



Technology Reference Guide

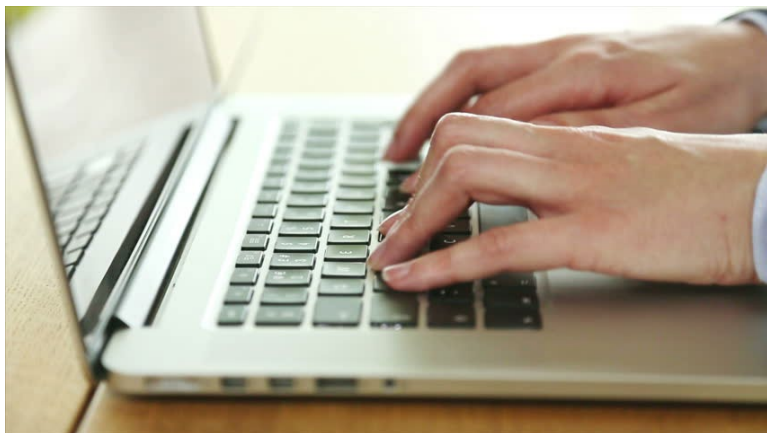


Table of Contents

About This Guide.....	6
IT Department.....	6
Useful Links and Websites	7
Intranet	8
Getting Help from IT	9
Submitting a TrackIt Request.....	9
Critical Support Requests.....	12
After Hours and Weekend Support	12
Security Considerations	13
Physical Security.....	13
Badges.....	13
Secure Areas.....	13
Reporting a Security Incident.....	16
What is a Security Incident?.....	16
What should you do if you witness a security incident?	16
Technology and Systems.....	17
Access by Employees	17
User Login	17
Password Policy.....	17
How to Reset Your Password	19
Multi-Factor Authentication (MFA)	21
Setting up Multi-Factor Authentication.....	21
Document Storage	28
Corporate Computers	29
What to do at the end of your workday	30

Email.....	31
How to Open Email and Use Microsoft Outlook.....	31
A Quick Word About Email Etiquette.....	31
Email Signatures.....	32
Data Loss Prevention (DLP)	32
Email Phishing	32
How to Give Another User Access to Your Email Temporarily	33
How to Schedule a Meeting.....	34
How to Maintain Your Mailbox Size Within Limits	35
How to Access Email Remotely (Web Mail).....	36
How to Access Email on a Mobile Device	37
Phone System (Mitel).....	38
How to Set Up Your Voicemail Greeting.....	38
How to View Directory.....	38
How to Access Voicemail	39
How to Set Status When Out of Office	39
How to Reset Your Voicemail PIN	40
How to transfer your extension to another phone temporarily.....	40
How to Access Your Voicemail From an External Phone	40
Internet Access.....	42
Browsers.....	42
Web Filtering.....	42
Appropriate Use	42
Wi-Fi Internet Access	42
Guest Wi-Fi Network.....	43
How to Access	43

Citrix	44
PrintStream MIS.....	45
Shopfloor – What is it?.....	45
Shopfloor – How to Access?.....	45
Shopfloor – How to punch in and out?	46
How to Access PrintStream.....	48
How to Get Support with PrintStream Issues	48
Crystal Reports.....	49
How to Access Crystal Reports.....	49
Remote Access - LogMeIn.....	51
What is It?	51
How to Set Up	51
Remote Access - VPN	54
What is It?	54
How to Set Up	54
FTP System	56
How our FTP works	56
How is FTP access organized and granted?	56
Requesting New External FTP User Setup.....	56
How an External FTP User Can Reset Their Password	57
How to Get Help With FTP Issues	57
Xerox Copiers	58
Locations	58
Desktop Printers.....	58
Paper and Toner Replenishment	58
Getting help	58

Resource Board58

 Purpose58

 How to Access58

 How to Use.....59

InSite Proofing Portal59

 Purpose59

 How to Access60

 How to Use.....60

 Getting Help60

Contact IT Support62

 Submit a TrackIt62

 Phone Numbers62

About This Guide

This guide is intended to serve as a resource to employees relating to technology at ENPOINTE. In it is information that we think you will find useful or serve as a future reference for frequently asked technology related questions.

IT Department

The Information Technology Department is divided into three functional areas:

IT Systems

This area focuses on the systems and infrastructure that run the business; for example, the network, virtualized servers, email, phone system, PrintStream ERP system, and various other systems and applications.

IT Developers

This group creates and manages DirectConnect e-commerce websites, automated POD programs, and customized reporting.

IT Workflow and Technology

This area focuses on workflow management and automation primarily in the print manufacturing side of the business.

Useful Links and Websites

Corporate website - <https://alwaysevenpointe.com/>

eHub - <https://ehub.alwaysevenpointe.com/>

Crystal Reports - <https://webreports.alwaysevenpointe.com/BOE/BI/>

FTP site – [sftp://filetransfer.alwaysevenpointe.com](https://filetransfer.alwaysevenpointe.com)

FTP site (web access) - <https://filetransfer.alwaysevenpointe.com>

Intranet - <http://intranet.alwaysevenpointe.com/>

Kodak Insite Prepress Portal - <https://insite.alwaysevenpointe.com>

Paycor - <https://www.paycor.com/>

Resource Board - <https://core.alwaysevenpointe.com/resourceboard/>

TrackIt - <http://bp-trackit114/TrackItWeb>

Track n Trace - <https://alwaysevenpointe.trackntrace.com/>

Web Mail - <https://www.outlook.com/owa/>

Intranet

How to Access

The ENPOINTE corporate Intranet is your go-to resource for updated access to corporate policies, controlled forms, department contacts, job postings, and other useful information. Below is a link to the intranet website. Note that this site is only accessible on the internal corporate network.

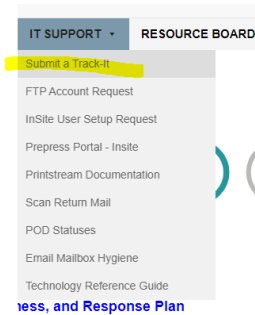
<https://intranet.alwaysenpointe.com>

Getting Help from IT

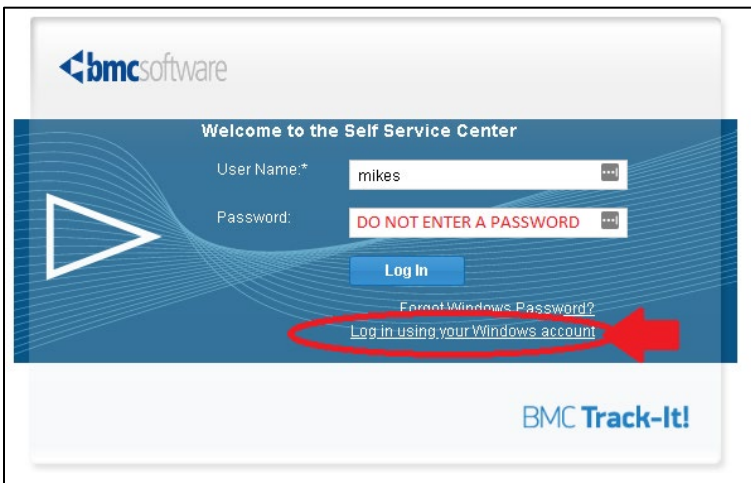
ENPOINTE utilizes a ticketing system called TrackIt to manage user requests for technology support. When you submit a ticket, the ticket is routed to the appropriate IT Team based upon the type and categories you select.

Submitting a TrackIt Request

1. To submit a TrackIt ticket, go to the corporate intranet at <http://intranet.alwaysenpointe.com> and hover the mouse over IT SUPPORT and then 'Submit a TrackIt'.



2. Click Log in using your Windows account.



3. Click the link to Add a New Work Order



Add a New Work Order

Submit a new Work Order request to IT for a problem that you are having.

4. Enter a summary of your issue along with selecting the priority, type, sub-type, and category that the issue would fall under. Accurately setting these fields helps us respond to your request as fast as possible. Also including a screenshot or other file attachment might help us understand the issue quicker. See example on next page.
5. Choose the right priority for your ticket. Setting an accurate priority to your ticket allows IT to address the problems that have the highest impact to the business first. Following are definitions of each priority type.
- **Critical** – A business critical system is non-functional or otherwise unable to produce work.
 - **High** – A non-critical system is not functional, or a critical system is not operating optimally and is negatively impacting productivity.
 - **Medium** – A system is not operating optimally for productivity but does not have a broad negative impact to productivity.

New Work Order

Common Requests Submit Work Order

Summary:*
Can't print a report

Call Back Number:
763-592-0579

Asset:
1249_D096GN02

Priority:
High

Type:*
Desktop Hardware

Subtype:
Printer or Copier

Category:
Not working

Note:
Nothing prints when I try to print my daily thingy report.

File Name:
Select a file

Browse... Clear

Submit

- **Low** – A system requires some maintenance or upgrade that is not negatively impacting productivity.
6. After you have submitted your ticket, an email will be sent to you confirming your submission. An email also gets sent to the assigned technician or group of technicians based on how you categorized your ticket.
 7. An IT Tech Support Technician will respond to your request based on the level of prioritization and overall impact to the business.

Critical Support Requests

If you have already submitted a TrackIt ticket but you need immediate assistance, please contact one of the following.

- For immediate assistance for computer, network, systems, logins, phones, hardware or software, please contact IT Support using the phone and email on the next page. IT Support consists of all members of both the IT Network Services and IT Business Systems teams.
 - **IT Support internal phone extension x5911**
 - **External phone number: 763-592-0591**
 - ITSupport@alwayssenpointe.com
- For all POD, DirectConnect eCommerce, and Crystal Reports support please contact the DirectConnect Services team.
 - **DirectConnect Support internal phone extension sx5551**
 - DirectConnectSupport@alwayssenpointe.com

After Hours and Weekend Support

For all after-hours and weekend support requests, please submit a TrackIt ticket. If the issue is critical and cannot wait until the following business day to be addressed, you can call the IT Support internal extension or external phone number. The IT Support team staff covers this number 24/7 on a rotating schedule.

- **IT Support internal phone extension x5911**
 - **External phone number: 763-592-0591**
- If you call the above extension and are unable to reach anyone, please call down the list of IT Support staff identified on the IT Related Emergencies call sheet posted on all Department bulletin boards.

Security Considerations

Physical Security

Badges

Badges are required to gain access to ENPOINTE facilities. Each team member depending on their role will be issued a badge that will allow them access to certain buildings and secure areas within.

Below are the four different types of badges that are issued.

- **Ocean** Badges for Employees
- **Yellow** Badges for Temp Staff
- **Coral** Badges for our Visitors and most Vendors
- **Shoal** Badges for Special Vendors and Contractors
- Visitors and vendors are required to show photo identification before being issued a visitor badge.
 - If a visitor does not have photo identification, a ENPOINTE employee needs to verify their identity and sign a form to accept responsibility
- **Do not let Temp Staff or Visitors tailgate behind you through any secure doors!**

Secure Areas

There are several higher security areas at ENPOINTE that require special badge access rights. Depending on your job role you may have access to some, all, or none of these areas. See below.

Highest Priority

- Server Rooms in All Buildings
- Network and Wiring Closets

- Fulfillment Center Distribution Cage
- Temp Staff are not allowed into these areas without supervision and prior background checks.
- Vendors must be directly supervised when in these locations.

Secondary Priority

- Sales/CSR/DP/Premedia work areas
- BP Digital Studio
- Inkjet/Lettershop
- BP Distribution/Kitting
- Mail Staging areas
- Marketing agency Office

What Should You Do If You See Someone Without a Badge?

- Remember to be positive and friendly - this may be a customer, new employee, or other visitor to ENPOINTE!
- Ask “Can I help you?”
- If the person does not have a legitimate reason for being in the building, you should escort this person to a Lead or Manager immediately.

Use of Cameras and Taking Photos

- Many clients require us to restrict the use of cameras ENPOINTE facilities.
 - Can only be used if required for your job
 - Includes traditional and cell phone cameras

- Includes visitors as well - You are responsible for your visitors!



- Other exceptions can be approved by Senior Leaders

Reporting a Security Incident

ENPOINTE and its customers regard security in the highest regard. Strict measures are taken to secure our employees, facilities, equipment, and data.

What is a Security Incident?

A security incident is attempted or actual:

- Unauthorized access, use, disclosure, modification, or destruction of information
- Interference with information technology operation
- Violation of campus policy, laws or regulations

Examples of security incidents include:

- Unauthorized access to building or secure areas
- Unauthorized access to, or use of, computers, systems, software, or data
- Loss or theft of equipment used to store or work with sensitive data
- Compromised user accounts such as shared passwords

What should you do if you witness a security incident?

It's important to report any security incident as soon as possible so that the proper action can be taken to minimize damage or loss.

If you think you have witnessed or are aware of a security incident report it to SecurityIncidents@alwayssenpointe.com and provide as much detail as possible on the incident. A member of IT Leadership will respond to your incident as soon as possible.

Technology and Systems

Access by Employees

ENPOINTE employees that need access to computer systems (e.g. desktops, laptops, or email) will be given a user login to our domain on their first day of employment. This user login is a centrally managed credential which can be used to grant access to many different systems depending on your role.

User Login

Your username will usually be your first name and the first letter of your last name. For example, Gary Garner's username would be 'GaryG'. When you are onboarded, you will receive an initial password from IT, you will then be required to change that password to something only you know the first time you log in.

Each time you sit down at your computer, you will need to enter your password in order to unlock the system. Screens are set to lock themselves after 15 minutes of inactivity. In some higher security areas those screen locks occur even sooner.

Password Policy

ENPOINTE requires complex passwords for all logins. Passwords should NEVER be shared with another user. Below are the current requirements for passwords.

Passwords must...

- be at least twelve characters long
- not contain your first or last name
- be different than your last 20 passwords
- include three of the four following characteristics:
 - an upper case character
 - a lower case character
 - a number
 - a special character (e.g. symbols or punctuation marks)

- Passwords must be changed every 60 days. You will begin to receive email notifications when your password is 14 days from expiring. You will also see popups in your Windows desktop session.

Tips for Secure Passwords:

1. Use phrases instead of words, since they are much easier to remember! For example:
 - Going2HaveFun
 - 4GoneConclusion
 - 8TooMuchFood
 - Need2ThinkMore
 - ListenLouder!
2. Do not use the same passwords for your home and work accounts.
3. Do not use nearly-identical passwords by simply changing the final character. (E.g. BigElephant1, BigElephant2, BigElephant3, etc.) That approach defeats the entire purpose of changing your passwords. If you use this approach and someone obtains one of your passwords, they will always be able to guess your future passwords.

Notifications about Password Expiration

Beginning at 14 days before expiration, you will start receiving email notifications about your upcoming password change as well as pop-up notices in Windows. You can change your password right away when you receive the first notice, or you can wait until the last day and change it then.

If you let your password expire, you will be unable to log in when you return.

If you do find yourself in a situation where you cannot log in, please contact IT Support at x5911 to get your account reactivated.

How to Reset Your Password

Windows PC

Press CTRL-ALT-Delete and choose Change Password. Once you have changed your password, restart your computer and log in with the new password. Also remember to update the new password on your mobile phone and tablet if you receive email on them.

Mac Computers

While logged into your Mac and connected to the corporate network, Open your Mac's system preferences, click Users & Groups, Click on your Name, and then click 'Change Password' enter your old password and then enter your new password twice. Once you've updated your password, reboot your Mac and if/when prompted to update the keychain, click yes.

Alternatively, you can change your password in Outlook Web Access using the instructions below.

Log in to [Web Mail](https://mail.alwaysenpointe.com) at <https://mail.alwaysenpointe.com> and click on Options, then Change Password. Once you have changed your password, restart your computer, and log in with the new password.

Also remember to update the new password on your mobile phone and tablet if you receive email on them.

Remote (LogMeIn)

1. When in the remote session (not in full screen mode), click on the button that looks like three little boxes located in the top right corner of the window. This is the CTRL+ALT+Delete for your work computer.
2. Click on the Change Password link on the screen.

Remote VPN (non LogMeIn)

1. Ensure that you are connected to ENPOINT VPN.
2. Press Ctrl+Alt+Delete on your keyboard
3. Select Change Password
4. Enter their current password and then their new password (twice).
5. Click OK to apply the change
6. Either lock your PC or log out and then sign back in with your new password in order to clear the old cached password.

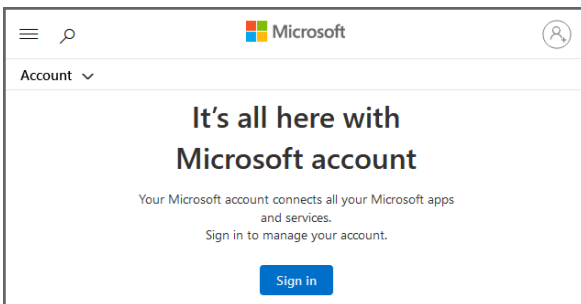
Multi-Factor Authentication (MFA)

Historically, user authentication has been accomplished by requiring a user to enter a username and password to access networked systems. Login with username and password is considered one-factor (the password) authentication. As adversaries and threat actors have become more advanced, so have information security practices and many organizations are implementing multi-factor authentication. MFA requires additional information such as a one-time pin or computer certificate to secure access.

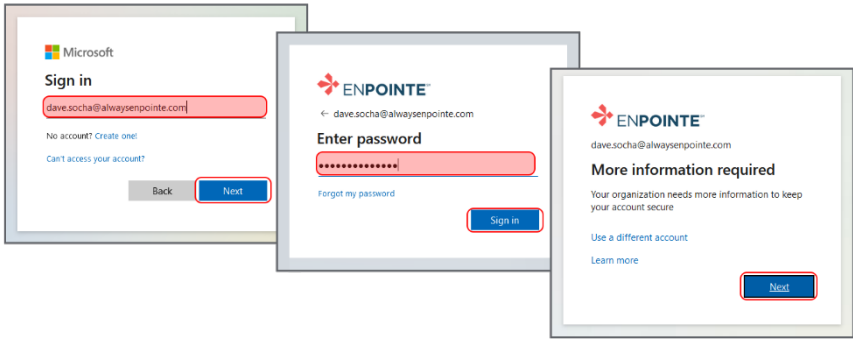
ENPOINTE has implemented MFA as a critical component of our security practices and procedures, and you may be prompted to setup MFA for your accounts.

Setting up Multi-Factor Authentication

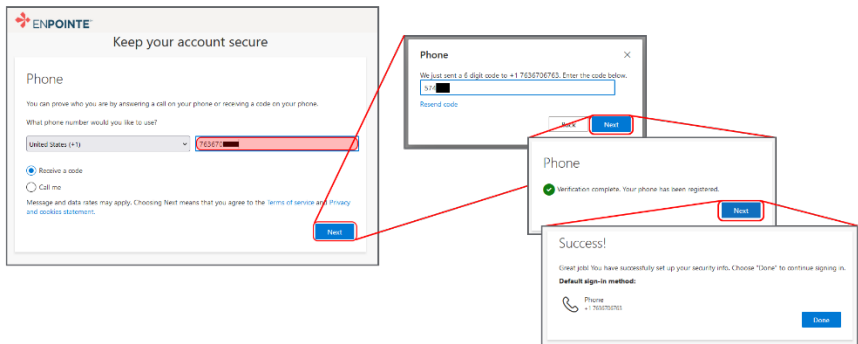
1. In a web browser, navigate to <https://account.microsoft.com>. Select the “Sign in” link in the center of the page, or the upper right hand corner of the page.



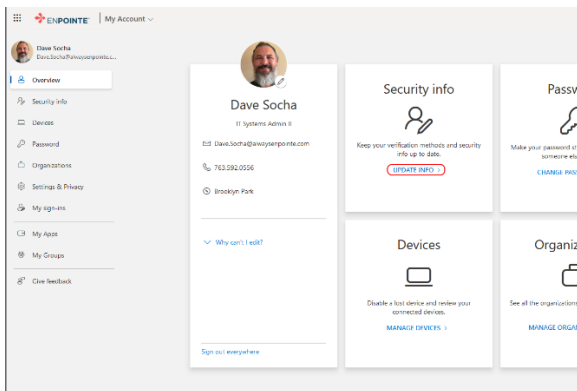
2. Enter your username and password at the relevant prompts. When prompted for more information select “Next”.



3. You will be asked for a phone number. Please ensure that the number you enter can receive both text messages and phone calls.
 - Enter the phone number in the block and select next. You will receive a notification at the number.
 - Enter the number received when prompted and continue through the prompts.
 - Select “Done” to move onto the next step.

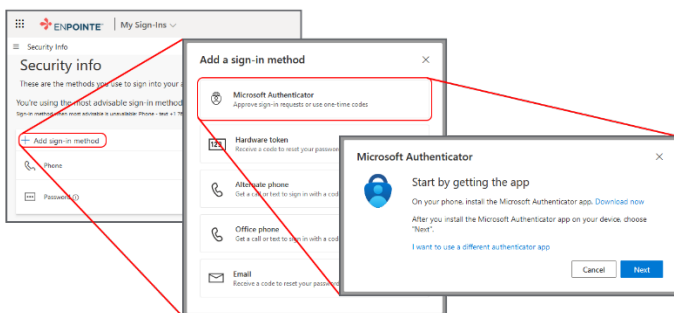


4. The webpage will navigate to the My Account page where you will enroll an authenticator app to your account. Prior to starting this step, please ensure that you have the Microsoft Authenticator app downloaded to your mobile device. Click on the “Update Info” link under the “Security info” card



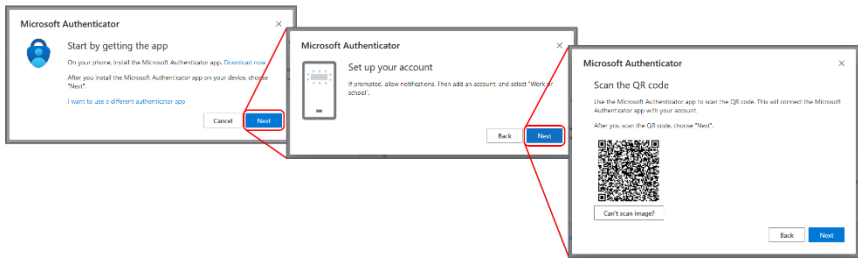
5. In the popup window, select “Add sign-in method”, then select “Microsoft Authenticator”. There are two methods of authenticating, number matching and one time pin generation, only one method is required.

- See step 6 for number matching setup
- See step 7 for one time pin generation setup.

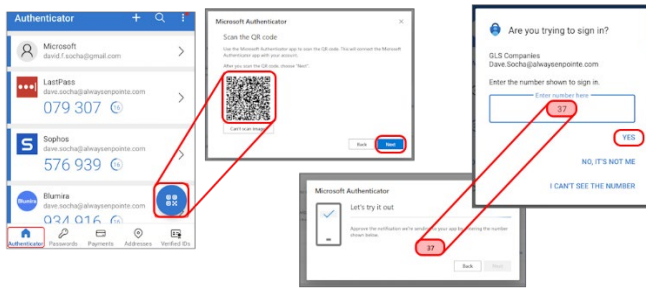


6. Number matching setup

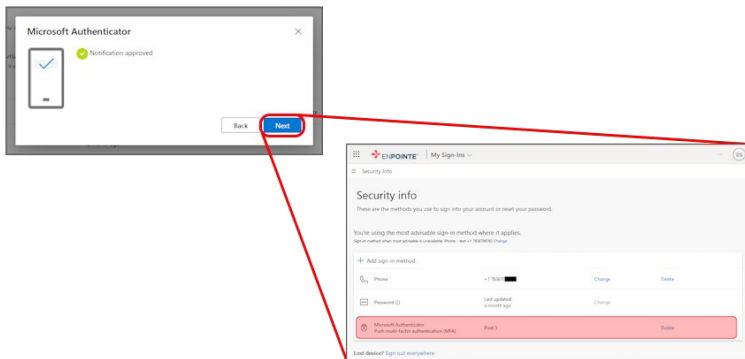
- On the “Start by getting the app” popup, select “Next” to continue with setup.
- On the “Set up your account” popup, select “Next”. This will load a popup with a QR Code to scan.



- In the authenticator app, scan the QR code. Select “Next” on the website. A popup will display containing a number. Enter the number in the authenticator app, and press yes.

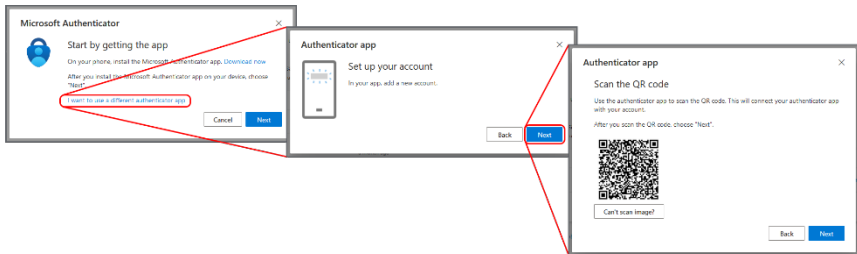


- You will see a confirmation message on the website, select “Next” to navigate back to the security info page. You will see the authentication method in the listing of authorized methods. Proceed to step 8 to update your default authenticator method.

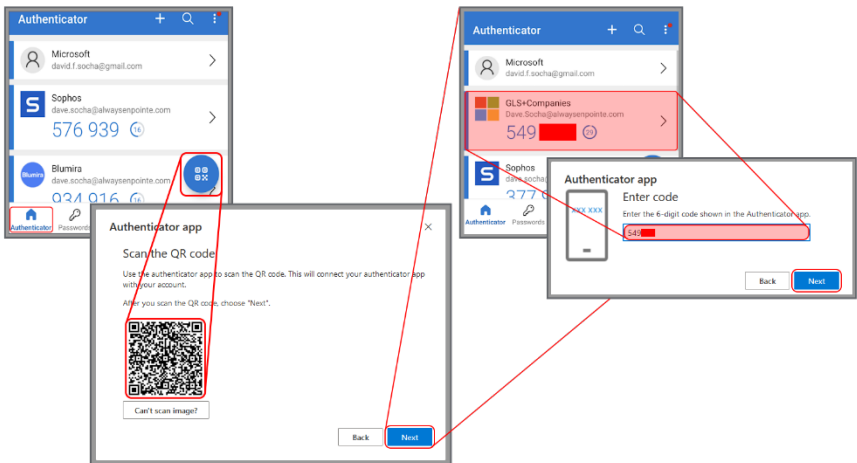


7. One Time Pin setup

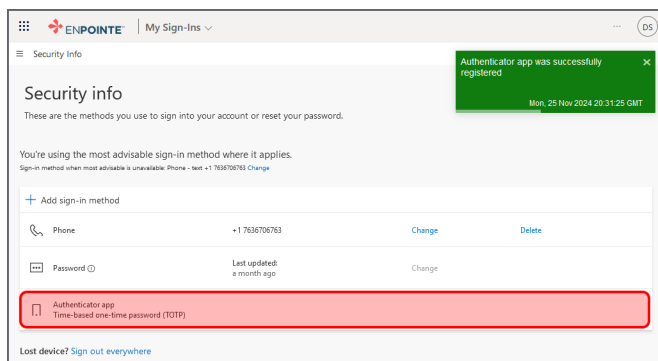
- On the “Start by getting the app” popup, select “I want to use a different authenticator app”. Please note the Microsoft Authenticator app will be used to complete the process.
- On the “Set up your account” popup, select “Next” to continue onto the “Scan the QR code” popup.



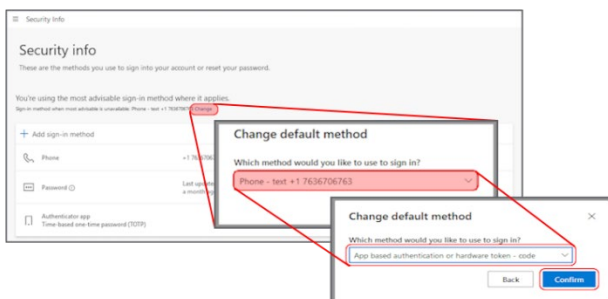
- In the authenticator app, scan the QR code. An entry will be added to the listing in the app.
- Click “Next” on the “Scan the QR code”. A popup will display where you will enter the number displayed on the authenticator app. After entering the number select “Next”.



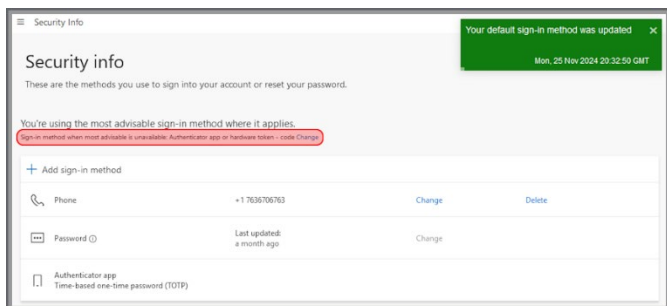
- The page will navigate back to the “Security Info” screen. You will see a confirmation message in the upper right corner and the authenticator app will be seen in the list. Proceed to step 8 to set your default authenticator method.



8. Setting your default authenticator method - Microsoft will use the phone you entered in step 3 as the default method. This should be changed to the authenticator app.
 - Above the grid where the sign-in methods are displayed, select “Change” next to your phone number.
 - A popup will display. Under “Which method would you like to use to sign in?” a dropdown will contain the list of login methods associated with your account.
 - Select the authentication method entered in step 6 or 7 above.
 - Select “Continue”



- The popup will be dismissed and a confirmation message will be displayed in the upper right corner. You will also see your selected default method displayed above the listing of authorized sign in methods.



Document Storage

ENPOINTE requires you to store all important data on a network share or in a folder that is backed up using OneDrive. If your computer's hard drive fails, ENPOINTE does not maintain backups of your local computer's storage, so any data on the computer would be lost.

Instead, all data should be stored in designated network shares for your department, OneDrive, or your personal network (P) drive.

P Drive

All users are set up with a mapped "P drive" when they log in. This folder is your private directory that no other users have access to. It is stored on a centralized file server and is regularly backed up to prevent data loss. **Note that no personal data should be stored on your P drive or anywhere on ENPOINTE assets.**

Corporate Computers

Daily Use Best Practices

- Always lock your computer when you leave your desk (see “Securing Your Workstation” below).
- NEVER store important documents on your local workstation such as the desktop. Your local computer does not get backed up and if they system fails you will lose all your data. **Always store your data on a network share such as your P drive or other department specific shared drive.**
- Reboot your system daily for optimal performance. Get in the habit of rebooting when you go home at night. But always keep your system powered on as we perform important system updates during the evenings.
- Do not use your ENPOINTE owned corporate device to store personal data.
- If you are issued a laptop device you are required to secure the device when you are not in the office. This could be by cable lock, locking in a drawer, or taking home with you.

Securing Your Workstation

ENPOINTE requires you to secure your workstation anytime you step away from your workstation.

- Windows / PC Users: Press **WINDOW+L** to lock your computer. You can also press **CTRL+ALT+DEL** and choose Lock.
- Apple / Mac Users: Press the **Apple logo and choose Lock.**

Standard Software Packages

Depending on your role the software packages preinstalled on your workstation will vary but standard applications installed on most workstations include Microsoft Office, Citrix Workspace, Google Chrome, Adobe Acrobat Reader, Sophos Anti-malware, and Mitel Communicator.




























Anti-Virus/Malware Protection

ENPOINTE deploys Sophos Anti-Malware software on all workstations to protect from viruses and other malicious software and websites. There are policies applied to your computer based upon your role which may limit which websites you can access or block CD drive or USB ports from being used.

What to do at the end of your workday

At the end of your workday you should either log off your username or restart your workstation. You should NOT shut down your computer, as IT often performs system updates during off hours. See the grid below.

METHODS OF ENDING A COMPUTER SESSION

Method	Lock <small>(or the Login Window)</small>	Log Off <small>(e.g. Log Out)</small>	Restart	Shut Down	Sleep <small>(e.g. Standby or Pause)</small>	Hibernat e <small>(N/A for Macs)</small>
When To Use	Do This When Temporarily Leaving Workstation	Do One of These At End of Each GLS Work Day		Do <u>Not</u> Do This at GLS Companies UNLESS You Are Installing Updates	These Functions DO NOT Log You Off	
Requires User's Password to View Display or Gain Access						
Disconnects User from GLS Network						
Disconnects Network Drives						
Stops All Programs from Running Under this User on the Computer						
Shuts Down Computer Hard Drives						
Temporarily Moves RAM Contents to Hard Drive and Reduces Power to RAM to Reduce Power Consumption						
Temporarily Moves RAM Contents to Hard Drive and Turns Off Power to RAM to Reduce Power Consumption						
Powers Computer Off and Disallows Workstation Maintenance to Occur						

Email

How to Open Email and Use Microsoft Outlook

ENPOINTE corporate email can be accessed several ways depending on your work role and access privileges. In most cases though you will be accessing your email from a desktop computer using Microsoft Outlook.

Microsoft Outlook is a component of Microsoft Office suite and will be preinstalled on your workstation in most cases.

Windows PC - To open Microsoft Outlook, click on the Start menu at the lower left corner of your screen and then browse or search for Microsoft Outlook.

macOS Computer - To open Microsoft Outlook on a Mac, browse to the Applications folder and then Open the Microsoft Office folder and find the application named Microsoft Outlook. A quicker way is to press CMD + Spacebar and begin typing Outlook.

A Quick Word About Email Etiquette

Communicating via email can sometimes lead to miss-communication, hurt feelings, or damage someone's reputation. Below are a few quick tips on how to keep your email effective and professional.

1. **Always include a subject** – Include a subject line that is descriptive of the topic discussed in the body of the email.
2. **Use Reply All sparingly** – Ask yourself does everyone need to see my reply to this email? If there is no benefit, do not reply all.
3. **Be cautious with humor** – Written communication can easily be taken out of context or misinterpreted. A joke may have been meant as something harmless but could come across as offensive.
4. **Proofread before sending** – More often than not, rereading your email before sending it will lead to caught mistakes and better wording.
5. **Should it be sent in an email** – Is the message you are sending appropriate for email? If the topic is sensitive or potentially upsetting, do not send it in an email. Also consider that an email

you send might be seen by individuals you did not intend to see it.

Email Signatures

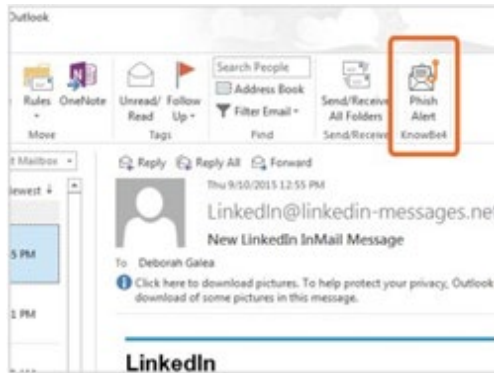
ENPOINTE centrally manages all email signatures. You do not create or manage your own email signatures in your Outlook client. When you are onboarded, the appropriate contact information and job title are entered. If you find that some of the information is not correct, please alert your department manager and they will submit a TrackIt ticket for the correction.

Data Loss Prevention (DLP)

ENPOINTE uses an email security solution to prevent ENPOINTE's or its customer's sensitive data from being sent outside ENPOINTE via email. Email is an inherently insecure method of sending information and thus we block certain types of information from being sent that way. For example, ENPOINTE will block you from sending credit card or social security numbers in an email. If you have a scenario where you need to send this kind of information outside ENPOINTE, contact IT Support for assistance.

Email Phishing

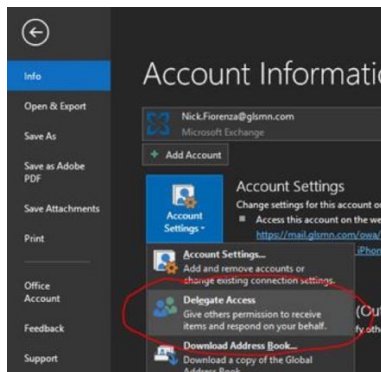
If you receive a suspicious email, the best thing to do is to report it to the IT Department so that we can review. To do so simply click on the Phish Alert icon in your Outlook toolbar. Note this is only available for PC users using Microsoft Outlook and will not be available to Mac users or users using web mail (Outlook Web Access OWA). For those users, simply forward the email to phishing@alwayssenpointe.com



How to Give Another User Access to Your Email Temporarily

If you want to have someone have access to your inbound email while you are away from the office for an extended period, you can provide them with what is called delegate access. Follow the instructions below to set this up.

1. Go to File -> Account Settings -> Delegate Access



2. Click Add. When the next screen pops up, search for the person you want, select them, click Add, and then click OK.

Add Users

Search: ☒ Name

dan von

Name

3. Set the level of access you would like the person to have.

Delegates

Delegate Permissions: Larry Wrolstad

This delegate has the following permissions

	Calendar	Editor (can read, create, and modify items)
<input checked="" type="checkbox"/>	Delegate receives copies of meeting-related messages sent to me	
	Tasks	Editor (can read, create, and modify items)
	Inbox	Author (can read and create items)
	Contacts	None
	Notes	None

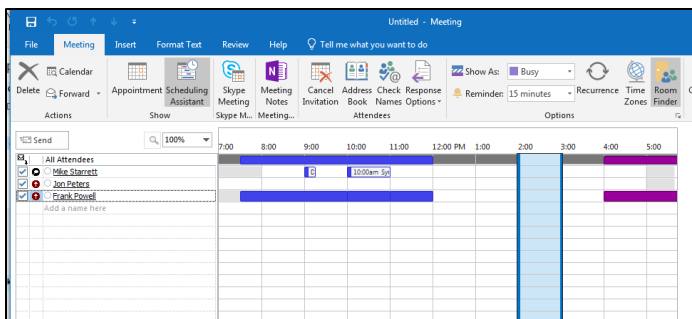
☐ Automatically send a message to delegate summarizing these permissions

☐ Delegate can see my private items

OK Cancel

How to Schedule a Meeting

1. In Outlook click on the **Calendar** icon
2. Click on **New Meeting**
3. In the **TO** field type in the names of the invitees. Names should resolve to your contact list.
4. Type in a subject for the meeting
5. Next to the Location field is a **Rooms** button, click that and select the meeting location if you plan to reserve a conference room for the meeting.
6. Click into the body of the window and enter any meeting details you want to provide.
7. Click on the **Scheduling Assistant** button at the top of the window to review availability of all invitees and adjust the meeting time and length as needed.



8. Click **Send**.

How to Maintain Your Mailbox Size Within Limits

Most companies have limits on e-mail storage to manage corporate risk and optimize the locating of critical correspondence. Large mailbox sizes also degrade a workstation's email, calendar and contact system performance. Thus, appropriate e-mail storage hygiene practices are required of ENPOINTE employees.

ENPOINTE Practices

- All ENPOINTE job-related data files are backed up and retained for only one year beyond invoicing date. This commitment to purge data files is made to all of ENPOINTE's clients.
- