Room Scheduling System

Room Agent™ Room Booking Software, TouchLink® Scheduling Panels, Wayfinding Devices, and System Status Indicators

User Guide

Room Scheduling

68-3051-01 Rev. T
08 25

Safety Instructions

Safety Instructions • English

WARNING: This symbol, , when used on the product, is intended to alert the user of the presence of uninsulated dangerous voltage within the product's enclosure that may present a risk of electric shock.

ATTENTION: This symbol, , when used on the product, is intended to alert the user of important operating and maintenance (servicing) instructions in the literature provided with the equipment.

For information on safety guidelines, regulatory compliances, EMI/EMF compatibility, accessibility, and related topics, see the Extron Safety and Regulatory Compliance Guide, part number 68-290-01, on the Extron website, **www.extron.com**.

تعليمات السلامة • العربية

تحذير: هذا الرمز، ، عند استخدامه على المنتج، مخصص لتنبيه المستخدم فيما يتعلق بوجود جهد كهربائي غير معزول على الغلاف الخارجي للمنتج وهو ما قد ينطوي على مخاطر حدوث صدمة كهربائية.

انتبه: هذا الرمز، ، عند استخدامه على المنتج، مخصص لتنبيه المستخدم بتعليمات التشغيل والصيانة الهامة (الخدمة) في المواد التي يتم توفيرها مع المعدات.

للحصول على المزيد من المعلومات حول إرشادات السلامة، والتوافقات التنظيمية، والتوافق الكهرومغناطيسي/المجال الكهرومغناطيسي، وإمكانية الوصول، والموضوعات ذات الصلة، يُرجى مراجعة دليل السلامة والتوافق التنظيمي **www.extron.com** الخاص بإكسترون، الجزء رقم 68-290-01، على موقع إكسترون،

Sicherheitsanweisungen • Deutsch

WARUNG: Dieses Symbol auf demProdukt soll den Benutzer darauf aufmerksam machen, dass im Inneren des Gehäuses dieses Produktes gefährliche Spannungen herrschen, die nicht isoliert sind und die einen elektrischen Schlag verursachen können.

VORSICHT: Dieses Symbol auf dem Produkt soll dem Benutzer in der im Lieferumfang enthaltenen Dokumentation besonders wichtige Hinweise zur Bedienung und Wartung (Instandhaltung) geben.

Weitere Informationen über die Sicherheitsrichtlinien, Produkthandhabung, EMI/EMF-Kompatibilität, Zugänglichkeit und verwandte Themen finden Sie in den Extron-Richtlinien für Sicherheit und Handhabung (Artikelnummer 68-290-01) auf der Extron-Website, **www.extron.com**.

Instrucciones de seguridad • Español

ADVERTENCIA: Este símbolo, , cuando se utiliza en el producto, avisa al usuario de la presencia de voltaje peligroso sin aislar dentro del producto, lo que puede representar un riesgo de descarga eléctrica.

ATENCIÓN: Este símbolo, , cuando se utiliza en el producto, avisa al usuario de la presencia de importantes instrucciones de uso y mantenimiento estas estan incluidas en la documentación proporcionada con el equipo.

Para obtener información sobre directrices de seguridad, cumplimiento de normativas, compatibilidad electromagnética, accesibilidad y temas relacionados, consulte la Guía de cumplimiento de normativas y seguridad de Extron, referencia 68-290-01, en el sitio Web de Extron, **www.extron.com**

Instructions de sécurité • Français

AVERTISSEMENT : Ce pictogramme, , lorsqu'il est utilisé sur le produit, signale à l'utilisateur la présence à l'intérieur du boîtier du produit d'une tension électrique dangereuse susceptible de provoquer un choc électrique.

ATTENTION : Ce pictogramme, , lorsqu'il est utilisé sur le produit, signale à l'utilisateur des instructions d'utilisation ou de maintenance importantes qui se trouvent dans la documentation fournie avec l'équipement.

Pour en savoir plus sur les règles de sécurité, la conformité à la réglementation, la compatibilité EMI/EMF, l'accessibilité, et autres sujets connexes, lisez les informations de sécurité et de conformité Extron, réf. 68-290-01, sur le site Extron, **www.extron.com**.

Istruzioni di sicurezza • Italiano

AVVERTENZA: Il simbolo, , se usato sul prodotto, serve ad avvertire l'utente della presenza di tensione non isolata pericolosa all'interno del contenitore del prodotto che può costituire un rischio di scosse elettriche.

ATTENTZIONE: Il simbolo, , se usato sul prodotto, serve ad avvertire l'utente della presenza di importanti istruzioni di funzionamento e manutenzione nella documentazione fornita con l'apparecchio.

Per informazioni su parametri di sicurezza, conformità alle normative, compatibilità EMI/EMF, accessibilità e argomenti simili, fare riferimento alla Guida alla conformità normativa e di sicurezza di Extron, cod. articolo 68-290-01, sul sito web di Extron, **www.extron.com**.

Instrukcje bezpieczeństwa • Polska

OSTRZEŻENIE: Ten symbol, , gdy używany na produkt, ma na celu poinformować użytkownika o obecności izolowanego i niebezpiecznego napięcia wewnątrz obudowy produktu, który może stanowić zagrożenie porażenia prądem elektrycznym.

UWAGI: Ten symbol, , gdy używany na produkt, jest przeznaczony do ostrzegania użytkownika ważne operacyjne oraz instrukcje konserwacji (obsługi) w literaturze, wyposażone w sprzęt.

Informacji na temat wytycznych w sprawie bezpieczeństwa, regulacji wzajemnej zgodności, zgodność EMI/EMF, dostępności i Tematy pokrewne, zobacz Extron bezpieczeństwa i regulacyjnego zgodności przewodnik, część numer 68-290-01, na stronie internetowej Extron, **www.extron.com**.

Инструкция по технике безопасности • Русский

ПРЕДУПРЕЖДЕНИЕ: Данный символ, , если указан на продукте, предупреждает пользователя о наличии неизолированного опасного напряжения внутри корпуса продукта, которое может привести к поражению электрическим током.

ВНИМАНИЕ: Данный символ, , если указан на продукте, предупреждает пользователя о наличии важных инструкций по эксплуатации и обслуживанию в руководстве, прилагаемом к данному оборудованию.

Для получения информации о правилах техники безопасности, соблюдении нормативных требований, электромагнитной совместимости (ЭМП/ЭДС), возможности доступа и других вопросах см. руководство по безопасности и соблюдению нормативных требований Extron на сайте Extron: , **www.extron.com**, номер по каталогу - 68-290-01.

安全说明 • 简体中文

警告:⚠产品上的这个标志意在警告用户, 该产品机壳内有暴露的危险电压, 有触电危险。

注意: ⚠ 产品上的这个标志意在提示用户, 设备随附的用户手册中有重要的操作和维护(维修)说明。

关于我们产品的安全指南、遵循的规范、EMI/EMF 的兼容性、无障碍使用的特性等相关内容, 敬请访问 Extron 网站 , **www.extron.com** ，参见 Extron 安全规范指南，产品编号 68-290-01。

安全記事 • 繁體中文

警告:⚠ 若產品上使用此符號，是為了提醒使用者，產品機殼內存在未隔離的危險電壓，可能會導致觸電之風險。

注意 ⚠ 若產品上使用此符號，是為了提醒使用者，設備隨附的用戶手冊中有重要的操作和維護（維修）說明。

有關安全性指導方針、法規遵守、EMI/EMF 相容性、存取範圍和相關主題的詳細資訊，請瀏覽 Extron 網站:**www.extron.com**，然後參閱《Extron 安全性與法規遵守手冊》，準則編號 68-290-01。

安全上のご注意 • 日本語

警告: この記号 ⚠ が製品上に表示されている場合は、筐体内に絶縁されていない高電圧が流れ、感電の危険があることを示しています。

注意: この記号 ⚠ が製品上に表示されている場合は、本機の取扱説明書に記載されている重要な操作と保守(整備)の指示についてユーザーの注意を喚起するものです。

安全上のご注意、法規厳守、EMI/EMF適合性、その他の関連項目については、エクストロンのウェブサイト **www.extron.com** より『Extron Safety and Regulatory Compliance Guide』(P/N 68-290-01) をご覧ください。

안전 지침 • 한국어

경고: 이 기호 ⚠가 제품에 사용될 경우, 제품의 인클로저 내에 있는 접지되지 않은 위험한 전류로 인해 사용자가 감전될 위험이 있음을 경고합니다.

주의: 이 기호 ⚠가 제품에 사용될 경우, 장비와 함께 제공된 책자에 나와 있는 주요 운영 및 유지보수(정비) 지침을 경고합니다.

안전 가이드라인, 규제 준수, EMI/EMF 호환성, 접근성, 그리고 관련 항목에 대한 자세한 내용은 Extron 웹 사이트(**www.extron.com**)의 Extron 안전 및 규제 준수 안내서, 68-290-01 조항을 참조하십시오.

Copyright

© 2017-2025 Extron. All rights reserved. **www.extron.com**

Trademarks

All trademarks mentioned in this guide are the properties of their respective owners.

The following registered trademarks (®), registered service marks (℠), and trademarks (™) are the property of RGB Systems, Inc. or Extron (see the current list of trademarks on the **Terms of Use** page at **www.extron.com**):

Registered Trademarks (®)
Cable Cubby, ControlScript, CrossPoint, DTP, eBUS, EDID Manager, EDID Minder, Extron, eLink, Everlast, Flat Field, FlexOS, Glitch Free, Global Configurator, Global Scripter, GlobalViewer, Hideaway, HyperLane, IP Intercom, IP Link, Key Minder, LinkLicense, LockIt, MediaLink, MediaPort, NAV, NetPA, PlenumVault, PoleVault, PowerCage, PURE3, Quantum, ShareLink, Show Me, SoundField, SpeedMount, SpeedSwitch, StudioStation, System *Integrator*, TeamWork, TouchLink, V-Lock, VN-Matrix, VoiceLift, WallVault, WindoWall, XPA, XTP, XTP Systems, and ZipClip.
Registered Service Mark(SM) : S3 Service Support Solutions
Trademarks (™)
AAP, AFL (Accu-RATE Frame Lock), ADSP (Advanced Digital Sync Processing), AVEdge, CableCover, CDRS (Class D Ripple Suppression), Codec Connect, ConferenceShare, DDSP (Digital Display Sync Processing), DMI (Dynamic Motion Interpolation), Driver Configurator, DSP Configurator, DSP Configurator PRO, DSVP (Digital Sync Validation Processing), EQIP, FastBite, Flex55, FOX, FOXBOX, InstaWake, IP Intercom HelpDesk, MAAP, MicroDigital, Opti-Torque, PendantConnect, ProDSP, QS-FPC (QuickSwitch Front Panel Controller), Room Agent, Scope-Trigger, SIS, Simple Instruction Set, Skew-Free, SpeedNav, Triple-Action Switching, True4K, True8K, Vector™ 4K, WebShare, XTRA, and ZipCaddy

Conventions Used in this Guide

Notifications

The following notifications are used:

ATTENTION:

- Risk of property damage.
- Risque de dommages matériels.

NOTE: A note draws attention to important information.

TIP: A tip provides a suggestion to make working with the application easier.

Software Commands

NOTE: For commands and examples of computer or device responses mentioned in this guide, the character “0” is used for the number zero and “O” represents the capital letter “o.”

Computer responses and directory paths that do not have variables are written in the font shown here:

```
Reply from 208.132.180.48: bytes=32 times=2ms TTL=32
C:\Program Files\Extron
```

Variables are written in *slanted form* as shown here:

`ping` *`xxx.xxx.xxx.xxx`* `–t`

`SOH R` *`Data`* `STX` *`Command`* `ETB ETX`

Selectable items, such as menu names, menu options, buttons, tabs, and field names are written in the font shown here:

From the **`File`** menu, select **`New`**.

Click the **`OK`** button.

Extron Glossary of Terms

A glossary of terms is available at **https://www.extron.com/technology/glossary.aspx**.

Contents

Introduction 1
About this Guide 1
New Features with Room Agent 2.8.0 1
About the Room Scheduling System 1
Calendar Servers 2
Compatible Devices 2
System Benefits 3
Security Overview 3
Network Traffic 4
Application Diagram 5
Features 6
Room Agent 6
TLS Panels 7
TLSI 9
SSI 10

Software Overview 12
Using the Room Agent Software (Overview) 12
Before You Start 12
Using Room Agent 13
Designing the interface 17
Downloading Software 18
Updating Firmware 22

Menu Button 23

Manage Tab 25
Discover Panels 25
Add Panels Manually 26
MANAGE Tab Features 27
Check Box 27
Panel Status 27
Search Box 27
Device Type Filter 27
MANAGE Tab Menu Bar 28
Status Link 28
Remove Panels 28

Actions Drop-down List 29
Actions 29
Edit Settings 29
Install Firmware 36
Reboot 37
Reset 37

Configure Tab 38
View a List of Touchpanels, SSI Devices, or Wayfinding Devices and Their Properties 38
Touchpanels 38
SSI Devices 39
Wayfinding Devices 40
Create or Edit Configuration Files 40
Set up a Proxy Server 40
Before Starting 41
Setting Up the Proxy Server 41
Troubleshooting 42
Ad Astra® 44
CollegeNET 25Live® 46
EMS 48
Prerequisites 48
Creating a Web Administrator for EMS 48
EMS Setup 50
Google Calendar™ 54
Google Calendar Overview 56
Microsoft Exchange 67
Set Up a Service Account 70
Delete a Service Account 72
Edit a Service Account 72
Verify the Exchange User ID is the UPN 73
Microsoft Office 365 74
Verify the UPN 75
QR Authentication for MS Office 365 76
Oauth for Office 365 77
Use Client Secret Workflow 79
Use Certificate Upload Workflow 91
Use Device Code Workflow 102
Korbyt Booking / NFS 111
Configure Individual TLS Panels 113
Sending and Retrieving Configurations 113
Rebuilding a System Configuration File from Individual Records 114
Retrieve and Clear the Activity File 115
Retrieve a template 116
Configure Wayfinding Devices 116
Save Configuration for Wayfinding Device 119
List Format 119
Map Format 120
Associating TLS Panels with a Wayfinding Device 120

Design Tab ... 121
Design Tab for Rooms ... 121
Templates Pane ... 122
Layout Tab ... 123
Options Tab ... 124
Background Tab ... 127
Date & Time Tab ... 129
Panel Message Tab ... 130
Room Occupancy Tab ... 130
Preview Panel ... 132
Design Tab for Desk ... 134
Templates Pane ... 135
Layout Tab ... 135
Options ... 136
Background Tab ... 139
Date & Time Tab ... 140
Panel Message Tab ... 141
Preview Panel ... 141
Design Tab for Indicators (SSI) ... 145
Templates Pane ... 146
Options Tab for Indicators ... 147
Panel Access ... 147
Room Occupancy for Indicators ... 148
Design Tab for Wayfinding (List Format) ... 150
Options ... 151
Background ... 152
Date & Time ... 152
Error Message ... 153
Permissions ... 153
Preview Pane ... 154
Design Tab for Wayfinding (Map) ... 158
Layout ... 159
Map ... 160
Options ... 162
Background ... 163
Date & Time ... 164
Errors ... 165
Permissions ... 165
Preview Panel ... 165

Hardware **169**
TLS Panels 169
Setup Checklist 170
Mount and Cable All Devices 170
Set up the TouchLink Panels for Network Communication 170
Configure the TouchLink Panels 170
Mounting 171
Front Panel Features 175
Rear Panel Features 176
Connecting the Power Injector 178
Reset Modes 179
Setup Menu 179
TLSI Devices 180
Setup Checklist 180
Rear Panel Connectors and Features 181
Front Panel Features 183
Reset Modes 184
Setup Menu 184
TLSI 201 Web Page 185

Reference Information **186**
Network Port Requirements and Licensed Third-Party Software 186
Supported Languages 186
Room Scheduling Analytics 186
Downloading the Microsoft Power BI Template 186
Exporting the Activity File as the Data Source from Room Agent 187
Importing an Activity File as the Data Source 187
Retrieving an Activity File via SFTP 189
Secure Sockets Layer (SSL) Certificates 190
IEEE 802.1X Certificates 190
Certificate File Requirements 191
Private Key File Requirements 191
SNMP 192

Introduction

- About this Guide
- New Features with Room Agent 2.8.0
- About the Room Scheduling System
- Application Diagram
- Features

About this Guide

This guide provides information about the hardware and software required to install, configure, and operate the Extron Room Scheduling System.

The topics include:

- Room Agent Software
- TouchLink Scheduling panels (TLS)
- Wayfinding device (TLSI)
- System Status Indicator (SSI)

New Features with Room Agent 2.8.0

Room Agent 2.8 supports Extron System Status Indicators. These devices may also be referred to as SSI devices or Indicators in this help file.

About the Room Scheduling System

The Extron Room Agent system consists of the software (Room Agent) and the hardware on which it runs (TLS panels and TLSI devices). A list of **Compatible Devices** is on the following page.

When the system is running, conference rooms are booked in advance through any of the available calendar systems. A list of available **Calendar Servers** is on the following page.

The touchpanel outside the conference room displays the schedule for that conference room for the next three hours. If the conference room is not booked at any point during the next three hours, users can schedule a "walk-up" ad hoc meeting during the free time.

The Room Agent configuration program is available for download from the Extron website (see **Downloading Software** on page 18 for more information). The program allows a system administrator to integrate and configure all the touchpanels in the system, which can vary in size from one to thousands of panels. The system configurations can be saved and the individual configuration file for each touchpanel can be saved on that touchpanel. If required, the configuration files from all the individual touchpanels can be pulled back to the control PC to rebuild the system configuration file.

Wayfinding devices collate information from all the TLS panels in the system. This allows room availability to be viewed and rooms to be booked from a single centralized location. It is ideal for use in high traffic areas, including building lobbies, meeting room hallways, and corridors.

Calendar Servers

The Room Agent software interfaces with the following calendar servers to provide scheduling capabilities for all the conference rooms in the system.

- Ad Astra®
- CollegeNET 25Live®
- EMS Software™
- Google™ Calendar™
- Microsoft® Exchange™
- Microsoft Office 365™
- Korbyt Booking / NFS Technology

NOTE: Our Room Scheduling devices are capable of integrating with additional Scheduling Services. Contact Extron for further details.

Compatible Devices

As of June 2021, Extron recommends the following TLS panels for use with the Room Agent software. These models ship with the latest firmware for the scheduling system. No firmware update is required.

Check with **www.extron.com** to see a list of the latest recommended TLS panels.

- **TLS 300M** — A 3.5-inch (measured diagonally), wall-mounted panel with a 320x480 resolution. See the *TLP Pro 300M and TLS 300M User Guide* for complete information about the product, including mounting options.
- **TLS 525M** — A 5-inch wall-mounted panel with an 800x480 capacitive glass touchscreen. See the *TLP Pro 525, 725, and 1025 Series User Guide* for complete information about the product, including mounting options.
- **TLS 725M** — A 7-inch, wall-mounted panel with an 1024x600 capacitive glass touchscreen. See the *TLP Pro 525, 725, and 1025 Series User Guide* for complete information about the product, including mounting options.
- **TLS 1025M** — A 10-inch, wall-mounted panel with a 1280x800 capacitive touchscreen. See the *TLP Pro 525, 725, and 1025 Series User Guide* for complete information about the product, including mounting options.
- **TLSI 201** — An Interactive Wayfinding Interface that collates information from all the TLS panels in the system. This information is displayed on a large third-party display screen, which allows room availability to be viewed and rooms to be booked from a single centralized location. The interface supports resolutions up to 4K. See the *TLSI 201 User Guide* for complete information about the product.
- **SSI Indicator devices** — Room Agent software works with SSI Indicator devices, either as standalone devices or in conjunction with TLS panels and TLSI devices.

For information about mounting and basic setup for these panels, see **Hardware** on page 169. More detailed information is available in the user guide for the corresponding touchpanel.

Unlike other applications that use Extron touchpanels, there are no controllers to be configured.

The panels do not require complicated setup or programming. Users can book a room from any device connected to the room calendar, including their mobile devices, a connected panel, or a Wayfinding device.

All panels can receive power and communication over a single Ethernet cable. Power over Ethernet (PoE) eliminates the need for a local power supply. PoE requires a PoE injector, which is sold separately.

Room Agent software, installed on a computer with network access, allows system administrators to set up the Extron TouchLink Scheduling panels as room scheduling appliances by filling in the required fields that correspond with areas of the user interface. Customization options allow a variety of fields to be shown or hidden, depending on user preference.

Booking a room from the panel is as easy as tapping the **Reserve** button on the panel. The intuitive interface also provides at-a-glance room availability and a timeline view of the status of the room (see **figure 1** on page 3). The TLS 525M, 725M, and 1025M show a timeline of half a day (four hours). The TLS 300M timeline is a full day.

In addition to the customizable panel interface, bright LEDs within the bezel provide at-a-glance room availability status from a distance.

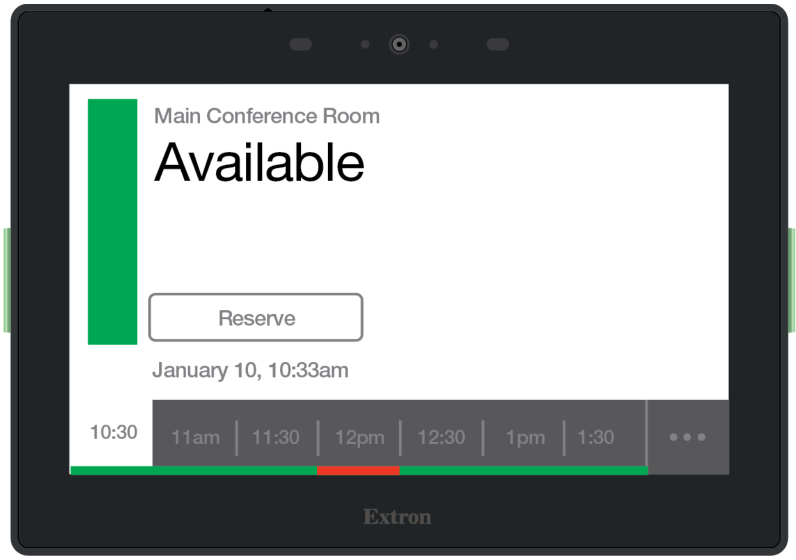


Figure 1. Typical Room Display on a TLS 725M Scheduling Panel

System Benefits

The Room Scheduling System can be integrated into any network and requires minimal network bandwidth for communication between each panel and the room calendar server. Benefits of being room calendar server clients, communicating directly with the room calendar server, include:

- **Ensures the security of information** — Each panel maintains a separate connection to a dedicated resource calendar that is assigned to the room associated with the panel through 25Live, EMS, Google Calendar, Microsoft Exchange, Office 365, and Rendezvous by NFS. Each resource calendar has a unique username and password that the panel uses to connect to the server. Administrators can manage the information of each room scheduling panel using tools, accounts, and privileges provided by their scheduling calendar console.
- **Simplifies system management** — This direct communication simplifies user access management for the administrator, and does not require any middleware or additional products to be placed on the network.
- **Eliminates a single point of failure** — The Room Scheduling System requires no middleware or intermediate server between the panels and the calendar server, eliminating the possibility of a single point of failure.

Security Overview

- All communications between the Room Agent software and the panels, between the Wayfinding devices and the TLS panels, and between the panels and the calendar room server are encrypted.
- When you are using the Room Agent Software to configure the panels, all communications between the software and the touchpanels are encrypted.

- Each conference room is assigned a unique room mailbox. This mailbox is restricted so that it cannot be used for interactive log-ons (the ability to send or receive e-mail).
- As part of the Room Agent software configuration process, the administrator enters the authentication information for each room. These values are sent as part of the configuration file to the panel. No other user ids or passwords are used.
- The software encrypts the account data. If a password is displayed on the user interface it is obscured, and any sensitive information is encrypted when stored on the administrator PC.
- Administrators can choose to save the panel configurations, including the account credentials, on their PCs in a password-protected file.

  NOTE: The protected configuration files include the authentication data for each account. Use discretion when allowing access to these files.

- All panels are password protected. The factory configured passwords for all accounts on this device have been set to the device serial number. Passwords are case sensitive.

  NOTE: If the device is reset to default settings, the password is the default password configuration. The default password is `extron` (for either admin or user).

- During configuration, there is an opportunity to change the password and Extron strongly recommends that you do.

Network Traffic

The traffic generated on the network consists of requests for data and responses from the room calendar server. Communications occur at regular intervals, such as when requesting meetings, sending meeting invitations, or when administrators retrieve an activity file for a room from the panel. Panel configuration, typically completed once during the initial setup of the system, also produces traffic on the network. The panel provides options to create an ad hoc meeting, extend a meeting, end a meeting, and confirm a meeting using the **`Check-In`** button, provided that these options were made available to the user when the administrator configured the panel.

Application Diagram

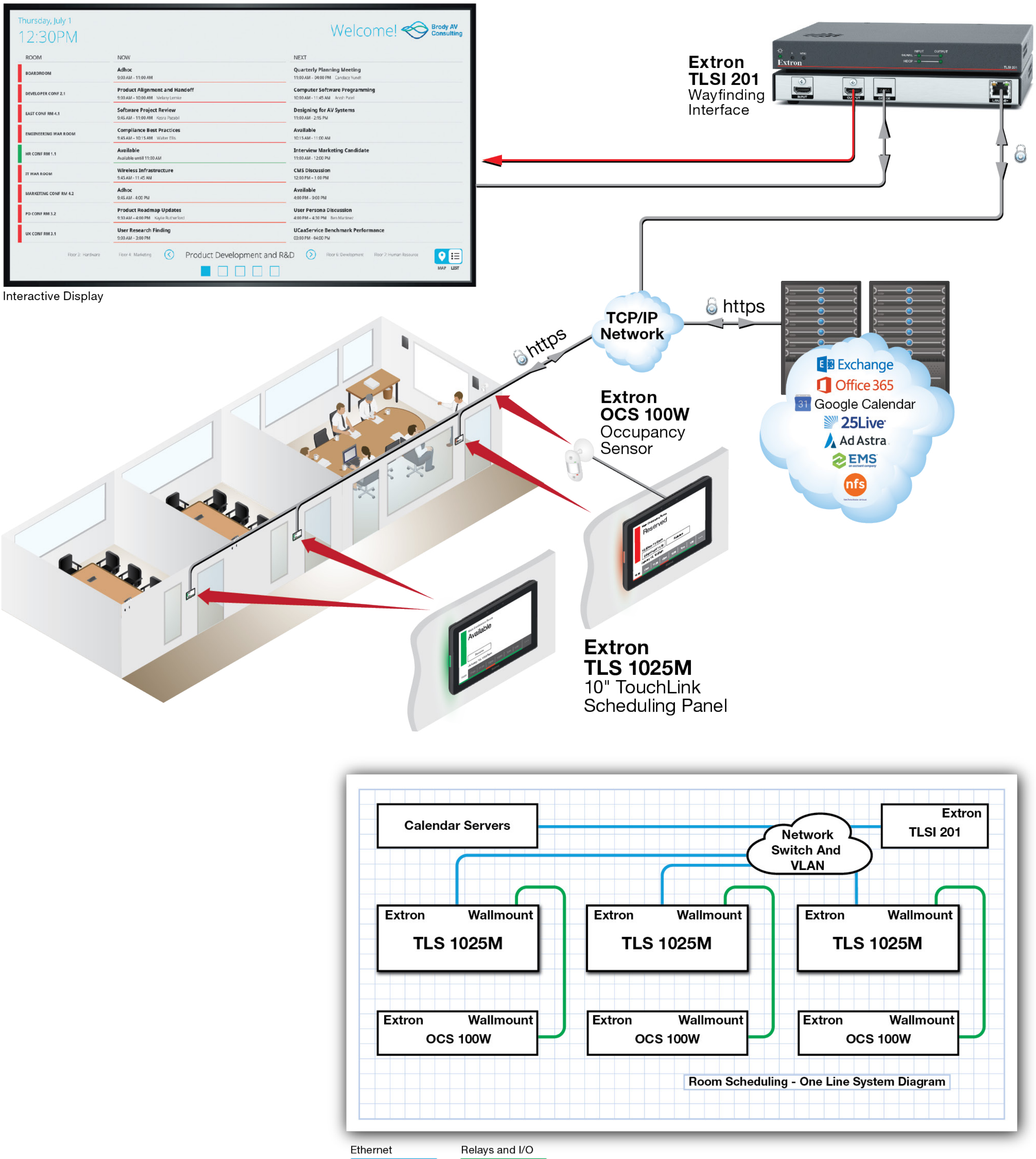


Figure 2. Typical Extron Room Scheduling System Application

Features

Room Agent

- **Make on-demand reservations from the touchpanel, computer, or any smartphone or tablet that connects to Microsoft® Exchange and Office 365®, Google Calendar™, 25Live®, EMS, NFS, and Ad Astra®.**
- **25Live dropdown selection** — A dropdown selection for 25Live allows 25Live users to set a Meeting Event Title.
- **Microsoft 365 GCC High support** — TLS panels support Microsoft Government Community Cloud High (GCC High) calendaring functionality.
- **Supports TLS 300M Desk Scheduling Touchpanel** — Provides at-a-glance space availability for individual workspaces and flexible spaces
- **Supports TLSI 201 Interactive Wayfinding Interface to provide real-time meeting space availability, status, and location information using a centralized display.**
- **Support for SSI 100 System Status Indicator** — Room Agent supports the SSI 100 device in calendaring mode.
- **Supports 27 languages** — Multi-language support now allows TLS panel and TLSI Interactive Wayfinding users the option to:
  - **Display up to 2 languages simultaneously (for example display both English and Canadian French translations on the TLS panel user interface).**
  - **Display multiple languages, one at a time.**
  - **Room Agent software fully translated into Simplified Chinese.**

  (For a list of supported languages, see Supported Languages on page 149.)
- **Ability to download a room Activity File without using Room Agent** — Users can now retrieve the activity file without the need of Room Agent by connecting to the TLS using an SFTP client.
- **Deploy a single touchpanel, or multiple touchpanels with similar settings very easily**
- **Ability to push firmware to a single panel or multiple panels, simultaneously**
- **Room usage data provides insight into trends and activity** — Each touchpanel includes a downloadable Scheduling Activity file that enables you to generate analytics on usage, activity patterns, and trends using data from across the enterprise or organization.
- **View and edit network adaptor information in Room Agent** — Users can now view network adaptor information via the `Manage` tab in Room Agent software.
- **Provides service account and impersonation support** — Touchpanels can be configured using a service account with Microsoft Exchange or 365, simplifying administrative tasks.
- **Supports two factor authentication (OAuth) required for Microsoft 365.**
- **Alternative Microsoft 365 authentication options** — Administrators have Microsoft 365 authentication options using either Client Secret or Certificate Upload methods in Room Agent for extended TLS Panel - Server connection. These workflows are supported for the TLS 300M and the TLS x25 devices and require MSGraph Application permissions in Microsoft Azure.
- **QR Code Booking Support for Microsoft 365 and Google Calendars** — Users can leverage this feature to authenticate themselves to a TLS panel, then reserve, extend, check-in, and release meetings at the TLS panel by scanning a QR code for Microsoft 365 or Google calendars. Meeting organizers will have editing permissions exclusively for their own meetings.
- **NTLMv2 Authentication Support** – TLS panels now include support for NTLMv2 with extended protection.
- **Support for 802.1X certification on TLS panels, which can be managed via Extron Toolbelt software.**

- **Support for expanded ControlScript Calendar API functionality for Room Scheduling Devices** — The TLS firmware can interface with IPCP Pro xi and IPCP Pro Qxi Control Processors running ControlScript Pro xi v1.5.3 and later. Room Agent v2.4.3 or later is required. See the Demo and Demo Documentation for the ControlScript Sample Project for incorporating the RoomSchedulingInterface library into ControlScript projects.
- **Perform specific commands using the GC Plus TLS Driver** — Perform room scheduling functions such as reserve or check in, extend, and release a scheduled meeting using the GC Plus TLS Driver. For a complete list of functions, refer to the System Templates section for the communications sheet.
- **SSH update** — SSH v9.8 is supported on both the TLS x25 and TLS 300 panels.
- **Make meeting rooms available as soon as a scheduled meeting ends.**
- **Check-In Button confirms attendance for the scheduled meeting and retains the reserved status of the room, even if the start of the meeting is delayed**
- **Microsoft Exchange and 365 auto-discovery streamlines system setup.**
- **Two color themes, custom loaded background images, and transparency controls provide personalized branding options.**
- **Customizable date and time formats with a preview showing how the UI will look on the touchpanel.**
- **View details of the meetings scheduled for the day.**
- **Customizable room availability hours** — Allows one to select the start and end times for the availability of a room.
- **Meetings scheduled as private will, by default, have the meeting details hidden for meetings scheduled with Microsoft Exchange, 365, and Google Calendar.**
- **Display up to 50 characters from the meeting body details for panels configured with Microsoft Exchange and 365** — The TLS can display up to 50 characters from the meeting body for any selected custom dropdown.
- **Meeting Subject Line accommodates up to 2 lines of text.**
- **No annual subscription or maintenance fees.**
- **Ability to view meeting attendees for panels configured with Microsoft Office 365, Exchange, and Google.**
- **View upcoming meeting via TLS panel** — Users can now view the next upcoming meeting via the TLS panel user interface.
- **Ability to set or view room capacity via TLS panel** — Users can now set/view the room capacity via the TLS panel user interface. Users can also view details of the meetings scheduled for the day.
- **Ability to “Search Domains” via communication settings for TLS and TLSI devices** — Users can now search for a specific domain in Room Agent software.
- **PIN access for TLS panels configured with Microsoft Office 365, Exchange, Google, and 25Live, enabling users to reserve, book, check-in and extend a meeting via a PIN (English Only).**

TLS Panels

- **TLS panels have capacitive edge-to-edge glass touchscreen and come in four sizes:**
  - **3.5 inch touchscreen with 320x480 resolution.**
  - **5 inch touchscreen with 800x480 resolution.**
  - **7 inch touchscreen with 1024x600 resolution.**
  - **10 inch touchscreen with 1280x800 resolution.**
- **Gorilla Glass® screen is tough, scratch, and smudge-resistant** — Corning Gorilla Glass is stronger and more scratch-resistant than standard glass, while maintaining touch sensitivity, color saturation, and brightness.
- **All panel updates are conveniently handled through Room Agent.**

- **Easily deploy and make updates to one or more touchpanels** — Using Room Agent software, copy and modify the settings to add additional touchpanels, update a single touchpanel, or make bulk updates.
- **Make on-demand reservations from the touchpanel, computer, or any smartphone or tablet that connects to Microsoft® Exchange, Office 365™, Google Calendar™, 25Live®, EMS, NFS, and Ad Astra®**
- **25Live dropdown selection** — A dropdown selection for 25Live allows 25Live users to set a Meeting Event Title.
- **Supports OAuth 2.0 required for Microsoft 365** — Allows use of a convenient single set of credentials to deliver secure, user-friendly authentication.
- **Alternative Microsoft 365 authentication options** — Administrators have Microsoft 365 authentication options using either Client Secret or Certificate Upload methods in Room Agent for extended TLS Panel - Server connection. These workflows require MSGraph Application permissions in Microsoft Azure.
- **Microsoft 365 GCC High support** — TLS panels now support Microsoft's Government Community Cloud High (GCC High) calendaring functionality.
- **NTLMv2 Authentication Support** — NTLMv2 Authentication Support – TLS panels now include support for NTLMv2 with extended protection.
- **Support for 802.1X certification on TLS panels, which can be managed via Extron's Toolbelt software**
- **SSH update** — SSH v9.8 is supported on both the TLS x25 and TLS 300 panels.
- **QR Code Booking Support for Microsoft 365 and Google Calendars** — Users can leverage this feature to authenticate themselves to a TLS panel, then reserve, extend, check-in, and release meetings at the TLS panel by scanning a QR code for Microsoft 365 or Google calendars. Meeting organizers will have editing permissions exclusively for their own meetings.
- **Microsoft Exchange auto-discovery** — Streamlines system set up and makes it easy for your client application to configure itself with minimal user input.
- **Provides service account and impersonation support** — TLS panels can be configured using a service account with Exchange or Office 365, simplifying administrative tasks.
- **Perform specific commands using the GC Plus TLS Driver** — Perform room scheduling functions such as reserve or check in, extend, and release a scheduled meeting using the GC Plus TLS Driver. For a complete list of functions, refer to the System Templates section for the communications sheet.
- **Real-time calendar updates and synchronization** — Ensures accurate and up-to-date information for efficient use of shared spaces, preventing scheduling conflicts.
- **Meetings scheduled as private will by default have the meeting details hidden for meetings scheduled with Microsoft Exchange, Office 365, and Google Calendar.**
- **Ability to view meeting attendees for panels configured with Microsoft 365, Exchange, and Google.**
- **All communication between the touchpanel and calendar server is encrypted and secure.**
- **Support for expanded ControlScript Calendar API functionality for Room Scheduling Devices** — The TLS firmware can interface with IPCP Pro xi and IPCP Pro Qxi Control Processors running ControlScript Pro xi v1.5.3 and later. Room Agent v2.4.3 or later is required. See the Demo and Demo Documentation for the ControlScript Sample Project for incorporating the RoomSchedulingInterface library into ControlScript projects.
- **Digital input allows connection to an occupancy sensor, such as the Extron OCS 100.**
- **Ability to set or view room capacity via TLS panel** — Users can now view the next upcoming meeting via the TLS panel user interface.
- **Check-In Button confirms attendance for the scheduled meeting and retains the reserved status of the room, even if the start of the meeting is delayed.**
- **PIN access for TLS panels configured with Microsoft 365, Exchange, Google, and 25Live, enabling users to reserve, book, check-in and extend a meeting via a PIN (English Only)**
- **Two color themes, custom loaded background images, and transparency controls provide personalized branding options** — Customizable layouts using the free Room Agent software feature a preview of color themes, custom background image, logo, and opacity.

- **Customizable date and time formats with a preview showing how the UI will look on the touchpanel.**
- **Customizable room availability hours** — Allows one to select the start and end times for the availability of a room.
- **Make meeting rooms available as soon as a scheduled meeting ends**
- **View the complete day's reservations and availability** — Allows for planning efficiency and usability.
- **Room usage data provides insight into trends and activity** — Each touchpanel includes a downloadable Scheduling Activity file that enables you to generate analytics on usage, activity patterns, and trends using data from across the enterprise or organization.
- **Display up to 50 characters from the meeting body details for panels configured with Microsoft Exchange and Office 365** — The TLS can display up to 50 characters from the meeting body for any selected custom dropdown.
- **Meeting Subject Line accommodates up to 2 lines of text.**
- **Two bright LED lights make it easy to see if a room is occupied or available even from down the hall.**
- **Rear-facing light bars reflect off the mounting surface providing enhanced visibility of room status (TLS 725 and 1025 only).**
- **Power over Ethernet** — PoE allows the TLS panel to receive power and communication over a single Ethernet cable, eliminating the need for a local power supply.
- **A variety of mounting options available** — See the product page for each touchpanel for a list of compatible mounting kits.

TLSI

- **Find and book a meeting space for current day or week from a centralized location.**
- **Easily navigate real-time information on a landscape or portrait display using a dual view list layout and customer-provided map.**
- **Connects directly with TouchLink scheduling panels.**
- **Configurable with free Room Agent software.**
- **Ideal for use with third-party screens 40 inches or larger and up to 4K resolution.**
- **Set screen transition times** — Users of the Wayfinding Interface can specify screen transition durations via Room Agent.
- **Ability to view meeting attendees via Wayfinding (TLSI) device for rooms configured with Microsoft 365, Exchange, and Google.**
- **Ability to view room capacity via Wayfinding (TLSI) device.**
- **Support for SSI 100 System Status Indicator** — The TLSI 201 Wayfinding Interface supports the SSI 100 device in calendaring mode.
- **Requires no additional programming or external processors.**
- **PoE+ compatible** — Product is powered directly by a PoE+ switch or injector, eliminating the need for bulky local power supplies.
- **One high speed USB 2.0 port for third-party touchscreens or HID support.**
- **Simple customization options including logo, personalized message, and color themes.**
- **Flexible meeting information fields can be turned on or off as needed.**
- **Compact 1 inch high, half rack width low profile metal enclosure allows discreet installation behind a flat panel display.**

SSI

- **Multi-color real-time illuminated status from a distance** — Users can get a visual indication of room occupancy, activity, safety protocols, and dozens of other applications, with no disruption to the workflow.
- **Configurable multi-color backlighting** — The two-sided acrylic lens, combined with multi-color backlighting, blends simplicity with architectural appeal.
- **Custom engravable to identify a space** — An optional lens can be used to brand a space using text, font, and size options or an engraved logo. Supports 27 languages. For a complete list of the supported languages, refer to the Description.
- **Ceiling and wall mount options** — Choose the right mount for your space to fit a variety of environments without disrupting aesthetics.
- **Supports three modes of operation** —
    - **Digital Input Mode uses 1 digital input port** – Using Digital Input mode, 2 colors (green and red) signal when the space is available or occupied.
    - **Calendar Mode** – Using Calendar mode, 2 colors (green and red) signal when the space is available or occupied.
    - **SPD Mode** – Using SPD mode, the SSI 100 can be configured via GCP or CSDU software to communicate room status. This mode supports an array of up to 16.7 million RGB colors defined in hex.
- **Ideal for a variety of environments** — The SSI 100 can be used in a broad range of environments including studios, esports facilities, hot desking areas, meeting rooms, labs, instructional spaces, and command and control centers.
- **Functions in standalone applications** — The SSI 100 indicates room status using an occupancy sensor without the need for additional software or other Extron products.
- **Use Extron control for custom functionality** — In Secure Platform Device (SPD) mode, configure colors to fade in and out, alternate, or blink on and off.
- **Complements Room Scheduling products** — For Extron Room Scheduling and Wayfinding users, the engraved, illuminated SSI 100 adds further value by displaying room names and the status in bright red or green. Scheduling is streamlined with direct calendar server communication, using Room Agent software. Customers can also use the SSI 100 in Calendar Mode with the Wayfinding interface, eliminating the need for a separate TouchLink Scheduling panel.
- **Room usage data provides insights into trends and activity** — When using Room Agent software, generate a downloadable Scheduling Activity file to generate analytics on usage, activity patterns, and trends using data from across the Enterprise.
- **Communication between the SSI and calendar server is secure** — Encrypted communication protects sensitive usage data and reduces the risk of unauthorized access.
- **Powered via PoE or locally via optional power supply** — PoE allows the SSI 100 to receive power and communicate over a single Ethernet cable. Power locally via optional 12V power supply.
- **Two configurable digital inputs** — The SSI 100 can connect to occupancy sensors and to Extron control for visual indication of a room status.
- **Power Input Port Mode** — This ensures the SSI 100 functions if the PoE system should fail, providing redundancy and a back-up power source.
- **Power Output Port Application** — This supports the ability to supply power to multiple devices, such as occupancy sensors.
- **Utilizes LED technology for borders, text, and logo** — The SSI 100 indicators ensure easy visibility from a distance. LED technology offers lower power consumption and environmental friendliness.
- **Available in white with a paintable cover to fit with any decor.**
- **Wall Mountable** — The Wall Indicator installs in a 1 gang junction box or with included mud ring, screws and cover plate. Refer to the User Manual for additional information.

- **Ceiling Mountable** — The Ceiling Indicator installs in a 4 inch square U.S. junction box with 1 gang reducer cover plate or with 1-gang included mud ring. Supports optional seismic cable. Refer to the User Manual for additional information.
- **PoE injector sold separately.**
- **3 years parts and labor warranty.**

Software Overview

This section provides an overview of how to use the Room Agent software and describes how to download software and firmware.

- **Using the Room Agent Software (Overview)**
- **Downloading Software**
- **Updating Firmware**

Using the Room Agent Software (Overview)

Before You Start

TLS, TLSI, and SSI devices should be mounted and connected to the network.

Obtain the following network information for all your devices:

- **DHCP status** — (on or off). If DHCP is off, you must also obtain:
  - **IP address**
  - **Subnet mask**
  - **Gateway**
- **User name** — This can be either `admin` or `user`.
- **Password** — The factory configured passwords for all accounts on this device have been set to the device serial number. Passwords can be changed during configuration. Passwords are case sensitive.

  NOTE: If the device is reset to default settings, the password is the default password configuration. The default password is `extron` (for both `admin` or `user`).
- Make a note of the Touchpanel **MAC address**, which can be found on a rear-panel label.
- Download and install Room Agent and Toolbelt on the control PC (see **Downloading Software** on page 18).

SSL security certificates and IEEE 802.1X authentication — TLS panels come with a factory-installed Secure Sockets Layer (SSL) security certificate. IEEE 802.1X authentication is also supported once enabled. See **Secure Sockets Layer (SSL) Certificates** on page 190 or see **IEEE 802.1X Certificates** on page 190 for more information.

Minimum system requirements

To configure the system, you must download the Room Agent software onto a PC that has the following minimum requirements:

- **CPU** — Intel® Core 2 Duo or equivalent processor
- **Operating System** — Windows® 10 or Windows 11
- **Memory** — 4 GB of RAM
- **Hard disk space** — 500 MB of available hard disk space
- **Display Resolution** — 1280 x 768 minimum
- **Network connection** — A data transfer rate of 10 Mbps. Recommended: 100 Mbps
- **Microsoft .NET Framework 4.8**

Using Room Agent

Application Licensing

When Room Agent is started, or after log-out from a previous session, the `Application Licensing` dialog box opens.

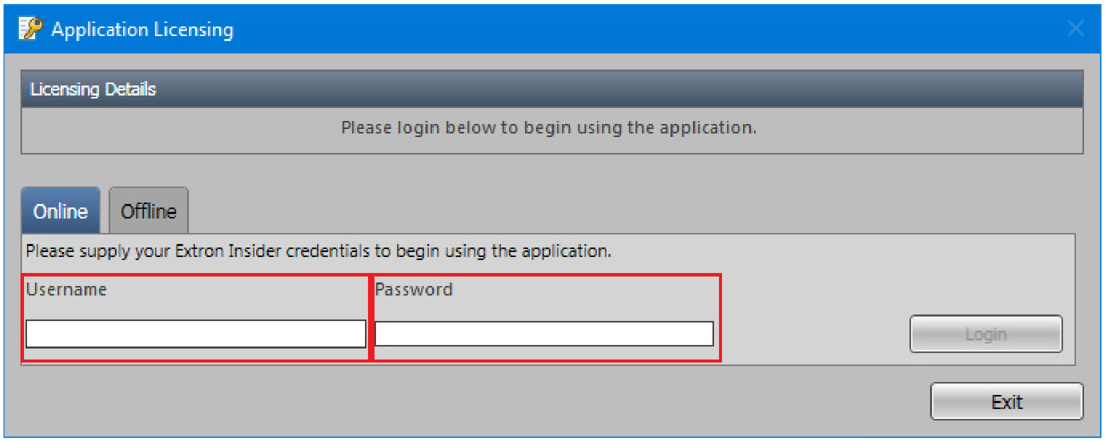


Figure 3. Log in to Room Agent

To attain full functionality, enter your Extron Insider `Username` and `Password` in the appropriate fields and click **`Login`**. When verified, the application can be run with full functionality.

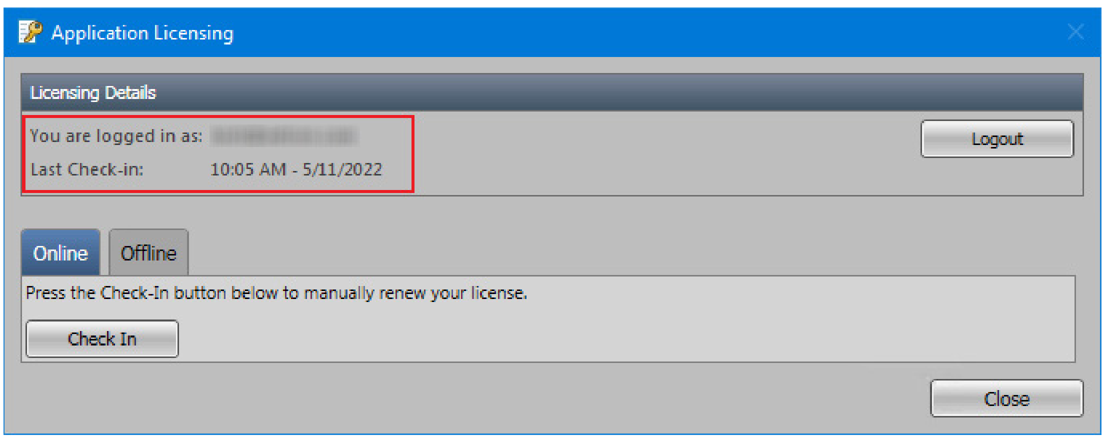


Figure 4. Check in to Room Agent

When a user is logged in, the `Licensing Details` shown are:

- Username (blurred out in figure 4)
- Date of last check-in

Click **`Check In`** to renew the license.

Click **`Close`** to close the dialog and start working with Room Agent.

Alternatively, if you are not online, and are unable to link directly to a network, click on the **Offline** tab.

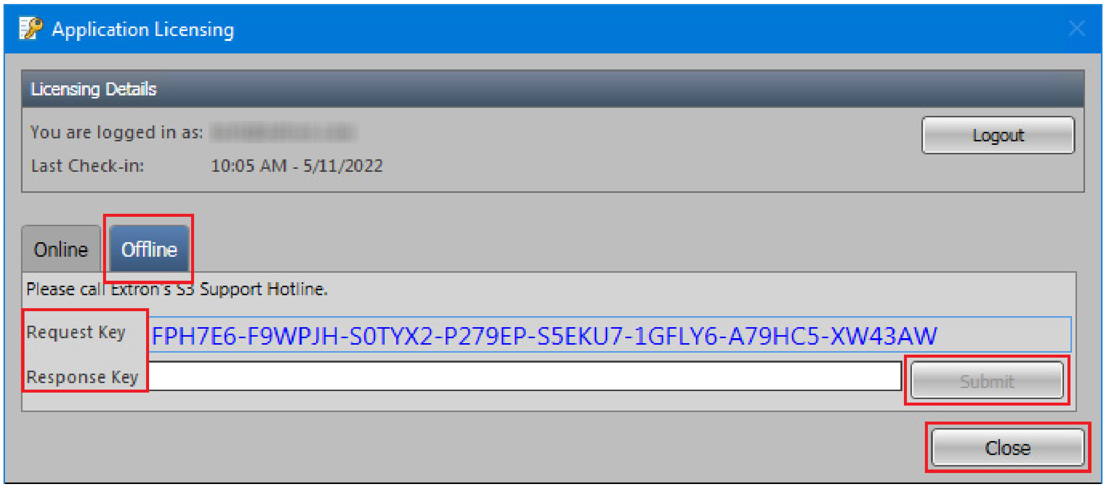


Figure 5. Application Licensing Offline

An auto generated `Request Key` is given. Follow the instructions given in the dialog box to obtain a response key and click **Submit** to activate to full functionality.

Click **Close** to close the window and begin using Room Agent.

The user can log out from the session, which removes the saved credentials (`Username` and `Password`). If a user logs out a confirmation dialog box opens.

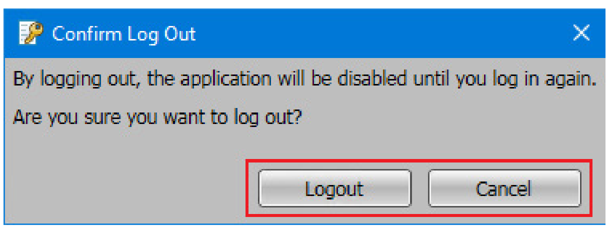


Figure 6. Confirm Log Out Dialog

To log out and exit the application, click **Logout** in the `Confirm Log Out` dialog box.

Click **Cancel** to keep the session open.

Discovering devices

1. Open Room Agent. By default, the program opens with the **MANAGE** tab selected. If required, select the **MANAGE** tab. For complete information, see **Manage Tab** on page 25.

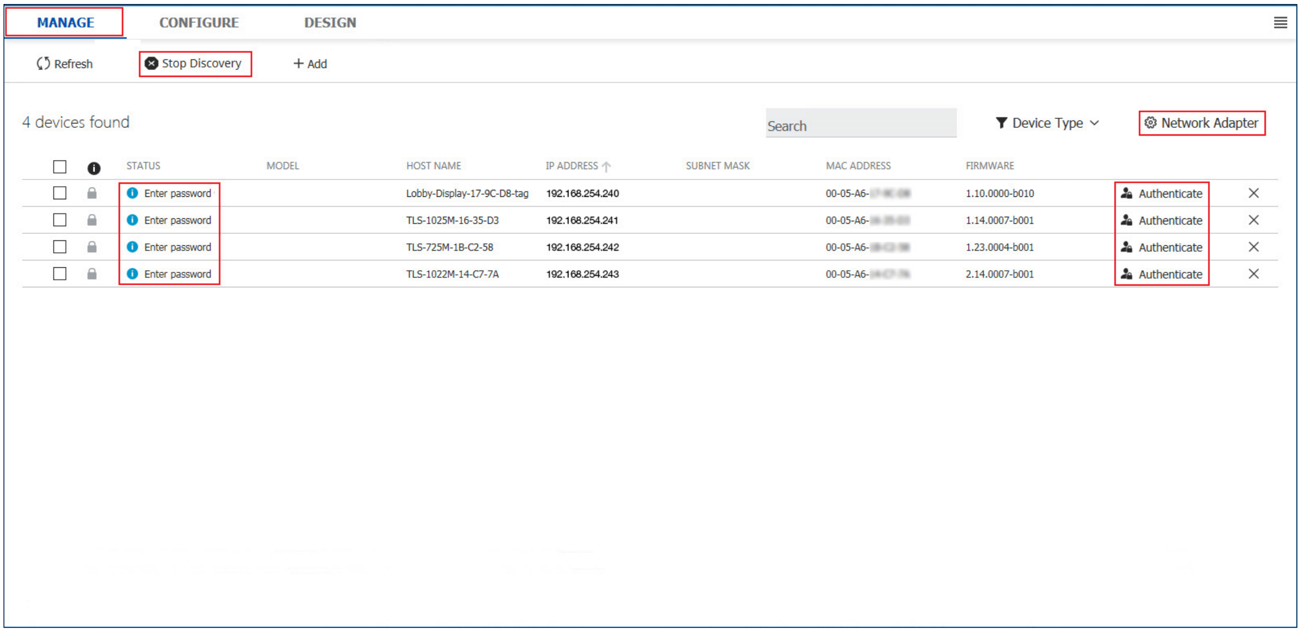


Figure 7. MANAGE Tab

2. Click **`Discover`**. The button text changes to `Stop Discovery`.

   A list of devices that are available on the same subnet as the PC is shown.

   NOTES:
   - After clicking **`Discover`**, the discovery process continues until you click **`Stop Discovery`**.
   - The discovery process find all devices on the subnet that could be used by Room Agent, even if they have another function.

3. If required, click **`Network Adapter`** to search a different sub-network.

   Any new devices that have been discovered are added to the list.

4. Repeat step 3 with additional sub-networks, as required.
5. Click **`Authenticate`** for one of the devices.
6. Enter the password for that device. Once the device has been authenticated, the **`Authenticate`** button is replaced by an `Actions` menu and the `Enter Password status` is replaced by the message `Ready`.
7. Repeat steps 5 and 6 to authenticate all required devices.

Device configuration

1. Once all the touchpanels are set up, click **`CONFIGURE`** to open the `CONFIGURE` tab.

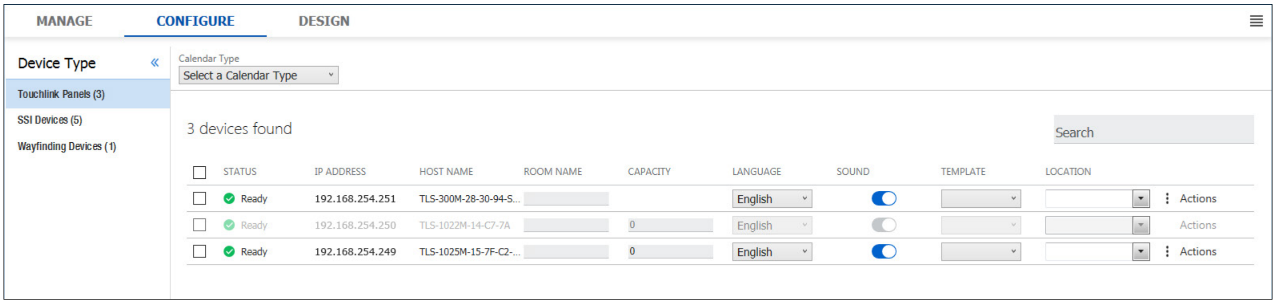


Figure 8. CONFIGURE Tab (TouchLink Panels)

2. Select **`TouchLink Panels`** or **`Wayfinding Device`**. Figure 8 shows **`TouchLink Panels`** selected.
3. Select the **`STATUS`** checkbox for one or more TLS panels.
4. Select a **`Calendar Type`**.

   The column headings change, depending on the calendar type selected. Figure 8 shows the **`NFS`** calendar selected.
5. Assign a **`LOCATION`** to the TLS panel. This allows the touchpanel to be linked to a wayfinding device.
6. If required, repeat steps 4 and 5 to select a new group of panels and associate them with a different calendar server.
7. Select the **`Wayfinding Devices`** button in the top left corner of the screen.

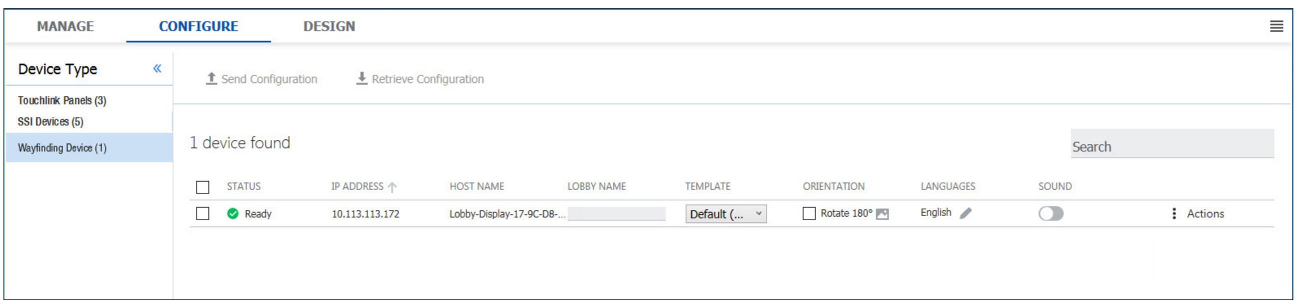


Figure 9. CONFIGURE Tab (Wayfinding Devices)

For detailed instructions about configuring touchpanels and wayfinding devices, and saving the configurations, see **Configure Tab** on page 38.

Designing the interface

Click **DESIGN**.

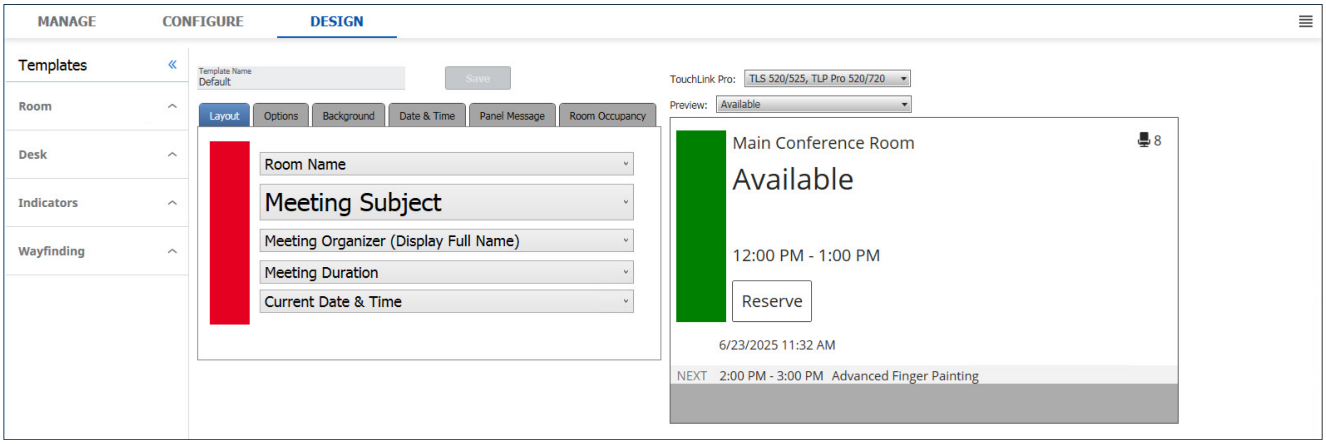


Figure 10. DESIGN Tab

The **DESIGN** tab is used to determine how information is presented on the TLS panels and on the Wayfinding devices. Figure 10 shows the **DESIGN** tab for the TLS panels.

The information shown on Wayfinding devices can be presented as a list or as a map. Choose the template that meets your need from the menu on the left side of the screen.

After modifying the design, you can overwrite an existing template or save the template with a new name.

For more detailed instructions about using the **DESIGN** tab, see **Design Tab** on page 121.

Downloading Software

The Extron Room Scheduling System requires you to install both the Room Agent software and Toolbelt software on a control PC.

This software must be downloaded from the Extron website (**www.extron.com**). You need an Extron Insider account to download either program. If you need to set up an account, contact your Extron sales representative.

To download Room Agent or Toolbelt, follow these instructions:

1. Open the Extron website in your browser.

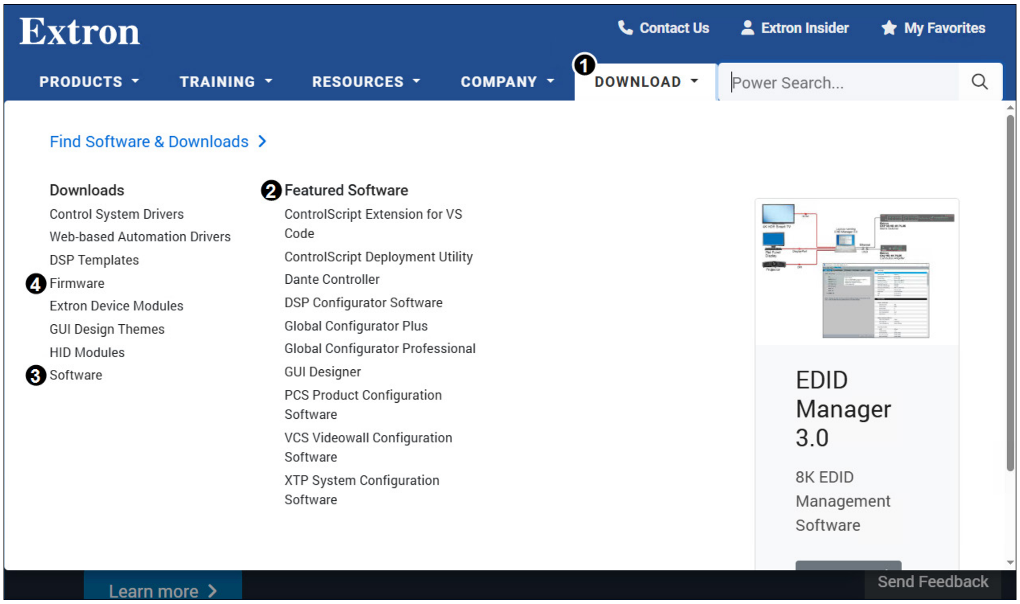


Figure 11. Download from the Extron Page

2. Click the **`DOWNLOAD`** tab in the top menu bar.

3. Check to see if the software you want is in the `Featured Software` list (❷). If it is, click on the name and the link takes you to the product page for that software.

4. Click on the **`Download`** button on that page and follow the instructions from step 8 onwards. If your software is not in the `Featured Software` list, click **`Software`** in the `Downloads` list (3).

NOTE: To download firmware, click **`Firmware`** in the `Downloads` list (❹) and follow steps 5-7, on the next page. To install firmware, see **Updating Firmware** on page 22.

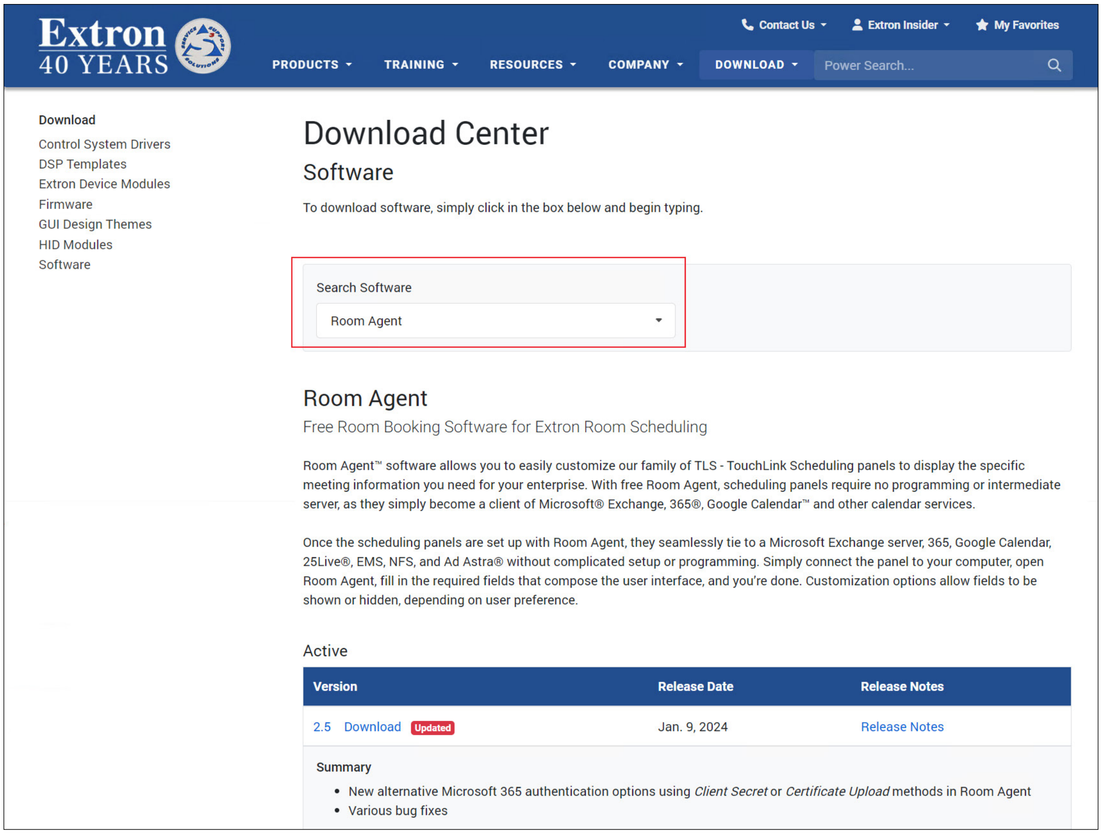


Figure 12. Find Room Agent for Download

5. Start typing the name of the software in the text box.

   When you have entered enough characters, the name is auto-filled.

6. Click on the software name.

   A description of the software and a **`Download`** button are shown.

   Figure 12 shows **`Room Agent`** selected. The procedure is the same for Toolbelt.

7. Click the **`Download`** link at the bottom of the page.

8. Provide the information requested and follow the instructions on the screen. Note where the downloaded file is stored.

9. Navigate to the folder where the downloaded file was stored and click the **`Install`** icon. The InstallShield Wizard opens at the `Welcome` page.

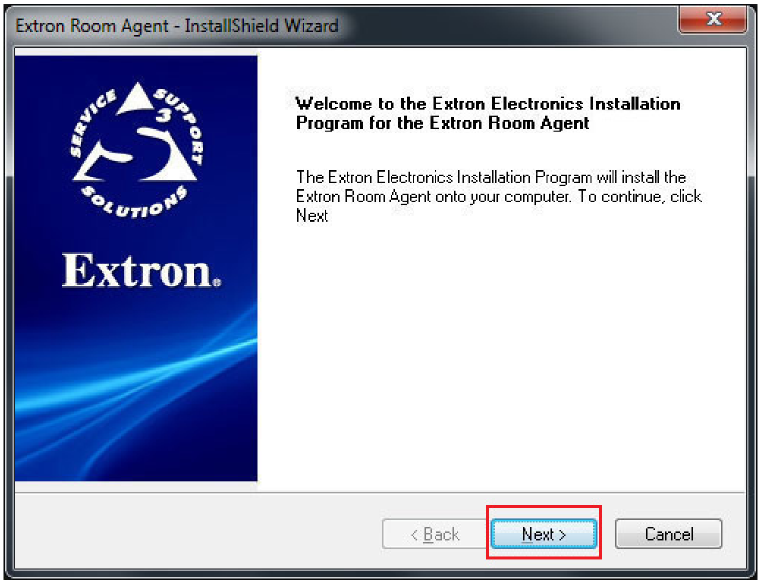


Figure 13. Start Room Agent Download

10. Click **`Next >`**.

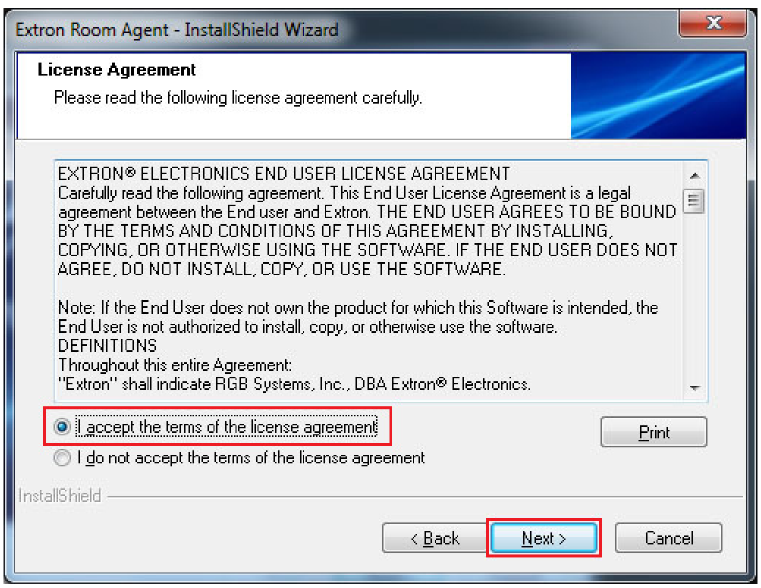


Figure 14. Accept license Agreement

11. Read the license agreement and print it (if desired).
12. Select the **`I accept the terms of the license agreement`** button.
13. Click **`Next >`**. You are prompted to save the software in the default folder. The default folder for Room Agent is `C:\Program Files (x86)\Extron\Extron Room Agent`.
14. If you want to install the program at another location, click **`Browse`** and select a different destination folder.
15. Click **`Next >`**.

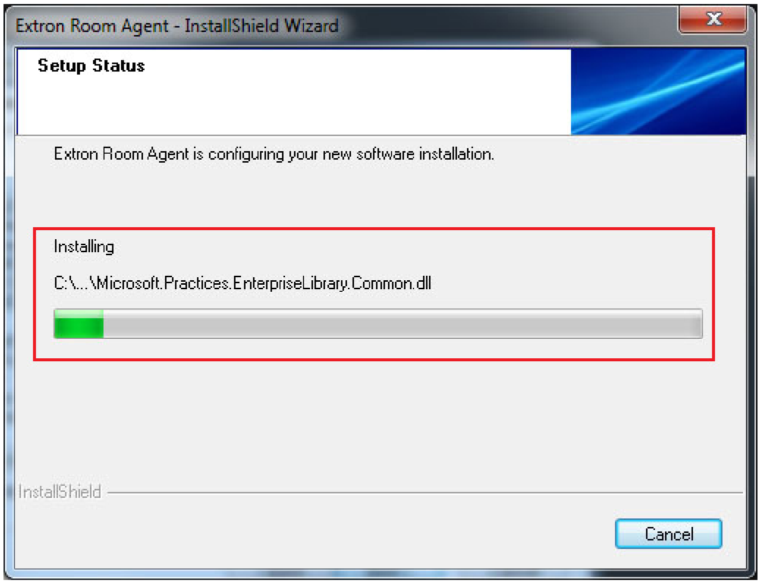


Figure 15. Installation in Progress

The program is downloaded and installed. A green bar on the `Setup Status` screen shows the progress of the installation.

16. When the installation is completed, the final screen appears. Leave the box checked to add a desktop shortcut.

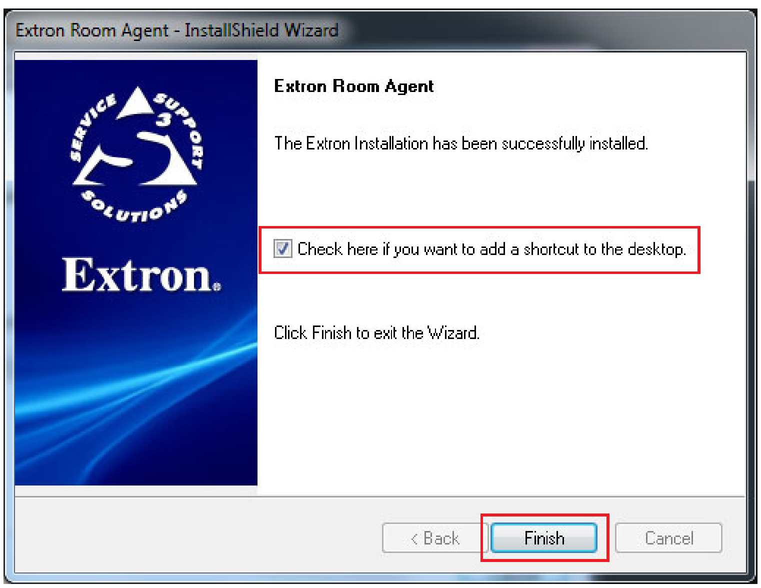


Figure 16. Installation Complete

17. Click **`Finish`**. The program is now installed and ready for use.

Updating Firmware

Extron TLS panels and TLSI devices have the latest firmware version when they are shipped from the factory. Over time, as new features are added, newer versions of the Room Agent software become available. In order to run the newer software versions, you may need to update the firmware on your panels.

The latest version of the firmware is packaged with the new software. Copy the firmware file to a computer on the same network as the touchpanel.

By default, when you download Room Agent to your PC, the firmware can be found at `C:\ProgramData\Extron\TLPScheduler\firmware\`.

> **NOTE:** The TLSI 201 and the TLS panels use different firmware. Ensure you obtain the correct firmware for your product.

