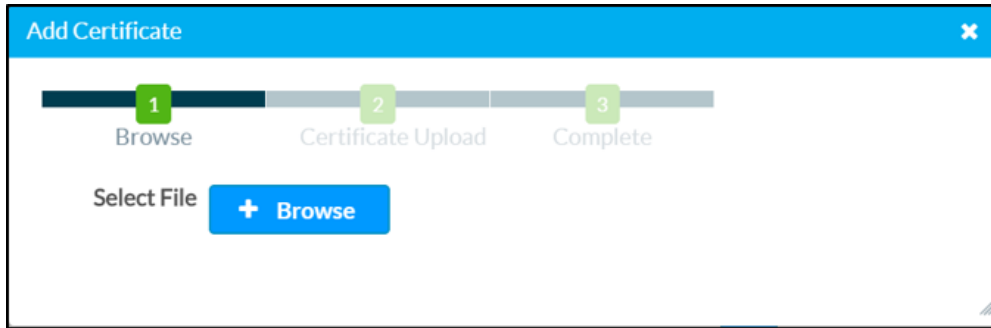
- **Name:** The CA name
- **Expiry Date:** The date and time that the CA is set to expire

If the CAs span multiple pages, use the navigation arrows on the bottom of the page to move forward or backward through the pages, or select a page number to navigate to that page.

Select the trashcan button  in the **Actions** column for a CA to delete it. A pop-up dialog box is displayed asking if the CA should be deleted. Select **Yes** to delete the certificate or **No** to cancel.

Select **Add [Type] Certificate** to add a CA of one of the four available types (**Root**, **Intermediate**, **Machine**, or **Web Server**) to the list of CAs. The **Add Certificate** pop-up dialog box is displayed.

Add Certificate Dialog Box



To add a new certificate:

1. Select **Browse**.
2. Navigate to the CA file on the host computer.
3. Select the CA file, and then select **Open**.
4. Select **Load** to load the CA file to the touch screen. The upload progress is shown in the dialog box.
5. Once the touch screen has completed the upload, select **OK**.

Select the **x** button to close the **Add Certificate** dialog box at any time during the upload process. Selecting the **x** button before the CA file is uploaded to the touch screen cancels the upload.

Select the **x** button to close the **Manage Certificates** dialog box and to return to the **802.1x Authentication** page.

Auto Update

Select **Auto Update** to configure automatic firmware updates for the touch screen.

NOTE: The **Auto Update** accordion can be used to configure auto update settings for firmware only. Automatic application updates are not affected by these settings.

Settings Tab - Auto Update

The screenshot shows the 'Auto Update' settings interface. At the top, there is a blue header bar with a dropdown arrow and the text 'Auto Update'. Below this, the 'Auto Update' toggle is set to 'Disabled'. The 'Custom URL Path' is a text input field containing 'https://crestrondevicefiles.blob.core.windows.'. Under the 'Schedule' section, 'Day of Week' is a dropdown menu set to 'Daily', 'Time of Day' is a text input field set to '02:36', and 'Poll Interval' is a text input field set to '0'. At the bottom, there is a blue button labeled 'Update Now'.

- **Auto Update:** Turn on the toggle to use automatic firmware updates.
- **Control URL Path:** Enter the URL path for the update server.
- **Day of Week:** Select the day of week when the touch screen will check for updates. Select **Daily** to have the touch screen check for updates every day.
- **Time of Day:** Enter a time of day (in 24-hour format) when the touch screen will check updates on the scheduled day.
- **Poll Interval:** Enter the polling interval (in hours) for when the touch screen will poll the server for updates.
- Select **Update Now** to check the update server for new firmware and to update the touch screen immediately if new firmware is available.

Applications

Select **Applications** to select an application to run on the touch screen.

Settings Tab - Applications

The screenshot shows the 'Applications' settings interface. At the top, there is a blue header bar with a dropdown arrow and the text 'Applications'. Below this, the 'Application Mode' is a dropdown menu set to 'User Project'. Underneath, there is a text input field containing 'User Project'. At the bottom, the 'Language' is a dropdown menu set to 'en-US'.

Use the **Application Mode** drop-down menu to select a touch screen application from the available selections.

Once a new application is selected, select **Save Changes** from the **Actions** menu. A pop-up dialog box is displayed stating that the touch screen must be restarted for the new application to take effect. Select **Yes** to restart the touch screen now or **No** to restart the touch screen later. The touch screen restarts with the new application running.

For more information on configuring the provided third party scheduling applications, refer to the [TSW-560, TSW-760, and TSW-1060 Supplemental Guide](#) or the [TSS-7 and TSS-10 Supplemental Guide](#).

Device Pairing

Select **Device Pairing** to configure settings for pairing the touch screen to a CEN-ODT-C-POE. The CEN-ODT-C-POE provides local occupancy reporting for supported room scheduling apps.

NOTE: For more information on the occupancy sensor, refer to the [CEN-ODT-C-POE Supplemental Guide](#). For more information on configuring the occupancy source in the scheduling application, refer to [Room on page 58](#).

Settings Tab - Device Pairing

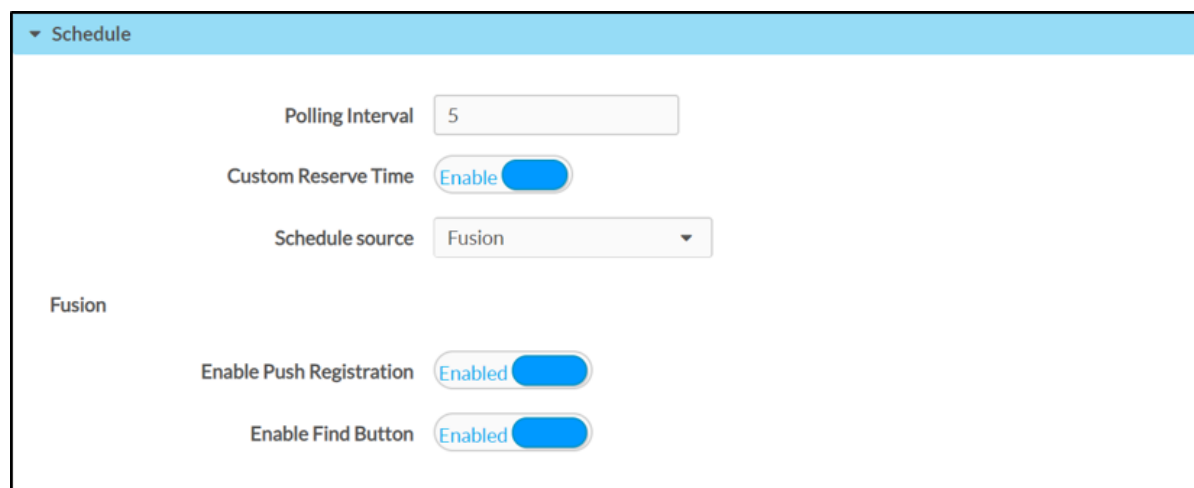
The screenshot shows the 'Device Pairing' settings tab. It features a light blue header with a dropdown arrow. Below the header, the 'Device Model' is set to 'POE Occ Sensor' in a dropdown menu. The 'Pairing Retry Time (Mins)' is set to '1' in a text input field. The 'Pairing Status' is 'Offline'. The 'Device IP Address/FQDN' field is empty, with a red error message 'Device IP Address/FQDN is invalid' to its right. Below this is a section titled 'Device Authentication' with a minus sign icon. Inside this section, there are two text input fields: 'Device Username' and 'Device Password'.

- **Device Model:** Use the drop-down menu to select **POE Occ Sensor**.
- **Pairing Retry Time (Mins):** Enter a duration (in minutes) that must elapse before the CEN-ODT-C-POE reattempts to pair to the touch screen.
- **Pairing Status:** Reports whether the CEN-ODT-C-POE is paired to the touch screen (**Online**) or not (**Offline**).
- **Device IP Address/FQDN:** Enter the IP address or fully qualified domain name of the CEN-ODT-C-POE. This is required for device pairing.
- **Device Authentication:** Enter authentication credentials for the CEN-ODT-C-POE (if required):
 - **Device Username:** Enter a valid username used to access the device.
 - **Device Password:** Enter a valid password used to access the device.

Schedule

Select **Schedule** to choose the scheduling calendar provider and to configure scheduling integration settings.

Settings Tab - Schedule



The screenshot shows a settings window titled "Schedule" with a light blue header. Inside, there are several configuration options: "Polling Interval" is a text input field containing the number "5"; "Custom Reserve Time" is a toggle switch labeled "Enable" which is turned on; "Schedule source" is a dropdown menu currently showing "Fusion"; and below a "Fusion" section header, there are two more toggle switches: "Enable Push Registration" and "Enable Find Button", both labeled "Enabled" and turned on.

- **Polling Interval:** Enter the interval (in minutes) that the scheduling application waits to poll the network for scheduling calendar data if changes are not pushed to the application.
- **Custom Reserve Time:** Turn on the toggle to allow the room to be reserved for a custom duration.

NOTE: If **Custom Reserve Time** is turned off, available reservation end times are limited to times that end on the next half hour, the next hour, or the next hour and a half.

- **Schedule source:** Select the scheduling calendar source from the drop-down menu that provides scheduling information to the application (Google Calendar, Crestron Fusion, Microsoft Exchange, Ad Astra, CollegeNet 25Live, or Demo Mode).

Depending on the scheduling calendar source that is selected for **Schedule source**, the following subsections are displayed.

Exchange

Select **Exchange** under **Schedule source** to display options for integrating a Microsoft Exchange account with the scheduling application.

For more information on connecting to a Microsoft Exchange account, refer to [Connect to Microsoft Exchange Using EWS on page 7](#).

Settings Tab - Schedule (Exchange EWS)

- Turn on the **Enable Modern Authentication** toggle to use Modern Authentication for the EWS (Exchange Web Services) account. For instructions on configuring Modern Authentication for use with the Crestron Room Scheduling application, refer to [Appendix A: Configure Modern Authentication for EWS on page 75](#).
- Enter the email address associated with the Microsoft Exchange scheduling calendar in the **Exchange Calendar Email Address** text field.
- Enter the username for the Microsoft Exchange account in the **Exchange Account Username** text field.

NOTE: The username must include the ".com" suffix similar to the email address entered in the **Exchange Calendar Email Address** text field.

- Enter the password for the Microsoft Exchange account in the **Exchange Account Password** text field.
- Enter the domain name associated with the Microsoft Exchange account in the **Exchange Domain** text field.

NOTE: The **Exchange Domain** text field must be left blank if using Office 365® software.

- Enter the Microsoft EWS (Exchange Web Services) server URL that the scheduling calendar uses to access Microsoft Exchange scheduling data in the **Exchange Web Services URL** text field.

O365

Select **O365** under **Schedule Source** to display options for integrating an Office 365 account with the scheduling application using Microsoft Graph.

For more information on connecting to a Microsoft Exchange account, refer to [Connect to Office 365 Using Microsoft Graph on page 9](#).

Settings Tab - Schedule (O365)

NOTE: The **Client ID (Application ID)**, **O365 Tenant ID**, and **Client Secret** values are generated within the Microsoft Entra portal for the Microsoft Entra app. For more information, refer to [Appendix B: Configure Microsoft Graph for Crestron Room Scheduling on page 90](#).

- Enter the email address associated with the Office 365 scheduling calendar in the **Exchange Calendar Email Address** text field.
- Enter the client (application) ID generated for the Microsoft Entra app in the **Client ID (Application ID)** text field.
- Enter the directory (tenant) ID generated for the Microsoft Entra app in the **O365 Tenant ID** text field.
- Enter the client secret generated for the Microsoft Entra app in the **Client Secret** text field.

Crestron Fusion

Select **Crestron Fusion** under **Schedule source** to display options for integrating a Crestron Fusion account with the scheduling application.

For more information on connecting to a Crestron Fusion account, refer to [Connect to Crestron Fusion on page 6](#).

Settings Tab - Schedule (Crestron Fusion)

The screenshot shows the 'Schedule' settings tab for Crestron Fusion. It includes a 'Polling Interval' set to 5, a 'Custom Reserve Time' toggle set to 'Enable', and a 'Schedule source' dropdown set to 'Fusion'. Below these, there are two more toggles: 'Enable Push Registration' and 'Enable Find Button', both set to 'Enabled'.

| Schedule | |
|--------------------------|---------|
| Polling Interval | 5 |
| Custom Reserve Time | Enable |
| Schedule source | Fusion |
| Fusion | |
| Enable Push Registration | Enabled |
| Enable Find Button | Enabled |

- Turn on the **Enable Push Registration** toggle to have Crestron Fusion push scheduling calendar data to the scheduling application. If **Enable Push Registration** is turned off, the scheduling application polls the network for scheduling calendar data.
- Turn on the **Enable Find Button** toggle to display a find button on the scheduling application so that a user may look up nearby rooms that are available for meetings.

Google

Select **Google** under **Schedule source** to display options for integrating a Google account with the scheduling application.

For more information on connecting to a Google account, refer to [Connect to Google Calendar on page 10](#).

Settings Tab - Schedule (Google)

The screenshot shows the 'Schedule' settings tab for Google. It includes a 'Polling Interval' set to 5, a 'Custom Reserve Time' toggle set to 'Enable', and a 'Schedule source' dropdown set to 'Google'. Below these, there is a 'Google Calendar' text input field.

| Schedule | |
|---------------------|--------|
| Polling Interval | 5 |
| Custom Reserve Time | Enable |
| Schedule source | Google |
| Google | |
| Google Calendar | |

Enter the calendar account name or ID in the **Google Calendar** text field if more than one calendar is available for the Google account. If this field is left empty, the scheduling application uses the primary calendar set for the account.

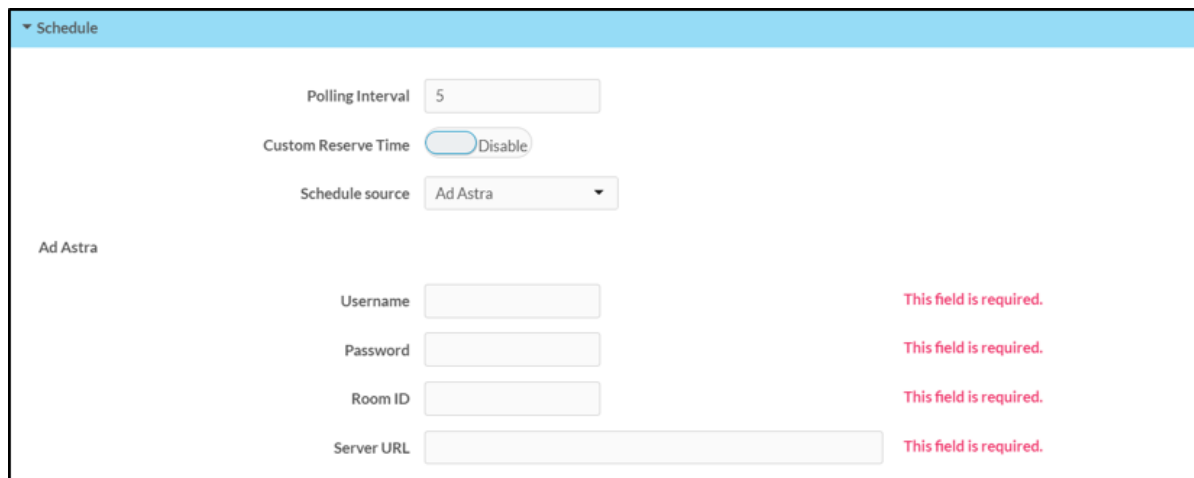
NOTE: To switch to a different calendar on the same Google account, enter the new calendar account name or ID in the **Google Calendar** text field.

