Workplace Advisor Subscription

+

Steelcase Find

Administrator Guide

Last updated: May 1, 2019

Steelcase®

Table of Contents

Introduction

This document is a resource for an IT or network administrator planning to install Steelcase Workplace Advisor Subscription, a continuous space measurement tool, and Steelcase Find, a companion app that helps employees find the right space at the right time.

Visit www.steelcase.com/workplace-advisor-subscription to learn more about how these systems work. The Workplace Advisor Subscription Technical Guide overviews system components, the implementation journey and provides technical specifications.

Workplace Advisor Subscription

The Role of IT

One of the most important pieces of hardware infrastructure required for Workplace Advisor Subscription is the Steelcase gateways. These gateways are responsible for forwarding on occupancy data detected by our sensors to the Microsoft Azure® platform.

It is important for the professionals in your IT department to understand that they will be responsible for providing the network connections at each gateway location as well as the installation of these gateways. If a firewall is in use to control outbound traffic, it will need to allow outbound network connections. Please refer to the Steelcase Insight Brief, **Networking Requirements and Guidelines**, for further details on this topic.

Hardware

The Workplace Advisor Subscription system involves the installation of two pieces of physical hardware that will reside on your network: sensors and gateways.

SENSORS

Wireless sensors installed in the workspace work together to detect motion with passive infrared (PIR) technology. Each sensor securely and wirelessly sends occupancy information to a gateway via Bluetooth Low Energy (BLE v4.2 - 2.4 GHz). Sensors are powered via a CR123A battery that is rated to last for three years.

GATEWAYS

Gateways send secure sensor data across the internet to the Steelcase platform. Gateways receive power through the Power over Ethernet (PoE) 802.3af specification. The gateways run a custom built version of the Linux operating system.

Setup and Installation

Please refer to the Steelcase Insight Brief, Networking Space Measurement Tools, to understand network requirements, options and specifications.

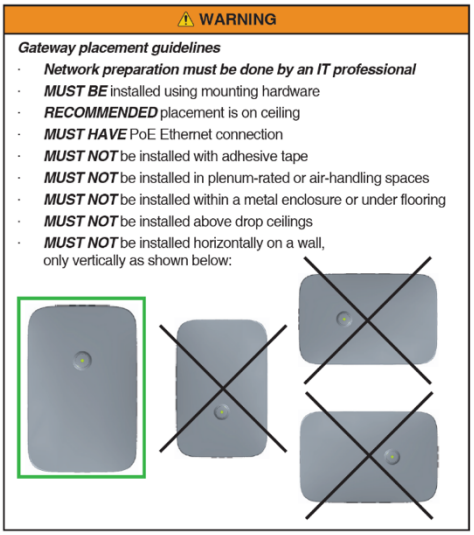
SYSTEM AND NETWORK REQUIREMENTS

- Wired PoE network connection for each gateway
- Gateways will need access to the internet to communicate with the platform
- If a firewall is in use to control outbound traffic, it will need to allow outbound network connections on the ports listed below in the Gateway Network Information section
- Gateways will need to be able to access a DHCP and a DNS service

BEFORE YOU BEGIN

Prior to Installation

- Steelcase dealer design team gives planned locations for gateways to your organization's IT
- Review gateway placement guidelines



What's Included

- Gateway
- Wall/ceiling mounting bracket
- Acoustic tile/drop ceiling backing plate
- Mounting hardware (not shown):
    - 2 self-tapping screws
    - 2 M3 Screws

INSTALLATION FOR FIXED CEILING OR WALL

Before installing, record the gateway media access control (MAC) address and location where device is installed on the installation plan provided by the Steelcase dealer so you can use the Workplace Advisor Subscription Space Manager to update each gateway name/location

1. Slide wall/ceiling mounting bracket off the back of the gateway
2. Attach mounting bracket to wall/ceiling with two self-tapping screws
3. Slide gateway back onto mounting bracket

For additional installation options please refer to the gateway assembly instructions included in your box of gateways.