Use one of the following options to upload and install the firmware on a TLSI 201, SSI, or TLS panel:

- Toolbelt (see *Toolbelt Help File*)
- Room Agent **MANAGE** tab (see **Install Firmware** on page 36)

The TLSI 201 firmware can also be installed using the **TLSI 201 Web Page** (see page 185).

Menu Button

Click the **`Menu`** button in the top right corner of the screen to open a drop-down list that allows you to create new configurations, open existing configurations, and save configurations.

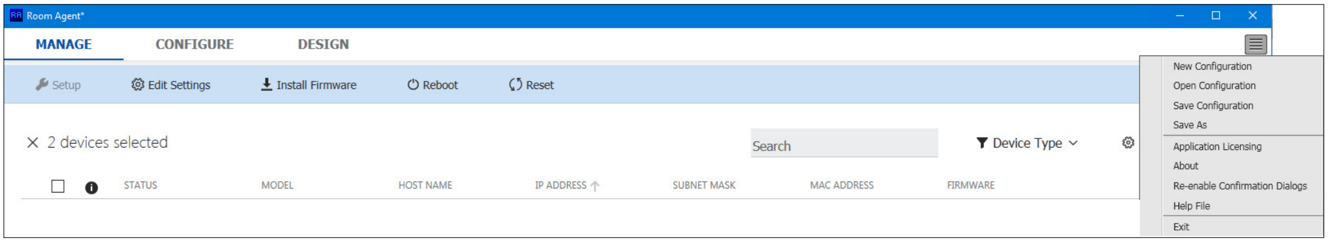


Figure 17. Menu Button

It also provides access to the `About` screen.

The following options are available:

Figure 18. Menu Button Options

NOTES:

- Each touchpanel has an individual configuration file that describes how that touchpanel is set up. The system configuration file contains the individual records for every touchpanel in the system.
- The individual records are uploaded to the corresponding touchpanel, where they are saved and used to configure the touchpanel. If the system configuration file is lost or corrupted, it can be regenerated by pulling the individual records from all the individual touchpanels in the system.

- **New Configuration** — Opens a new (unnamed) system configuration file (see NOTES, above).
- **Open Configuration** — Allows you to open and modify an existing system configuration file (see NOTES, above).

  Navigate to the location where the configuration file was saved, then select a file. You are prompted to enter the password that you provided when you saved the file.
- **Save Configuration** — Saves changes to an existing system configuration file (see NOTES, above).

- **Save As...** — Saves changes to a new (unnamed) configuration or allows you to save a copy of an existing configuration file (see **NOTES** on page 23).

  When you click this option, you are prompted to enter and reenter a password to protect the configuration file.

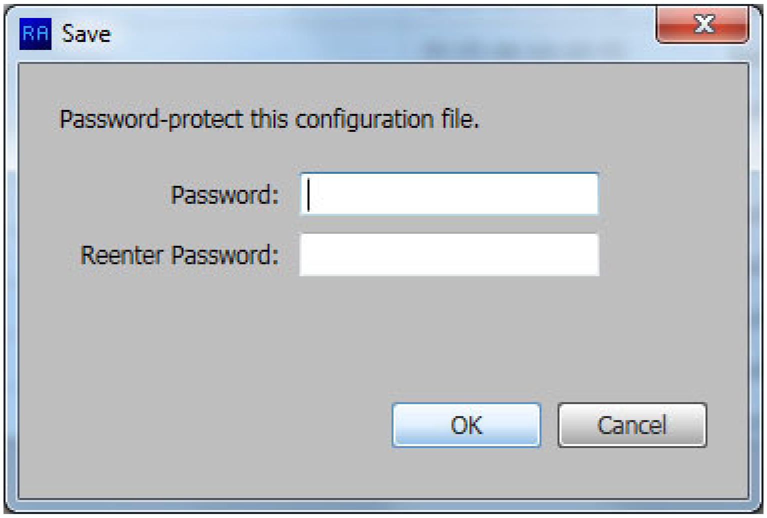
  

  Figure 19. Save Configuration

  1. Enter and reenter a password and Extron recommends that you use a strong password to protect the configuration file.
  2. Click **`OK`**. A `Save As` dialog box opens.
  3. Name the file and navigate to the folder where the file is to be saved.
  4. Click **`Save`**.

- **Application Licensing** — See **Application Licensing** on page 13.
- **About** — Opens a splash screen that provides basic information about the program.

  Figure 20. About Room Agent

  Click **`Details`** or **`Licenses`** for more information.

  Click **`OK`** to close the screen.

- **Re-enable Confirmation Dialogs** — Re-enables all dialogs that had previously been disabled by the user.
- **Help File** — Opens the Extron *Room Agent Help file*.
- **Exit** — Closes the program. You are prompted to save changes to the system configuration file before you close the program.

Manage Tab

- Discover Panels
- Add Panels Manually
- MANAGE Tab Features
- Remove Panels
- Actions Drop-down List
- Actions

Extron Room Agent opens to the `MANAGE` tab:

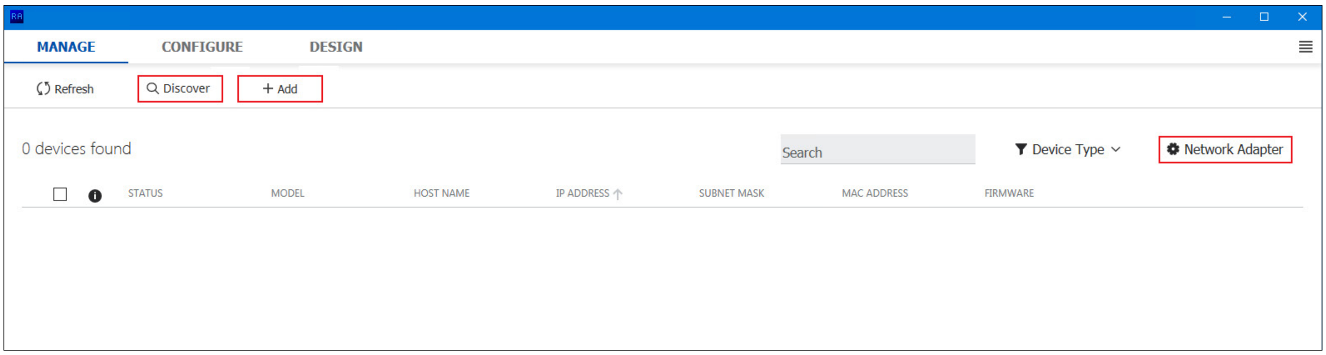


Figure 21. Room Agent MANAGE Tab

Discover Panels

Press **`Discover`** to list all the devices (panels and Wayfinding Devices) that Room Agent is able to find automatically. Only panels that are on the same subnet as the control PC are auto discovered.

When the Discover process begins, the text on the button changes to **`Stop Discovery`**. The discover process may take several minutes. Even after all the available panels have been discovered, the process remains active until you click **`Stop Discovery`**.

> **NOTE:** The discover process finds all touchpanels in the subnet that could be used by the Room Agent system, even if they have another function.

If the control PC has access to more than one subnetwork, click **`Network Adapter`** to connect to other available subnetworks.

The `Available Network Adapters` dialog box opens:

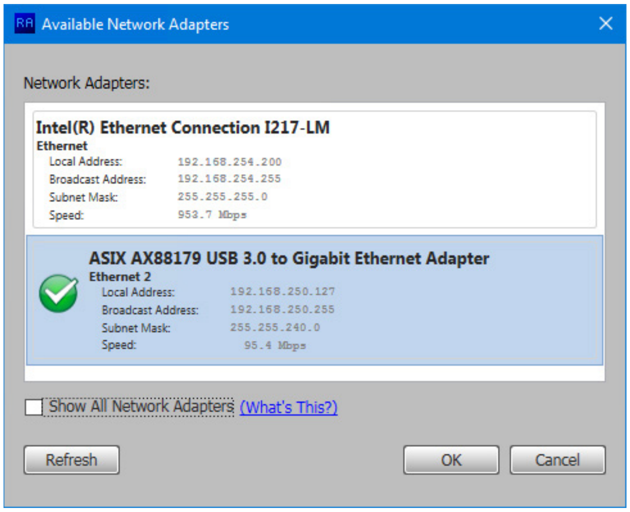


Figure 22. Network Adapter

1. Select one of the available networks and then click **`OK`**.
2. The dialog box closes. Click **`Discover`** in the `MANAGE` tab (see **figure 21** on page 25) to find panels that are available on the new network.

Add Panels Manually

TLS panels that are not available on any of the subnets accessed by the network adapter must be added manually.

1. Click **+ `Add`** (see **figure 21**).

   The `Add Device` dialog box opens.

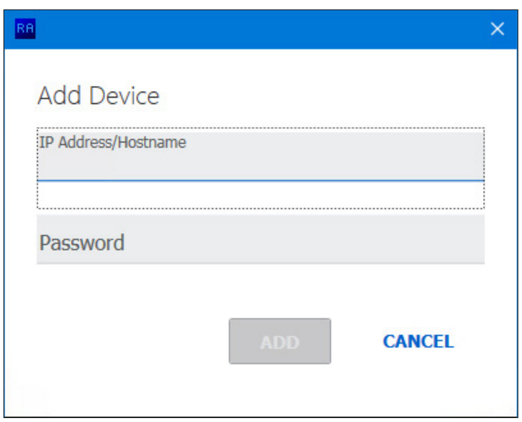


Figure 23. Add Device Dialog Box

2. Enter the `IP Address/Hostname` and `Password` in the corresponding fields.

NOTES:

- All panels are password protected. The factory configured passwords for all accounts on each device have been set to the device serial number. Passwords are case sensitive.
- Passwords can be changed during panel setup and Extron strongly recommends that you do this.
- If the device is reset to default settings, the password is reset to the default password configuration, which is `extron` (for either `admin` or `user`).

3. Click **`Add`**.The new TLS panel is added to the `Panels` list.

4. Repeat steps 1-3 to add more panels manually. If you have several touchpanels to enter, it is good practice to save the configuration periodically (see **Menu Button** on page 23).

   Once the panels have been discovered or added manually, they are listed in the `MANAGE` tab.

   NOTE: TLS panels and Wayfinding devices are all listed together.

MANAGE Tab Features

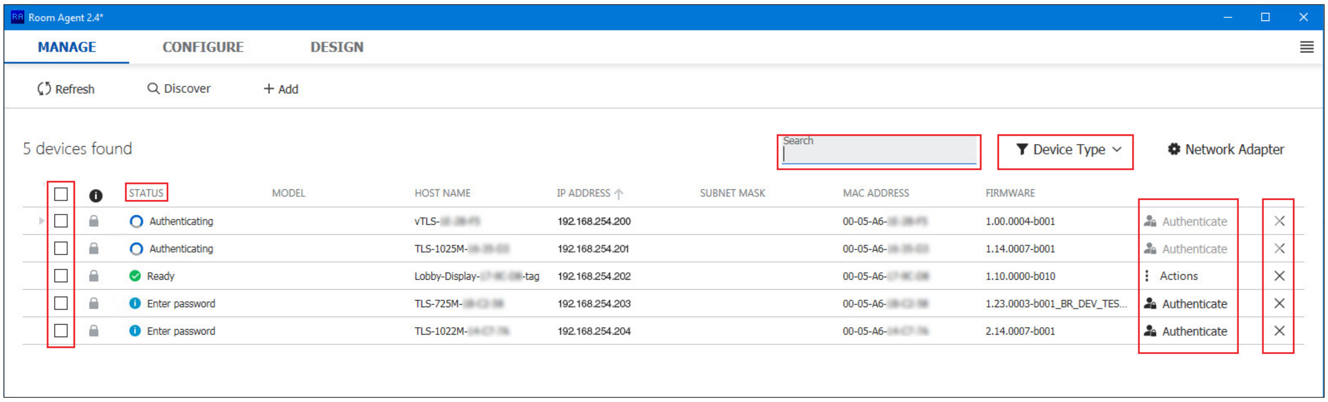


Figure 24. Panels Listed in the Manage Tab

The `MANAGE` tab has the following features:

- Check Box
- Panel Status
- Search Box
- Device Type Filter
- **Status Link**
- **Remove Panels**

Check Box

The check boxes (see figure 25) allow you to select and configure one or more panels. When one or more panels are selected the **MANAGE Tab Menu Bar** (see page 28) appears at the top of the screen.

Panel Status

The panel `STATUS` column, on the left of the screen, (see figure 24) shows the current status of each panel. When the panel is first discovered, it shows `Enter Password`. While the password is being authenticated, it shows `Authenticating`. Once the password is authenticated, it shows `Ready`. Other messages can appear, depending on the status of the panel.

Search Box

The `Search` box (see figure 24) allows you to search the list for a single panel or for a group of panels that share a common characteristic. You can search by:

- `Status`
- `Host Name`
- `IP address` (any octet that is unique to the panel)
- `Firmware version`

Device Type Filter

The Device Type filter (see figure 24) allows you to select all the devices in either of these categories:

- `Panels`
- `Wayfinding Devices`

MANAGE Tab Menu Bar

Use the check boxes at the left of the screen to select one or more panels (see **figure 24** on page 27).

When one or more panels are selected, a new menu bar appears at the top of the page:

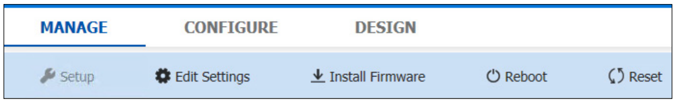


Figure 25. MANAGE Tab Menu Bar

The menu bar allows you to:

- Setup
- Edit Settings
- Install Firmware
- Reboot
- Reset

Most of these options are also available from the **Actions Drop-down List** (see page 29). However, the **`Actions`** drop-down list does not have the `Setup` option.

The `MANAGE` tab menu bar allows you to carry out these actions on multiple panels in a batch. The actions shown in the **`Actions`** drop-down list are carried out on only the single panel selected.

Status Link

The Status link on the right of the screen (see **figure 24**) shows the status of each panel and allows the user to carry out actions on the panel:

1. Initially all the panels show `Authenticate`.
2. Click **`Authenticate`**.

   The `Authenticate to Device` dialog opens:

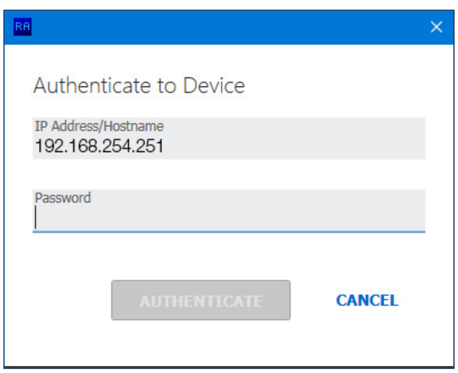
   

   Figure 26. Authenticate to Device Dialog
3. Enter the password and click **`AUTHENTICATE`**.
   - The dialog box closes and the panel status changes to `Authenticating`.
   - Once the password is authenticated, the panel status changes to `Ready`.
   - The status link changes to `Actions`.
4. Click **`Actions`** to see a list of actions that can be carried out on that device.

Remove Panels

To delete an unwanted panel:

1. When you click **`Discovery`** (see **figure 24**), the label changes to `Stop Discovery`. Click **`Stop Discovery`**.
2. Click the **`X`** at the end of the row for the touchpanel to be removed. The touchpanel is deleted from the list.

Actions Drop-down List

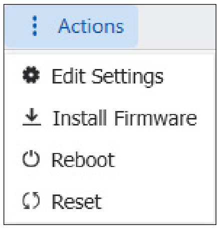


Figure 27. Actions Drop-down Menu

The **Actions** drop-down list allows you to:

- **Edit Settings**
- **Install Firmware**
- **Reboot**
- **Reset**

The **Actions** drop-down list allows you to carry out the same functions as the **MANAGE Tab Menu Bar** (see page 28). However, these actions are carried out on a single panel instead of a batch.

The **Actions** drop-down list does not have the **Setup** option.

Actions

Edit Settings

To edit settings for one or more panels simultaneously, use the check boxes to select one or more panels and, in the top menu bar that appears, click **Edit Settings** (see **figure 25** on page 28).

To edit settings for a single panel, click **Actions** in the line for that panel and, in the drop-down list that appears, click **Edit Settings** (see **figure 28** on page 30).

The **Edit Settings** window opens, showing two tabs:

- **General** on page 30
- **Network** on page 35

General

By default, the `Edit Settings` window opens with the **`GENERAL`** tab selected (see figure 28). The options available are different for TLS Panels and Wayfinding Devices.

TLS Panels

The **`GENERAL`** tab for TLS panels has four expandable sections: **`Display`**, **`Audio`**, **`Date and Time`**, and **`Passwords`**. Click on any of the headings to expand that section.

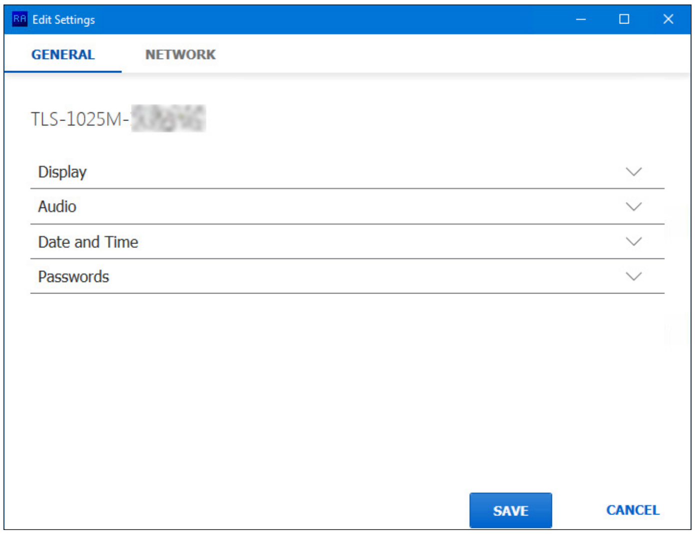


Figure 28. General Settings (TLS Panels)

Display

By default, the `Display` section is already open when the **`GENERAL`** tab is selected.

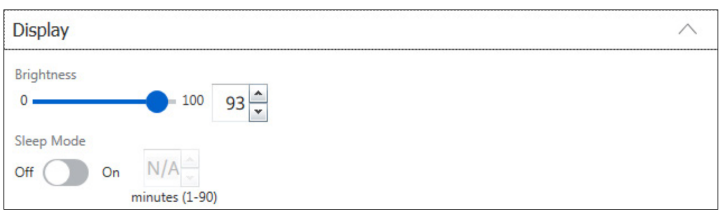


Figure 29. Display Settings

Use the `Brightness` slider or multibox to set the screen brightness. This setting needs to be higher when the ambient light is brighter.

`Sleep Mode` is an energy saving feature. When no activity is detected near the touchpanel for a user-defined period of time, the screen goes dark. When activity is detected near the touchpanel, the screen is activated again. Set sleep mode by toggling the **`On`** or **`Off`** switch. If sleep mode is on, set how long the period of inactivity should be before the touchpanel enters sleep mode.

When all the changes have been made, click **`SAVE`** or **`CANCEL`** at the bottom of the page (see figure 28).

Audio

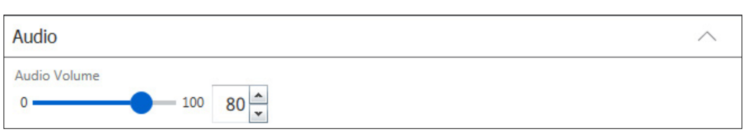


Figure 30. Audio Settings

Use the `Audio Volume` fader or the multibox to set the audio volume. This determines the volume of the audible feedback from the touchpanel (for example, from button clicks).

When all the changes have been made, click **`SAVE`** or **`CANCEL`** at the bottom of the page (see figure 28).

Date and Time

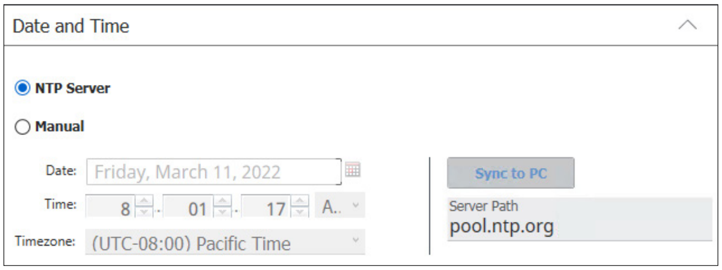


Figure 31. Date and Time Settings

Decide how to set the time on the panel. The options are:

- **Synchronize with an NTP server** — Select the `NTP Server` radio button and enter the Server path. You can use an IP address or a Fully Qualified Domain Name (FQDN). When this option is selected, all other options (except `Server Path`) are grayed out and unavailable.
- **Set the time manually** — Select the `Manual` radio button. `Server Path` is grayed out and unavailable but all other options are now available.
  - Select the `Timezone` from the drop-down list. By default, this is `(UTC-08:00) Pacific Time`.
  - Click **`Sync to PC`** to sync the panel with the control PC
  - Set the time and date manually by entering values in the `Date` and `Time` text boxes.

When all the changes have been made, click **`SAVE`** or **`CANCEL`** at the bottom of the page (see **figure 28** on page 30).

Passwords

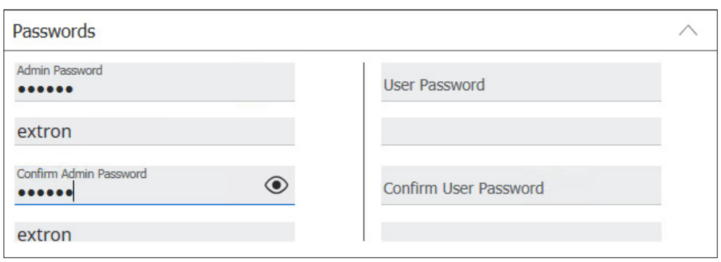


Figure 32. Password Settings

This panel allows you to reset the passwords for the TLS panel. The panel can have an `Admin Password` and a `User Password`.

NOTES:

- You cannot set a `User Password` until an `Admin Password` has been set.
- The factory configured passwords for all accounts on each device have been set to the device serial number. Passwords are case sensitive.
- If the device is reset to default settings, the password is reset to the default password configuration, which is `extron` (for either `admin` or `user`).

Enter the new password in the `Admin Password` text box. By default, the new password is masked. To see the new password, click the **eye** icon.

Enter the new password again in the `Confirm Admin Password` text box.

The old password is displayed in the textbox underneath each text box.

Once the `Admin Password` is saved, repeat the process to set the `User Password`.

When all the changes have been made, click **`SAVE`** or **`CANCEL`** at the bottom of the page (see **figure 28**).

General Settings for Multiple Devices

If you select multiple devices by clicking two or more check boxes in the **`MANAGE`** tab, (see **figure 24** on page 27), you can configure all of the selected devices as a batch.

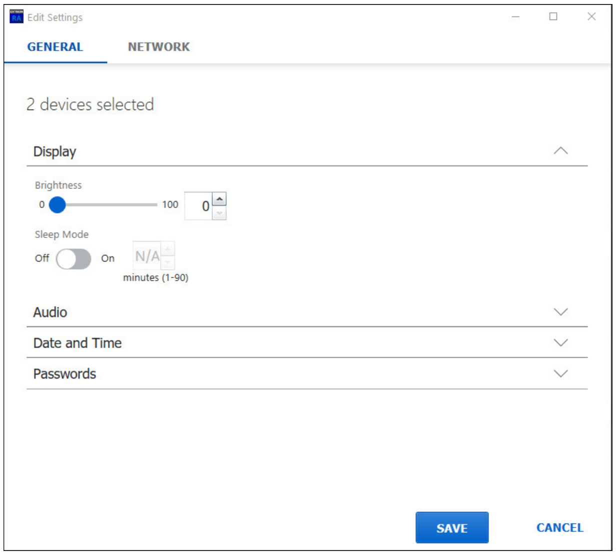


Figure 33. General Settings for Multiple Devices

When multiple devices are selected, the `Display`, `Audio`, `Date and Time`, and `Passwords` settings that are configured with the **`GENERAL`** tab are applied to all the selected devices.

You can also configure the network settings for multiple devices in a batch.

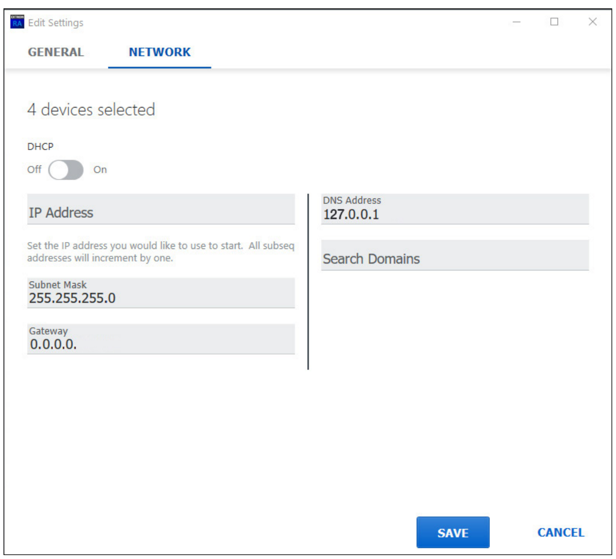


Figure 34. Network Settings for Multiple Devices

The `Subnet Mask`, `Gateway address`, and `DNS Address` that you set are applied to all devices.

The `IP Address` that you set is applied to the first device in the list of selected devices. The first IP Address is incremented by one and applied to the second device and so forth. For example, if the first IP address is set to `192.168.254.200`, the second device is assigned the IP address `192.168.254.201`, and the third device is assigned `192.168.254.202`.

If an address is already assigned to another device, that address is skipped and the next available address is used. For example, in the example above, if the address `192.168.254.202` was not available, the third device is assigned `192.168.254.203.`

Wayfinding Devices

The **GENERAL** tab for Wayfinding devices (see figure 35) is different from the TLS panels.

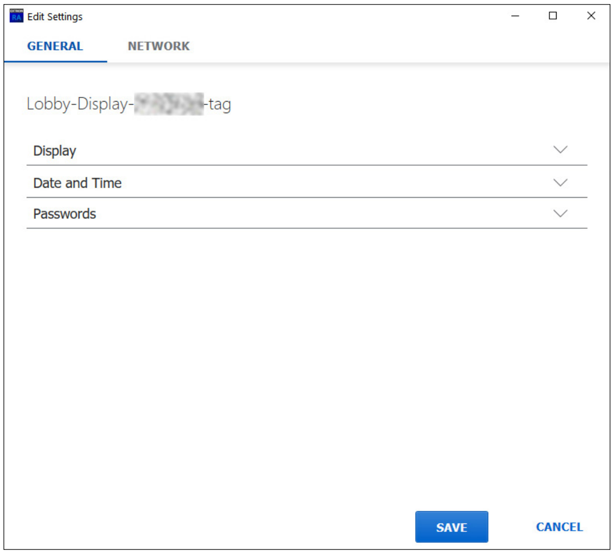


Figure 35. General Settings (Wayfinding Devices)

There are no controls to set audio.

Display

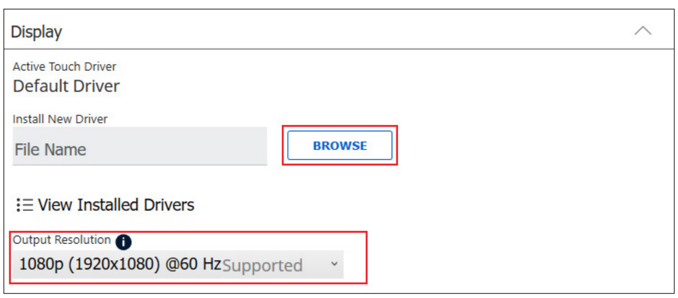


Figure 36. Display Settings (Wayfinding Devices)

Room Agent provides a default driver for use with the display device connected to the Wayfinding device. You can replace it with your own driver:

1. Upload the driver to the control PC.
2. Click **BROWSE** (see figure 36) and navigate to the folder where the driver was stored and select it.
3. Upload the driver to the TLSI.

You can also select the resolution and frequency for the connected display.

When all the changes have been made, click **SAVE** or **CANCEL** at the bottom of the page (see figure 35).

Date and Time

The `Date and Time` settings for the TLSI panel are the same as those for the TLS panels.

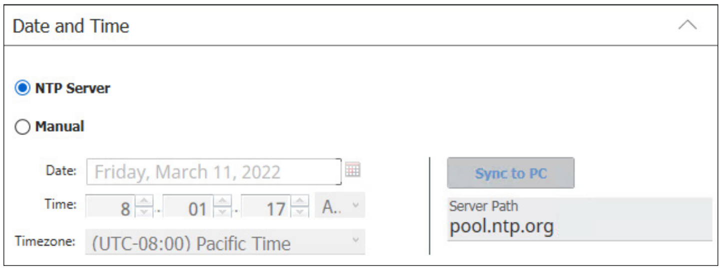


Figure 37. Date and Time Settings

Decide how to set the time on the panel. The options are:

- **Synchronize with an NTP server** — Select the **`NTP Server`** radio button and enter the `Server path`. You can use an IP address or a Fully Qualified Domain Name (FQDN). When this option is selected, all other options (except `Server Path`) are grayed out and unavailable.
- **Set the time manually** — Select the **`Manual`** radio button. `Server Path` is grayed out and unavailable but all other options are now available.
  - Select the **`Timezone`** from the drop-down list. By default, this is `(UTC-08:00) Pacific Time`.
  - Click **`Sync to PC`** to sync the panel with the control PC
  - Set the time and date manually by entering values in the `Date` and `Time` text boxes.

When all the changes have been made, click **`SAVE`** or **`CANCEL`** at the bottom of the page (see **figure 35** on page 33).

Passwords

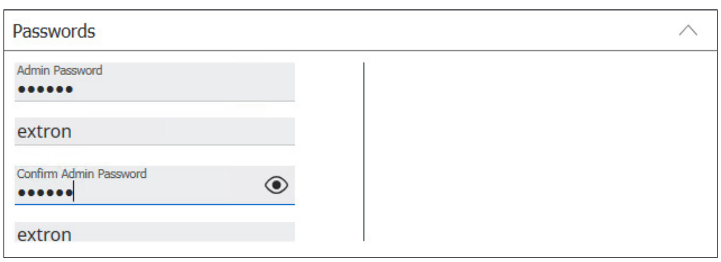


Figure 38. Password Settings

This panel is the similar to the `Passwords` panel for the TLS panels. However, the TLSI can have an `Admin Password` only. There is no `User` Password.

> **NOTES:**
>
> - The factory configured passwords for all accounts on each device have been set to the device serial number. Passwords are case sensitive.
> - If the device is reset to default settings, the password is reset to the default password configuration, which is `extron` (for either `admin` or `user`).

1. Enter the new password in the `Admin Password` text box. By default, the new password is masked. To see the new password, click the **eye** icon.
2. Enter the new password again in the `Confirm Admin Password` text box.

   The old password is displayed in the textbox underneath each text box.
3. Click **`SAVE`** or **`CANCEL`** at the bottom of the page (see **figure 35** on page 33).

Network

The **NETWORK** tab for both TLS panels, Wayfinding devices, and SSI devices is similar:

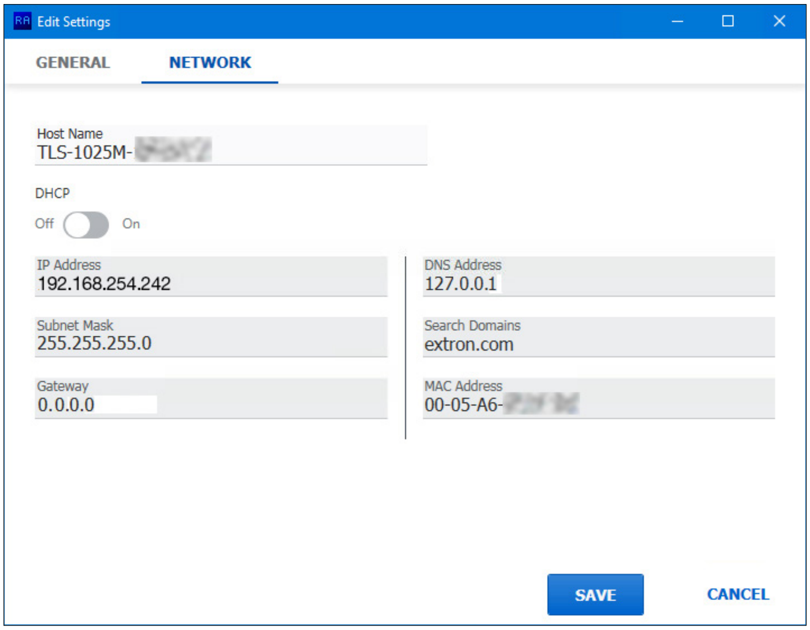


Figure 39. Edit Settings Dialog Box

1. Set DHCP to **Off** or **On**, as required.
   - If DHCP is **On**, the network addresses cannot be edited.
   - If DHCP is **Off**, you can edit the network addresses.
2. Edit the network addresses for a single panel or multiple panels.
   - If you selected a single panel, enter the IP address for that panel.
   - If you selected multiple panels, enter the IP address that is to be assigned to the first panel. The next available IP address is assigned to the second panel and so forth.

     For example, if you assign `192.168.254.200` to the first panel, Room Agent assigns `192.168.254.201` to the second panel unless `192.168.254.201` is already in use. In that case the second panel is assigned `192.168.254.202`.

     Edit the `IP Address`, `Subnet Mask`, `Gateway`, or `DNS Address`, as required. You can also enter the network address of a domain you wish to search.

     If more than one panel was selected, the `Subnet Mask`, `Gateway`, and `DNS Address` that you enter is assigned to all the selected panels.
3. When all the changes are made, click **SAVE** or **CANCEL** at the bottom of the page (see **figure 35** on page 33).

Install Firmware

Ensure at least the minimum recommended version of the firmware is installed on all panels.

> **TIP:** Check the firmware release notes (at **www.extron.com**). If the latest firmware version adds features that are not needed in your system, updating is optional.

1. If you have not already done so, copy the firmware from the Room Agent software package to a PC on the same subnet as the panel that you are updating (see **Updating Firmware** on page 22).

   Some devices use the same firmware. For example, the TLS 525, TLS 725, and TLS 1025 all use the same firmware.

   However, other devices use different firmware. For example, the TLSI 201 and the TLS 525 use different firmware. You must download the correct firmware file for each device.

2. To update firmware for one or more panels simultaneously, select one or more panels and, in the top menu bar that appears, click **`Install Firmware`**.

   To edit settings for a single panel, click **`Actions`** in the line for that panel and, in the drop-down list that appears, click **`Install Firmware`**.

   The `Install Firmware` dialog box opens:

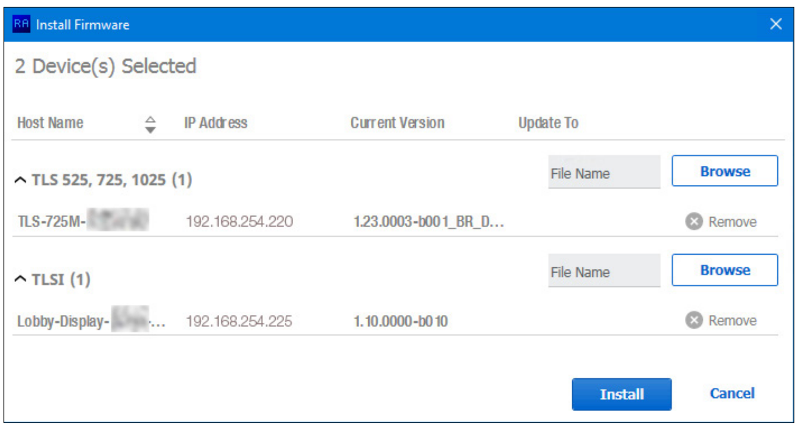
   

   Figure 40. Install Firmware dialog box

   If you are updating multiple panels simultaneously, they are listed by firmware group. For example, all TLS 525M, 725M, and 1025M panels use the same firmware and all of those panels are listed under the `TLS 525, 725, 1025` heading. In the example above, only one panel in this group was selected.

   If you are updating a single panel, only that panel is shown.

   The Wayfinding devices are listed under the `TLSI` heading. In the example above, only one TLSI was selected.

3. Click **`Browse`** and navigate to the folder where the firmware file for that group of panels was saved in step 1.
4. Select the firmware file.
5. Click **`Install`**. This procedure updates all the panels in a single group.
6. To update the firmware for another group of panels, repeat steps 2-5.

Reboot

The device goes through a power cycle. No settings are changed.

1. In the top menu bar, click **`Reboot`**.
2. A dialog box opens asking you to confirm that you wish to reboot the device.
3. A power cycle is performed on all the selected devices.

   While the reboot is taking place, the text in the `Status` column changes to `Connecting...`.

   Once the reboot is complete, the text changes to `Reboot Complete`.

Reset

Reset removes any config files uploaded to the device. All other settings (network, firmware, and so forth) are unchanged.

1. In the top menu bar, click **`Reset`**.
2. A reset is performed on all the selected devices. While the reset is taking place, the text in the `Status` column changes to `Connecting...`.

   Once the reset is complete, the text changes to `Reset Complete`.

Configure Tab

This section provides the following information about the CONFIGURE tab:

- View a List of Touchpanels, SSI Devices, or Wayfinding Devices and Their Properties
- Create or Edit Configuration Files
- Set up a Proxy Server
- Ad Astra®
- CollegeNET 25Live®
- EMS
- Google Calendar™
- Microsoft Exchange
- Microsoft Office 365
- Korbyt Booking / NFS
- Configure Individual TLS Panels
- Retrieve and Clear the Activity File
- Configure Wayfinding Devices
- Save Configuration for Wayfinding Device

View a List of Touchpanels, SSI Devices, or Wayfinding Devices and Their Properties

Touchpanels

By default, the **CONFIGURE** tab opens with TLS Panels selected, to show a list of all the panels that were auto-discovered or manually added.

Figure 41. CONFIGURE Tab — TLS Panels

Use the check boxes at the start of each row to select individual panels or select the check box in the column heading to select all panels.

Use the drop-down list to select the calendar associated with the TLS panels.

The options in the top menu bar also change for different calendar types.

See the descriptions for each calendar type to find which options are available with each calendar.

Information about the panels is organized under column headings. By default, the column headings are `STATUS`, `IP ADDRESS`, `HOST NAME`, `ROOM NAME`, `CAPACITY`, `LANGUAGE`, `SOUND`, `TEMPLATE`, and `LOCATION`.

These headings may change depending on which `Calendar Type` is selected from the drop-down list. For example, figure 42 shows the headings with **`Ad Astra`®** selected.

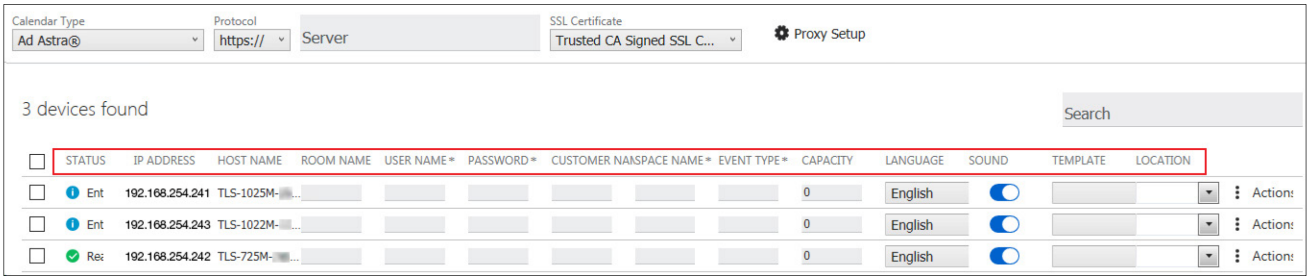


Figure 42. CONFIGURE Tab Headings with Ad Astra Calendar

When you check the status box to select a device, a new menu bar appears at the top of the page:

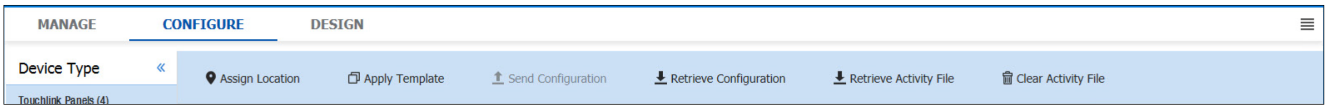


Figure 43. CONFIGURE Tab — Top Menu Bar

- **`Assign Location`** — Allows you to assign a location tag to the selected TLS panel. The location tag allows nearby rooms to be grouped, for example “Floor 1”. This is displayed as the room location in the Wayfinding Device. When rooms are shown as a list on the Wayfinding Device, they are grouped by their location tag.
- **`Apply Template`** — The layout of the panel can be configured using the DESIGN Tab. You can select one of the saved panel design files from this drop-down list.
- **`Send Configuration`** and **`Retrieve Configuration`** — See **Sending and Retrieving Configurations** on page 113.
- **`Retrieve Activity File`** and **`Clear Activity File`** — See **Retrieve and Clear the Activity File** on page 115.

SSI Devices

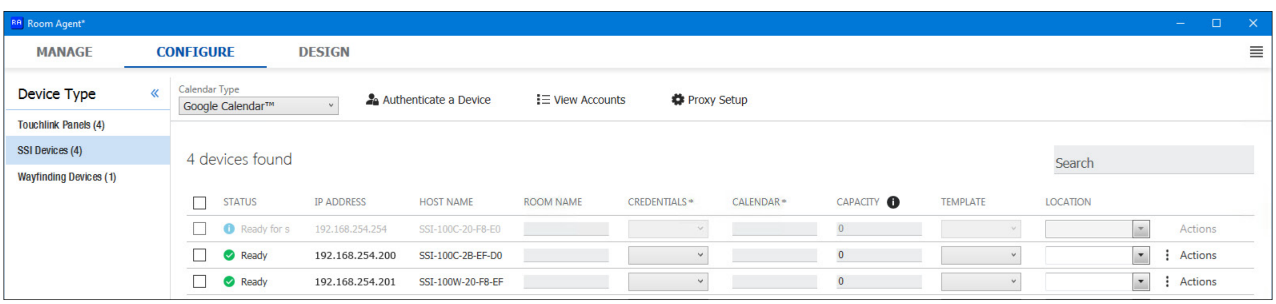


Figure 44. SSI CONFIGURE Tab Headings with Google Calendar

For SSI devices, the default headings are `STATUS`, `IP ADDRESS`, `HOST NAME`, `ROOM NAME`, `CAPACITY`, `TEMPLATE`, and `LOCATION`.

> **NOTE:** These headings change, depending on the `Calendar Type` selected. However, they are identical to the headings for the TLS devices using the corresponding `Calendar Type` except that SSI devices do not have `LANGUAGE` or `SOUND` headings.

When you check the status box to select a device, a new menu bar appears at the top of the page. This is the same as the menu bar shown in figure 43.

Wayfinding Devices

The `CONFIGURE` tab options for Wayfinding devices are also different.

Click **`Wayfinding Devices`** to view a list of Wayfinding devices (see **figure 41** on page 38).

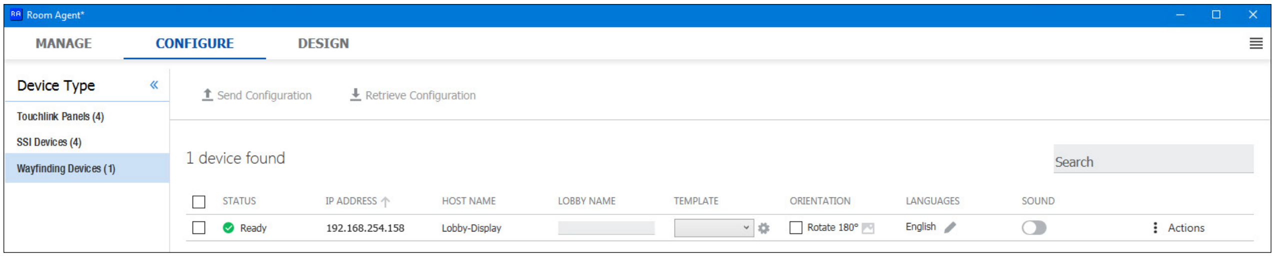


Figure 45. CONFIGURE Tab — Wayfinding Devices

For information about configuring Wayfinding devices, see **Configure Wayfinding Devices** on page 116.

Create or Edit Configuration Files

You can create a configuration file and upload it to the TLS panel, where it is saved and used to configure that panel. Alternatively, you can download a previously created configuration file for editing by clicking **`Retrieve Configuratio`**n. After editing, the configuration file is uploaded back to the TLS panel for the changes to take effect by clicking **`Send Configuration`**.

> **NOTE:** Saving each individual configuration file on the corresponding TLS panel is a useful feature: if the system configuration file on the control PC is accidentally deleted or becomes corrupted, rebuild it by pulling the individual records from all the touchpanels.

To configure a TLS panel:

1. Select the **`CONFIGURE`** tab at the top of the page.
2. Select a calendar type using the `Select a Calendar Type` drop-down list. The options are:
   - **`Ad Astra`**
   - **`CollegeNET 25Live`**
   - **`EMS`**
   - **`Google Calendar`**
   - **`Microsoft Exchange`**
   - **`Microsoft Office 365`**
   - **`NFS`**

   > **NOTE:**
   > - Depending on the version of Room Agent, you may not see all the calendar types listed.
   > - When you select a calendar type, different options appear on the page for connecting to the server and for configuring the TLS panels. The next sections describe how to configure TLS panels for each calendar type.

   After selecting the calendar see **Configure Individual TLS Panels** on page 113.

Set up a Proxy Server

If you use the `https://` protocol to connect a TLS panel to the calendar server, the Proxy Server must be setup as TLS Pass Through. This is required for the TLS to validate the calendar server’s SSL certificate.

Before Starting

Your proxy server administrator must provide you with the following information:

- **Proxy Server IP Address/Hostname** – This tells the TLS how to find the proxy server.
- **Proxy Server IP Port** – This tells the TLS how to connect to the proxy server.
- **Protocol(s)** (`http://` or `https://`) – This tells the TLS what kind of traffic to send through the proxy server.
- **Proxy Username** – The username needed to be allowed through the proxy server.
- **Proxy Password** – The password needed to be allowed through the proxy server.

Setting Up the Proxy Server

1. Click the **`Proxy Setup`** button. It does not appear until you have selected a `Calendar Type`.

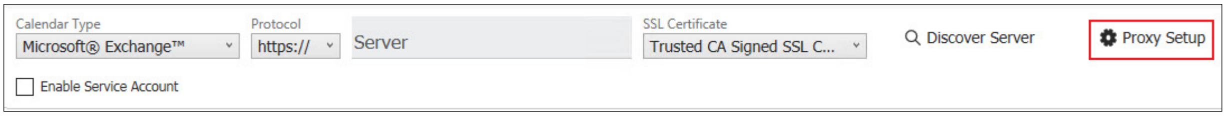


Figure 46. Proxy Setup Button

The `Proxy Settings` dialog box opens:

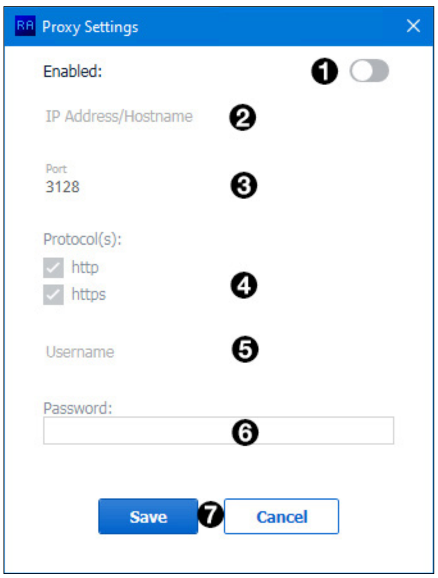


Figure 47. Proxy Settings Dialog

2. Ensure the **`Proxy Server`** switch is enabled (see figure 47, ❶).
3. Enter the `IP Address/Hostname` (❷), `Port` (❸), `Protocols` (❹, `Username` (❺), and `Password` (❻), (see **Before Starting** on page 41). These settings are only available if the **`Proxy Settings`** switch is enabled.
4. Click **`Save`** (❼) to save any changes and close the `Proxy Settings` dialog box or click **`Cancel`** to exit the dialog box without saving changes.
5. Add the TLS in Toolbelt.Connect to the TLS and go to the **`Security`** tab.
6. Click on **`Manage Certificates`**.
7. Click **`Add`**, then for the certificate type select **`CA`**.
8. Select the proxy server security certificate, give it an alias, then click **`Add Certificate`**.

Troubleshooting

If your TouchLink screen cannot communicate to the calendar server through the proxy server, check the following:

- **Can the TouchLink screen communicate with the proxy server?**
- **Are your proxy credentials correct?**

Can the TouchLink screen communicate with the proxy server?

Toolbelt is an Extron software product that provides device discovery, device information, firmware updates, and configuration of network settings, system utilities, and user management for network based devices. For further information, see the *Toolbelt Help File*.

1. Use Toolbelt to test the connection between the TLS and the Proxy server.

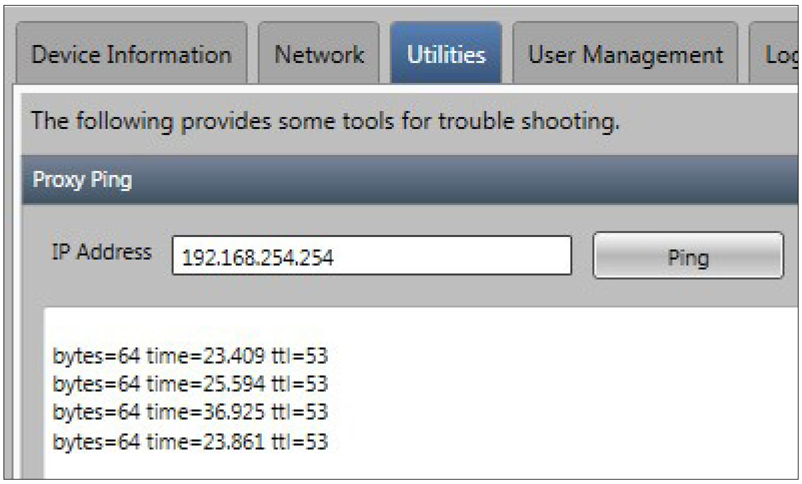


Figure 48. Toolbelt Utilities — Ping

2. Go to **`Utilities > Proxy Ping`**.
3. Enter the `IP Address` or `Hostname` of the proxy server.
4. Press **`Ping`**.

   You should see four successful pings as shown above. If you see any error messages, your TLS cannot connect to the proxy server. You should check with your network administrator.

Are your proxy credentials correct?

1. Open the Windows **`Start`** menu but do not click any of the icons.
2. Type `Proxy`.

The `Start` menu provides a manual `Proxy` setup dialog:

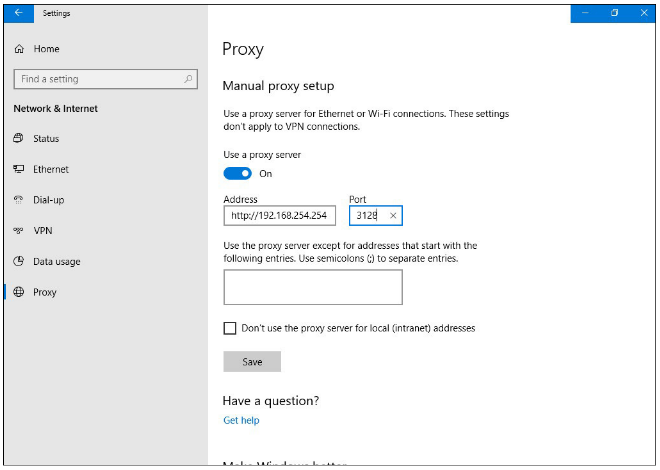


Figure 49. Manual Proxy Setup Dialog

> **NOTE:** If you are not an administrator on your PC, or if your PC is managed by an IT group, the proxy setting may be locked out. Contact your administrator for assistance.

3. Enter your proxy information into the Manual proxy setup section.
4. Click **Save**.
5. Open a web browser and try to access any external web page (for example, **https://www.extron.com**).

   You should be prompted to enter your `username` and `password`.
6. If the username or password is NOT correct, you receive an error message.

   If this happens, confirm your username and password with the proxy administrator.
7. If your username and password are correct, you are allowed to access the site.

   You may also receive a message like `This site is blocked by the proxy`. This means your username and password are correct, but you have tried to access a site that is explicitly blocked by the proxy server.
8. Once you have confirmed your username and password are correct, you should try to access the domain for the calendar server used by the TLS or SSI device. For example, if you are using Microsoft Office 365, then use your web browser to open `https://outlook.office365.com`.

   If you get a message that this site it blocked, you should contact your proxy administrator.

Ad Astra®

NOTE: To run the Ad Astra calendar type, the TLS touchpanels must have firmware version 1.12.0001-b001 (or later) installed.

1. Open the **CONFIGURE** tab and select **Ad Astra** from the `Calendar Type` drop-down list.

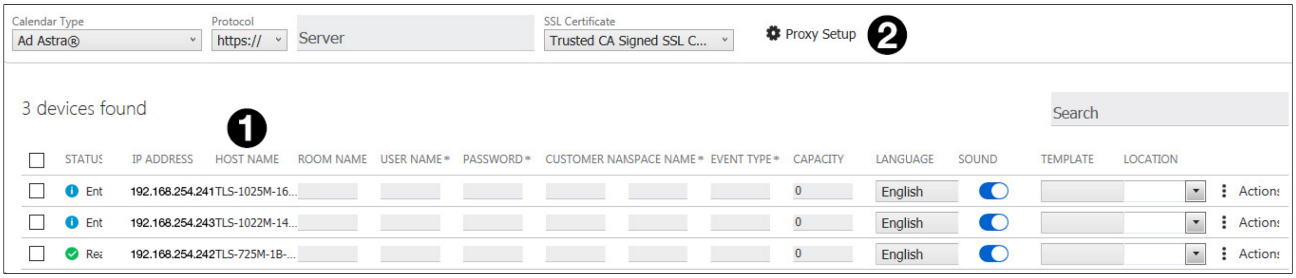


Figure 50. Ad Astra Column Headings

2. Use the top menu bar (see figure 50, ❷) to:
   - Select a protocol (`http://` or `https://`).

     If you use `https://` the Proxy Server must be setup as **TLS Pass Through**. This is required for the TLS to validate the calendar server's SSL certificate (see **Set up a Proxy Server** on page 40).
   - Enter the name of the Ad Astra Server.
   - Select the SSL Certificate preference (**Trusted CA Signed SSL Certificate** (Default) or **No Verification of SSL Certificate**).
3. The following column headings (❶) are available:
   - `STATUS` — Use this check box to select individual panels for configuration.
   - `IP ADDRESS` — This cell contains the IP address of the TouchLink panel.
   - `HOST NAME` — The hostname is a fully qualified domain name that uniquely identifies the computer. It is required for the computer to communicate with other devices on the network.
   - `ROOM NAME` — This is the name that appears on the touchscreen, once it is configured.
   - `USER NAME` — This is the user name that is used to log into the Ad Astra web interface.
   - `PASSWORD` — This is the password that is used to log into the Ad Astra web interface.
   - `CUSTOMER NAME` — This is listed on the Ad Astra web page (see figure 51). In the main menu bar, select **Settings > People**. From the `People List`, select the required name. This is the `Customer Name` and should be copied and pasted to ensure it is an exact match.

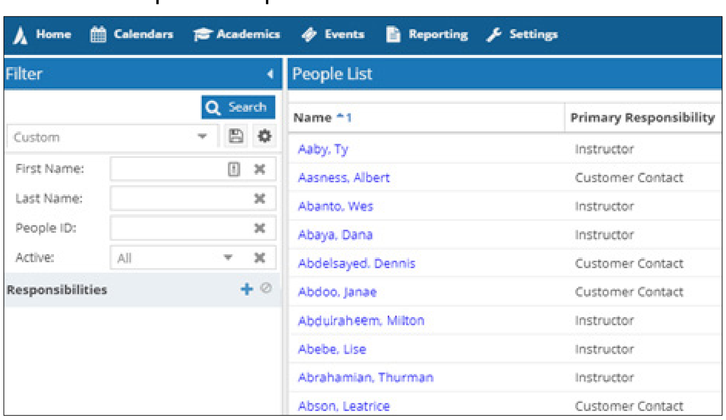


Figure 51. Ad Astra Customer Name

   - `SPACE NAME` — This is listed on the Ad Astra web page (see figure 52). In the main menu bar, select **Settings > Rooms**. From the `Room List`, select the required name. This is the `Room Name` and should be copied and pasted to ensure it is an exact match.

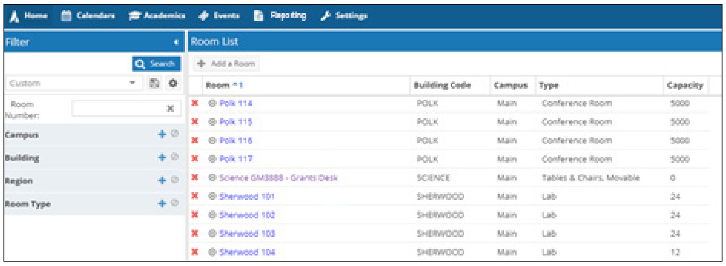


Figure 52. Ad Astra Space Name

- EVENT TYPE — This is listed on the Ad Astra web page (see figure 53). In the main menu bar, select **Events > Event Types**. From the Master List, select the required name. This is the Event Type and should be copied and pasted to ensure it is an exact match.

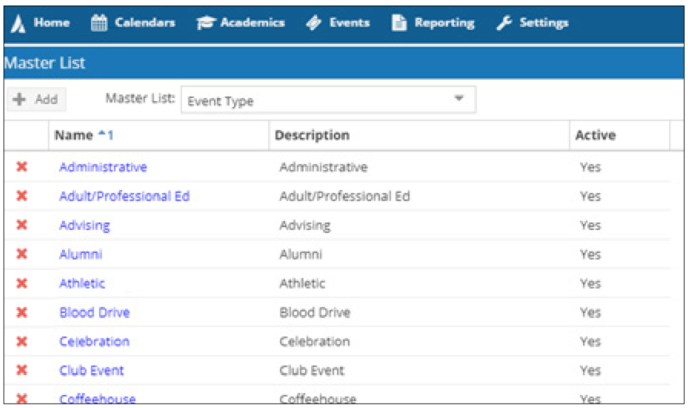


Figure 53. Ad Astra Event Type

- CAPACITY — Set the maximum number of people allowed in the room in this column.
- LANGUAGE — Select an option from the LANGUAGE drop-down list. By default, the language is English.
- SOUND — Set the **Sound** switch to **Off** or **On**. When it is set to on, pressing a button provides audible feedback. If it is set to off, there is no sound.
- TEMPLATE— The layout of the panel can be configured using the **DESIGN** Tab. You can select one of the saved panel design files from this drop-down list.
- LOCATION — Use a location tag to group nearby rooms, for example Floor 1. This is displayed as the room location in the Wayfinding Device. When rooms are shown as a list on the Wayfinding Device, they are grouped by their location tag.

There is also an Actions drop-down list for each touchpanel:

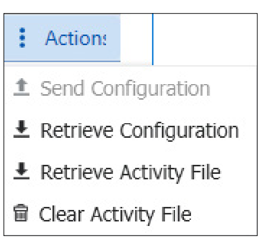


Figure 54. Configure Tab —Actions List

After verifying that the information is correct for all TLS panels, select one or more panels and click **Send Configuration** to save the configuration on the control PC. Alternatively, click **Retrieve Configuration** to retrieve a previously saved configuration and apply it to the selected panel.

You can also retrieve or clear the activity file associated with that panel (see **Room Scheduling Analytics** on page 186).

CollegeNET 25Live®

1. Open the **CONFIGURE** tab and select **CollegeNET 25Live** from the Calendar Type drop-down list.

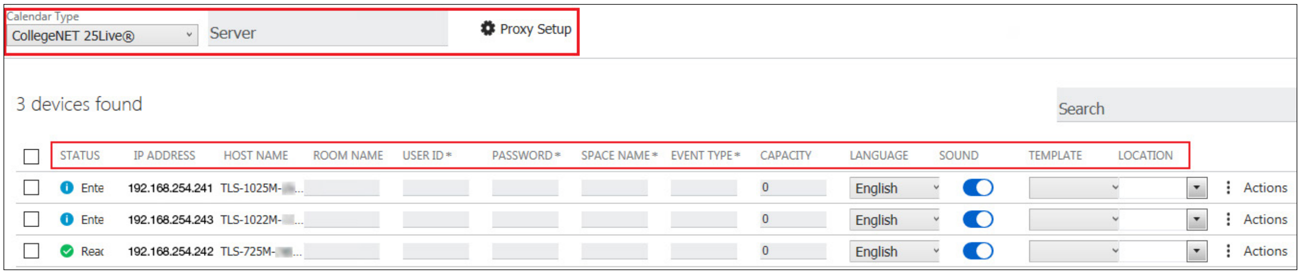
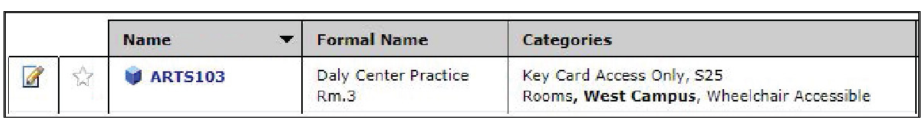


Figure 55. CollegeNET 25Live Column Headings

2. Use the top menu bar to:
   - Enter the name of the 25Live server in the Server field. This value is the full URL of the address you use to log in to your regular CollegeNET 25Live account and has the format: `https://25live.collegenet.com/<college-name>`.
   - Set up the Proxy Server (see **Set up a Proxy Server** on page 40).
3. The following column headings appear in the lists of panels:
   - STATUS — Use this check box to select individual panels for configuration.
   - IP ADDRESS — This cell contains the IP address of the TouchLink panel.
   - HOST NAME — The hostname is a fully qualified domain name that uniquely identifies the computer. It is required for the computer to communicate with other devices on the network.
   - ROOM NAME — This is the name that appears on the touchscreen, once it is configured.
   - USER ID — Enter the ID for an account that has access to the CollegeNET server. This is typically an administrator account.
   - USER PASSWORD — enter the password for an account that has access to the CollegeNET server. This is typically an administrator account.
   - SPACE NAME — Provides the meeting information on the touchpanel. It must match exactly the Space Name setup up on the 25Live server. Check the name by searching for the Formal Name in the Locations section of 25Live.



		Name	Formal Name	Categories
		ARTS103	Daly Center Practice Rm.3	Key Card Access Only, S25 Rooms, **West Campus**, Wheelchair Accessible

Figure 56. CollegeNET 25Live Space Name

   - EVENT TYPE — Enter the appropriate name for the event type to be used by the touchpanel. These are created by the 25Live administrator. Different event types have different requirements, such as head counts, features, or registrations, when creating bookings.

     These requirements are not applicable to ad hoc events.

     The requirements for these events are not recognized by Room Agent. For an Event Type to correctly coordinate with Room Agent, it cannot have any requirements other than the Space Name and Event Type.

     Extron recommends using **Ad Hoc** as an Event Type, but you can create your own Event Type on the 25Live server.

     Verify the options in the 25Live webpage.

     1. Select the **Events** tab.
     2. Click **Types EDIT** link and select from the Event Types list.

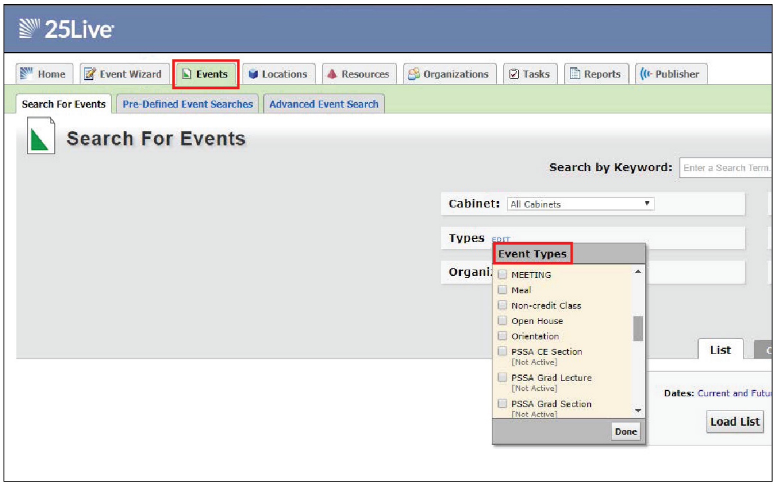


Figure 57. CollegeNET 25Live Event Type

- `CAPACITY` — Set the maximum number of people allowed in the room in this column.
- `LANGUAGE` — Select an option from the `LANGUAGE` drop-down list. By default, the language is `English`.
- `SOUND` — Set the **`Sound`** switch to **`Off`** or **`On`**. When it is set to on, pressing a button provides audible feedback. If it is set to off, there is no sound.
- `TEMPLATE`— The layout of the panel can be configured using the **`DESIGN`** Tab. You can select one of the saved panel design files from this drop-down list.
- `LOCATION` — Use a location tag to group nearby rooms, for example `Floor 1`. This is displayed as the room location in the Wayfinding Device. When rooms are shown as a list on the Wayfinding Device, they are grouped by their location tag.

There is also an `Actions` drop-down list for each touchpanel:

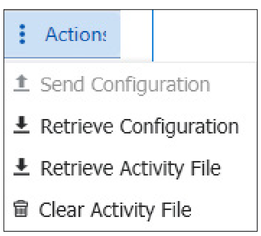


Figure 58. Configure Tab —Actions List

After verifying that the information is correct for all TLS panels, select one or more panels and click **`Send Configuration`** to save the configuration on the control PC. Alternatively, click **`Retrieve Configuration`** to retrieve a previously saved configuration and apply it to the selected panel.

You can also retrieve or clear the activity file associated with that panel (see **Room Scheduling Analytics** on page 186).

EMS

Prerequisites

NOTE: Extron recommends the Google Chrome browser for all EMS Web operations.

- The EMS Version must be version 44 or higher.
- The EMS version can be confirmed by accessing the EMS platform (typically http://<your_server_name>/EmsPlatform).
- The EMS Platform Services API must be installed.
- The EMS Web Administrator must be able to obtain client application information (see "Creating a Web Administrator for EMS", below).
- The EMS Desktop installer must have Administrator privileges.

Creating a Web Administrator for EMS

A web administrator role is required to log into the EMS administrator portal to create client IDs. Create a web Administrator as follows:

1. Open the `EMS Desktop` application and log in as an administrator, with the appropriate permissions. The application opens to the `Main Menu` (see figure 59).

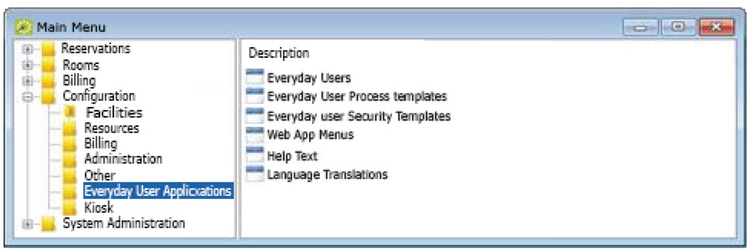


Figure 59. Main Menu

2. Click **`Configuration` > `Everyday User Applications` > `Everyday user Security Templates`**.

   The `Everyday User Security Templates` dialog box opens (see figure 60).

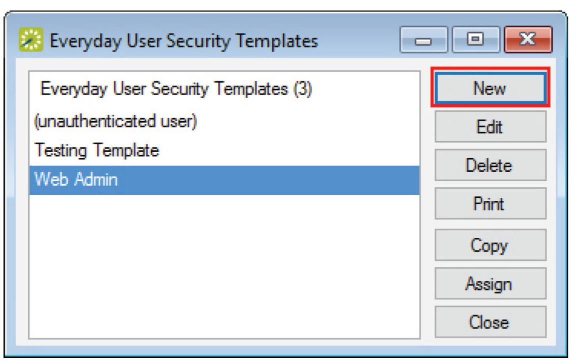


Figure 60. Everyday User Security Templates Dialog Box

3. Click **`New`**.

A new security template dialog box opens.

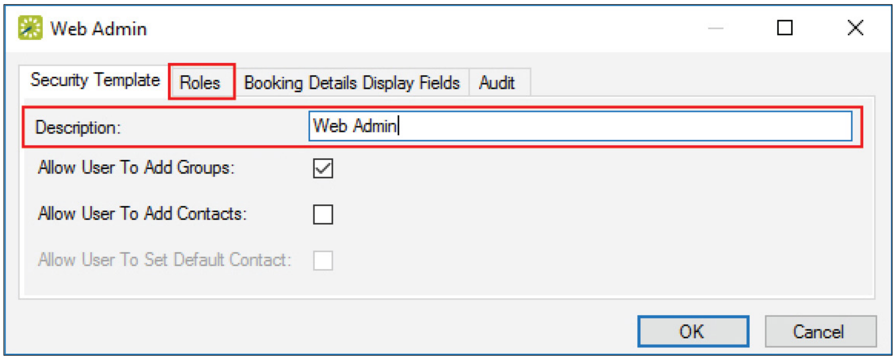


Figure 61. Security Template Dialog Box

4. Enter a description for the security template (see figure 61).
5. Click the **Roles** tab.

   The new security role dialog box opens.

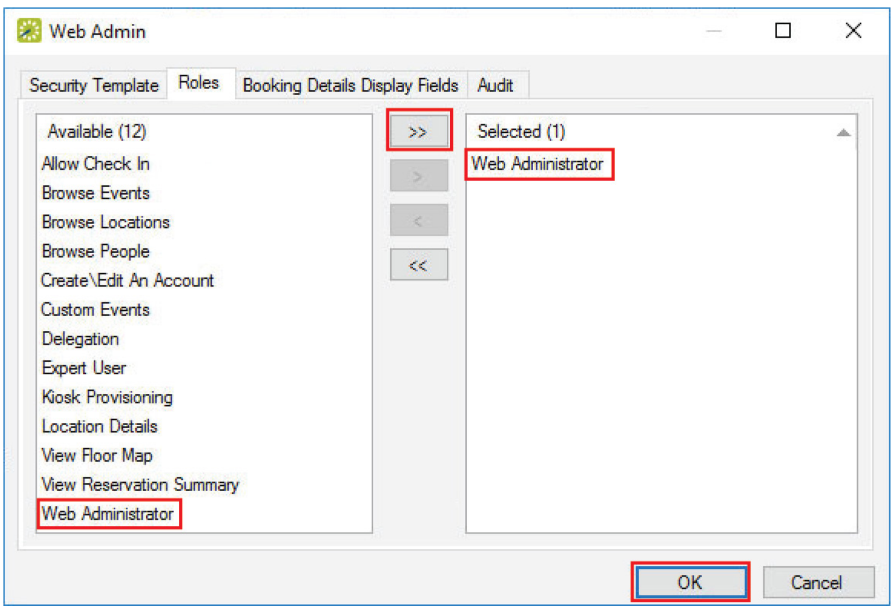


Figure 62. New Template Dialog Box

6. Click to highlight and select **Web Administrator** in the left field (see figure 62) and click the **Move Right** button (**>>**) to transfer it into the right field.
7. Move any other necessary roles to the right field.
8. Click **OK**.

EMS Setup

1. Open the **CONFIGURE** tab and select **EMS** from the `Calendar Type` drop-down list.

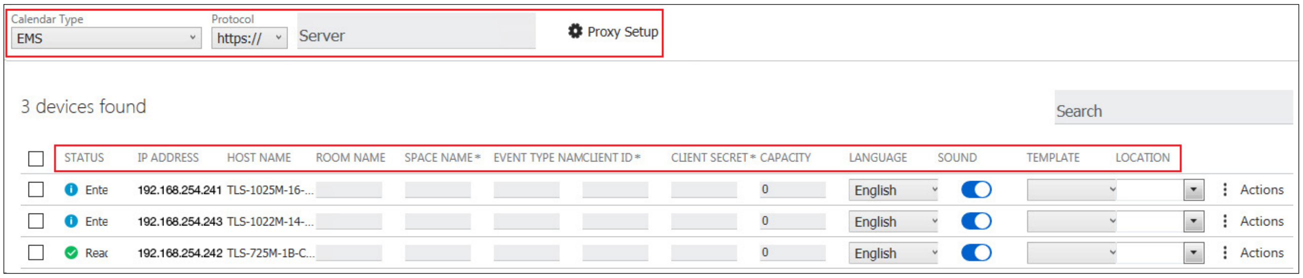


Figure 63. EMS Column Headings

2. Use the top menu bar to:
   - Select a protocol (**`http://`** or **`https://`**)

     If you use `https://` the Proxy Server must be setup as TLS Pass Through. This is required for the TLS to validate the calendar server's SSL certificate (see **Set up a Proxy Server** on page 40).
   - Enter the name of the EMS server in the `Server` field. Typically this is `https://<your_server_name>/EmsPlatform`.
3. The following column headings appear in the lists of panels:
   - `STATUS` — Use this check box to select individual panels for configuration.
   - `IP ADDRESS` — This cell contains the IP address of the TouchLink panel.
   - `HOST NAME` — The hostname is a fully qualified domain name that uniquely identifies the computer. It is required for the computer to communicate with other devices on the network.
   - `ROOM NAME` — This is the name that appears on the touchscreen, once it is configured.
   - `SPACE NAME` — This must be the same as the space listed in the EMS server. The exact space name can be found using the EMS Desktop Client.

     > **NOTE:** The list of rooms must be created by the EMS administrator prior to appearing in the EMS Desktop Client. If there are any issues getting a Room Name, please contact your EMS administrator.

     To find the `Space Name`:

     1. Open the EMS Desktop Client.
     2. Select **`Configuration`**.
     3. Select **`Facilities`**.
     4. Click **`Rooms`**.

