IC 360

St. John Ambulance

Co-Managed Services Manual

How to Reach Us

Business Application Support (D365, SR365, Web, LMS, VMS) and SharePoint/Teams

servicedesk@sja.ca
1-844-SJA-AIDE (752-2433)

All Other Requests

help@ic360.ca

Use your work email only. Personal email is ignored for security reasons.

Urgent Requests

Call 613-319-5043 option 1

Leave a voicemail and we will respond asap.

Escalations

escalation@ic360.ca

If an issue requires escalation, use this email.

General Feedback

feedback@ic360.ca

If there is anything we should be doing better, we want to know!

Table of Contents

Introduction

Your organization has subscribed to “Managed Services”. Managed Services is a term used to describe the outsourcing of your IT department.

We will manage, monitor, and support your IT systems, specifically:

- Microsoft accounts and data (e.g., Outlook, Teams, OneDrive, etc.)
- Corporate computers and phones (device management)
- Network equipment and configuration

SJA uses Microsoft 365

Your workplace is set up to be cloud-first, which means your computers are managed over the internet. We will provide an email address and password for your Microsoft 365 account. This is used to access all of the apps at www.office.com, and/or log in to your corporate Windows computer.

Our Services

Microsoft 365 Training

Microsoft has excellent, free online training resources.

We partnered with Microsoft to offer dedicated training sessions for groups of 30 or more. If interested, kindly email us at help@ic360.ca.

To access Microsoft training:

https://support.Microsoft.com/en-us/training

Our Policies

Policies Overview

Our standard practices intend to meet the following objectives:

1. Consistent and positive user experience
2. Optimized security
3. Minimal need to log helpdesk tickets
4. Efficient use of staff time

Managing User Accounts

We strive for a few best user accounts practices:

- *No Shared Accounts*
  Since we require Multifactor Authentication (MFA), shared accounts are not possible. If multiple people require access to one email address, we will create a Shared Inbox. This is much simpler for everyone and does not require a license.

- *No Recycling of Accounts*
  Every individual should have a fresh account when starting. If previous data is needed, that data should reside in a Teams/SharePoint and/or a Shared Inbox. Recycling accounts creates privacy and security risks and makes onboarding more difficult.

- *One Account per Person*
  Except for Global Administrators, each employee should have a **single** account. If multiple email addresses are required, this can be accomplished with Shared Inboxes and/or email aliases.

- *Changing Permissions*
  We often receive additional access requests, such as delegating access to another email inbox or being added to a shared inbox or team. For such changes involving permissions, we need written approval for the change.

- *Onboarding Users*
  Email help@ic360.ca and provide the following details (ideally at least a week before they start):
    - Full name
    - Title
    - Phone number
    - Desired email address
    - Any Teams or Groups to join them to
    - Who they report to (their Manager/Supervisor)
    - Start date
    - Do they require any hardware to be ordered?

- *Offboarding Users*
  Email help@ic360.ca and provide the following details (ideally at least a week before they depart):
    - End date
    - Do we wipe/reset any devices? If so, we need the computer name or the serial number of those devices.
    - Do we reassign their OneDrive data to anyone or just delete it?
    - Do we convert their mailbox to Shared Inbox and reassign or just delete it?

- *End-User Contact Information*
    - We require an email and phone number for all users. When we create a ticket, the automatic response will share what we have on file.

Patching

We have policies to automate the patching of corporate computers. Computers must be rebooted at least once per week and left on and connected to power overnight as much as possible. If computers are not being rebooted, we may need to force a reboot to ensure patches are being completed and devices are kept secure from known vulnerabilities.

When computers require a reboot, you will receive notifications until the computer is eventually automatically rebooted.

Regularly rebooting is critical to computer performance and security.

Browser Support

Figure 1

We support the Microsoft Edge browser. You may use other browsers, but they may expose computers to security risks. Additionally, we cannot backup browser data from other browsers. If you use Chrome, log in to it with your Google/Gmail account to sync the browser data.

Troubleshooting Limits / Computer Resets

If we are experiencing an intermittent issue or unknown bug/error message, this can often be due to a corrupt installation of Windows. If we cannot resolve the issue within one (1) hour of troubleshooting, we may reset the computer, ensuring a clean operating system installation.

Exclusions from Regular Support

Anything that represents an Add, Move, or Change, is outside the scope of regular support. This is not to be restrictive but to ensure the sustainability of our services. We can help with the full range of IT issues and projects but cannot work them into a fixed support budget, as it is dedicated to addressing regular support requests only.

Examples of exclusions include but are not limited to:

- Deploying a new application
- Designing new Teams or SharePoint structures
- Moving to or opening a new office
- Redesigning security protocols
- Changing your email address/primary domain
- Upgrading from Windows 10 Home to Pro

Other support exclusions:

- Support of out of warranty equipment
- Personal device support, aside from accessing web-based resources (e.g., www.office.com)
- Personal internet connections: performance and settings are to be supported by the Internet Service Provider
- Home network configuration, performance or troubleshooting
- Smart devices (e.g., smart speakers, lights, etc.)

Remote Monitoring and Management Software (RMM)

- *What is it?*

We use the Datto RMM Agent to manage and monitor corporate computers. It gathers real-time information about the devices' health and status.

RMM is only for corporate computers, not personal ones.

- *Why do we need it?*

The RMM provides the same level of access a traditional IT department would have, but over the internet. This enables faster remote support.

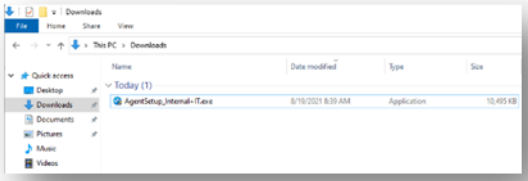
It can proactively monitor a device, deploy patches and policies, create alerts, execute scripts, run scheduled jobs, or enable a remote connection to the device. It grants IC 360 remote control access as well. We will always ask for permission before taking over a device. There is also an audit log of all technician access of devices.

- *How to install the RMM?*

If you need to manually install the RMM, we will email you a link to the file. The installation is quick and does not provide much feedback or confirmation post-installation. (It will just start running in the background.) You will see an icon in the system tray (down by the clock on Windows or along the top menu bar on Mac).

- *Remote Management Installation – Windows*

1. Download the agent by clicking the link provided in your email.
2. Go to the "Downloads" folder and double click on the downloaded ".exe" file.



3. Click on "Yes" to continue, and the agent will be installed automatically.
4. To verify, click on "^" at the bottom right corner of the screen and look for this icon (it will be blued briefly, and after a few minutes it will display our icon).

Figure 2

New Computer Setup Steps

Need Help?

If you are experiencing **any** issues, contact us at help@ic360.ca.

If you need assistance with following our instructions, we can arrange a call.

Step 1: Set up your Microsoft 365 Account

On any computer, go to www.office.com and log in with your new password. It will force you to choose a new password, as well as follow steps to set up multi-factor authentication (MFA).

Step 2: Setting up Multifactor Authentication (MFA)

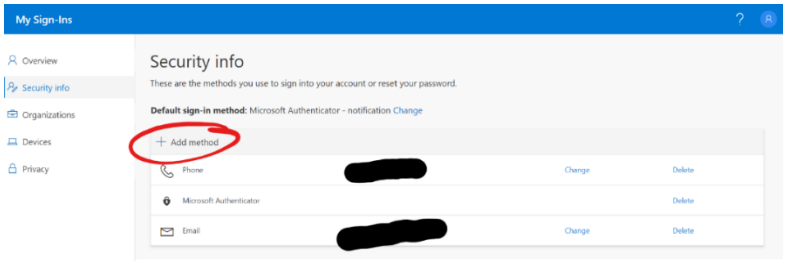
- *What is Multifactor Authentication (MFA)?*

MFA is a standard practice to secure all your accounts. Without MFA, the only thing between the internet and your data is your password. Enabling MFA improves your security by over 99.9% by adding a layer of protection to the sign-in process. It serves as a secondary method to confirm your identity, such as a text message or phone notification. This way, you need to know your password, but also have your phone with you.

- *Steps to set up MFA:*

1) Install Microsoft Authenticator on your phone. (iPhone / Android)
2) Go to https://mysignins.microsoft.com/security-info and set up at least two (2) alternate methods as illustrated in Figure 2.
    a. We recommend the Microsoft Authenticator app as the primary method.

Figure 3



3) Open the Microsoft Authenticator app *(Figure 17)* on your phone.
4) If you see a login prompt when you start the app, cancel it.
5) Tap the **+** > **Work or school account** as shown in *Figure 18.*
6) Click **Scan a QR code** *(Figure 19).*
7) Use your phone to scan the QR square that is on your computer screen.
8) Once you see the account on your phone screen with your company name, switch back to your computer and click next.
9) Add your phone number as a secondary method by clicking **Add Method**.
10) Add any additional methods, if required.

Figure 4

Figure 5

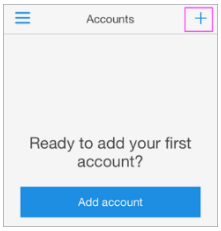
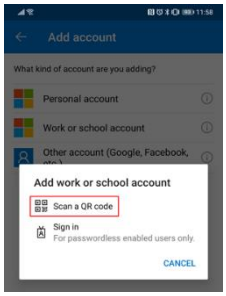


Figure 6



- *Resetting Your Password*

Your Microsoft account should allow for a self-reset. If you are trying to log into any Microsoft services and receive an incorrect password notice, look for the password reset or forgot password option. It should walk you through a quick reset. If not, ask your manager to email help@ic360.ca to request a reset (an email from them will verify your identity with our team).

Step 3: Setting up your Corporate Windows Computer

If you receive a new computer with a login prompt after turning it on, sign in using your work email and password.

If it asks you to set up for personal use or work, choose "Work".

It will then ask you to log in with your **work** email and password.

By following this step, you will join the computer to your work's "Cloud" network. It will automatically install any automated applications, such as Microsoft Outlook and other Office apps, and apply the necessary policies. (This will depend on your employer's settings.)

The process above is called Autopilot. It can take up to 2–3 hours depending on the applications and settings and may reboot a couple of times. This is normal.

- *What is Autopilot?*

Autopilot makes it a breeze for new users to set up company-issued computers. The computer automatically installs the required applications, settings, and policies. (The IT team handles all else, and you do not need to physically bring the computer to a technician.)

Step 4: Manual App Installations

You may have applications that do not automatically install. Discuss with your internal IT lead (if applicable) or email help@ic360.ca for assistance with any such installations.

Step 5: Printers

If you have "Managed" Printers, you will see the printer's name with a **"– Managed"** beside them. Those printers are automatically deployed through our policies. Other printers are manually installed.

Step 6: Microsoft Teams

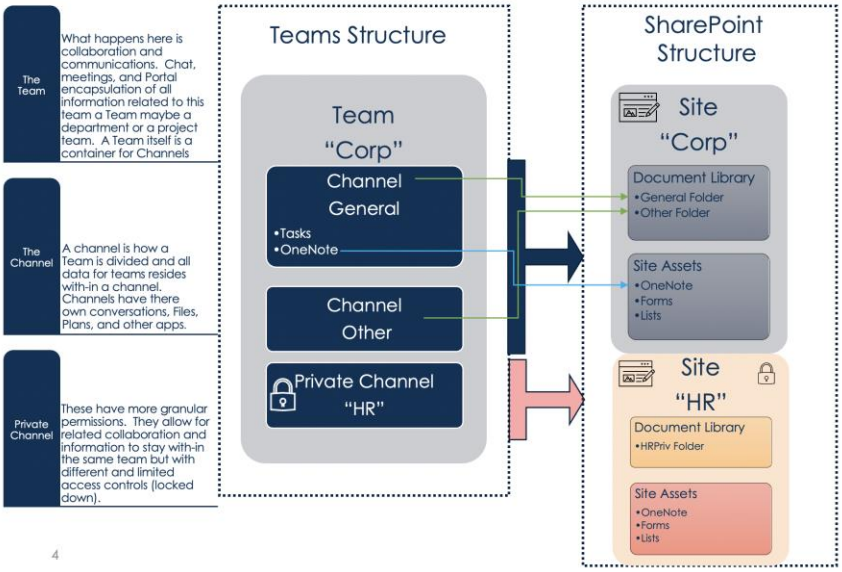
When your account was created, you should have been added to the correct Teams. They will appear when you sign into Teams on your computer or phone. If you are missing any, ask your manager to review first. If you still do not have the right access, email help@ic360.ca.

Step 7: Sync Teams and SharePoint

It is important to understand that Teams and SharePoint are linked. Teams allows you to work with your team. It is the hub for teamwork. SharePoint allows you to work across your organization. It is known as the intelligent intranet. Teams sits "on top" of SharePoint.

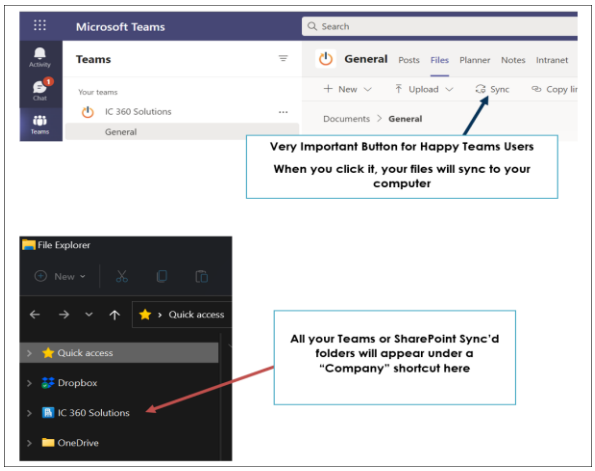
When you create a Team, a SharePoint site is created in the background to store the data. This also happens if you create a "Private Channel" within a Team (see Figure 20).

Figure 20



Syncing Teams and SharePoint is often the difference between hating Teams and loving it! To access files directly, make sure you are first logged into your OneDrive work account, then click the Sync button on the folder you want to sync *(Figure 21).* All your Teams and SharePoint synced folders will appear under a Company shortcut in File Explorer.

Figure 21



Phone Set-Up: Steps for Employees

There are the apps that should be downloaded on your phone:

iPhone
- Microsoft Authenticator (Required)
- Microsoft Outlook (Required)
- Microsoft Office
- Microsoft OneDrive

Android
- Microsoft Authenticator – Apps on Google Play
- Microsoft Outlook – Apps on Google Play
- Microsoft OneDrive – Apps on Google Play
- Microsoft Office: Word, Excel, PowerPoint & More – Apps on Google Play

iOS Instructions

1) Opening Outlook for the first time on your device, you will receive a prompt to register your device *(Figure 25)*.
2) Click **registe**r.
3) You will receive a notification that your IT administrator is helping you protect work in the app *(Figure 25)*. Click **ok**.
4) Proceed to set a PIN *(Figure 26)*. This PIN is different from your phone PIN and will be used to access your company resources.

Figure 24

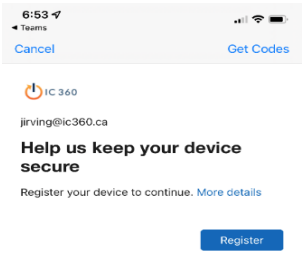


Figure 25

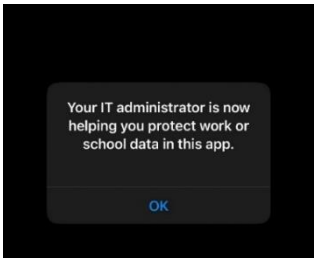
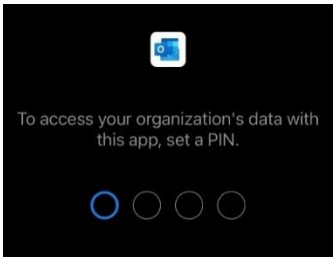


Figure 26



5) After setting the PIN, you can use it to sign in and access your email *(Figure 27)*.
6) If you try to access your email with any other application besides Outlook, you will receive the message that "*You can't get them from here*" as shown in *Figure 28.*

Figure 27

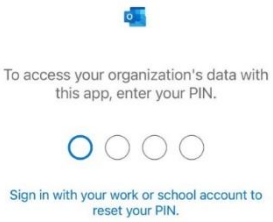
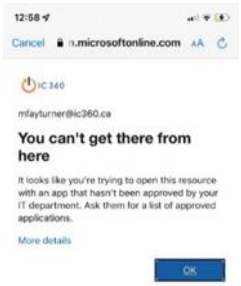


Figure 28



Android Instructions

1) After downloading Outlook on your Android device, you will receive a prompt to get an additional application *(Figure 29).*
2) Click 'Get the app' and install the Intune Company Portal *(Figure 30).*
3) Follow prompts to configure the application *(Figure 31).*

Figure 29

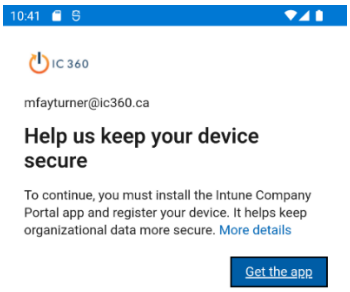


Figure 30

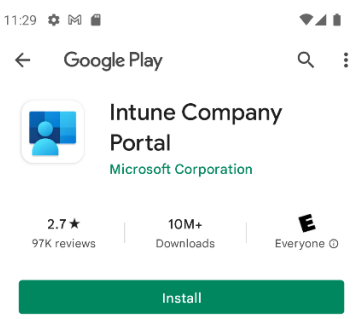
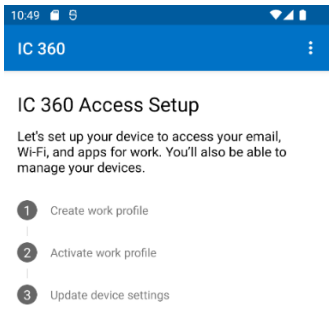


Figure 31



4) Choose the category for this device *(Figure 32)* and continue following the prompts *(Figure 33)* until you reach the 'Your new network setup' screen *(Figure 34*). You have successfully installed the Company Portal.

Figure 32

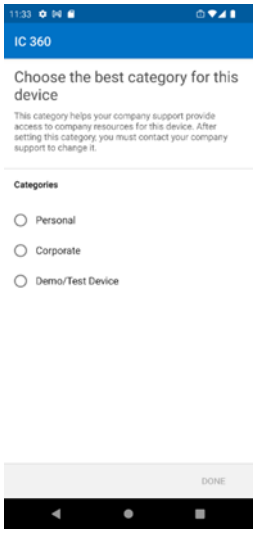


Figure 33

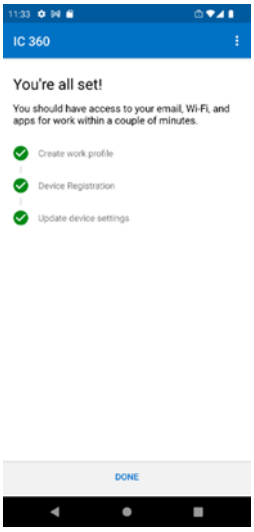
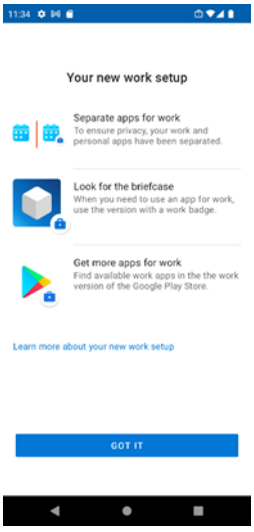


Figure 34



5) Reopen Outlook, and it will prompt you to register your device *(Figure 35).*

6) **Click register** and set a PIN *(Figures 3 6& 37)*. This PIN is different from your phone PIN and will be used to access your company resources.

Figure 35

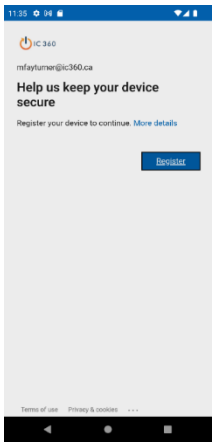


Figure 36

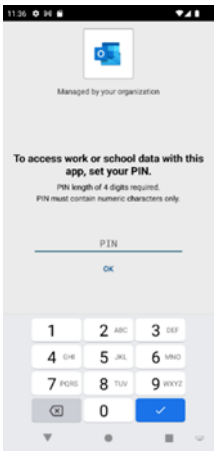


Figure 37