POST-INSTALLATION

1. Log in to Workplace Advisor Subscription and navigate to the Space Manager tab (URL, username and password will be provided by Steelcase or your Steelcase dealer)
2. Confirm that all gateways are online
3. Add a note for each gateway indicating the location where it is physically installed (use MAC address noted in Installation step 1)
4. Alert your Steelcase dealer that gateway installation is complete; after this step, sensor installation scheduling can begin

TROUBLESHOOTING

Issue: LED Ethernet indicators not on

Possible reason: Network switch port is not live/active

- Action: Verify connection by plugging laptop or other device in to check network activity (LEDs will blink)
- Solution: Network technician confirms/activates jack

Possible reason: Broken network cable

- Action: Test cable from data drop to PoE splitter
- Solution: Cable must be repaired or replaced

Issue: Gateway does not connect to platform

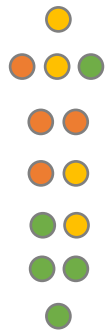
Possible reason: Network switch is not providing internet activity to reach cloud platform

- Actions: Refer to LED status indicator table below to see which port is not connected; plug in laptop or device to access the internet
- Solution: Network technician resolves

Possible reason: Outbound HTTPS or MQTT is blocked

- Action: Network technician confirms
- Solution: Network technician resolves

LED Status Indicator

LED COLOR AND BLINK PATTERN		DESCRIPTION
Boot Sequence		
	Solid yellow	Booting kernel
	Cycle through red, yellow, green (1 sec each)	Kernel started successfully, executing startup scripts
	Blinking red	Waiting for IP address (DHCP)
	Blinking red and yellow	Waiting for network time (NTP – Port 123)
	Blinking green and yellow	Connecting to SBS servers (HTTPS – Port 443)
	Blinking green	Connecting to Steelcase servers (MQTT – Port 8883)
	Solid green	Connected to Steelcase servers, all ports correctly configured
TROUBLESHOOTING INDICATORS		
	Solid red	Critical fault (security fault)

Privacy and Security

DATA STORAGE

- Software, gateways and sensors are rigorously penetration tested and reviewed by a third-party security partner
- The system has no ability to make or permit inbound connections to your network
- Network activity and data are continuously monitored for security events with a 24/7-staffed third-party security partner
- Advanced firewall and web application firewalls are strictly controlled and monitored
- Wireless adapters and information are secured in transit from the sensors to the gateways and are protected by AES128 encryption and authentication
- Ethernet adapters and network traffic information are secured in transit and encrypted from the gateway to the Steelcase platform with TLS 1.2 and up to 2,048-bit SHA256
- Gateways accept “pairing” and registration from devices during installation only, and refuse pairing and registration from devices that are not sensors
- Gateways are protected; no default passwords or keys are used, and no unused services are enabled

SOC 2 FRAMEWORK

To safeguard the confidentiality and privacy of the data collected with Workplace Advisor Subscription and the Steelcase Find app, Steelcase uses the Service Organization Controls (SOC 2 Type 2) framework. This standard was developed by the American Institute of Certified Public Accountants and, much like accepted financial standards, includes third-party audits.

Workplace Advisor Subscription and Find systems will be audited annually against the SOC framework by independent third-party auditors. This audit is based on security and privacy principles for each service. The certification reports and summaries will be available to Steelcase Workplace Advisor Subscription and Find customers once complete.

In addition, Workplace Advisor Subscription and Find meet the requirements of General Data Protection Regulation, or GDPR, the new global standard for privacy protection effective in Europe as of May 2018. While GDPR is expressly designed to protect the privacy of people in Europe, Steelcase complies with this standard for all of our Smart + Connected products serving organizations around the world.

FAQs

WORKPLACE ADVISOR SUBSCRIPTION

How many gateways are needed? This can vary; an average installation involves approximately five rooms per gateway or 30 sensors per gateway. Room proximity to the gateway can also affect this count. Rooms next to each other can use the same gateway; if they are too far apart they will require separate gateways.