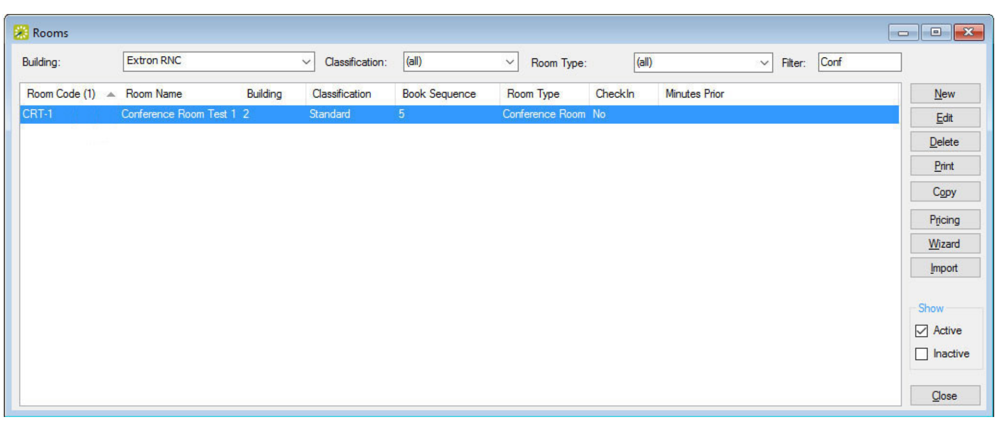


Figure 64. EMS Space Name

5. In the `Rooms` popup, enter filter options (for example the building name) to shorten the list of room names.

   The correct `Space Name` should appear in the `Room Name` column (see figure 64).

- `EVENT TYPE NAME` — This is the event type to be used for ad hoc meetings booked on behalf of the scheduling panel. The EMS server requires a `template name` or `Event Type`, when a new meeting is booked. This information can be obtained from the EMS Desktop Client.

> **NOTE:** The list of `Event Types` must be created by the EMS administrator prior to appearing in the EMS Desktop Client. If there are any issues getting a Room Name, please contact your EMS administrator.

1. Open the EMS Desktop Client.
2. Select **`Configuration`**.
3. Select **`Other`**.
4. Click **`Event Types`**.

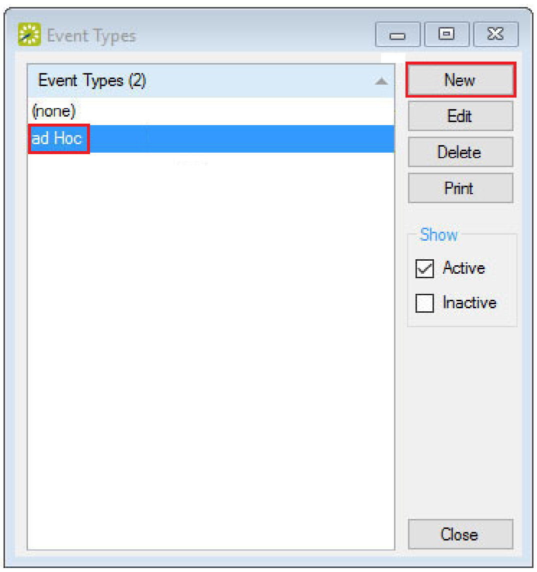


Figure 65. EMS Event Types Dialog

The `Event Types` dialog lists the event types that can be used on the server. In this example, `ad hoc` is the appropriate `Event Type` name (see figure 65).

5. If no event types are listed or you wish to create a new event type, click **`New`**.

   The `Event Type` dialog box opens:

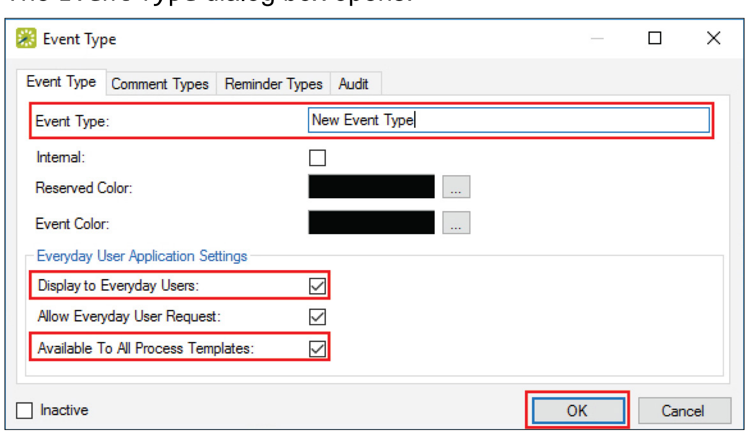


Figure 66. Event Type Dialog Box

6. Enter a name in the `Event Type` field (see figure 66).

7. Check **Display to Everyday Users** and **Available to All Process Templates**.
8. Click **OK**.

   The dialog box closes and the display returns to the Event Type page.

   NOTE: Enter this name in the `Event Type Name` field of the `CONFIGURATION` tab. The name is case sensitive.

- `CLIENT ID` — This is a unique client ID generated by EMS to use the API. It grants a secure point for the panels to communicate with the server. Before third-party clients can access the EMS API, a valid `Client ID` must be generated.

NOTES:

- You may use the default EMS Web Application ID or a new client can be created in the administrator console. The new client must be created by an EMS administrator.
- You can use a single client for all touchpanels or create multiple clients that are each associated with a subset of panels.

1. Log in to the administrator console.

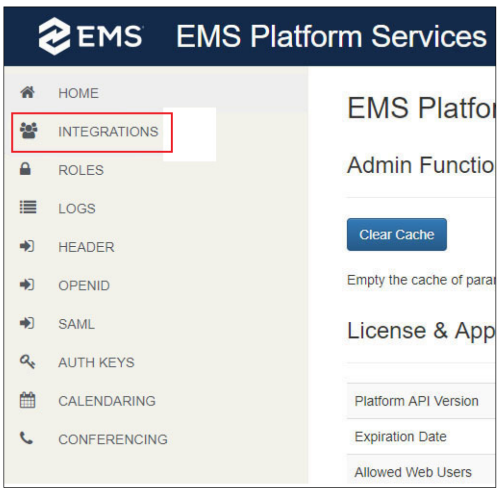


Figure 67. EMS Administrator Console Home

2. Select **INTEGRATIONS** (see figure 67).

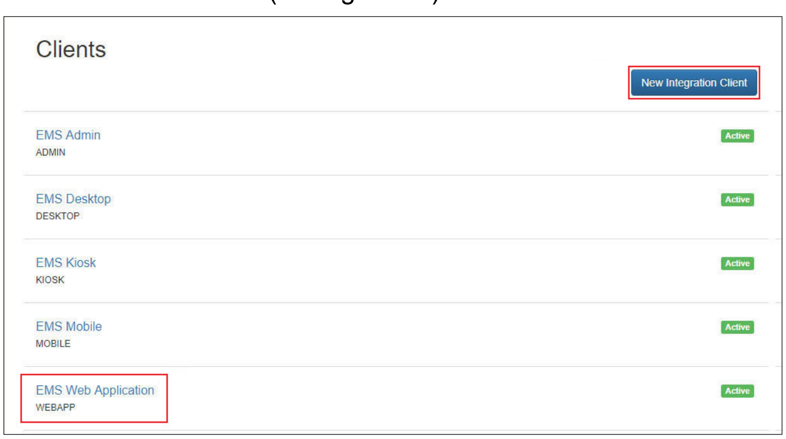


Figure 68. EMS Clients

3. Select the appropriate web client. In this example, the default is shown (see figure 68).
4. To use a new client, click **New Integration Client**.

The `Clients/New` page opens:

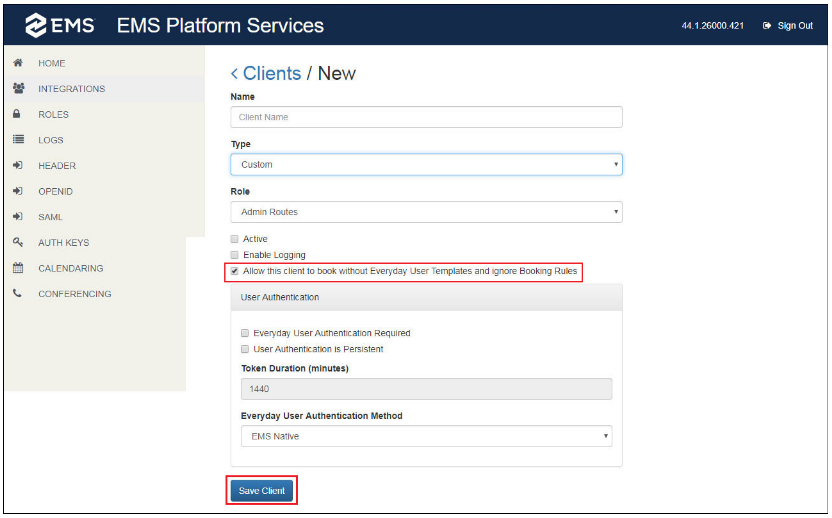


Figure 69. EMS Clients/New Page

5. Configure the new client as recommended by your EMS representative.
6. How the client is configured depends on your requirements and is beyond the scope of this guide. However, to allow touchpanels to make ad hoc bookings, you must select **`Allow this client to book without Everyday User Templates and ignore Booking Rules`** (see figure 69).
7. Click **`Save Client`**.

   The `Clients/New` page closes and the `EMS Web Clients` page opens with the new client listed.
8. Click the new client.

   Whether you clicked on a new or existing client, the `Clients/EMS Web Application` page opens.

   The `Client ID` listed (see figure 70) is the one required by Room Agent.

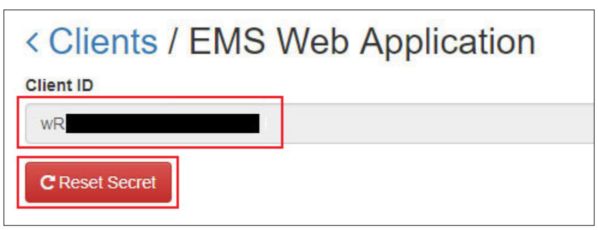


Figure 70. EMS Client ID

- `CLIENT SECRET` — This is a number generated by the EMS web site (see figure 70), which is required for secure communication between the touchpanels and the EMS calendar server.
  1. Click **`Reset Secret`**.
  2. A pop-up opens, warning `This action is permanent. Would you like to continue?` Click **`OK`**.
  3. The `Client Secret` is displayed (it is blurred out in figure 71).

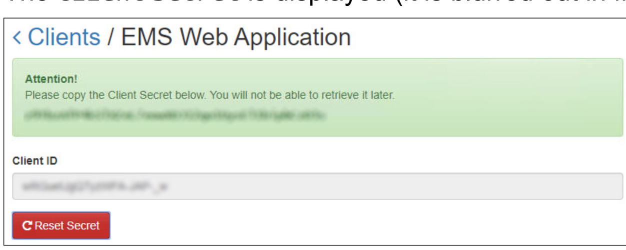


Figure 71. EMS Client Secret

4. Copy the `Client Secret` into the Room Agent `CONFIGURE` tab.

   NOTE: This is the only time this code is displayed. You must copy it now and store it in a safe location to continue using it.

- `CAPACITY` — Set the maximum number of people allowed in the room in this column.
- `LANGUAGE` — Select an option from the `LANGUAGE` drop-down list. By default, the language is **`English`**.
- `SOUND` — Set the **`SOUND`** switch to **`Off`** or **`On`**. When it is set to **`On`**, pressing a button provides audible feedback. If it is set to **`Off`**, there is no sound.
- `TEMPLATE`— The layout of the panel can be configured using the `DESIGN` tab. You can select one of the saved panel design files from this drop-down list.
- `LOCATION` — Use a location tag to group nearby rooms, for example “Floor 1”. This is displayed as the room location in the Wayfinding Device. When rooms are shown as a list on the Wayfinding Device, they are grouped by their location tag.

There is also an `Actions` drop-down list for each touchpanel:

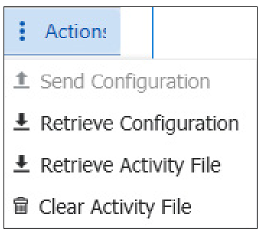


Figure 72. Configure Tab —Actions List

After verifying that the information is correct for all TLS panels, select one or more panels and click **`Send Configuration`** to save the configuration on the control PC. Alternatively, click **`Retrieve Configuration`** to retrieve a previously saved configuration and apply it to the selected panel.

You can also retrieve or clear the activity file associated with that panel (see **Room Scheduling Analytics** on page 186).

Google Calendar™

If you select **`Google Calendar`**, you can have multiple devices using the same calendar or multiple calendars.

When you use Google, Microsoft Exchange, or Office 365 calendars, you can create private meetings. For these meetings, the subject title defaults to `Private Meeting` and the meeting organizer is hidden.

1. Open the **`CONFIGURE`** tab and select **`Google Calendar`** from the `Calendar Type` drop-down list.

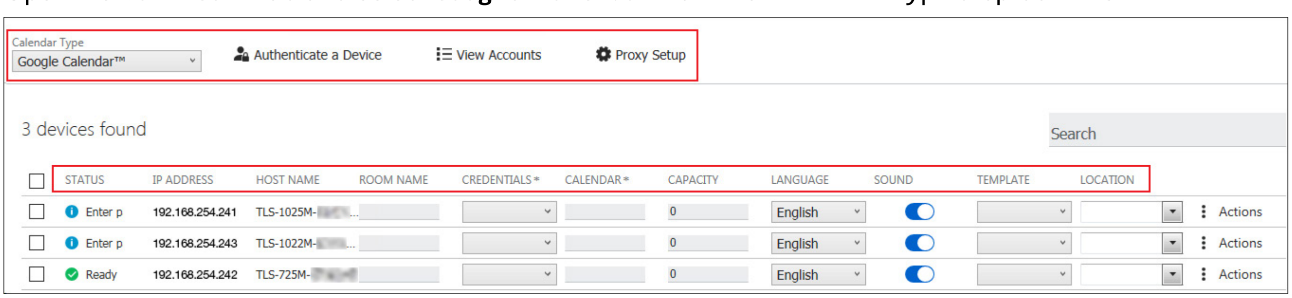


Figure 73. Google Calendar Column Headings

2. Use the top menu bar to:
   - Select a protocol (**http://** or **https://**)

     If you use `https://` the Proxy Server must be setup as TLS Pass Through. This is required for the TLS to validate the calendar server SSL certificate (see **Set up a Proxy Server** on page 40).
   - Select a touchpanel and click **Authenticate a Device** to connect to the calendar that is to be associated with that touchpanel. You must have downloaded a JSON file (see **Google Calendar Overview** on page 56 or **Step 3: Authenticate a Device to Google** on page 62).
   - You may also click View all available accounts, which shows all the Google accounts providing the calendars.
3. The following column headings appear in the lists of panels:
   - `STATUS` — Use this check box to select individual panels for configuration.
   - `IP ADDRESS` — This cell contains the IP address of the TouchLink panel.
   - `HOST NAME` — The hostname is a fully qualified domain name that uniquely identifies the computer. It is required for the computer to communicate with other devices on the network.
   - `ROOM NAME` — This is the name that appears on the touchscreen, once it is configured.
   - `CREDENTIALS` — Google Calendar allows you to use multiple calendars. Select the account that is being used for that touchpanel (see **Google Calendar Overview**).
   - `CALENDAR` — Select the calendar for the account that is being used (see **Google Calendar Overview**).
   - `CAPACITY` — Set the maximum number of people allowed in the room in this column.
   - `LANGUAGE` — Select an option from the `LANGUAGE` drop-down list. By default, the language is `English`.
   - `SOUND` — Set the **SOUND** switch to **Off** or **On**. When it is set to **On**, pressing a button provides audible feedback. If it is set to **Off**, there is no sound.
   - `TEMPLATE`— The layout of the panel can be configured using the **DESIGN** tab. You can select one of the saved panel design files from this drop-down list.
   - `LOCATION` — Use a location tag to group nearby rooms, for example `Floor 1`. This is displayed as the room location in the Wayfinding Device. When rooms are shown as a list on the Wayfinding Device, they are grouped by their location tag.

There is also an `Actions` drop-down list for each touchpanel:

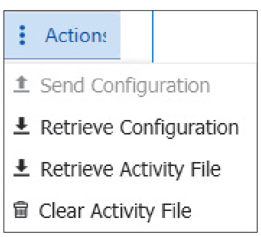


Figure 74. Configure Tab —Actions List

After verifying that the information is correct for all TLS panels, select one or more panels and click **Send Configuration** to save the configuration on the control PC. Alternatively, click **Retrieve Configuration** to retrieve a previously saved configuration and apply it to the selected panel.

You can also retrieve or clear the activity file associated with that panel (see **Room Scheduling Analytics** on page 186).

Google Calendar Overview

Step 1: Creating Resource Accounts

> **NOTE:** This section is required if you wish to use Google Calendar resources with the Room Scheduling system. If you are using existing user or personal Gmail account calendars, go to **Step 2: Creating Access Credentials** on page 58.

1. Log in to the Google `Admin` console at **https://admin.google.com/**.

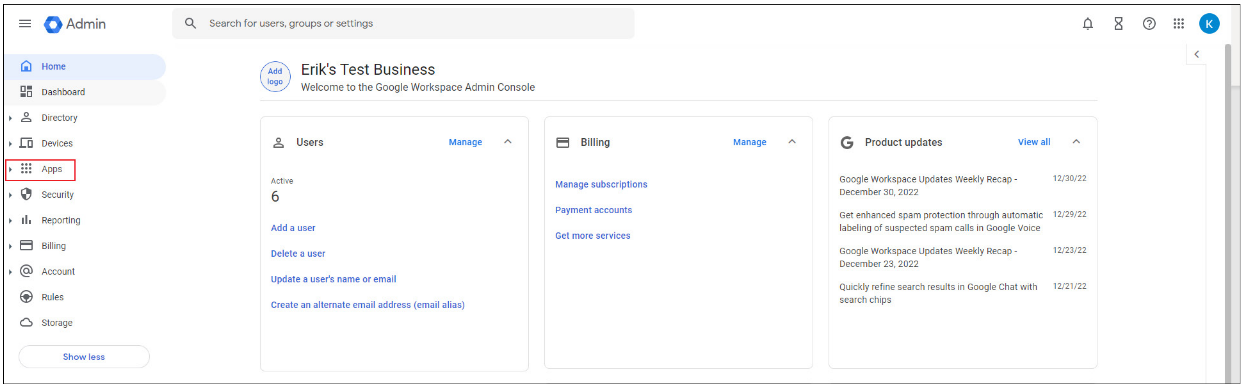


Figure 75. Google Admin Console

2. From the console, select **`Apps`** (see figure 76).

The `Apps` menu expands.

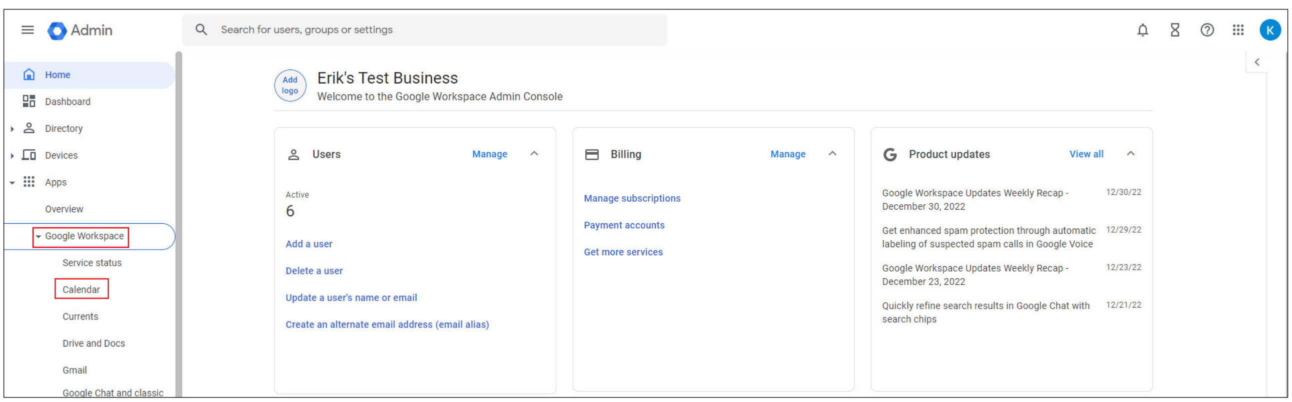


Figure 76. Apps Window

3. Click **`Google Workspace`** (see figure 76).

4. Double-click **`Calendar`**.

> **NOTES:**
>
> - Double-click an app name to configure the service in a new window.
> - Select or deselect a checkbox to turn the corresponding service off or on.
> - If `Calendar` is not available, you need to click **`Add Service`**.

The `Calendar` window opens.

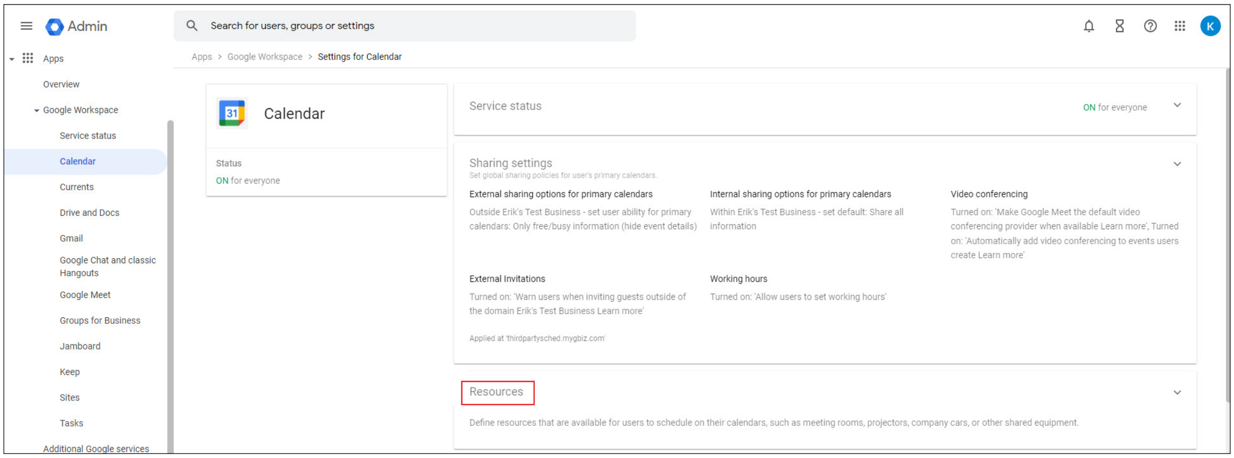


Figure 77. Google Calendar page

5. Click **`Resources`** (see figure 77).

   The `Resources` window opens.

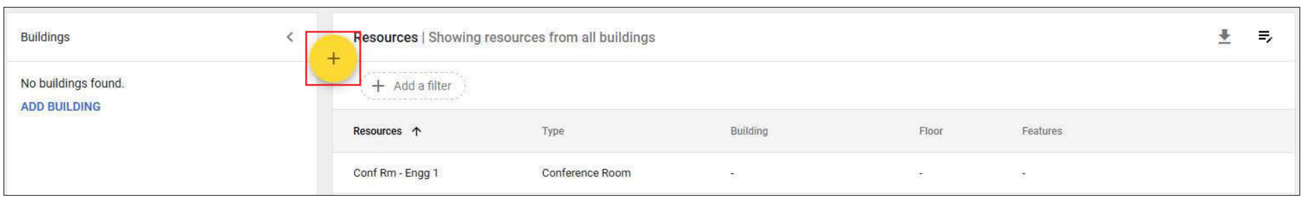


Figure 78. Resources Window

6. Click **+** to add a new resource (see figure 78).

   The `Add resource` window opens with a newly created resource.

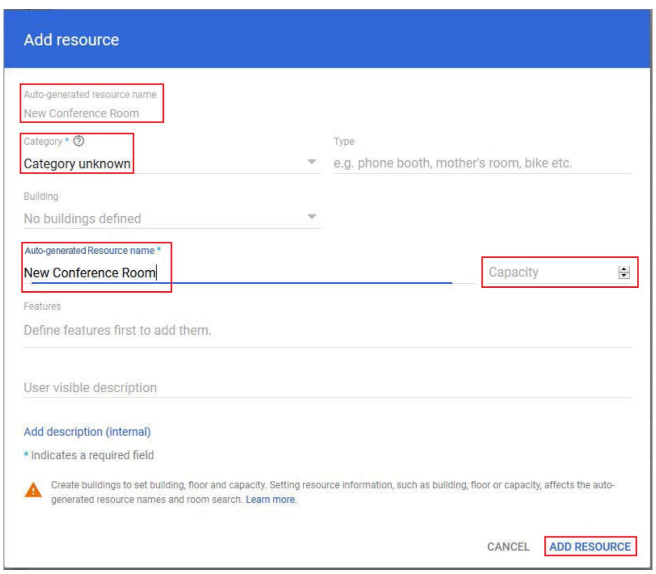


Figure 79. Add Resources Window

The `Auto-generated resource name` (see figure 79) initially shows as `-123456789.contoso.com`. The `Resource name` field is initially empty but is a required field.

As the user enters more information, it is concatenated to the auto-generated resource name.

For example, if the user enters `room-1` in the `Resource name` field, the Auto-generated resource name shows `room-1-123456789.contoso.com`.

If the user now enters `20` in the optional capacity field, the Auto-generated resource name shows `room-1-123456789.contoso.com (20)`.

> **NOTES:**
> - Resources created before or during October 2017 may not have the `Category` set (see **figure 79** on page 57).
> - In some environments, `Auto-generated Resource name` may appear as `Resource name` + *<Domain>* + *<Capacity>*, if `Capacity` is entered.

7. After adding the information, click **`ADD RESOURCE`**.

   The `Add resource` window closes. The Resources window (see **figure 78** on page 57) now lists the new resource that has been added.

> **NOTE:** Make a note of the resource name exactly as it appears here. The name is required when you set up Room Agent.

Step 2: Creating Access Credentials

> **NOTE:** As of December 2021 this information is correct. However, this site is not controlled by Extron and may change.

1. Open the `Google Cloud Platform` Dashboard.

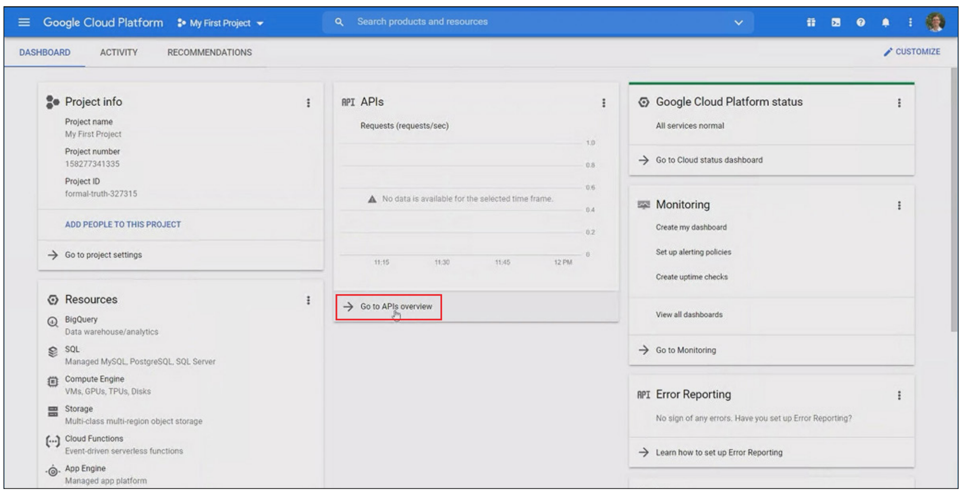


Figure 80. Google Cloud Platform Dashboard

2. Click **`Go to APIs overview`** (see figure 80).

The `APIs & Services` page opens.

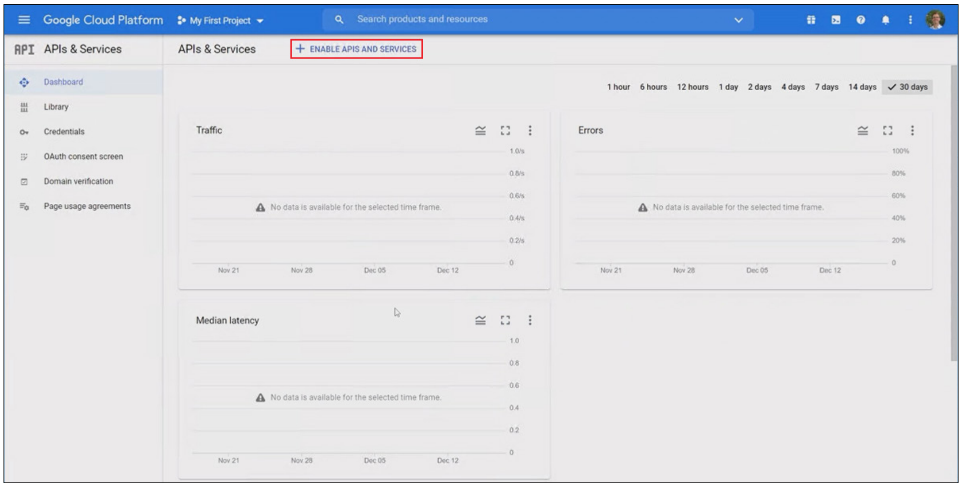


Figure 81. APIs & Services page

3. Click **`+ ENABLE APIS AND SERVICES`** (see figure 81).

   The `API Libarary` page opens.

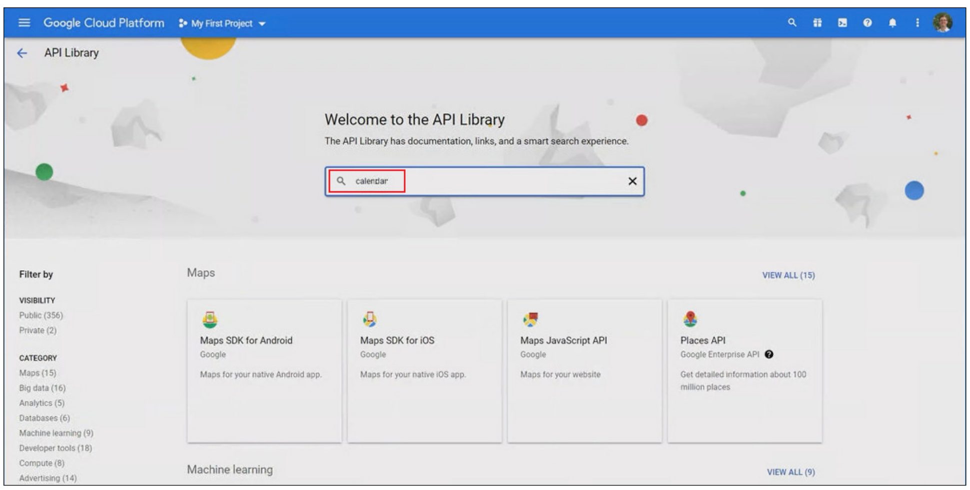


Figure 82. API Library

4. Enter `Calendar` in the search window (see figure 82) and click **`<Enter>`**.

   A list of available calendars is shown.

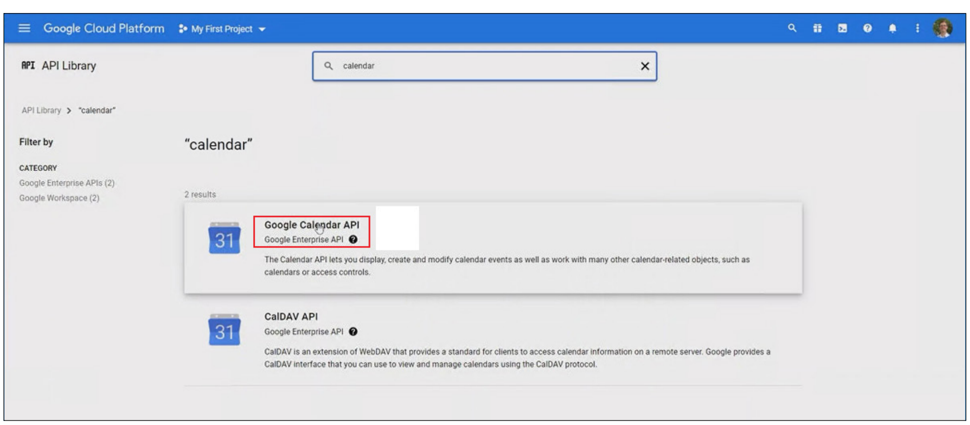


Figure 83. Search Results for "Calendar"

5. From the search results, select **`Google Calendar API`** (see figure 83).

The `Google Calendar API` page opens.

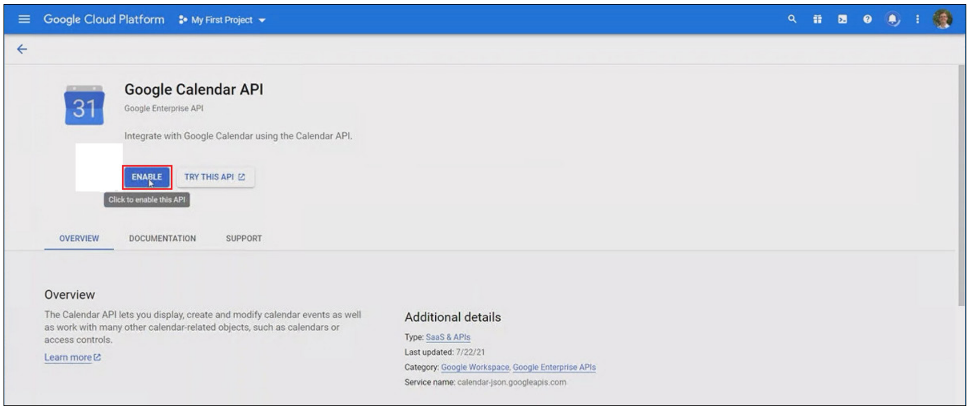


Figure 84. Google Calendar API Page

6. Click **`ENABLE`** (see figure 84).

   The `Overview` page opens.

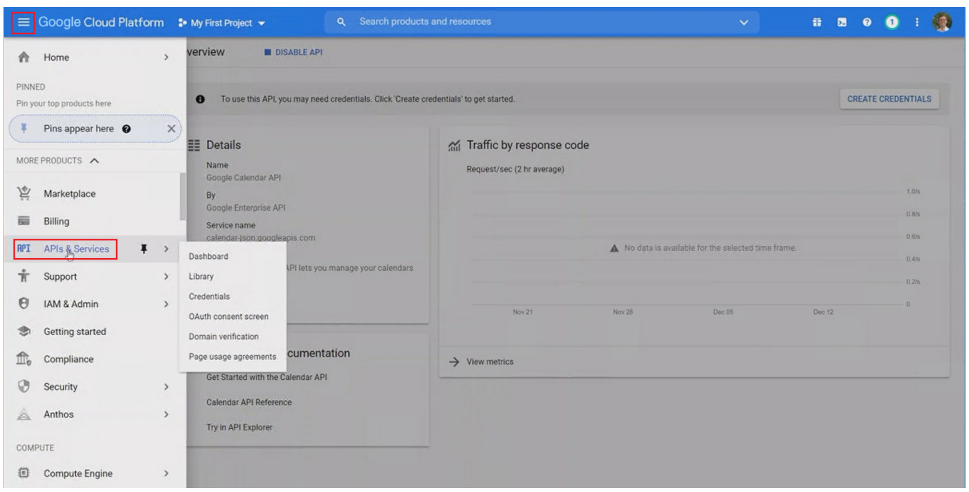


Figure 85. Overview Page

7. Click the **`menu`** icon in the top left corner (see figure 85).
8. From the drop-down list, click **`APIs & Services`**.

   The `APIs & Services` page opens.

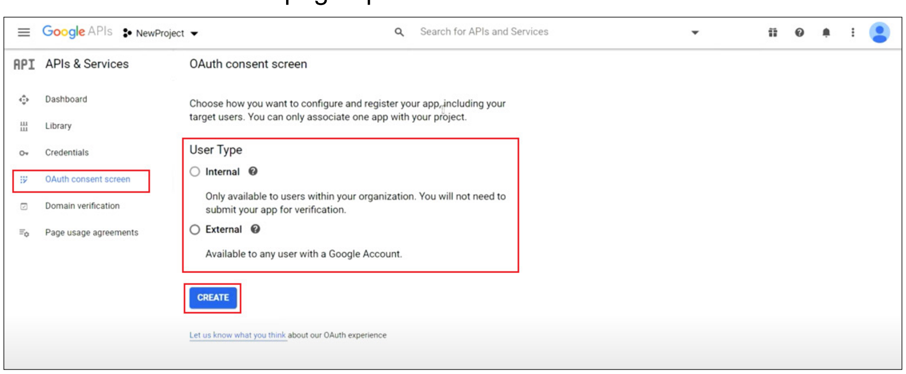


Figure 86. APIs & Services page

9. Click **`OAuth consent screen`** (see figure 86).
10. Select the **`User Type`** for your app, then click **`Create`**.

11. Complete the app registration form, then click **Save and Continue**.
12. If you are creating an app for use outside of your Google Workspace organization, click **Add or Remove Scopes**.
13. Add and verify the authorization scopes required by your app, then click **Save and Continue**.
14. If you selected **External** for user type, add `test users`:
    a. Under `Test users`, click **Add users**.
    b. Enter an `email address` for the user.
    c. Repeat steps a and b to add any other authorized test users
    d. Click **Save and Continue**.
15. Review your app registration summary. To make changes, click **Edit**. If the app registration looks okay, click **Back to Dashboard**.

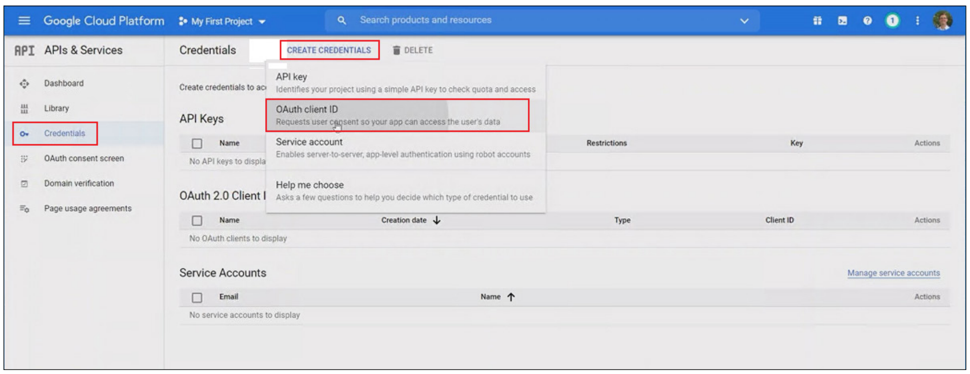


Figure 87. APIs & Sevices Page

16. In the menu at the left of the screen, click **Credentials** (see figure 87).
17. On the page that opens next, click **CREATE CREDENTIALS**.
18. From the drop-down list, click **OAuth client ID**.

    The `Create OAuth client ID` page opens.

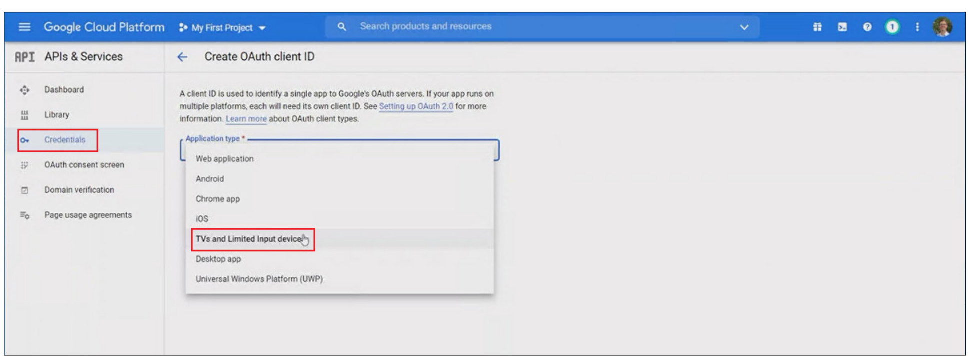


Figure 88. Create OAuth client ID Page

19. Click **Application type** (see figure 88).

    The `Application type` drop-down list opens.
20. Click **TVs and Limited Input devices**.

The `Application type` drop-down list closes.

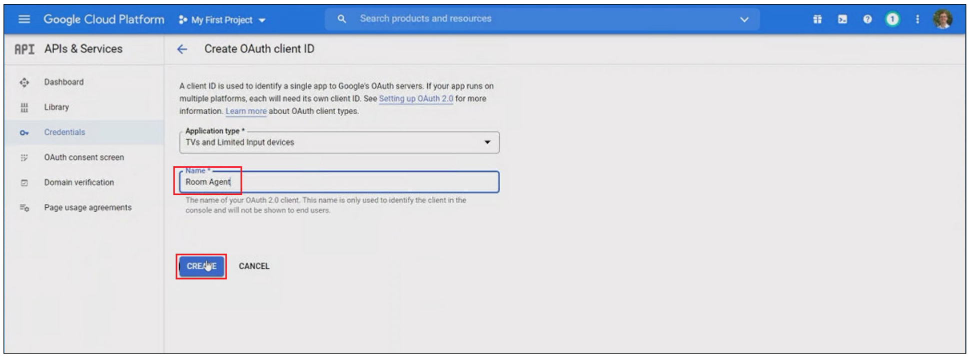


Figure 89. Create OAuth client ID Page

21. Enter a name in the `Name` field (see figure 90).

22. Click **`CREATE`**.

The `OAuth client created` dialog box opens.

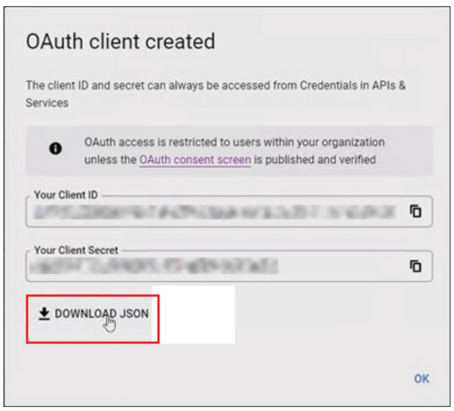


Figure 90. OAuth Client Created Dialog Box

23. Click **`DOWNLOAD JSON`** (see figure 90).

24. Save the `.json` file and make a note of where it was saved.

Step 3: Authenticate a Device to Google

1. Open Room Agent and click on the **`CONFIGURE`** tab.

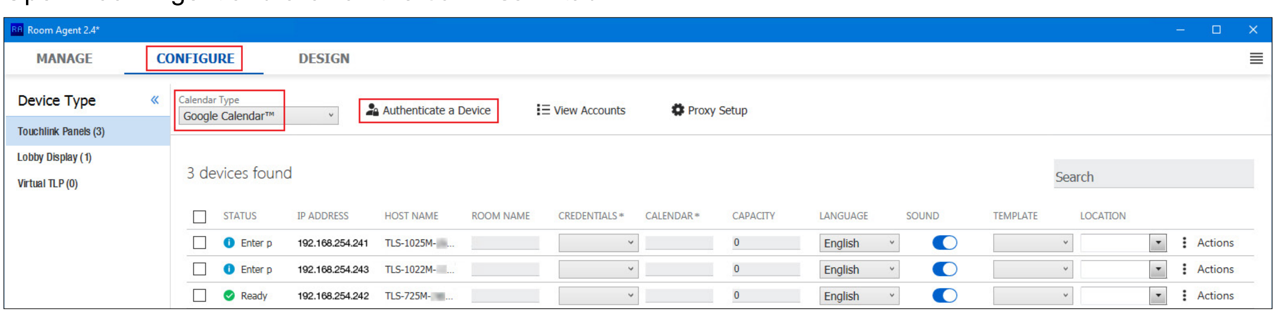


Figure 91. Room Agent CONFIGURE Tab

2. Select **`Google Calendar™`** from the `Calendar Type` drop-down list (see figure 91).

3. Click **`Authenticate a Device`**.

The `Authenticate a Device to Google` dialog box opens.

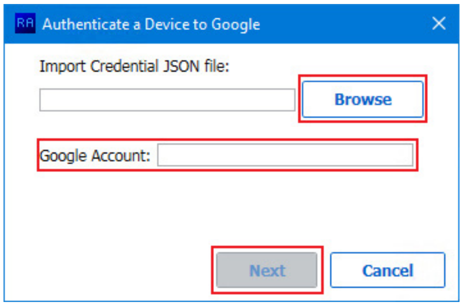


Figure 92. Authenticate a Device to Google dialog box

4. Click **`Browse`** (see figure 93) and navigate to the location of the JSON file saved in **step 23** of the previous section, on page 62.
5. Enter the `Google Account` name. This can be any character string that allows you to identify the account.
6. Click **`Next`**.

   The `Authenticate a Device to Google` dialog box displays the user code (see figure 93).

Figure 93. User Code

   This code is valid for 30 minutes.

7. Scan the **`QR`** or click the **https://www.google.com/device** link.

   The `Connect a Device` dialog box opens.

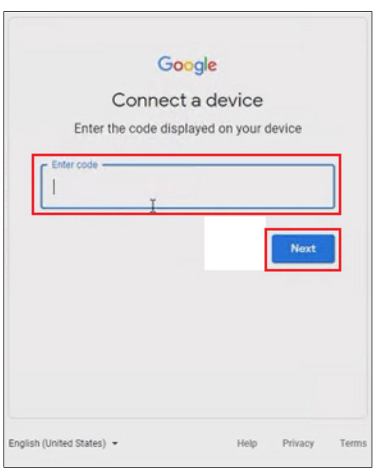


Figure 94. Connect a Device dialog box

8. Enter the user code from step 6 (see figure 93).
9. Click **`Next`** (see figure 94).

The `Sign in with Google` dialog box opens:

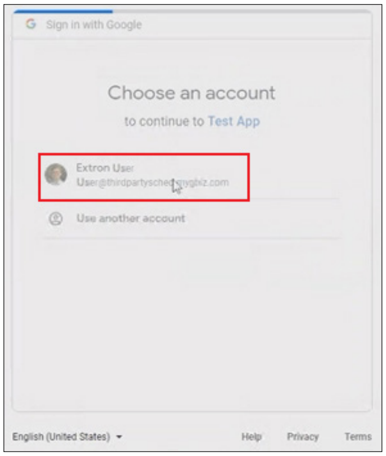


Figure 95. Choose an Account

10. Select an account (see figure 95).

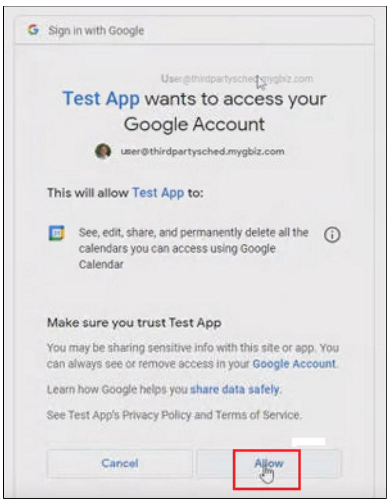


Figure 96. Allow Google to Access your Account

11. Click **`Allow`** to permit Google to access your Google account (see figure 96).

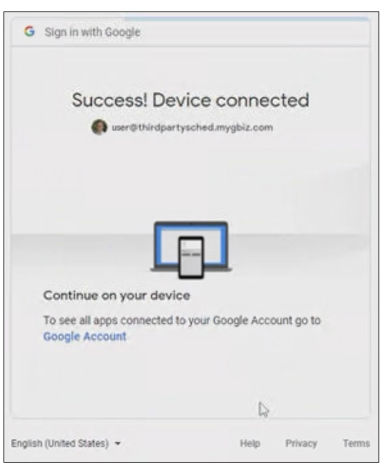


Figure 97. Device Connected

When Google is able to connect to your account, the `Success! Device connected` message is shown.

The `Sign In with Google` window closes and you return to Room Agent.

12. Click `Check Authentication` Status.

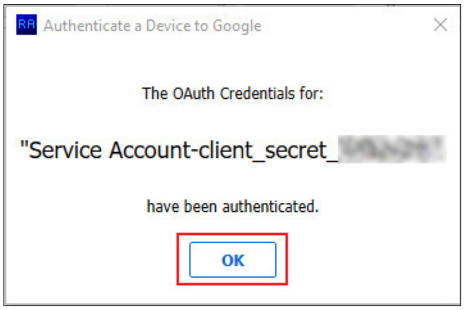


Figure 98. Authentication Complete

Room Agent shows `The OAuth Credentials for` *`<service account name>`* `have been authenticated`.

13. Click `OK` (see figure 98).

The new account is added to the list of available accounts and can be viewed by either of the following methods:

- By clicking `View accounts` at the top of the `CONFIGURE` tab (see figure 99).

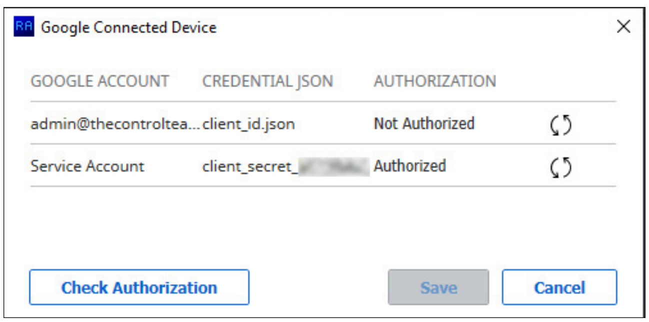


Figure 99. View all available accounts

- By clicking on the `CREDENTIALS` cell of any of the panels listed on the `CONFIGURE` tab. A drop-down list shows the available accounts (see figure 100).

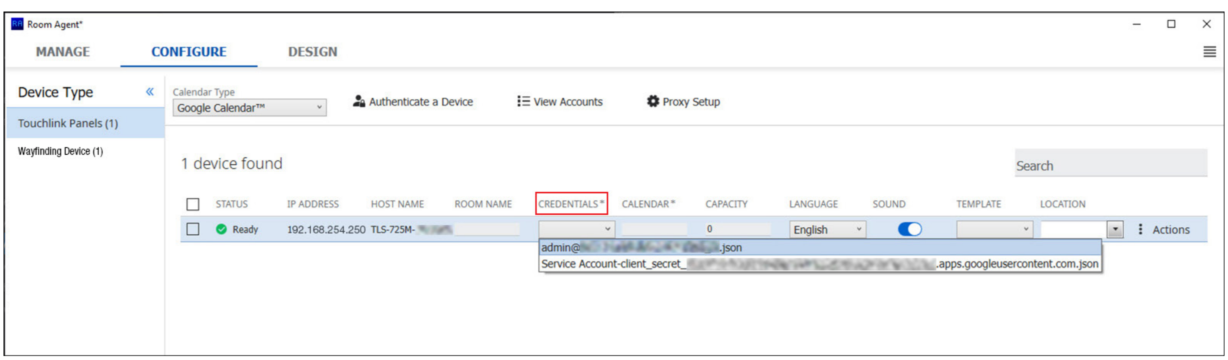


Figure 100. Google Account Cell

Troubleshooting

If a Room Agent configuration has been loaded onto the TouchLink Scheduling Panel but the touchpanel is showing that the panel is disconnected (red ellipses in the lower right corner of the panel), verify the following items:

- Make sure that the Google Account in the Room Agent software and the account that approved the user code in your browser are the same.
- Go to **https://console.developers.google.com/** and verify that you can see traffic from the panel. This updates periodically and shows the requests made to the project that was created when setting up the JSON file.

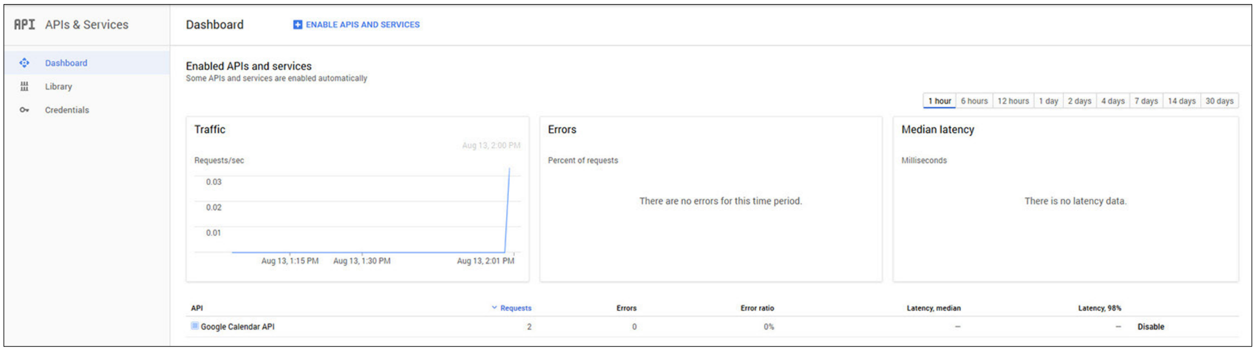


Figure 101. Google Dashboard Showing Traffic from the Panel

If you are using Calendar Resources but only the Google Service Account calendar is showing, make sure the `Account Calendar` in Room Agent matches exactly the `Calendar Resource name` as it appears in the Google `Admin Console` (including special character for numbers and occupancy if added when creating the panel).

In order for the TouchLink Scheduling Panel to read the calendar, the `Admin` account must be subscribed to the Room Account Calendar as follows:

1. While logged in with the Admin account, go to `calendar.google.com`.

Figure 102. Open Other Calendars

2. Click the **+** icon next to the `Other Calendars` section.

Figure 103. Select Subscribe to Calendar

3. Click on the **`Subscribe to calendar`** option.

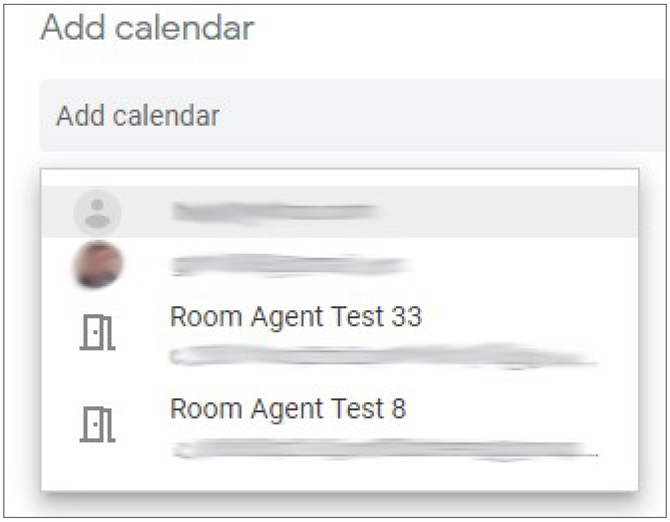


Figure 104. Select Calendar

4. Select a calendar from the dropdown list.

Microsoft Exchange

The Extron Room Scheduling System works with the following Microsoft Exchange versions:

- Exchange 2007, Service Pack 1
- Exchange 2010
- Exchange 2013
- Exchange 2016

In Exchange servers, the Room Scheduling System uses the Exchange Web Services (EWS) protocol to tie in to the server room mailboxes; no plugins or additional software are required on the server.

The Room Scheduling System subscribes to the room mailboxes. The EWS protocol includes push notifications. The server pushes change notifications to the Room Scheduling System whenever calendar changes occur.

NOTES:

- Room Agent provides an additional feature when you use the Microsoft Exchange or Microsoft Office 365 calendars. In the `DESIGN` Tab, the drop-down lists contain an additional `Custom Field` option, which displays up to 50 characters from the body of the meeting invitation.
- When you use Google, Microsoft Exchange, or Office 365 calendars, you can create private meetings. For these meetings, the subject title defaults to Private Meeting and the meeting organizer is hidden.
- With Microsoft Exchange, each conference room is assigned a unique Room Mailbox. This is a special type of mailbox that is restricted so that it cannot be used for interactive logons (the ability to send or receive emails).
- The fully qualified domain name (`name@domain.com`) must be entered as the user ID.
- As part of the Room Agent configuration process, the Microsoft Exchange user ID and password for each room are entered by the administrator and sent as part of the configuration file to the panel. No other user IDs or passwords are used.
- The software encrypts the password; when displayed on the user interface it is obscured, and it is encrypted when stored on the administrator PC.
- The administrator can choose to save the panel configurations, including the panel passwords, on their PC. This file is password protected.

1. Open the **CONFIGURE** tab and select **Microsoft® Exchange™** from the `Calendar Type` drop-down list.

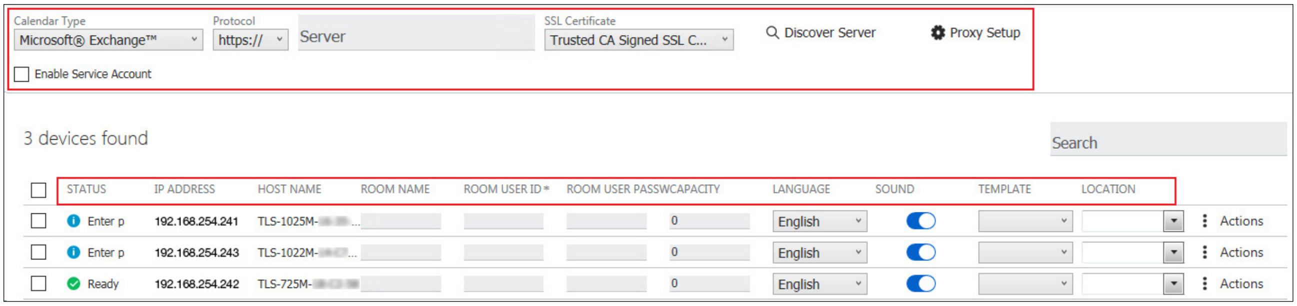


Figure 105. Selecting Microsoft Exchange Calendar

1. Click **Discover Server** (see figure 106) to search for the Microsoft Exchange server.
2. If you click **Discover Server** but Room Agent cannot discover the server automatically, a dialog box opens. Enter your email credentials and click **Discover**.

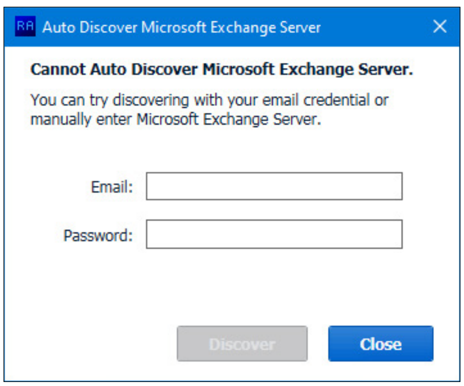


Figure 106. Auto Discover Microsoft Exchange Server Dialog

3. Click **Protocol** (see figure 106) and select **http://** or **https://**.

   To use the `https://` protocol to connect to the Microsoft Exchange Calendar, the Proxy Server must be set up as **TLS Pass Through**. This is required for the TLS to validate the calendar server SSL certificate (see **Set up a Proxy Server** on page 40).

4. Click inside the `Server` text box and enter the address of the server.
5. Select whether the `SSL Certificate` is verified.

   Room Agent validates certificates that are signed by trusted Certificate Authorities. If the Exchange server is using self-signed SSL certificates, selecting **No Verification of SSL Certificate** bypasses this option. This option should normally left at the default selection. If you are unsure, consult the Exchange administrator for the connecting server.

6. Select the checkbox to **Enable Service Account** (see **Set Up a Service Account** on page 70).

> **NOTE:** The **Enable Service Account** checkbox allows one or more service accounts to be used to configure the panels.

7. The following column headings appear in the lists of panels:
   - `STATUS` — Use this check box to select individual panels for configuration.
   - `IP ADDRESS` — This cell contains the IP address of the TouchLink panel.
   - `HOST NAME` — The host name is a fully qualified domain name that uniquely identifies the computer. It is required for the computer to communicate with other devices on the network.

- ROOM NAME — This is the name that appears on the touchscreen, once it is configured.

> **NOTE:** If you select the **Enable Service Account** checkbox (see **figure 105** on page 68), the Room User ID column heading changes to Service Account, and the Room User Password column heading changes to Room Resource Account.

- ROOM USER ID — Enter the ID for an account that has access to the Microsoft server. This is typically an administrator account.

  User ID requires the User Principal Name (UPN, the name of a Windows network user in an SMTP e-mail address format) for the room resource user ID. The UPN must have an SMTP e-mail address assigned to it. Abbreviated Exchange User IDs (aliases) do not work. (See **Verify the Exchange User ID is the UPN** on page 73.)

- ROOM USER PASSWORD — Enter the password for an account that has access to the Microsoft server. This is typically an administrator account. .

> **NOTES:**
> - If service accounts are enabled, the Room User ID and Room User Password column headings change to Service Account and Room Resource Account.
> - The Exchange User ID requires the User Principal Name (UPN: the name of a Windows network user in an e-mail address format) for the room resource user ID. The UPN must have an SMTP e-mail address assigned to it

- CAPACITY — Set the maximum number of people allowed in the room in this column.
- LANGUAGE — Select an option from the LANGUAGE drop-down list. By default, the language is English.
- SOUND — Set the **Sound** switch to **Off** or **On**. When it is set to **On**, pressing a button provides audible feedback. If it is set to **Off**, there is no sound.
- TEMPLATE— The layout of the panel can be configured using the DESIGN tab. You can select one of the saved panel design files from this drop-down list.
- LOCATION — Use a location tag to group nearby rooms, for example Floor1. This is displayed as the room location in the Wayfinding Device. When rooms are shown as a list on the Wayfinding Device, they are grouped by their location tag.

There is also an Actions drop-down list for each touchpanel:

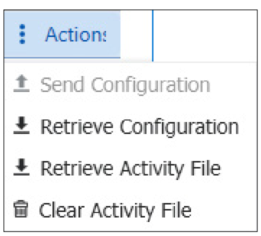


Figure 107. Configure Tab —Actions List

After verifying that the information is correct for all TLS panels, select one or more panels and click **Send Configuration** to save the configuration on the control PC. Alternatively, click **Retrieve Configuration** to retrieve a previously saved configuration and apply it to the selected panel.

You can also retrieve or clear the activity file associated with that panel (see **Room Scheduling Analytics** on page 186).

Set Up a Service Account

Service accounts allow the user to manage multiple touchpanels from a single account. When passwords are updated, only the service account password needs to be changed, not the passwords for all the individual touchpanels in the account.

NOTE: The service account requires the UPN, the name of a Windows network user in an e-mail address format. The UPN must have an SMTP e-mail address assigned to it.

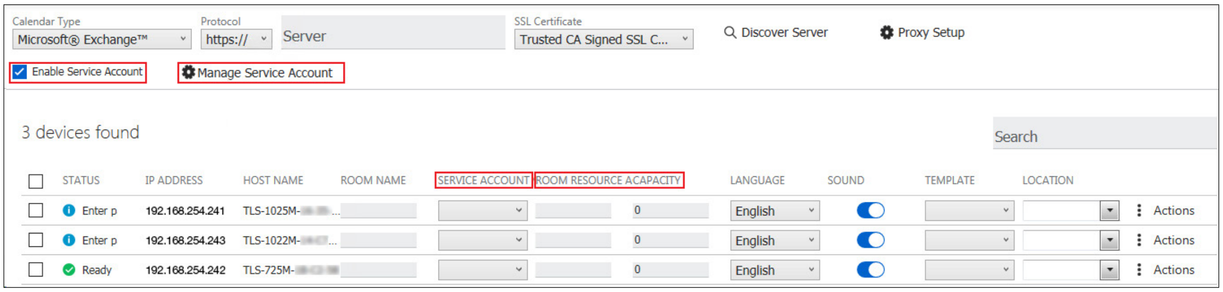


Figure 108. Microsoft Exchange Service Account

To set up a service account:

1. Select the **`Status`** check boxes of the touchpanels to be configured.
2. Check the **`Enable Service Account`** checkbox (see figure 108).

   When the checkbox is enabled, a new `Service Account Manager` button appears.

   The `Room User ID` column heading changes to `Service Account.`

   The `Room User Password` column heading changes to `Room Resource`.
3. Click **`Manage Service Account`**.

   The `Service Account Manager` dialog opens with the **`Assign Service Account`** tab selected.

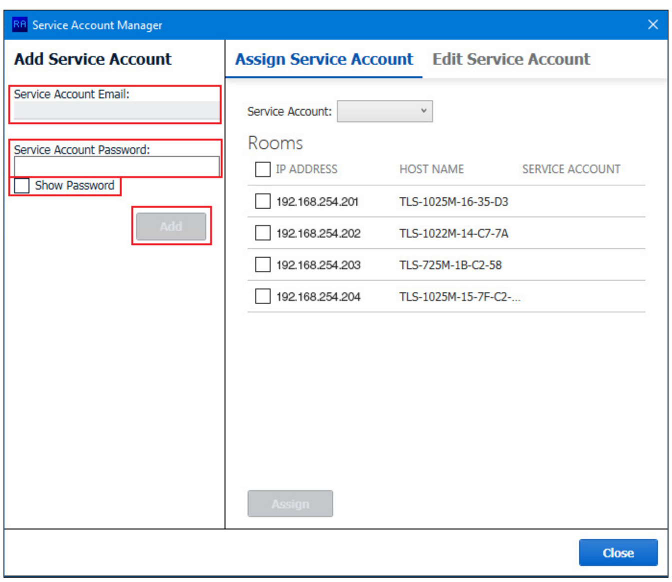


Figure 109. Service Account Manager — Assign Service Account

4. Enter a `Service Account Email` (see figure 109).
5. Enter a `Service Account Password`.
6. If you select the **`Show Password`** checkbox, the characters of the password are visible. If you do not select the checkbox, the characters are masked by filled circles.
7. Click **`Add`**.

The `Service Account Email` is added to the `Service Account` dropdown list (see figure 110).

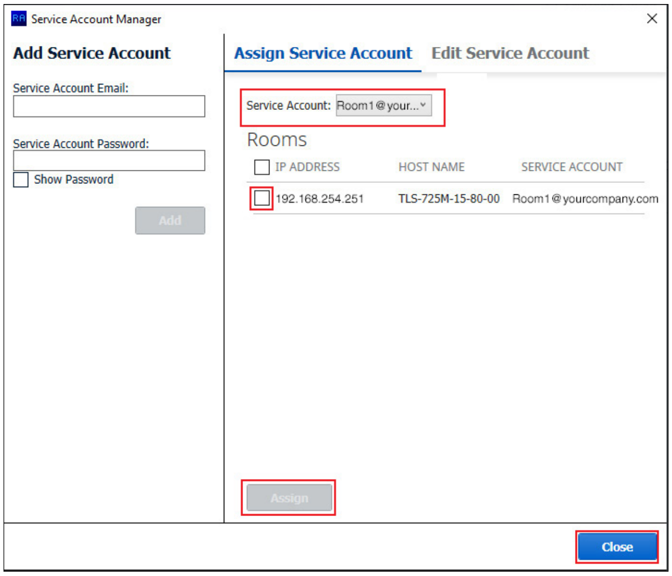


Figure 110. Service Account Email Added to Service Account List

If required, additional service accounts can be created and added to the `Service Account` list.

To assign one or more touchpanels to a service account:

1. Select the checkbox next to each of those touchpanels.
2. Ensure that the correct service account is selected from dropdown menu.
3. Click **`Assign`**.

   The service account name appears next to the selected TLS panels.
4. Repeat steps 1-3 to add touchpanels to another service account.
5. Once all the touchpanels are assigned as required, click **`Close`**.

   In the main **`CONFIGURE`** tab, the service account associated with the panel is now shown.

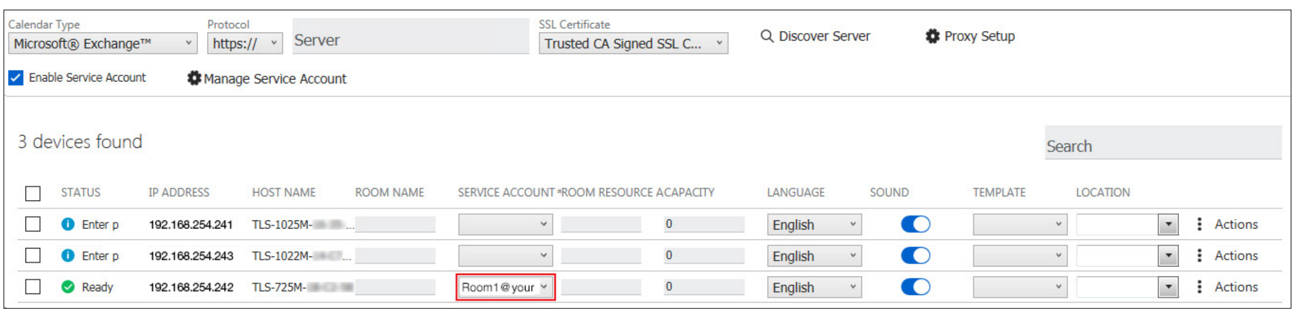


Figure 111. Configure Tab with Service Accounts Added

Once one or more service accounts have been added, using `Manage Service Account`, you can add that service account from the main **`CONFIGURE`** tab. Click on the **`Service Account`** cell for the appropriate touchpanel. A dropdown menu is now accessible, listing all the available service accounts.

> **NOTE:** In the main **`CONFIGURE`** tab you can add only one touchpanel at a time to a specific service account. With `Manage Service Account`, you can select multiple touchpanels and add them all to a service account simultaneously.

Enter the room email address in the `Room Resource Account` column.

> **NOTE:** You can assign some TLS panels in your system to service accounts and other TLS panels can be individually configured. However, Extron recommends that the system configurations used to save TLS panels associated with service accounts should be separate from those used to save individually configured TLS panels.

Delete a Service Account

1. In the **`CONFIGURE`** tab, click **`Manage Service Account`**.
2. Click the **`Edit Service Account`** tab.

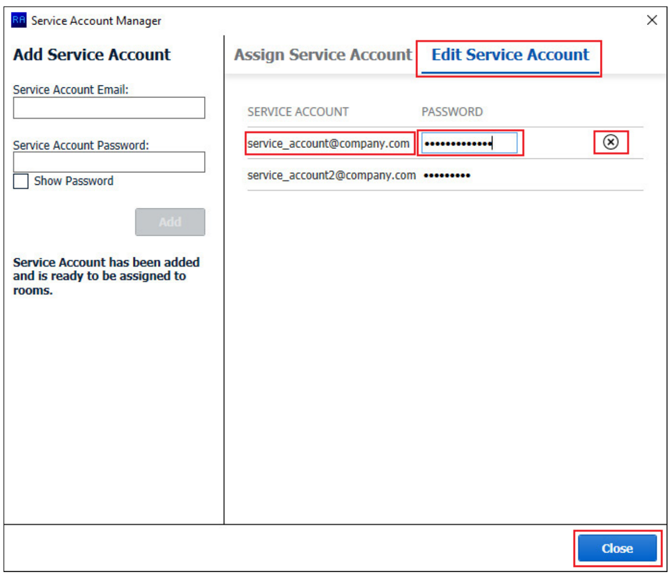


Figure 112. Service Account Manager — Edit Service Account

All the available service accounts are listed.

3. To delete an account, click on the account. Click the delete (**`X`**) button for that row.

Edit a Service Account

1. Double-click in the **`Password`** field for the service account to be edited (see figure 112).
2. Highlight the password and type a new value.
3. Press **`<Enter>`** on the keyboard.

> **TIP:** The `PASSWORD` field is normally masked (•••). When the existing password is deleted, the **`Show`** option activated. Click **`Show`** to toggle between viewing or masking the password characters as you type.

4. Click **`Close`** to save the changes and exit the `Service Account Manager` dialog.

Verify the Exchange User ID is the UPN

Verify the UPN as follows:

1. Access the Exchange server `Active Directory Users and Computers` window.

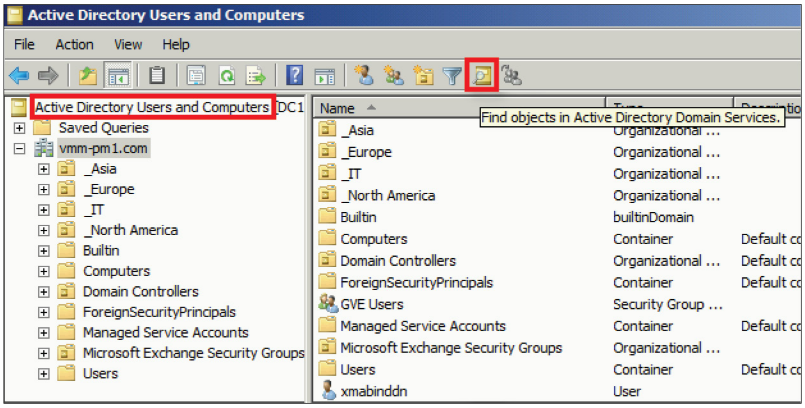


Figure 113. Active Directory

2. Click the **`Find Object`** ( ) icon (see figure 113).

   The `Find Users, Contacts, and Groups` dialog box opens.

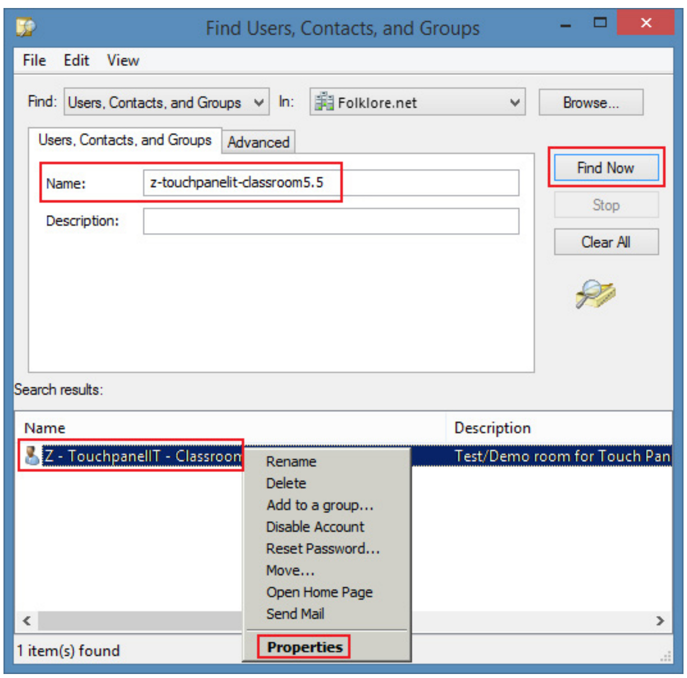


Figure 114. Find Users, Contacts, and Groups Dialog Box

3. Enter the name of the room to be verified in the `Name` field (see figure 114).
4. Click **`Find Now`**.

   The `Search results:` pane displays the room.
5. **`<Right-click>`** the room in the `Search results:` pane and click **`Properties`**.

The `Properties` dialog box opens.