Ad Astra

Select **Ad Astra** under **Schedule source** to display options for integrating an Ad Astra account with the scheduling application.

For more information on connecting to an Ad Astra account, refer to [Connect to Ad Astra on page 12](#).

Settings Tab - Schedule (Ad Astra)



The screenshot shows the 'Schedule' settings tab for Ad Astra. It includes a 'Polling Interval' set to 5, a 'Custom Reserve Time' toggle set to 'Disable', and a 'Schedule source' dropdown set to 'Ad Astra'. Below these are four required text fields: 'Username', 'Password', 'Room ID', and 'Server URL', each with a red error message 'This field is required.' to its right.

| Field | Value | Requirement |
|---------------------|----------|-------------------------|
| Polling Interval | 5 | |
| Custom Reserve Time | Disable | |
| Schedule source | Ad Astra | |
| Ad Astra | | |
| Username | | This field is required. |
| Password | | This field is required. |
| Room ID | | This field is required. |
| Server URL | | This field is required. |

- Enter the username for the Ad Astra account in the **Username** text field.
- Enter the password for the Ad Astra account in the **Password** text field.
- Enter the room ID associated with the Ad Astra scheduling calendar in the **Room ID** text field.
- Enter the URL of the Ad Astra scheduling calendar server in the **Server URL** text field.

CollegeNet 25Live

Select **25Live** under **Schedule source** to display options for integrating a CollegeNet 25Live account with the scheduling application.

For more information on connecting to a CollegeNet 25Live account, refer to [Connect to CollegeNet 25Live on page 12](#).

Settings Tab - Schedule (25Live)

▼ Schedule

Polling Interval 5

Custom Reserve Time ☐ Disable

Schedule source 25Live ▼

25Live

Username This field is required.

Password This field is required.

Space ID This field is required.

Server URL This field is required.

- Enter the username for the CollegeNet 25Live account in the **Username** text field.
- Enter the password for the CollegeNet 25Live account in the **Password** text field.
- Enter the space ID associated with the CollegeNet 25Live scheduling calendar in the **Space ID** text field.
- Enter the URL of the CollegeNet 25Live scheduling calendar server in the **Server URL** text field.

Demo Mode

Select **Demo Mode** under **Schedule source** to enable running demo mode on the scheduling application. When demo mode is turned on, the scheduling application cycles through demonstrations of various application features.

Settings Tab - Schedule (Demo Mode)

▼ Schedule

Polling Interval 5

Custom Reserve Time ☐ Disable

Schedule source Demo Mode ▼

Reservation

Select **Reservation** to configure the behavior of reservation functions for the scheduling application.

Settings Tab - Reservation

▼ Reservation

General

Max Reservation Length

120

Min Reservation Length

25

Reserve Now Even End Time

Disabled

Reservation Enable

Enabled

End Early

End Early

Minutes

Minutes Before End Early

3

Percent Before End Early

0

Extend Reservation

Extend Reservation

Minutes

Show Extend Meeting Minutes

25

Show Extend Meeting %

0

- **General**

- **Max Reservation Length:** Enter the maximum length (in minutes) of a meeting that may be reserved from the touch screen using the **Reserve Now** feature. This value must be between 30 and 480 minutes.
- **Min Reservation Length:** Enter the minimum length (in minutes) of a meeting that may be reserved from the touch screen using the **Reserve Now** feature. This value must be between 5 and 60 minutes in 5-minute increments.

- **Reserve Now Even End Time:** Turn on the toggle to allow meetings reserved from the touch screen to be set to end on even time intervals based on the value entered for **Min Reservation Length**.
 - If **Reserve Now Even End Time** is turned off and **Min Reservation Length** is set to "10", a meeting booked at 10:13 may be set to end at 10:23, 10:33, and so forth.
 - If **Reserve Now Even End Time** is turned on and **Min Reservation Length** is set to "10", a meeting booked at 10:13 may be set to end at 10:20, 10:30, and so forth.
 - These options are available provided that another meeting is not already booked during the next time period. If another meeting is booked, the last selectable end time will be the start time of the next meeting.
- **Reservation Enabled:** Turn on the toggle to allow meetings to be reserved from the touch screen using the **Reserve Now** feature.
- **End Early**
 - **End Early:** Use the drop-down menu to select whether an **End** button appears on the touch screen user interface that allows the meeting to be ended early.

NOTE: Select **Minutes** to have the **End** button appear on the touch screen after a specified number of minutes have elapsed. Select **Percentage** to have the **End** button appear on the touch screen after a specified percentage of the meeting has passed.
 - **Minutes Before End Early:** If **Minutes** is selected for **End Early**, enter the number of minutes that must elapse in a meeting before the **End** button appears on the touch screen.
 - **Percent Before End Early:** If **Percentage** is selected for **End Early**, enter the percentage of a meeting that must pass before the **End** button appears on the touch screen.
- **Extend Reservation**

NOTE: The extend reservation feature is available only if a meeting has not been booked directly after the current meeting.

 - **Extend Reservation:** Use the drop-down menu to select whether an **Extend** button appears on the touch screen user interface that allows the meeting to be extended.

NOTE: Select **Minutes** to have the **Extend** button appear on the touch screen after a specified number of minutes have elapsed. Select **Percentage** to have the **Extend** button appear on the touch screen after a specified percentage of the meeting has passed.
 - **Show Extend Meeting Minutes:** If **Minutes** is selected for **Extend Reservation**, enter the number of minutes that must elapse in a meeting before the **Extend** button appears on the touch screen.
 - **Show Extend Meeting %:** If **Percentage** is selected for **Extend Reservation**, enter the percentage of a meeting that must pass before the **Extend** button appears on the touch screen.

UI Settings

Select **Reservation** to configure various settings for the scheduling application UI (user interface).

Settings Tab - UI Settings

- **Minutes Before:** Enter the duration (in minutes) that the active screen remains on the display before a meeting begins, even if the idle timeout has elapsed.
- **Minutes After:** Enter the duration (in minutes) that the active screen remains on the display after a meeting begins, even if the idle timeout has elapsed.
- **Theme/Style Override URL:** Enter the URL of a custom CSS (Cascading Style Sheets) file to override the default application themes.

NOTE: For more information on programming a custom scheduling application CSS file, refer to the [Crestron Room Scheduling Panels Programming Guide](#).

- **Bidirectional Language Flow:** Use the drop-down menu to select the direction that scheduling application text displays on the scheduling application. Select **Default** to use the default direction for the chosen primary language.
- **Work Hours Idle Timeout:** Enter the duration (in minutes) that the touch screen must remain idle before the scheduling application enters the idle screen during work hours.
- **Screen Layout:** Use the drop-down menu to select the direction of the scheduling application layout and timeline (**Horizontal** or **Vertical**).

NOTES:

- Horizontal right-to-left layout and horizontal left-to-right layout is determined by the chosen primary language.
 - The TSW-560P only supports the **Vertical** layout.
- **Project Theme:** Use the drop-down menu to select the application theme from the available options (**Light** or **Dark**).
 - **Logo Image:** Enter the URL of a custom logo image to replace the default scheduling application logo image on the touch screen. Supported file types for the custom logo are PNG, JPG, and SVG.
 - **Occupied/Unscheduled Status:** Turn on the toggle to have the scheduling app report when occupancy is detected in the room when no meeting is scheduled. The room must contain occupancy-sensing equipment to use this feature.
 - **Enable Reserved Color for Check-in:** Turn on the toggle to have the scheduling app show as reserved during the specified check-in period. For more information on the check-in functionality, refer to [Automation on page 59](#).
 - **Disable Idle Screen:** Turn on the toggle to prevent the idle screen from displaying after the specified idle timeout duration elapses.

Display

Select **Display** to customize the background of the scheduling application with supported image or video files.

Settings Tab - Display

▼ Display

Backgrounds

Active Screen When Reserved

Reserved/Active Background URL Enabled ☐ Disabled

Reserved/Active Background URL

Reserved/Active Background Media Type

Reserved/Active Background Media Sub Type

Idle Screen When Reserved

Reserved/Idle Background URL Enabled ☐ Disabled

Reserved/Idle Background URL

Reserved/Idle Background Media Type

Reserved/Idle Background Media Sub Type

Active Screen When Available

Available/Active Background URL Enabled ☐ Disabled

Available/Active Background URL

Available/Active Background Media Type

Available/Active Background Media Sub Type

Idle Screen When Available

Available/Idle Background URL Enabled ☐ Disabled

Available/Idle Background URL

Available/Idle Background Media Type

Available/Idle Background Media Sub Type

(Continued on following page)

Settings Tab - Display (continued)

Active Screen When Available and Occupied

Available/Active Background URL Enabled ☐ Disabled

Available/Active Background URL

Available/Active Background Media Type

Available/Active Media Sub Type

Idle Screen When Available and Occupied

Available/Idle Background URL Enabled ☐ Disabled

Available/Idle Background URL

Available/Idle Media Type

Available/Idle Media Sub Type

Background media may be set for various application states, including **Active Screen When Reserved**, **Idle Screen When Reserved**, **Active Screen When Available**, **Idle Screen When Available**, **Active Screen When Available and Occupied**, and **Idle Screen When Available and Occupied**.

The settings below may be configured for each application state:

- **Background URL Enabled:** Turn on the toggle to use background media for the chosen application state.
- **Background URL:** If **Background URL Enabled** is turned on, enter the URL of the background media file for the chosen application state.
- **Background Media Type:** If **Background URL Enabled** is turned on, use the drop-down menu to set the media type of background media file (image or video) for the chosen application state.
- **Background Media Sub Type:** If **Background URL Enabled** is turned on, select the media subtype of the background media file for the chosen application state.

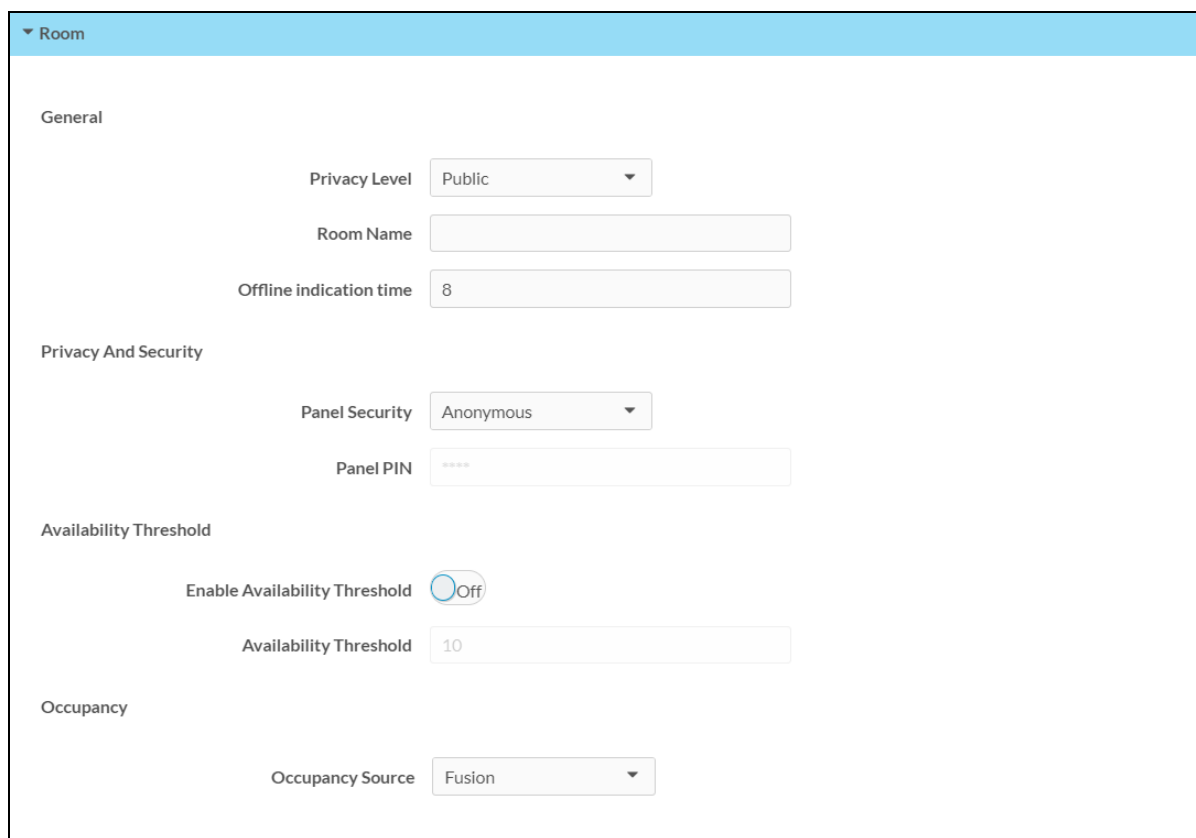
NOTES:

- Supported image file types are JPEG, GIF, and PNG. For optimal image quality, images should be sized to 960 x 540 pixels for a TSW-560, 540 x 960 pixels for a TSW-560P, 1024 x 600 pixels for a TSW-760/TSS-7 and 1280 x 800 pixels for a TSW-1060/TSS-10.
- The supported video file type is WEBM (compressed with a VP8 codec). The first and last seconds of the video should display the same still image to avoid flickering on the loop playback.

Room

Select **Room** to configure display and functionality settings for the room connected to the scheduling application.

Settings Tab - Room



▼ Room

General

Privacy Level

Room Name

Offline indication time

Privacy And Security

Panel Security

Panel PIN

Availability Threshold

Enable Availability Threshold ☐

Availability Threshold

Occupancy

Occupancy Source

- **General**

- **Privacy Level:** Use the drop-down menu to select the privacy level used by scheduling application for the room.

NOTE: The selections for **Privacy Level** control how much information is displayed about each meeting on the scheduling application. Select **Public** to show the meeting subject, organizer, and attendees. Select **Semi-Private** to show the meeting organizer but not the subject or attendees. Select **Private** to not show any meeting information except for whether the room is free or reserved.

- **Room Name:** Enter a custom room name that overwrites the calendar name.
- **Offline indication time:** Enter the duration (in hours) that the connected scheduling calendar must be offline before the scheduling application displays an offline notification.

- **Privacy And Security**

- **Panel Security:** Use the drop-down menu to select the security level used by the scheduling application for the room.

NOTE: If **Anonymous** is selected, a user may access scheduling application functions from the touch screen without entering a PIN. If **Touch Screen PIN** is selected, a user must first enter a PIN before accessing scheduling application functions.

- **Panel PIN:** If **Touch Screen PIN** is selected for **Panel Security**, enter a four-digit PIN that must be entered to gain access to scheduling application functions.
- **Availability Threshold**
 - **Enable Availability Threshold:** Turn on the toggle to use availability threshold behavior for the room.
 - **Availability Threshold:** Enter the duration (in minutes) that a meeting cannot be booked from the touch screen before a scheduled meeting begins.
- **Occupancy**
 - **Occupancy Source:** Use the drop-down menu to select whether occupancy is reported to the scheduling application via Crestron Fusion or via a local CEN-ODT-C-POE occupancy sensor (if the room includes occupancy-detecting equipment).

NOTES:

- A CEN-ODT-C-POE must be paired to the touch screen prior to selecting **Local** occupancy. For more information, refer to [Device Pairing on page 45](#).
- **Local** occupancy is supported by Crestron Fusion, Microsoft Exchange, and Google scheduling calendars at this time.

Automation

Select **Automation** to configure the behavior of automated settings for the scheduling application.

Settings Tab - Automation

The screenshot shows the 'Automation' settings tab. It is divided into two main sections: 'Decline for No Show' and 'Check-in'. In the 'Decline for No Show' section, there is a toggle for 'Decline for No Show' which is currently 'Disabled'. Below this are input fields for 'Decline reservations up to (min)' set to 120, 'Expiration Time (min)' set to 15, and a radio button for 'Decline at Exact Minute' set to 'No'. The 'Check-in' section has a toggle for 'Require Check-In' which is also 'Disabled'. Below this are input fields for 'Check-In Time' set to 5 and 'Check-In End' set to 5.

| Section | Setting | Value |
|---------------------|----------------------------------|----------|
| Decline for No Show | Decline for No Show | Disabled |
| | Decline reservations up to (min) | 120 |
| | Expiration Time (min) | 15 |
| | Decline at Exact Minute | No |
| Check-in | Require Check-In | Disabled |
| | Check-In Time | 5 |
| | Check-In End | 5 |

- **Decline for No Show**

- **Decline for No Show:** Turn on the toggle to decline meetings automatically in the event of a no show.

NOTE: When **Decline for No Show** is turned on, a user must tap a check-in button on the touch screen or occupancy must be detected in the room during the specified check-in period, otherwise the meeting is removed from the scheduling calendar. For recurring meetings, if a no show event is detected for the third consecutive time, the room will be freed from the recurrence.

- **Decline reservations up to (min):** If **Decline for No Show** is turned on, enter the maximum meeting duration (in minutes) that is affected by the **Decline for No Show** feature. All meetings that are longer than the set duration are not affected by this feature.
- **Expiration time (min):** If **Decline for No Show** is turned on, enter a duration (in minutes) that must elapse without any occupancy being detected before a meeting is declined.

- **Decline at Exact Minute:** If **Decline for No Show** is turned on, turn on the toggle to have the room check for occupancy at the exact time the duration set for **Expiration time (min)** elapses.

For example, if **Expiration time (min)** is set to 10 minutes and a meeting is scheduled to start at 10:00AM, the room will check for occupancy at 10:10AM and will decline the meeting if no occupancy is detected at this time. This helps to prevent a false positive if occupancy is detected prior to the expiration timeout.

- **Check-in**

- **Require Check-In:** Turn on the toggle to require an attendee to check in to the meeting from the touch screen during a specified period.
- **Check-In Time:** Enter the duration (in minutes) that a **Check In** button is available on the touch screen before a meeting begins.

NOTE: If the **Check In** button from the prior meeting is still active and has not been pressed, the **Check In** button from the next meeting does not appear until the previous button expires.

- **Check-In End:** Enter the duration (in minutes) that a **Check In** button is available on the touch screen after a meeting begins.

NOTE: If the length of a meeting is shorter than the set **Check-In End** value, the **Check-In End** time is limited to the length of the meeting.

Work Hours

Select **Work Hours** to configure the auto-on settings for the connected touch screen, which are triggered and controlled by a time range.

Settings Tab - Work Hours

▼ Work Hours

| Enable | Day | On Time | Off Time |
|---------------------|-----------|------------------|------------------|
| <div>Enabled</div> | Monday | <div>08:00</div> | <div>18:00</div> |
| <div>Enabled</div> | Tuesday | <div>08:00</div> | <div>18:00</div> |
| <div>Enabled</div> | Wednesday | <div>08:00</div> | <div>18:00</div> |
| <div>Enabled</div> | Thursday | <div>08:00</div> | <div>18:00</div> |
| <div>Enabled</div> | Friday | <div>08:00</div> | <div>18:00</div> |
| <div>Disabled</div> | Saturday | <div>08:00</div> | <div>18:00</div> |
| <div>Disabled</div> | Sunday | <div>08:00</div> | <div>18:00</div> |

During the set date and time range, the touch screen display remains on regardless of whether meetings are scheduled.

NOTE: All other standby configuration options are disabled when the touch screen is in scheduling mode. The options set through the **Work Hours** selection always dictate when the connected display turns on or off.

The following settings may be configured for each day of the week listed in the adjacent **Day** column:

- **Enable:** Turn on the toggle to use auto-on controls for the chosen day of the week.
- **On Time:** Enter the time (in 24-hour format) that the connected touch screen display is turned on automatically for the chosen day of the week.
- **Off Time:** Enter the time (in 24-hour format) that the connected touch screen display is turned off automatically for the chosen day of the week.

Broadcast Messages

Select **Broadcast Messages** to configure broadcast message behavior on the scheduling application.

Settings Tab - Broadcast Messages

▼ Broadcast Messages

Broadcast Enable

Enabled ☒

Broadcast Timeout

Broadcast Enable: Turn on the toggle to show broadcast messages on the scheduling application.

Broadcast Timeout: Enter the duration (in minutes) that a broadcast message is displayed before timing out. Enter "0" for no timeout.

Crestron Fusion Configuration

Once the scheduling application is connected to Crestron Fusion, scheduling application settings may be configured through Crestron Fusion by using custom properties.

Custom properties expand the functionality of the scheduling application, such as passing properties for the touch screen to display and announcing an emergency alert generated by Crestron Fusion. Custom properties provide information that is important to the user and that can be included in the description of the room. Custom properties that communicate settings to the device are defined for each room and are set through the Crestron Fusion Setup web client.

NOTE: Custom properties set in Crestron Fusion have precedence over settings configured using the web browser interface.

For more information on setting up rooms and adding devices to rooms in Crestron Fusion Cloud, refer to the [Getting Started Guide for Adding Devices to Crestron Fusion Software](#).

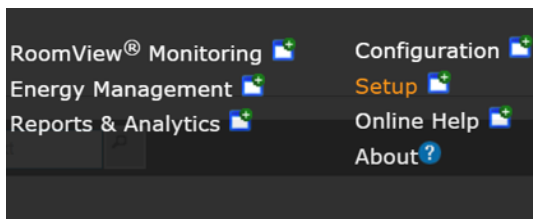
Add Custom Properties to a Room

Before attempting the procedure below, ensure that the scheduling application has been selected on the touch screen and that a connection to Crestron Fusion has been established. The touch screen must also have already been added to the appropriate room in the Crestron Fusion server.

To add custom properties to a room in Crestron Fusion:

1. Log in to the Crestron Fusion server.
2. Select **Open > Setup** from the Crestron Fusion header.

Crestron Fusion Page - Header



3. Select the **Objects** tab on the bottom of the **Rooms** tree on the left side of the page.

Crestron Fusion Page - Objects Tab



4. Select **Custom Properties > Rooms** from the **Objects** tree, and then select **Add**.
5. Enter the following information for each custom property that is being added:
 - **ID:** Enter the ID of the custom property exactly as it appears in this document.
 - **Name:** Enter any descriptive name for the property.

- **Type:** Enter the custom property type (integer, string, Boolean, and so forth).
- **Searchable:** Check this box to make the custom property searchable (optional).

Add - Custom Property (Room) Dialog Box

6. Select **Save & Close** to save any changes. Select **Close** to cancel the addition.

Set Custom Properties for the Scheduling Application

After adding custom properties to the room as described in [Add Custom Properties to a Room on page 64](#), use the **Custom Property** tab to configure the custom properties for the scheduling application.

To set custom properties for the scheduling application in Crestron Fusion:

1. Navigate to the **Rooms** tree as described in the first three steps of the [Add Custom Properties to a Room on page 64](#).
2. Select the **Rooms** tab if it is not already selected.
3. Select the **+** (plus) sign next to the root directory to expand the directory tree.
4. Double-click on the desired room to open the **Edit - Room** dialog box.
5. Select the **Custom Properties** tab to view the available custom properties for that room.
6. To enable a custom property, either add a valid value to the appropriate text box or check the appropriate check box.
7. Select **Save & Close** to apply the selected properties. Select **Close** to cancel any changes.

Scheduling Application Custom Properties

The following tables list the Crestron Fusion custom properties that may be configured for the scheduling application. These custom properties correlate with the settings that are configurable via the web configuration interface.

For a complete list of custom properties for the scheduling application in the order that they appear in Crestron Fusion, refer to [All Scheduling Application Custom Properties on page 73](#).

Work Hours Settings

Custom Properties - Work Hours Settings

| Custom Property | Types and Supported Value(s) | Description | Default Value | Notes |
|--------------------------------------|--|---|--|---|
| WorkHoursEn[Mon-Sun] ¹ | Boolean TRUE = enabled, FALSE = disabled | Sets the days of the week that the display's auto-on settings are in effect | enabled [Mon-Fri], disabled [Sat-Sun] | Disabling a day turns the display off for that entire day |
| WorkHoursStart[Mon-Sun] ¹ | String [00:00-23:59] | Sets when the display turns on automatically for a given day (in 24-hour format) | 08:00 | Time must be earlier than the WorkHoursStop time |
| WorkHoursStop[Mon-Sun] ¹ | String [00:00-23:59] | Sets when the display turns off automatically for a given day (in 24-hour format) | 18:00 | Time must be later than the WorkHoursStop time |

¹ The table below correlates the abbreviation following each of the above properties with a day of the week.

| Abbreviation | Day of Week |
|--------------|-------------|
| Mon | Monday |
| Tue | Tuesday |
| Wed | Wednesday |
| Thu | Thursday |
| Fri | Friday |
| Sat | Saturday |
| Sun | Sunday |

Display Settings

Custom Properties - Display Settings

| Custom Property | Types and Supported Value(s) | Description | Default Value | Notes |
|---------------------|---|---|---------------|-------|
| BackgroundAvailable | String [URL of background source file] | Sets the background source file URL for the available screens | empty | |
| BackgroundReserved | String [URL of background source file] | Sets the background source file URL for the reserved screens | empty | |

Broadcast Message Settings

Custom Properties - Broadcast Message Settings

| Custom Property | Types and Supported Value(s) | Description | Default Value | Notes |
|------------------------|--|--|---------------|---|
| BroadcastEmgTimeOut | Integer [0–90 minutes] | Sets the number of minutes before an emergency broadcast times out | 90 | BroadcastTimeOutEnable must be enabled; 0 = no timeout |
| BroadcastTimeOutEnable | Boolean TRUE = enabled, FALSE = disabled | Sets whether a timeout for broadcast messages is enabled or disabled | TRUE | Time must be earlier than the WorkHoursStop time |
| EnBroadcastMessage | Boolean TRUE = enabled, FALSE = disabled | Sets whether the scheduling application shows broadcast messages | TRUE | |

UI Settings

Custom Properties - UI Settings

| Custom Property | Types and Supported Value(s) | Description | Default Value | Notes |
|----------------------------|--|--|---------------|--|
| DisableIdleScreen | Boolean TRUE = enabled, FALSE = disabled | Sets whether the idle screen will be displayed after the specified idle timeout duration elapses. | FALSE | |
| ForceActiveAfterResStart | Integer [0–15 minutes] | Sets the time that the active screen remains on the display after a meeting begins (even if the idle timeout has elapsed) | 5 | 0 = disable this behavior |
| ForceActiveBeforeResStart | Integer [0–15 minutes] | Sets the time that the active screen remains on the display before a meeting begins (even if the idle timeout has elapsed) | 5 | 0 = disable this behavior |
| IdleTimeout | Integer [1–20 minutes] | Sets the time that the application must be idle before displaying the idle screen | 5 | |
| LEDReservedColorForCheckIn | Boolean TRUE = enabled, FALSE = disabled | Sets whether the scheduling app will show as reserved during the specified check-in period. | FALSE | ForceOrgCheckIn must be enabled |
| ProjectIconUrl | String [URL of custom application icon] | Provides a URL reference to a custom application icon graphic file to replace the default application icon | empty | Supported graphic file types are PNG, JPG, and SVG |
| ProjectLayout | String [Horizontal, Vertical] | Sets the layout orientation for the application | Horizontal | |
| ProjectTheme | String [Light, Dark] | Sets the look and feel of the application theme | Dark | |

Automation Settings

Custom Properties - Automation Settings

| Custom Property | Types and Supported Value(s) | Description | Default Value | Notes |
|----------------------------|--|--|---------------|---|
| DeclineForNoShowAppliesDur | Integer [30–480 minutes] | If EnDeclineForNoShow is enabled, limits this feature to reservations up to and including the set number of minutes | 120 | |
| EnDeclineForNoShow | Boolean TRUE = enabled, FALSE = disabled | Sets whether a meeting is declined after a certain duration if is not checked in from the touch screen | FALSE | ForceOrgCheckIn must be enabled |
| ForceOrgCheckIn | Boolean TRUE = enabled, FALSE = disabled | Sets whether the reservation must be checked in from the touch screen | FALSE | |
| ForceOrgCheckInEndMin | Integer [0–30 minutes] | Sets how long the check-in button displays after the start of a reservation | 5 | Configuration limited to the length of a meeting; 0 = button is unavailable after meeting begins |
| ForceOrgCheckInMin | Integer [0–2880 minutes] | Sets how long the check-in button displays before the start of a reservation | 5 | Button does not appear if previous reservation still is not checked in; 0 = button is unavailable before meeting begins |

Room Settings

Custom Properties - Room Settings

| Custom Property | Types and Supported Value(s) | Description | Default Value | Notes |
|---------------------------------|---|--|---------------|--|
| AvailabilityThresholdMin | Integer [1–120 minutes] | Sets the time that a room cannot be booked prior to the start of a meeting | 10 | Required if AvailabilityThresholdRoomState is enabled |
| AvailabilityThresholdRoom State | Integer 0 = Disabled, 1 = Enabled | Sets whether the availability threshold behavior is enabled or disabled | 0 | |
| DateFormat | Integer [0–9] | Sets the date format of the display | 0 | |
| OfflineExpiry | Integer [0–24 hours] | Sets the time to delay the "Display Offline" message after the display is no longer connected to the network | 8 | A value of 0 shows the offline screen immediately upon loss of connection. |
| PanelPin | String | Sets the four-digit PIN that must be entered to access scheduling application features | 1234 | Required if PanelSecurity is set to Touch Screen PIN |

| Custom Property | Types and Supported Value(s) | Description | Default Value | Notes |
|--------------------|---|---|---------------|--|
| PanelSecurityLevel | Integer 0 = Disabled/ Anonymous, 1 = Touch Screen PIN | Sets the security level of the scheduling application | 0 | |
| RoomFriendlyName | String | Sets a custom room name that overwrites the calendar name | empty | |
| RoomPrivacyLevel | Integer 0 = Public, 1 = Semi-Private, 2 = Private, 3 = Custom | Sets the privacy level of the scheduling application (what meeting information is shared on the touch screen) | 0 | Refer to Room on page 58 for more information. |
| TimeFormat | Boolean TRUE = 12hr, FALSE = 24hr | Sets the time format of the display | TRUE | |

¹ The table below correlates the date format with the required integer.

| Format | Definition | Example | Property |
|--------|--|------------------------|--------------|
| WMDY | Day of week, Month Day, Year | Tuesday, March 3, 2020 | DateFormat=0 |
| WDMY | Day of week, Day-Month-Year | Tuesday, 3-March-2020 | DateFormat=1 |
| WMD | Day of week, Month Day | Tuesday, March 3 | DateFormat=2 |
| WDM | Day of week, Day-Month | Tuesday, 3-March | DateFormat=3 |
| MDY | Month Day, Year | March 3, 2020 | DateFormat=4 |
| DMY | Day-Month-Year | 3-March-2020 | DateFormat=5 |
| M.DY | Month.Day Year | March.3 2020 | DateFormat=6 |
| D.MY | Day.Month Year | 3.March 2020 | DateFormat=7 |
| WYMD | Day of week, Year-Month-Day (ISO format) | Tuesday, 2020-March-3 | DateFormat=8 |
| YMD | Year-Month-Day (ISO format) | 2020-March-3 | DateFormat=9 |

Reservation Settings

Custom Properties - Reservation Settings

| Custom Property | Types and Supported Value(s) | Description | Default Value | Notes |
|-------------------------|--|---|---------------|---|
| EnFreeUpRoom | Boolean TRUE = enabled, FALSE = disabled | Sets whether a meeting may be ended early from the touch screen | TRUE | |
| ExtendReservationEnable | Boolean TRUE = enabled, FALSE = disabled | Sets whether the reservation can be extended from the touch screen | TRUE | |
| ExtendReservationMin | Integer [0–59 minutes] | Sets the number of minutes that must elapse before the extend reservation button is displayed | 15 | Extend ReservationType must be set to "0" |
| ExtendReservationPer | Integer [0–100%] | Sets the percentage of a meeting that must elapse before the extend reservation button is displayed | 25% | Extend ReservationType must be set to "1" |
| ExtendReservationType | Integer 0 = Minutes, 1 = Percentage | Sets whether the extend reservation function is controlled by elapsed minutes or elapsed percentage | 0 | Extend ReservationEnable must be enabled |
| FreeUpRoomEnMin | Integer [0–59 minutes] | Sets the number of minutes that must elapse before the end early button is displayed | 10 | FreeUpRoomEn UseMin must be enabled |
| FreeUpRoomEnPer | Integer [0–100%] | Sets the percentage of a meeting that must elapse before the end early button is displayed | 5% | FreeUpRoomEn UsePer must be enabled |
| FreeUpRoomEnUseMin | Boolean TRUE = enabled, FALSE = disabled | Sets whether the end early button displays after a set number of minutes has elapsed | TRUE | EnFreeUpRoom must be enabled |
| FreeUpRoomEnUsePer | Boolean TRUE = enabled, FALSE = disabled | Sets whether the end early button displays after a set percentage of the reservation has elapsed | FALSE | EnFreeUpRoom must be enabled |
| ReservationEnable | Boolean TRUE = enabled, FALSE = disabled | Sets whether meetings can be reserved from the touch screen | TRUE | |
| ReserveNowEvenEndTime | Boolean TRUE = enabled, FALSE = disabled | Sets whether the available reservation end time options end exactly on the half hour or hour | FALSE | If disabled, reservation end time options are set in 30 minute intervals from the current time; Reservation Enable must be enabled |
| ReserveNowMinDur | Integer [5–60 minutes, in 5-minute increments] | Sets the minimum duration of a meeting that can be reserved from the touch screen | 30 | Reservation Enable must be enabled |

| Custom Property | Types and Supported Value(s) | Description | Default Value | Notes |
|------------------|------------------------------|---|---------------|---|
| ReserveNowMaxDur | Integer [30–480 minutes] | Sets the maximum duration of a meeting that can be reserved from the touch screen | 120 | Reservation Enable must be enabled |

Schedule Settings

Custom Properties - Schedule Settings

| Custom Property | Types and Supported Value(s) | Description | Default Value | Notes |
|-----------------|--|---|---------------|--|
| EnPushModel | Boolean TRUE = enabled, FALSE = disabled | Sets whether Crestron Fusion uses push registration instead of polling the network for scheduling updates | TRUE | Available only if Crestron Fusion is set to be the scheduling provider |
| FindBtnEnable | Boolean TRUE = enabled, FALSE = disabled | Sets whether the find button is displayed on the touch screen | TRUE | Available only if Crestron Fusion is set to be the scheduling provider |
| PollTime | Integer [5–60 minutes] | Sets how often the application polls the scheduling server when updates are not pushed to the application | 5 | |
| ReserveCustomEn | Boolean TRUE = enabled, FALSE = disabled | Sets whether custom reservation lengths can be selected for the room | FALSE | If disabled, reservations lengths are provided in 30 minute increments |

All Scheduling Application Custom Properties

The table below lists the custom properties for the scheduling application in the order that they appear in the Crestron Fusion custom properties list.

For more information on a custom property, refer to that property's associated page number.

Scheduling Application Custom Properties

| Custom Property | Grouping |
|--------------------------------|---|
| AvailabilityThresholdMin | Room Settings on page 69 |
| AvailabilityThresholdRoomState | Room Settings on page 69 |
| BackgroundAvailable | Display Settings on page 67 |
| BackgroundReserved | Display Settings on page 67 |
| BroadcastEmgTimeOut | Broadcast Message Settings on page 67 |
| BroadcastTimeOutEnable | Broadcast Message Settings on page 67 |
| DateFormat | Room Settings on page 69 |
| DeclineForNoShowAppliesDur | Automation Settings on page 69 |
| DisableIdleScreen | UI Settings on page 68 |
| EnBroadcastMessage | Broadcast Message Settings on page 67 |
| EnDeclineForNoShow | Automation Settings on page 69 |
| EnFreeUpRoom | Reservation Settings on page 71 |
| EnPushModel | Schedule Settings on page 72 |
| ExtendReservationEnable | Reservation Settings on page 71 |
| ExtendReservationMin | Reservation Settings on page 71 |
| ExtendReservationPer | Reservation Settings on page 71 |
| ExtendReservationType | Reservation Settings on page 71 |
| FindBtnEnable | Schedule Settings on page 72 |
| ForceActiveAfterResStart | UI Settings on page 68 |
| ForceActiveBeforeResStart | UI Settings on page 68 |
| ForceOrgCheckIn | Automation Settings on page 69 |
| ForceOrgCheckInEndMin | Automation Settings on page 69 |
| ForceOrgCheckInMin | Automation Settings on page 69 |
| FreeUpRoomEnMin | Reservation Settings on page 71 |
| FreeUpRoomEnPer | Reservation Settings on page 71 |
| FreeUpRoomEnUseMin | Reservation Settings on page 71 |
| FreeUpRoomEnUsePer | Reservation Settings on page 71 |
| IdleTimeout | UI Settings on page 68 |
| LEDReservedColorForCheckIn | UI Settings on page 68 |

| Custom Property | Grouping |
|-------------------------|---|
| OfflineExpiry | Room Settings on page 69 |
| PanelPin | Room Settings on page 69 |
| PanelSecurityLevel | Room Settings on page 69 |
| PollTime | Schedule Settings on page 72 |
| ProjectIconUrl | UI Settings on page 68 |
| ProjectLayout | UI Settings on page 68 |
| ProjectTheme | UI Settings on page 68 |
| ReservationEnable | Reservation Settings on page 71 |
| ReserveCustomEn | Schedule Settings on page 72 |
| ReserveNowEvenEndTime | Reservation Settings on page 71 |
| ReserveNowMaxDur | Reservation Settings on page 71 |
| ReserveNowMinDur | Reservation Settings on page 71 |
| RoomFriendlyName | Room Settings on page 69 |
| RoomPrivacyLevel | Room Settings on page 69 |
| TimeFormat | Room Settings on page 69 |
| WorkHoursEn[Mon–Sun] | Work Hours Settings on page 66 |
| WorkHoursStart[Mon–Sun] | Work Hours Settings on page 66 |
| WorkHoursStop[Mon–Sun] | Work Hours Settings on page 66 |

Appendix A: Configure Modern Authentication for EWS

This appendix provides the procedures required to configure Modern Authentication (OAuth 2) support for the Crestron Room Scheduling App in the Microsoft® EWS (Exchange Web Services) service. These procedures apply to TSW-x60 touch screen firmware version 2.009.01x or higher.

The Modern Authentication authorization model is provided by the Azure® Active Directory® service to integrate managed API applications with the same authentication model used by the Office 365® software REST APIs. Once Modern Authentication is configured in EWS, the Crestron Room Scheduling app uses this access method to provide heightened user authentication.

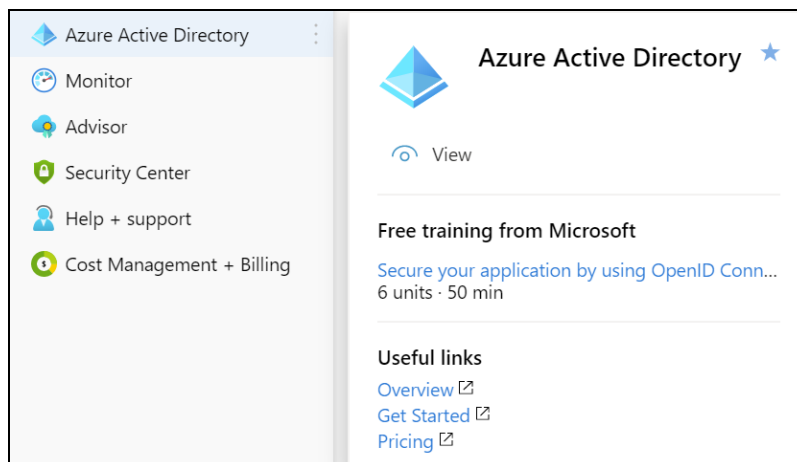
Configure the Crestron Room Scheduling EWS App

Use the following procedures to define a new application in Azure Active Directory.

Create the Crestron Room Scheduling App

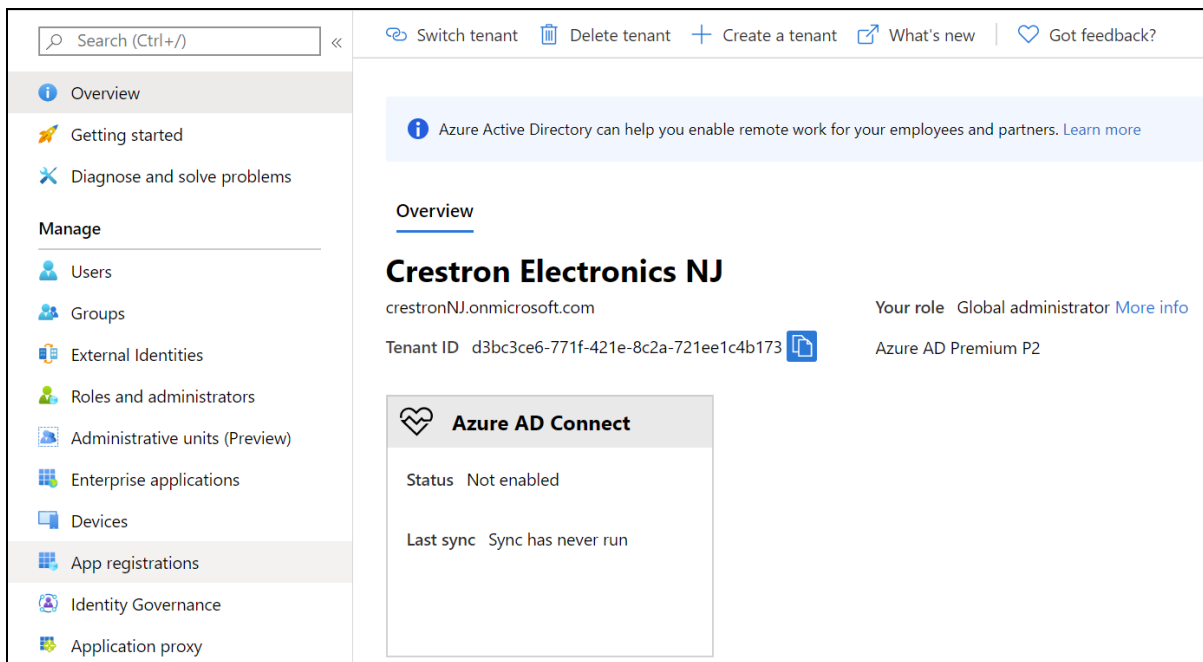
1. Sign into the Azure portal with a user ID with sufficient permissions to create an app.
2. Select **Azure Active Directory** from the left navigation menu.

Azure Active Directory Selection



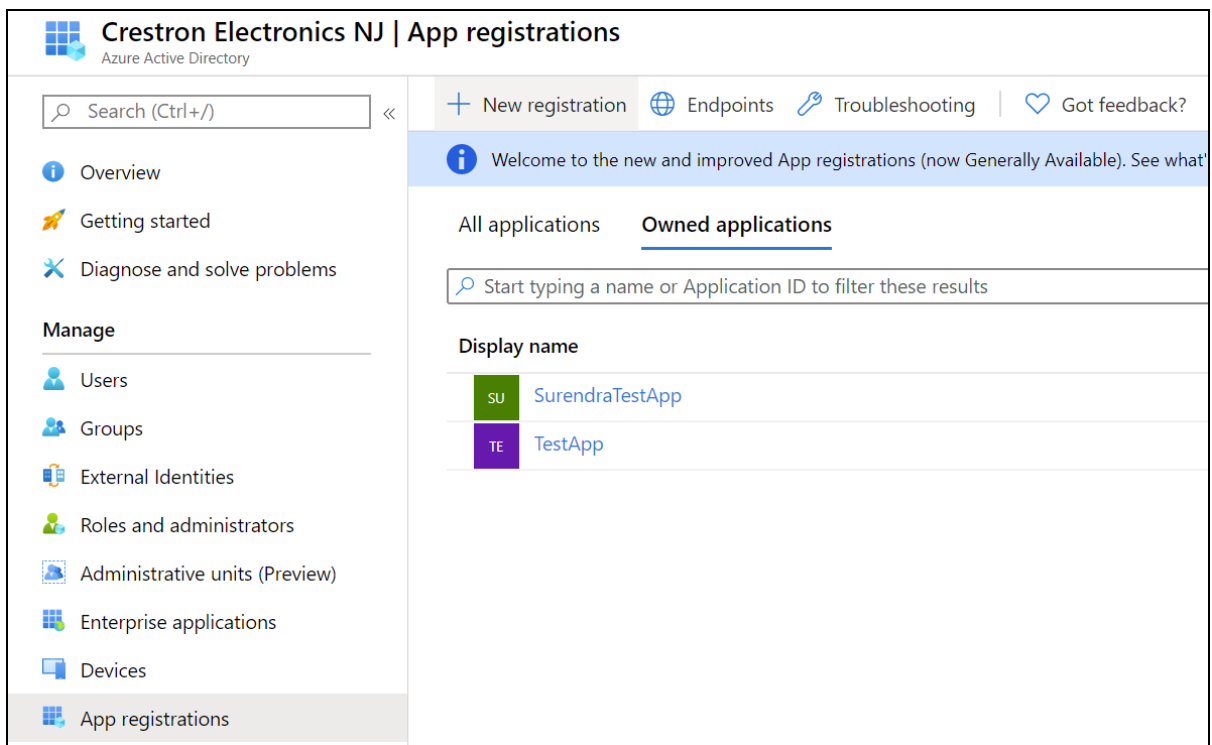
3. Select **App registrations** from the Azure widget menu.

App registrations Selection



4. Select **+ New registration**.

App registrations - New registration Screen



A dialog box for creating the app is displayed.

Register an application Dialog Box

Home > Crestron Electronics NJ | App registrations > Register an application

Register an application

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

Crestron Scheduling Device ✓

Supported account types
Who can use this application or access this API?

☒ Accounts in this organizational directory only (Crestron Electronics NJ only - Single tenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

[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 ▼ e.g. https://myapp.com/auth

5. Enter the following information:

- **Name:** Enter a user-facing name of the application (in the Azure environment). This can be any string 120 characters or less. It is possible to have more than one application registered with the same display name.
- **Supported account types:** Select the supported account type. Only the **Accounts in this organizational directory only** option is supported by the Crestron Room Scheduling app at this time.

NOTE: The **Redirect URI (optional)** settings are not configured for this application.

6. Select **Register**.

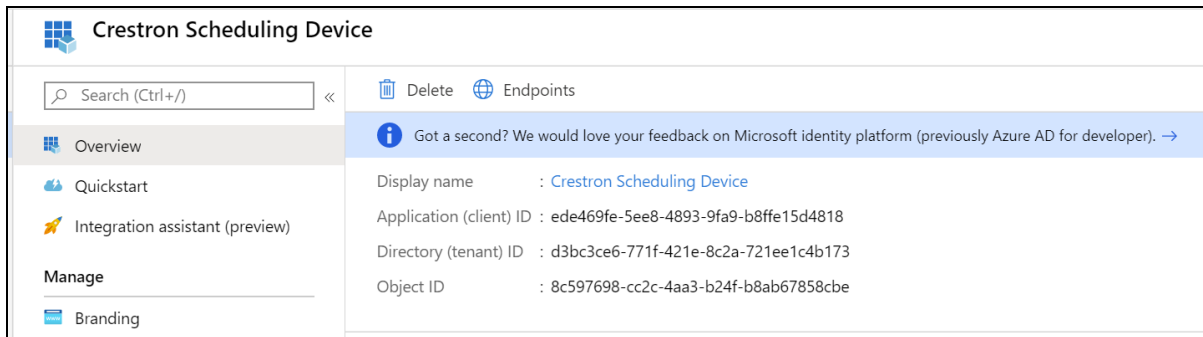
Obtain Authentication IDs

Once the app is registered, the application and directory IDs must be obtained to connect the Room Scheduling app to the Azure AD app.

1. Select **App registrations** from the Azure widget menu.
2. Select the application created for the Crestron Room Scheduling app. An application dialog box is displayed.

3. Select **Overview** from the navigation menu. Information about the Azure app is provided.

Application Overview Screen



4. Copy the following fields from the **Overview** pane to an accessible location. Use the **Copy to Clipboard** button that appears when hovering over each field to ensure accuracy.
 - **Application (client) ID:** The unique identification string for the Azure app.
 - **Directory (tenant) ID:** The unique identification string for the Azure directory.

Configure Additional Settings

The following additional settings can be configured for the Azure app. These settings define the user consent experience, authentication details, and API access scopes available to the application.

Branding

Select **Branding** under the **Manage** section of the application navigation menu to configure branding settings for the app.

Application Branding Screen

Home > Crestron Electronics NJ | App registrations > Crestron Scheduling Device | Branding

Crestron Scheduling Device | Branding

Search (Ctrl+/) Save Discard


Overview
Quickstart
Integration assistant (preview)


Manage

Branding
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
Owners
Roles and administrators (Previ...
Manifest

Support + Troubleshooting
Troubleshooting
New support request

Name * ⓘ Crestron Scheduling Device ✓



Logo



Upload new logo ⓘ Select a file 


Home page URL ⓘ https://www.crestron.com

Terms of service URL ⓘ e.g. https://myapp.com/termsofservice

Privacy statement URL ⓘ e.g. https://myapp.com/privacystatement

Publisher domain ⓘ  crestronNJ.onmicrosoft.com [Update domain](#)
The application's consent screen will show 'Unverified'.
[Learn more about publisher domain](#) 

Publisher verification (preview)
Associate a verified Microsoft Partner Center (MPN) account with your application. A verified badge will appear in various places, including the application consent screen. [Learn more](#) 

MPN ID Add MPN ID to verify publisher
 The application publisher domain is set to crestronNJ.onmicrosoft.com, but onmicrosoft.com publisher domains are not allowed. Please use a custom domain in order to proceed. Note: this domain must be a DNS verified domain on the tenant and match the primary contact domain for your MPN account.

Publisher display name Not provided

The following branding settings can be configured for the Crestron Room Scheduling app:

- **Name: Required.** Set the user-friendly name of the application. This is the same name that was defined when registering the application, but it can be changed here.
- **Upload New Logo:** Set a user-facing logo for this application that appears on the consent screen. The image file for the logo must meet the following requirements:
 - Image dimensions of 215 x 215 pixels
 - Central image dimensions of 94 x 94 pixels
 - Uses the file type .bmp, .jpg, or .png
 - File size less than 100 KB
- **Privacy statement URL:** Provides a link to the application privacy statement in the consent screen.
- **Publisher domain:** Sets the process that must be completed to verify ownership of the domain. Most users will probably already have a verified domain. If the domain is not verified, the application will work, but the consent screen will warn the user they are consenting to an unverified application.

Authentication

Select **Authentication** under the **Manage** section of the application navigation menu to configure authentication settings for the app.

Application Authentication Screen

Crestron Scheduling Device | Authentication

Search (Ctrl+ /)

Save Discard Got feedback?

Overview

Quickstart

Integration assistant (preview)

Manage

Branding

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

Owners

Roles and administrators (Previ...

Manifest

Support + Troubleshooting

Troubleshooting

New support request

Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

+ Add a platform

Supported account types

Who can use this application or access this API?

Accounts in this organizational directory only (Crestron Electronics NJ only - Single tenant)

Accounts in any organizational directory (Any Azure AD directory - Multitenant)

Help me decide...

Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts, you can do so using the manifest editor. [Learn more about these restrictions.](#)

Advanced settings

Default client type ⓘ

Treat application as a public client.

Required for the use of the following flows where a redirect URI is not used:

Resource owner password credential (ROPC) [Learn more](#)

Device code flow [Learn more](#)

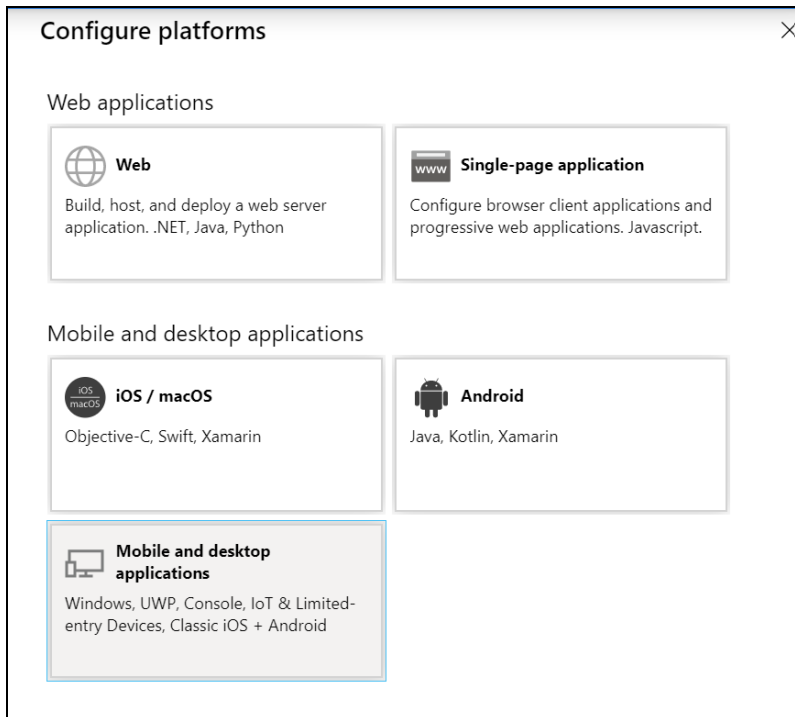
Integrated Windows Authentication (IWA) [Learn more](#)

Yes No

The following authentication settings can be configured for the Crestron Room Scheduling app:

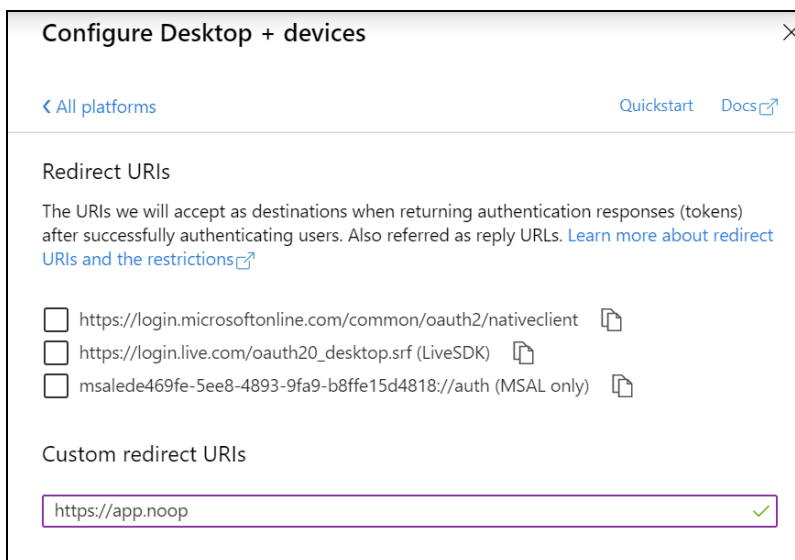
- **Add a Platform:** Click this button to create a platform for app authentication. The **Configure platforms** pane is displayed on the right side of the screen.

Configure platforms Pane



Select **Mobile and desktop applications** to display settings for configuring this platform.

Configure Desktop + devices Pane



Azure AD requires the use of a redirect URI, but the Crestron Room Scheduling app does not. Enter a valid URI address and select **Configure**.

NOTE: Certain sites require selecting the third checkbox (**MSAL only**) within this pane in order for authentication to work properly.

- **Supported account types:** Select an account type for the app. This setting is the same as the one set when registering the app and should not change from **Accounts in this organizational directory only**.
- **Default Client Type:** The **Treat application as a public client** toggle must be set to enabled.

API Permissions

Select **API Permissions** under the **Manage** section of the application navigation menu to configure API permissions for the app.

API Permissions Screen

Crestron Scheduling Device | API permissions

Search (Ctrl+/) Refresh

Overview
Quickstart
Integration assistant (preview)

Manage

Branding
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
Owners
Roles and administrators (Previ...
Manifest

Support + Troubleshooting

Troubleshooting
New support request

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission Grant admin consent for Crestron Electronics NJ

| API / Permissions name | Type | Description | Admin consent req... | Status |
|------------------------|-----------|-------------------------------|----------------------|--------|
| Microsoft Graph (1) | | | | ... |
| User.Read | Delegated | Sign in and read user profile | - | ... |


The following API permissions settings can be configured for the Crestron Room Scheduling app.

Select **Add a Permission** to create a new API permission for the app. The **Request API permissions** pane is displayed on the right side of the screen.


Request API permissions Pane

Request API permissions


applications in the cloud

 **Azure Data Lake**


Access to storage and compute for big data analytic scenarios

 **Azure Import/Export**


Programmatic control of import/export jobs

 **Azure Key Vault**


Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

 **Customer Insights**


Create profile and interaction models for your products

 **Data Export Service for Microsoft Dynamics 365**


Export data from Microsoft Dynamics CRM organization to an external destination

 **Dynamics CRM**


Access the capabilities of CRM business software and ERP systems

 **Dynamics ERP**


Programmatic access to Dynamics ERP data

 **PowerApps Runtime Service**

Powerful data storage, modeling, security and integration capabilities


 **Speech**

Create powerful speech-enabled features using speech to text and text to speech conversion


 **Universal Print**

Programmatic access to create and manage printer and print job resources

Supported legacy APIs

 **Azure Active Directory Graph**

Programmatic access to directory data and objects

 **Exchange**

A powerful, easy-to-use way to access and manipulate Exchange data

To set the API permissions for EWS:

1. Select **Exchange** to display a list of permissions for EWS.

Request API permissions Pane - Exchange

Request API permissions

[← All APIs](#)
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.

Select permissions [expand all](#)

Type to search

| Permission | Admin consent required |
|---|------------------------|
| > Calendars | |
| > Contacts | |
| > EAS | |
| ▼ EWS (1) | |
| <input checked="" type="checkbox"/> EWS.AccessAsUser.All Access mailboxes as the signed-in user via Exchange Web Services ⓘ | - |
| > Exchange | |
| > Group | |
| > MailboxSettings | |
| > Mail | |
| > Notes | |
| > People | |
| > Place | |
| > Tasks | |

[Add permissions](#) [Discard](#)

2. Expand the EWS accordion.
3. Fill the checkbox next to **EWS.AccessAsUser.All** to allow the application to make requests to the Exchange Web Services API on behalf of the configured user.

To set the API permissions for the Microsoft® Graph function:

1. Select **Microsoft Graph** to display a list of permissions for Microsoft Graph.

Request API permissions Pane - Microsoft Graph

Request API permissions

< 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.

Select permissions expand all

Type to search

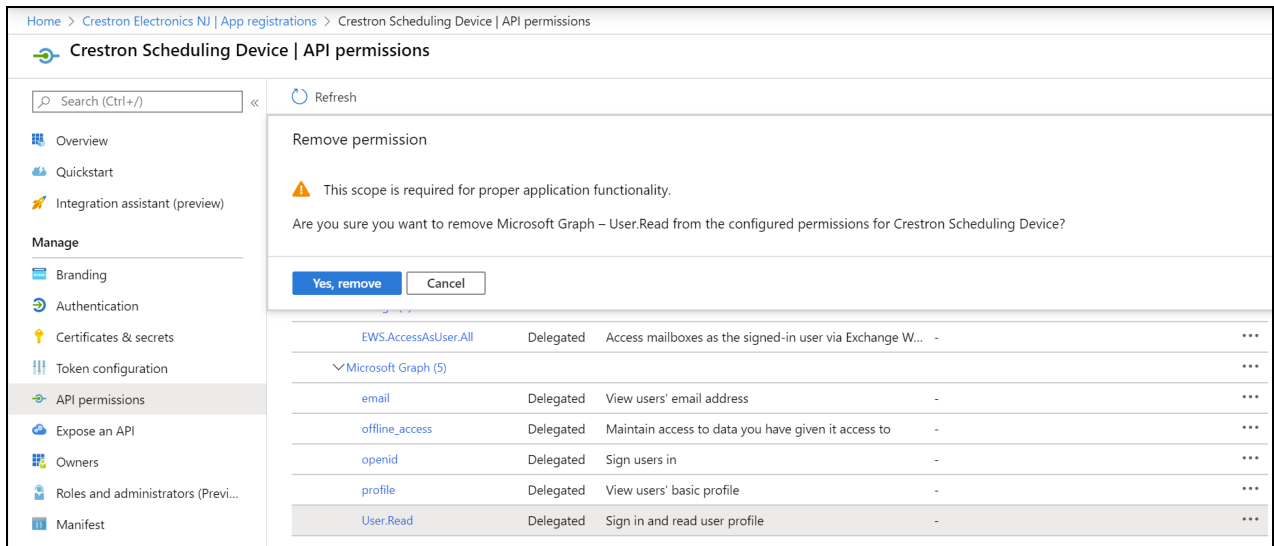
| Permission | Admin consent required |
|---|------------------------|
| <input checked="" type="checkbox"/> email View users' email address ⓘ | - |
| <input checked="" type="checkbox"/> offline_access Maintain access to data you have given it access to ⓘ | - |
| <input checked="" type="checkbox"/> openid Sign users in ⓘ | - |
| <input checked="" type="checkbox"/> profile View users' basic profile ⓘ | - |
| > AccessReview | |
| > AdministrativeUnit | |
| > AgreementAcceptance | |
| > Agreement | |
| > Analytics | |

Add permissions Discard

2. Fill the checkboxes next to the following settings to enable the functionality described below:
 - **offline_access:** Allows the application to receive a Refresh Token, which can be exchanged for a new Access Token, when it expires. This is required for long running applications, so user consent is not required each time an access token expires.
 - **openid:** Allows the application to receive an ID Token, which provides basic profile information about the authenticated user. This scope is required for the next two scopes, as they are delivered in the ID Token.
 - **email:** provides the email address of the authenticated user. The application uses this to get the calendar address if none is entered during device configuration.
 - **profile:** Provides basic profile information about the authenticated user, such as the display name and photo URL.

If the Microsoft Graph **User.Read** scope is added automatically, it can be removed. If there is a warning, it can be ignored.

API Permissions Screen - User.Read Scope



Connect the Scheduling App to EWS

Once an app has been registered in Azure AD, the Crestron Room Scheduling app can be connected to EWS from the touch screen web configuration interface.

To connect the Crestron Room Scheduling App to EWS:

1. Navigate to **Settings > Schedule**.
2. Select **Exchange EWS** from the **Schedule Source** drop-down menu.
3. Turn on the **Enable Modern Authentication** toggle.

Settings Tab - Schedule (Exchange EWS) - Enable Modern Authentication

Schedule

Polling Interval
5

Custom Reserve Time
Disable

Schedule source
Exchange EWS

Exchange EWS

Enable Modern Authorization
Enabled

Exchange Calendar Email Address

O365 Tenant ID

Client ID (Application ID)

This field is required.

This field is required.

4. Enter the following information in the appropriate fields:
 - Enter the email address associated with the Microsoft Exchange scheduling calendar in the **Exchange Calendar Email Address** text field.
 - Copy and paste the application client ID obtained in [Obtain Authentication IDs on page 77](#) into the **Client ID (Application ID)** text field.
 - Copy and paste the directory tenant ID obtained in [Obtain Authentication IDs on page 77](#) into the **O365 Tenant ID** text field.
5. Select **Save Changes** from the **Action** menu.
6. Navigate to **Status > Schedule**. The **Exchange** subsection displays a **Register now** button.

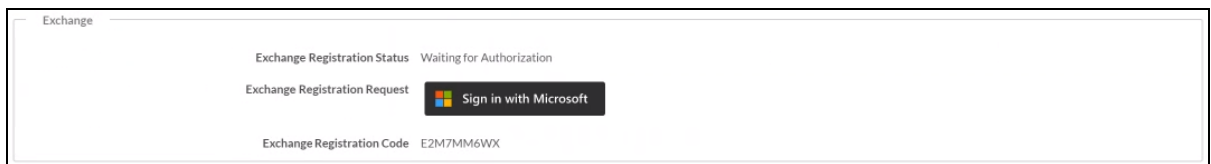
Status Tab - Schedule (Register now Button)



7. Select **Register Now**.

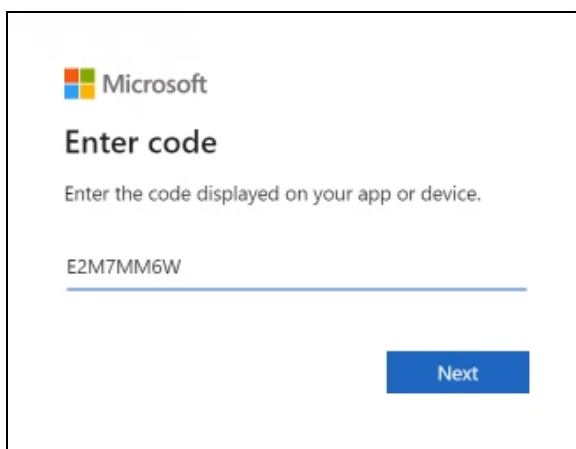
When the web configuration interface refreshes, the **Exchange** subsection displays a **Sign in with Microsoft** button next to **Exchange Registration Request** and an **Exchange Registration Code**.

Status Tab - Schedule (Registration URL and Code)



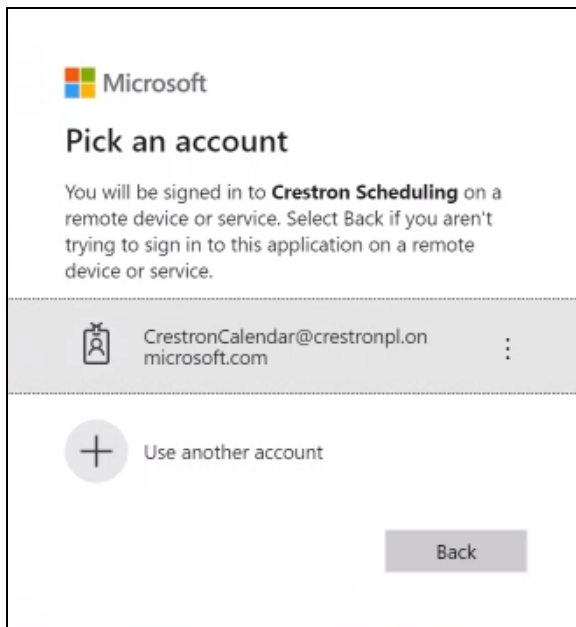
8. Select **Sign in with Microsoft**. An **Enter Code** dialog box is displayed.

Enter Code Dialog Box



9. Enter the provided Exchange registration code in the text field and select **Next**. The **Pick an account** dialog box is displayed.

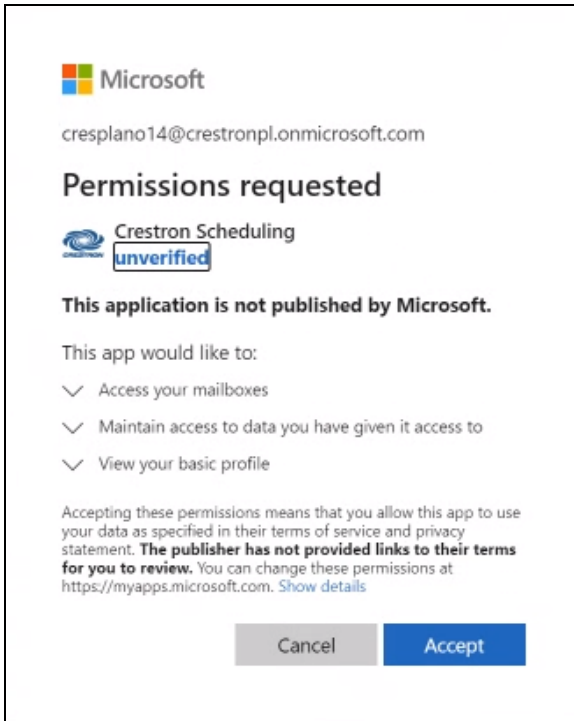
Pick an account Dialog Box



10. Select the EWS account that contains the desired scheduling calendar and enter the account password if prompted.

11. If the account has not yet been verified, a **Permissions requested** dialog box is displayed. Select **Accept** to verify the account.

Permissions requested Dialog Box



When the web configuration interface refreshes, the **Exchange Registration Status** updates to **Registered**. The Exchange scheduling calendar connects to the scheduling application without requiring a restart.

Status Tab - Schedule (Registered)



Appendix B: Configure Microsoft Graph for Crestron Room Scheduling

This appendix provides the procedures required to configure Microsoft Graph support for the Crestron Room Scheduling App. These procedures apply to TSW-60 touch screen firmware version 3.200.2x or higher.

Microsoft Graph is provided by the Microsoft Entra® service to allow access to Microsoft Cloud service resources. Once Microsoft Graph is configured, the Crestron Room Scheduling app uses this access method to provide heightened user authentication.

NOTE: If access has not been granted for Microsoft Graph configuration or if account has not been provided to access the Microsoft Entra tenant, contact the tenant administrator within your organization's IT department.

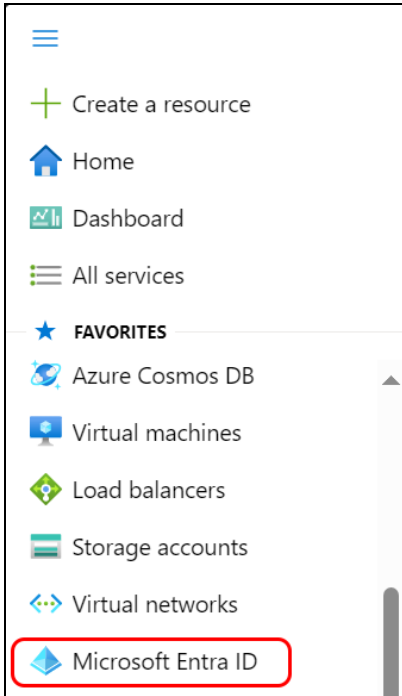
Configure the Crestron Room Scheduling App

Use the following procedures to define a new application in Microsoft Entra.

Create the Crestron Room Scheduling App

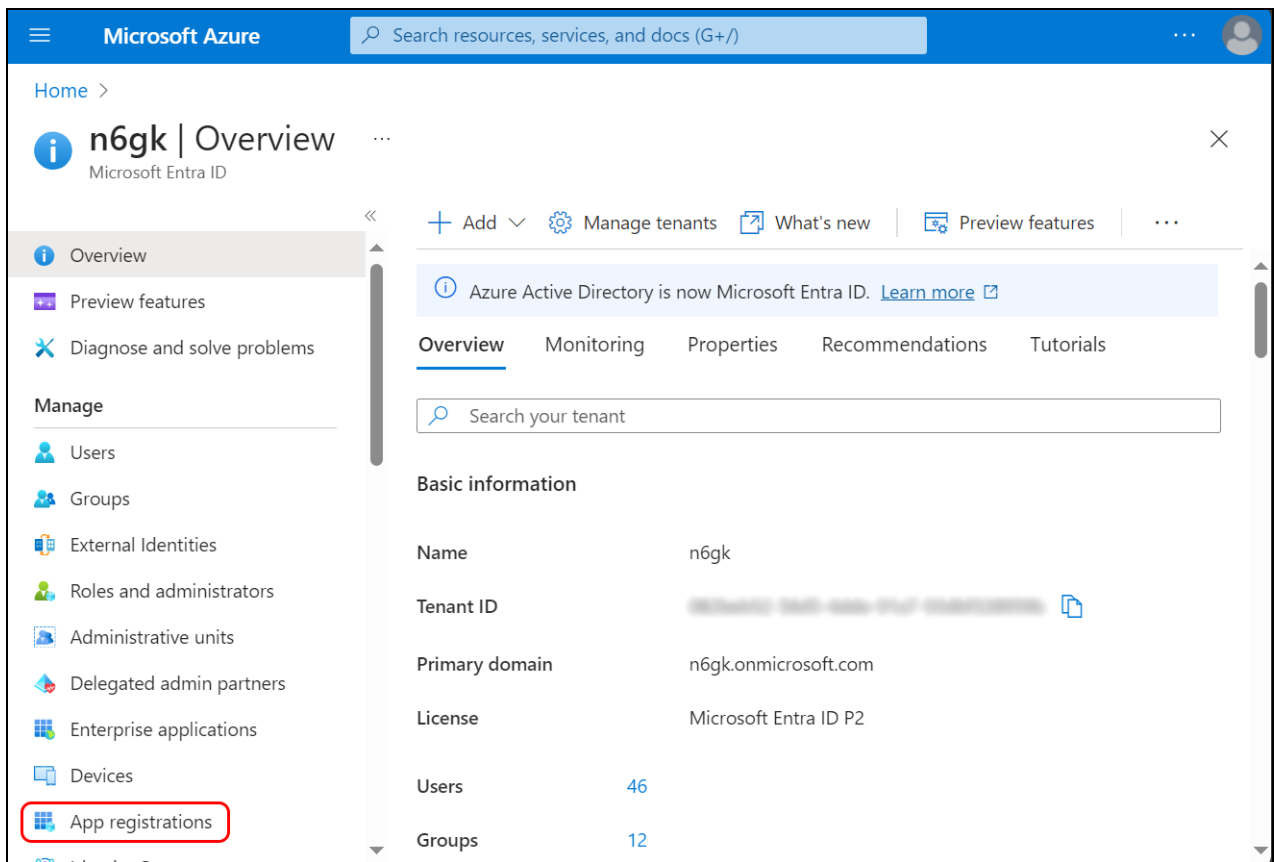
1. Sign into the Microsoft Entra portal with a user ID with sufficient permissions to create an app.
2. Select **Microsoft Entra ID** from the left navigation menu.

Microsoft Entra ID Selection



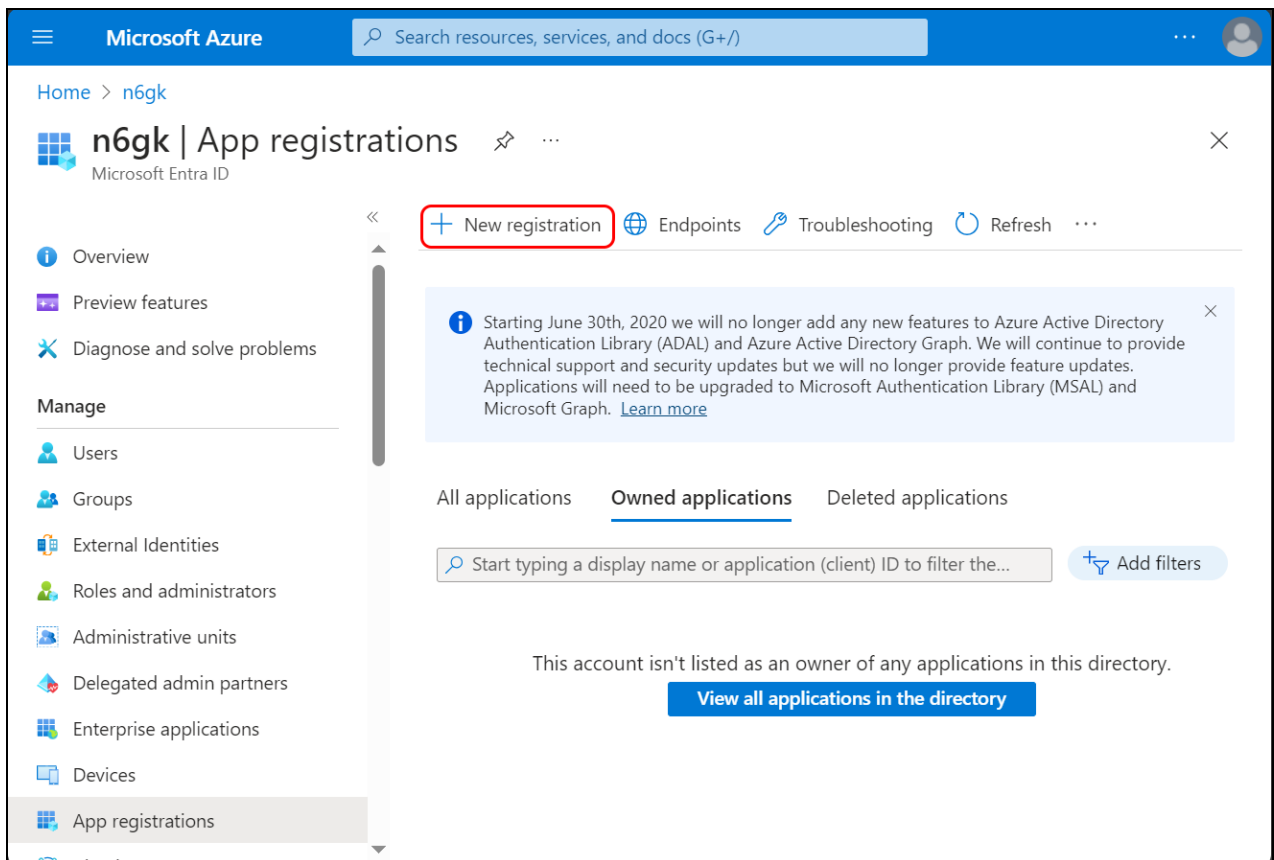
3. Select **App registrations** from the Microsoft Entra widget menu.

App registrations Selection



4. Select **+ New registration**.

App registrations - New registration Selection



A dialog box for creating the app is displayed.

Register an application Dialog Box

Microsoft Azure Search resources, services, and docs (G+/)

Home > n6gk | App registrations >

Register an application

* Name

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

Crestron Scheduling for Graph API ✓

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (n6gk only - Single tenant)

☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

☐ Personal Microsoft accounts only

[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.

Select a platform e.g. https://example.com/auth

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

[By proceeding, you agree to the Microsoft Platform Policies](#)

Register

5. Enter the following information:

- **Name:** Enter a user-facing name of the application (in the Microsoft Entra environment). This can be any string 120 characters or less. It is possible to have more than one application registered with the same display name.
- **Supported account types:** Select the supported account type. Only the **Accounts in this organizational directory only** option is supported by the Crestron Room Scheduling app at this time.

NOTE: The **Redirect URI (optional)** settings are not configured for this application.

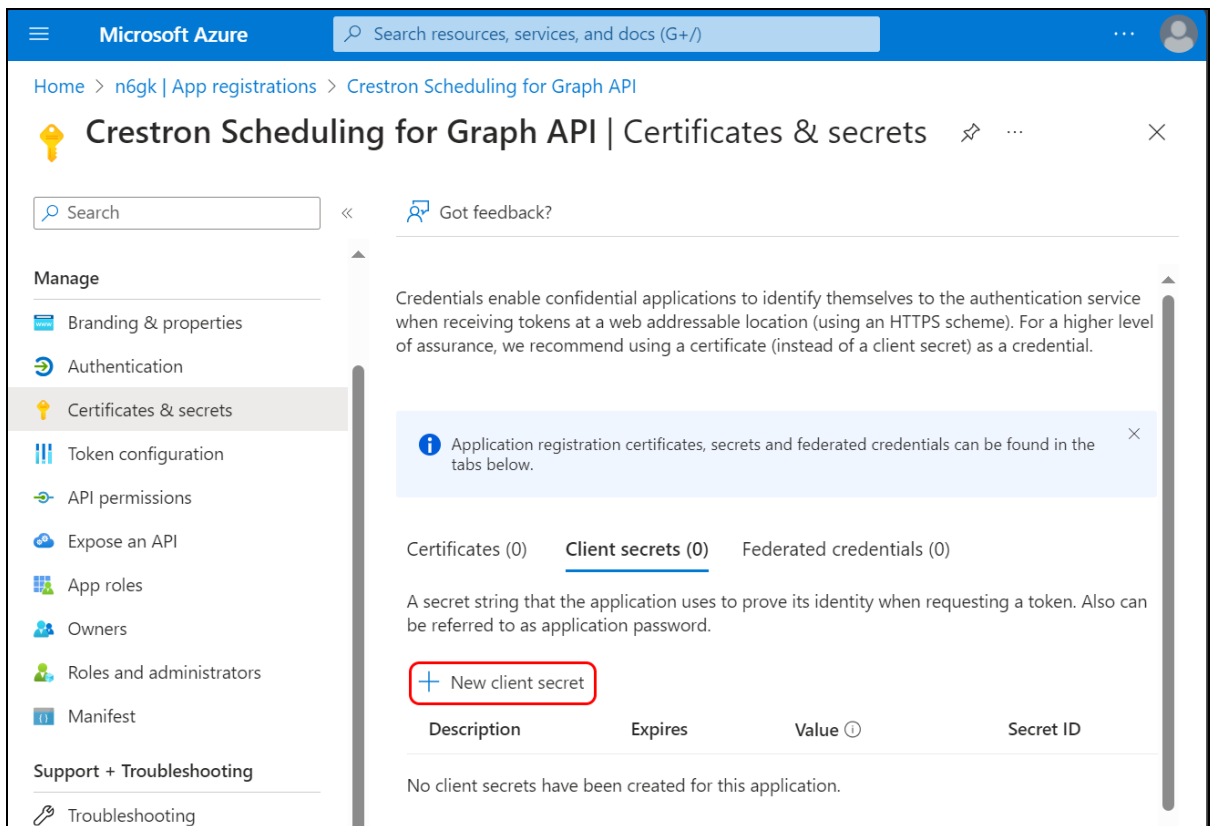
6. Select **Register**.

Create a Client Secret

Once the app is registered, a client secret must be created to connect the Crestron Room Scheduling App to the Microsoft Entra app.

1. Select **App registrations** from the Microsoft Entra widget menu.
2. Select the application created for the Crestron Room Scheduling App. An application dialog box is displayed.
3. Select **Certificates & secrets** from the navigation menu. The **Certificates & secrets** page for the Microsoft Entra app is displayed.

Certificates & secrets Page



4. Select **+ New client secret**. The **Add a client secret** dialog box is displayed.

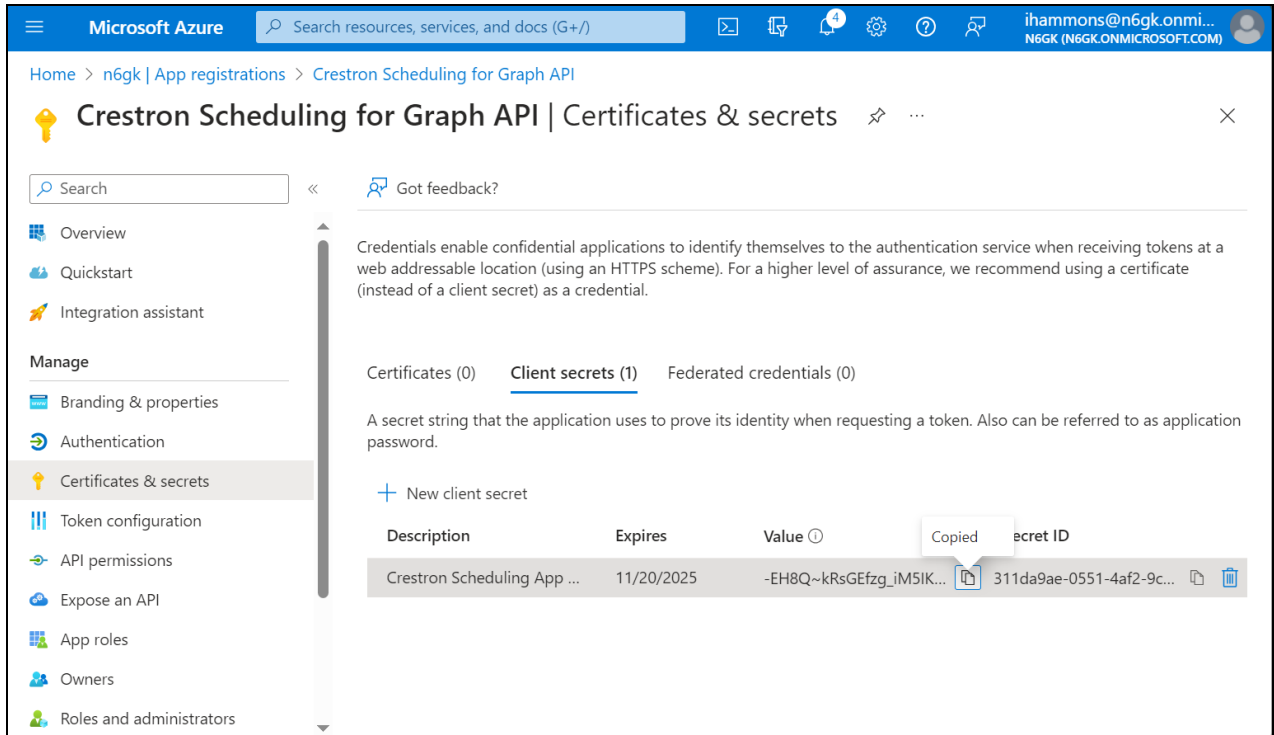
Add a client secret Dialog Box

The dialog box is titled "Add a client secret" and features a close button (X) in the top right corner. It contains two input fields: "Description" with the text "Crestron Scheduling App Key" and "Expires" with a dropdown menu showing "730 days (24 months)". At the bottom, there are two buttons: "Add" (blue) and "Cancel" (white).

5. Enter the following information:
 - **Description:** Enter a description for the client secret.
 - **Expires:** Select the duration before the client secret expires from the drop-down menu.
6. Select **Add**. The new client secret is added to the **Certificates & secrets** page for the Microsoft Entra app.
7. Copy the client secret **Value** to the clipboard or a location where it can be accessed later when configuring the Crestron Room Scheduling App as described in [Connect the Scheduling App to Microsoft Graph on page 104](#).

NOTE: The client secret **Value** is available only after it is first created. If the client secret **Value** is not copied before navigating away from the **Certificates & secrets** page, it will no longer be visible, and a new client secret must be created.

Certificates & secrets Page - Added Client Secret



Add API Permissions

Use the following procedure to set Microsoft Graph API permissions for the Crestron Room Scheduling App.

NOTE: The Microsoft Entra app is created with one global API permission by default (**Users.Read**). This permission can be removed since it will be added later at the application level.

1. Select **App registrations** from the Microsoft Entra widget menu.
2. Select the application created for the Crestron Room Scheduling App. An application dialog box is displayed.

3. Select **API permissions** from the navigation menu. The **API permissions** page for the Microsoft Entra app is displayed.

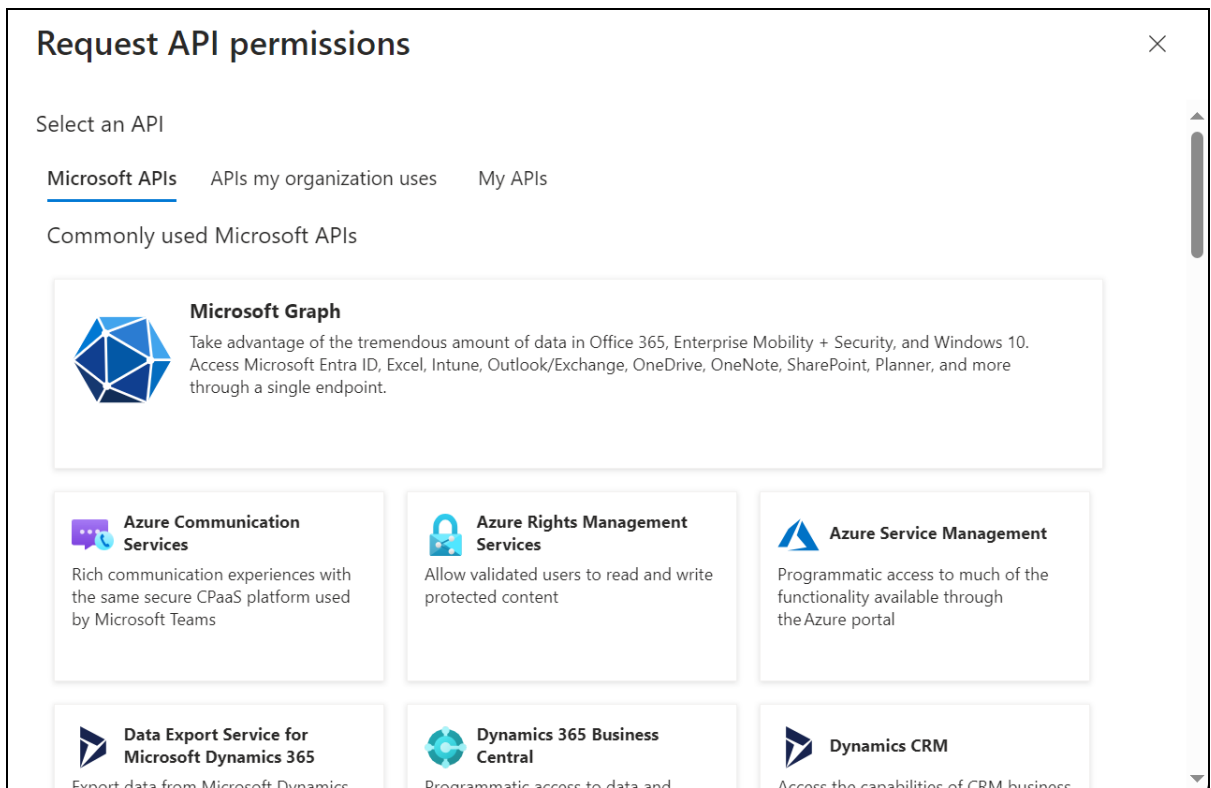
API permissions Page

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and a user profile icon. The breadcrumb trail indicates the path: Home > n6gk | App registrations > Crestron Scheduling for Graph API. The main heading is 'Crestron Scheduling for Graph API | API permissions'. On the left, a navigation menu lists various app management options, with 'API permissions' highlighted. The main content area features a search bar, a refresh button, and a 'Got feedback?' link. A blue information banner explains the 'Admin consent required' column. Below this, the 'Configured permissions' section provides an overview of the consent process. A table lists the configured permissions, showing one permission for 'Microsoft Graph (1)'. The table has columns for 'API / Permissions name', 'Type', 'Description', and 'Admin consent required'.

| API / Permissions name | Type | Description | Admin consent required |
|------------------------|-----------|-------------------------------|------------------------|
| ▼ Microsoft Graph (1) | | | |
| User.Read | Delegated | Sign in and read user profile | No |

4. Select **+ Add a permission**. The **Request API permissions** dialog box is displayed.

Request API permissions Dialog Box




5. Select **Microsoft Graph**. Permissions for the Microsoft Graph API are displayed.
6. Select **Application permissions** for the required permission type.

NOTE: Delegated permissions require that the app acts on the behalf of a logged-in user. Since the app has its own key, permissions are granted to the app directly.

Request API permissions (Microsoft Graph) Dialog Box

Request API permissions

< 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.

Select permissions [expand all](#)

| Permission | Admin consent required |
|----------------|------------------------|
| > AccessReview | |
| > Acronym | |

Add permissionsDiscard

7. Fill the appropriate check boxes to select the following permissions:

- Within the **Calendars** section, select **Calendars.ReadWrite**.

Calendars (1)

| | | |
|-------------------------------------|---|-----|
| <input type="checkbox"/> | Calendars.Read ⓘ Read calendars in all mailboxes | Yes |
| <input type="checkbox"/> | Calendars.ReadBasic.All ⓘ Read basic details of calendars in all mailboxes | Yes |
| <input checked="" type="checkbox"/> | Calendars.ReadWrite ⓘ Read and write calendars in all mailboxes | Yes |

- Within the **MailboxSettings** section, select **MailboxSettings.Read**.

MailboxSettings (1)

| | | |
|-------------------------------------|---|-----|
| <input checked="" type="checkbox"/> | MailboxSettings.Read ⓘ Read all user mailbox settings | Yes |
| <input type="checkbox"/> | MailboxSettings.ReadWrite ⓘ Read and write all user mailbox settings | Yes |

- Within the **User** section, select **User.ReadAll**.

| User (1) | | |
|-------------------------------------|---|-----|
| <input type="checkbox"/> | User.EnableDisableAccount.All ⓘ Enable and disable user accounts | Yes |
| <input type="checkbox"/> | User.Export.All ⓘ Export user's data | Yes |
| <input type="checkbox"/> | User.Invite.All ⓘ Invite guest users to the organization | Yes |
| <input type="checkbox"/> | User.ManageIdentities.All ⓘ Manage all users' identities | Yes |
| <input checked="" type="checkbox"/> | User.Read.All ⓘ Read all users' full profiles | Yes |
| <input type="checkbox"/> | User.ReadWrite.All ⓘ Read and write all users' full profiles | Yes |

8. Select **Add permissions**. The three permissions are added under the **Configured permissions** section of the **API permissions** page for the Microsoft Entra app.
9. Select **Grant admin consent for [Microsoft Entra Account Name]** for the three added permissions, where **[Microsoft Entra Account Name]** is the name of the active Microsoft Entra account, then select **Yes** when prompted within the dialog box that is displayed.

API permissions Page - Grant admin consent Selection

Microsoft Azure | Search resources, services, and docs (G+)

Home > n6gk | App registrations > Crestron Scheduling for Graph API

Crestron Scheduling for Graph API | API permissions

Search | Refresh | Got feedback?

Grant admin consent confirmation.
Do you want to grant consent for the requested permissions for all accounts in n6gk? This will update any existing admin consent records this application already has to match what is listed below.

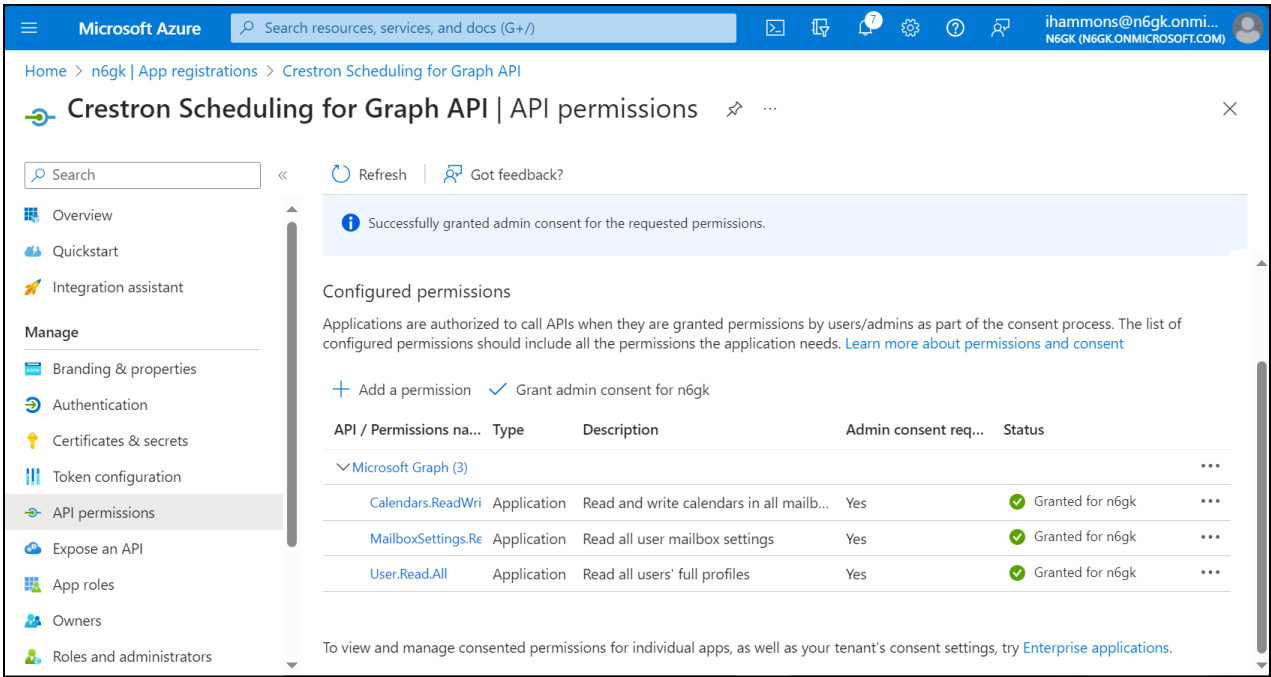
+ Add a permission **✓ Grant admin consent for n6gk**

| API / Permissions na... | Type | Description | Admin consent req... | Status |
|-------------------------|-------------|--|----------------------|------------------------|
| Microsoft Graph (3) | | | | |
| Calendars.ReadWrite | Application | Read and write calendars in all mailb... | Yes | ⚠ Not granted for n6gk |
| MailboxSettings.Re | Application | Read all user mailbox settings | Yes | ⚠ Not granted for n6gk |
| User.Read.All | Application | Read all users' full profiles | Yes | ⚠ Not granted for n6gk |

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

10. Verify that the **Status** column for each permission changes to show a green check icon and states that permission has been granted for the active Microsoft Entra account.

API permissions Page - Admin Consent Granted



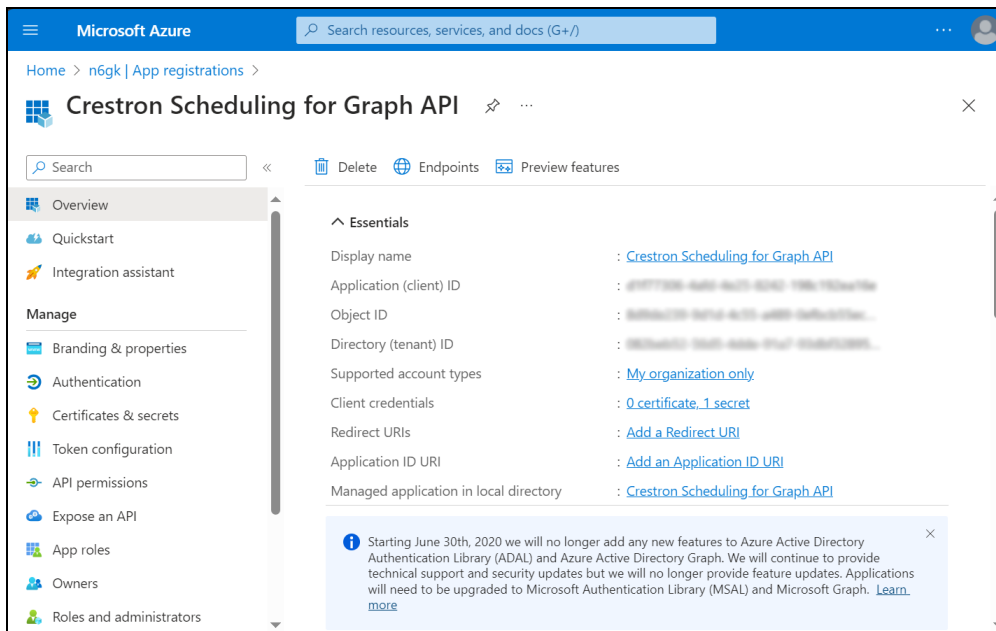
Obtain Authentication IDs

Use the following procedure to obtain the application and directory IDs that are required to connect the Room Scheduling app to the Microsoft Entra app.

1. Select **App registrations** from the Microsoft Entra widget menu.
2. Select the application created for the Crestron Room Scheduling app. An application dialog box is displayed.

3. Select **Overview** from the navigation menu. Information about the Microsoft Entra app is provided.

Application Overview Page



4. Copy the following fields from the **Overview** pane to an accessible location. Use the **Copy to Clipboard** button that appears when hovering over each field to ensure accuracy.
 - **Application (client) ID:** The unique identification string for the Microsoft Entra app.
 - **Directory (tenant) ID:** The unique identification string for the Microsoft Entra directory.

Connect the Scheduling App to Microsoft Graph

Once an app has been registered in Microsoft Entra, the Crestron Room Scheduling app can be connected to Microsoft Graph from the touch screen web configuration interface.

To connect the Crestron Room Scheduling App to Microsoft Graph:

1. Navigate to **Settings > Schedule**.
2. Select **O365** from the **Schedule Source** drop-down menu.

Settings Tab - Schedule (O365)

The screenshot shows the 'Schedule' configuration page for the O365 source. At the top, there's a 'Polling Interval' set to 5 minutes and a 'Custom Reserve Time' toggle switch. Below these, the 'Schedule Source' is set to 'O365'. A section titled 'Exchange' contains four text input fields: 'Exchange Calendar Email Address', 'Client ID (Application ID)', 'O365 Tenant ID', and 'Client Secret'. Each field has a red asterisk indicating it is required.

3. Enter the following information in the appropriate fields:
 - Enter the email address associated with the Microsoft Exchange scheduling calendar in the **Exchange Calendar Email Address** text field.
 - Copy and paste the directory tenant ID obtained in [Obtain Authentication IDs on page 102](#) into the **O365 Tenant ID** text field.
 - Copy and paste the application client ID obtained in [Obtain Authentication IDs on page 102](#) into the **Client/Application ID** text field.
 - Copy and paste the client secret obtained in [Create a Client Secret on page 95](#) into the **Client Secret** text field.
4. Select **Save Changes** from the **Action** menu. The Office 365 scheduling calendar connects to the scheduling application without requiring a restart.