Can gateways be installed above ceiling tiles? We recommended installing gateways 7 feet or higher above ground. Gateways cannot be installed in the floor or above ceiling tiles.

What is the range of a gateway? Gateways currently support a range of about 13 meters (45 feet).

What is a PIR sensor? PIR stands for passive infrared radiation. Sensors equipped with PIR technology measure thermal radiation being emitted from objects within a certain range. They are most often designed to detect motion.

What data is being collected? Low risk, anonymous occupancy data. This information is sent to the secure Steelcase platform powered by Microsoft Azure®, where it is processed through our algorithm to display real-time occupancy, historical trend data and information about space utilization.

What authentication is used when signing into the dashboard? Workplace Advisor Subscription uses the Office 365/Microsoft account that you designate to provide authentication for logging into the dashboard.

NETWORKING

What is an IP address and DNS? An Internet Protocol (IP) address is a network address consisting of 4 bytes usually presented in dotted decimal notation such as 12.250.0.100. The most common type of IP address used by corporate networks today is IPv4, although some use IPv6. An IP addresses is similar to a phone number in that the numbers are often difficult to remember but are required to send and receive communications.

A Domain Name System (DNS) works like a phone book that maps easily remembered names to the more difficult to remember numeric IP addresses that computers understand. An example is ftp.steelcase.com which maps through DNS to a public IP address of 198.105.65.27.

Why DHCP vs. Static IP? Dynamic Host Control Protocol (DHCP) is an automated method of assigning IP addresses to computers and other networked devices. On many devices, a static address can be manually assigned, but this is difficult to manage and many newer IoT devices do not support this configuration method. Smart and connected products do not support static IP addresses. Organizations generally assign a dynamic IP address through DHCP when devices connect to their wired or wireless networks. They are also usually able to reserve and allocate static IP addresses using DHCP if there is a requirement for a static (unchanging) IP address. DHCP is not considered less secure by most network engineers as the connecting device is assumed to have access permission if it is able to plug into a hardware port or if it is provided the wireless security key.

VLANs and segmentation routing – why does it matter? VLANs and network segments are used to limit the size of a network broadcast domain. By convention, a device that sends out a broadcast will be detected by every other device on the same layer 2 network. If a segment is too large (more than several hundred devices), devices are overloaded with broadcast traffic and significantly slowed. Routing is a higher, layer 3 protocol, which directs packets (traffic) to and from other broadcast domains based on their IP (layer three) addresses. Layer 3 devices are typically routers or layer 3 switches. VLANs and network segments are designed by the network architect both to create manageable broadcast domains and to isolate network segments from each other. High security segments, such as HR or payroll, can be isolated for limited or no connectivity to other network segments, such as sales and general operations. Traffic can also be segmented to isolate network segments hosting potentially high-risk clients, such as a guest network segment or an IoT network segment, from business-critical network segments that assume all connecting clients are safe.

802.1x – what is access control why don't many have it? 802.1x is a protocol for port-based network access control (NAC) that specifies device access to a wired or wireless network. Early systems were designed to inspect the status of a connecting device (such as whether it had current antivirus signatures) and determine what network it would be allowed to connect to. These early products took a lot of effort to manage and did not penetrate much of the market. Most popular network equipment and computers today support 802.1x even if rarely used. The "handshake" required for 802.1x, as well as the cost and processing power required for implementation, has made its adoption into IoT ecosystems unlikely. Simpler alternatives, such as 802.1ar, are being promoted; however, it may be a few years before a standard is accepted by the market.

How do DHCP and NTP work together? Every device on a data network needs an IP address and devices often need accurate date and time information to perform as expected. Today, most devices connected to a network are automatically provided an IP address by the network's Dynamic Host Configuration Protocol (DHCP) service. When a typical device connects to a wired or wireless network, the DHCP service provides, at minimum, three things: the IP address that the device should use, the gateway or default router IP address to communicate with other devices and the subnet mask of the layer 2 network (which determines the size of the local network). Usually other settings are available to the device, such as the IP address of DNS servers, the domain name of the network, the IP address of a Network Time Protocol (NTP) server and the lease time or length of time the IP address is valid before expiration. NTP is a means for the device to synchronize its own time and date with a known accurate, precise time source. Such sources are often hosted on the internet but they may also be located on your organization's network.

Smart and connected gateways can receive their IP address information and other parameters through only through DHCP, as there is currently no mechanism to set this information manually. The NTP server address is hard coded by Steelcase, but it may become possible to set through DHCP in a future software release.

What are private (RFC) and public addressing? The IPv4 address space allows for only 4 billion total addresses available worldwide, and every public IP address must be globally unique, so the IANA (Internet Assigned Numbers Authority) that controls these addresses set aside some addresses for use in private networks. These private addresses are not routable on the public internet. The ranges of these private addresses are typically 10.*.*.*, 172.16-31.*.*, and 192.168.*.*. Network Address Translation (NAT) is used to funnel the outbound traffic to a small group of public IP addresses (Steelcase uses 198.105.64-79.*). RFC 1918 addresses are not usable directly on the internet and must be mapped to a public IP address in order to function.

What is NAT? Network Address Translation is a technique to map internal IP address ranges to an organization's small range of publicly routable IP addresses. This function is usually handled by a firewall or router. A single public IP address can hide more than 65,000 private addresses using a technique called Port Address Translation or "one to many NAT." NAT obfuscates the structure and internal addressing of the private network but should not be relied on as a method of securing the network.

What is the value of PoE and what specs should be considered? Power Over Ethernet is a convenient way to deliver power over the existing Ethernet network wires and can eliminate the need for a power adapter by an end device such as a camera, a WiFi antenna or a Smart + Connected gateway. It can be very expensive for an organization to run power to a device mounted in the ceiling so PoE is a great alternative. Switches that provide PoE are significantly more expensive than switches that do not provide PoE, so we do not assume that an organization uses switches with PoE ports. An alternative to a switch providing PoE is for an organization to use a power injector between the Ethernet port and the Ethernet cable going to the device. PoE sources are always rated on their power capacity, both for the individual port (PD) and the entire switch.

There are four power level types: (typically 40-50 48V DC but can range 44-57 V DC)

- Type 1 - max 13 watts
- Type 2 - max 26 watts

- Type 3 - max 51 watts
- Type 4 - max 71 watts

A powered device (PD) must always consume fewer watts than the capacity of the PoE supply. Steelcase gateways consume a maximum of 10 watts so we are compatible with any PoE supply type.

How are Ethernet speed and distance handled? Most organizations use copper wiring for Ethernet, generally limited to 100 meters from their distribution closet to the device without special equipment. The IT team will handle the data jack drop and ensure it is situated within the right margins for distance. Because the installation takes place within an office environment, margins should not be an issue. Cost is a consideration: running a data jack into the ceiling can cost $200 per drop. Some organizations also struggle with keeping enough port capacity available and must request additional drops, which can cost further time and money. Our equipment is set to auto-negotiate Ethernet speed and duplex and is compatible with standard 10/100 and gigabit Ethernet ports.

GLOSSARY OF TERMS

Data network: An electric or fiberoptic system for carrying information to connected nodes. These nodes may be computers, phones, printers, IoT devices or even medical devices. Originally simple messages were carried over networks, but today voice calls, movies and even medical imaging are often carried by networks.

BYOD: “Bring Your Own Device” refers to the modern reality that many people bring personal or individually purchased devices to the workplace, drawing on shared bandwidth and requiring additional consideration and support for compatibility.

IoT: “Internet of Things,” a term coined by Kevin Ashton, MIT Auto-ID Lab cofounder, in a presentation to Proctor & Gamble in 1999. It refers to the network of computing devices that are embedded into a wide variety of real-world objects, enabling these objects to send and receive information. The resulting system(s) of smart, connected objects present new possibilities for adding value and increasing efficiency.

LAN: Local Area Network is a network typically for a building or part of a building. The most common Ethernet wiring for such a network is copper and can travel up to 100 meters (Cat-5, Cat-5e, or Cat-6 twisted pair). Ethernet also can run over fiber, which today can run for miles but is more expensive.

WAN: Wide Area Network is the connection of LANs over a significant distance. The Internet is an example of a very large WAN. WAN connections include dedicated links between buildings or campuses and can reach across cities, countries or even continents.

VLAN: Virtual LANs allow multiple network segments to travel across the same wire by tagging a data packet with a VLAN ID. The concept is to virtualize the network by using software to create different networks without having to buy individual pieces of network hardware for each segment.

SDN: Software Defined Network.

L3 switching: Layer 3 switching.

PoE: Power over Ethernet allows a port to send data and power over the same wires so that devices like cameras and WiFi antennas do not need power through a separate adapter.

MAC address: Media Access Control address is a globally unique 6 byte (48 bit) Ethernet hardware address used by IPv4 and IPv6 and usually printed on a label affixed to the device it represents. It is a layer 2 address within a single IP broadcast domain. MAC addresses are visible only on a layer 2 network by other devices on the same network within a subnet boundary. The MAC address is used by DHCP to handle dynamic IP address assignment and to handle static IP address reservations provided by DHCP. The MAC address is also used by layer 3 devices such as routers and layer 3 switches to address packets to the correct device. IPv6 addresses use a similar concept called Interface Identifier and often use the MAC address to create a full IPv6 address. IPv6 is not supported yet by Steelcase Smart + Connected products because few enterprises support IPv6 on their internal networks.

IPv4: Internet Protocol version 4 was developed in 1983 as a means to allow computers to communicate with each other over great distances. It is still the most common protocol for interconnecting different networks around the world. Other protocols – including AppleTalk, DECnet, IPX, and NetBEUI – have since faded from use. IPv4 is limited to a total of slightly more than 4 billion possible unique IP addresses, however allocation of addresses is not very efficient so that the availability of unique addresses for organizations is a challenge. For instance, Steelcase has a range of 4,096 unique IP addresses, and we use 5% to 10% of them.

IPv6: Internet Protocol version 6 was developed to address shortcomings of IPv4, such as a lack of possible IP numbers and security. The number of available IP addresses has been compared to “more than 10 million trillion times the total number of grains of sand on all the beaches in the world.” IPv6 is in use today on the internet and used by cell phone companies to deal with the growing number of phones and devices. Very few companies use IPv6 for their internal networks. Steelcase Smart + Connected products do not yet support IPv6.

Private VLAN: Also known as port isolation, Private VLAN restricts traffic from a device port to a specific destination port. While effective, using a private VLAN is cumbersome and does not scale well in a large network where there are lots of ports requiring restriction.

ACL: Access Control List.

802.1x: A standard for port-based network access control (PNAC). IoT devices do not generally support 802.1x as supplicants, and new variants such as 802.1ar have been proposed although they have not been widely adopted yet. Steelcase will continue to monitor standards for adoption.

Steelcase Find

The Role of IT

Steelcase Find is a mobile app that helps employees within a space see all available spaces that meet their needs, secure a space and invite others to join. The app requires certain Office 365 permissions that must be granted by someone within your organization who has “Global Administrator” privileges within your tenant. The complete list of permissions is included in the “Room Preparation in Office 365” section of this guide.

IT is also responsible to provide level 1 support for users of Find within their organization.

Setup and Installation

Successful deployment of Find requires properly setting up your Workplace Advisor Subscription platform and provisioning the Steelcase Find app. Setting up the platform correctly may take some time, depending on the size of your Workplace Advisor Subscription installation – it’s important to do this well so that once the app is deployed employees using it have a great experience.

PREREQUISITES

Before you begin setting up Steelcase Find for your users, please make sure that these two dependencies are met:

1. You have a valid Workplace Advisor Subscription account
2. You have signed and returned the Steelcase Find Addendum
3. The calendaring service that you use is Office 365 cloud

ROOM PREPARATION ON WORKPLACE ADVISOR SUBSCRIPTION DASHBOARD

To ensure that the Find app displays all rooms correctly you must verify that they are set up properly on the Workplace Advisor Subscription dashboard. Settings are edited and verified on the platform by navigating to a space within the “Space Manager” tab on the platform. This includes verifying the following space information:

- The amenities for each space are correct
- Space type is set to “Room”
- The reservable field is set to “Yes”
- The room’s email addresses are correctly entered on the platform

Any changes to a space’s traits or amenities are polled by the Find app on a weekly basis. It is possible to force an update to these changes by signing out of the app and signing back in.

If these settings are not adjusted correctly, users of the Find app will have a less helpful experience.

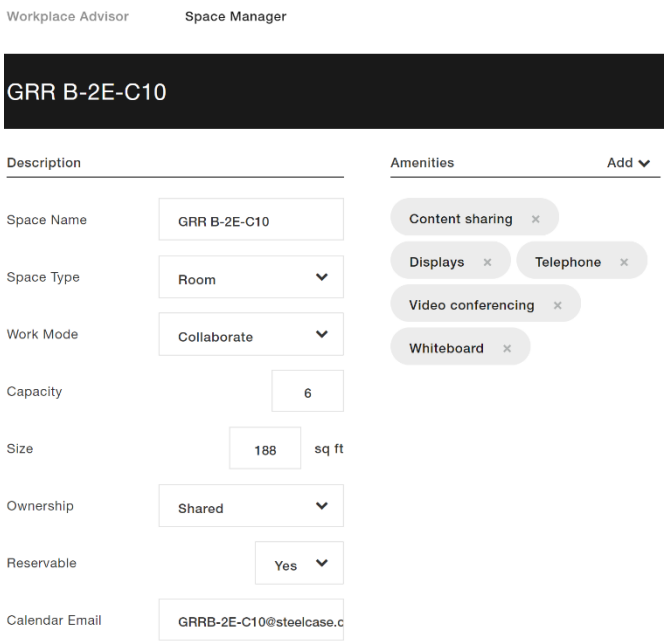
ROOM PREPARATION IN OFFICE 365

A few steps must also be completed within your Office 365 environment to allow proper functionality of Steelcase Find.

All the rooms that you want enabled in Find must have a valid O365 email address and their room calendars must be shared with all users.

It is also important that your rooms are setup with the proper O365 permissions so the find app can read room availability. The permissions of each room need to be set to a level of “Reviewer” or higher.

Rooms with “Availability Only” or “Limited Details” are not reservable through the Find app.



Note: Your room email addresses do not need to be licensed. If your users can book the rooms through Outlook, the Find app will work.

Note: It may take up to 24-48 hours for room permission changes in Exchange to propagate to the Find app.

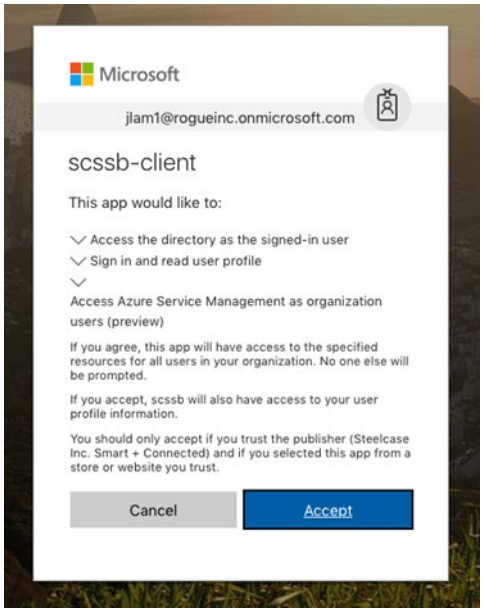
Provisioning the Find app: Steelcase Workplace Advisor, Steelcase Find, and our ecosystem of features have been built on a microservice architecture. As such, Azure AD will ask you to approve each service for your users. Each piece has a purpose essential to the system as a whole. Below are approval links for each service that requires your IT admin’s approval and a brief description of what each service does.

This will allow future features such as Auto Release and Auto Reserve to access the calendar events in O365 Exchange for configured rooms to add/edit meetings.

Important: The steps on the next page must be performed by someone who has Global Administrator privileges within Office 365.

In addition to this the links must be clicked in the correct order to avoid issues.

After visiting each of the following links you will be presented with a screen similar to that shown here. Please accept all of the links in the order in which they appear.



Note: After accepting these links they will return a blank page. please navigate to the end of the URL and confirm it ends in "true" or "accept."

1. **Scssb Approval** - This service stores and manages the space hierarchy including rooms, locations, devices. Scssb was developed by Microsoft in partnership with Steelcase.

2. **Smart-spaces-prod Approval** - Smart spaces is an adapter service that encapsulates scssb and adds some Steelcase-specific customizations to it.

3. **Nro-algorithm-prod Approval** - NRO stands for near real-time occupancy. The algorithm service contains implementations of the algorithms put together by Steelcase's data science team to determine an occupancy confidence score for a space over a given time period.

4. **Nro-webservice-prod Approval** - NRO Webservice provides NRO data access to the rest of the ecosystem.

5. **FindNroService-prod Approval** - Originally developed for Steelcase Find, this service correlates occupancy data with a room's calendar of meetings and makes changes to the calendar to align with the occupancy.

6. **SteelcaseFIND prod Approval** - This allows your users to use the Steelcase Find mobile app, pending some configuration on the Steelcase side.

DOWNLOADING THE APP

The Steelcase Find app is a free download on both the iOS App Store and the Google Play Store.

Direct users to download the app from the app store:

- Android: https://play.google.com/store/apps/details?id=com.steelcase.find
- iOS: https://itunes.apple.com/us/app/steelcase-find/id1348824266?mt=8

Upon launching the app, users will sign in with their O365 credentials. They will also have the option to opt into push notifications. Steelcase Find supports iOS 9+ and Android OS 5+.

Steelcase Find + RoomWizard

The Steelcase Find app and RoomWizards do not communicate directly with one another. Instead, they both use Office 365 as an intermediary so that when you book a room through the Find app your reservation is displayed on a RoomWizard. With this in mind, here are some common behaviors that can be expected.

- When booking a room through the Find app it may take a few minutes for the reservation to show on the RoomWizard unit. This is dependent on what the poll interval is set to on the RoomWizard itself.
- If a meeting is extended from the RoomWizard the event is switched to a 'RoomWizard account' and the Find app no longer has visibility to it because it looks for the event tied to a user's account. You will no longer be able to end the reservation or receive notifications about the meeting via the Find app when this occurs.
    - This same behavior will occur if you check in to a meeting that was created through the Find app via a RoomWizard.

Troubleshooting

Are users experiencing issues with the Find app? Try these fixes for common situations.

Room is not showing up as reservable in the app. Only rooms that are being sensed by Workplace Advisor Subscription are supported by Steelcase Find. Ensure that rooms include sensors are configured correctly on the Workplace Advisor Subscription dashboard:

- Room has an email address associated with it
- Room has the reservable option set to “Yes”
- Room’s space type is set to “Room” and not “Open plan”
- Find must also interact with Office 365. Ensure that:
- The room’s email address is associated with a server
- The room’s email address is not a duplicate

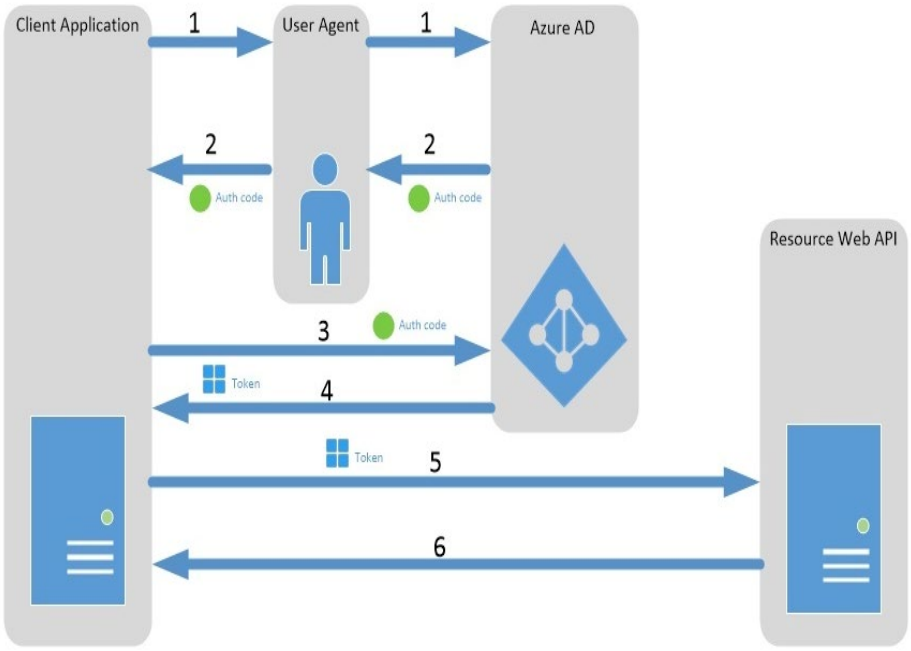
User is not able to make a reservation on a reservable room. Ensure that the room is configured on your Office 365 tenant in the following way:

- The room’s calendar is shared with all users
- The room’s email address is associated with a server
- The user has privileges to book the room

Privacy and Security

OAUTH2 WORKFLOW

The Steelcase Find app uses OAuth2 for authentication and authorization. This diagram illustrates the authorization grant flow.



The interaction among the layers and components are depicted by the numbered circle in the diagram.

1. Client applications use OAuth2 to obtain a bearer token. User is prompted to enter login/password when the app is first opened or after the token has expired.
2. If the login is valid, a bearer token will be returned to the client app, which it will subsequently use to invoke against the Calendar micro-service.
3. The client app will invoke the CalendarRestfulApi using the bearer token acquired.
4. The CalendarRestfulApi will have authentication setup for the on-behalf of pattern. It obtains a second bearer token using the first one passed in from the client app, the Graph API client credential and the user assertion. This second token allows the service to obtain data from the Graph API based on the user privileges in O365.
5. Once this second token is acquired, it is added to the header for all calls against the Graph API.
6. The Graph APIs then return the data based on the user's privileges back to the service. The service returns the response back to client application.

SECURITY

Our layered defense strategy combines protective tools with active monitoring to keep both you and the organization you work for secure. We continually evaluate our protections and adopt industry-best practices to offer a reliable, tailored approach to privacy that includes the following:

- Steelcase Find is rigorously penetration-tested and reviewed by a well-respected, third-party security partner.
- Steelcase Find utilizes iOS and Android embedded encryption.
- Network and behavioral activity and data are continuously monitored for security events with a 24/7-staffed third-party security partner.
- Advanced firewall and web application firewalls are strictly controlled and monitored.
- Network traffic is secured in transit and encrypted from the device to the Steelcase platform with TLS 1.2, and 2,048-bit SHA356.

PERSONAL DATA

Steelcase is committed to protecting your privacy. We do not collect or share personal data unless you authorize it.

How we use data:

- We use anonymized data to track app usage
- We do not track individuals or store data about your meetings
- No personal information is reported back
- The login email your users provide is used to facilitate our app and services, and to send occasional communications
- For additional details on privacy and security please visit the Workplace Advisor and Steelcase Find EULA and Privacy Policy pages:
    - https://wpa.steelcase.com/eula
    - https://www.steelcase.com/steelcase-workplace-advisor-privacy/
    - https://www.steelcase.com/steelcase-find-privacy-security/

CONTACT US

If you encounter an issue or have a question or request, please contact Steelcase CX (TechCX@steelcase.com) or 888.STEELCASE (888.783.3522)

(Outside the U.S.A., Canada, Mexico, Puerto Rico and the U.S. Virgin Islands, call 1.616.247.2500)

steelcase.com

Steelcase®