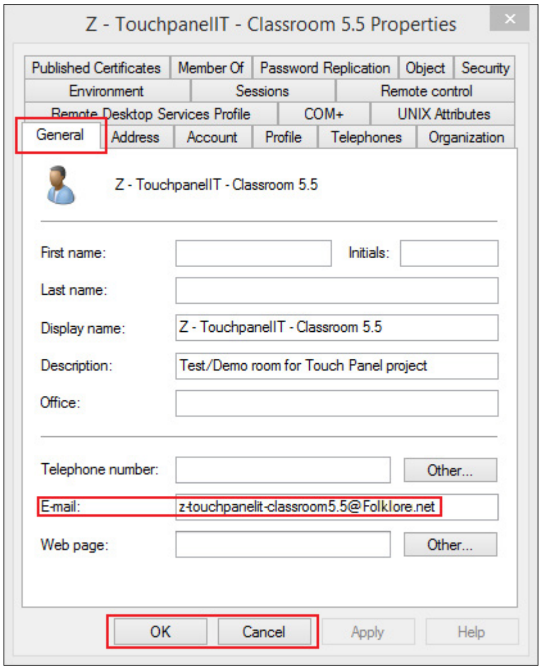


Figure 115. E-mail Address Displayed on the General Tab

6. If necessary, click the **`General`** tab (see figure 115). The general properties for the room are displayed.
7. Note the room `E-mail` address shown. This value is the UPN, the value used as the only valid `Exchange User ID` for this room in the Room Scheduling System.
8. Click **`OK`** or **`Cancel`** to exit the display.
9. Repeat steps 3 through 8 for each desired room. .

TIP:	Write down the UPNs of all rooms for setting up the Room Scheduling System.

Microsoft Office 365

NOTES:

- Room Agent provides an additional feature when you use the Microsoft Office 365 calendar. In the **`DESIGN`** tab, the drop-down lists contain an additional `Custom Field` option, which displays up to 50 characters from the body of the meeting invitation.
- When you use `Google`, `Microsoft Exchange`, or `Office 365` calendars, you can create private meetings. For these meetings, the subject title defaults to `Private Meeting` and the meeting organizer is hidden.
- Microsoft is planning to end single-factor authorization in Oct 2020 and has moved to 2-factor authorization (OAuth).

When QR code authentication is enabled with TLS x25 or TLS 300 models, the TLS can be configured to require a user to authenticate via a QR code to perform actions such as reserve, release, extend, and checkin. Microsoft O365 requires additional configuration. For information about setting up this feature, see **QR Authentication for MS Office 365** on page 76.

For Microsoft Office 365, the QR code feature is supported exclusively with the Microsoft Client Secret and Microsoft Certificate authentication methods only.

Microsoft Office 365 provides three different ways to obtain OAuth credentials. These are described in the **Oauth for Office 365** on page 77. Use the information provided to decide which method you wish to use and follow the link to the section for that method. These pages also describe how to assign the OAuth credentials to the touchpanels.

Microsoft Office 365 also supports Microsoft Government Community Cloud (GCC). GCC High uses different endpoints for Microsoft Graph compared to commercial environments. Instead of the standard graph.microsoft.com, the solution will be interacting with graph.microsoft.us .gov etc.

1. Open Room Agent and select the **`CONFIGURE`** tab.
2. Select **`Microsoft® Office 365™`**.

   The server address is discovered automatically. The server address and protocol (`https://`) cannot be altered.

   To use the `https://` protocol to connect to the Microsoft Office 365, the Proxy Server must be set up as **`TLS Pass Through`**. This is required for the TLS to validate the calendar server SSL certificate (see **Set up a Proxy Server** on page 40).

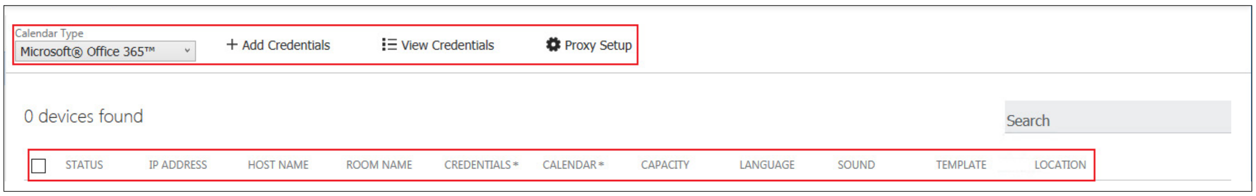


Figure 116. Microsoft Office CONFIGURE menu

3. With Microsoft Office 365, you get the following column headings:
   - `STATUS` — Use this check box to select individual panels for configuration.
   - `IP ADDRESS` — This cell contains the IP address of the TouchLink panel.
   - `HOST NAME` — The hostname is a fully qualified domain name that uniquely identifies the computer. It is required for the computer to communicate with other devices on the network.
   - `ROOM NAME` — This is the name that appears on the touchscreen, once it is configured.
   - `CREDENTIALS` — This is the name that was used when the device was authenticated to Office365.
   - `CALENDAR` — This is the account that provides authorization for Room Agent to access the calendar (see **Assigning Oauth Credentials to Touchpanels** on page 110 and **Verify the UPN** on page 75).
   - `CAPACITY` — Set the maximum number of people allowed in the room in this column.
   - `LANGUAGE` — Select an option from the `LANGUAGE` drop-down list. By default, the language is **`English`**.
   - `SOUND` — Set the **`Sound`** switch to **`Off`** or **`On`**. When it is set to **`On`**, pressing a button provides audible feedback. If it is set to **`Off`**, there is no sound.
   - `TEMPLATE` — The layout of the panel can be configured using the `DESIGN` tab. You can select one of the saved panel design files from this drop-down list.
   - `LOCATION` — Use a location tag to group nearby rooms, for example `Floor 1`. This is displayed as the room location in the Wayfinding Device. When rooms are shown as a list on the Wayfinding Device, they are grouped by their location tag.

Verify the UPN

1. From `https://portal.azure.com/#home` go to **`Microsoft Entra ID`**.
2. Select **`Users`** from the manage section of the menu on the left.
3. Find the desired user account in the list and check the 2nd column of the table labeled `User Principal Name` (UPN).
4. Make sure the UPN is used in the calendar field in Room Agent.

There is also an `Actions` drop-down list for each touchpanel:

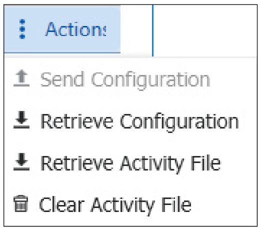


Figure 117. Configure Tab —Actions List

After verifying that the information is correct for all TLS panels, select one or more panels and click **`Send Configuration`** to save the configuration on the control PC. Alternatively, click **`Retrieve Configuration`** to retrieve a previously saved configuration and apply it to the selected panel.

You can also retrieve or clear the activity file associated with that panel (see **Room Scheduling Analytics** on page 186).

QR Authentication for MS Office 365

The Azure app registration needs an additional Microsoft Graph delegated API permission added, openid. Additionally, all users wanting to use this feature need to be added to the app registration. For directions on how to add an API permission or users to your Azure App registration, see section Obtaining OAuth Credentials.

For Microsoft Office 365, the QR code feature is supported exclusively with the Microsoft Client Secret and Microsoft Certificate authentication methods only.

Always Needed	Assignment Required ON	Assignment Required OFF
• Allow Public Client Flows toggle ON. • openID delegated API permission added by an Azure admin.	• Users booking and rooms being booked must be added to the app registration. • Admin approval of a user upon first use.	• Room being booked must be added to the app registration.

1. Navigate to `Microsoft Azure` then click **`Microsoft Entra ID`**.
2. Click **`Enterprise Applications`** then select your app registration.

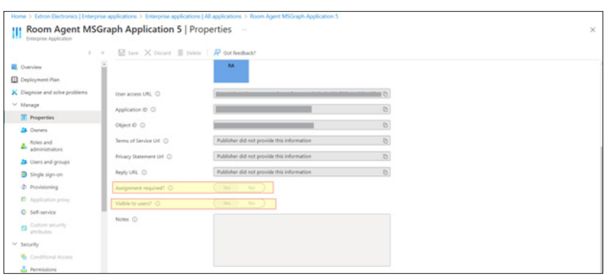


Figure 118. Enterprise Applications: App Registration

3. In the manage section click on **`Properties`**.
4. Enable the **`Visible to Users`** toggle.
5. Decide whether you want to enable the **`Assignment Required`** toggle. If disabled, anyone in the tenant will be able to use this feature. If enabled, first time QR code users will need to be approved by an admin.

   If you disable the **`Assignment Required`** toggle, no further action is required.

   If **`Assignment Required`** is enabled, the steps for approving a first-time user are as follows:
6. From the `Microsoft Azure` home page, click **`Microsoft Entra ID`**, then **`Enterprise Applications`**.
7. In the `Security` section, click **`Consent and Permissions`**, then **`Admin consent settings`**.

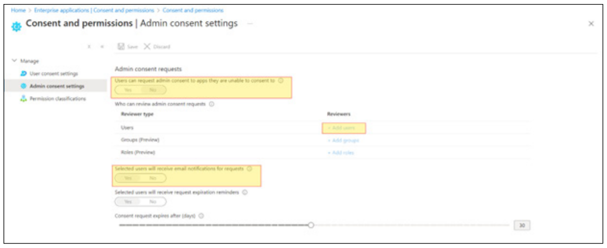


Figure 119. Admin consent settings

8. Enable the first 2 toggles and add any users that will review admin consent requests.
9. When a user attempts to authenticate with a QR code for the first time, they will be shown this screen:

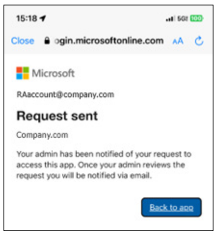


Figure 120. User Request Sent

10. Have an Azure admin navigate from the `Azure` home page to `Microsoft Entra ID`.
11. Click on **`Enterprise Applications`** on the left side menu.
12. In the `Activity` section of the `Enterprise Applications` menu, click **`Admin consent requests`**.
13. Click on the name of the application that the user requesting access is associated with. The `details` menu appears.
14. Click **`Review permissions and consent`**. A dialog asking you to login to the admin account appears.
15. Once the admin account is authenticated, click **`accept`** on the `Permissions requested` dialog. The user can now use QR codes to interact with the TLS. This process must be repeated for each user.

Oauth for Office 365

This section provides an overview of the three methods for obtaining Office 365 OAuth Credentials. Read the following information carefully and decide which method is best for your organization. Once you have decided on a method, click on the link for that method to see a complete description of that method.

Which Microsoft OAuth Workflow is Right for My Organization?

	Client Secret	Certificate Upload	Device Code
Maximum Lifetime	2 Years	Configurable	90 Days
Required Information	Client ID Tenant ID Credential Server URL Calendar Server URL Client Secret	Client ID Tenant ID Credential Server URL Calendar Server URL Certificate Thumbprint Certificate File Private Key File Private Key Password (optional)	Client ID Tenant ID Credential Server URL Calendar Server URL
3rd party purchase required?	No	3rd Party purchase from certificate authority required	No
Admin approval required for Azure permissions?	Yes	Yes	No

NOTE: Client Secret and Certificate Upload workflows are not supported for TLS 520, TLS 720, TLS 1020, and TLS 1022 devices.

- **Use Client Secret Workflow** on page 79
- **Use Certificate Upload Workflow** on page 91
- **Use Device Code Workflow** on page 102

GCC

Room Agent 2.6 and later versions support Microsoft 365 Government Community Cloud (GCC), which uses different endpoints for Microsoft Graph. Commercial environments use the standard graph.microsoft.**com**. GCC solutions intereact with graph.microsoft.**mil**, .**us**, .**gov**, etcetera.

When obtaining Office 365 OAuth Credentials, ensure that the proper permissions (delegated or application) are set for the Graph API access or EWS access.

In Room Agent, update the credential server URL and calendar server URL as necessary (e.g., .mil, .us, .gov). The default settings are configured for standard 365 services.

- Credential server URL (example: `login.microsoftonline.gov`)
- Calendar server URL (example: `graph.microsoft.gov`)

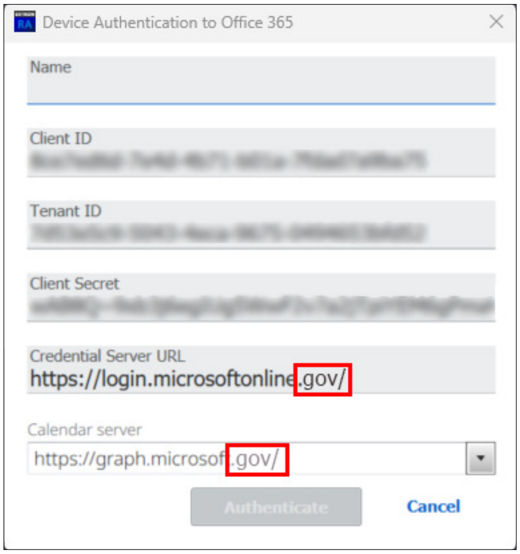


Figure 121. Device Authentication with GCC

These updates apply regardless of the authentication method chosen.

Use Client Secret Workflow

This section describes how to obtain Microsoft Office 365 OAuth credentials using the Client Secret workflow and how to assign those credentials to the Room Agent touchpanels.

- **Obtaining OAuth Credentials** (see page 79)
- **Assigning Credentials to Touchpanels** (see page 90)

Obtaining OAuth Credentials

> **NOTE:** Client Secret and Certificate Upload workflows are not supported for TLS 520, TLS 720, TLS 1020, and TLS 1022 devices.

To obtain OAuth credentials using client secret authorization, follow these steps.

1. Go to **https://portal.azure.com/**.

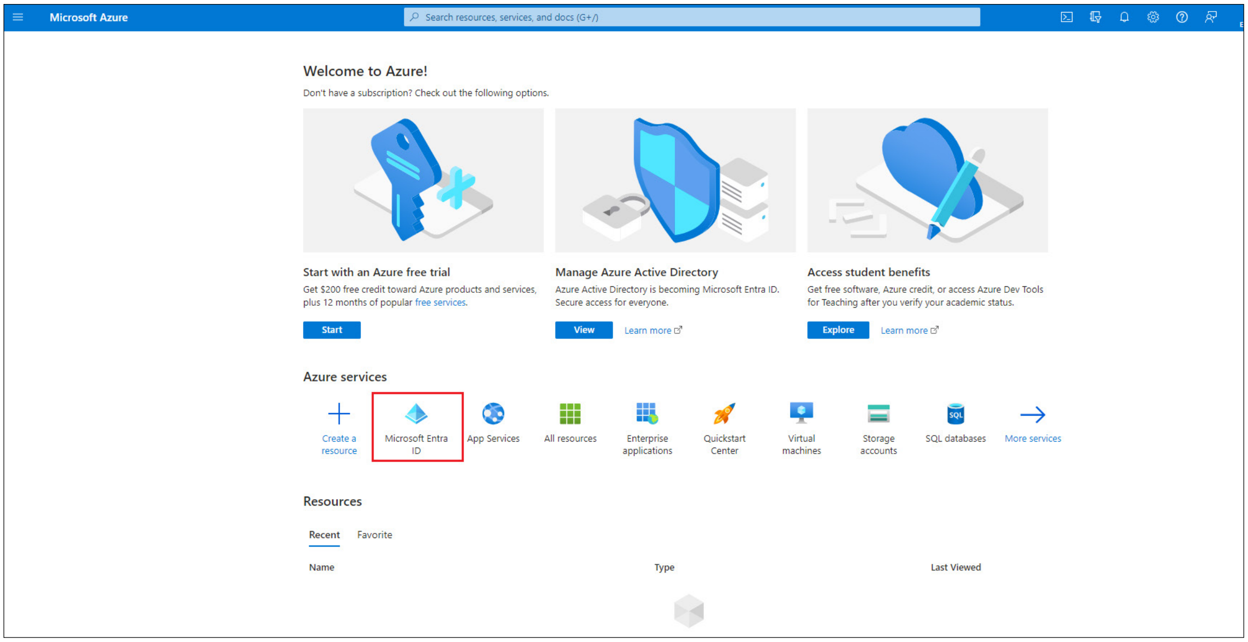


Figure 122. Microsoft Azure Website

2. Click `Microsoft Entra ID`.

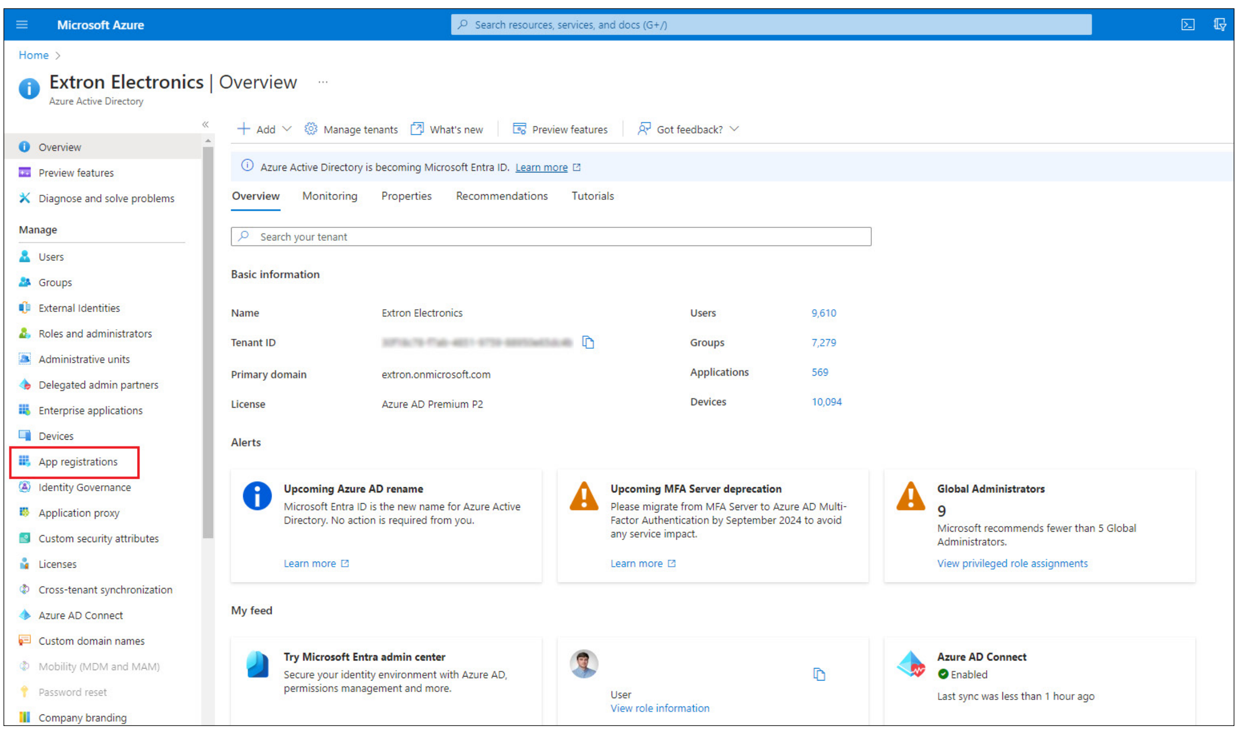


Figure 123. Company Page on Microsoft Website

3. Click `App registrations`.

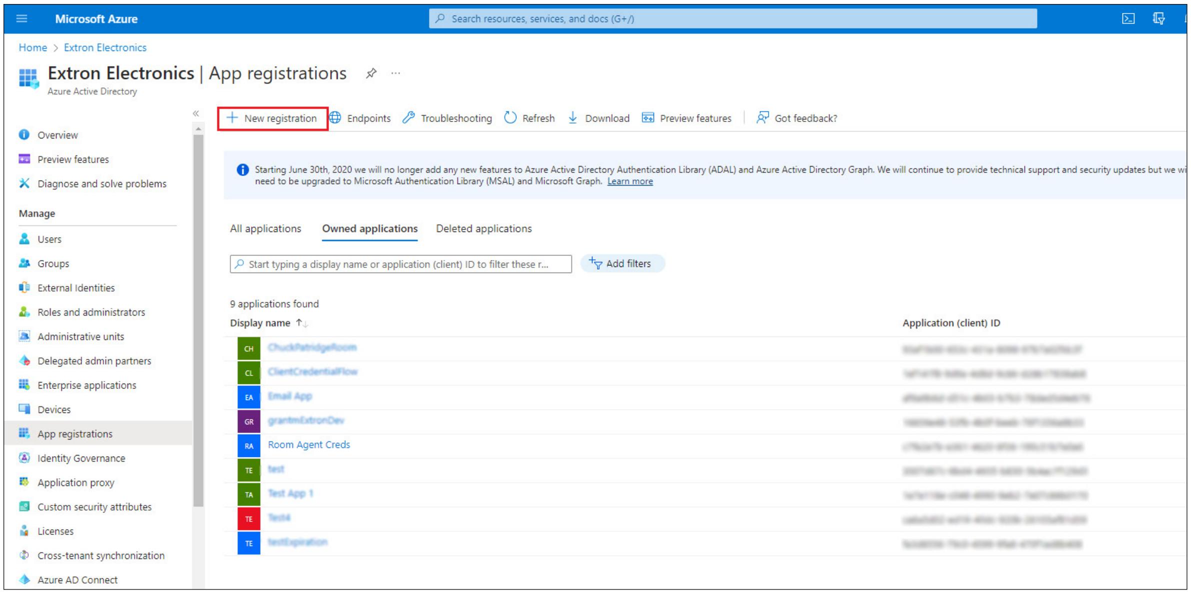


Figure 124. App registrations

4. Click **`+ New registration`**.

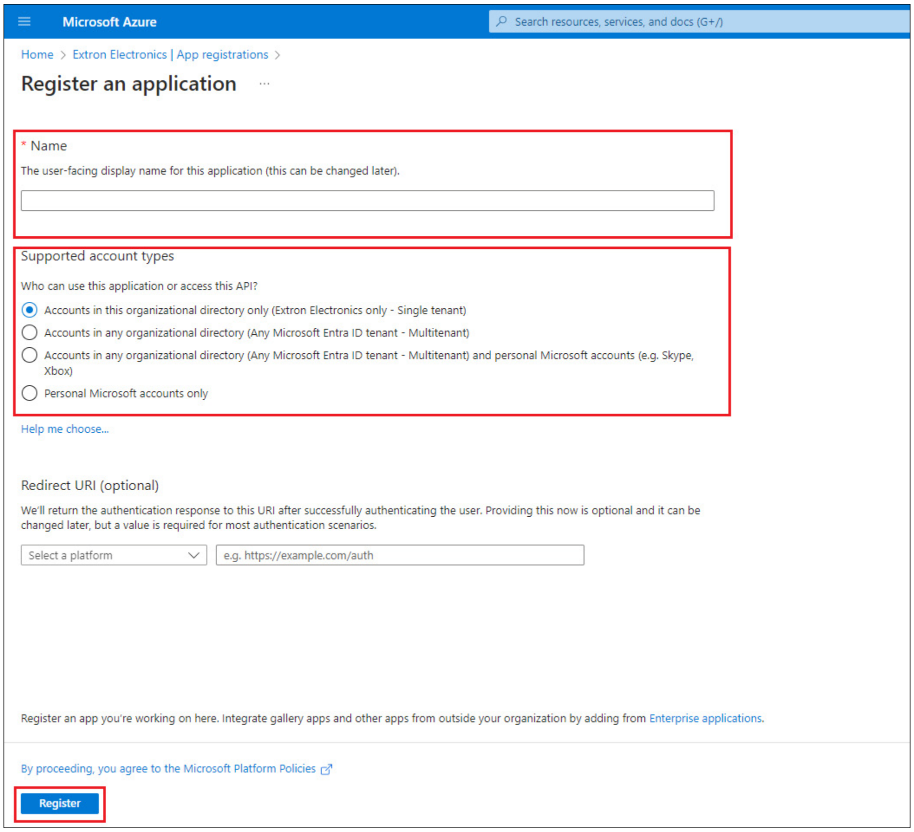


Figure 125. Register an Application

5. Provide a `Name` for the App. This can be edited later.
6. Check the radio button to select from the `Supported account type`. This determines who can use the app or access the API.
7. Click **`Register`**.

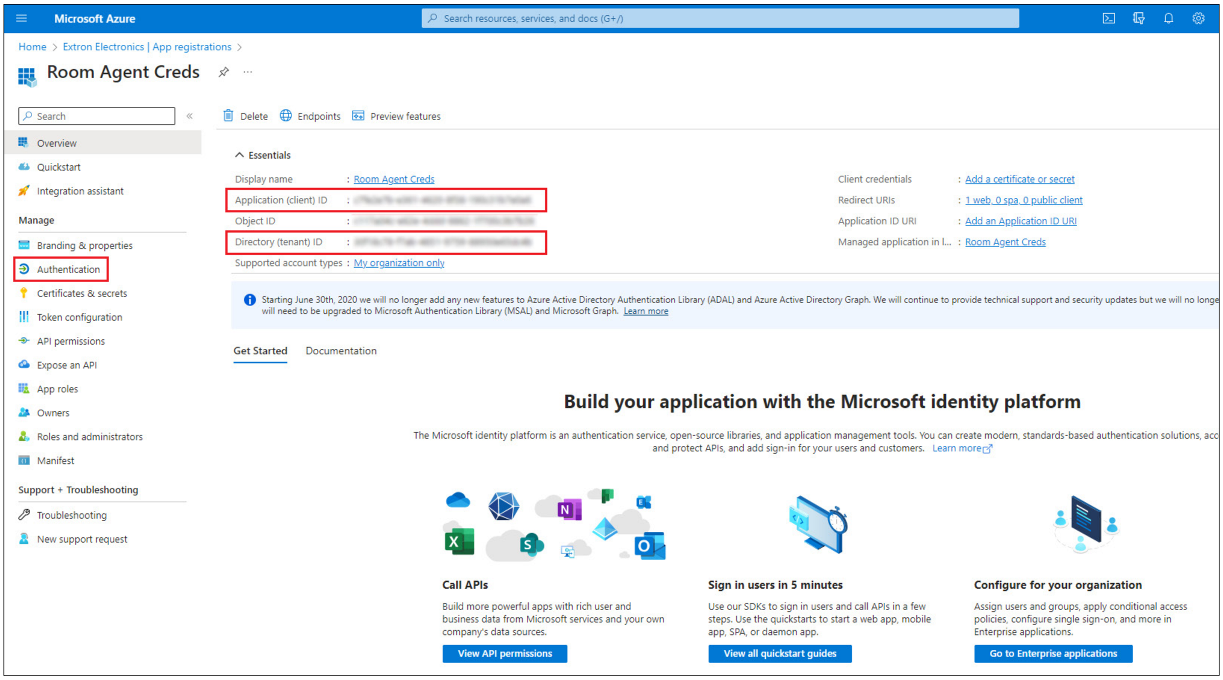


Figure 126. Room Agent Credentials

8. Make a note of the `Application (client) ID` and the `Directory (tenant) ID` (see figure 122). You will need these to access the calendar from Room Agent.
9. Click **`Authentication`**.

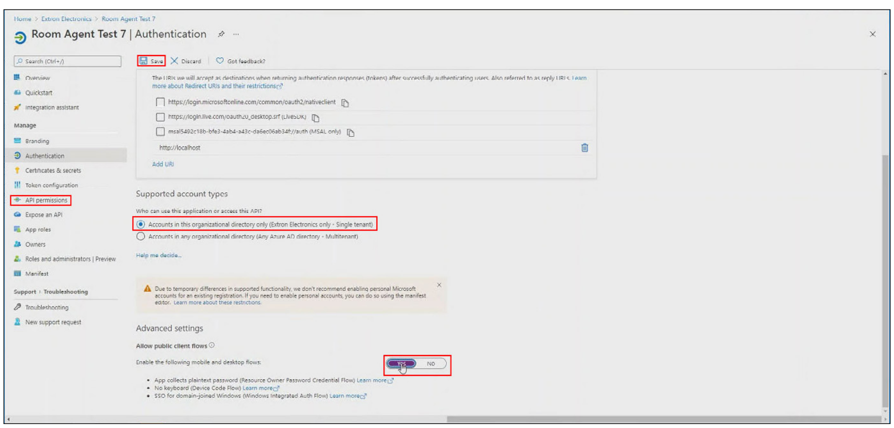


Figure 127. Room Agent Credentials — Authentication

10. Select **`Accounts in this organizational directory`**.
11. Select **`Yes`** for the `Allow public client flows` toggle in the `Advanced Settings` section.
12. Click **`Save`**.
13. Click **`API permissions`**.

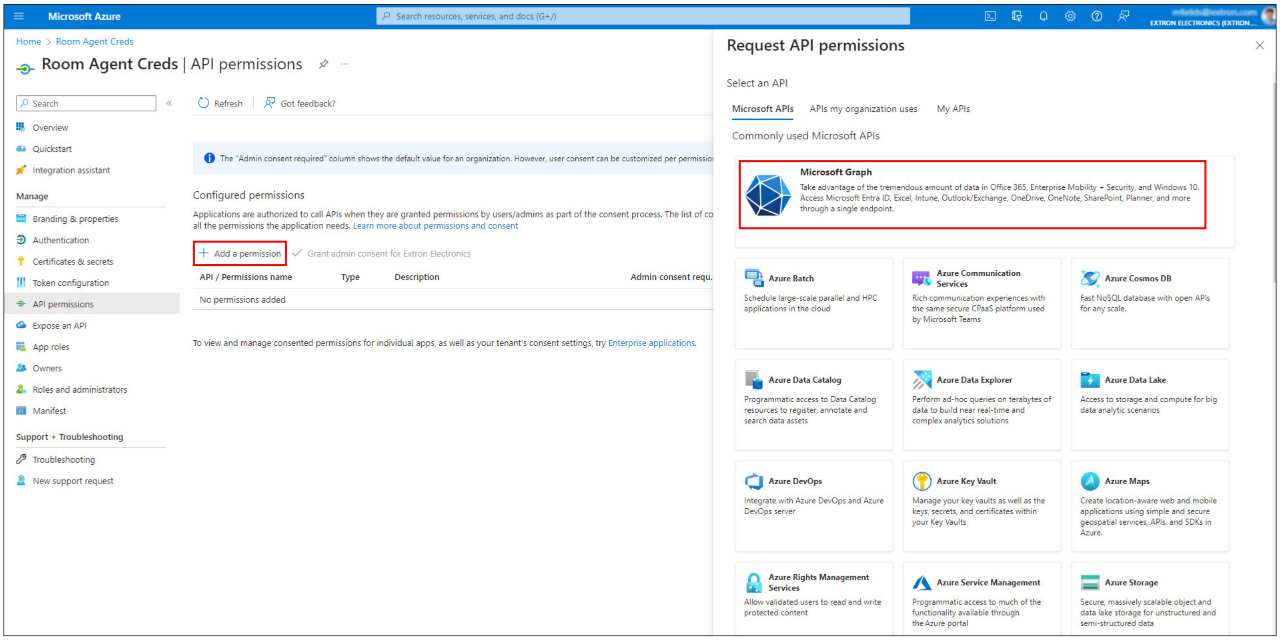


Figure 128. API Permissions

14. Click **+ Add a permission**. The `Request API permissions` pane opens.
15. Click **Microsoft Graph**.

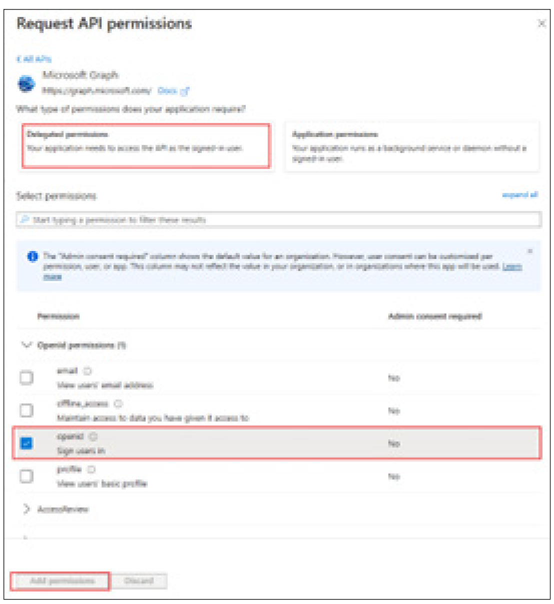


Figure 129. Request Delegated Permissions

16. Click **Delegated permissions**. A list of permission categories opens.
17. Select **openid**.
18. Click **Add permissions**.
19. If necessary, click **API permissions** (see **step 13** on page 83).
20. Click **Add a permission**. The `Request API permissions` page opens.
21. Click **Microsoft Graph**.

Figure 130. Request API Permissions

22. Click **`Application permissions`**. A list of permission categories opens.
23. Click **`Application`** to expand the list of `Application` options.
24. Select **`Application.Read.All`**.

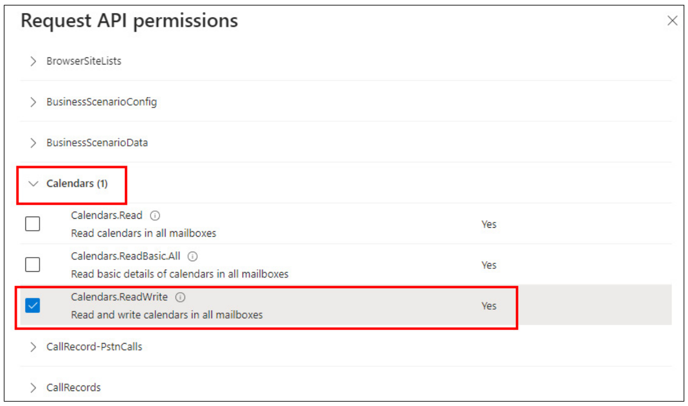


Figure 131. Add Calendar Permissions

25. Click **`Calendars`** to expand the list of `calendar` options.
26. Select **`Calendars.ReadWrite`**.

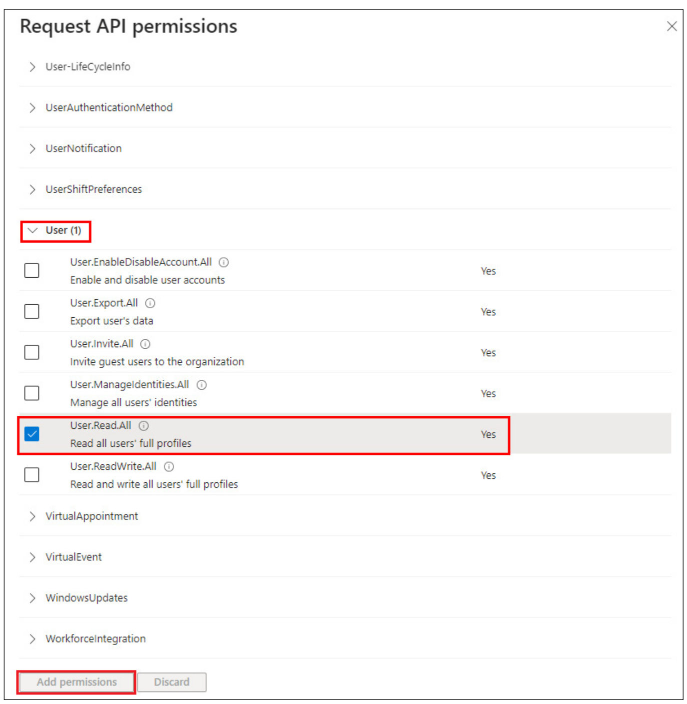


Figure 132. Add User Permissions

27. Click **`User`** to expand the list of `user` options.
28. Select **`User.Read.All`** and click **`Add Permissions`**.

29. After adding permissions if the status reads `Not granted for (organization name)`, you will need to contact your IT department to have your Azure admin grant these permissions to you.

30. Click **`Overview`**.

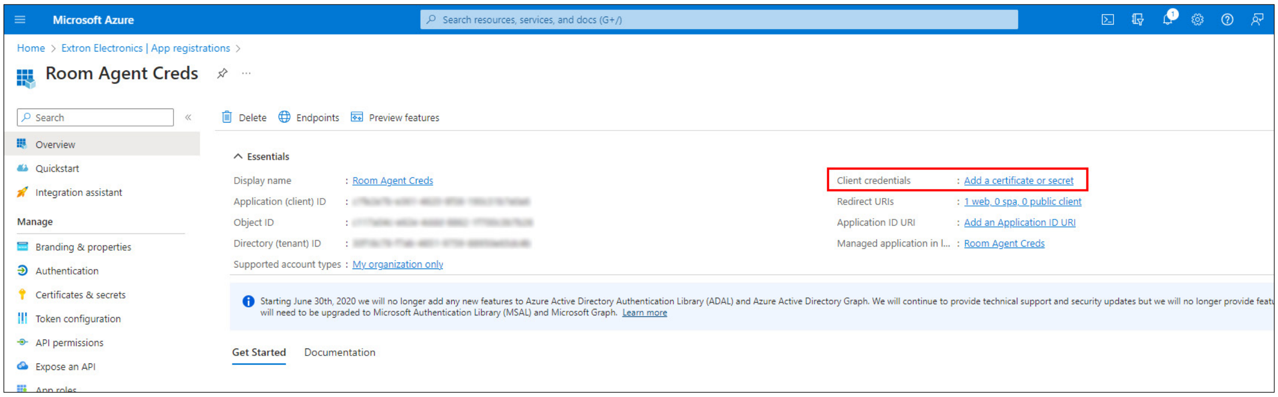


Figure 133. Room Agent Credentials Overview

31. Click on the link next to `Client Credentials`.

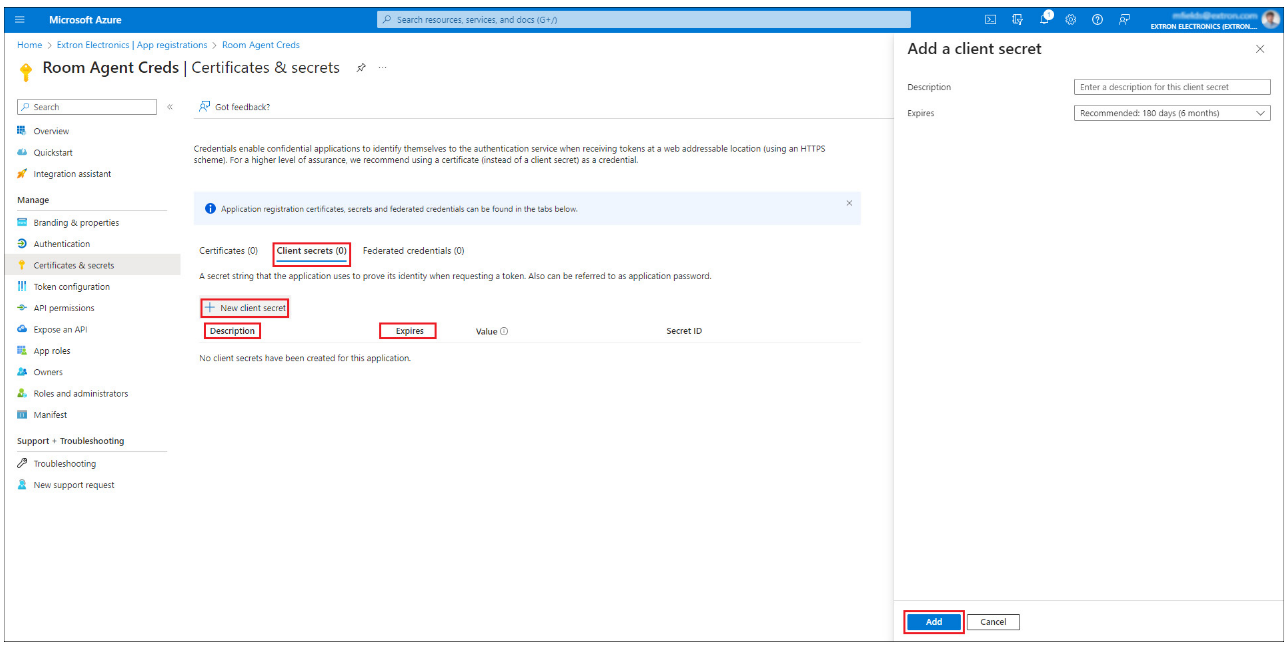


Figure 134. Room Agent Credentials — Certificates & secrets

32. Click on the **`Client Secrets`** tab and then **`+ New Client Secret`**.

33. Give the secret a `description` and `expiration` duration.

34. Click **`Add`**.

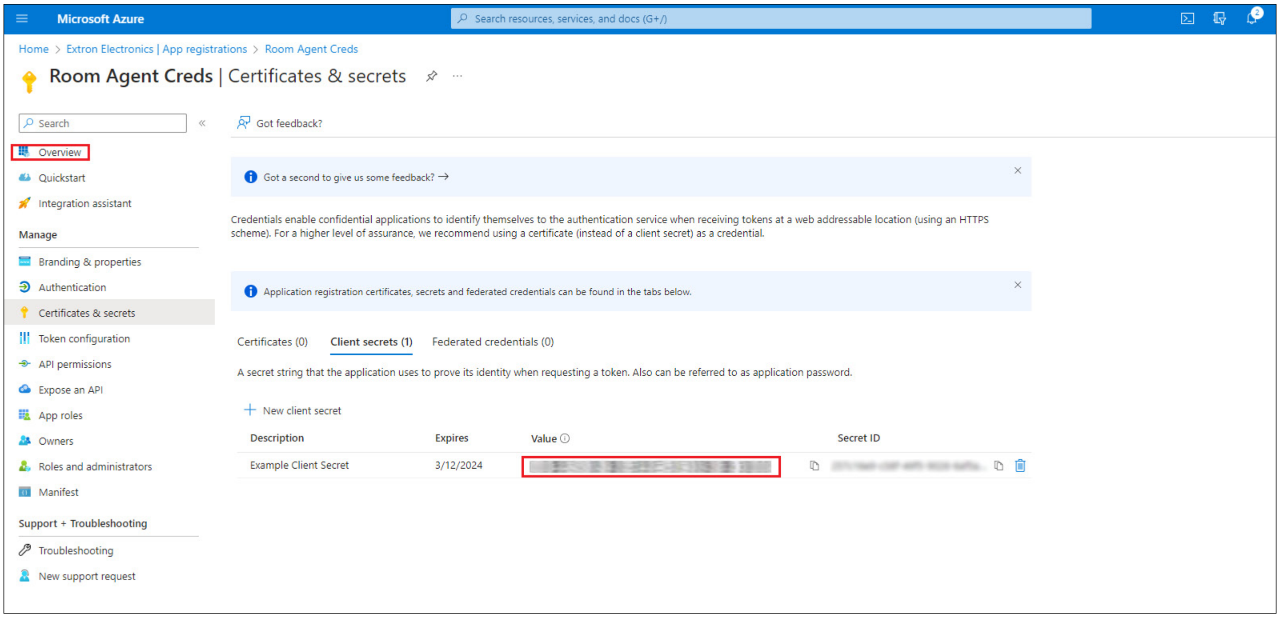


Figure 135. Room Agent Credentials

35. The value of the `Client Secret` is displayed. Copy the value for later use in Room Agent. Note that if you leave this page, you will not be able to see this value again and will need to create a new one.
36. Click **`Overview`**.

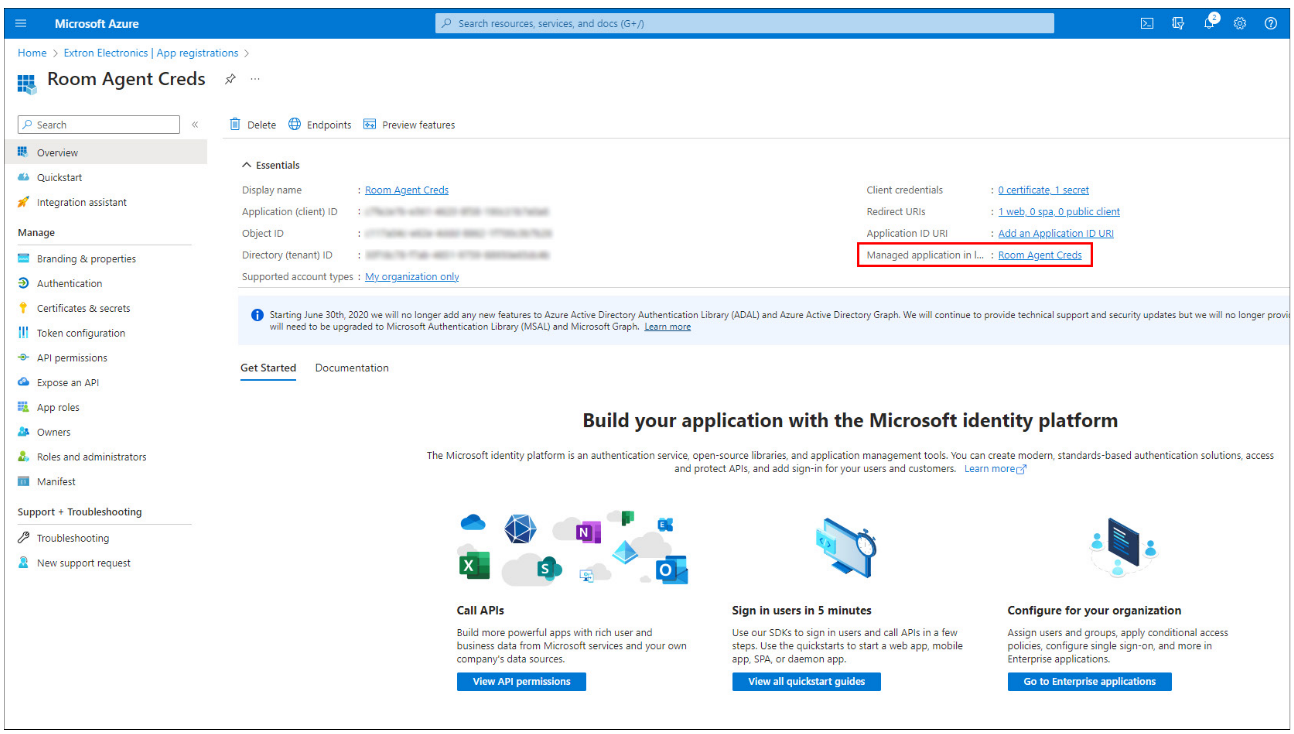


Figure 136. Room Agent Credentials

37. Click the link next to `Managed Application in Local Directory`.

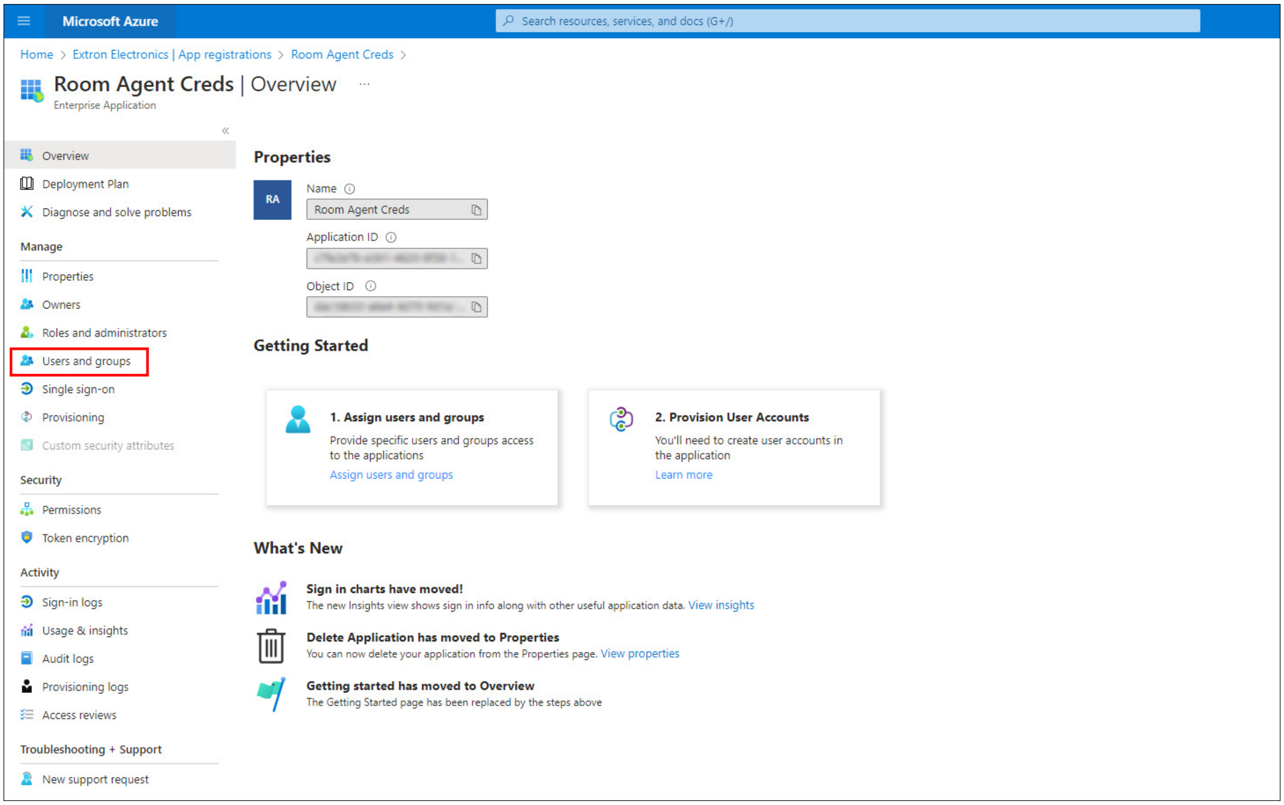


Figure 137. Room Agent Credentials Overview

38. Click on `Users and Groups`.

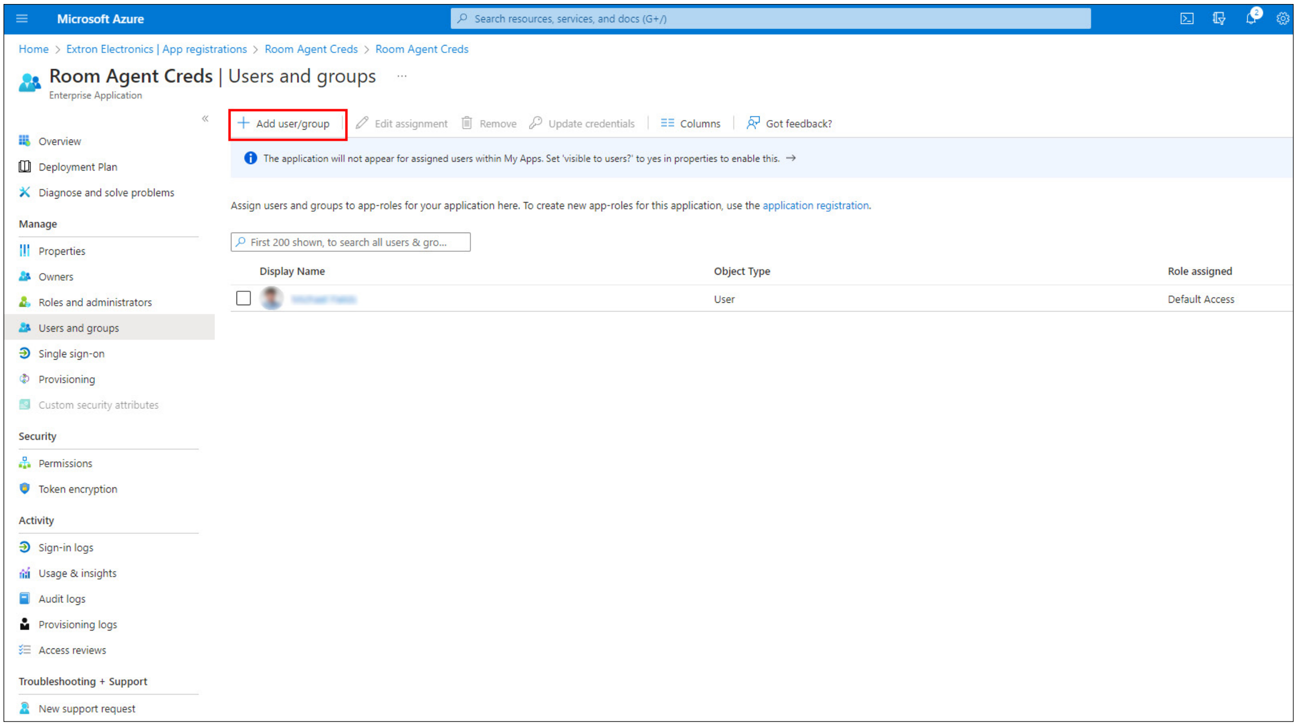


Figure 138. Users and groups

39. Click on **`Add User/Group`**.

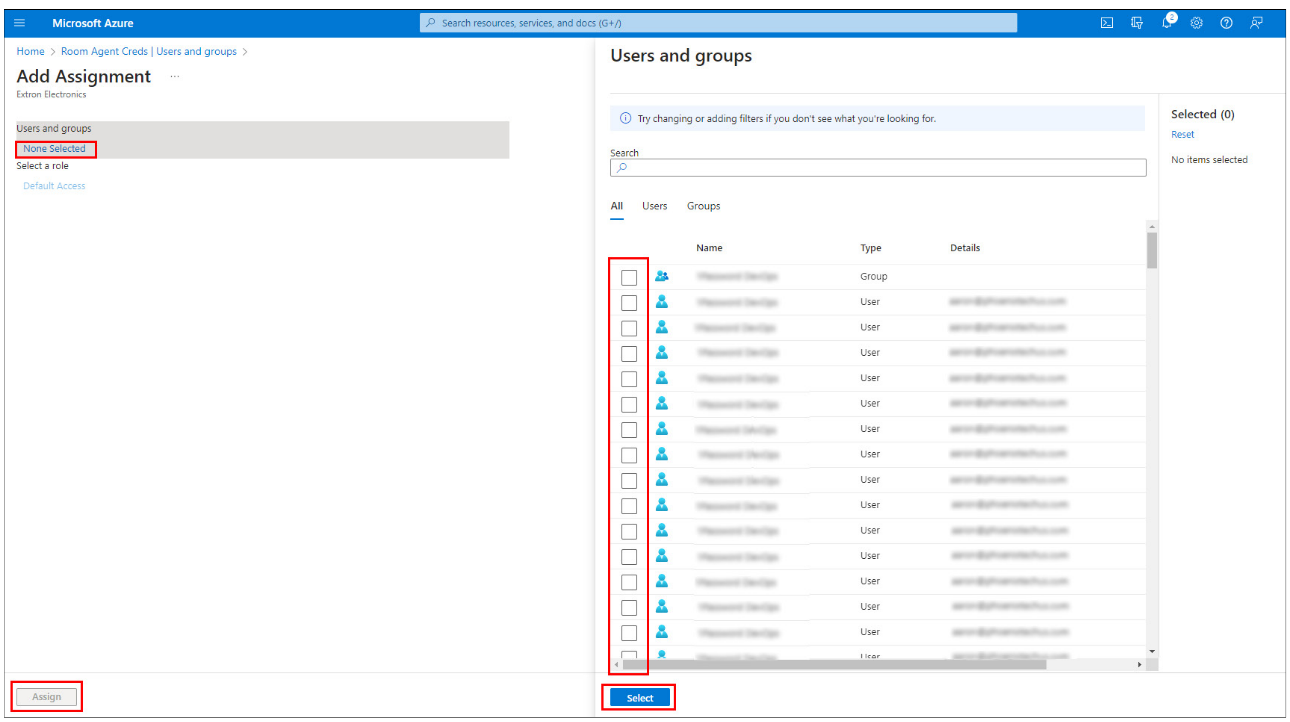


Figure 139. Select Users

40. Click **`None Selected`**.
41. Select all the users that you want to add and click on the **`Select`** button at the bottom of the page.
42. Click **`Assign`**.

Assigning Credentials to Touchpanels

1. Open Room Agent and select the **CONFIGURE** tab.

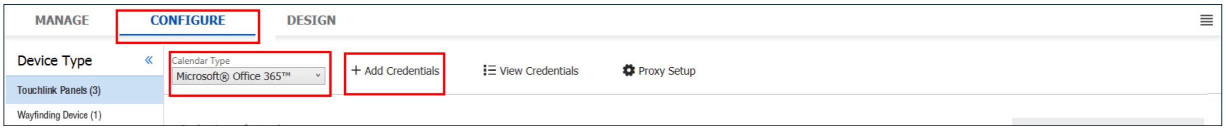


Figure 140. Microsoft Office 365 CONFIGURE Tab

2. From the drop-down list of calendars, select **Microsoft® Office 365™**.
3. Click **+ Add Credentials**.

   The Device Authentication to Office 365 dialog box opens.

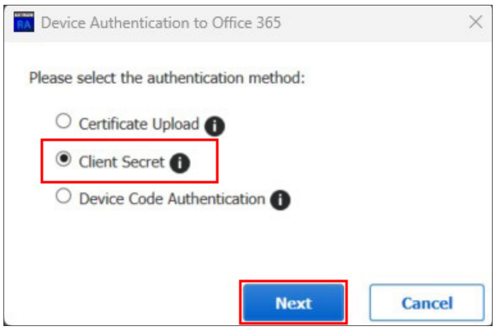


Figure 141. Device Authentication to Office 365 — 1

4. Select **Client Secret** and then **Next**.

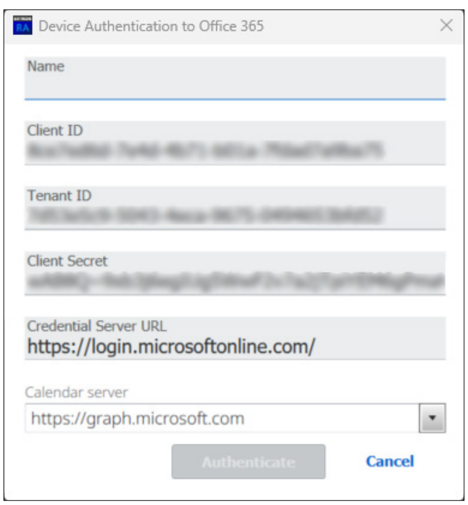


Figure 142. Device Authentication to Office 365 — 2

5. Provide a Name for the credentials.
6. Enter the Client ID and Tenant ID (see **step 8** of the previous section, on page 83), and Client Secret (see **step 35** of the previous section, on page 87).
7. If necessary, change the credential server URL. The default URL, which appears in the user interface is `https://login.microsoftonline.com/`. If you are using GCC, ensure that the correct URL is entered: for example `login.microsoftonline.gov`.
8. Enter the `calendar server` URL. For the Client Secret credential type, the default is `graph.microsoft.com`. If you are using GCC, ensure that the correct URL is entered: for example `graph.microsoft.gov`.
9. Click **Authenticate**.
10. If successful, a confirmation dialog displays. Click **OK**.

Use Certificate Upload Workflow

This section describes how to obtain Microsoft Office 365 OAuth credentials using the Certificate Upload workflow and how to assign those credentials to the Room Agent touchpanels.

- **Obtaining OAuth Credentials** on page 91
- **Assigning Credentials to Touchpanels** on page 101

Obtaining OAuth Credentials

> **NOTE:** Client Secret and Certificate Upload workflows are not supported for TLS 520, TLS 720, TLS 1020, and TLS 1022 devices.

To obtain OAuth credentials by uploaded certificate authorization, follow these steps.

1. Go to **https://portal.azure.com/**.

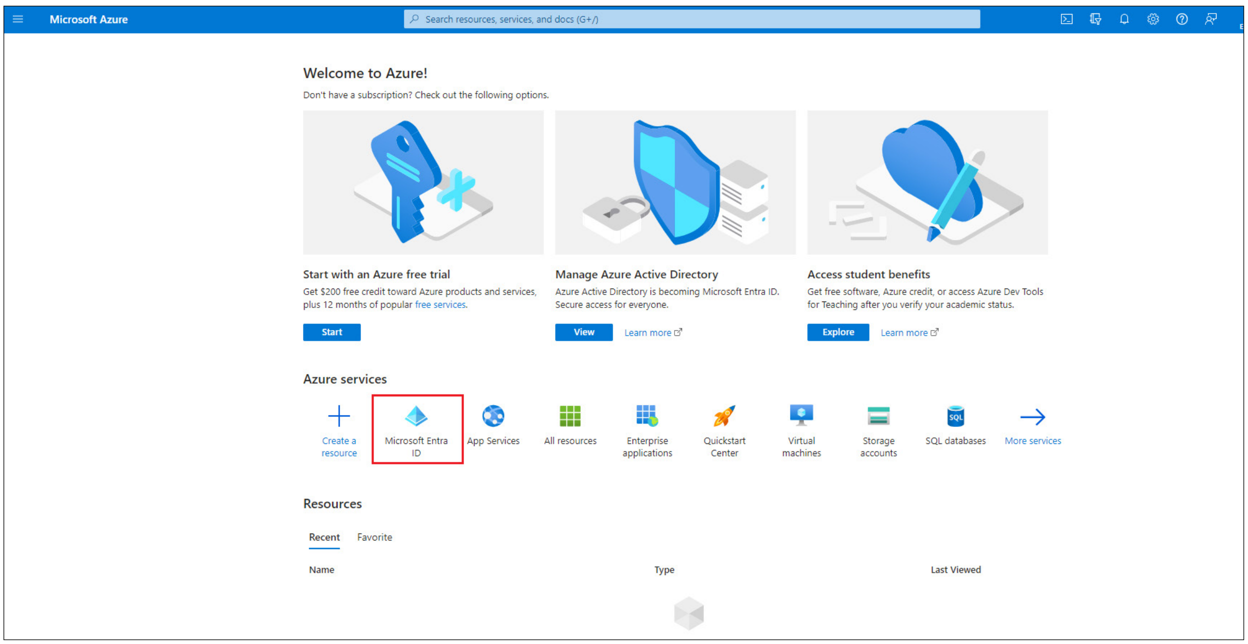


Figure 143. Microsoft Azure Website

2. Click `Microsoft Entra ID`.

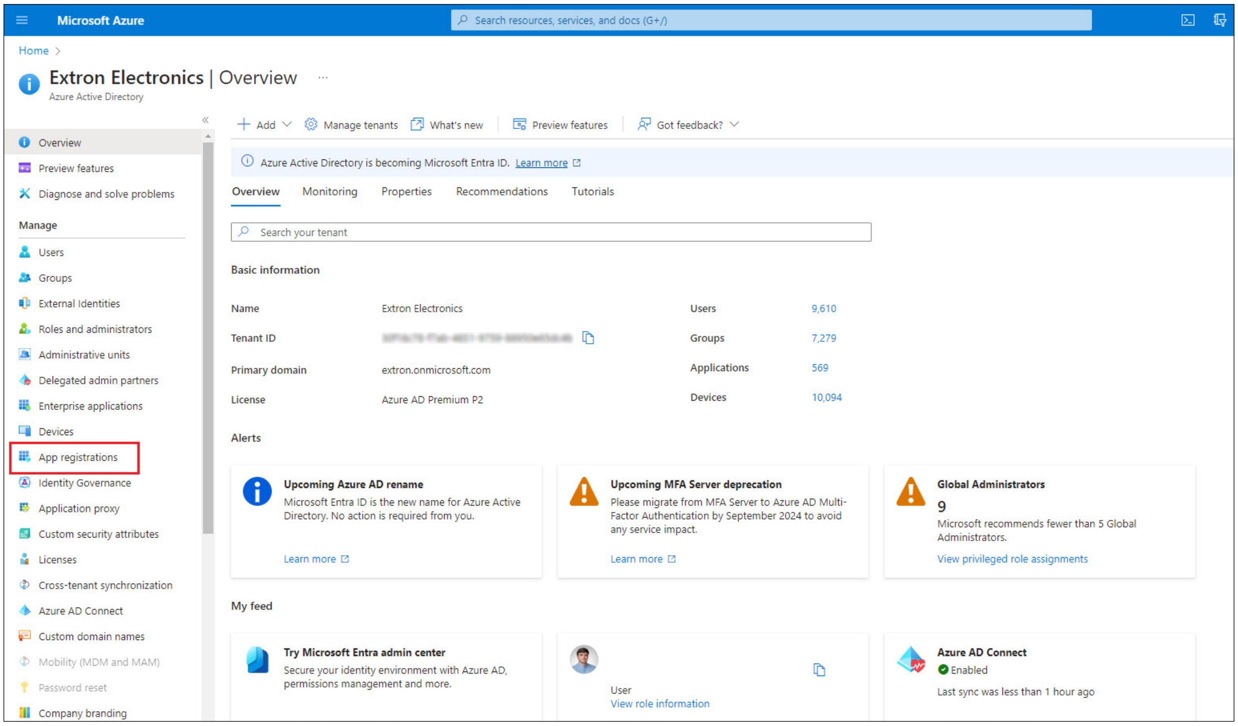


Figure 144. Company Page on Microsoft Website

3. Click `App registrations` in the menu bar to the left of the screen.

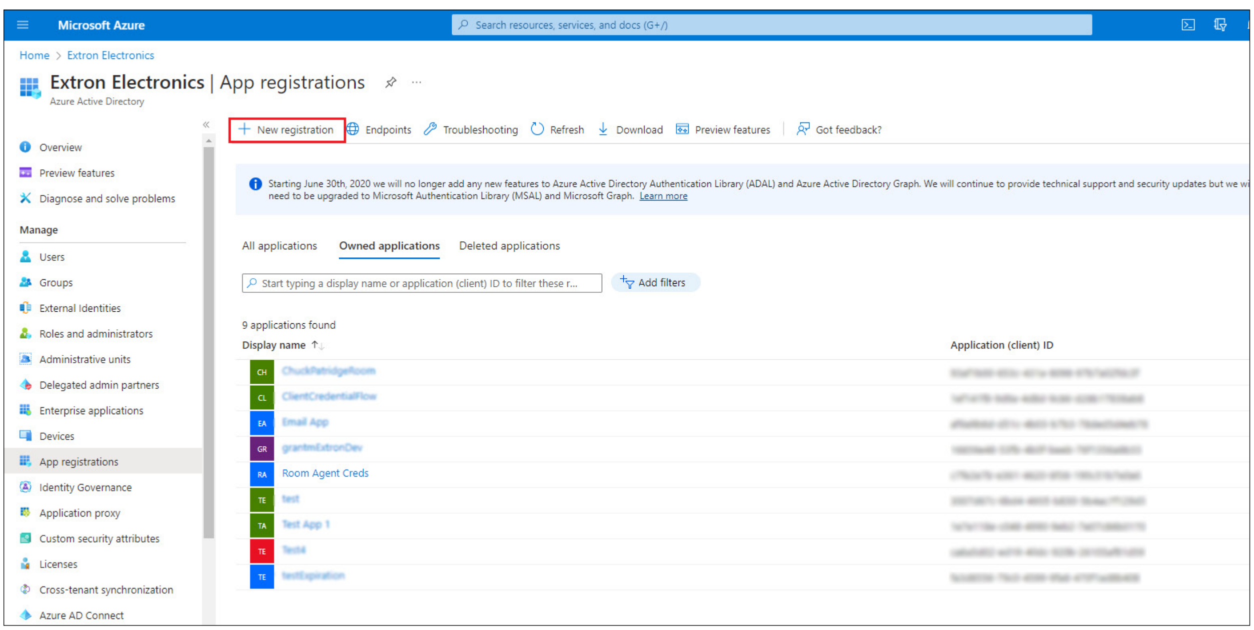


Figure 145. App registrations

4. Click **+ New registration**.

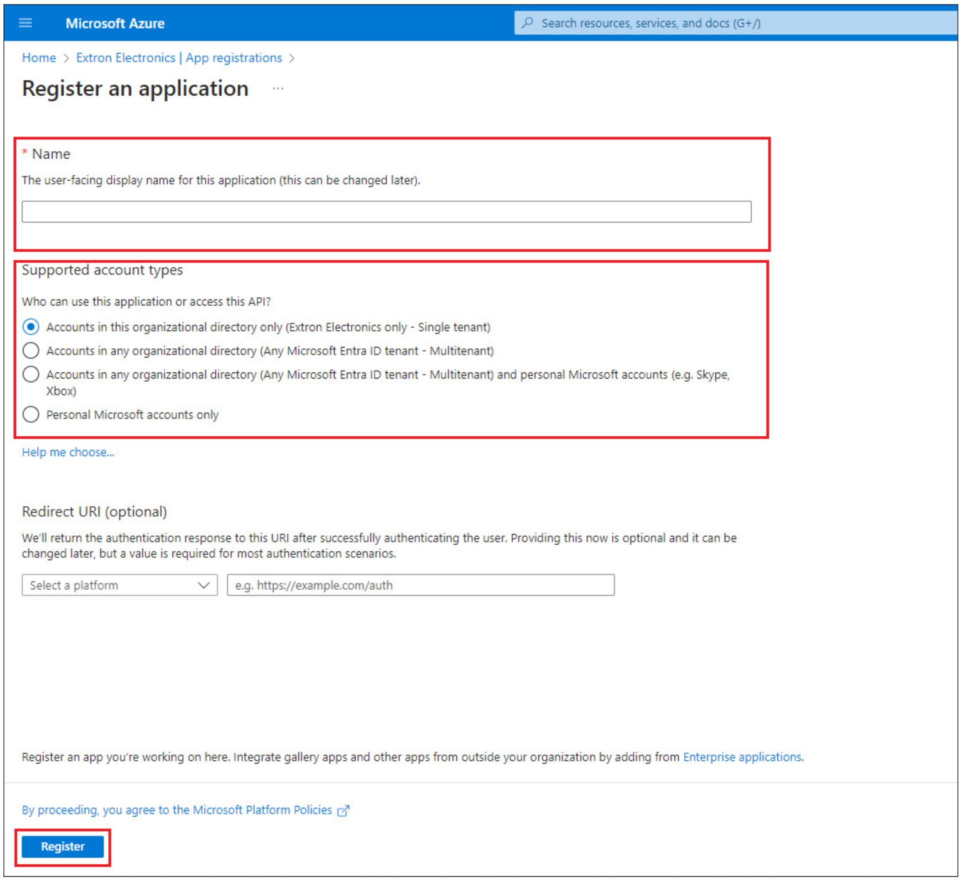


Figure 146. Register an Application

5. Provide a `Name` for the App. This can be edited later.
6. Check the radio button to select from the `Supported account type`. This determines who can use the app or access the API.
7. Click **`Register`**.

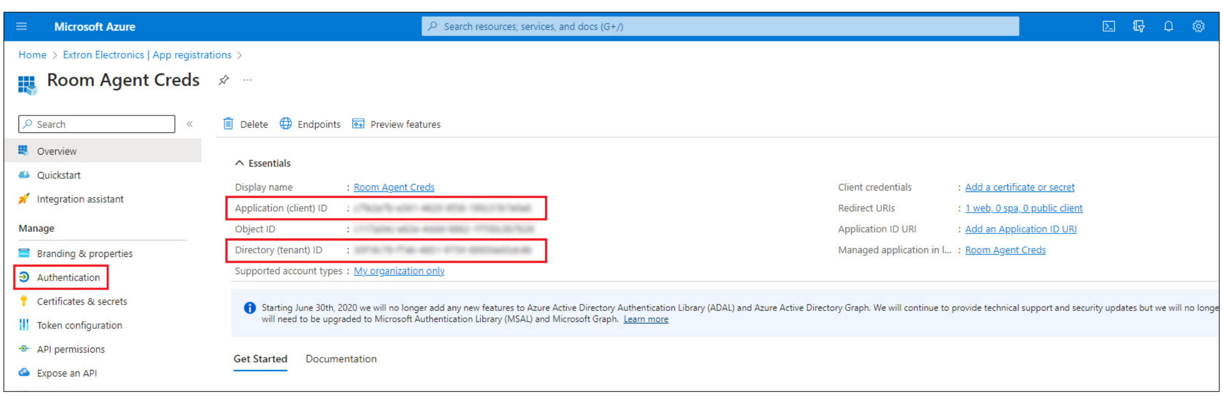


Figure 147. Room Agent Credentials

8. Make a note of the `Application (client) ID` and the `Directory (tenant) ID`. You will need these to access the calendar from Room Agent.
9. Click **`Authentication`** in the menu bar to the left of the screen.

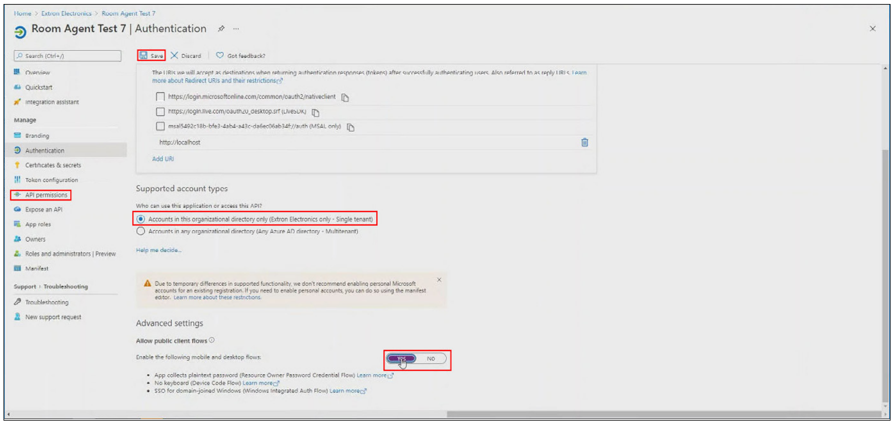


Figure 148. Room Agent Credentials — Authentication

10. Select **`Accounts in this organizational directory`**.
11. Select **`Yes`** for the `Allow public client flows` toggle in the `Advanced Settings` section.
12. Click **`Save`**.
13. Click **`API permissions`**.

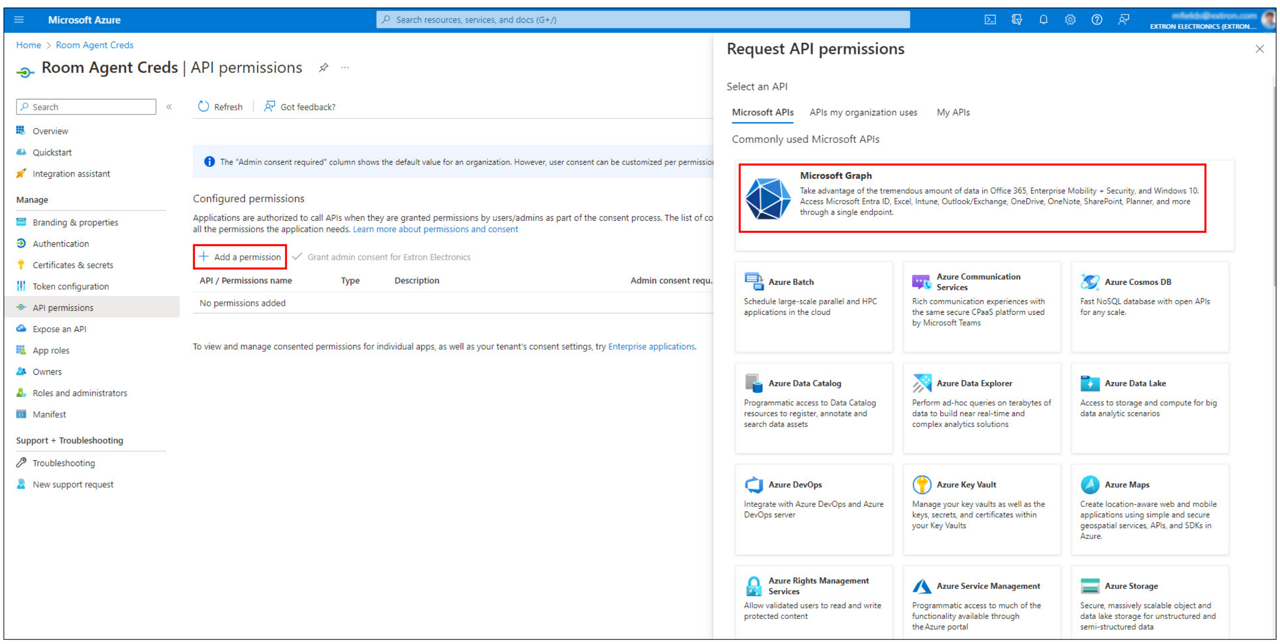
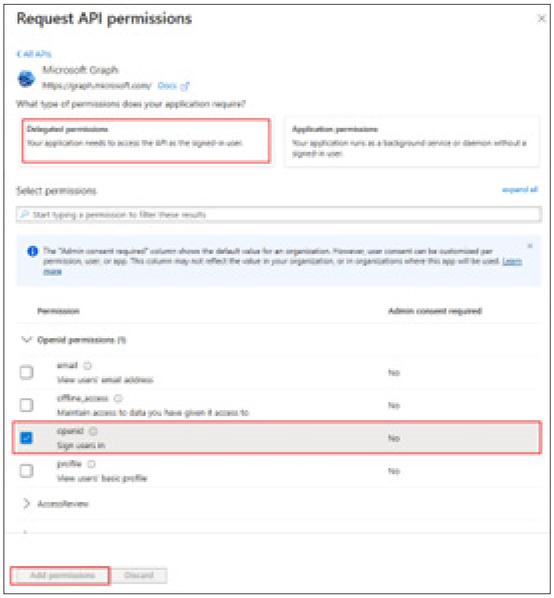


Figure 149. API Permissions

14. Click **`+ Add a permission`**. The `Request API permissions` pane opens.
15. Click **`Microsoft Graph`**.



16. Click **`Delegated permissions`**. A list of permission categories opens.
17. Select **`openid`**.
18. Click **`Add permissions`**.
19. If necessary, **`API permissions`** (see step 13).
20. Click **`Add a permission`**. The `Request API permissions` page opens.
21. Click **`Microsoft Graph`**.

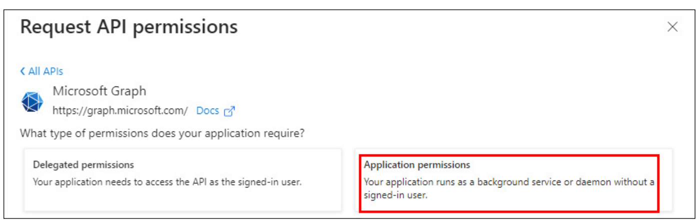


Figure 150. Request API Permissions

22. Click **`Application permissions`**. A list of permission categories opens.
23. Click **`Applicaton`** to expand the list of application options.
24. Select **`Application.Read.All`**.

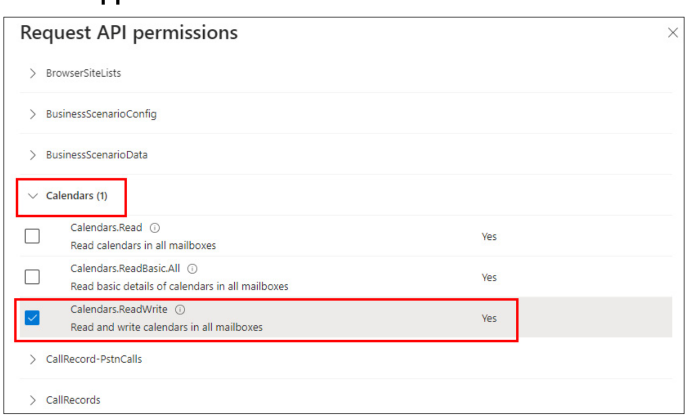


Figure 151. Add Calendar Permissions

25. Click **`Calendars`** to expand the list of calendar options.
26. Select **`Calendars.ReadWrite`**.

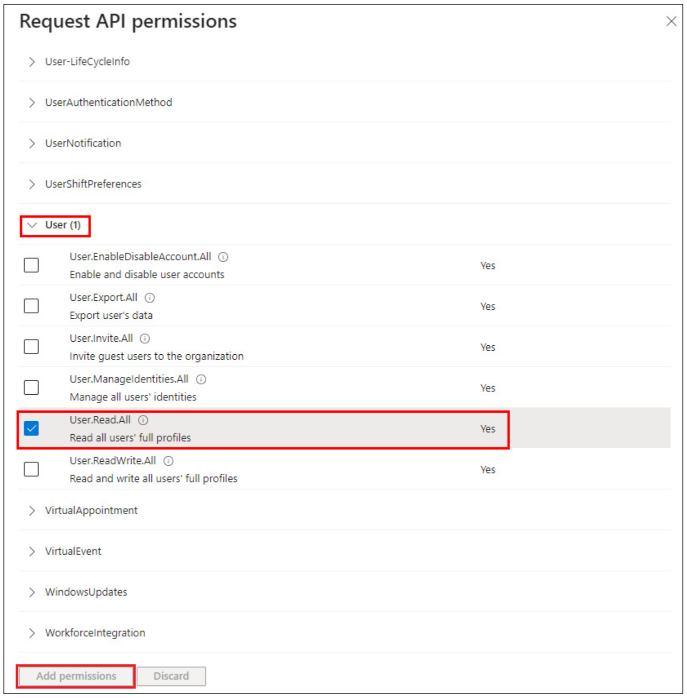


Figure 152. Add User Permissions

27. Click **`User`** to expand the list of user options.
28. Select **`User.Read.All`** and click **`Add Permissions`**.

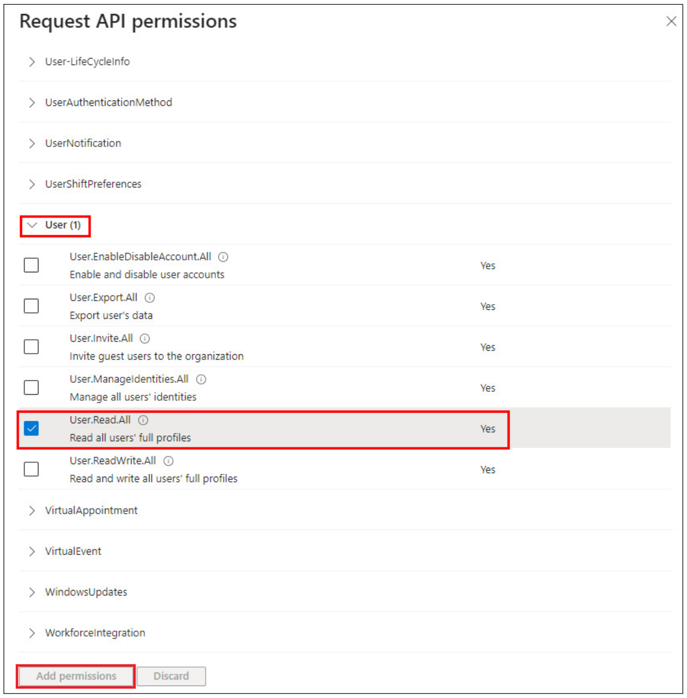


Figure 153. Add User Permissions

29. After adding permissions if the status reads `Not granted for` *`(organization name)`*, you will need to contact your IT department to have your Azure admin grant these permissions to you.

30. Click **`Overview`**.

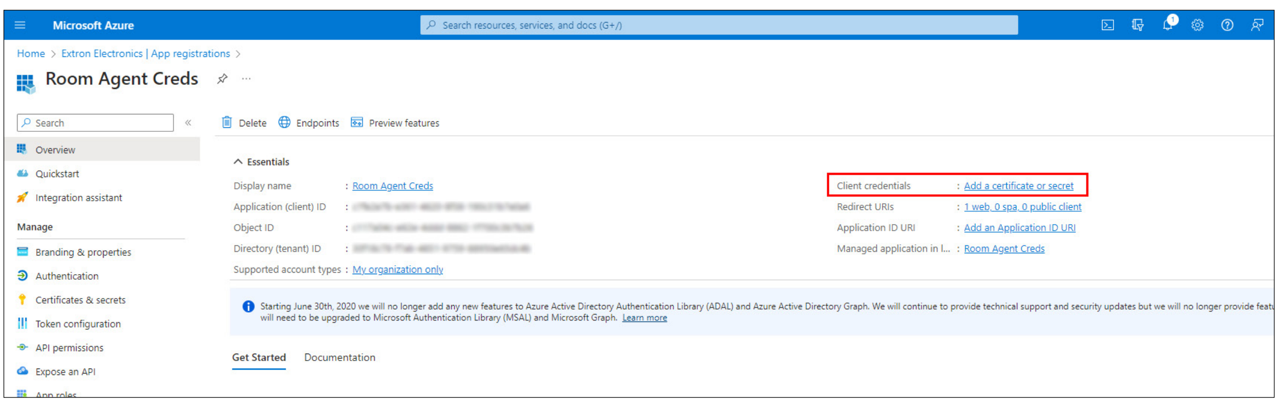


Figure 154. Room Agent Credentials Overview

31. Click the link next to `Client Credentials`.

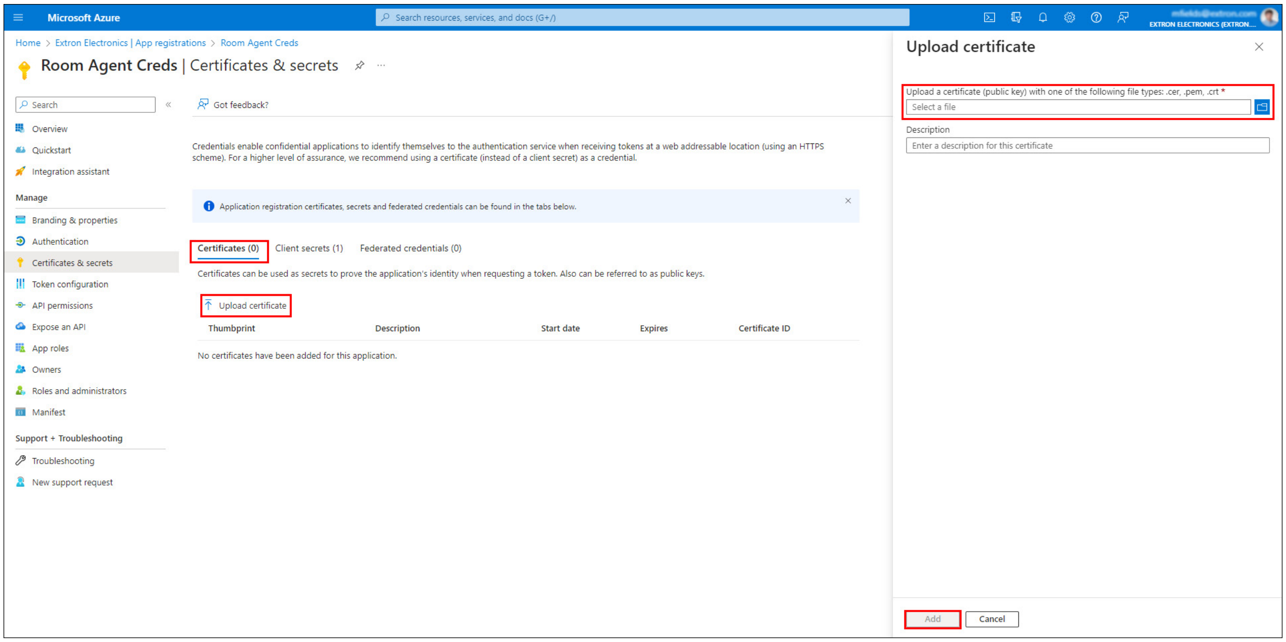


Figure 155. Upload Certificate

32. Click on the **`Certificates`** tab and then click **`Upload Certificate`**.
33. Upload a valid certificate of one of the following file types: `.pem`, `.cer`, `.crt`.
34. Give the certificate a meaningful description then click **`Add`**.

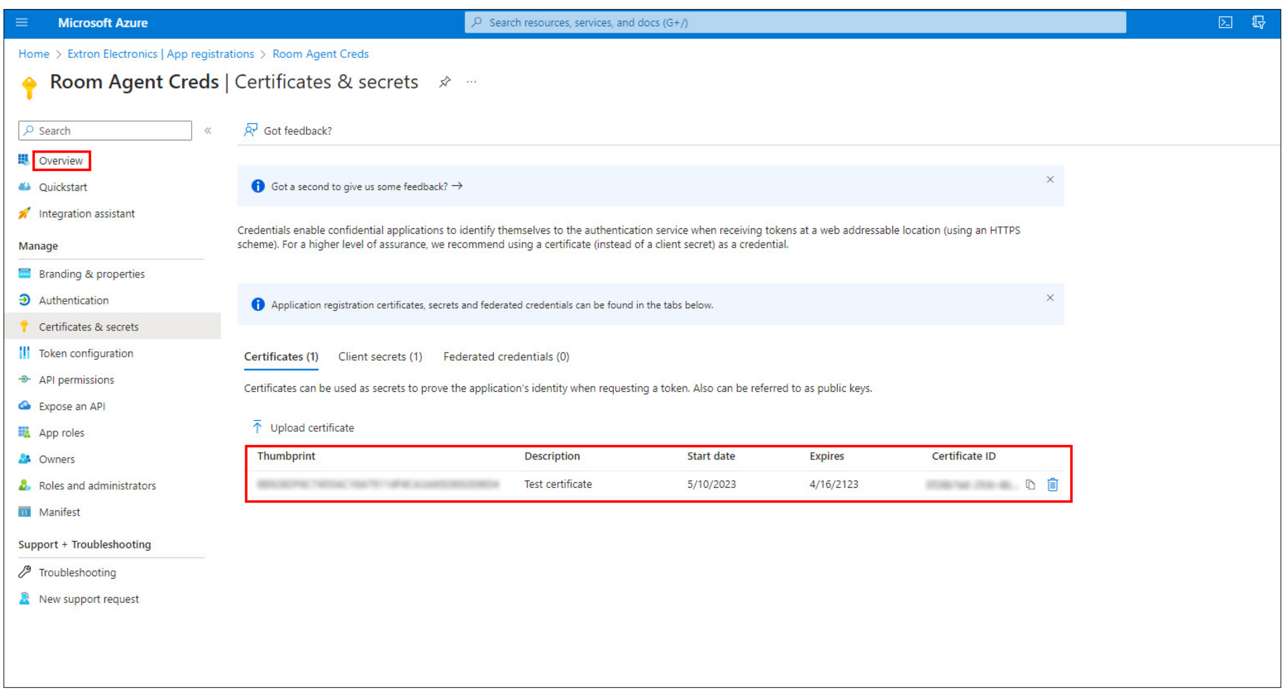


Figure 156. Room Agent Credentials — Certificates & secrets

35. You will see a new entry giving you the `Thumbprint`, `Description`, `start` and `expiration` dates, and the `Certificate ID`. Copy the thumbprint for use with Room Agent. The thumbprint is retrievable even if you leave the page and come back later.
36. Click **`Overview`**.

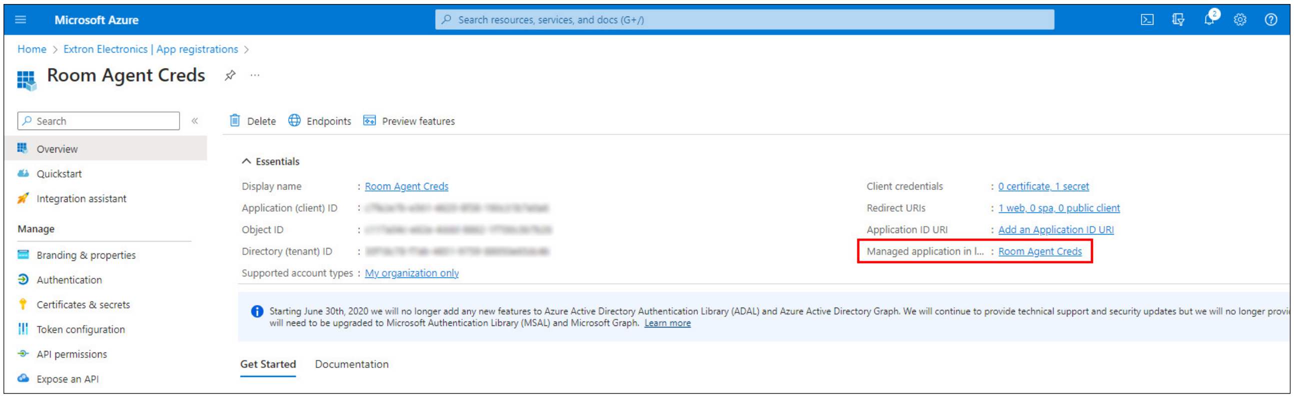


Figure 157. Room Agent Credentials

37. Click the link next to `Managed Application in Local Directory`.

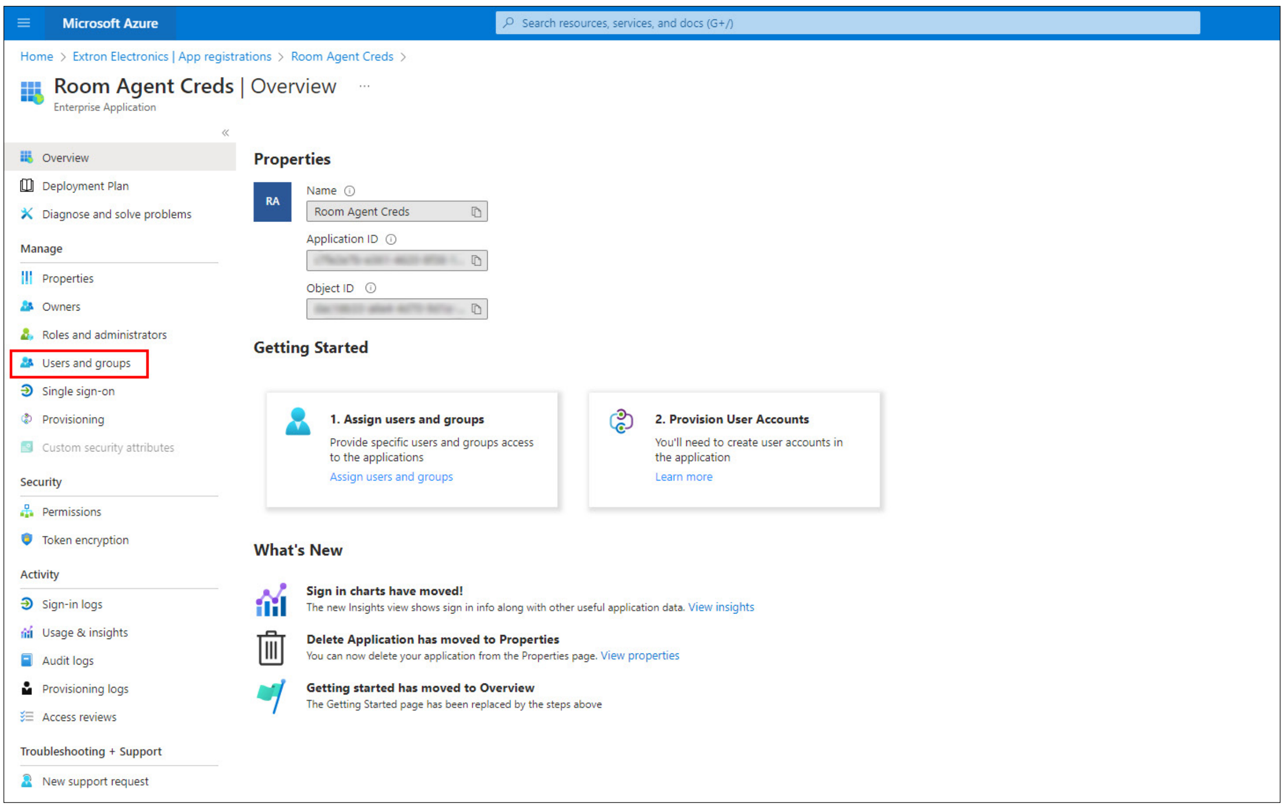


Figure 158. Room Agent Credentials Overview

38. Click on **`Users and Groups`**.

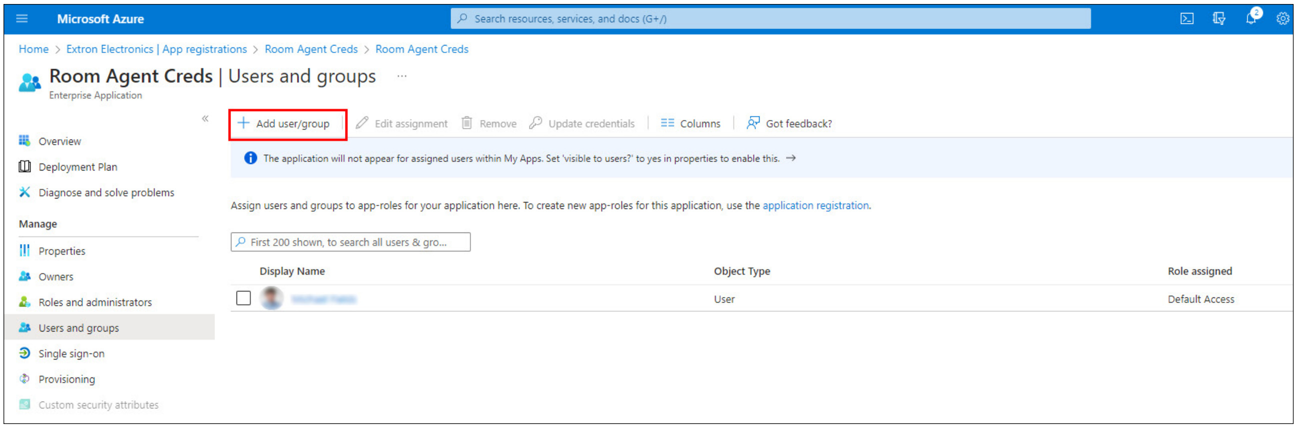


Figure 159. Users and groups

39. Click on **`Add user/group`**.

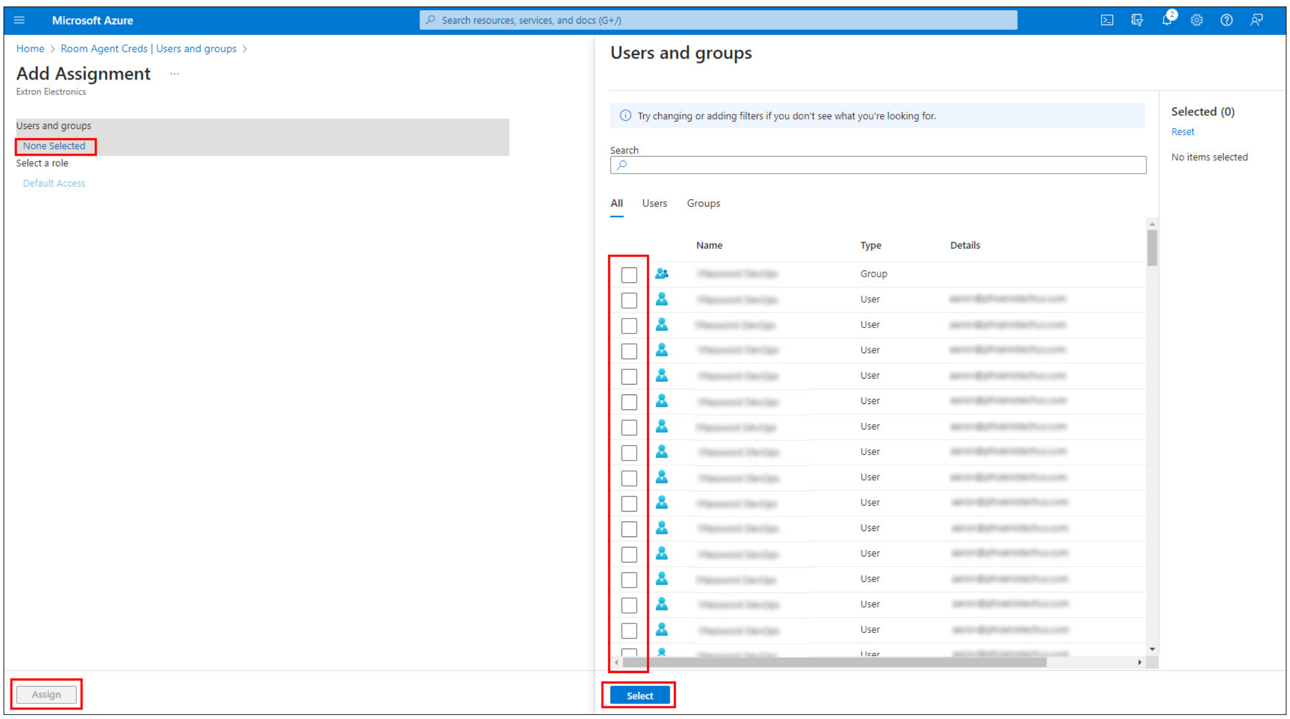


Figure 160. Select Users

40. Click **`None Selected`**.
41. Select all the users that you want to add and click on the **`Select`** button at the bottom of the page.
42. Click **`Assign`**.

Assigning Credentials to Touchpanels

1. Open Room Agent and select the **CONFIGURE** tab.

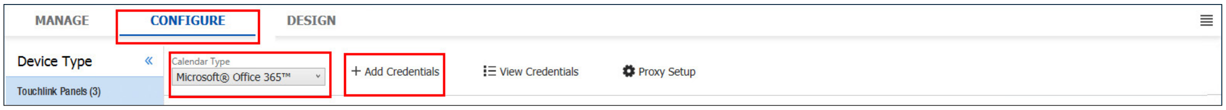


Figure 161. Microsoft Office 365 CONFIGURE Tab

2. From the drop-down list of calendars, select **Microsoft® Office 365™**.
3. Click **+ Add Credentials**. The Device Authentication to Office 365 dialog box opens.

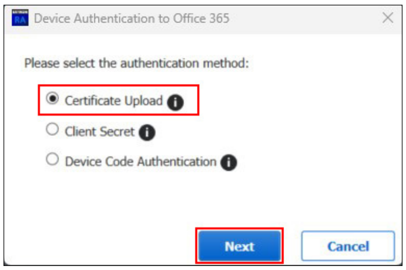


Figure 162. Select Certificate Upload

4. Select **Certificate Upload** and then click **Next**.

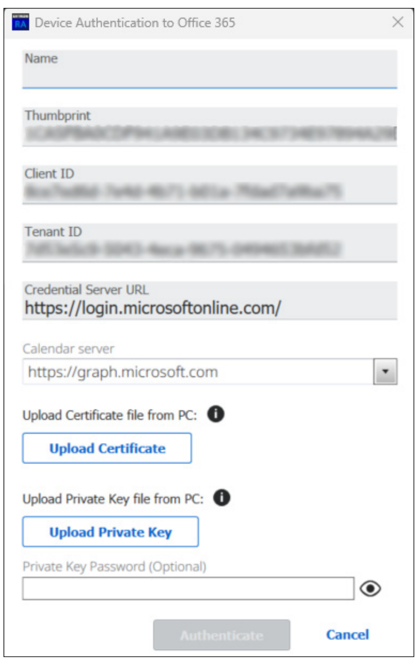


Figure 163. Upload Certificate

5. Provide a Name for the credentials.
6. Enter the Certificate Thumbprint (see **step 35**, in the previous section, on page 98) Client ID, and Tenant ID (see **step 8**, in the previous section, on page 93).
7. If necessary, change the credential server URL. The default URL, which appears in the user interface is `https://login.microsoftonline.com/`. If you are using GCC, ensure that the correct URL is entered: for example `login.microsoftonline.gov`.
8. Enter the calendar server URL. For the Certificate Upload credential type, the default is `graph.microsoft.com`. If you are using GCC, ensure that the correct URL is entered: for example `graph.microsoft.gov`.

9. Upload a valid `Certificate file` and `Private Key file`.
10. (Optional) Enter the password for the private key if it is password protected.
11. Click **`Authenticate`**. If successful, a confirmation dialog will display. Click **`OK`**.

Use Device Code Workflow

This section describes how to obtain Microsoft Office 365 OAuth credentials using the Device Code workflow and how to assign those credentials to the Room Agent and to touchpanels.

- Obtaining OAuth Credentials
- **Assigning Oauth Credentials to Room Agent** on page 107
- **Assigning Oauth Credentials to Touchpanels** on page 110

Obtaining OAuth Credentials

NOTE: Microsoft has ended single-factor authorization and now uses two-factor authorization (OAuth).

To obtain OAuth credentials by two-factor authorization, follow the steps below.

1. Go to **https://portal.azure.com/**.

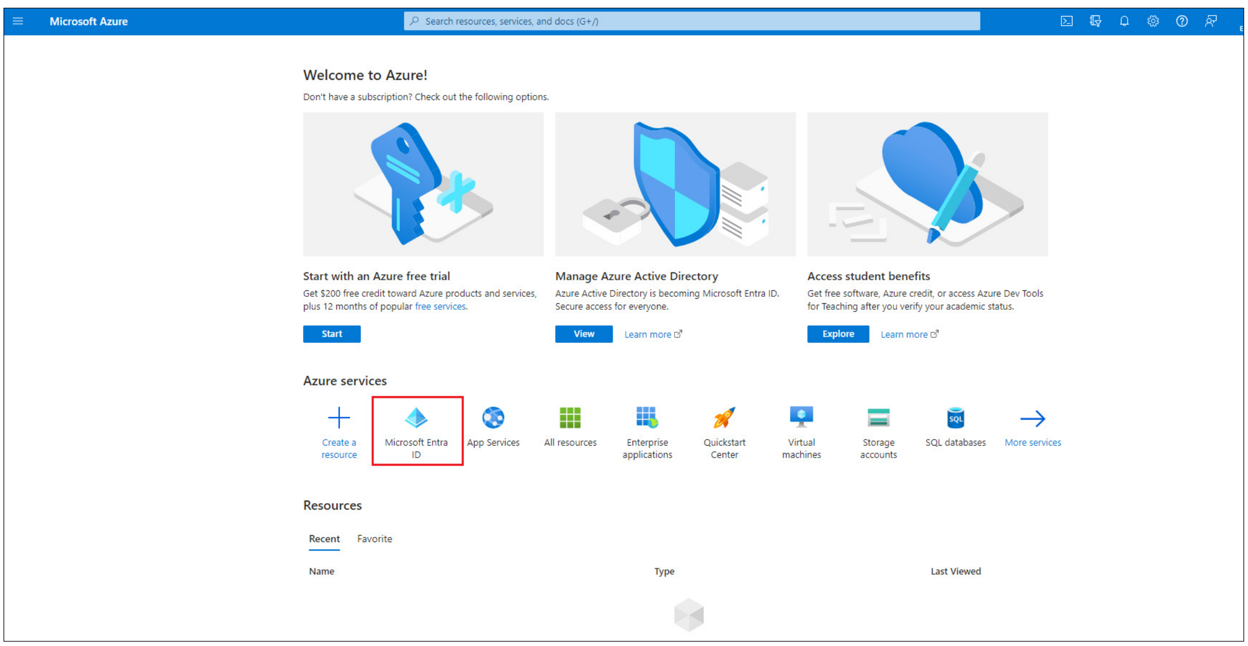


Figure 164. Microsoft Azure Website

2. Click **`Microsoft Entra ID`**.

The `Overview` page for your organization opens:

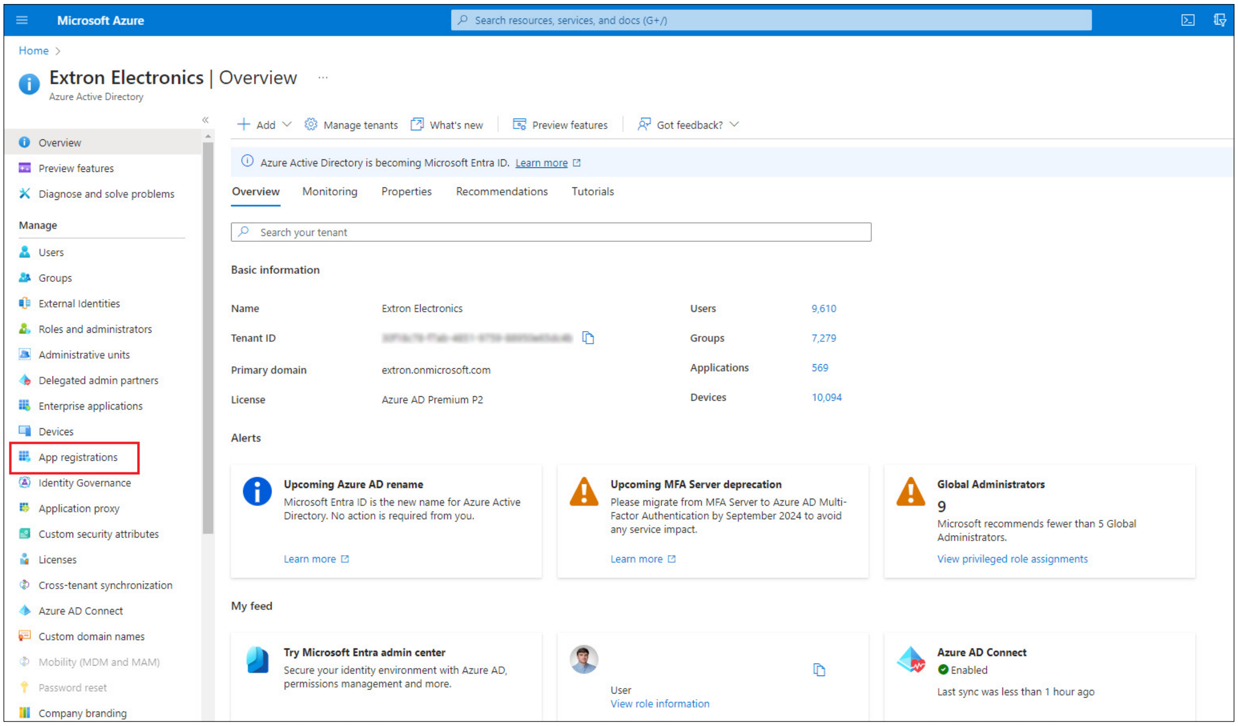


Figure 165. Company Page on Microsoft Website

3. Click **`App registrations`** in the menu bar to the left of the screen.

   The `App registrations` page opens:

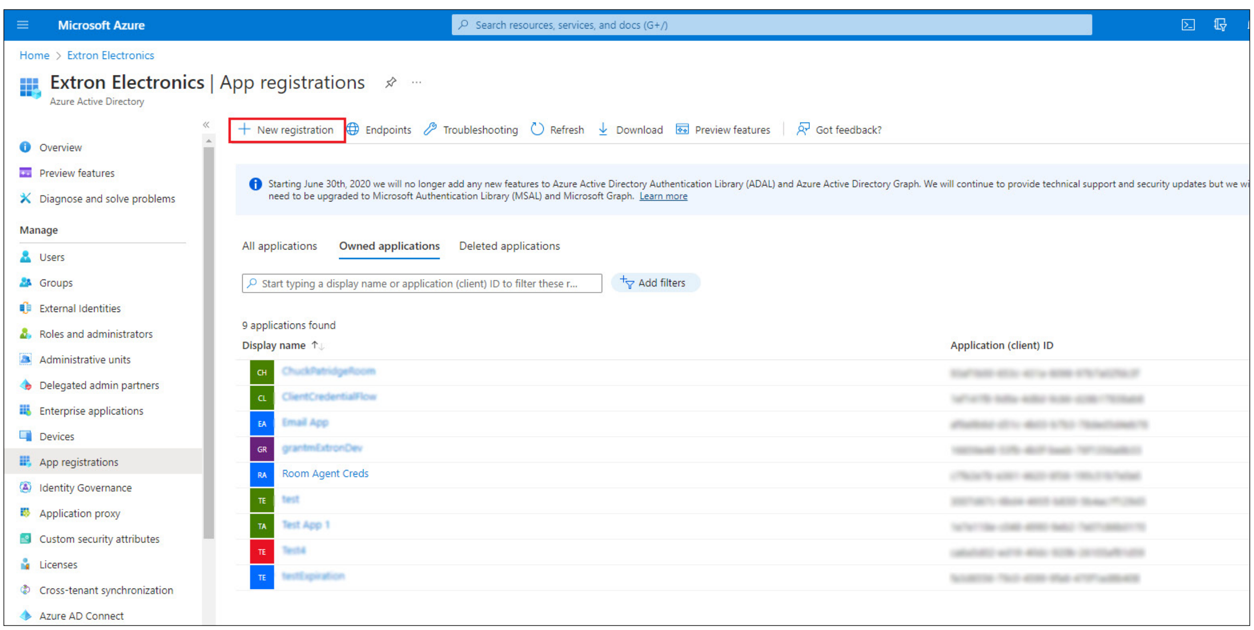


Figure 166. App registrations

4. Click **`+ New registration`** in the menu bar at the top of the screen.

   The `Register an application` page opens:

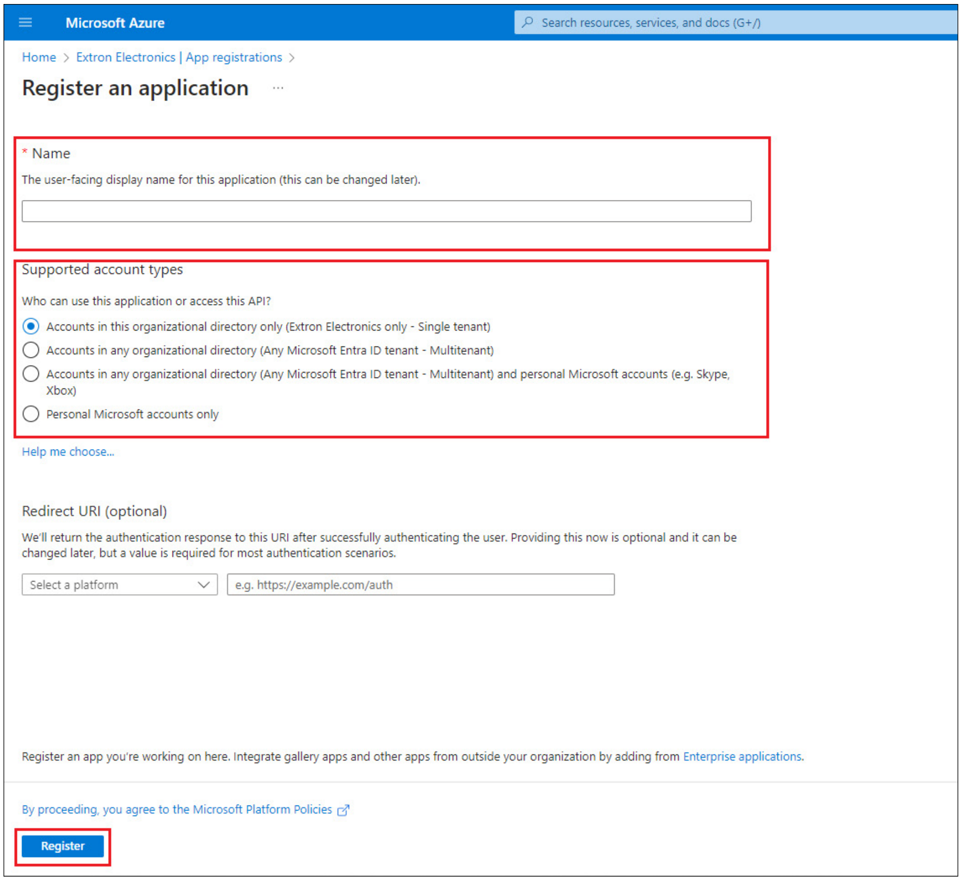


Figure 167. Register an Application

5. Provide a `Name` for the App. This can be edited later.
6. Check the radio button to select from the **`Supported account types`**. This determines who can use the app or access the API.
7. You must enter a reply address such as `http://localhost`. This is required for Room Agent to work.
8. Click **`Register`**.

   The page for your new app opens:

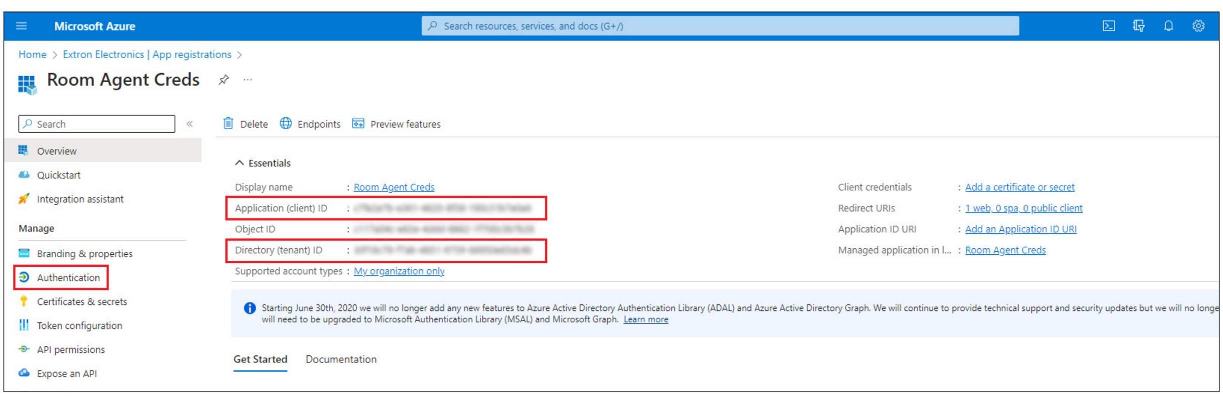


Figure 168. Room Agent Credentials

9. Make a note of the `Application (client) ID` and the `Directory (tenant) ID`. You will need these to access the calendar from Room Agent.

10. Click **`Authentications`**.

    The `Authentication` page for your app opens:

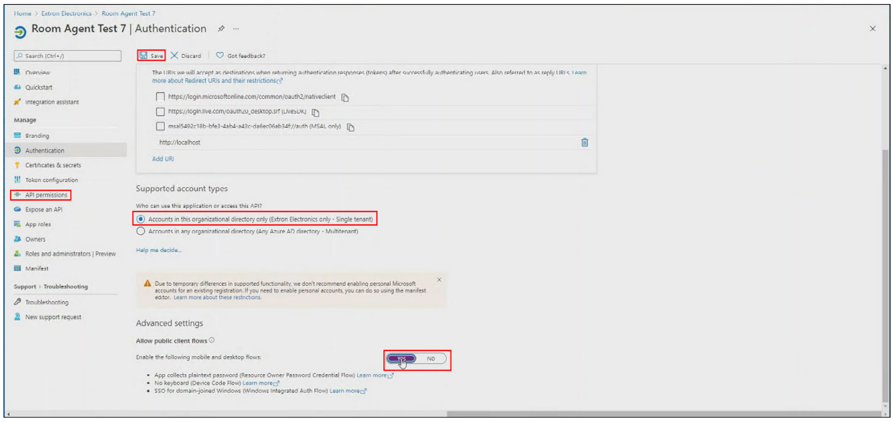


Figure 169. Room Agent Credentials — Authentication

11. Select **`Accounts in this organizational directory only`**.

12. Select **`Yes`** for the `Allow public client flows` toggle in the `Advanced Settings` section.

13. Click **`Save`**.

14. Click **`API permissions`**.

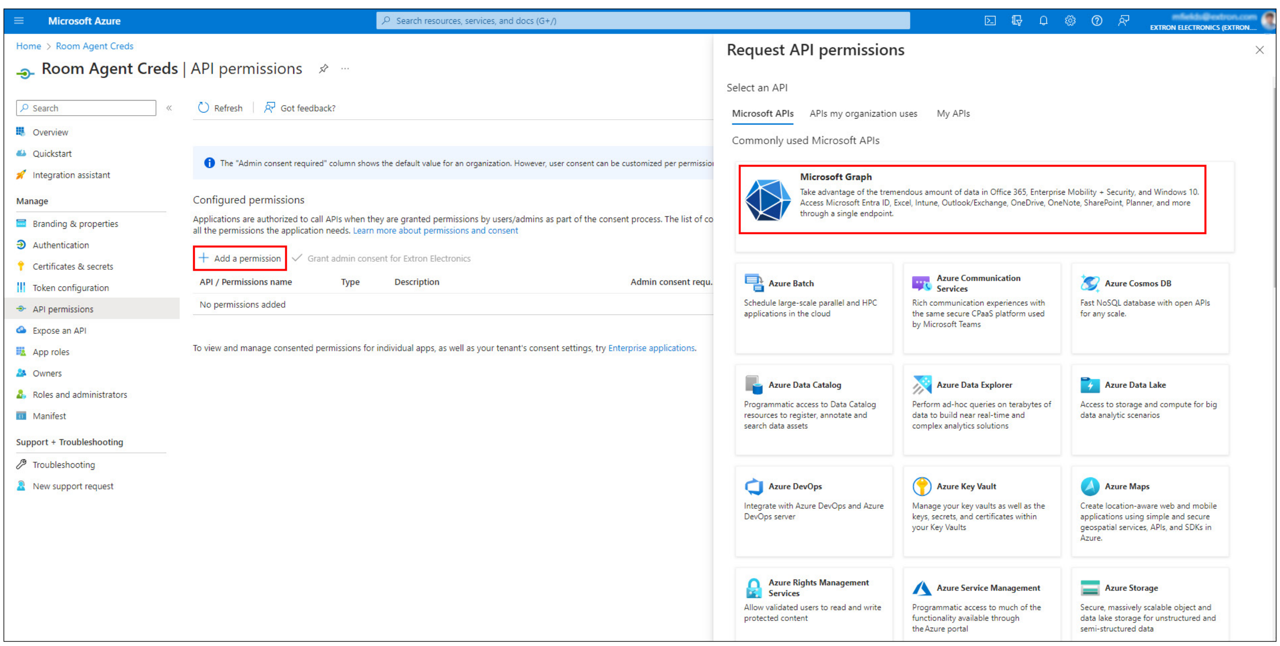


Figure 170. API Permissions

15. Click **`+ Add a permission`**. The `Request API permissions` pane opens.

16. Click **`Microsoft Graph`**.

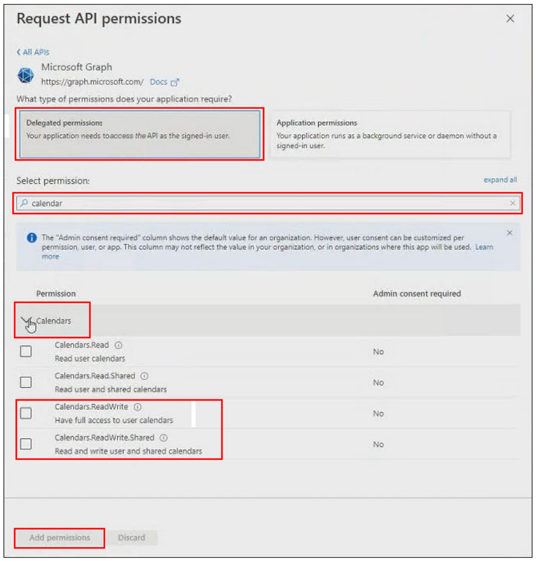


Figure 171. Request API Permissions

17. Click **`Delegated permissions`**. A list of permission categories opens.
18. (Optional) Enter `Calendars` in the `Select permission` search box. This narrows the number of options listed.
19. Click **`Calendars`** to expand the calendar options.
20. Select the **`Calendars.ReadWrite`** and **`Calendars.ReadWrite.Shared`** check boxes.
21. Click **`Add permissions`**.

    The added permissions are listed.

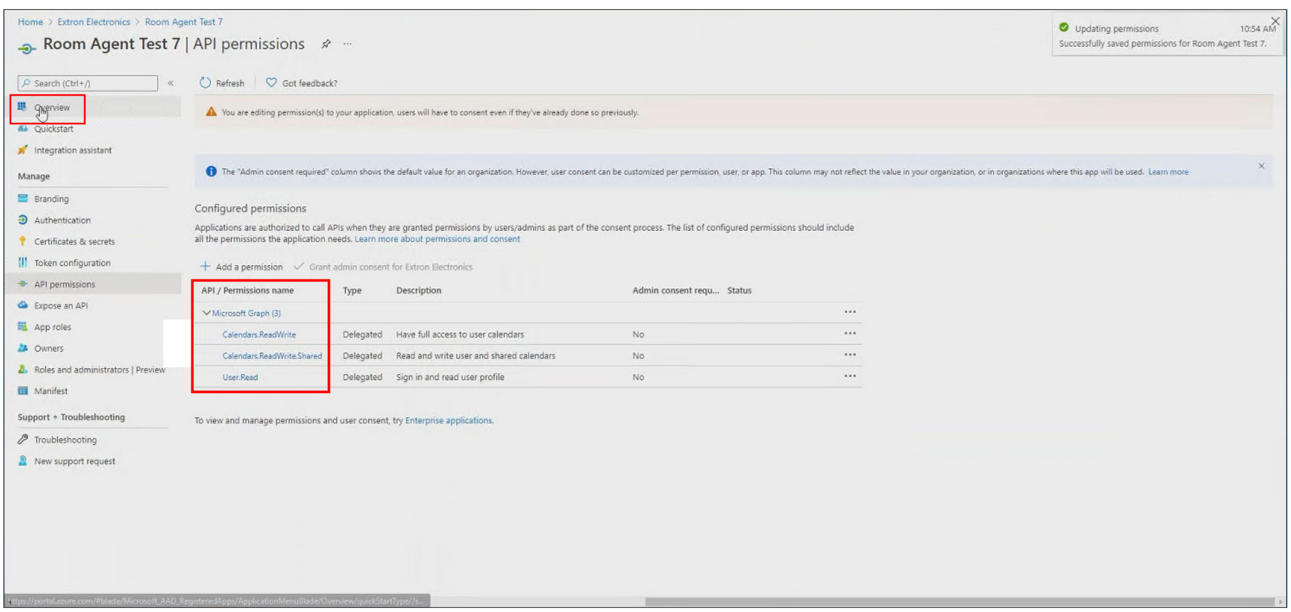
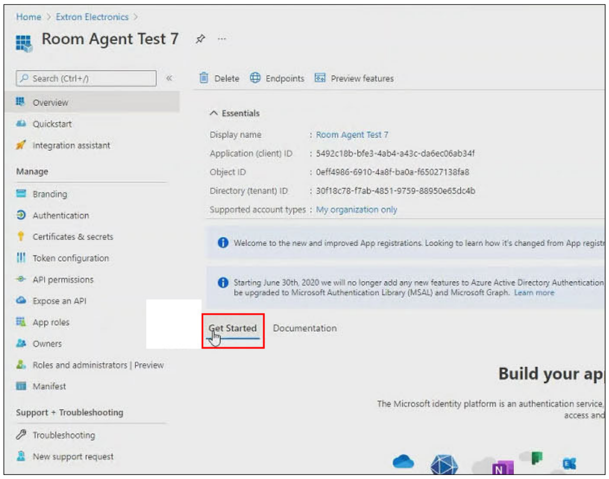


Figure 172. Permissions Granted

22. Click **`Overview`**.

The `Overview` page opens:



23. Click **`Get Started`**.

Assigning Oauth Credentials to Room Agent

1. Open Room Agent and select the **`CONFIGURE`** tab.

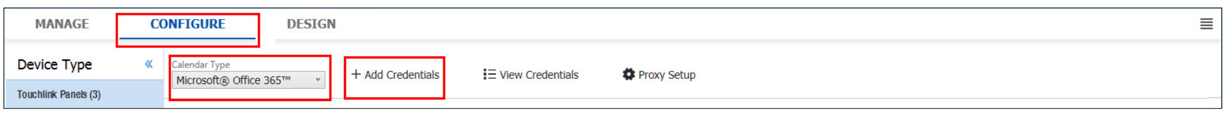


Figure 173. Microsoft Office 365 CONFIGURE Tab

2. From the drop-down list of calendars, select **`Microsoft® Office 365™`**.

3. Enter the calendar server URL path. Usually this is `outlook.office365.com`, but it is not shown in the user interface.

4. Click **`+ Add Credentials`**.

The `Device Authentication to Office 365` dialog box opens.

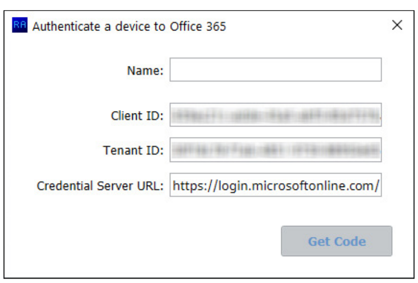


Figure 174. Device Authentication to Office 365

5. Provide a `Name` for the Credentials.

6. Enter the `Client ID` and `Tenant ID`, which were obtained in **step 9** of the previous section, on page 105.

7. If necessary, change the `Credential Server` URL. The default URL, which appears in the user interface is `https://login.microsoftonline.com/`. If you are using GCC, ensure that the correct URL is entered: for example `login.microsoftonline.gov`.
8. Click **`Get Code`**.

   The dialog displays a QR and a code.

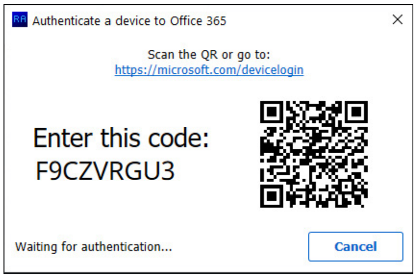


Figure 175. QR Code for Device

9. Scan the **`QR`** or enter `www.microsoft.com/devicelogin` into a browser.

   The Microsoft website opens:

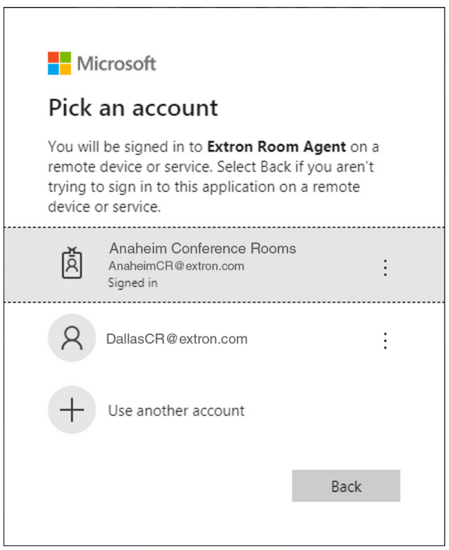


Figure 176. Select Account

10. Select an account that will provide authorization for Room Agent to read its calendar.

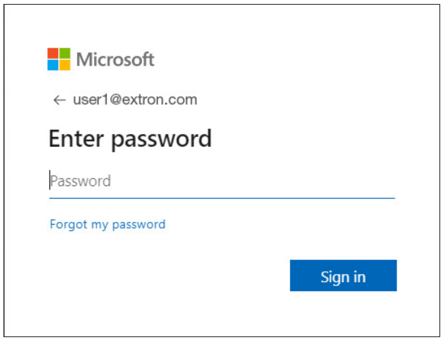
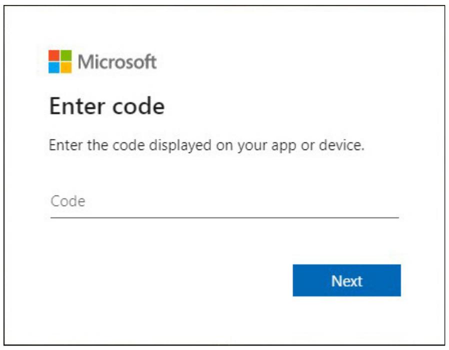


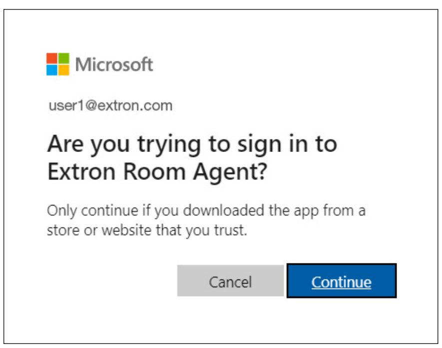
Figure 177. Enter Password for Account

11. Log in to that account.



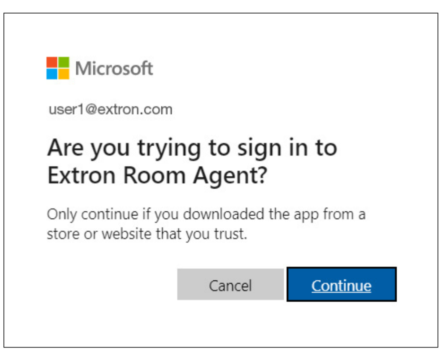
12. Enter the code for that account (see **step 8** on page 108).
13. Click **`Next`**.

    Microsoft requests verification that you are signing in to Room Agent.

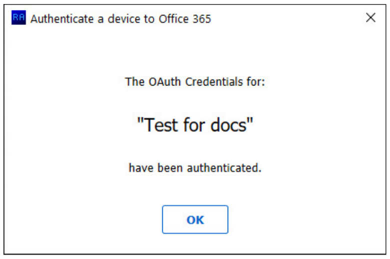


14. Click **`Continue`**.

    The Microsoft website confirms that the OAuth process is complete.



The Room Agent `Authenticate a device to Office 365` dialog box also confirms that the credentials have been authenticated.



15. Click **OK**.

Assigning Oauth Credentials to Touchpanels

In the **CONFIGURE** tab, use the `Credentials` drop-down list for a touchpanel to ensure that the OAuth Credentials match the name given when you authenticated the device to Office 365 in **step 9** on page 108.

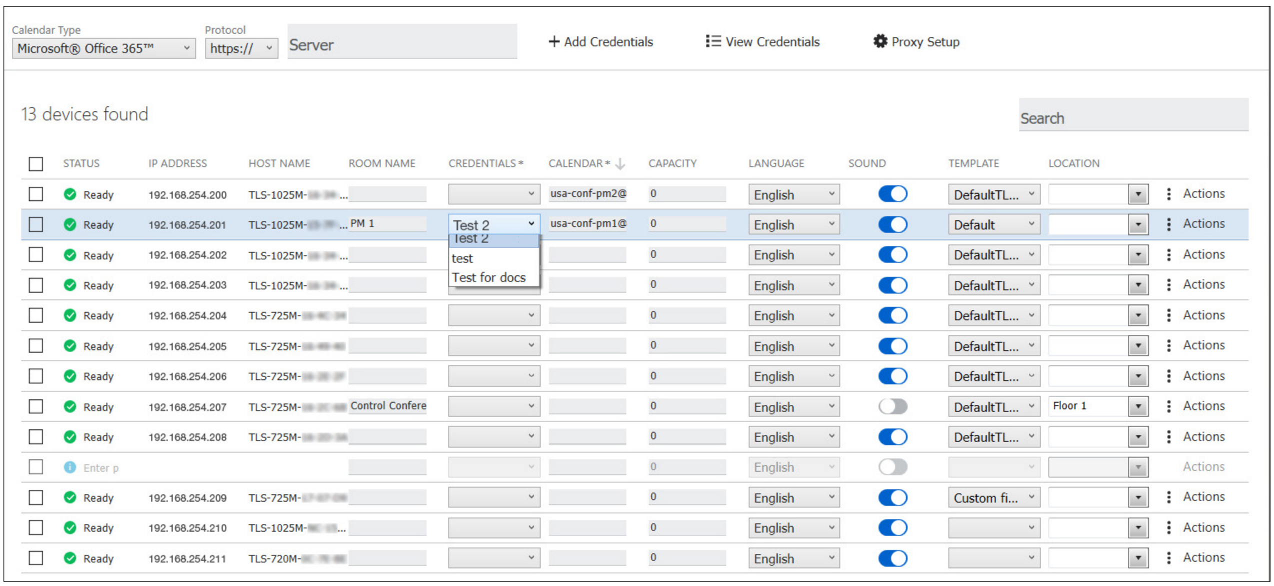


Figure 178. Assigning OAuth Credentials to Touchpanels

Korbyt Booking / NFS

1. Open Room Agent and select the **CONFIGURE** tab.
2. Select **NFS** from the `Calendar type` drop-down list(see figure 179)

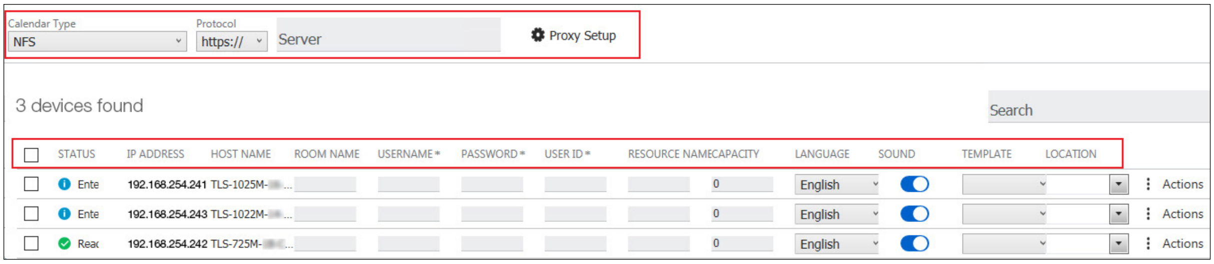


Figure 179. NFS Calendar Column Headings

3. Select a protocol (**`http://`** or **`https://`**).

   If you use the `https://` protocol to connect to the calendar server, the proxy server must be set up as **`TLS Pass Through`**. This is required for the TLS to validate the calendar server SSL certificate (see **Set up a Proxy Server** on page 40).
4. Enter the name of the NFS server in the `Server` field.
5. The following column headings appear in the lists of panels:
   - `STATUS` — Use this check box to select individual panels for configuration.
   - `IP ADDRESS` — This cell contains the IP address of the TouchLink panel.
   - `HOST NAME` — The hostname is a fully qualified domain name that uniquely identifies the computer. It is required for the computer to communicate with other devices on the network.
   - `ROOM NAME` — This is the name that appears on the touchscreen, once it is configured.
   - `USERNAME` — this is the user name for an account with access to the NFS server. It is typically an administrator account.

     NOTE: The password and User ID are both provided by an NFS administrator. These are API credentials that may be the same as the web page login credentials but this is not required.

   - `PASSWORD` — this is the password for the account with access to the NFS server.
   - `USER ID` — this is a field assigned to the user by NFS and required for booking events from a panel. The User ID can be a name, such as `Extron User` or it can be an email address.

     Log on to the NFS server. The User ID is shown in the top right corner (see figure 180).

     NOTE: You need an administrator account to log in to the NFS server.

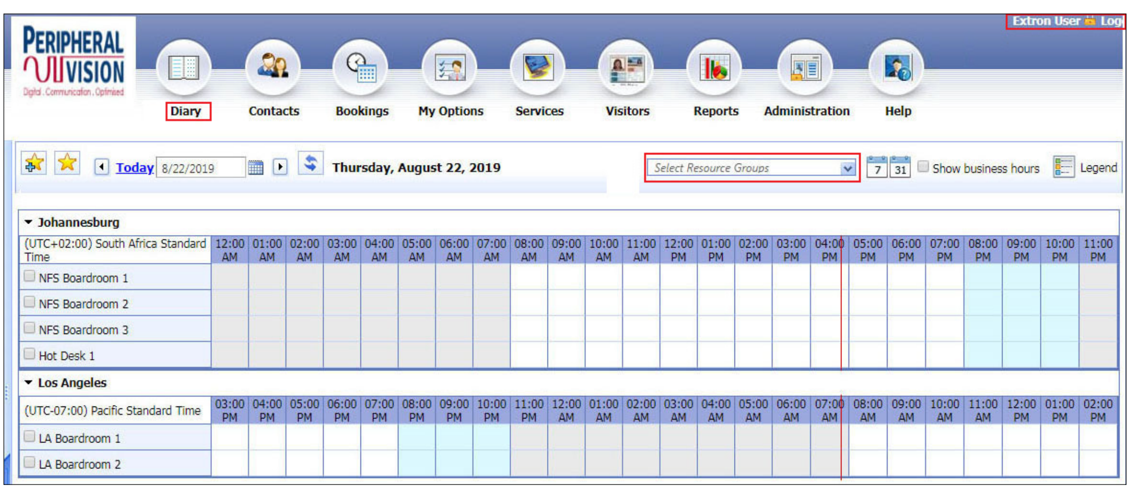


Figure 180. NFS Server

- `RESOURCE NAME` — this field must match exactly the name set up on the NFS server. Check the name by searching for the resource in the NFS server setup.

  a. Log on to the NFS server.

  b. Click **`Diary`**.

  c. Choose a **`Resource Group`** from the drop-down list. A list of resources in the selected group or groups is shown.

  To add a new resource:

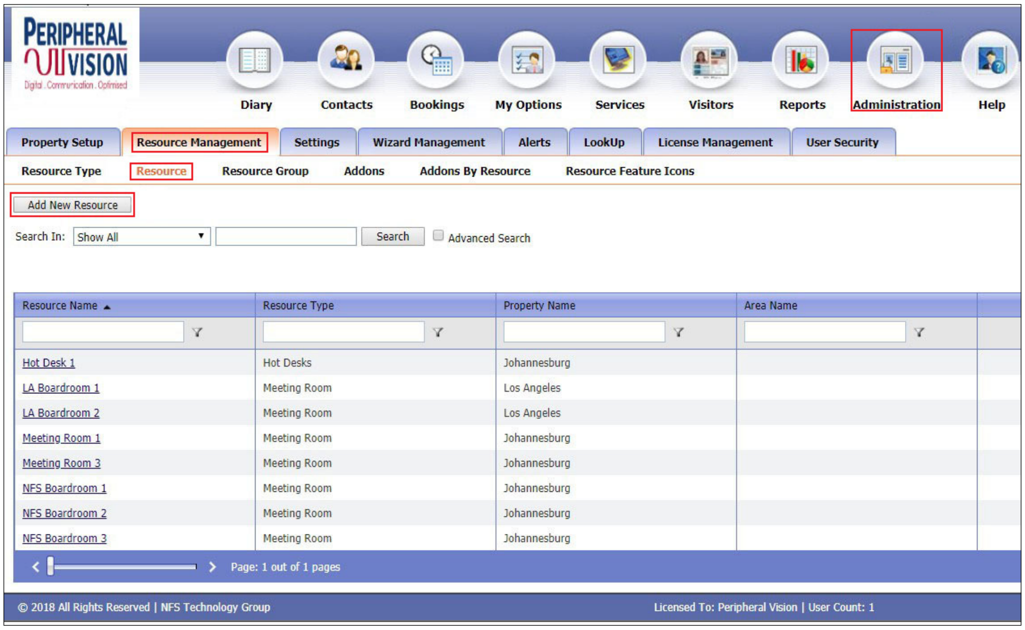


  Figure 181. NFS — Add a New Resource

  a. Click **`Administration`** (see figure 181).

  b. Select the **`Resource Management`** tab.

  c. Select **`Resource`**.

  d. Click **`Add New Resource`** and provide the required information.

- `CAPACITY` — Set the maximum number of people allowed in the room in this column.
- `LANGUAGE` — Select an option from the `LANGUAGE` drop-down list. By default, the language is **`English`**.
- `SOUND` — Set the **`Sound`** switch to **`Off`** or **`On`**. When it is set to **`On`**, pressing a button provides audible feedback. If it is set to **`Off`**, there is no sound.
- `TEMPLATE`— The layout of the panel can be configured using the `DESIGN` tab. You can select one of the saved panel design files from this drop-down list.
- `LOCATION` — Use a location tag to group nearby rooms, for example "Floor 1". This is displayed as the room location in the Wayfinding Device. When rooms are shown as a list on the Wayfinding Device, they are grouped by their location tag.

There is also an `Actions` drop-down list for each touchpanel:

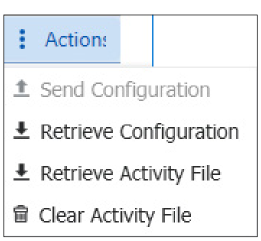


Figure 182. Configure Tab —Actions List

After verifying that the information is correct for all TLS panels, select one or more panels and click **`Send Configuration`** to save the configuration on the control PC. Alternatively, click **`Retrieve Configuration`** to retrieve a previously saved configuration and apply it to the selected panel.

You can also retrieve or clear the activity file associated with that panel (see **Room Scheduling Analytics** on page 186).

Configure Individual TLS Panels

Figure 183 shows the **`CONFIGURE`** tab headings for Microsoft Office 365. A few of the column headings depend on the calendar server that was selected. For Microsoft Office 365, these are `ROOM NAME`, `CREDENTIALS`, and `CALENDAR`. The other headings (`STATUS`, `IP ADDRESS`, `HOSTNAME`, `CAPACITY`, `LANGUAGE`, `SOUND`, `TEMPLATE`, and `LOCATION`) are common for all calendar servers.

Refer to the section about your calendar server for the specific information required for each column when configuring the TLS panels for that calendar server.

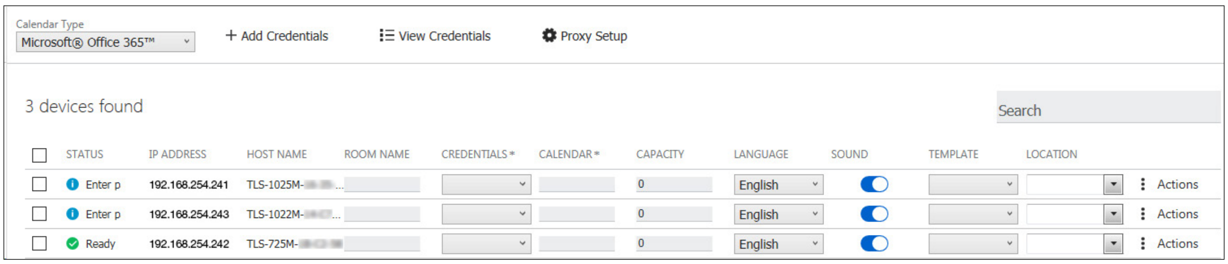


Figure 183. Select Microsoft® Office 365™ Calendar Server

1. Select **`Touchlink Panels`** from the menu on the right.
2. Select the **`Status`** check box for the TLS panel you wish to configure.
3. Enter the correct information in each field. All fields are required. The `IP ADDRESS` and `HOSTNAME` are usually filled automatically.
4. After you have configured one or more panels, you can upload the configuration file to the panel and save it there.
   - To upload the configuration to the touchpanel, click **`Send Configuration`** (for more information, see **Saving Individual Configuration Files to the Appropriate Touchpanels** on page 113.
   - If you have previously configured one or more panels and saved your configuration to the panel, you can retrieve that configuration file by clicking **`Retrieve Configuration`** (for more information, see **Retrieving a Configuration** on page 114).
   - If you have previously configured the entire system and uploaded the individual configuration files to the appropriate touchpanels, you can retrieve all the individual records from the touchpanels to rebuild the system configuration file.

Sending and Retrieving Configurations

Saving Individual Configuration Files to the Appropriate Touchpanels

Once you have edited one or more configuration files, you can upload the individual files to the corresponding touchpanels. That information is used to configure that panel. You can retrieve the most recently sent configuration from the panel and save it to the system configuration file if the system configuration file gets deleted or becomes corrupted.

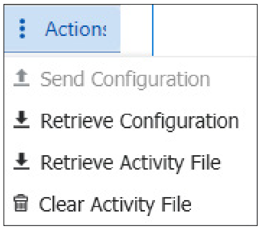


Figure 184. Sending and Retrieving Configurations

1. Click the **Actions** drop-down list on the line for the touchpanel you have configured.
2. Click **Send Configuration**.

> **NOTE:** The **Send Configuration** button may be unavailable for either of these reasons:
> - The device has not been set up.
> - All fields must all contain valid values. If one or more of those values is missing, the configuration file is incomplete and cannot be sent.

3. The individual configuration files are uploaded and saved on the touchpanels they apply to.

Alternatively, you can select a touchpanel by selecting the check box at the start of the line. From the menu that appears at the top of the page, click **Send Configuration**.

Retrieving a Configuration

If you have previously configured one or more panels and saved the individual configuration files on the corresponding touchpanel, you can retrieve the configuration and save it into the system configuration file.

To retrieve a configuration:

1. Click the **Actions** drop-down list on the line for the touchpanel you have configured.
2. Click **Retrieve Configuration**.

Alternatively, you can select a touchpanel by selecting the check box at the start of the line. From the menu that appears at the top of the page, click **Retrieve Configuration**.

Retrieving Multiple Configurations Simultaneously

To download the complete configuration information from multiple touchpanels at once:

1. Select the check boxes next to all the appropriate panels.
2. From the menu that appears at the top of the page, click **Retrieve Configuration**. All the individual records are downloaded from the touchpanels to the control PC.

Rebuilding a System Configuration File from Individual Records

If the system configuration file on the control PC is accidentally deleted or becomes corrupted, it can be rebuilt by pulling the individual records from some or all the touchpanels.

1. Select the **Status** checkboxes for the required touchpanels.
2. Click **Retrieve Configuration**.

   The individual records for each touchpanel are pulled back to the control PC.
3. Click the **Menu** button and select **Save Configuration**.

Retrieve and Clear the Activity File

Each TLS panel maintains an activity file and a log of scheduling information (such as the meeting subject, meeting organizer, booking date, meeting date and starting time and duration) among other data for the assigned room. The activity file can be retrieved and written to the PC running the Room Agent software as an Microsoft Excel spreadsheet or cleared (erased) from the panel. You can use data analytics tools to transform this activity data to create usage reports.

> **NOTE:** The panel has 4 Mb of activity file memory. The number of entries varies depending on the size of each entry, but may number in the hundreds. When the memory becomes full, the newest entries overwrite the oldest. There is no notification when the memory becomes full.

Retrieve one or more activity files as follows:

1. Select one or more **`Status`** checkboxes.
2. Click the **`Retrieve Activity File`** option from the `Action` menu (see **figure 184** on page 114) to fetch the schedule log and from one or more panels and save it in a spreadsheet. The Room Agent software opens the `Panel Activity File` dialog box.
3. If required, navigate to the folder where the file is to be saved.
4. Enter a name for the retrieved activity file (see figure 180).
5. Click **`Save`**.

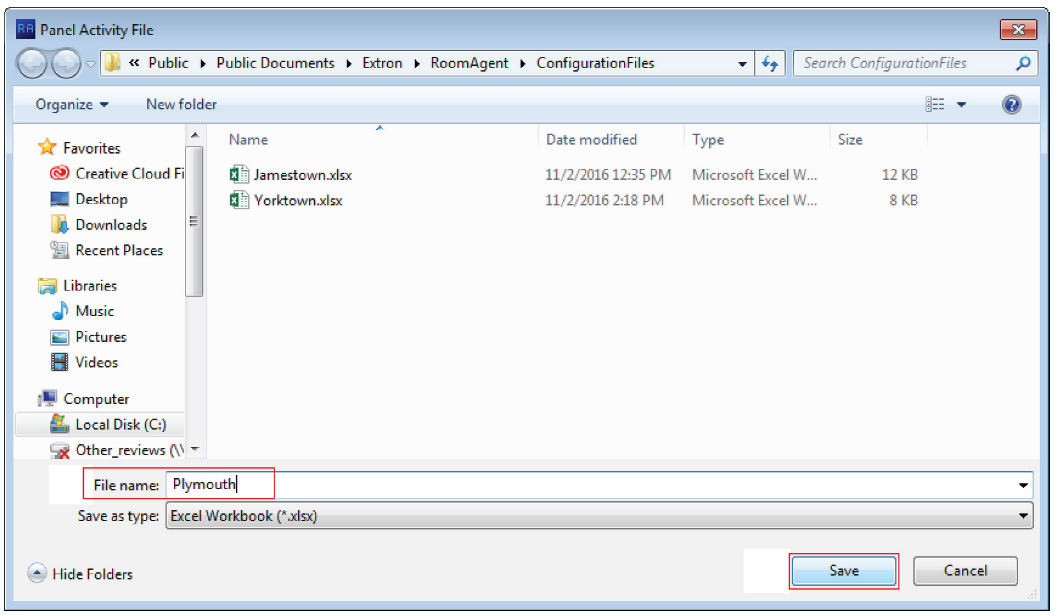


Figure 185. Panel Activity File

The Room Agent software saves the file. It reports that the `Status is in progress` () and then reports `Activity retrieved` and `All activities have been retrieved successfully`.

Clear one or more activity files as follows:

1. Click the **`Clear Activity File`** drop-down list option (see **figure 184**) to erase the schedule log from one or more panels.

   For the clear operation, the Room Agent software reports that the Status is in progress () and then reports `Cleared` and `All panel activity logs have been cleared successfully`.
2. Click **`OK`** to exit the clear operation.

For more information, see **Room Scheduling Analytics** on page 186.

Retrieve a template

Templates allow you to create a number of customized panel appearances.

Templates can be designed and saved, using the **CONFIGURE** tab. Once they are saved, they are available in the `Templates` pane.

You can retrieve the template assigned to a panel, for example to use as a starting point for designing a new panel layout, as follows:

1. Right-click the panel in the `STATUS` column.
2. Click the pop-up **`Retrieve Template for Design`** button. The `Retrieve Template` dialog box opens:

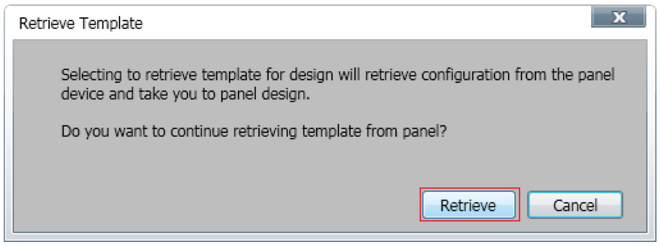


Figure 186. Retrieve Template Dialog Box

3. Click **`Retrieve`** (see figure 181). Room Agent software displays the `Retrieving Template ... activity` indicator while it loads the template and then automatically jumps to the `DESIGN` tab (see **Design Tab** on page 121).

Configure Wayfinding Devices

1. Open Room Agent.
2. Click **`CONFIGURE`**.
3. Select the **`Wayfinding Devices`** option in the menu on the left side of the page.

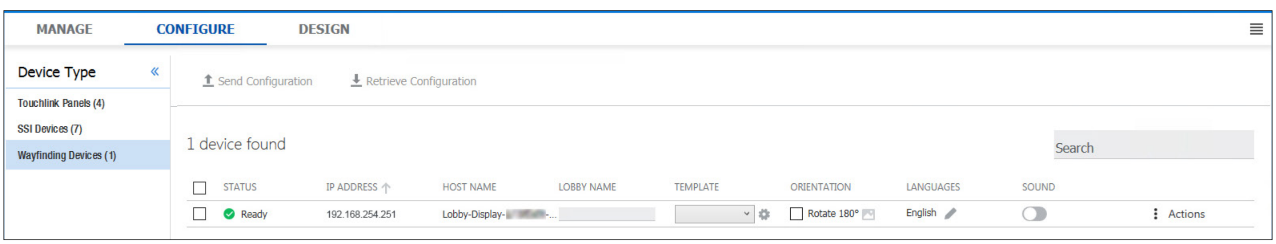


Figure 187. Configure Wayfinding Devices

4. Click in the cell in the `TEMPLATE` column for the device you wish to configure.
5. You can choose to display in **`List`** or **`Map`** format and in **`landscape`** or **`portrait`** orientations. If you have saved other configurations, these are also listed.

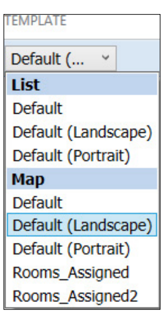


Figure 188. Wayfinding Device — Design Options

6. (Optional) Select the **ORIENTATION** check box (see **figure 187** on page 116). This flips the screen from top to bottom (in landscape orientation) or from right to left (in portrait orientation). This is useful if the display devices have been pre-installed in an unsuitable orientation.
7. Click on the **Select Rooms** link to assign TLS panels to a specific Wayfinding device (see **Associating TLS Panels with a Wayfinding Device** on page 120).
8. There are seven column headings. These are not affected by the calendar setting:
   - STATUS — Use this check box to select individual panels for configuration.
   - IP ADDRESS — This cell contains the IP address of the TLSI 201 Interface.
   - HOST NAME — The hostname is a fully qualified domain name that uniquely identifies the computer. It is required for the computer to communicate with other devices on the network.
   - LOBBY NAME — This is the name that appears on the Wayfinding Device, once it is configured.
   - TEMPLATE — Click on this box to open a drop-down list that allows you to select one of the saved panel design templates. You can choose one of the List templates or one of the Map templates. The templates must have been created in advance (see **Design Tab for Indicators (SSI)** on page 145 or **Design Tab for Wayfinding (Map)** on page 158).

     This column may also contain a hyperlink, allowing you to organize the room panels associated with the Wayfinding Device (see **Associating TLS Panels with a Wayfinding Device**).
   - SOUND — Set the **Sound** switch to **Off** or **On**. When it is set to **On**, pressing a button provides audible feedback. If it is set to **Off**, there is no sound.
   - LANGUAGE — The TLSI can be configured to show
     - A single language.
     - Two languages side by side.
     - Multiple languages, one after another.

     The default is English as a single language.

     1. Click the link to open the Language Settings dialog box.

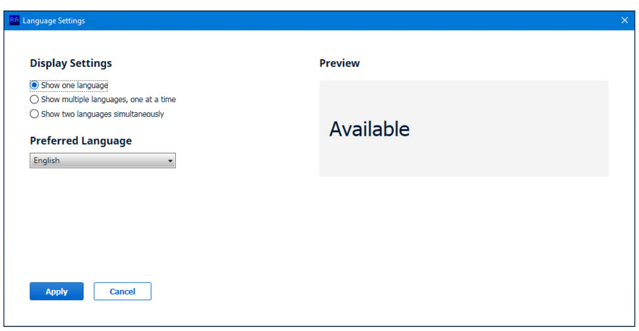
     

     Figure 189. Language Settings — Show One Language

     2. Select an option by clicking the appropriate radio button.
        - **Show one language**
        - **Show multiple languages, one at a time**
        - **Show two languages simultaneously** on page 119

Show one language

Select a language from the Preferred Language drop-down list (see **figure 191** on page 118) and click **Apply**.

Show multiple languages, one at a time

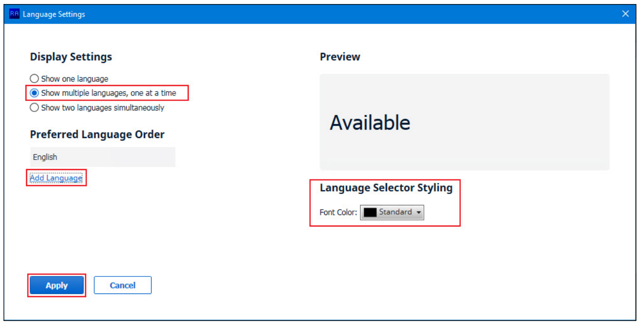


Figure 190. Language Settings — Multiple Languages

1. Select `Show multiple languages, one at a time`.
2. Click `Add Language`.
3. The `Add Language` dialog box opens.

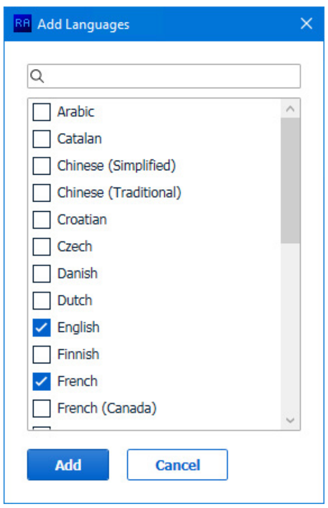


Figure 191. Add Language Dialog Box

By default `English` is selected. You can remove English by deselecting the box and selecting other languages.

4. Select one or more languages and click `Add`.

The `Add Language` dialog closes and a list of the selected languages is shown.

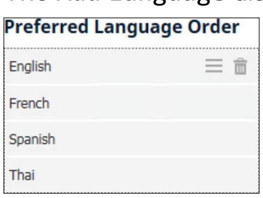


Figure 192. List of Selected Languages

When you hover the mouse over one of your choices, you see the list and trash icons. You can click on the `trash` icon to remove the language from the list or click and drag the language to a different position in the list.

You can also show the language in `Standard` (black) font or `Highlight` color.

In figure 192, the Wayfinding device displays information in English, then in French, then in Spanish, and finally in Thai, before beginning the cycle again.

Show two languages simultaneously

If you select this radio button, the options are the same as Show multiple languages, one at a time but only the first two languages in the `Preferred Language Order` table are available. Any other languages added to the table are grayed out and unavailable unless they are moved into the top two.

Figure 193. Selecting Two Languages Simultaneously

In figure 193, English and French are shown at the same time and Czech is not shown.

Save Configuration for Wayfinding Device

1. Select the check box next to the Wayfinding Device that you have just configured.
2. The top menu becomes available.
3. Click **`Send Configuration`**.

List Format

1. Design the Wayfinding display layout (see **Design Tab for Indicators (SSI)** on page 145).
2. Save the template.
3. Assign rooms to the required locations (see **Associating TLS Panels with a Wayfinding Device** on page 120).
4. In the **`CONFIGURE`** tab, select the check box in the `STATUS` column that is next to the Wayfinding Device that you are configuring.
5. Click in the **`TEMPLATE`** column for that Wayfinding Device.

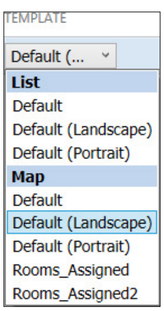


Figure 194. Wayfinding Device — Template Options

6. Select one of the templates shown under the `List` heading.
7. Click **`Send Configuration`**.

Map Format

1. Design the Wayfinding Device layout (see **Design Tab for Wayfinding (Map)** on page 158).
2. If required, create multiple maps to show multiple locations.
3. Assign rooms to the map (see **Add rooms to the map** on page 161).
4. Save the template.
5. In the **`CONFIGURE`** tab, select the check box in the `STATUS` column that is next to the Wayfinding Device that you are configuring.
6. Click in the **`TEMPLATE`** column for that Wayfinding Device.
7. Select one of the templates shown under the `Map` heading.
8. Click **`Send Configuration`**.

Associating TLS Panels with a Wayfinding Device

1. Click the hyperlink in the `TEMPLATE` column.

   The `Select Rooms` dialog box opens:

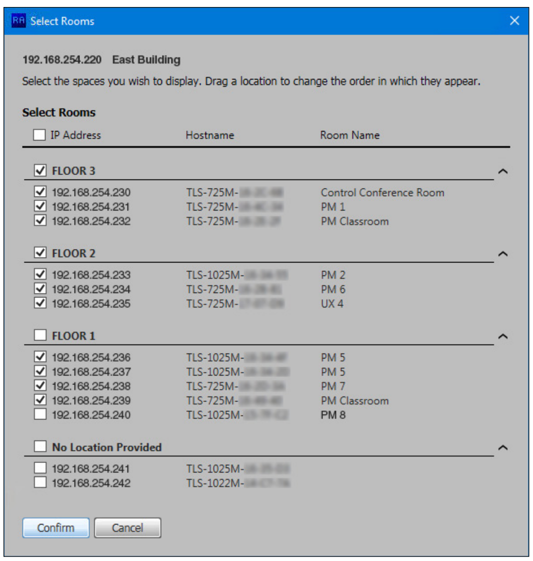
   

   Figure 195. Select Rooms Dialog Box

   The rooms are grouped by the location selected in the location column when configuring the individual rooms.

   All the rooms from a single location are shown by the Wayfinding Device as a single group. For example the three rooms shown for the `FLOOR 3` location are listed together by the Wayfinding Device.

2. Select the rooms that are to be displayed by selecting the checkbox next to that room.

   The first four rooms shown for the `FLOOR 1` location are listed together by the Wayfinding Device. The fifth room is not listed because the checkbox was not selected.

3. Click and drag the locations into the desired order.

   The rooms for the first location in this list are shown on the first screen of the Wayfinding Device.

   The rooms for the second location are shown on the second screen and so on.

4. Click **`Confirm`** to save the selection.

   The TLSI 201 interface uses Room Agent software to obtain and collate scheduling information from individual touchscreens in the system and display that information on a large third-party touchscreen.

   This provides a centralized display of real-time information about meeting space availability, status, and location. Users can locate and book meeting spaces for the day or week on an interactive grid or map with ease. For more information about the TLSI 201, see the *TLSI 201 User Guide*, at **www.extron.com**.

Design Tab

The controls in the DESIGN tab allow you to design and configure the appearance and function of the TLS panels and Wayfinding devices.

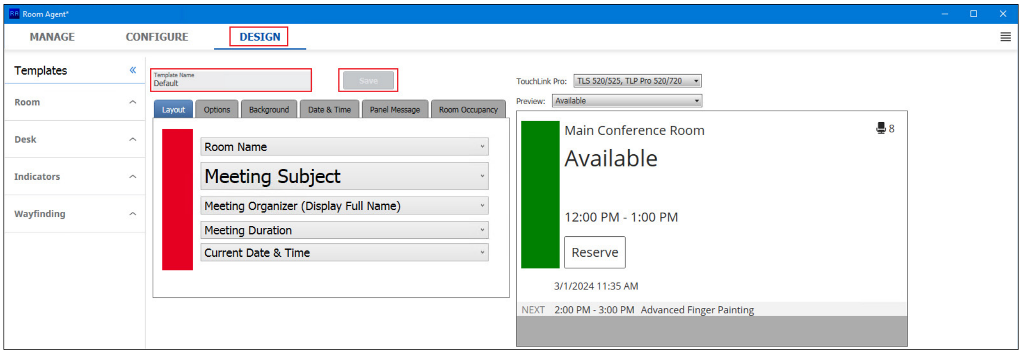


Figure 196. Design tab for TLS Panels

To configure the GUI for a touchpanel or Wayfinding Device:

1. Open Room Agent and click **DESIGN** (see figure 196).
2. Use the Templates side bar to find available templates for rooms and Wayfinding Devices. By default the DESIGN tab opens with Room Templates selected.
3. The Templates side bar can be collapsed into the side of the window.

For more information about the DESIGN tab go to the following sections:

- Design Tab for Rooms
- **Design Tab for Desk** on page 134
- **Design Tab for Indicators (SSI)** on page 145
- **Design Tab for Wayfinding (List Format)** on page 150
- **Design Tab for Wayfinding (Map)** on page 158

Design Tab for Rooms

The controls in the DESIGN Tab allow you to design and configure the graphical user interface (GUI) for each touchpanel (see figure 196)

1. Open Room Agent and click **DESIGN**.
2. Select **Templates > Room** in the sidebar on the left side of the screen.

   A list of available room templates opens. Initially there is only one template available, called DefaultTLPTemplate. As you create and save your own templates, they are added to this menu.
3. Select a template from the list. The name of the template that you selected appears in the Template Name text box.
4. Save the template:
   - If you make changes to the existing template that you wish to save, click **Save** (see figure 196). The template is saved with the same name, but incorporating the changes you made.
   - If you make changes to the template that you wish to save as a new template, type the new template name into the Panel Template text box and click **Save**. The new template is saved and the original template, without changes, is still available.
   - If you have retrieved a template, the name shown in the text box is grayed out (not selectable). Click **Save**. The name is shown in normal text and is listed in the Templates panel on the left of the screen.

5. Use the controls in any of the following `DESIGN` tabs to configure the GUI appearance:
   - **`Layout`** tab
   - **`Options`** tab
   - **`Background`** tab
   - **`Date & Time`** tab
   - **`Panel Message`** tab
   - **`Room Occupancy`** tab
   - The `Preview` panel allows you to see how the configuration affects the appearance of the different touchpanel screens.

Templates Pane

Templates allow you to create a number of customized panel appearances. Each panel in a system can have its own template, assigned on the `CONFIGURE` window. Select the templates in the `Templates` pane.

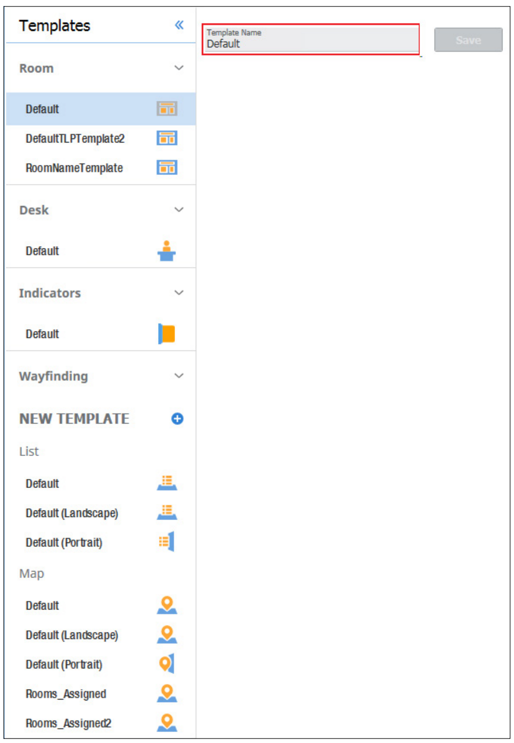


Figure 197. Templates Pane and Drop-down list

To add a new template or rename an existing template:

1. Type a name in the `Panel Template:` field.
2. Click the **`Save`** button.

To delete a template, move the mouse over the icon next to the template name in the Template list. The icon changes to a trash can. Click on the **`trash can`** and confirm that you wish to delete the template.

To assign a saved template to a TLS panel, open the `CONFIGURE` tab and select the TLS panel. Click in the **`Design cell`** for that panel and select a template from the list.

Layout Tab

After you have chosen the Room template, use the **Layout** tab to assign values to the text boxes. Changes to the template are shown in the Preview pane (see **figure 196** on page 121).

NOTES:

- When you select **Retrieve Template for Design** in the **CONFIGURE** tab (see **Sending and Retrieving Configurations** on page 113), the layout tab opens to show the template that has been retrieved.
- When the tab opens, the name in the Panel Template text box (see figure 198, ❶) is unavailable, even if the name is in the Templates list in the panel on the left side of the window (❷). Click **Save**. If a template of the same name is already available, you are asked if you want to overwrite the existing version with the downloaded version. If the template was not already available, it is added to the list. The name of the template in the Panel Template text box (❶) is now available.

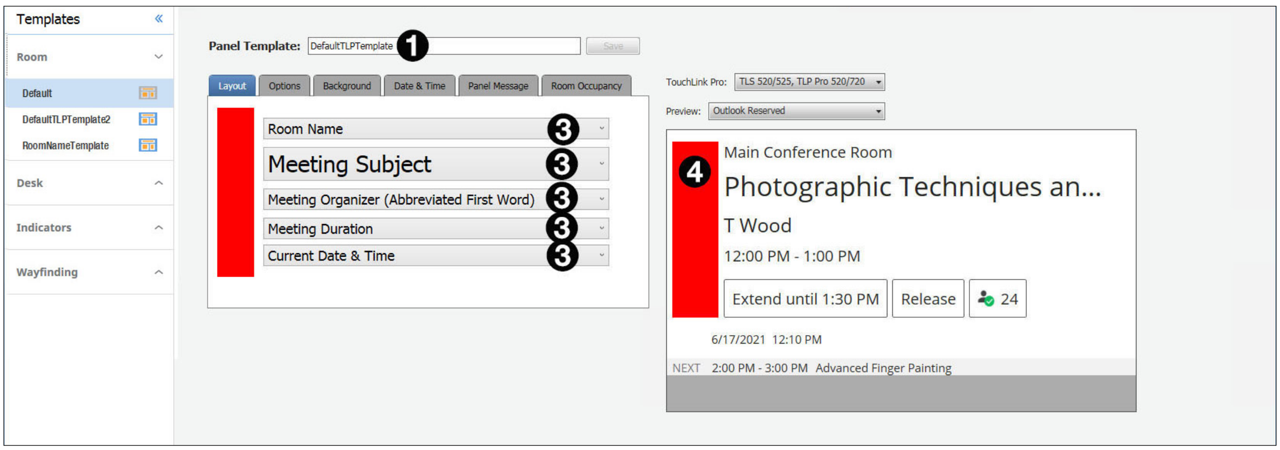


Figure 198. TLS Layout Tab

Several drop-down lists (❸) allow you to select the text that the user sees in the corresponding box of the live screen.

The menu for each box offers the following options:

- **Room Name**
- **Meeting Subject**
- **Meeting Organizer (Display Full Name)**
- **Meeting Organizer (Abbreviated First Word)**
- **Organization**
- **Meeting Duration**
- **Current Date & Time**
- **Current Date**
- **Current Time**
- **Blank**
- ***Custom Field**

* This option is available only when Microsoft Exchange or Microsoft Office 365 is selected as the calendar type. It displays up to 50 characters from the body of the meeting invitation.

NOTES:

- Any line can be set to any of the values listed above. For example, you can switch Meeting Subject and Room Name so that Meeting Subject is in the first box and Room Name is underneath it.
- If no meeting has been booked, the Meeting Subject field is set to Available and the Organizer and Duration fields are blank.
- When you use Google, Microsoft Exchange, or Office 365 calendars, you can create private meetings. For these meetings, the subject title defaults to Private Meeting and the meeting organizer is hidden.

Options Tab

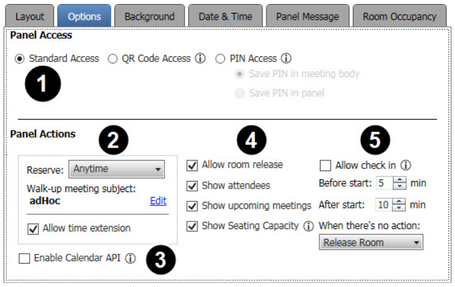


Figure 199. TLS Options Tab

The **Options** tab allows users to set options for:

- **Panel Access**
- **Check the Allow room release box (4) to allow the user to release the room if the meeting is canceled or finishes early.**
- **Reserving and extending meetings**
- **Scheduling ad hoc meetings**
- **Enabling the calendar API**
- **Allow room release if meeting called off or ends early**
- **Show room capacity and attendees**
- **Show upcoming meetings**
- **Allow check in to meetings**

Panel Access

Use the `Panel Access` section (see figure 199, ❶) to decide how the panel will be accessed:

- **`Standard Access`** – Use this radio button for normal access with no security features.
- **`QR Code Access`** – Use this radio button to enable QR code use. When this feature is enabled, the TLS requires a user to authenticate via a QR code to perform actions such as reserve, release, extend, and check in.

  When a user approaches the TLS, the only action available on the UI will be authenticate. Once the user presses authenticate, the TLS displays a QR code and one-time passcode. The user scans the QR code with their phone and is taken to a log in page where they enter the one-time passcode and choose the account they want to use. Once a user has authenticated, the normal reserve, release, extend, and checkin actions are available if enabled. After interacting with the TLS the user can press the log out button to lock the panel again. Once a meeting is booked via QR code, only the meeting organizer can edit the meeting.

  For Microsoft Office 365, the QR code feature is supported exclusively with the Microsoft Client Secret and Microsoft Certificate authentication methods only.

  If QR Code Access is enabled for a Google configuration, anyone in the tenant will be able to book to rooms calendars.

  > **NOTE:** This feature is available only on TLS x25 and TLS 300 models and only with Google and Microsoft Office 365 calendars. Microsoft O365 requires additional configuration.

- **`PIN Access`** – When this feature is enabled, the TLS includes a 5-digit PIN in the meeting body. This PIN is used for checking in to meetings, releasing meetings, and creating ad hoc meetings.

  Select either:

  - **Save PIN in meeting body**
  - **Save PIN in panel**

PIN access

When this feature is enabled, the TLS includes a 5-digit PIN in the meeting body. This PIN is used for checking in to meetings, releasing meetings, and creating ad hoc meetings.

Save PIN in meeting body

This feature is only available when using Microsoft Office365, Microsoft Exchange, or Google Calendar.

When enabled, the user will be prompted for a five-digit PIN anytime they attempt to Reserve, Extend, Check In, or Release the room.

Figure 200. Enter PIN Dialog

When creating an adhoc reservation, the user will be prompted to create their PIN. This PIN will be saved to the meeting body as shown in the figures below.

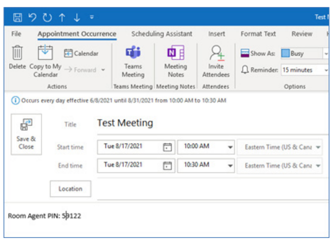


Figure 201. PIN saved for Office 365

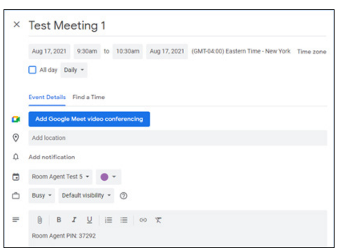


Figure 202. PIN saved for Google Calendar

If a meeting is created on the calendar server, the TLS will insert a random PIN into the first line of the meeting body.

Any existing content will remain intact, below the first line. If the user forgets the PIN or wants to change the PIN, they view or change it inside the calendar server interface.

Save PIN in panel

This feature works the same as “Save PIN in Meeting Body” but it does not modify the meeting body. The PIN is stored in the TLS memory only.

Reserving and extending meetings

Use the **Reserve:** drop-down list (see figure 199, ❷, on page 124) to configure how the user can make reservations:

- **Anytime** – Any visible time slot that is open can be reserved by the walk-up user.

  NOTE: Meeting notices cannot be sent for meetings booked by a walk-up user.

- **Current time only** – Only the currently available time slot can be reserved by the walk-up user.
- **Never** – No walk-up reservations are permitted.

Scheduling ad hoc meetings

Click **Edit** (❷) to open the `Walk-up meeting subject` dialog box.

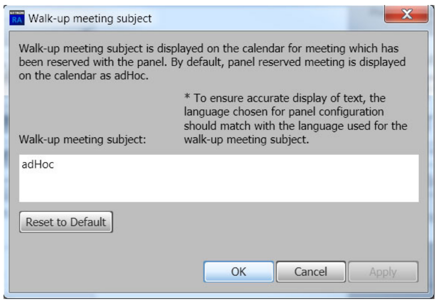


Figure 203. Walk-up meeting subject Dialog

Enabling the calendar API

Check or uncheck the **Enable Calendar API** checkbox (❸). When the checkbox is selected, other Extron devices, such as IP Link Pro xi control processors, can access the Room Calendar information. The user password can be updated from the device Manage tab.

NOTE: This feature may require a firmware update. Please talk to your Extron Representative.

Allow room release if meeting called off or ends early

Check the **Allow room release** box (❹) to allow the user to release the room if the meeting is canceled or finishes early.

Show room capacity and attendees

Check the **Show Attendees** box (❹) to allow meeting attendees to be seen. This feature is available with Google, Microsoft Exchange, and Microsoft Office 365 calendars.

When the box is selected the `Show Attendees` icon is shown in the preview panel. When the touchpanel is configured, pressing the icon displays a list of all the participants in the meeting.

Show upcoming meetings

Check the **Show Upcoming Meetings** box to allow meetings following the current meeting to be seen.

Allow check in to meetings

1. Check the **`Allow check in`** box to allow meetings that have been booked in advance to be confirmed and to release the room if nobody confirms within a certain time of the scheduled meeting start.

   If this box is checked, a **`Check in`** button appears on the panel for a scheduled meeting. The button disappears from a panel once it is pressed.

2. Click the information icon for additional information.

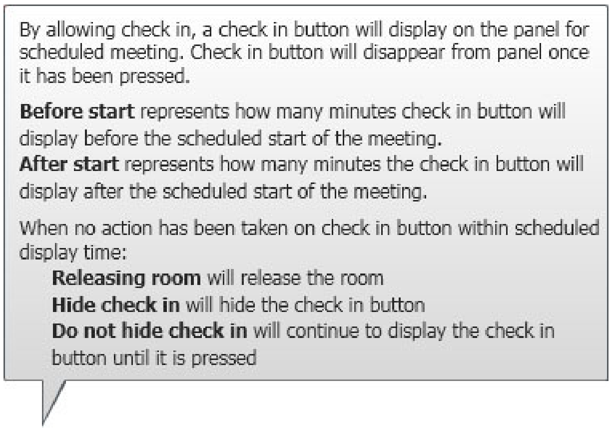


Figure 204. Check In Information Pop-up

Background Tab

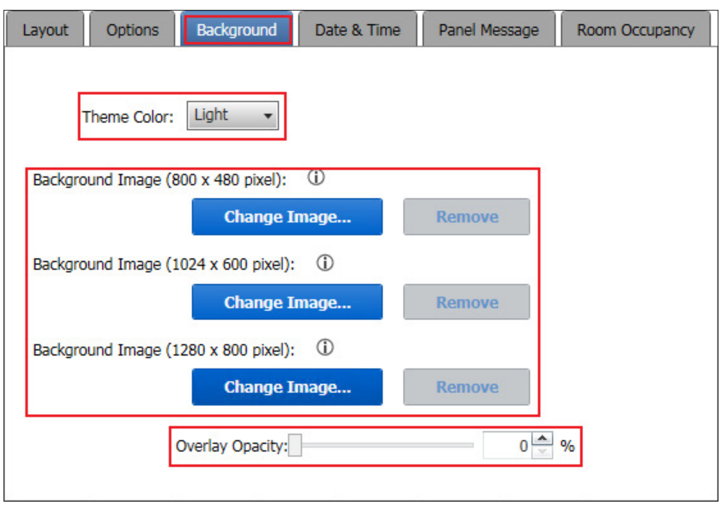


Figure 205. Background Tab — Light Theme

The **`Background`** tab (see figure 205) allows you to configure the background of the touchpanel GUI.

1. Select the theme color from the `Theme Color` drop-down list. The options are:
   - **`Light`**
     - Buttons are white.
     - Fonts are black.
     - Background is white.
     - When the background image is loaded, the opacity overlay is white.
   - **`Dark`**
     - Buttons are dark gray with a white border.
     - Fonts are white.
     - Background is dark gray.
     - When the background image is loaded, the opacity overlay is dark gray.
2. Click the **`Change Image`** button that corresponds to the resolution of your touchscreen, to select a background image, or remove the image if one has been previously selected.

   Click on the information symbol (ⓘ) to open a popup box with information about the images that can be used. The exact information depends on which touchpanel is being used:

   - Group A (TLS 1025)

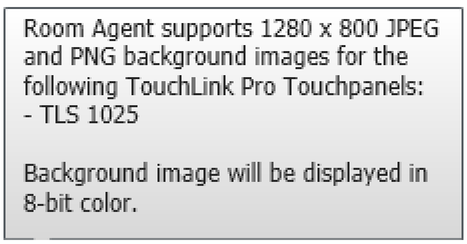


Figure 206. Background Image Information for 1280x800 TLS Panels

   - Group B (TLS 725 and TLS 1022)

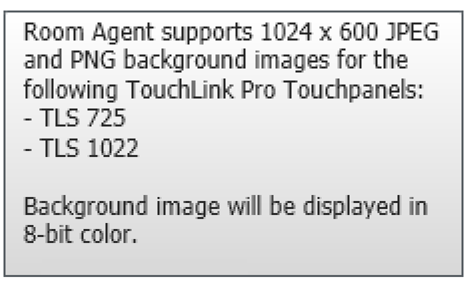


Figure 207. Background Image Information for 1024x600 TLS Panels

Group C (TLS 520, TLS 525, TLP Pro 520, and TLP Pro 720)

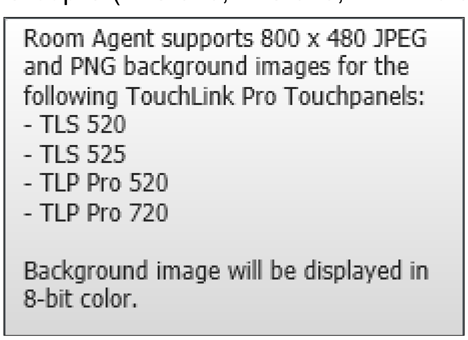


Figure 208. Background Image Information for 800x480 TLS Panels

3. Set the overlay opacity with the **`Overlay Opacity`** slider or text box (see **figure 205** on page 127).

> **NOTE:** Take great care in selecting and configuring the background image. Using an unsuitable image can make the text placed over the image difficult to read. For a complete guide to configuring the background image, see *Extron Room Agent Background Images Hints and Tips*, which is available at **www.extron.com**. Some of the key points are listed here:
>
> - Images must be correct resolution for the touchpanel being configured.
> - Images must be in JPEG, JPG, PNG, or SVG format, with 8 bit colors.
> - Avoid using images that have vertical or horizontal lines.
> - Avoid using images that have a great variety of colors.
> - Avoid using images that have areas of sharp contrast between light and dark
> - Extron recommends setting the overlay opacity higher than 70% (to make the image lighter, if theme color was set to **`Light`**, or darker, if theme color was set to **`Dark`**).

Date & Time Tab

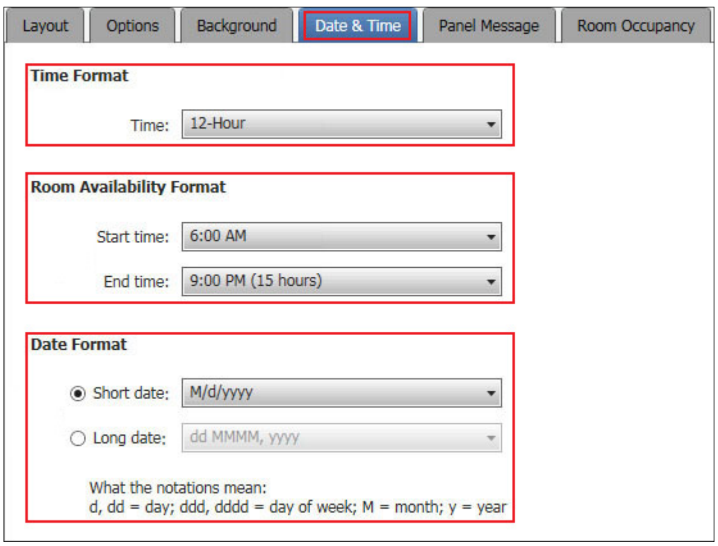


Figure 209. TLS Panels — Date & Time Tab

The `Date & Time` tab (see figure 209) allows you to configure the date and time displayed in the TLS panels.

1. Select the `Time format`. The options are **`12-Hour`**, **`24-Hour US`**, or **`24-Hour International`**.
2. Select the `Room Availability Format` from the **`Start time`** and **`End time`** drop-down lists.
3. Select either the **`Short date`** or **`Long date`** radio button and then select an option from the drop-down lists.

> **NOTE:** The abbreviations used below have the following meanings:
>
> - *d* is a single or double digit representation of the day of the month: 1, 2, 3... 31
> - *dd* is a double digit representation of the day of the month: 01, 02, 03... 31
> - *dddd* is the day of the week: Sunday, Monday, Tuesday... Saturday
> - *M* is a single or double digit representation of the month: 1, 2, 3... 12
> - *MM* is a double digit representation of the month: 01, 02, 03... 12
> - *MMM* is a three-character abbreviation for the month: Jan, Feb, Mar... Dec
> - *MMMM* is the complete name of the month: January, February, March... December
> - *yy* abbreviates the year to two digits: 2015 is shown as 15
> - *yyyy* shows the year in four digits: 2015 is shown as 2015

The options are shown below along with how they display Friday, January 02, 2015:

Short Date Format	Long Date Format
• `M/d/yyyy (1/2/2015)` • `M/d/yy (1/2/15)` • `MM/dd/yy (01/02/15)` • `MM/dd/yyyy (01/02/2015)` • `yy/MM/dd (15/01/02)` • `yyyy-MM-dd (2015-01-02)` • `dd-MMM-yy (02-Jan-15)`	• `dddd, MMMM dd, yyyy (Friday, January 02, 2015)` • `MMMM dd, yyyy (January 02, 2015)` • `dddd, dd MMMM, yyyy (Friday, 02 January, 2015)` • `dd MMMM, yyyy (02 January, 2015)`

Panel Message Tab

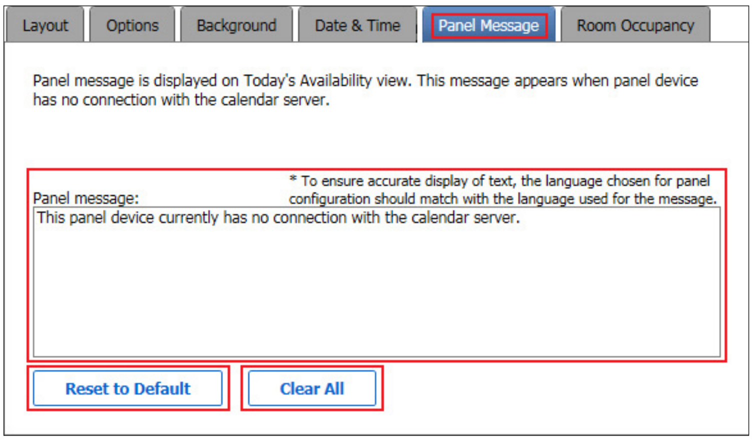


Figure 210. TLS Panels — Panel Message Tab

By default, if the panel is not connected to a calendar server, the `Today’s Availability` screen displays a message stating `This panel device currently has no connection with the calendar server`.

The `Panel Message` tab (see figure 210) allows the user to edit the message and view the change in the `Preview` panel.

You can also return to the default message by pressing **`Reset to Default`**, or remove the message by pressing **`Clear All`**.

Room Occupancy Tab

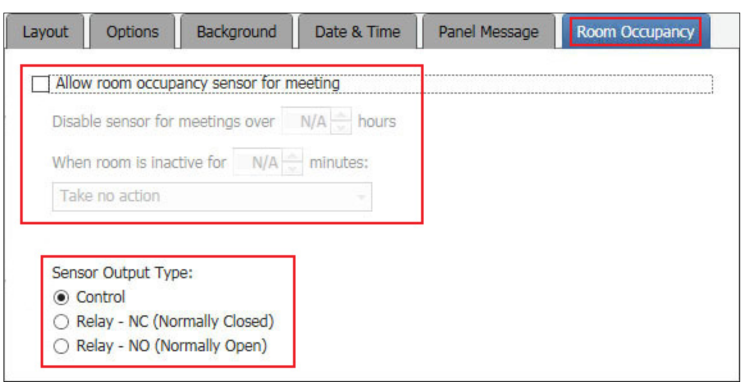


Figure 211. TLS Panels — Room Occupancy Tab

Use the `Room Occupancy` tab (see **figure 211** on page 130) to:

- **`Allow room occupancy sensor for meeting`** — If this option is selected, other options become available:

  You can disable the sensor for meetings lasting longer than a user-defined period.

  When the room is inactive for a user-defined period, you can select Take no action or Release room.

- **`Choose a Sensor Output Type`** —

NOTE: At present, this feature works only with the TLS 520M series, TLS 525M series, TLS 725M series, and TLS 1025M series TLS panels as other TLS panels do not have the digital I/O connectors needed to connect the OCS 100 Occupancy Sensors.

To wire the occupancy sensor, see figure 212 and select the corresponding radio button in the **`Room Occupancy`** tab.

NOTE: The diagrams below show only the configuration of the control connections. They do not show power to the sensors or the touchpanels.

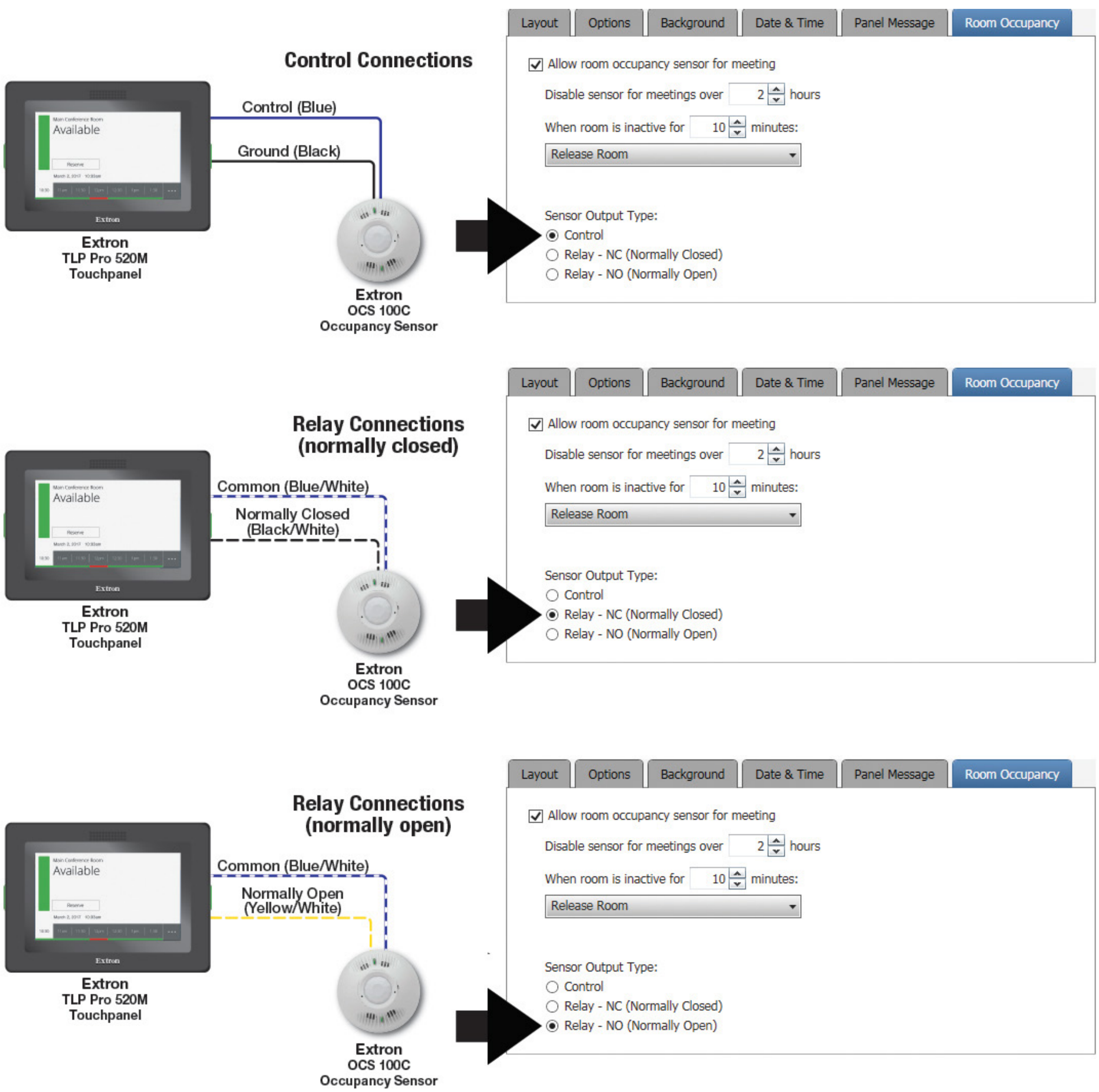


Figure 212. Connecting Room Sensor to TLS Panel

NOTE: Wire colors may be different, depending on the occupancy sensor model.

Preview Panel

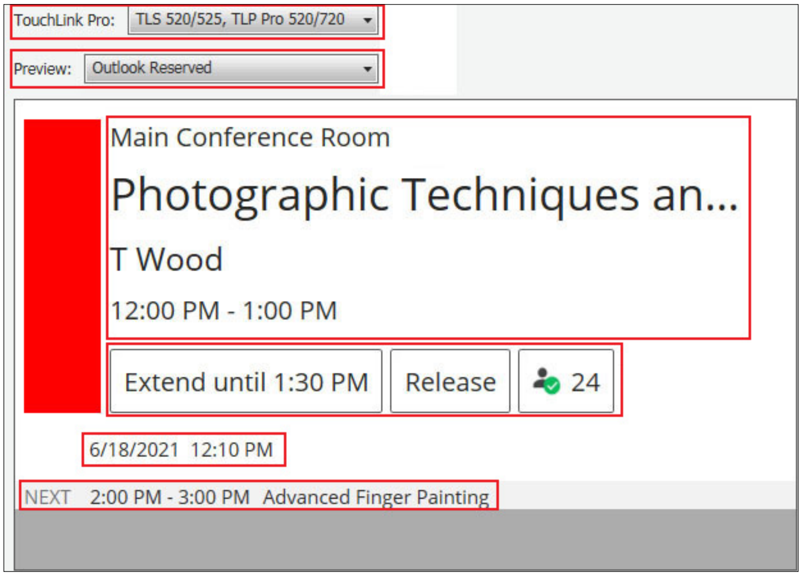


Figure 213. TLS Panels — Preview Panel

The `Preview` panel allows you to preview how the user screens appear after configuration.

> **NOTE:** The preview pane contains hardcoded, sample, entries. The layout and appearance of this pane change to reflect changes in the design pane, but, other than the date and time, the contents, such as `Main Conference Room`, do not change.

Select the touchpanel model from the **`TouchLink Pro`** drop-down list (see figure 213), to preview at the correct resolution.

Use the **`Preview`** drop-down list to select which of the seven user screens to preview. The choices are:

- **`Available`**
- **`Outlook Reserved`**
- **`Confirm Release`**
- **`Future Reservation`**
- **`Future Availability`**
- **`Today’s Availability (No Connection)`**
- **`Walk Up Reserved`**

The `Preview` screen shows the information selected in the **Layout Tab** (see page 123), **Options Tab** (see page 124), **Date & Time Tab** (see page 129), and a preview of the next meeting.

NOTES:

- If **`Anytime`** or **`Current`** is selected in the **`Layout`** tab (see **figure 197** on page 123), the `Walk Up Reserved` screen is available for preview.
- If **`Never`** is selected in the **`Layout`** tab, the `Walk Up Reserved screen` is not available for preview.
- If the **`Allow room release`** checkbox is not checked, then the `Confirm Release` screen is not available for preview.

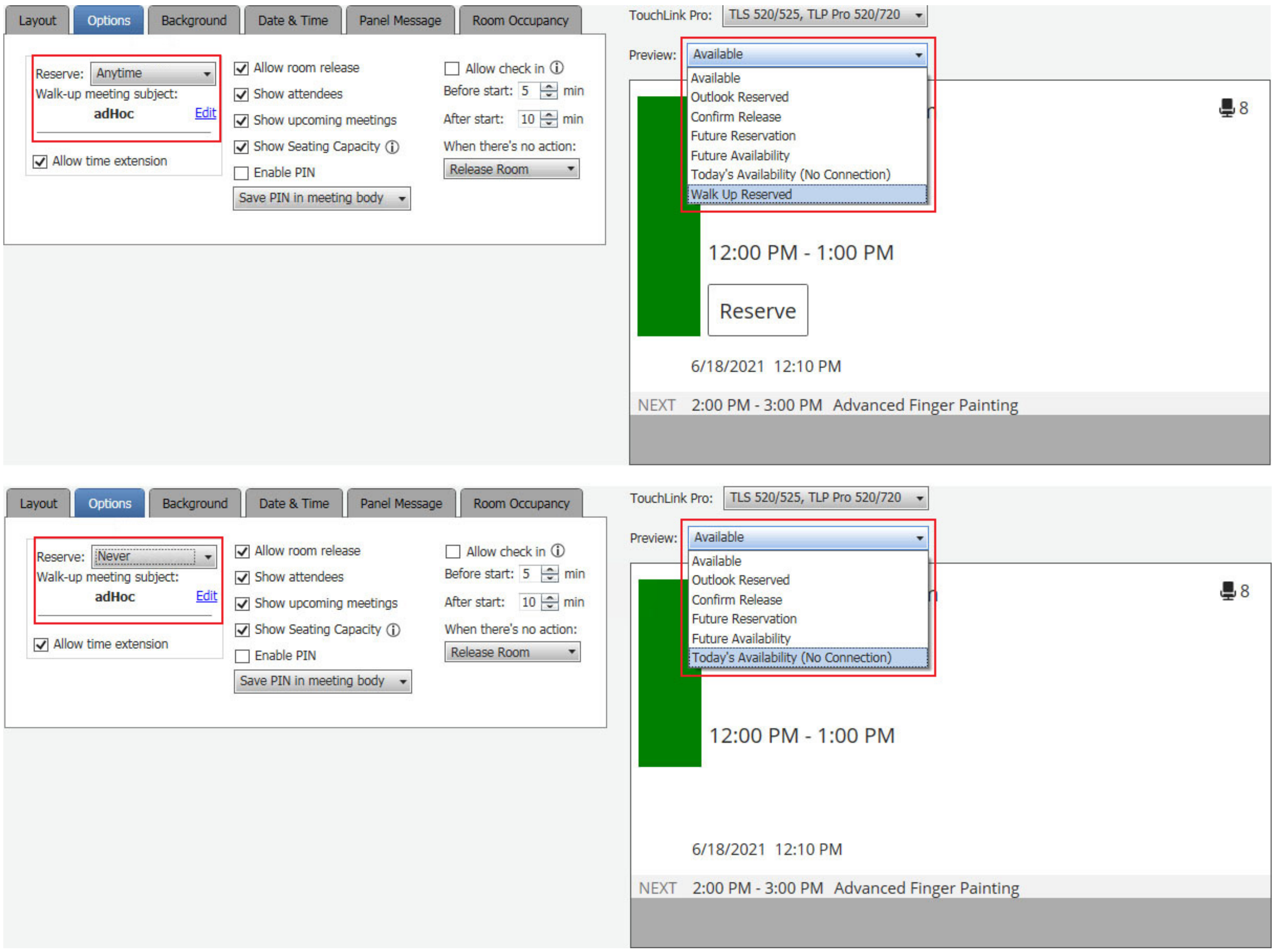


Figure 214. TLS Panels Preview Screen Options — Reserve Anytime or Never

The screens above shows the `Room Available` screen using the configuration options shown in the screen captures of the **Layout Tab**, **Options Tab**, **Background Tab**, and **Date & Time Tab**.

Design Tab for Desk

1. If required, select the **DESIGN** tab (❶).

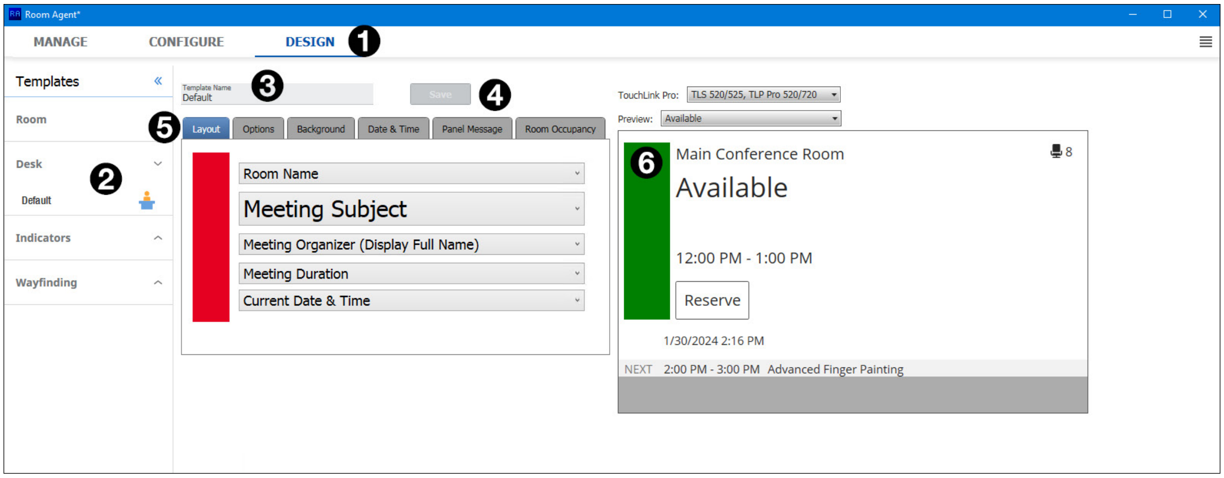


Figure 215. Design Tab for Desk

2. Open the **Desk** drop-down list in the sidebar on the left side of the screen (❷).

   A list of available room templates opens. Initially there is only one template available, called `Default`. As you create and save your own templates, they will be listed in this menu.

3. Select a template from the list.

   The name of the template that you selected appears in the `Panel Template` text box (❸).

4. Save the template:

   - If you make changes to the existing template that you wish to save, click **Save** (❹). The template will be saved with the same name, but incorporating the changes you made.
   - If you make changes to the template that you wish to save as a new template, type the new template name into the `Panel Template` text box and click **Save** (❹). The new template is saved and the original template, without changes, is still available.
   - If you have retrieved a template, the name shown in the text box is grayed out (not selectable). Click **Save** (❹). The name is shown in normal text and is listed in the `Templates` panel on the left of the screen.

5. Use the controls in any of the following `DESIGN` tabs (❺) to configure the GUI appearance:

   - **Layout Tab**
   - **Options**
   - **Background Tab**
   - **Date & Time Tab**
   - **Panel Message Tab**
   - The **Preview Panel** (❻) allows you to see how the configuration affects the appearance of the different touchpanel screens.

Templates Pane

Templates allow you to create a number of customized panel appearances. Each panel in a system can have its own template, assigned on the `CONFIGURE` tab. Select the templates on the `Templates` pane.

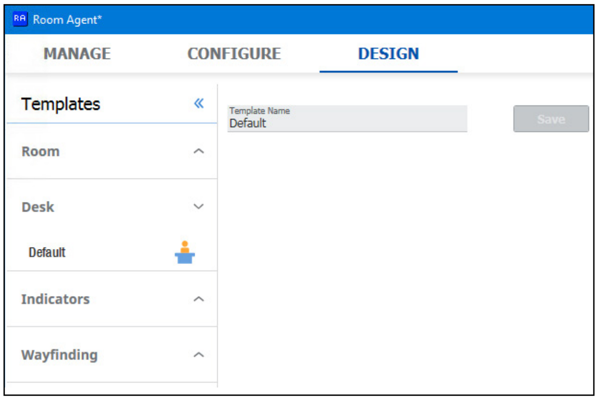


Figure 216. Design Tab Templates for Desk

- To add a new template or rename an existing template:
  1. Type a name in the `Template Name` field.
  2. Click the **`Save`** button.
- To delete a template, move the mouse over the icon next to the template name in the `Template` list. The icon changes to a trash can. Click on the trash can and confirm that you wish to delete the template.
- To assign a saved template to a TLS panel, open the `CONFIGURE` tab and select the TLS panel. Click in the **`DESIGN`** cell for that panel and select a template from the list.

Layout Tab

After you have chosen the `Desk` template, use the **`Layout`** tab (see figure 217, ❶) to assign values to the text boxes. Changes to the template are shown in the `Preview` pane (❺).

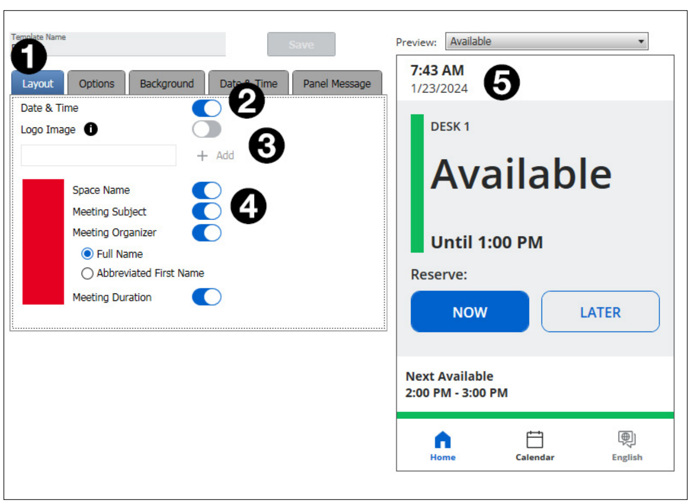


Figure 217. Layout Tab for Desk

NOTE:

- When you select **`Retrieve Template for Design`** in the `Panel Configuration` tab (see **Sending and Retrieving Configurations**), the layout tab opens to show the template that has been retrieved.
- When the tab opens, the name in the `Panel Template` text box (see **figure 217**, 1, on page 135) is unavailable, even if the name is in the `Templates` list in the panel on the left side of the window. Click **`Save`**. If a template of the same name is already available, you are asked if you want to overwrite the existing version with the downloaded version. If the template was not already available, it is added to the list. The name of the template in the `Panel Template` text box is now available.

Use the toggle switches to determine which of the following items appear on the TLS 300 screen.

- **`Date & Time`** (see 2) – This option will display the date and time. Date and time must be set in the `Date & Time` tab.
- **`Logo Image`** (3) – If this option is selected, click **`+ Add`** and navigate to where the logo image is saved. This image is displayed on the screen
- **`Space Name`** (4) – Shows the name of the meeting space.
- **`Meeting Subject`** (4) – Shows the subject of the meeting.
- **`Meeting Organizer`** (4) – Shows the name of the meeting organizer. If this option is selected, you can choose to show the **`Full Name`** or **`Abbreviated First`** Name of the organizer.
- **`Meeting Duration`** (4) – Shows how long the meeting lasts.If no meeting has been booked, the `Meeting Subject` field is set to `Available` and the `Organizer` and `Duration` fields are blank.

Options

1. Select the **`DESIGN`** tab.
2. Select a template from the Desk drop-down list (see figure 218, 1).
3. Select the **`Options`** tab (2)

   There are three main categories within the **`Options`** tab:

   - **`Panel Access`** (3)
   - **`Actions`** (4)
   - **`Calendar API`** (5)

   There is also a preview pane (6)

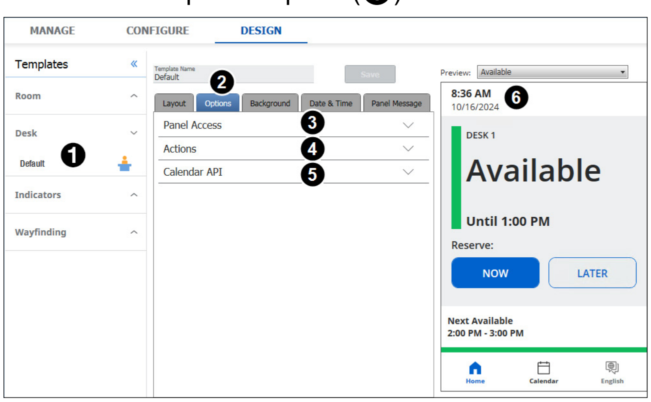


Figure 218. Options Tab for Desks

Panel Access

Open the **`Panel Access`** accordion to enable QR code access.

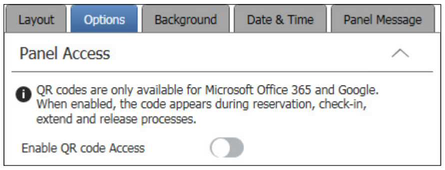


Figure 219. Panel Access for Desks

Enable this switch to use QR code authentication. When this feature is enabled, the TLS requires a user to authenticate via a QR code to perform actions such as reserve, release, extend, and checkin.

When a user approaches the TLS, the only action available on the UI will be authenticate. Once the user presses authenticate, the TLS displays a QR code and one-time passcode. The user scans the QR code with their phone and is taken to a log in page where they enter the one-time passcode and choose the account they want to use. Once a user has authenticated, the normal reserve, release, extend, and checkin actions are available if enabled. After interacting with the TLS the user can press the log out button to lock the panel again. Once a meeting is booked via QR code, only the meeting organizer can edit the meeting.

If QR Code Access is enabled for a Google configuration, anyone in the tenant will be able to book to rooms calendars.

> **NOTE:** This feature is available only on TLS x25 and TLS 300 models and only with Google and Microsoft Office 365 calendars. Microsoft O365 requires additional configuration.

Actions

Open the **`Actions`** accordion (see figure 220) to set options for:

- Reserving rooms (❶)
- Ad hoc meetings (❶)
- Default meeting duration (❷)
- Calendar API (❹)
- Extend a meeting (❸)
- Release the meeting space (❸)
- Enable **`Check In`** (❹)

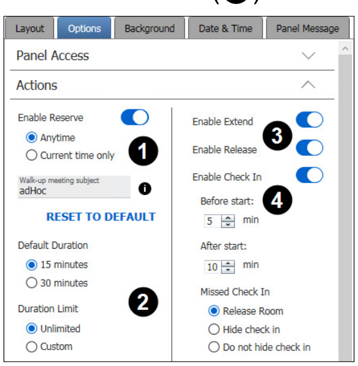


Figure 220. Actions for Desks

1. Use the **`Enable Reserve`** toggle switch (❶) to configure how the user can make reservations:
   - **`Anytime`** – Any visible time slot that is open can be reserved by the walk-up user.

     > **NOTE:** Meeting notices cannot be sent for meetings booked by a walk-up user.

   - **`Current time only`** – Only the currently available time slot can be reserved by the walk-up user.

2. For an ad hoc meeting, enter the meeting subject in the `Walk-up meeting subject` text box. Click the information button next to the text box for additional information.

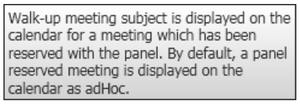


Figure 221. Ad hoc Meeting Information Pop-up

3. Set the default meeting duration (see figure 220, ❷, on page 137) to either **`15 minutes`** or **`30 minutes`**. You can also set the meeting duration to **`unlimited`** (by repeatedly clicking **`Extend`**, the meeting can last all day or until another meeting is scheduled) or create a custom meeting duration.
4. Select **`Enable Extend`** (❹) to allow the room reservation to be extended if the meeting goes beyond its scheduled time and the room is free. If this switch is on, the **`Extend until`** button appears on the panel. **`Extend until`** extends the reservation of a room in half-hour increments if the room is free. The **`Extend until`** button does not appear if there is a conflict.
5. Several other options can be activated by selecting the appropriate toggle switch (❹). Select **`Enable Release`** to allow the user to release the room if the meeting is canceled or finishes early.
6. Select the **`Enable Check In`** option (❹) to allow meetings that have been booked in advance to be confirmed and to release the room if nobody confirms within a certain time before or after the scheduled meeting start.

   If this option is selected, a **`Check in`** button appears on the panel for a scheduled meeting. The button disappears from a panel once it is pressed.

   There are also three options for how Room Agent behaves if the **`Check in`** button is not pressed in time:

   - **`Release the room`** — the meeting is canceled
   - **`Hide Check in`** button — the meeting continues. No check in is available.
   - **`Keep Check in`** button — the meeting continues. Users can still check in.

Calendar API

Click to open the Calendar API accordion (see figure 218, ❺, on page 136) for additional information:

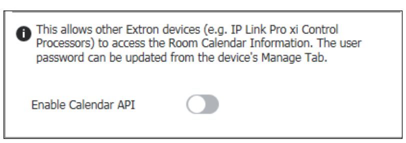


Figure 222. Calendar API Options for Desk

Select **`Enable Calendar API`** to allow other Extron devices to access the Room Calendar information.

NOTE: This feature may require a firmware update. Please talk to your Extron Representative.

Background Tab

The `Background` tab allows you to configure the background of the touchpanel GUI.

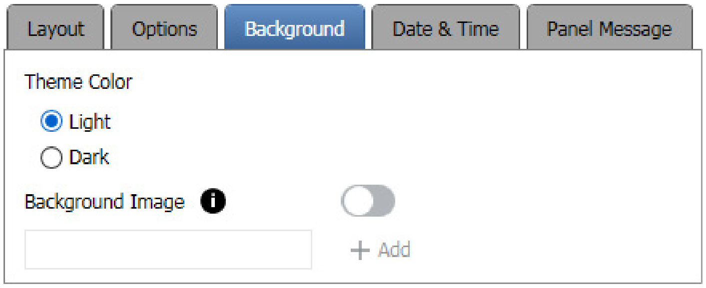


Figure 223. Background Tab for Desk

1. Select the theme color from the `Theme Color` radio buttons. The options are:
   - **`Light`**
     - Buttons are white.
     - Fonts are black.
     - Background is white.
     - When the background image is loaded, the opacity overlay is white.
   - **`Dark`**
     - Buttons are dark gray with a white border.
     - Fonts are white.
     - Background is dark gray.
     - When the background image is loaded, the opacity overlay is dark gray.
2. Select the **+ `Add`** to add a background image, or remove the image if one has been previously selected.
3. Click on the information symbol to open a popup box with information about the images that can be used.

Figure 224. Background Pop-up for Desk

> **NOTES:** Take great care in selecting and configuring the background image. Using an unsuitable image can make the text placed over the image difficult to read. For a complete guide to configuring the background image, see *Extron Room Agent Background Images Hints and Tips*, which is available at **www.extron.com**. Some of the key points are listed here:
>
> - Images must be correct resolution for the TLS 300.
> - Images must be in JPEG or PNG with 8 bit colors.
> - Avoid using images that have vertical or horizontal lines.Avoid using images that have a great variety of colors.
> - Avoid using images that have areas of sharp contrast between light and dark.
> - Extron recommends setting the overlay opacity higher than 70% (to make the image lighter, if theme color was set to **`Light`**, or darker, if theme color was set to **`Dark`**).

Date & Time Tab

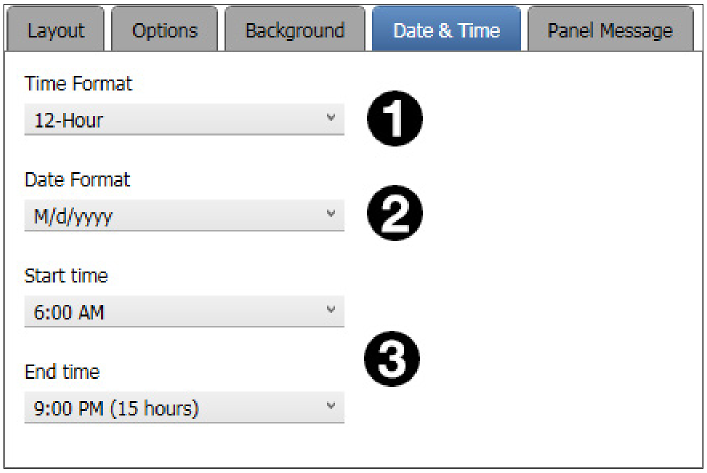


Figure 225. Date & Time Tab for Desk

1. The `Date & Time` tab allows you to configure the date and time displayed in the TLS 300 panels. Select the **`Time format`** (see figure 225, ❶). The options are
   - **`12-Hour`**
   - **`24-Hour US`**
   - **`24-Hour International`**.
2. Select the **`Date Format`** from the drop-down menu (❷).

   NOTES: The abbreviations used below have the following meanings:
   - *d* is a single or double digit representation of the day of the month: 1, 2, 3... 31
   - *dd* is a double digit representation of the day of the month: 01, 02, 03... 31
   - *M* is a single or double digit representation of the month: 1, 2, 3... 12
   - *MM* is a double digit representation of the month: 01, 02, 03... 12
   - *MMM* is a three-character abbreviation for the month: Jan, Feb, Mar... Dec
   - *yy* abbreviates the year to two digits: 2015 is shown as 15
   - *yyyy* shows the year in four digits: 2015 is shown as 2015

   The available options are shown below along with how they display Friday, January 02, 2015:
   - *M/d/yyyy* (1/2/2015)
   - *M/d/yy* (1/2/15)
   - *MM/dd/yy* (01/02/15)
   - *MM/dd/yyyy* (01/02/2015)
   - *yy/MM/dd* (15/01/02)
   - *yyyy-MM-dd* (2015-01-02)
   - *dd-MMM-yy* (02-Jan-15)
3. Select the **`Room Availability`** format from the `Start time` and `End time` drop-down lists (❸).

Panel Message Tab

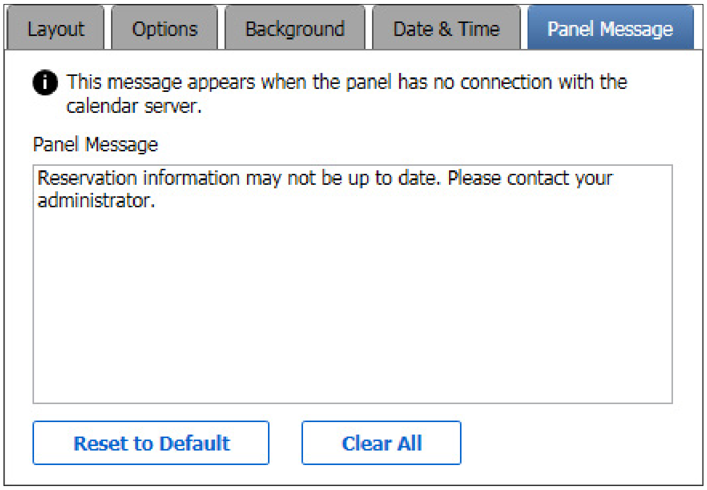


Figure 226. Panel Message Tab for Desk

By default, if the panel is not connected to a calendar server, the `Today's Availability (No Connection)` screen displays a message stating `Reservation information may not be up to date. Please contact your administrator`. The **`Panel Message`** tab allows the user to edit the message.

You can also return to the default message by pressing **`Reset to Default`**, or remove the message by pressing **`Clear All`**.

Preview Panel

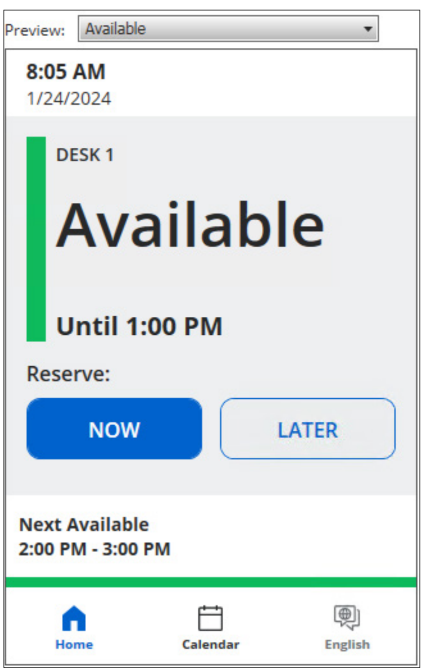


Figure 227. Preview Panel for Desk Showing Room Available

The `Preview` panel allows you to preview how the user screen appears after configuration with the **`Layout`**, **`Options`**, **`Background`**, and **`Date & Time`** tabs.

NOTE: The preview pane contains hardcoded, sample, entries. The layout and appearance of this pane change to reflect changes in the design pane, but, other than the date and time, the contents, such as "`DESK 1`", do not change.

Use the `Preview` drop-down list to select which of the seven user screens to preview. The choices are:

- **`Available`** – Shows the current status of the meeting space if it is available. It allows the user to reserve that space for an ad hoc meeting. The reserve option is available only if it has been activated in the **Options** tab (see page 136).

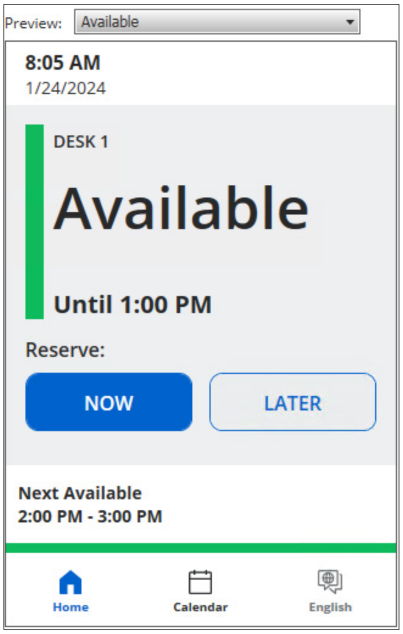


Figure 228. Preview Panel for Desk Showing Room Available

- **`Outlook Reserved`** – Shows the current status of the meeting space if it has been reserved. The meeting can be extended if the meeting space is still available, or released if the meeting ends early. **`EXTEND`** and **`RELEASE`** are available only if they have been selected in the **Options** tab.

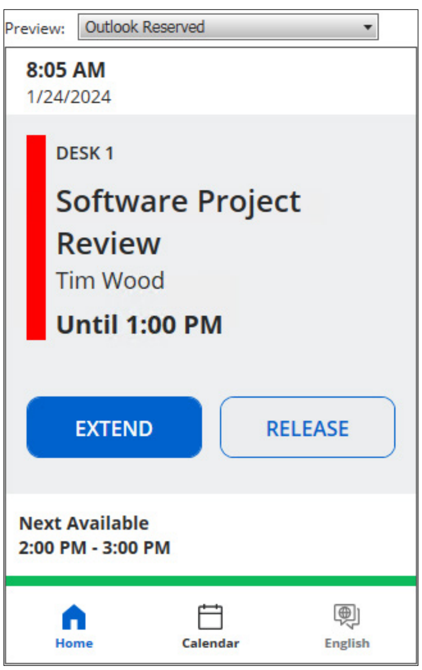


Figure 229. Preview Panel for Desk Showing Outlook Reserved

- **`Future Reservation`** – Shows the status of the meeting space for an upcoming meeting that has been reserved. It allows the user to **`CHECK IN`** or **`RELEASE`** the meeting space. These options are available only if they have been activated in the **Options** tab (see page 136).

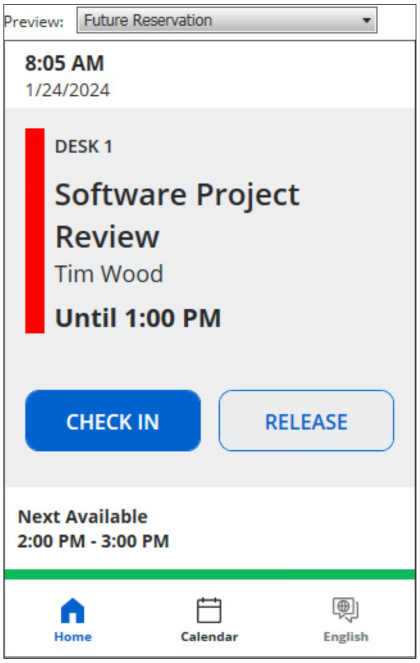


Figure 230. Preview Panel for Desk Showing Future Reservation

- **`Future Availability`** – Shows the future availability of the meeting space and allow the user to reserve the space **`NOW`** or at a **`LATER`** time. The reserve options are available only if they have been activated in the **Options** tab.

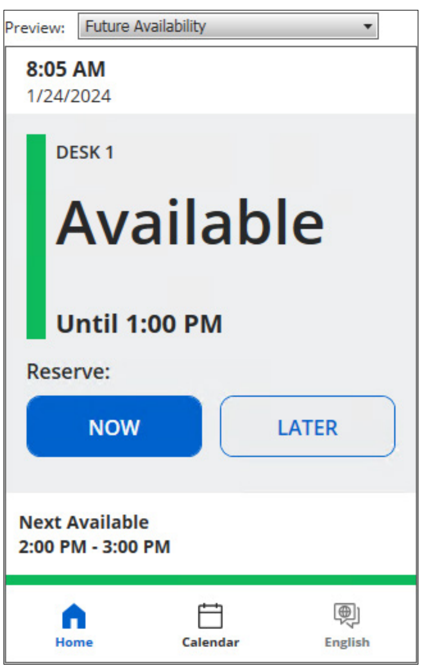


Figure 231. Preview Panel for Desk Showing Future Availability

- **`Today’s Availability (No Connection)`** – Displays a message if the touchpanel is disconnected from the calendar server. The image below shows the default message. The message that is displayed can be edited in the **Panel Message Tab** (see page 141).

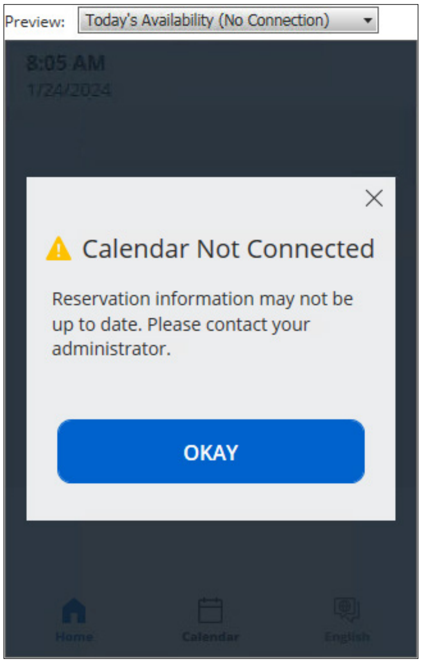


Figure 232. Preview Panel for Desk Showing Today’s Availability (No Connection)

- **`Confirm Release`** – When a meeting finishes earlier, the meeting space can be made available for other meetings by clicking the **`RELEASE`** button (see **Outlook Reserved** on page 142 or **Future Reservation** on page 143). When this button is pressed, another screen, requesting the user to **`CONFIRM`** (or **`CANCEL`**) the room release. This screen is available only if the reserve option has been activated in the **Options** tab (see page 136).

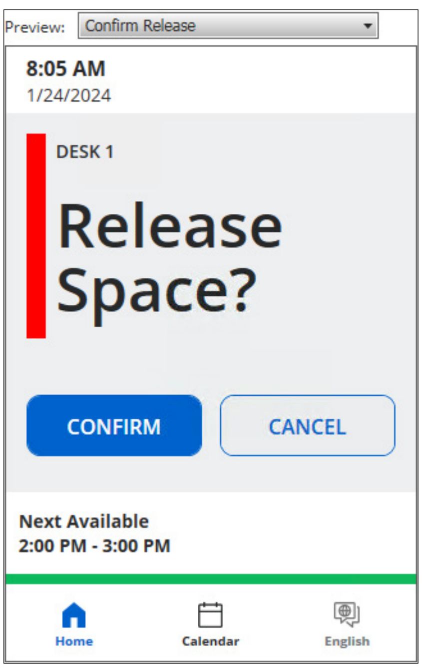


Figure 233. Preview Panel for Desk Showing Confirm Release

- **`Walk Up Reserved`** – Shows the current status of the meeting space if it has been reserved. The meeting can be extended if the meeting space is still available, or released if the meeting ends early. **`EXTEND`** and **`RELEASE`** are available only if they have been selected in the **Options** tab (see page 136).

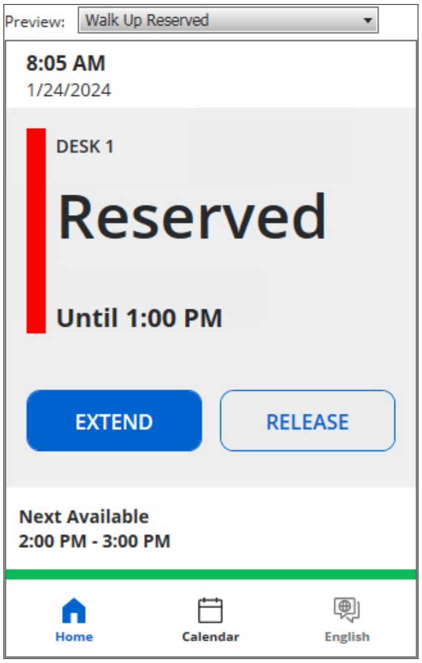


Figure 234. Preview Panel for Desk Showing Walk Up Reserved

Design Tab for Indicators (SSI)

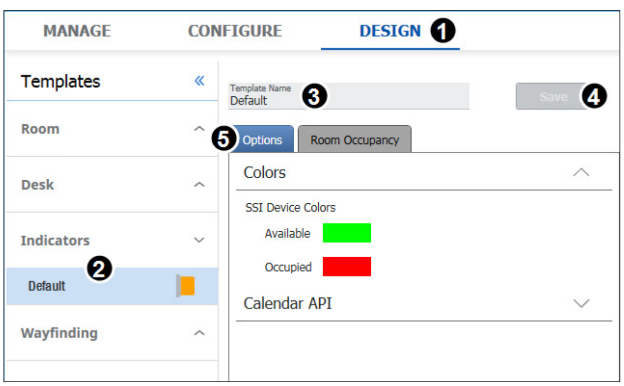


Figure 235. Design Tab for Indicators

1. If required, select the **`DESIGN`** tab (see figure 235, ❶).
2. Open the Indicators drop-down list in the sidebar on the left side of the screen (❷).

   A list of available room templates opens. Initially there is only one template available, called `Default`. As you create and save your own templates, they will be listed in this menu.
3. Select a template from the list.

   The name of the template that you selected appears in the `Panel Template` text box (❸).
4. Save the template:

   - If you make changes to the existing template that you wish to save, click **`Save`** (❹). The template will be saved with the same name, but incorporating the changes you made.

- If you make changes to the template that you wish to save as a new template, type the new template name into the `Panel Template` text box and click **Save**. The new template is saved and the original template, without changes, is still available.
- If you have retrieved a template, the name shown in the text box is grayed out (not selectable). Click **Save**. The name is shown in normal text and is listed in the Templates panel on the left of the screen.

5. The **DESIGN** tab provides two sets of controls (see **figure 235**, ❺, on page 145) to configure the GUI appearance:
   - **Options Tab for Indicators** on page 147
   - **Room Occupancy for Indicators** on page 148

The **DESIGN** tab for Indicators does not have a preview screen.

Templates Pane

Templates allow you to create a number of customized panel appearances. Each panel in a system can have its own template, assigned on the **CONFIGURE** tab. Select the templates on the `Templates` pane.

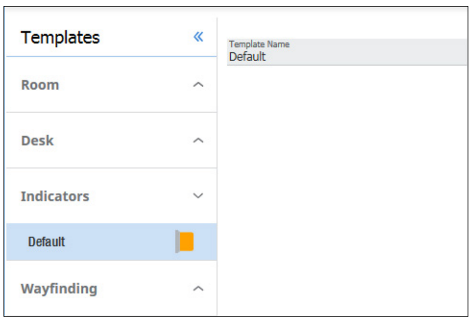


Figure 236. Selecting a Template

- To add a new template or rename an existing template:
  1. Type a name in the `Template Name` field.
  2. Click the **Save** button.
- To delete a template, move the mouse over the icon next to the template name in the Template list. The icon changes to a trash can. Click on the trash can and confirm that you wish to delete the template.
- To assign a saved template to a TLS panel, open the **CONFIGURE** tab and select the TLS panel. Click in the **DESIGN** cell for that panel and select a template from the list.

Options Tab for Indicators

1. Select the **DESIGN** tab (see figure 237, ❶).
2. Select a template from the **Indicators** drop-down list (❷).
3. Select **Options** (❸)

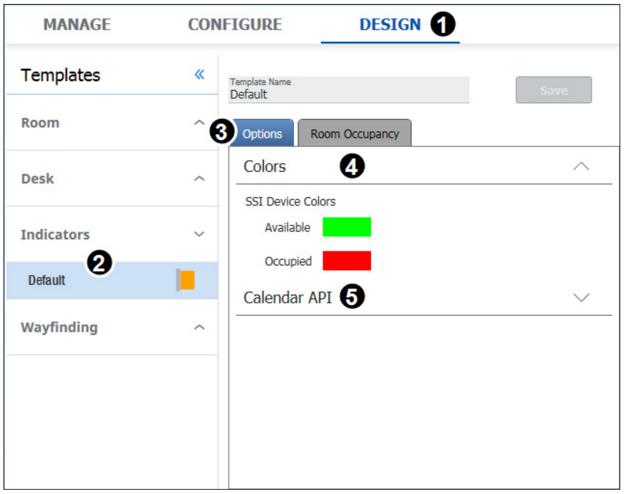


Figure 237. Options Tab for Indicators

Panel Access

The **Options** tab offers two accordion choices:

- Colors (❹)
- Calendar API (❺)

Colors

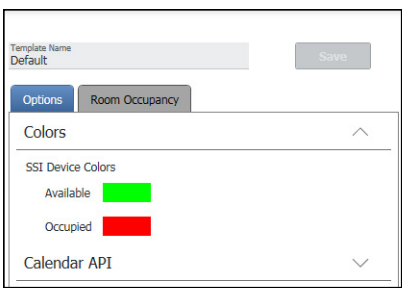


Figure 238. Color Options for Indicators

The SSI device color is green when the room is available and red when the room is occupied. These colors cannot be changed.

Calendar API

Click the **`Calendar API`** accordion for additional information:

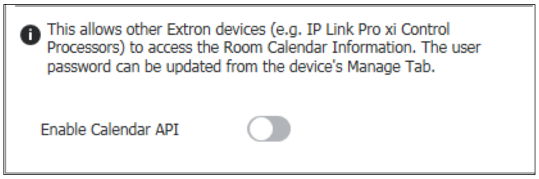


Figure 239. Calendar API Options for Indicators

Select **`Enable Calendar API`** to allow other Extron devices to access the Room Calendar information.

Room Occupancy for Indicators

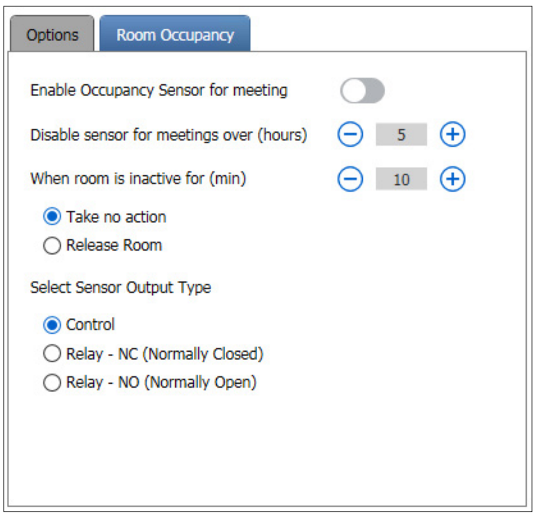


Figure 240. Room Occupancy Tab for Indicators

Use the **`Room Occupancy`** tab to:

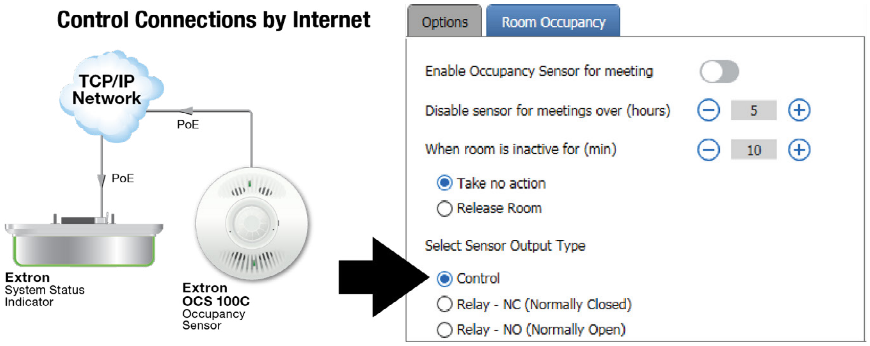
- **`Enable room occupancy sensor`** for meeting. If this option is selected, other options become available:

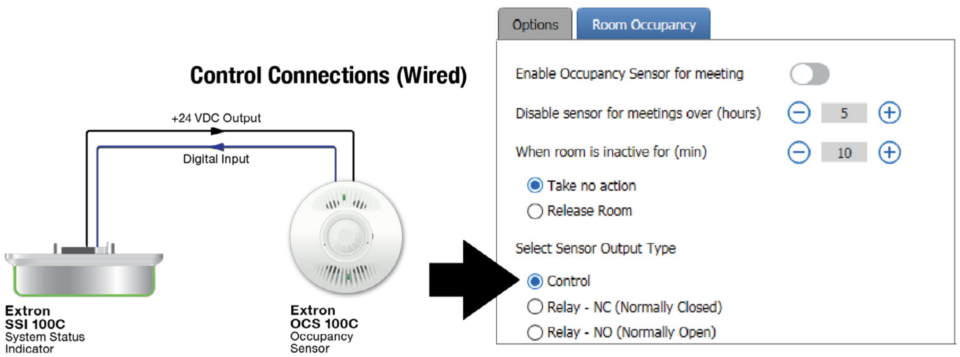
  You can disable the sensor for meetings lasting longer than a user-defined period.

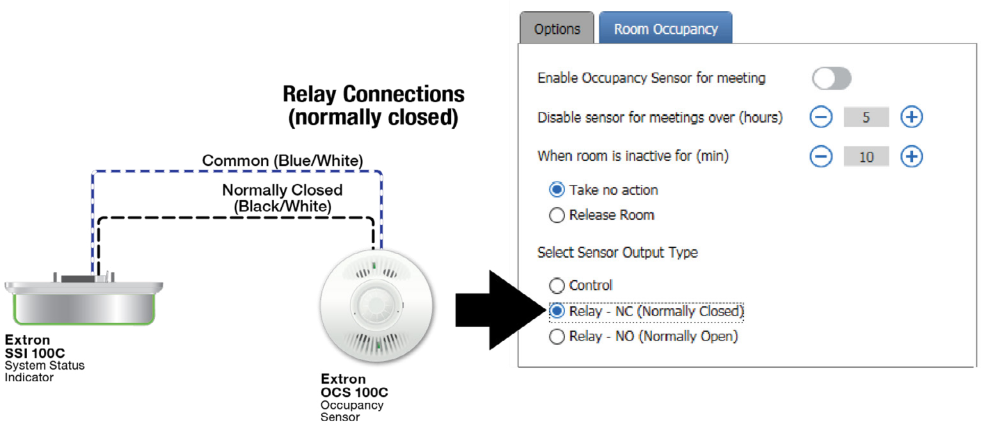
  When the room is inactive for a user-defined period, you can select **`Take no action`** or **`Release Room`**.
- Choose a **`Sensor Output Type`**.

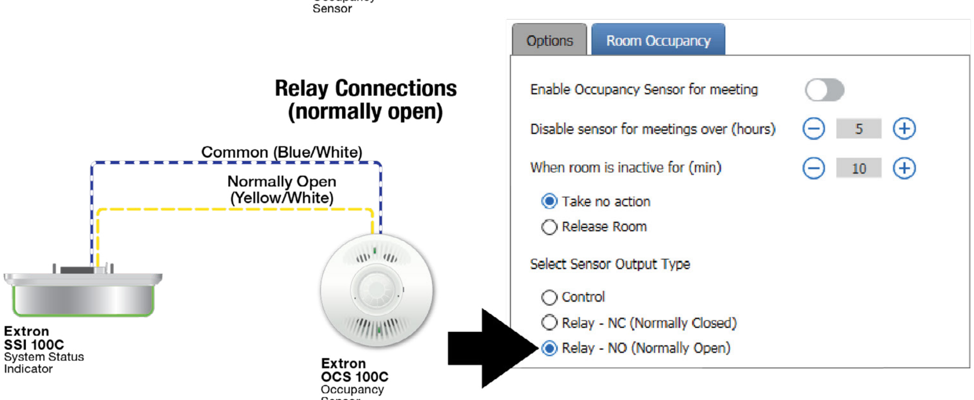
To wire the occupancy sensor, see the diagram below and select the corresponding radio button in the **`Room Occupancy`** tab.

NOTE: The diagrams below show only the configuration of the control connections. They do not show power to the sensors or the touchpanels.









Wire colors may be different, depending on the occupancy sensor model.

Design Tab for Wayfinding (List Format)

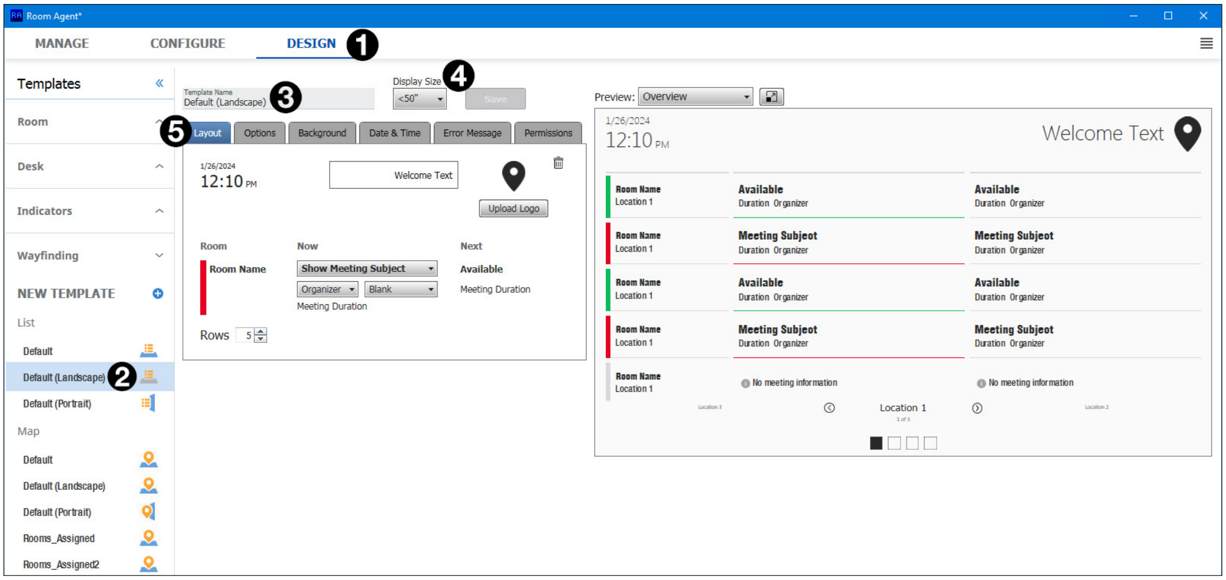


Figure 241. DESIGN Tab — Wayfinding Device (List Format)

1. Open Room Agent and select the **`DESIGN`** tab (see figure 229).
2. Select a template from the **`Templates > Wayfaring`** list.

   There are four default templates for the Wayfinding devices. Information is presented as a list, in portrait or landscape orientation, or as a map (see **Design Tab for Wayfinding (Map)** on page 158), in portrait or landscape orientation. Figure 235 shows the `List Default (Landscape)` template.

   The template opens with the **`Layout`** tab shown..

   If you modify the default template you can save it with the same name to overwrite the default template. Or you can save it with a new name by entering the new name in the `Template Name` textbox and clicking **`Save`**.

   Once it is saved, the new template becomes available in the `Wayfinding > List` templates.
3. Select the **`Display Size`**. The options are **`<50"`**, **`50"-59"`**, and **`>59"`**. This option is available with all the tabs in all the Wayfinding templates.
4. Use the pane on the left of the screen to modify the display. Preview the modifications in the pane on the right of the screen.

   There are six tabs available to modify the appearance of the Wayfinding List:

   - **Layout Tab** on page 151
   - **Options** on page 151
   - **Background** on page 152
   - **Date & Time** on page 152
   - **Error Message** on page 153
   - **Permissions** on page 153

   - There is also a **Preview Pane** (see page 154) to show the effect of the modifications.

Layout Tab

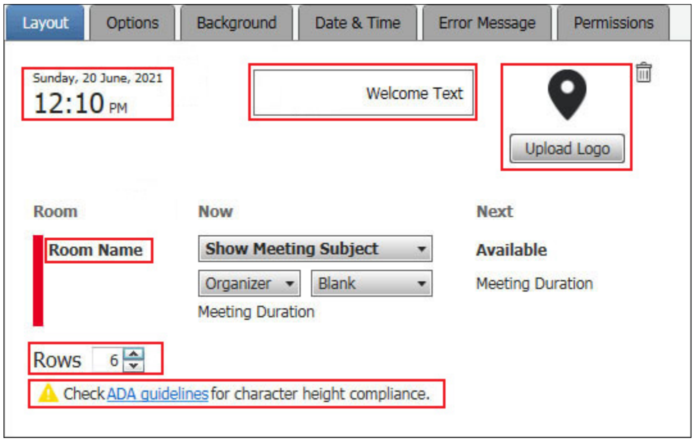


Figure 242. Wayfinding Devices — Layout Tab

1. Click the `Layout` tab.

   The time and date are read only.

2. Enter `Welcome Text`, which is displayed on the Wayfinding Device screen.
3. Click **`Upload Logo`** to place the logo of your organization on the Wayfinding Device screen.
4. Navigate to the folder where your logo is stored and upload it. The logo must be in `.bmp`, `.jpeg`, `.jpg`, `.png`, or `.svg` format. The maximum size is 112 pixels (H) x 258 pixels (W).
5. The `Room Name` is the name of the individual panel that was provided during room configuration.
6. The current status of each room can be configured to show:
   - **`Meeting subject`** — Select **`Show Meeting Subject`** to display the meeting subject retrieved from the individual panel. Select **`Hide Meeting Subject`** to leave the field blank.
   - **`Organizer`** — Select **`Organizer`** to display the meeting organizer retrieved from the individual panel. Select **`Blank`** to leave the field blank.
   - **`Organization`** — Select **`Organization`** to display the organization retrieved from the individual panel. Select **`Blank`** to leave the field blank.
   - The status of the room during 30-minute period immediately after the current session is also shown.
7. Adjust the number of rows displayed on each screen. The default number depends on the screen resolution and whether the screen is in landscape or portrait orientation. If the number of rows exceeds the number recommended by the **Americans with Disabilities Act (ADA)**, a warning message appears, although you are still able to adjust the setting.

Changes in the layout can be seen in the **Preview Pane** (see page 154).

Options

Figure 243. Wayfinding Devices — Options Tab

The **`Options`** tab allows you to toggle between:

- **`Show`** or **`Hide`** room `Seating Capacity`.
- **`Show`** or **`Hide`** a list of `Attendees`.

Background

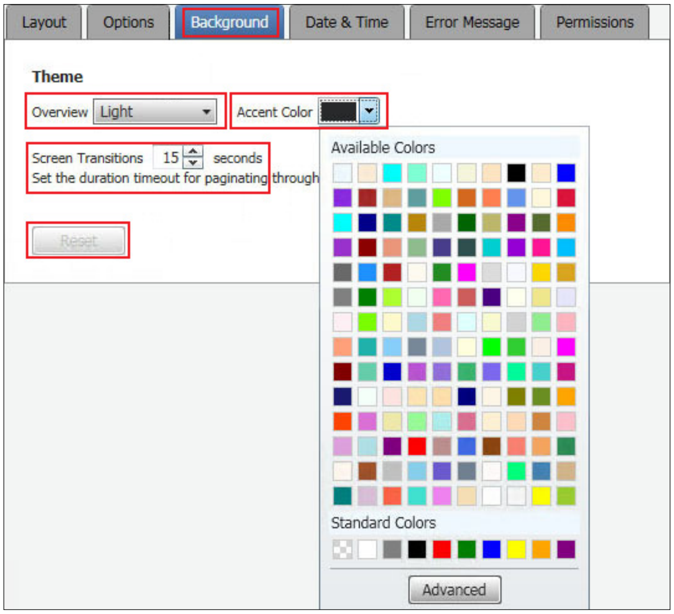


Figure 244. Wayfinding Devices — Background Tab

1. Click **`Background`** (see figure 244).
2. Select the **`Overview`** theme. The choices are **`Light`** or **`Dark`**.
3. Select the **`Accent Color`**.

   You can choose from the **`Available Colors`** or click **`Advanced`** to create your own color.
4. Set the **`Screen Transitions`** time. When multiple pages are displayed as a slide show, this determines how long each screen is displayed.
5. If changes are made, the **`Reset`** button becomes available to restore the settings to the previously saved version.

Changes in the layout can be seen in the **Preview Pane** (see page 154).

Date & Time

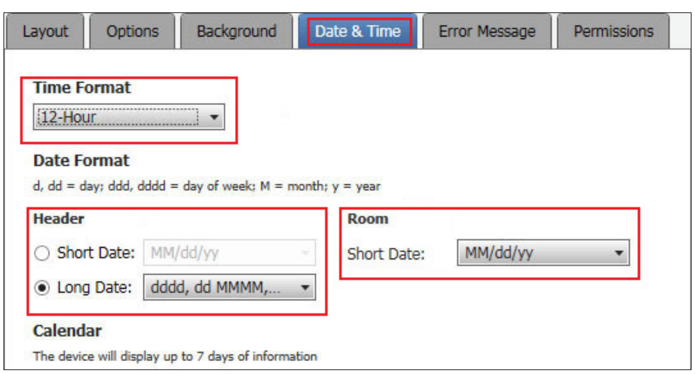


Figure 245. Wayfinding Devices — Date & Time Tab

1. Click **`Date & Time`** tab (see figure 245).
2. Select the **`Time Format`**. The choices are
   - **`12-Hour`**
   - **`24-Hour US`**
   - **`24-Hour International`**

3. Select either the **Short Date** or **Long Date** radio button for the time format used in the Wayfinding Device Header.

   The time format associated with the individual rooms must be in one of the **Short Date** formats (4). The options for each drop-down list are:

Header Short Date	Header Long Date	Room Short Date
M/d/yyyy — 5/20/2020	*dd MMMM, yyyy* — 20 May, 2020	*M/d/yyyy* — 5/20/2020
M/d/yy — 5/20/20	*dddd, dd MMMM, yyyy* — Wednesday, 20 May, 2020	*M/d/yy* — 5/20/20
MM/dd/yy — 05/20/20	*dddd, MMMM dd,* **yyyy** — Wednesday, May 20, 2020	*MM/dd/yy* — 05/20/20
MM/dd/yyyy — 05/20/2020	*MMMM dd, yyyy* — May 20, 2020	*MM/dd/yyyy* — 05/20/2020
yy/MM/dd — 20/05/20		*yy/MM/dd* — 20/05/20
yyyy-MM-dd — 2020-05-20		*yyyy-MM-dd* — 2020-05-20
dd-MMM-yy — 20-May-20		*dd-MMM-yy* — 20-May-20

Changes in the layout can be seen in the **Preview Pane** (see page 154).

Error Message

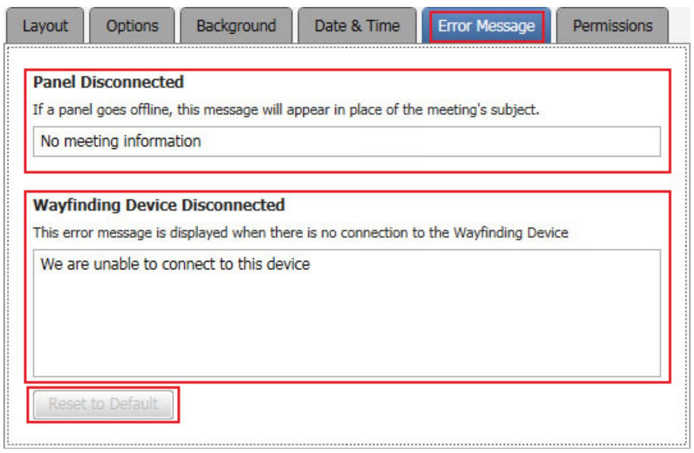


Figure 246. Wayfinding Devices — Error Message Tab

You can customize the messages that are displayed when one of the individual room panels goes offline (`Panel Disconnected` message) or when the Wayfinding Device is disconnected (`Wayfinding Device Disconnected` message).

The default messages are shown in the image above. When you make changes to either message, the **Reset to Default** button becomes available, allowing you to discard any changes you have made.

Changes in the layout can be seen in the preview pane (see below).

Permissions

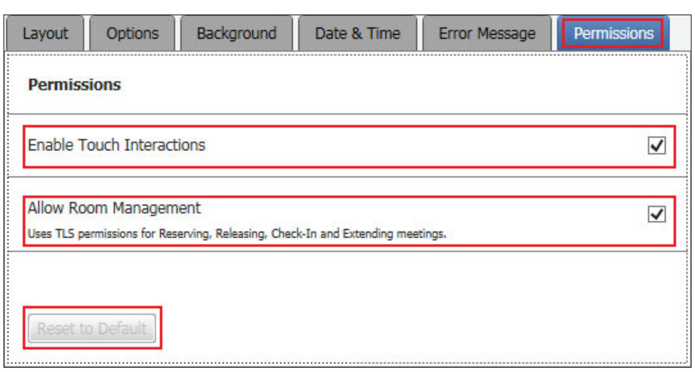


Figure 247. Wayfinding Devices — Permissions Tab

This tab allows you to **`Enable Touch Interactions`** and **`Allow Room Management`**.

By default, both options are enabled.

> **NOTE:** Room management requires to touch interactions to be enabled. If **`Enable Touch Interactions`** is not selected, **`Allow Room Management`** is unavailable for selection.

Preview Pane

The right pane shows previews of various screens that are available. Use the drop-down list to select the preview you wish to view. The options are:

- **Overview** on page 154
- **Available Space** on page 156
- **Reserved Space** on page 156
- **Weekly view** on page 157
- **Device Offline** on page 157

Overview

This view lists all the rooms, in order. If there are too many rooms to be seen on a single screen, you can move between screens by pressing the right and left arrows at the bottom of the screen.

The rooms can be listed in landscape or portrait orientations.

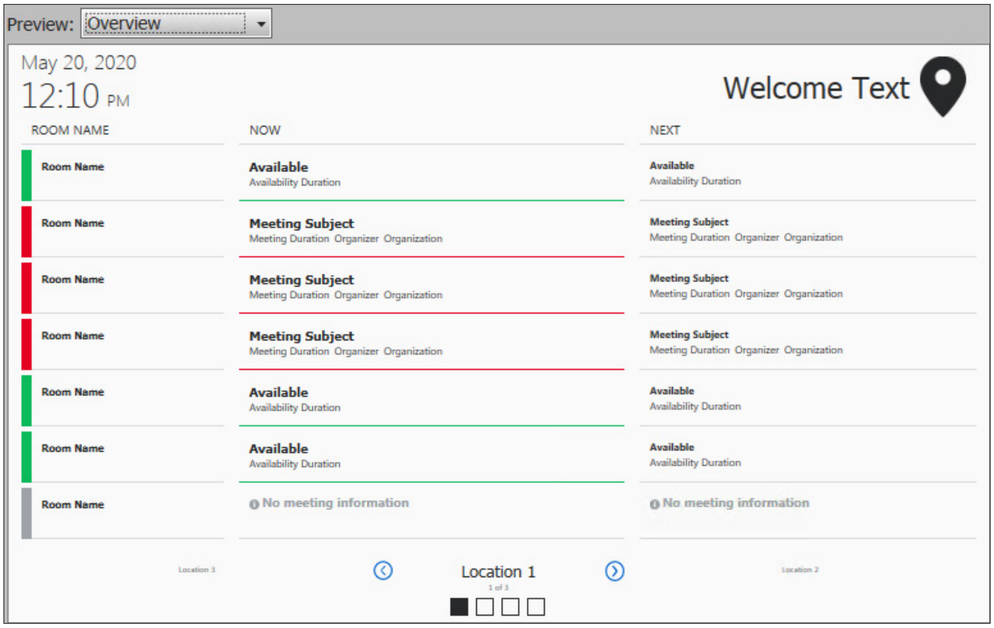


Figure 248. Wayfinding Device List — Landscape View

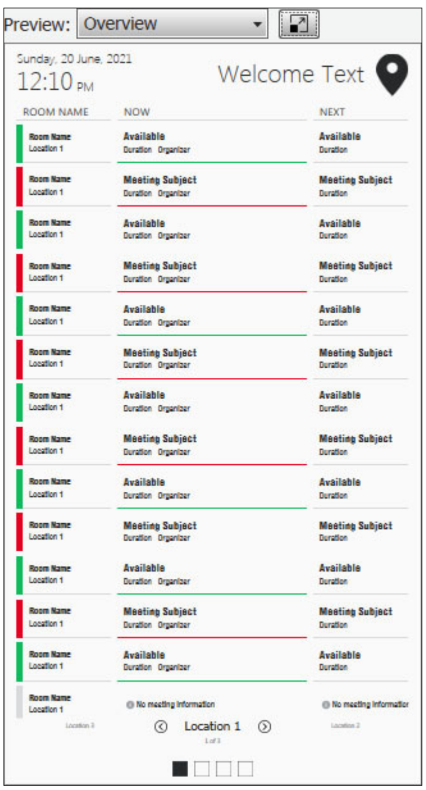


Figure 249. Wayfinding Device List — Portrait View

- A green bar next to the room name and a green line under the meeting name indicate the room is currently available. Information about the next meeting is also shown.
- A red bar next to the room name and a red line under the meeting name indicate the room is currently occupied. Information about the next meeting is also shown.
- A gray bar next to the room name and a `No meeting information` message under the meeting name indicate the room is offline and information is not available.

Available Space

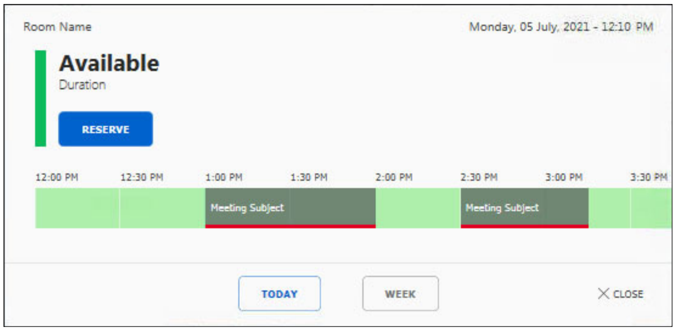


Figure 250. Wayfinding Device List — Available Space

Press one of the available rooms listed in the overview screen.

The time-line for that room shows when it is available (green bar) or occupied (gray bar underlined in red).

The default view shows the meetings for that day for four hours from the current time. To see the room availability for the entire week, press **WEEK**. To return to the default view, press **TODAY**.

To reserve the room, press one of the buttons with a green bar to select a period when the room is free and then press **RESERVE**.

Reserved Space

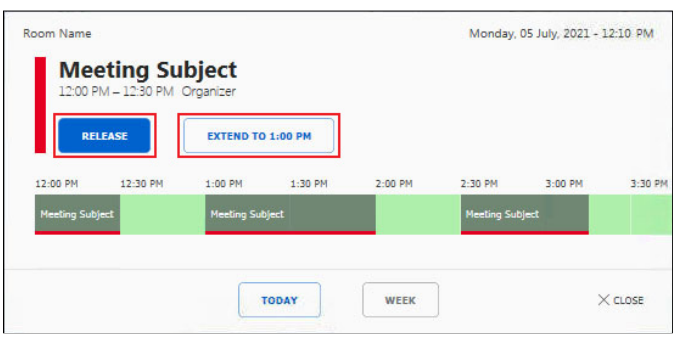


Figure 251. Wayfinding Device List — Reserved Space

In the overview, press a room that has been reserved for the meeting. The time-line shows when the room is available (green bar) or occupied (gray bar underlined in red). The default view shows the meetings for that day for four hours from the current time. To see the room availability for the entire week, press **WEEK**. To return to the default view, press **TODAY**.

If the `Check In` feature has been configured in advance, a **CHECK IN** button is available. Press **CHECK IN**. The room is prepared automatically for the meeting: blinds can be closed, lights can be dimmed, as required, computers and projectors can be turned on.

The meeting shown in the figure above is scheduled to finish at 12:30 pm. If the meeting is running later than expected and the room is available during the next time slot (12:30 to 1:00 pm), press **EXTEND TO 1:00 PM** to reserve the room for an additional 30 minutes.

If the meeting is cancelled or finishes early, press **RELEASE**. This makes the room available for other users.

NOTE: These options require the individual room panels to have the `Allow check in`, `Allow time extension`, and `Allow room release` options selected in the Room **Options Tab** (see page 124).

Weekly view

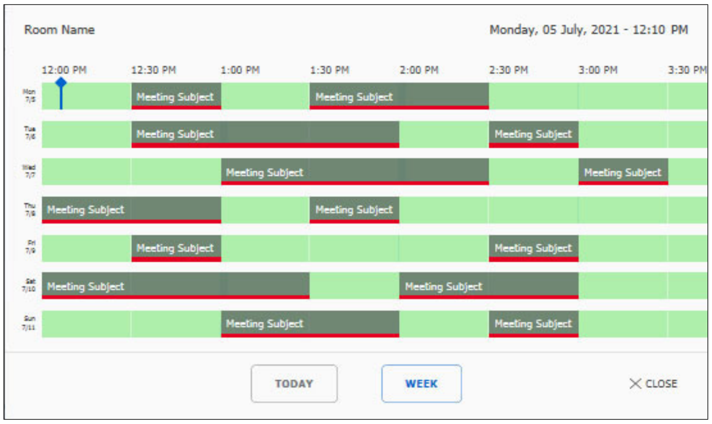


Figure 252. Wayfinding Device List — Weekly View

The `Weekly` view shows room availability, 24 hours each day, for the next seven days, starting with the current day.

Device Offline

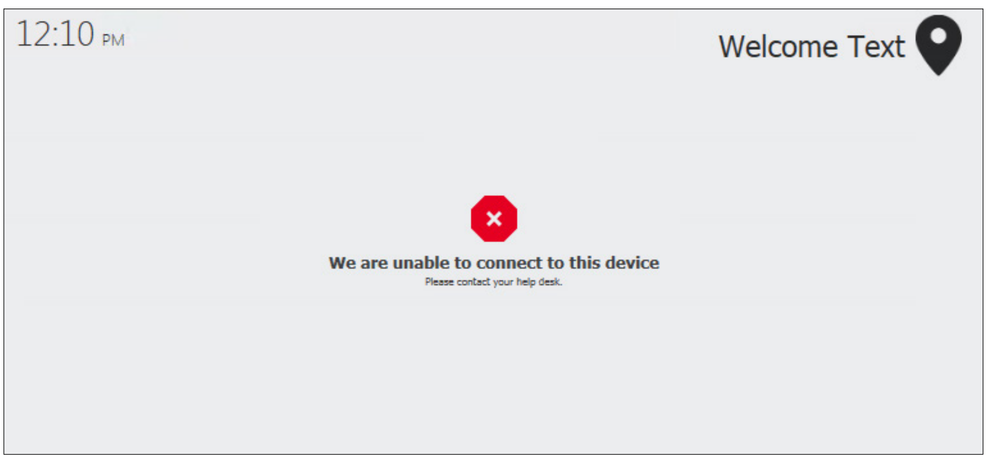


Figure 253. Wayfinding Device List — Device Offline Preview

This message is displayed if the Wayfinding device is offline.

The message above is the default message. It can be changed in the **Error Message** (see page 153).

Design Tab for Wayfinding (Map)

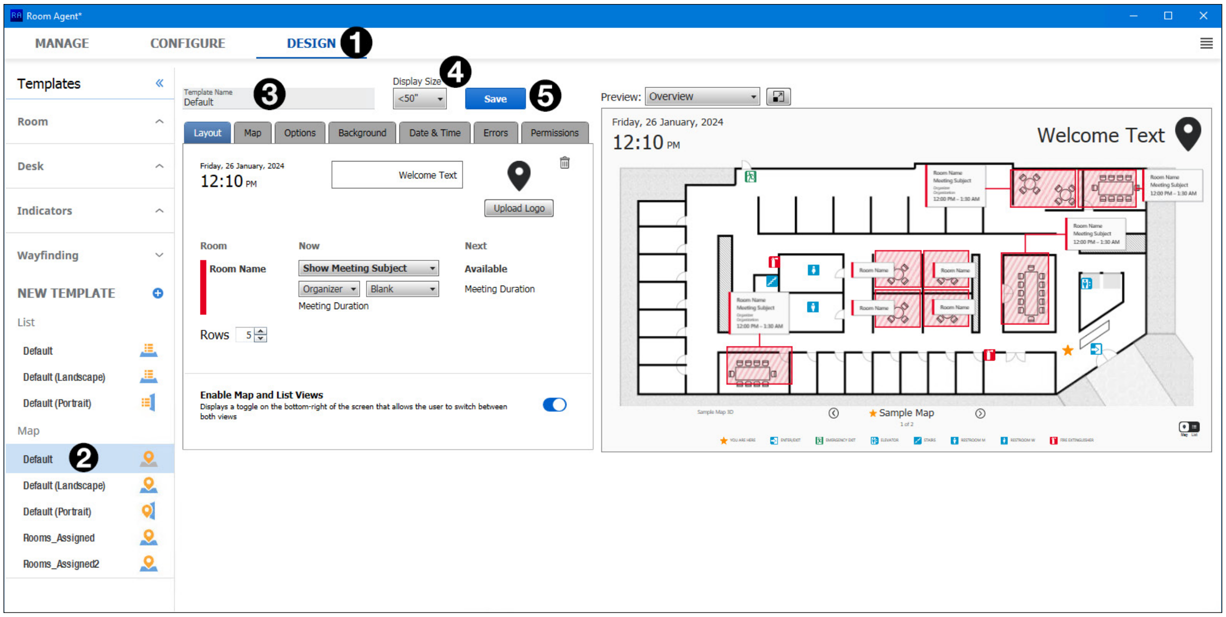


Figure 254. Design Tab — Wayfinding Device (Map Format)

1. Select the **`DESIGN`** tab (see figure 254, ❶).
2. Select one of the **`Wayfinding > Map`** templates (❷). The map can be displayed in landscape or portrait orientation, depending on which template you choose.
3. Select the display size. The options are **`<50"`**, **`50"-59"`**, and **`>59"`** (❹).
4. Use the pane on the left of the screen to modify the display and see a preview of the modifications in the pane on the right of the screen.

   If you modify the default template you can save it with the same name to overwrite the default template (❸). Or you can save it with a new name by entering a new name in the `Template Name` text box and clicking **`Save`** (❺). Once it is saved, the new template becomes available in the `Wayfinding > Map` templates menu.
5. Use the pane on the left of the screen to modify the display. The `DESIGN` tab has seven subsections that are accessed by tabs:
   - **Layout** (see page 159)
   - **Map** (see page 160)
   - **Options** (see page 162)
   - **Background** (see page 163)
   - **Date & Time** (see page 164)
   - **Errors** (see page 165)
   - **Permissions** (see page 165)
   - Any changes to the screens can be previewed in the **Preview Panel** (see page 165) on the right side of the screen.

Layout

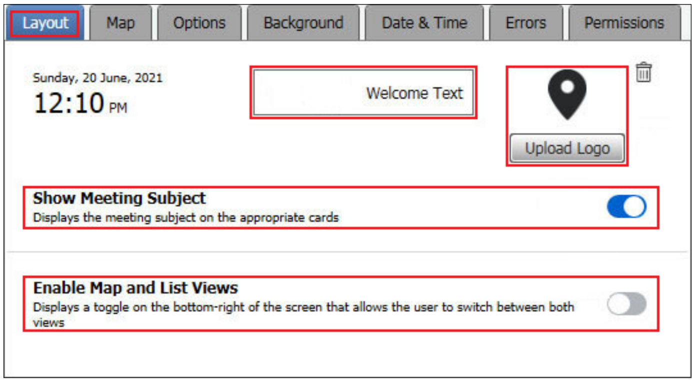


Figure 255. Wayfinding Devices — Layout Tab

1. Click the **`Layout`** tab.

   The date and time are read-only.

2. Enter the `Welcome Text` that is displayed on the Wayfinding Device screen.
3. Click **`Upload Logo`** to place the logo of your organization on the Wayfinding Device screen.
4. Navigate to the folder where your logo is stored and upload it. The logo must be in `.bmp`, `.jpeg`, `.jpg`, `.png`, or `.svg` format. The maximum size is 112 pixels (H) x 258 pixels (W).
5. To display the meeting subject with a room, toggle the **`Show Meeting Subject`** switch to the on position. In the map format, the space available for each room can be quite small and omitting the meeting subject can save space.
6. To enable the Wayfinder display to be toggled between map and list views, set **`Enable Map and List Views`** to the on position.

   When this is set to on, the panel expands, allowing you to provide meeting details for the list view.

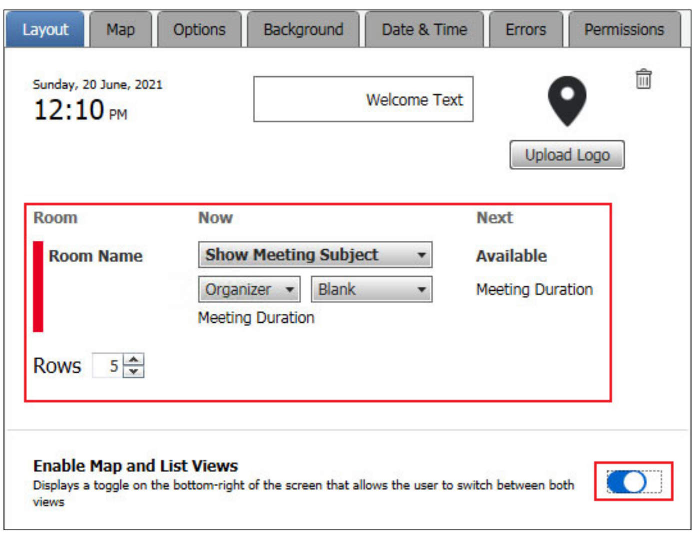
   

   Figure 256. Wayfinding Devices — Layout Tab expanded

   When **`Enable Map and List Views`** is set to **on**, a toggle switch is shown in the bottom right corner of the map and list views, allowing the viewer to toggle between the two views.

7. Adjust the number of rows displayed on each screen. The default number depends on the screen resolution and whether the screen is in landscape or portrait orientation. If the number of rows exceeds the number recommended by the **Americans with Disabilities Act (ADA)**, a warning message appears, although you are still able to adjust the setting.

Changes in the layout can be seen in the **Preview Panel** (see page 165).

Map

Room Agent provides two sample maps that you can practice on.

There is a standard `2D view`:

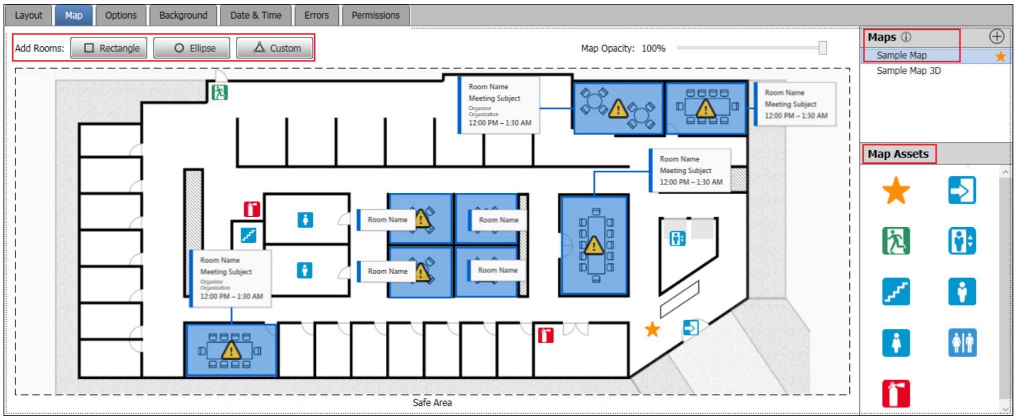


Figure 257. Default Map — 2D

There is also a `3D view`:

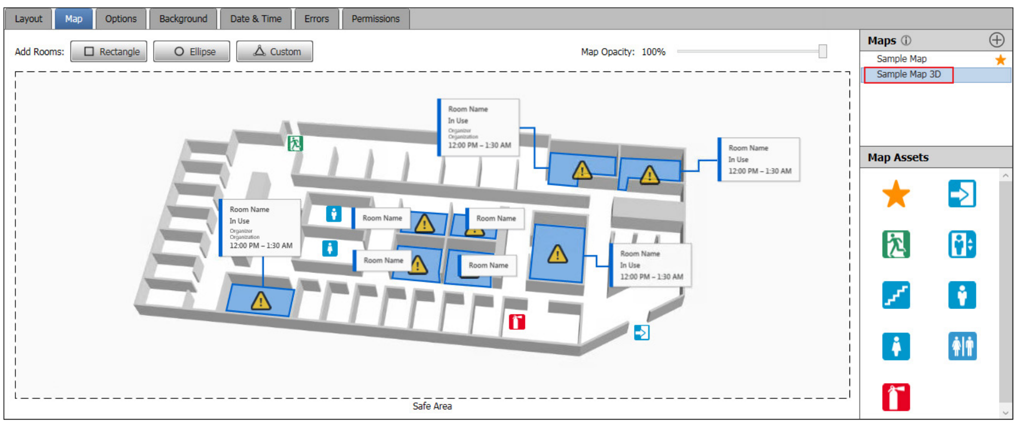


Figure 258. Default Map — 3D

1. To upload your own map, click the **+** symbol in the top right corner of the `Maps` panel.

   The `Add New Map` dialog box opens:

Figure 259. Add New Map Dialog Box

2. Click **`Select File`** and browse to the location where the map is stored. The map must be `.jpeg`, `.png`, `.bmp`, or `.svg` format.
3. Enter a `Map Title`.

4. If required, select the **Hide Map** check box. This can be used if your map is still a work in progress and not ready to be displayed on the screen.
5. Click **Add** to make the map available to Room Agent. The map is now added to the list of available maps.

> **NOTE:** When you select **Hide Map**, and then **Add**, the map is available for you to work on but is not shown until the **Hide Map** check box is no longer selected.

Add rooms to the map

1. Select a shape from the Add rooms choices (see **figure 257** on page 160). The choices are **Rectangle**, **Ellipse**, and **Custom**.
2. Click and drag on a space on the map to create an outline to your room (rectangle or ellipse).
3. To create a custom room, move the mouse and click on each corner. Complete the shape by clicking on the first corner again.

   When the shape is complete (rectangle, ellipse, or custom) the Room Properties dialog box opens, showing the new room:

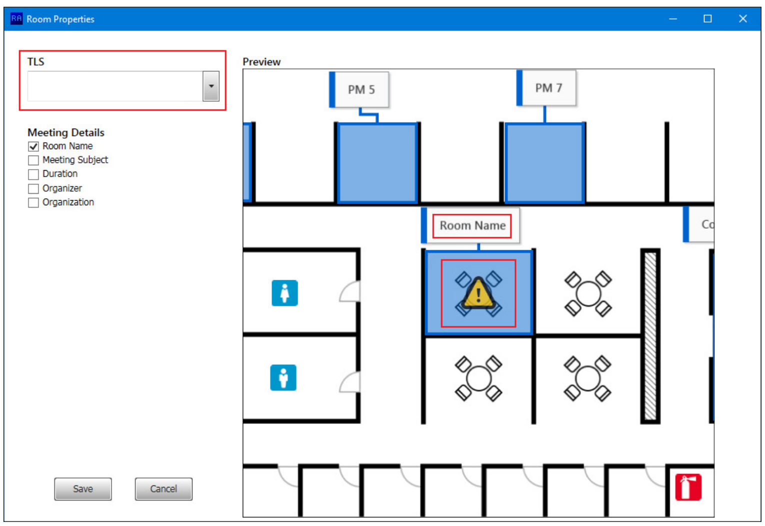


Figure 260. Room Properties Dialog Box

4. Until a room has been assigned to the shape, the associated information box is labelled Room Name and the shape has the yellow and black warning sign. Once you assign a room, that name appears in the information box and the warning sign disappears.

> **NOTE:** When you select a room, it is not removed from the TLS list. Be careful not to assign the same room to two different locations.

5. Click the **TLS** dropdown list. This contains a list of all the room panels that have not been associated with a room on the map.
6. Select a room from this list.
7. Check the meeting details that you want to appear on the room label. The options are:
   - **Room Name**
   - **Meeting Subject**
   - **Duration**
   - **Organizer**
   - **Organization**
8. Click **Save** to save the room properties.

The room still appears on the map if you click **Cancel**. To remove the room, right click on the shape and select **Delete** from the pop-up menu.

If you save a touchpanel room to the new map room, the name of the touchpanel room and any information you selected in steps 5-8 are shown on the map.

9. Add map assets as required by clicking on an icon in the `Map Assets` pane (see **figure 257** on page 160) and dragging it to its place on the map. The assets are:
   - You are here (yellow star). This is also the position of the Wayfinding Device.
   - Building entrance and exit
   - Fire escape
   - Fire extinguisher
   - Elevator
   - Stairs
   - Rest rooms
10. To save your changes, enter a name in the `Template Name` text box and click **Save**.
11. After saving the template, you must return to `CONFIGURE` tab to save the configuration.

Duplicate Maps

If you have two or more floors of the same building with the same room layout, you can duplicate a map and assign the appropriate rooms to each version.

For example, each version of the map can be used for a separate location: Floor 1, Floor 2, and so forth. The Wayfinding Device allows you to scroll through the different maps to find the location of your room on the correct floor.

To duplicate a map, right click on the file listed in the `Maps` pane in the top right corner of the screen and select **Duplicate** from the drop-down list. The file is automatically saved with a new name.

To edit the name assigned to the new map, right click the file name and select **Edit**. The `Edit Map` dialog box is identical to the `Add New Map` dialog box (see **figure 259** on page 160).

Edit the `Map Title` text box and click **Save**.

Options

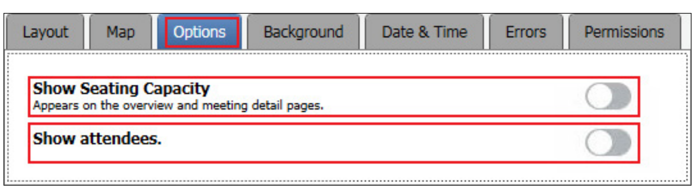


Figure 261. Wayfinding Devices — Options Tab

The **Options** tab allows you to toggle between:

- **Show** or **Hide** room `Seating Capacity`.
- **Show** or **Hide** a list of `Attendees`.

Background

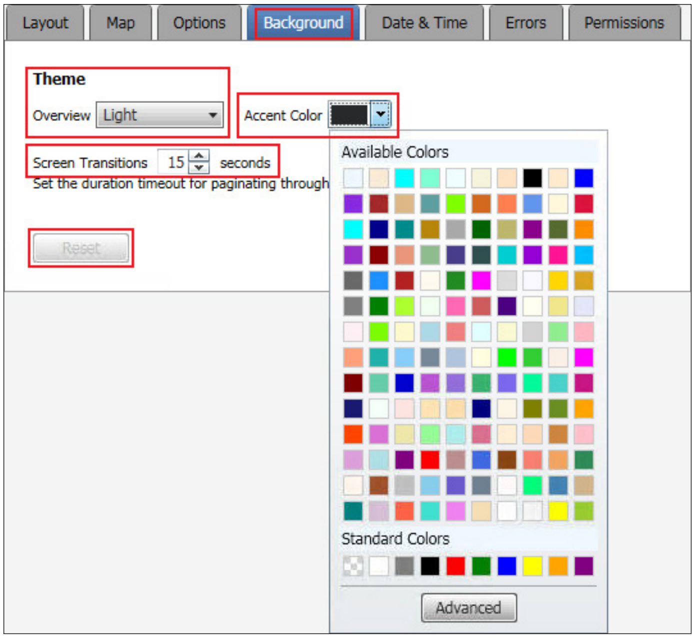


Figure 262. Wayfinding Devices — Background Tab

The `Background` tab allows you to set:

- `Theme Overview`:
    - **`light`**

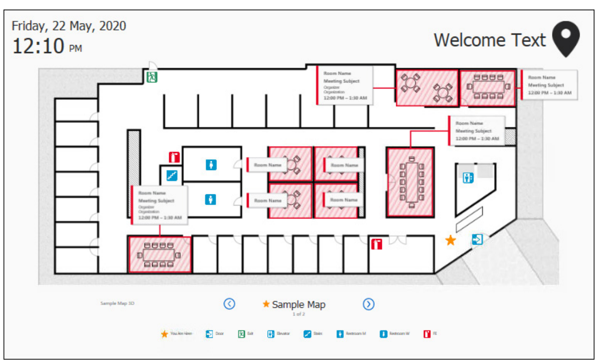


Figure 263. Wayfinding Devices — Theme Overview (light)

- **`dark`**

Figure 264. Wayfinding Devices — Theme Overview (dark)

- `Accent Color` – You can choose from the **`Available Colors`** or click **`Advanced`** to create your own color.
- `Screen Transitions` time – When multiple pages are displayed as a slide show, this determines how long each screen is displayed.

Changes in the layout can be seen in the **Preview Panel** (see page 165).

Date & Time

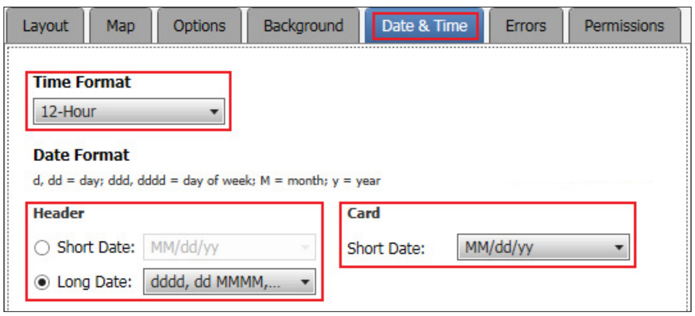


Figure 265. Wayfinding Devices — Date & Time Tab

1. Click **`Date & Time`**.
2. Select the `Time Format`. The choices are:
   - **`12-Hour`**
   - **`24-Hour US`**
   - **`24-Hour International`**
3. Select either the **`Short Date`** or **`Long Date`** radio button for the time format used in the Wayfinding device Header. The time format associated with the individual rooms must be in one of the Short Date formats. The options for each drop-down list are:

Header Short Date	Header Long Date	Room Short Date
M/d/yyyy — 5/20/2020	*dd MMMM, yyyy* — 20 May, 2020	*M/d/yyyy* — 5/20/2020
M/d/yy — 5/20/20	*dddd, dd MMMM, yyyy* — Wednesday, 20 May, 2020	*M/d/yy* — 5/20/20
MM/dd/yy — 05/20/20	*dddd, MMMM dd, yyyy* — Wednesday, May 20, 2020	*MM/dd/yy* — 05/20/20
MM/dd/yyyy — 05/20/2020	*MMMM dd, yyyy* — May 20, 2020	*MM/dd/yyyy* — 05/20/2020
yy/MM/dd — 20/05/20		*yy/MM/dd* — 20/05/20
yyyy-MM-dd — 2020-05-20		*yyyy-MM-dd* — 2020-05-20
dd-MMM-yy — 20-May-20		*dd-MMM-yy* — 20-May-20

Changes in the layout can be seen in the **Preview Panel** (see page 165).

Errors

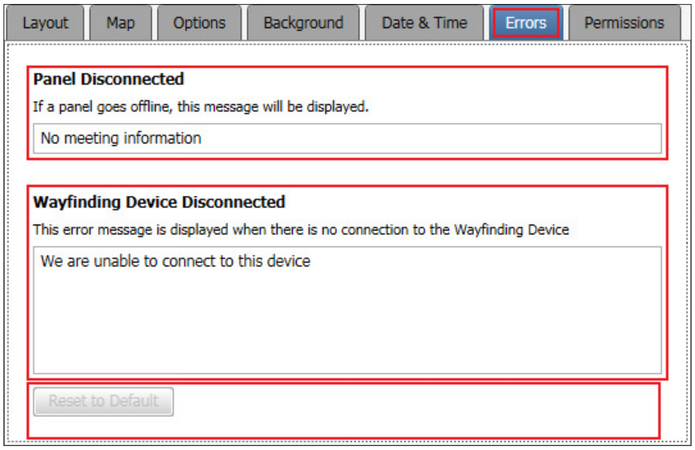


Figure 266. Wayfinding Devices — Errors Tab

You can customize the messages that are displayed when one of the individual room panels goes offline (`Panel Disconnected` message) or when the Lobby panel is disconnected (`Wayfinding Device Disconnected` message).

The default messages are shown in the image above. When you make changes to either message, the **`Reset to Default`** button becomes available, allowing you to discard any changes you have made.

Changes in the layout can be seen in the **Preview Panel** (see page 165).

Permissions

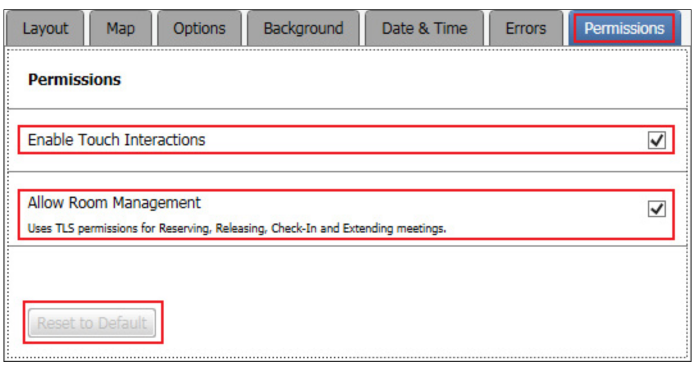


Figure 267. Wayfinding Devices — Permissions Tab

This tab allows you to **`Enable Touch Interactions`** and **`Allow Room Management`**. By default, both options are checked.

> **NOTE:** `Room management` requires `touch interactions` to be enabled. If **`Enable Touch Interactions`** is not selected, **`Allow Room Management`** is unavailable for selection.

Preview Panel

The right pane of the `DESIGN` tab (see **figure 241** on page 150) shows previews of various screens that are available. Use the drop-down list to select the preview you wish to view. The options are:

- **Map** (see page 166)
- **Available Space** (see page 166)
- **Reserved Space** (see page 167)
- **Weekly view** (see page 167)
- **Device Offline** (see page 168)

Map

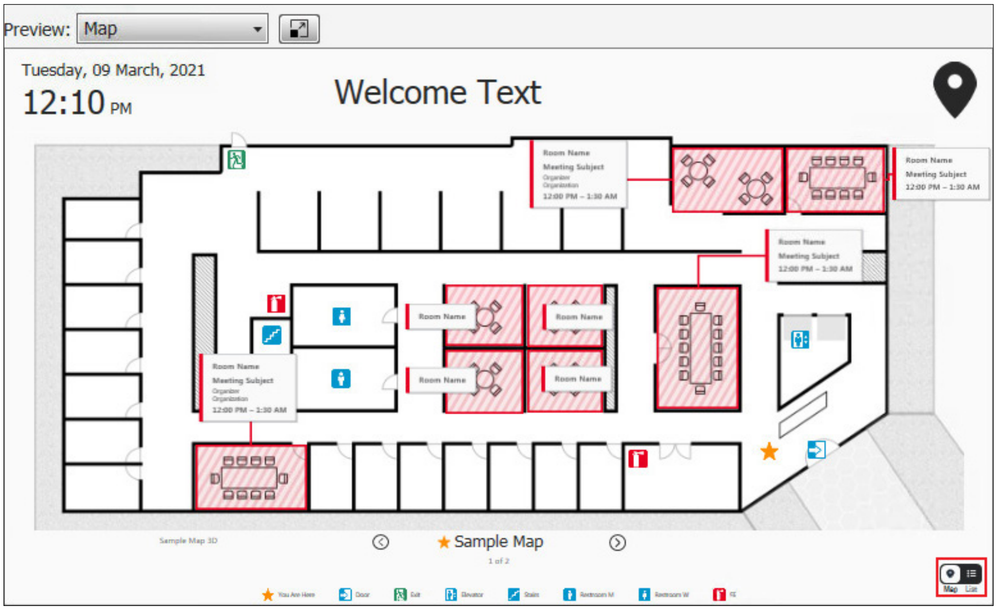


Figure 268. Wayfinding Device Map — Map Preview

The map preview shows the current version of a saved map. It can be the sample map that was used for practice or a map that accurately reflects your workspace. If `Enable Map and List Views` is **on**, a toggle switch is seen in the bottom right corner. This allows viewers using the Wayfinder screen to toggle between the map view and list view.

Available Space

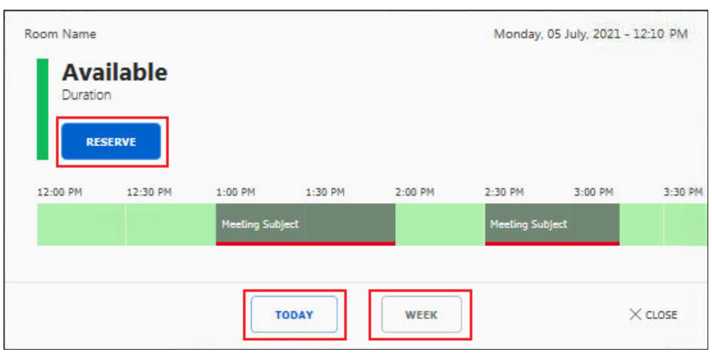


Figure 269. Wayfinding Device Map — Available Space

Press one of the available rooms listed in the overview screen.

The timeline for that room shows when it is available (green bar) or occupied (gray bar, underlined in red).

The default view shows the meetings for that day for four hours from the current time. To see the room availability for the entire week, press **`WEEK`**. To return to the default view, press **`TODAY`**.

To reserve the room, press one of the buttons with a green bar to select a period when the room is free and then press **`RESERVE`**.

Reserved Space

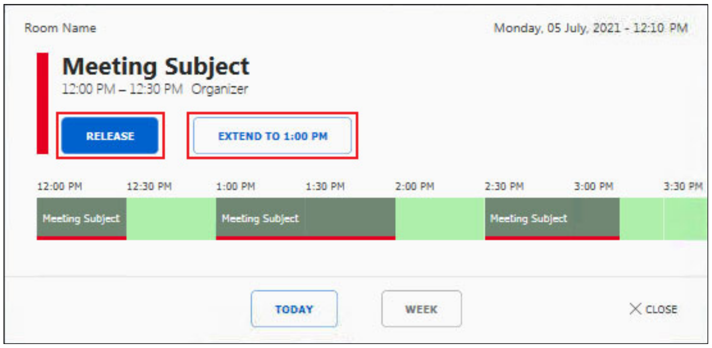


Figure 270. Wayfinding Device Map — Reserved Space

In the overview, press the room that has been reserved for the meeting.

The timeline shows when the room is available (green bar) or occupied (gray bar underlined in red).

The default view shows the meetings for that day for four hours from the current time. To see the room availability for the entire week, press `WEEK`.

If the `Check In` feature has been configured in advance, a `Check In` button is available.

Press `Check In`. The room is prepared automatically for the meeting: blinds can be closed, lights can be dimmed, as required, computers and projectors can be turned on.

The meeting shown in the figure above is scheduled to finish at 12:30 pm. If the meeting is running later than expected and the room is available during the next time slot (12:30 to 1:00 pm), press `EXTEND TO 1:00 PM` to reserve the room for an additional 30 minutes.

If the meeting is cancelled or finishes early, press `RELEASE`. This makes the room available for other users.

> **NOTE:** These options require the individual room panels to have the `Allow check in`, `Allow time extension`, and `Allow room release` options selected in the `Rooms` **Layout Tab** (see page 123)

Weekly view

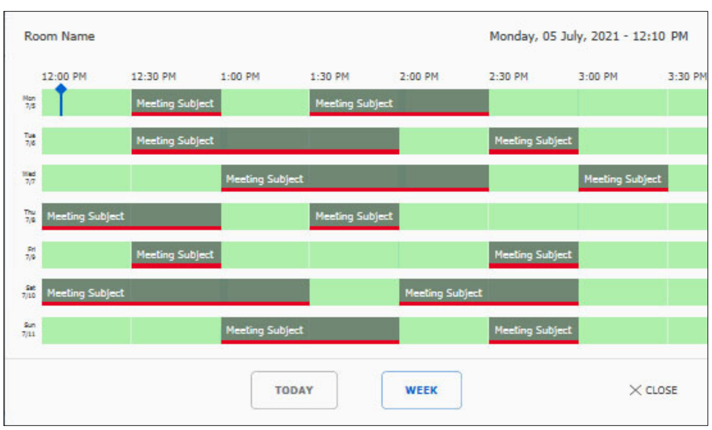


Figure 271. Wayfinding Device Map — Weekly View

The `Weekly` view shows room availability, 24 hours each day, for the next seven days, starting with the current day.

Device Offline

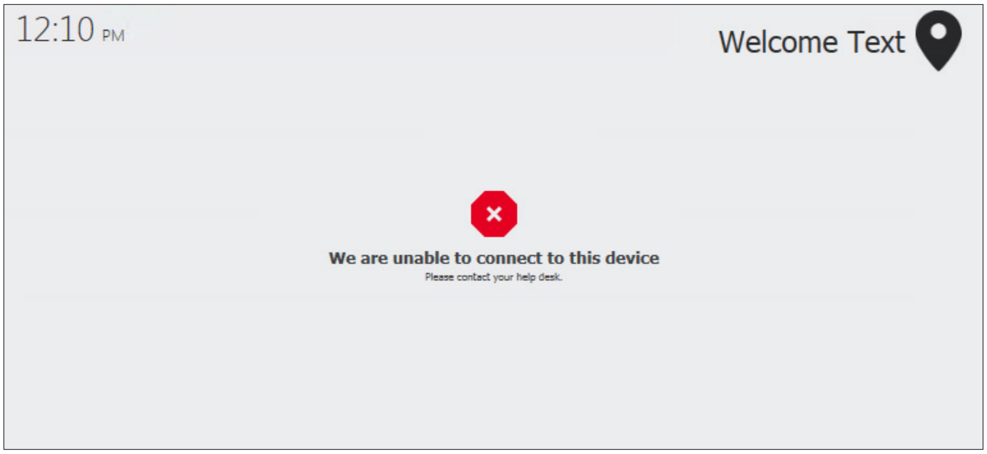


Figure 272. Wayfinding Device Map — Device Offline Preview

This message is displayed if the Wayfinding device is offline.

The message above is the default message. It can be changed in **Errors** (see page 165).

Hardware

This section provides an overview for installing the hardware. For more information, see the user guide for that product, which is available at **www.extron.com**. The topics covered in this section are:

- **TLS Panels**
- **TLSI Devices**

As of November 2023, Extron recommends the following TLS panels for use with the Room Agent software:

- TLS 300M
- TLS 525M
- TLS 725M
- TLS 1025M

Check with **www.extron.com** to see a list of the latest recommended TLS panels.

Room agent also supports the TLSI 201 Wayfinding device.

TLS Panels

The Extron TLS 300M, 525M, 720M, 725M, and 1025M are wall mounted, capacitive touchpanels with TFT active matrix color LCD screens with 24-bit color depth.

TLS 300M — A 3.5-inch (measured diagonally) touchscreen with a 320x480 resolution

TLS 525M — A 5-inch panel with an 800x480 resolution.

TLS 725M — A 7-inch, panel with an 1024x600 resolution.

TLS 1025M — A 10-inch panel with a 1280x800 resolution.

NOTE: For use in a high-security environment, the camera, Bluetooth, and microphone have been removed from the TLS 525M NC, 725M NC, and 1025M NC models. In all other respects, they are identical to the standard models.

Information about mounting and basic setup for these panels is shown on the following pages. For complete information, see the *TLP Pro 300M and TLS 300M User Guide* and *TLP Pro 525, 725, and 1025 Series User Guide* at **www.extron.com**.

These models ship with the latest firmware for the scheduling system. No firmware update is required.

Setup Checklist

Get Ready

- Download and install the latest version of the following software onto the PC being used to configure the TouchLink panel (see **Downloading Software** on page 18).
  - **Toolbelt** — Provides device discovery, device information, firmware updates, and configuration of network settings, system utilities, and user management for TouchLink Pro devices and scheduling panels.
  - **Room Agent** — Free room booking software for configuring the panels for room scheduling.

    NOTE: Both these software programs and supporting documentation are available from **www.extron.com**.
- Obtain the following network information from your network administrator:
  - **DHCP status** — (on or off). If DHCP is off, you must also obtain:
    - **IP address**
    - **Subnet mask**
    - **Gateway**
- **User name** — This can be either `admin` or `user`.
- **Password** — The factory configured passwords for all accounts on this device have been set to the device serial number. Passwords can be changed during configuration. Passwords are case sensitive.

  NOTE: If the device is reset to default settings, the password is the default password configuration. The default password is `extron` (for both `admin` or `user`).
- Make a note of the Touchpanel **MAC address**, which can be found on a rear-panel label.
- **SSL security certificates and IEEE 802.1X authentication** — TLS panels come with a factory-installed Secure Sockets Layer (SSL) security certificate. IEEE 802.1X authentication is also supported once enabled. See Secure Sockets Layer (SSL) Certificates on page 153 or see IEEE 802.1X Certificates on page 154 for more information.

Mount and Cable All Devices

ATTENTION:

- Do not power on the TouchLink panels until you have read the Attention in the “Rear Panel Features” section of the *TLP Pro 525, 725, and 1025 Series User Guide*.
- Ne branchez pas les écrans tactiles avant d’avoir lu la mise en garde dans la section « Rear Panel Features » du *TLP Pro 525, 725, and 1025 Series User Guide*.

- Mount the units. There are several mounting options for TouchLink panels (see **Mounting** on page 171).
- Connect the TouchLink panel to a Power over Ethernet injector.
- Connect the power injector to the LAN and power it on.

Set up the TouchLink Panels for Network Communication

- Connect the PC that you are using for setup, the control processor, and the touchpanel to the same Ethernet subnetwork.
- Use Room Agent **Network** (see page 35), the touchpanel **Setup Menu** (see page 179), or Toolbelt (see the *Toolbelt Help File*) to set the DHCP status and, if required, network addresses for the TouchLink panel.

Configure the TouchLink Panels

- The Room Agent **Manage Tab** (see page 25) and *Toolbelt Help File* provide information about configuring these panels.

Mounting

All these panels can be wall-mounted, either using a UL-listed junction box, an external wall box, or directly into drywall or furniture. Suitable mounting accessories can be found at **www.extron.com**.

ATTENTION:

- Do not install TouchLink panels in a fire resistant rated wall or partition assembly.
- Veuillez ne pas installer les écrans TouchLink dans un mur protégé par un dispositif coupe-feu ou dans une cloison.

- All structural steps and electrical installation must be performed by qualified personnel in accordance with local and national building codes and electrical codes.
- Toute étape structurelle et installation électrique, doit être effectuée par un personnel qualifié, conformément aux codes du bâtiment, aux codes incendie et sécurité, et aux codes électriques, locaux et nationaux.

Mounting the TLS 300M

Mounting with a UL-listed Electrical Box

The UL-listed electrical junction box must be purchased separately.

1. Cut a hole for the junction box at the required location.
2. If you are using the provided tether kit to deter theft, one loop of the tether kit should be secured to a wall stud with a screw (not provided).
3. Run cables to the installation site as required.
4. Pass the other end of the tether kit and the cables through a knock-out in the junction box.
5. Install the junction box using the manufacturer's instructions.
6. Secure the metal mounting plate to the junction box, using the provided screws.
7. Attach cables to the back of the touchpanel (see **Rear Panel Features** on page 176).
8. If a tether kit is being used, loosen the security screw on the back panel (see **figure 279**, F, on page 176) just enough to insert the loop of the tether kit.
9. Tighten the screw to clamp the tether in place.
10. Attach the touchpanel to the metal mounting plate. The touchpanel is held in place by magnets.

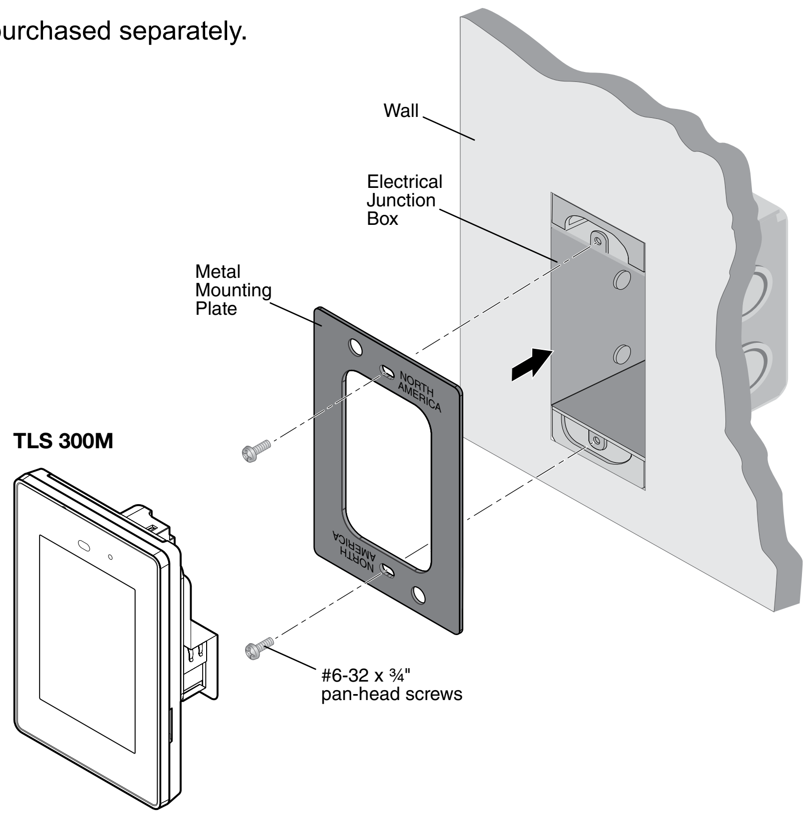


Figure 273. Mounting to a UL-Listed Electrical Box in the Portrait Orientation

Mounting to Drywall or Furniture

Figure 267 shows how to mount the TLS 300M in drywall. Follow the same procedure to mount into furniture.

1. Download the TLP Pro 300M Cut-out Template from **www.extron.com**. Ensure that it is printed at 100% size, with no scaling.
2. Remove the cut-out area from the template.
3. Attach the template to the wall in a suitable location, using a level to ensure the template is aligned correctly.
4. Use the template to mark and remove the cut-out area (❶) and drill two holes (❷) for the screws that secure the toothed clamping plates.
5. If you are using a tether kit to deter theft, one loop of the tether kit should be secured to a wall stud.
6. Run cables to the installation site as required.
7. Secure the metal mounting plate to the clamping plates, using the provided screws. As the screws turn, they tighten the grip of the clamping plates on the inside surface of the drywall.
8. Attach the tether kit and cables to the touchpanel and secure the touchpanel to the mounting plate as described in steps 7 through 10 in the previous section.

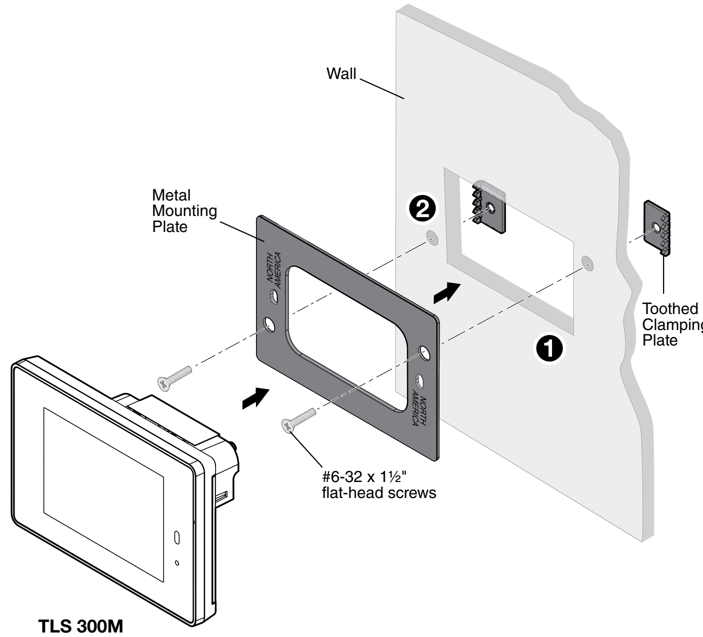


Figure 274. Mounting to Drywall or Furniture in the Landscape Orientation

Mounting the TLS 525M, 725M, and 1025M with a Wall Box or Junction Box

Some local building codes require the TouchLink panel to be mounted in a junction box. Junction boxes or wall boxes must be purchased separately. In **figure 275** on page 173, mounting the TLS 725M to a wall box is shown. Installation for the other panels is very similar.

NOTES:

- The 5 inch models mount to a 1-gang junction box. The US 1-gang junction box should be installed so that the long side is horizontal. EU or MK 1-gang junction boxes should be installed in the standard orientation.
- The 7 and 10 inch models mount to a 2-gang junction box.
- Extron provides four 3/4” #6-32 Philips pan head screws for mounting to US junction boxes.
- Extron provides two 16 mm M 3.5 Philips pan head screws for mounting to MK junction boxes.
- EU junction boxes are usually provided with their own screws.

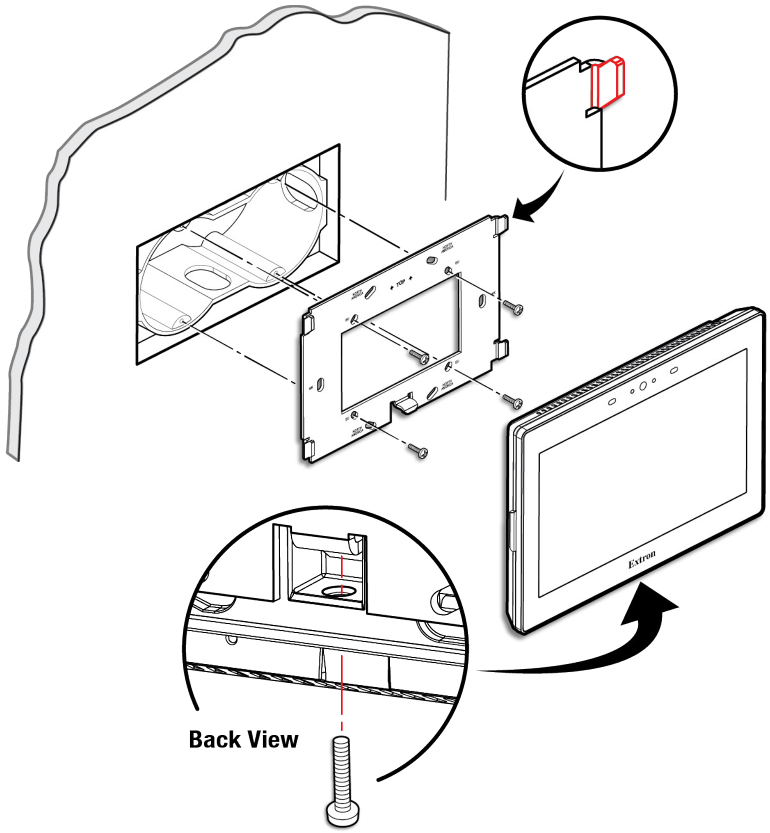


Figure 275. Mounting the TLS 725M with a wall box

Mounting the TLS panels with a wall box

1. Install a junction box or wall box (see figure 262), following the instructions provided by the manufacturer.
2. Fasten the mounting plate to the wallbox with the provided screws. Use the mounting holes that are appropriate to the junction box you are using (see **figure 276** on page 174).
3. Run and connect cables to the back of the touchpanel (see **Rear Panel Features** on page 176).

   The mounting plate for the 5 inch touchpanel has two hooks (one in each top corner). The mounting plate for the 7 and 10 inch panels has four hooks, one in each corner (see **figure 276**).
4. Position the touch panel so that the mounting slots (see **figure 280** on page 177) in the rear of the TouchLink panel align with these hooks.
5. Move the TouchLink panel inward and downward so that the panel sits securely on the hooks, and the tongue at the bottom of the mounting plate (see figure 268) sits in the groove in the bottom of the panel (see figure 268, bottom inset).
6. Fasten the TouchLink panel to the mounting plate with the lock screw.

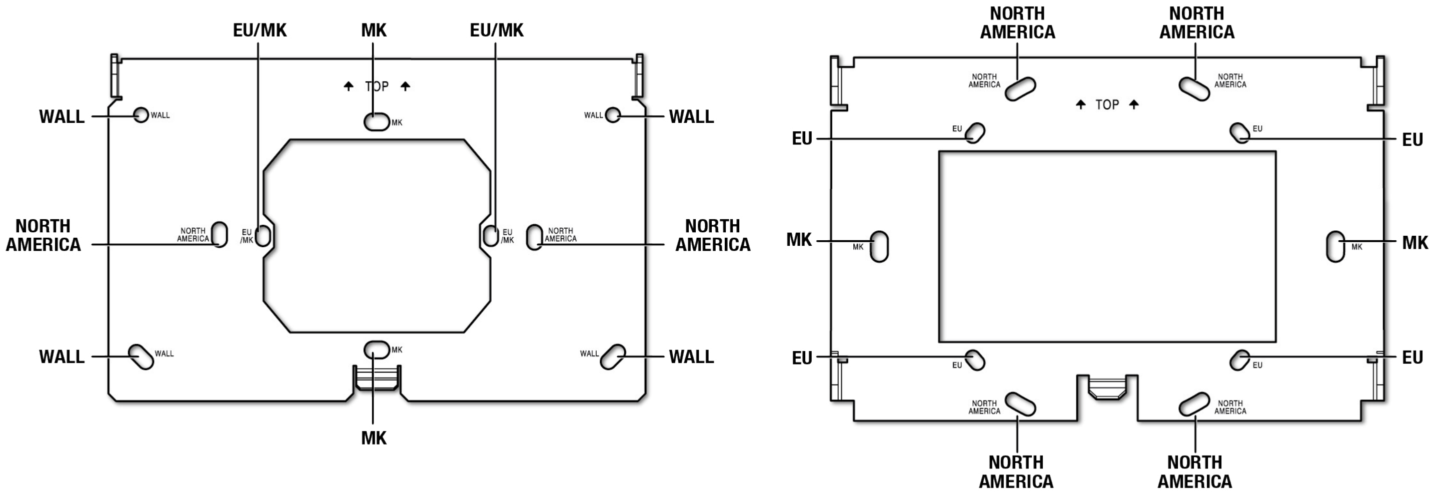


Figure 276. Mounting Plates for 5 inch models (left) and 7 or 10 inch models (right)

NOTE: The TLS 725M and TLS 1025M TouchLink panels use the same mounting plate.

Mounting the TLS panels without a wall box

If the wall box is not required by local building codes, you can mount the touchpanel directly into drywall.

1. Use the mounting plate as a template to mark the wall or download the cut-out template for your product from **www.extron.com**. Place the template or mounting plate against the wall or furniture in a suitable location and ensure that it is level.
2. Mark the position of the hole and cut the wall.
   - For the TLS 525, this hole is 2.4 inches (61 mm) wide x 2.1 inches (53 mm) high.
   - For the TLS 725 or 1025, this hole is 3.5 inches (89 mm) wide x 2.0 inches (51 mm) high.
3. Mark the slots labeled WALL (5 inch models) or MK (7 or 10 inch models) (see figure 264) and drill the pilot holes. Extron recommends using Molly bolts or SnapToggle bolts.
4. Secure the mounting plate to the wall (see **figure 275** on page 173).
5. Complete the installation as described in **steps 3 through 6** on page 173.

Front Panel Features

TLS 300M

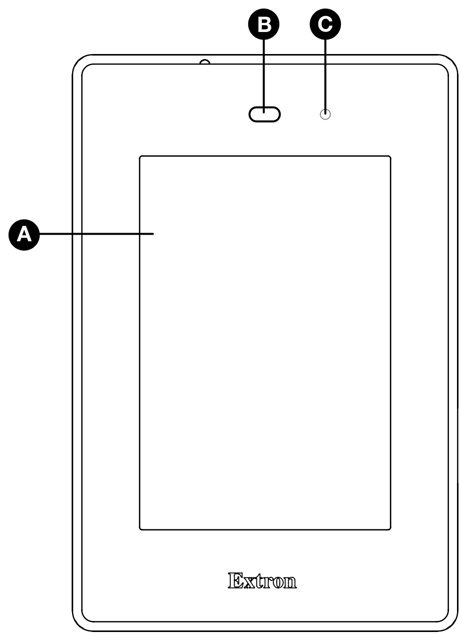


Figure 277. TLS 300M Front Panel

- **A LCD touchscreen** — The 3.5-inch, 320x480 resolution touchscreen is made with Corning® Gorilla® Glass, which is stronger and more scratch-resistant than standard glass, while maintaining touch sensitivity, color saturation, and brightness.
- **B Motion sensor** — Detects motion between three to five feet from the touchpanel, and at least 15° from the center axis.
- **C Light sensor** — Monitors ambient light level and adjusts screen brightness, based on the settings configured using the Setup Menu.

TLS 525M, 725M, and 1025M

NOTE: Figure 272 shows the front panel of the TLS 725M. The front panels of all the TouchLink panels have the same features and are almost identical apart from the size.

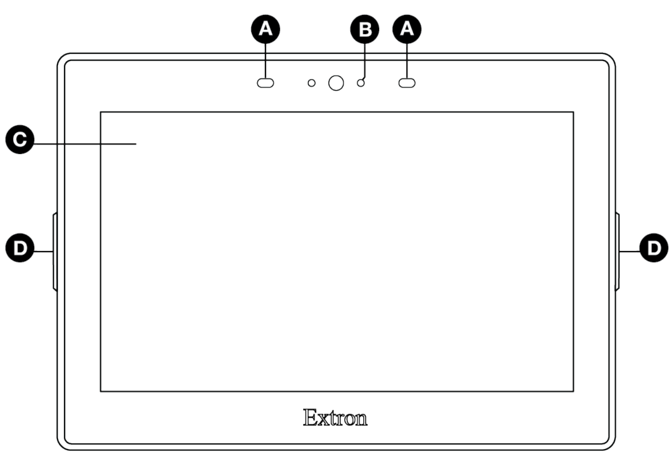


Figure 278. TLS 725M Front Panel

A Motion sensor — Detects motion between three to five feet from the TouchLink panel, and at least 15° from the center axis.

If the sleep timer has been set (see **Setup Menu** on page 179), and no motion has been detected for a user-defined period of time, the TouchLink panel enters sleep mode.

If Wake on Motion has been set (see **Setup Menu**), and motion is detected by the sensor while the screen is in sleep mode, the screen display is restored and active.

B Light sensor — Monitors ambient light level and adjusts screen brightness.

C Capacitive touchscreen

- The TLS 525M has a 5 inch screen with a 800x480 resolution.
- The TLS 725M has a 7 inch screen with a 1024x600 resolution.
- The TLS 1025M has a 10.1 inch screen with a 1280x800 resolution

D Status lights — Two LED light bars, one on either side of the screen. The LEDs light green when the room is currently available and red when the room is currently booked. They cannot be programmed.

Rear Panel Features

TLS 300M

Figure 273 shows the TLS 300M rear panel.

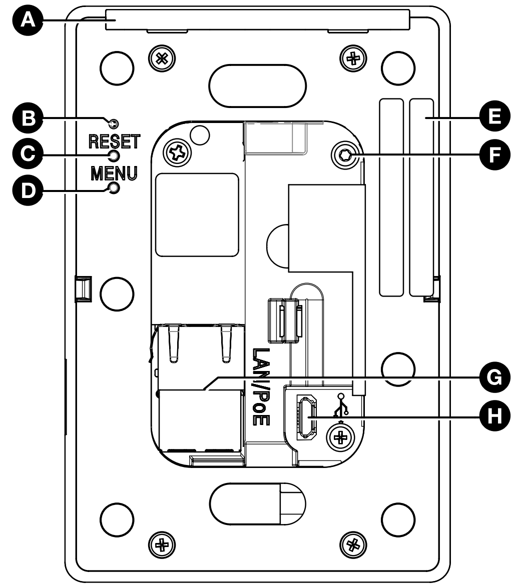


Figure 279. TLS 300M Rear Panel

A **Status light** — Provides system feedback. The LED can be configured to light red or green and to blink or light continuously, to provide system feedback.

For information about configuring or programming this light, see the *Global Configurator Help File* or the *ControlScript Deployment Utility Help File*.

B **RESET LED** — Provides feedback about the reset status when the user presses the **RESET** button. For more information, see **Reset Modes** (see page 179).

C **RESET Button** — Pressing the **RESET** button allows the unit to be reset in any of three different modes (see **Reset Modes**).

D **MENU Button** — Activates the setup menu. For more information, see **Setup Menu** on page 179.

E **Serial Number Label** — The serial number is on a label on the right edge of the rear panel, towards the top. The factory configured passwords for all accounts on this device have been set to this device serial number. Passwords are case sensitive.

> **NOTE:** If the device is reset to default settings, the password is the default password configuration. The default password is extron.

F **Security Screw** — Used to attach provided tether kit. It requires a Torx screwdriver (size T8).

G **LAN/PoE Connector** — Connect the touchpanel to a PoE power injector (not provided) using a twisted pair cable, terminated with an RJ-45 connector (see **Connecting the Power Injector** on page 178). Extron recommends the PI 130. Connect the power injector to the LAN through a network switch. An Extron IP Link Pro control processor must also be connected to the same network as the TouchLink Pro touchpanel.

> **ATTENTION:**
>
> - The TLS 300 is Power over Ethernet (PoE 802.3af, class 2) compliant. Do not power on the touchpanels until you have read the ATTENTION in the “Rear Panel Features” section of the *TLP Pro 300M and TLS 300 Series User Guide*.
> - Le TLS 300 supporte l’alimentation via Ethernet (PoE 802.3af, classe 2). Veuillez lire la partie « Attention » dans la section « Rear Panel Features » du *TLP Pro 300M and TLS 300 Series User Guide*, avant de mettre sous tension les écrans tactiles.

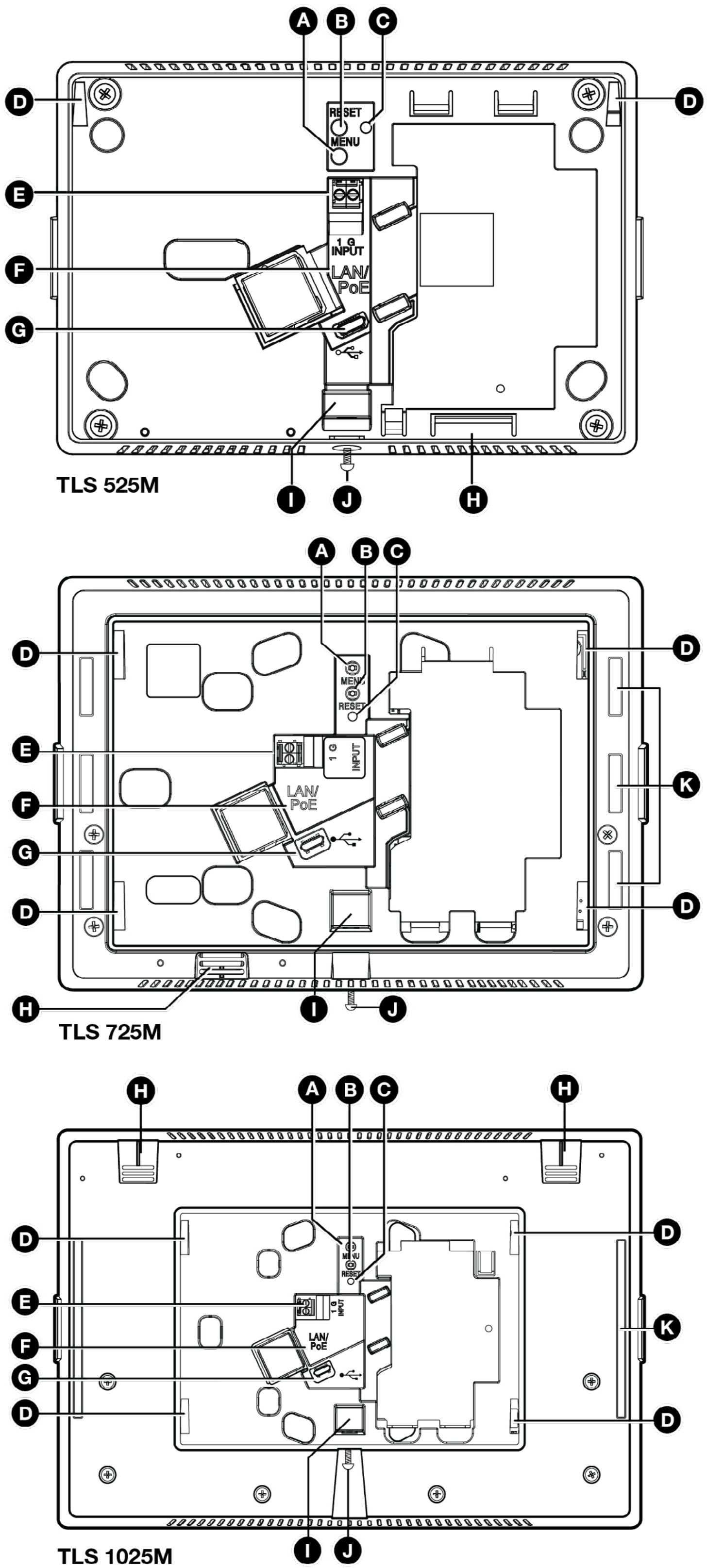
> **NOTE:** These touchpanels are shipped without a power injector. The power injector must be purchased separately.

H **USB Port** — One micro-B receptacle supports high-speed USB 2.0.

TLS 525M, 725M, and 1025M

NOTE: The panels shown in figure 268 are for illustration only and are not to the same scale.

Click the links on the right for more information on page 178.



- A MENU button
- B RESET button
- C RESET LED
- D Mounting slots
- E Digital input monitoring port
- F LAN/PoE connector
- G USB port
- H Speaker
- I Slot for mounting plate
- J Mounting screw
- K Rear panel status lights

Figure 280. TLS 525M, 725M, and 1025M Rear Panels

Ⓐ **MENU button** (see **figure 280** on page 177)— Activates the setup menu (see **Setup Menu** on page 179).

Ⓑ **RESET button** — Pressing the **RESET** button allows the unit to be reset in any of three different modes (for an overview, see **Reset Modes** on page 179).

Ⓒ **RESET LED** — Provides feedback about the reset status when the user presses the **RESET** button (see **Reset Modes**).

Ⓓ **Mounting slots** — The TLS 725M and TLS 1025M have four, one in each corner. The TLS 525M has two, one in each top corner. The hooks on the corners of the mounting plate (see **figure 275** on page 173) fit into these slots for wall mounting.

Ⓔ **Digital input monitoring port** — This two-pole captive screw port (1 = signal and G = ground) monitors digital input with or without a +5 VDC pull-up.

Ⓕ **LAN/PoE connector** — Connect the TouchLink panel to a PoE power injector (not provided) using a twisted pair cable, terminated with an RJ-45 connector (see “Connecting the Power Injector”, below). Connect the power injector to the LAN through a network switch.

ATTENTION:

- The TouchLink panels are Power over Ethernet (PoE 802.3af, class 3) compliant. Do not power on the touchpanels until you have read the Attention in the “Rear Panel Features” section of the *TLP Pro 525, 725, and 1025 Series User Guide*.
- Les écrans TouchLink supportent l’alimentation via Ethernet (PoE 802.3af, classe 3). Veuillez lire la partie « Attention » dans la section « Rear Panel Features » du *TLP Pro 525, 725, and 1025 Series User Guide*, avant de mettre sous tension les écrans tactiles.

NOTE: The TLS panels ship without a power injector. The power injector must be purchased separately. Extron recommends the Extron XTP PI 100 power injector (see figure 247). Your power injector may look different.

Ⓖ **USB port** — Compatible with USB 2.0.

Ⓗ **Speaker** — Provides audible feedback for the user. The TLS 525M and 725M each have a single speaker. The TLS 1025M has two (dual mono) speakers

Ⓘ **Slot for mounting Plate** — The tongue at the bottom of the mounting plate (see **figure 275**) fits into this slot, for wall mounting.

Ⓙ **Mounting screw** — Tightens against the tongue of the mounting plate to secure the touchpanel.

Ⓚ **Rear panel status lights** — These lights can be disabled for glass mount applications.

- **TLS 525M** — no lights
- **TLS 725M** — Six lights, three on each side of the panel
- **TLS 1025M** — Two lights, one on each side of the panel

The LEDs light green when the room is currently available and red when the room is currently booked. They cannot be programmed.

Connecting the Power Injector

The power injector must be purchased separately. Figure 275 shows the Extron PI 130. Your power injector may look different.

Connect a straight-through Ethernet cable from the power injector to a switch or router. This cable carries network information from the switch or router to the power supply input. A second straight-through cable carries the network information and 48 VDC from the power injector to the touchpanel LAN/PoE connector. Connect the IEC power cord to a convenient 100 VAC to 240 VAC, 50-60 Hz power source.

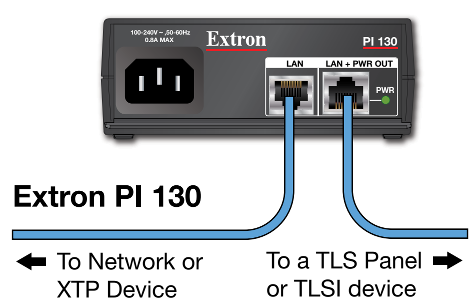


Figure 281. Connecting to a Power Injector

Reset Modes

These touchpanels provide the following reset modes (see the *TLP Pro 300M and TLS 300M User Guide* or *TLP Pro 525, 725, and 1025 Series User Guide* for complete information):

- **Use Factory Firmware** — With the unit powered off, press and hold the **`RESET`** button (see **figure 279** on page 176 [TLS 300M] or **figure 280** on page 177 [TLS 525M, 725M, and 1025M]) while reapplying power to the unit. Use this mode with Toolbelt software to replace firmware in the event of conflicts arising from uploading a firmware update.
- **Reset All IP Settings** — Press and hold the **`RESET`** button for 6 seconds. After the `RESET LED` blinks twice, release and momentarily press the **`RESET`** button. Use this mode to reset all network settings without affecting user-loaded files.
- **Reset to Factory Defaults** — Press and hold the **`RESET`** button for 9 seconds. After the `RESET LED` blinks three times, release and momentarily press the **`RESET`** button. Use this mode to return the TouchLink panel to factory default settings.

  NOTES:
  - The factory configured passwords for all accounts on this device have been set to the device serial number. Passwords are case sensitive.
  - If the device is reset to default settings, the password is the default password configuration. The default password is `extron` (for either `admin` or `user`).

- **Enable or Disable the DHCP Client** — This mode toggles between **`DHCP enabled`** and **`DHCP disabled`**. Press the **`RESET`** button five times, consecutively. After the fifth press, do not press the button again within 3 seconds. If DHCP was enabled, it is now disabled and the `Power LED` blinks three times. If DHCP was disabled, it is now enabled and the `Power LED` blinks six times.

Setup Menu

TLS 300M

Figure 276 shows the Setup menu STATUS screen for the TLS 300M. It may be necessary to scroll down to see all the information on the page.

Press the **`MENU`** button (see **figure 279**, **D**, on page 176) to open the `Setup menu`. Any of the six available screens (**`STATUS`**, **`NETWORK`**, **`DISPLAY`**, **`AUDIO`**, **`PROJECT INFORMATION`**, and **`ADVANCED`**) can be accessed by pressing the **`MENU`** button in the top left corner of the screen.

System Information allows the touchpanel to be connected to a control processor. Toggle the LinkLicenses switch to allow the device to function as a touchpanel or a control processor. These two functions can be accessed from the **`ADVANCED`** page of the `Setup menu`. (For more information, see the *TLP Pro 300 and TLS 300 User Guide*).

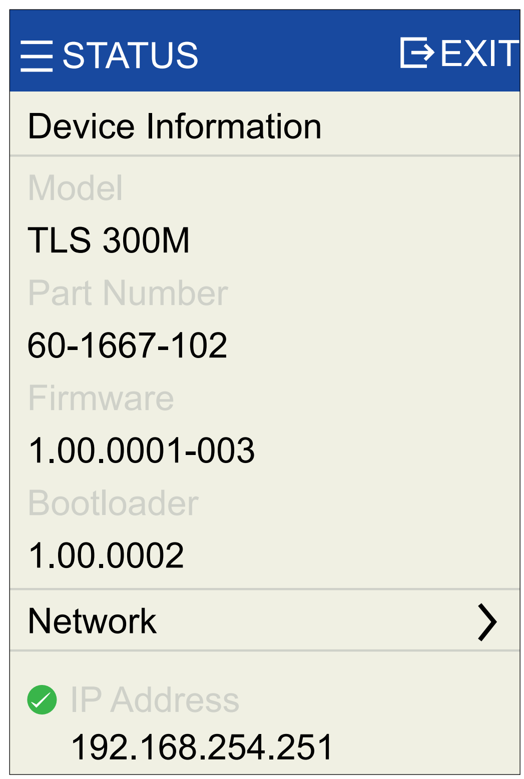


Figure 282. TLS 300M Setup Menu

TLS 525M, 725M, and 1025M

Figure 277 shows the `Status` screen for the TLS 725M. The screens for the TLS 525M, TLS 1025M are similar.

Press the **MENU** button (see **figure 280** on page 177) to open the `Setup menu`. Select any of the five available screens (**`Status`**, **`Network`**, **`Display`**, **`Audio`**, and **`Advanced`**) by pressing the appropriate button in the navigation bar at the top of the screen (for more information, see the *TLP Pro 525, 725, and 1025 Series User Guide*).

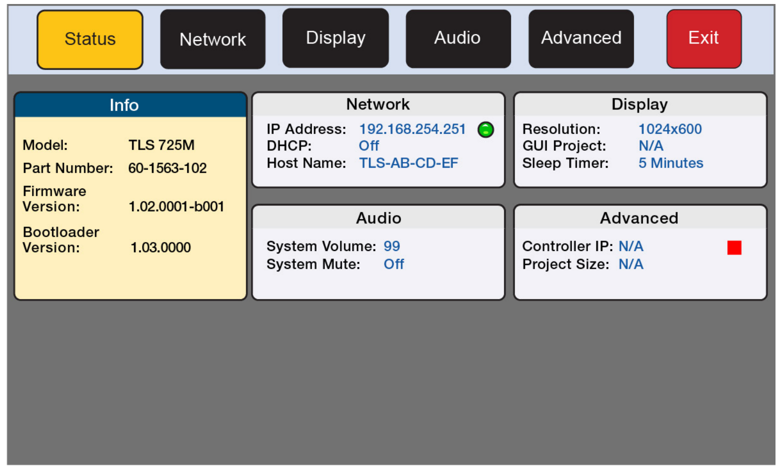


Figure 283. Setup Menu: Status Screen for TLS 725M

TLSI Devices

The Extron TLSI 201 Interactive Wayfinding Interface provides real-time meeting space availability, status, and location information using a centralized display. The TLSI 201 communicates over the Ethernet network directly with Extron TLS room scheduling panels and shows information about the TouchLink scheduler system on third-party touch and non-touch displays. The interface supports resolutions up to 4K.

Users can locate and book meeting spaces for the day or week on an interactive grid or map with ease. No additional programming or external processors are required.

This guide provides instructions for experienced installers to mount the TLSI 201 and to create a basic configuration. For more complete instructions, see the *TLSI 201 User Guide*, at **www.extron.com**.

Setup Checklist

Get Ready

- Download and install the latest version of **Room Agent** (see **Downloading Software** on page 18) — Room booking software for configuring the TLSI 201 for room scheduling. Room Agent can be downloaded (free of charge) from **www.extron.com**.
- Obtain the following network information from your network administrator:
  - **DHCP status** — (on or off). If DHCP is off, you must also obtain:
    - **IP address**
    - **Subnet mask**
    - **Gateway**
- **Username** — This can be either admin or user.
- **Password** — The factory configured passwords for all accounts on this device have been set to the device serial number. Passwords can be changed during configuration. They are case sensitive.

  NOTE: If the device is reset to default settings, the passwords are reset to the default password, which is extron (for either admin or user).

- Make a note of the **MAC address** for the TLSI 201.
- **SSL security certificates and IEEE 802.1X authentication** — TLSI 201 comes with a factory-installed Secure Sockets Layer (SSL) security certificate. IEEE 802.1X authentication is also supported once enabled. See Secure Sockets Layer (SSL) Certificates on page 153 or see IEEE 802.1X Certificates on page 154 for more information.

Mount and Cable All Devices

- Mount the units. The TLSI 201 can be discretely mounted behind a flat panel display. For available mounting options see the TLSI 201 product page at **www.extron.com**.

  To mount a third-party touchpanel follow the instructions provided by the manufacturer.
- Connect cables to the TLSI 201 (see “Rear Panel Connectors and Features”, below).
- Connect the HDMI output from the TLSI 201 to the third-party touchpanel.
- Connect the USB port from the TLSI 201 to the third-party touchpanel.

  NOTE: The USB connection passes information to the TLSI 201 about where on the screen the third-party touch display was pressed. If using a non-touch display, connect a USB mouse to the USB port on the TLSI 201 to click screen icons.
- Connect the Ethernet cable. The TLSI 201 must be powered by PoE+.

  ATTENTION:
  - Do not power on the TLSI 201 until you have read the Attention in the Rear Panel Features section of the *TLSI 201 User Guide*.
  - Ne branchez pas le TLSI 201 avant d’avoir lu la mise en garde dans la section « Rear Panel Features » du *TLSI 201 User Guide*.

Set up the TLSI 201 for Network Communication

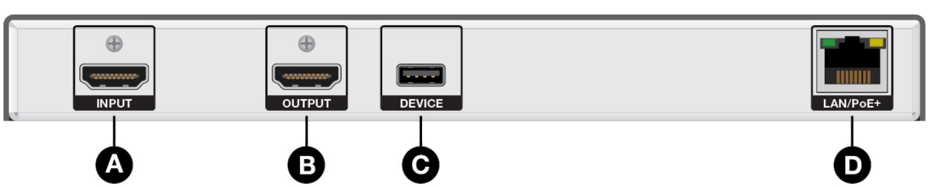
- Connect the PC used for setup on the same Ethernet subnetwork as the TLSI 201.
- Use the **Setup Menu** on page 184 to set the DHCP status and, if necessary, the IP address, subnet mask, gateway, and related settings for the network interface. You can also configure these settings in Room Agent.

Configure the User Interface, using the Room Agent software.

- Configure the TLSI 201, using the Room Agent software.

Rear Panel Connectors and Features

For complete information about the rear panel connectors and features, see the *TLSI 201 User Guide* at **www.extron.com.**



A HDMI input
B **HDMI output**
C **DEVICE port**
D **LAN/PoE+ port**

Figure 284. TLSI 201 Rear Panel

ATTENTION:
- The TLSI 201 is Power over Ethernet (PoE 803.3at, class 4) compliant. Do not connect the power supply before reading the “Attention” in the “Rear Panel Features” section of the *TLSI 201 User Guide*.
- Le TLSI 201 support l’alimentation via Ethernet (PoE 803.3at, classe 4). Veuillez lire la partie « Attention » dans la section « Rear Panel Features » du *TLSI 201 User Guide*, avant de mettre sous tension les écrans tactiles.

A **HDMI input** — At present, this port is not used by the TLSI 201.

B **HDMI output** (see figure 284 on page 181) — Connect this HDMI type A port to a third-party display. The TLSI 201 supports output resolutions up to 4K.

Use the provided LockIt HDMI lacing bracket to secure the HDMI connector:

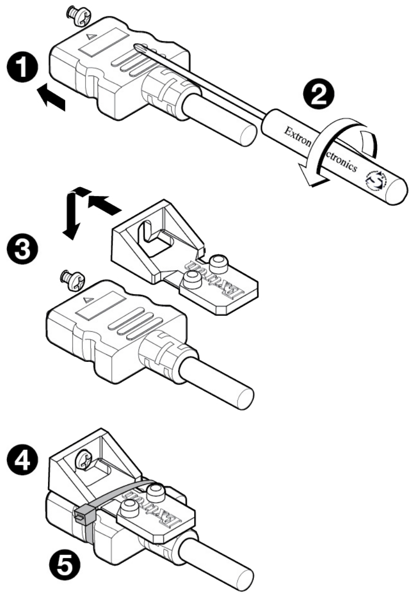


Figure 285. Securing the HDMI Connector with a LockIt bracket

1. Plug the HDMI cable into the TLSI 201 HDMI output port (see figure 273).
2. Loosen the HDMI connection mounting screw from the panel enough to allow the LockIt lacing bracket to be placed over it. The screw does not have to be removed.
3. Place the LockIt lacing bracket on the screw and against the HDMI connector, then tighten the screw to secure the bracket.

> **ATTENTION:**
>
> - Do not overtighten the HDMI connection mounting screw. The shield it fastens to is very thin and can easily be stripped.
> - Ne serrez pas trop la vis de montage du connecteur HDMI. Le blindage auquel elle est attachée est très fin et peut facilement être dénudé.

4. Loosely place the included tie wrap around the HDMI connector and the LockIt lacing bracket as shown.
5. While holding the connector securely against the lacing bracket, tighten the tie wrap, then remove any excess length.

C **DEVICE port** — supports High-speed USB 2.0 control. Plug a Type-A USB cable from the third-party touchpanel into this port.

> **NOTE:** If using a non-touch display, connect a USB mouse to the USB port on the TLSI 201 to click screen icons.

D **LAN/PoE+ port** (see **figure 284** on page 181) — Use an Ethernet cable to connect this port to the network via a PoE+ power sourcing equipment (PSE, not provided). This can be a power injector or PoE+ switch.

> **NOTE:** The TLSI 201 does not include any PoE+ power sourcing equipment. This must be purchased separately.

Extron recommends the Extron PI 130 power injector (see figure 286). Your power injector may look different.

Use an Ethernet cable to connect the LAN/PoE+ port of the TLSI 201 to the power output of the 803.3at, class 4 compliant PoE+ power injector.

Connect the network input of the power injector to a network switch or router.

Alternatively, use an Ethernet cable to connect the LAN/PoE+ port of the TLSI 201 to a PoE+ switch.

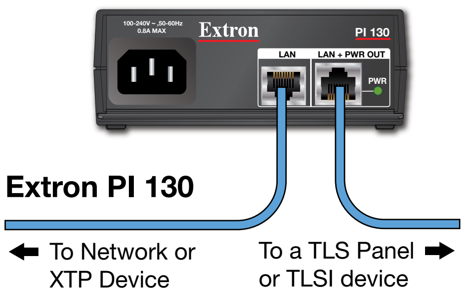


Figure 286. PI 130 Power Injector

Front Panel Features

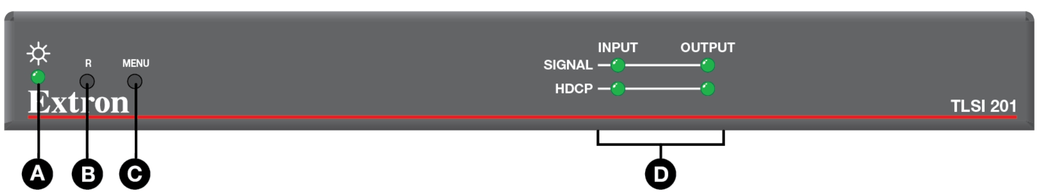


Figure 287. TLSI 201 Front Panel

A **Power LED** — Indicates the power status and the reset status of the unit.

B **Reset button** (recessed) — Allows the unit to be reset in any of three different modes. It also allows the user to toggle between enabling and disabling the DHCP client. A brief summary of the reset modes is given below. For more information see the TLSI 201 User Guide.

C **MENU button** (recessed) — Opens the **Setup Menu** (see page 184) and `Calibration` screen for the TLSI 201:

Setup Menu

a. Press the button briefly (less than 3 seconds) to open the internal menu screens.

b. Press the button briefly for a second time to exit the setup menu.

Calibration Screen

a. Press and hold the button (3 seconds or more) to open the `Calibration` screen. Follow the on-screen instructions to calibrate the touchpanel.

b. Complete the calibration process or press the button briefly (less than 2 seconds) for a second time to exit the `Calibration` screen.

D **Status LEDs** — The Signal LEDs light green when a video signal is detected and are unlit when no signal is detected.

The HDCP LEDs light green when HDCP content is detected and are unlit when HDCP content is not detected.

Reset Modes

The TLSI 201 offers the following reset modes:

- **Use Factory Firmware** — Press and hold the **`Reset`** button (see **figure 287** on page 183) while applying power to the unit. Use this mode to replace firmware in the event of firmware failure.
- **Reset Network Settings** — Press and hold the **`Reset`** button for 6 seconds. After the `Power LED` flashes twice, release and momentarily press the **`Reset`** button. Use this mode to reset all network settings without affecting user-loaded files.
- **Full Factory Reset** — Press and hold the **`Reset`** button for 9 seconds. After the `Power LED` flashes three times, release and momentarily press the **`Reset`** button. Use this mode to return the device to factory default settings.

NOTES:

- The factory configured passwords for all accounts on this device have been set to the device serial number. Passwords can be changed during configuration. They are case sensitive.
- If the device is reset to default settings, the passwords are reset to the default password, which is `extron` (for either `admin` or `user`).

- **Toggle DHCP Client** — This mode toggles between DHCP enabled and DHCP disabled. Press the **`Reset`** button five times, consecutively. After the fifth press, do not press the button again within 3 seconds. If DHCP was enabled, it is now disabled and the Power LED blinks three times. If DHCP was disabled, it is now enabled and the `Power` LED blinks six times.

Setup Menu

Press the **`MENU`** button (see **figure 287**) to open the setup menu (see figure 288). There are five available screens that are selected by pressing the appropriate button in the navigation bar on the left side of the screen.

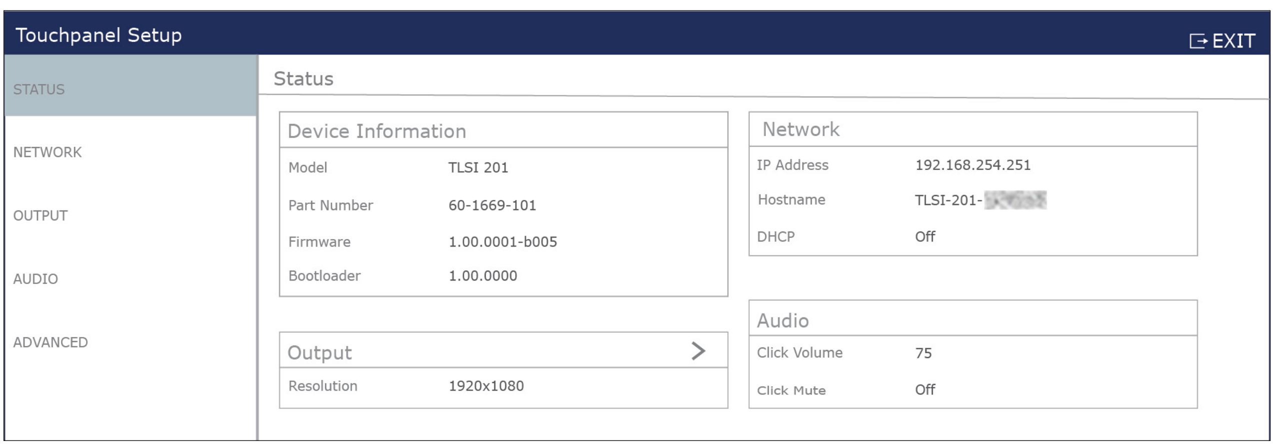


Figure 288. Setup Menu

- The **`STATUS`** screen is read-only and provides a summary of the other screens.
- The **`NETWORK`** screen is used to edit the network settings (DHCP setting, IP, subnet mask, gateway, and DNS Primary addresses).
- The **`OUTPUT`** screen is used to configure the image shown by the third-party display, using built-in test patterns and EDID.
- The **`AUDIO`** screen is used to set audio levels.
- The **`ADVANCED`** screen provides information about the system and the memory. It also allows you to add or reset a PIN.

Press the **`EXIT`** button to close the setup menu.

For more information about the setup menu, see the *TLSI 201 User Guide* at **www.extron.com**.

TLSI 201 Web Page

1. To access the TLSI 201 default web page, enter the IP address of the unit into the web browser of a PC connected to the same subnet.

   A dialog opens asking for the device username and password.

   NOTES:

   - The factory configured passwords for all accounts on this device have been set to the device serial number. Passwords can be changed during configuration. They are case sensitive.
   - If the device is reset to default settings, the passwords are reset to the default password, which is `extron` (for either `admin` or `user`).

   The single page (see figure 276) provides general and network information about the unit.

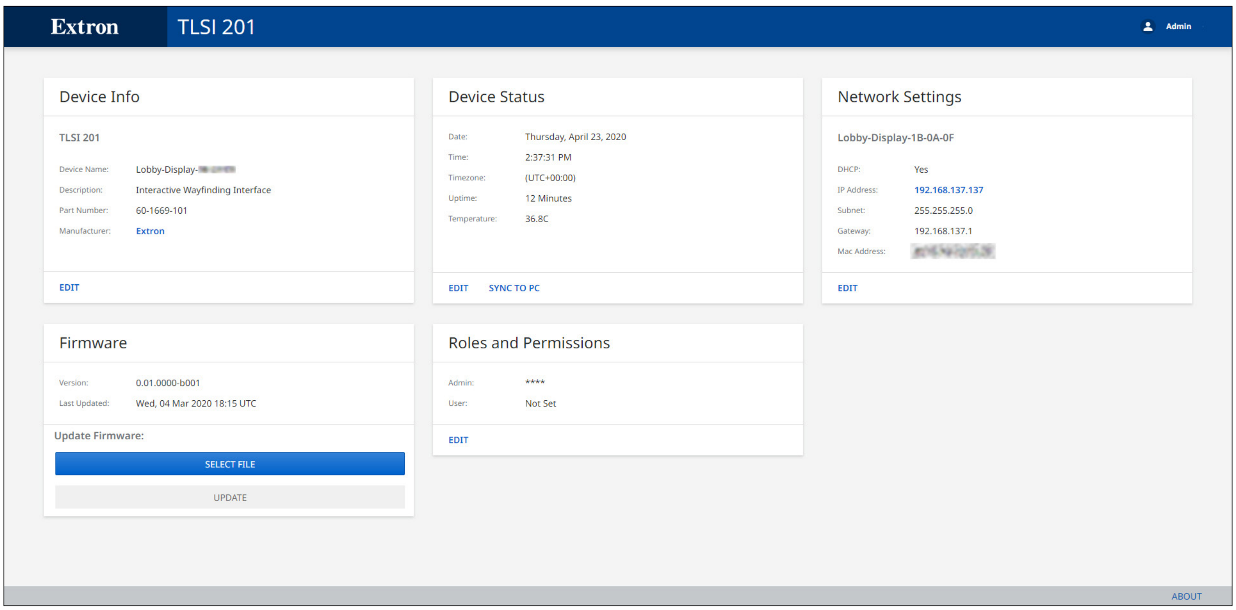


Figure 289. TLSI 201 Web Page

2. Click the various **`EDIT`** buttons to change the associated TLSI 201 settings.
3. Use the **`Network Settings EDIT`** button to configure the TLSI 201 network settings.

   You can also configure the network settings of the TLSI 201 by using the **Setup Menu** (see page 184) or Toolbelt (see the *Toolbelt Help File*).

To update the device firmware:

1. If necessary, download the firmware file to the control PC.
2. On the TLSI web page, click **`Select File`** and navigate to a firmware file saved on the PC.
3. Click **`Update`**.

   The new firmware is installed on the TLSI 201.

Reference Information

This section provides a central location for additional Room Scheduling System information, including:

- **Network Port Requirements and Licensed Third-Party Software**
- **Supported Languages**
- **Room Scheduling Analytics**
- **Secure Sockets Layer (SSL) Certificates**
- **IEEE 802.1X Certificates**
- **SNMP**

Network Port Requirements and Licensed Third-Party Software

For information about network port requirements and licensed third-party software for the touchpanels described in this guide, please refer to the *TouchLink Scheduling Panels Network Ports and Licenses Guide*, which is available at **www.extron.com**.

Supported Languages

Room Agent software supports scheduling panel displays in the following languages:

- English
- Arabic
- Catalan
- Chinese (simplified)
- Chinese (traditional)
- Croatian
- Czech
- Danish
- Dutch
- Finnish
- French
- German
- Hebrew
- Italian
- Japanese
- Korean
- Norwegian
- Polish
- Portuguese
- Russian
- Serbian
- Slovenian
- Spanish
- Swedish
- Thai
- Turkish
- Vietnamese

Room Scheduling Analytics

Room scheduling touchpanels provide the information needed to analyze room usage, activity patterns, and occupancy trends across the organization. A Scheduling Activity file with room usage and meeting data can be downloaded concurrently from multiple touchpanels. You can transform this readily-available information with data analytics tools to create powerful reports.

Extron provides a *Microsoft Power BI Usage Template* that can be used to visualize activity data.

Downloading the Microsoft Power BI Template

1. Download the template from the Room Agent page on the **Extron website**.
2. Unzip the `Extron Conference Room Scheduling Usage Template.zip. file`. This contains the Power BI template.

Exporting the Activity File as the Data Source from Room Agent

1. To export your data from your panels, navigate to the `CONFIGURE` tab (see figure 290, ❶).
2. Select the **Status** checkboxes (❷) for all the panels for which you wish Room Agent to download the activity file.
3. Click **Retrieve Activity File** (❸).

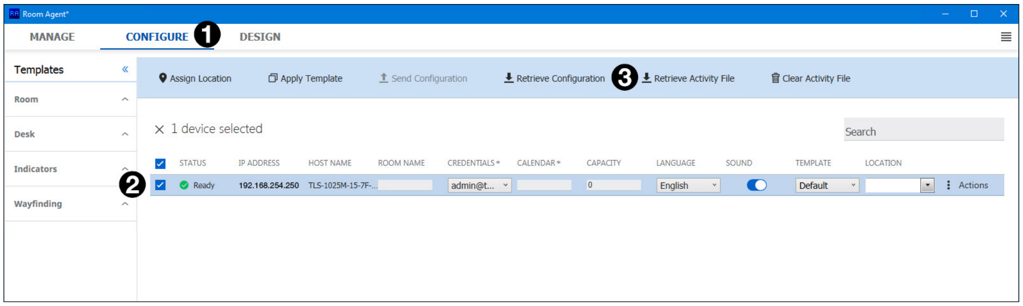


Figure 290. Retrieve Activity File

4. You are prompted to save the file. Make a note of where the file is saved so that it can be retrieved later.

Importing an Activity File as the Data Source

1. Double click **Extron Conference Room Scheduling Usage Template.pbit**.
2. Power BI launches with a prompt regarding a missing data. Close this dialog to see the skeleton view of the visual shown earlier.

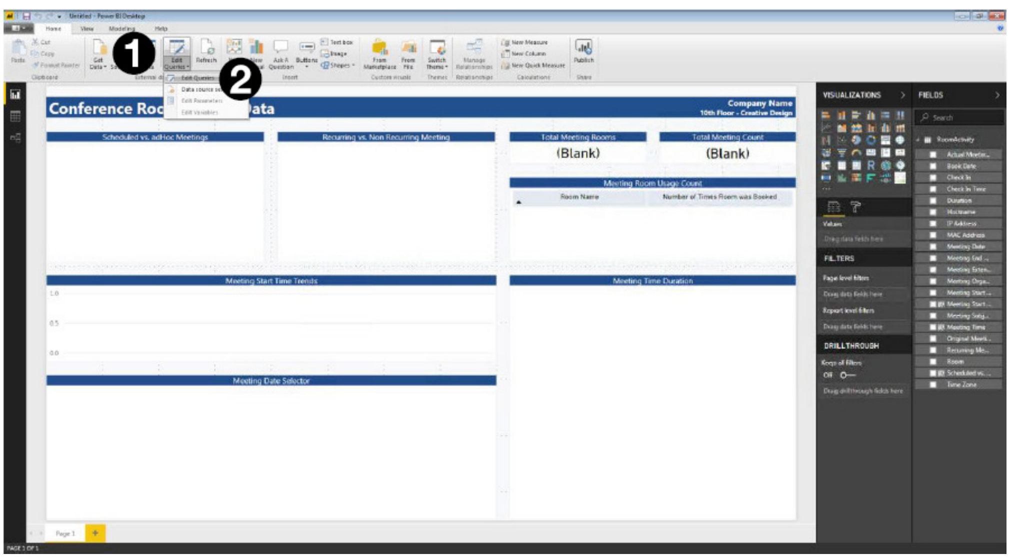


Figure 291. Power BI Selecting Edit Queries

3. From the **Edit Queries** drop-down list (see figure 291, ❶), select **Edit Queries** (❷).

4. The `Edit Queries` page opens.

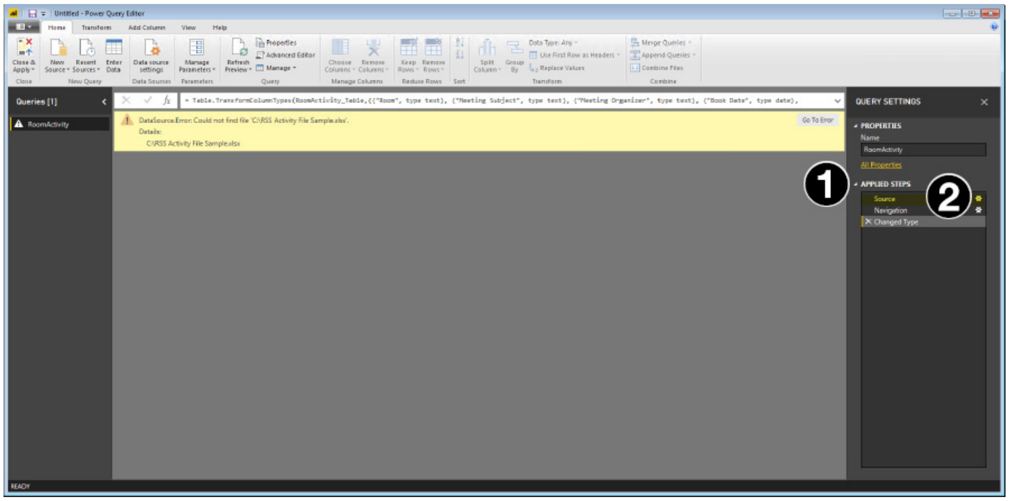


Figure 292. Power BI Edit Queries

5. In the `Applied Steps` section (see figure 292, ❶) of the `Query Settings` panel, click the **`Gear`** icon next to `Source` (❷).
6. Browse to the `Room Activity` file saved in **step 4** of the previous section and open it.

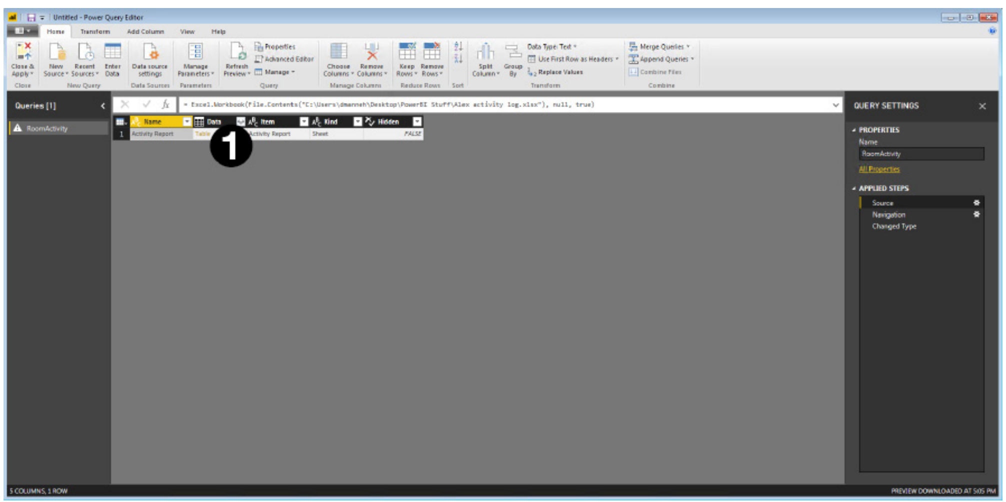


Figure 293. Select Table

7. Click **`Table`** (see figure 293, ❶).

   The `Navigation Step` dialog box opens:

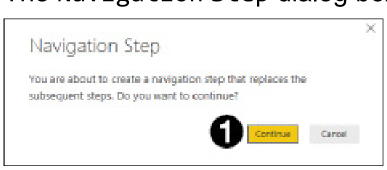


Figure 294. Navigation Step Dialog

8. Click **`Continue`** (see figure 294, ❶).

Your data is displayed in the Power BI Editor.

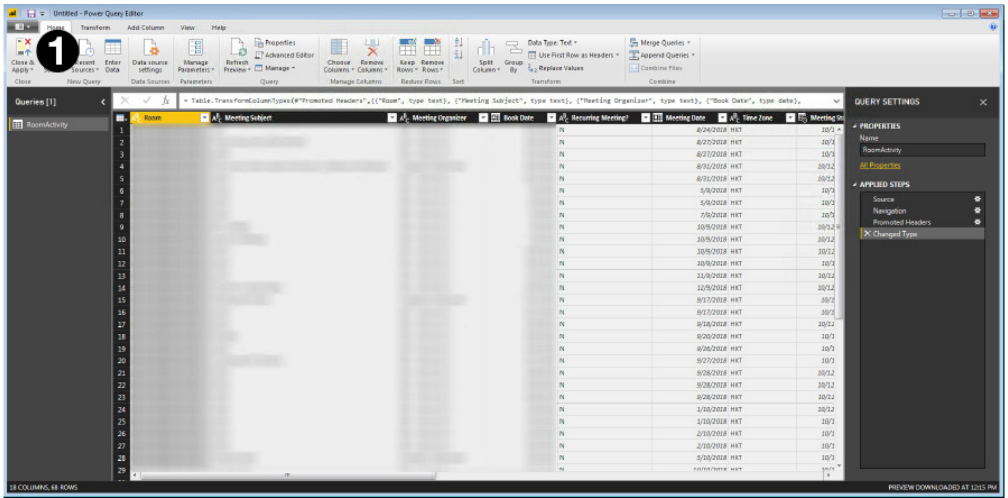


Figure 295. Data Displayed in Power BI Editor

9. Click **`Close & Apply`** (see figure 295, ❶). The dashboard displays your data.

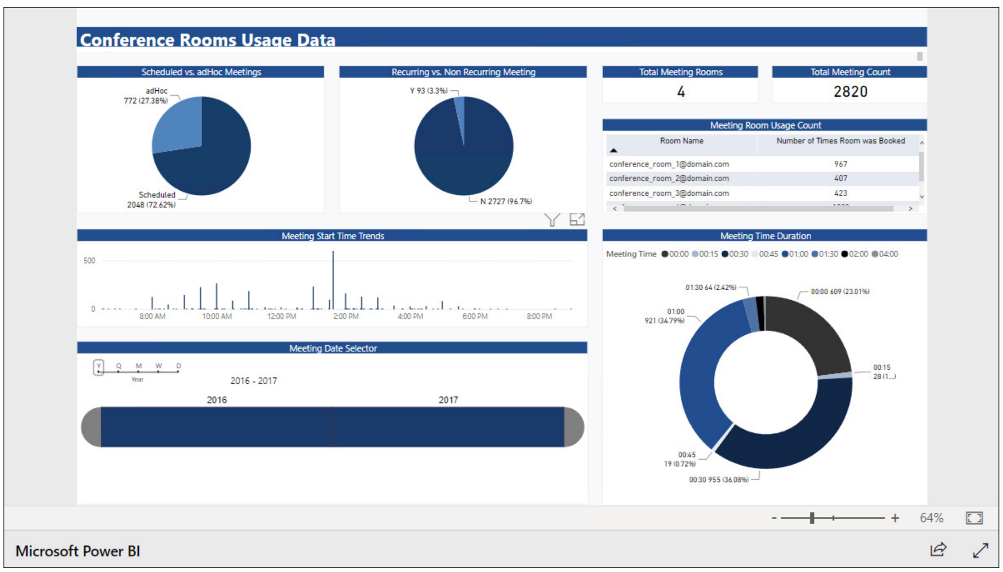


Figure 296. Power BI Dashboard with Data

Retrieving an Activity File via SFTP

This feature allows the user to obtain the raw activity log data over the network without using Room Agent software.

1. Connect to the TLS using an SFTP Client.
2. Enter the admin credentials on port 22022. By default, the user name is `admin` and the password is `extron`.
3. Navigate to the admin directory (`/var/uf/admin`) and locate the activity file (`activity.csv`). This contains all the activity information (including headers) in CSV format.

Secure Sockets Layer (SSL) Certificates

Extron TouchLink Pro control system products ship with factory-installed SSL certificates created by Extron. The factory default SSL Certificate is a self-signed SSL Certificate, seen on products in the factory default state. If you want or are required to use a different SSL certificate at your installation site, please contact your IT department to obtain a valid signed SSL Certificate. You can use system utilities in the Extron Toolbelt software to upload your new SSL certificate to the TouchLink Pro panel. The Toolbelt Help File provides instructions on how to apply an SSL certificate to a control system product.

NOTES:

- You must run Toolbelt as an administrator.
- Some certificates require a passphrase that is created when the certificate is created. If a passphrase is required, you must enter that passphrase before uploading and applying the certificate.

These devices support standard OpenSSL certificate encodings such as .pem (Privacy-enhanced Electronic Mail) and .der (Distinguished Encoding Rules) file types. PEM file types are ASCII encoded and are the required format for uploading to the Extron control product. DER file types are binary encoded and can typically have several file extension variations, such as `.crt` and `.cer`. There are many standard tools that can convert from DER to PEM file encodings if needed.

NOTE: A DER format file must be converted to PEM encoding before uploading it to the button panel, control processor, or collaboration receiver.

To properly create the certificate for uploading to Extron control devices, ensure that the certificate file meets the following requirements:

- contains X.509 certificate information
- contains public and private keys
- uses PEM encoding

NOTE: ITU-T standard X.509 covers aspects of public key encryption, digital cryptography, certificates, and validation.

Contact your IT administrator for more information on what tools and policies are required to obtain or create the SSL certificate and, if necessary, the corresponding passphrase.

IEEE 802.1X Certificates

IEEE 802.1X is a standard that enables port-based network access control via an authentication server. The protocol requires that all devices must be authenticated before gaining privileges to access the secure part of the network.

The Extron implementation of 802.1X supports PEAP - MSCHAPV2 and EAP - TLS methods of authentication. This section of the guide details the Certificate File Requirements and the **Private Key File Requirements** (see page 191) to be used in the system.

Extron provides resources for learning about 802.1X implementation:

The *Extron 802.1X Technology Reference Guide*, available from **www.extron.com**, is the primary resource for background information, system planning, topology, and how to set up these systems.

The *Toolbelt Help file* provides detailed step-by-step information on using the software to set up 802.1X for TouchLink scheduling (TLS) panels and on troubleshooting.

The *802.1X Primer white paper*, also available from **www.extron.com**, provides a general overview of the protocol and its use within a control system.

NOTES:

- You must run Toolbelt as an administrator.
- Machine certificates require a private key file, which can be encrypted.

Certificate File Requirements

PEM (Privacy-enhanced Electronic Mail) file types are ASCII encoded, and they are the required format for 802.1X authentication for TLS panels. DER (Distinguished Encoding Rules) file types are binary encoded and can typically have several file extension variations, such as .crt and .cer.

> **NOTE:** DER encoded files (files with .der, .crt, or .cer extensions that are encoded in DER binary format) must be converted to a PEM encoded file type (.pem) before being used for authentication.

DER encoded certificates must be converted to PEM encoding using a third-party tool. Contact your IT administrator for more information on required tools.

To create the 802.1X security certificate for uploading to Extron TLS panels, ensure that the certificate file meets the following requirements:

- It contains X.509 certificate information.
- It contains a private key (for machine certificates only).
- It is PEM encoded.
- It has a file extension that is .crt or .pem.
- Its file name consists of the following types of valid characters:
  - Alphanumerical (A-Z, a-z, 0-9) characters
  - Some special characters (colon [:], underscore [_], and hyphen [-])

    > **NOTE:** Spaces are not permitted anywhere in the name.

Private Key File Requirements

Private key files are required only when employing machine certificates. Follow these requirements for creating a private key:

- Its file name consists of the following types of valid characters:
  - Alphanumerical (A-Z, a-z, 0-9) characters
  - Some special characters (colon [:], underscore [_], and hyphen [-])
- It has a file extension that is .key or .pem.
- It can have optional encryption (via password or passphrase).

SNMP

Extron control products support Simple Network Management Protocol (SNMP). SNMP facilitates the exchange of basic network management information between network devices. It helps in the monitoring of operations and factors such as packet usage, memory usage, remote password resets, and collection of error information. An information technology administrator can use common IT tools to monitor those factors, as well as look up device location and the name of the contact person for the device.

The SNMP controls within Toolbelt provide a way to enable or disable SNMP. They also allow you to specify related information such as the name of a contact person, the physical location of the unit, and a community name. The text that is specified in these fields is seen by the network community when the unit is queried.

Extron control products support the following security levels:

- Management Information Base 2 (MIB-II)
- SNMPv2c.

> **NOTE:** By default, SNMP is disabled for the TLSI 201. Select the **`Enable SNMP`** checkbox in the Toolbelt **`Utilities`** tab (see figure 284) to enable it.

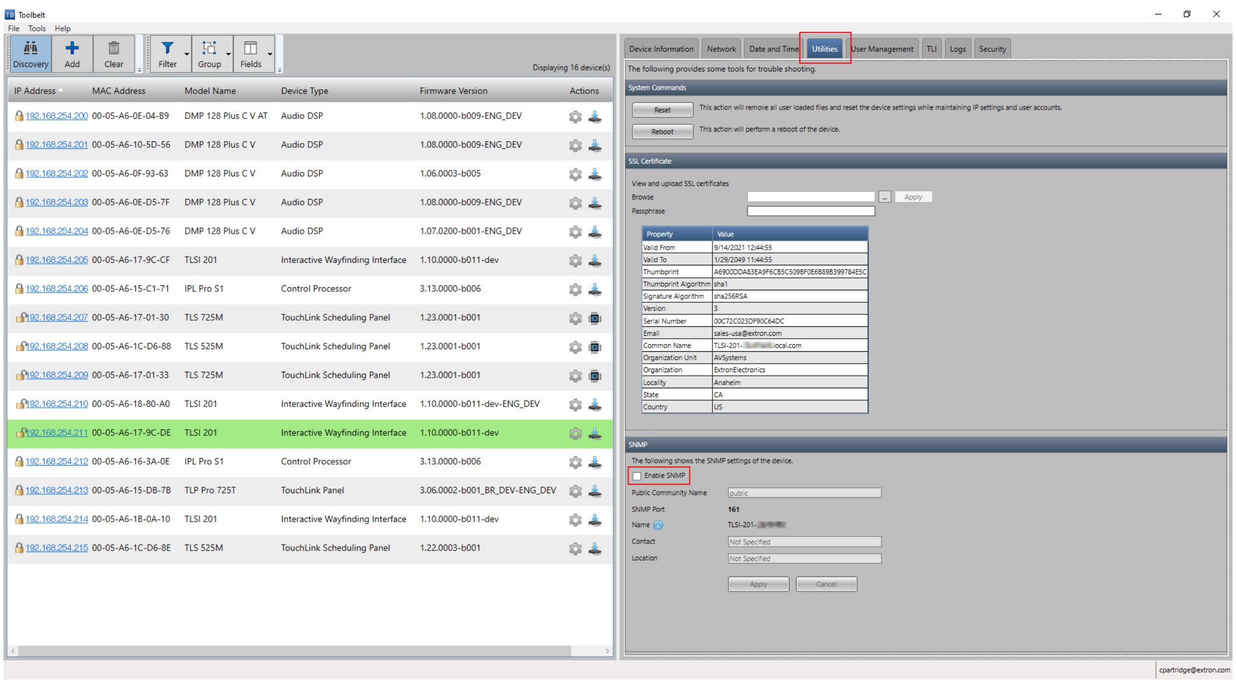


Figure 297. Enable SNMP

Extron Warranty

Extron warrants its powered products against defects in materials and workmanship for a period of three years from the date of invoice. In the event of malfunction during the warranty period, Extron will repair or replace a product to whatever extent it shall deem necessary to restore the product to proper operating condition.

This Limited Warranty does not apply if the fault has been caused by misuse, improper handling care, electrical or mechanical abuse, abnormal operating conditions or non-Extron authorized modification to the product. Extron Electronics makes no further warranties either expressed or implied with respect to the product and its quality, performance, merchantability, or fitness for any particular use. In no event will Extron Electronics be liable for direct, indirect, or consequential damages resulting from any defect in this product even if Extron Electronics has been advised of such damage. Please note that laws vary from state to state and country to country, and that some provisions of this warranty may not apply to you.

Powered Warranty Exception

Everlast™ Power Supplies — Extron warrants Everlast power supplies against any defects in materials and workmanship for a period of seven years from the date of invoice. In the event of a malfunction during the warranty period, Extron will repair or replace the power supply to its original operating condition. Extron engineers will examine the returned product and determine whether the Everlast Power Supply Warranty or Powered Product Warranty applies.

Speakers — Extron warrants Flat Field®, SoundField®, SpeedMount®, Column Array, and System INTEGRATOR® speakers against any defects in materials and workmanship for a period of five years from the date of invoice.

Touchscreens — Extron warrants touchscreen display and overlay components against any defects in materials and workmanship for a period of one year from the date of invoice.

Annotator 300 — Extron warrants the Annotator 300 against any defects in materials and workmanship for a period of five years from the date of invoice.

Non-Powered Warranty Exception

Cable Cubby, Hideaway Surface Access Enclosures and Retractors — Extron warrants Cable Cubby cable access enclosures, HSA Hideaway Surface Access enclosures, and Retractor cable retraction modules for a period of three years from the date of invoice.

Active Cables and Active Adapters — Extron warrants active cables and active adapter cables for a period of three years from the date of invoice.

Cable Termination Tools and Dies — Extron warrants cable termination tools for a period of three years from the date of invoice, excluding the die.

Return Information

Units must be returned insured, with shipping charges prepaid. If not insured, you assume the risk of loss or damage during shipment. Returned units must include the serial number and a description of the problem, as well as the name of the person to contact in case there are any questions.

NOTE: To assure the highest level of service, a return authorization number must be obtained from Extron before products are returned for service. Products must be shipped to Extron, prepaid along with proof of purchase **only** after obtaining a Return Authorization (RA) number from the Extron Customer Support department.

Please contact Extron to receive an RA (Return Authorization) number:

USA:	714.491.1500 or 800.633.9876	**Asia**:	65.6383.4400
Europe:	31.33.453.4040 or 800.3987.6673	**Japan**:	81.3.3511.7655
Africa and Middle East:	971.4.299.1800		

Worldwide Headquarters: Extron USA West, 1025 E. Ball Road, Anaheim, CA 92805, 800.633.9876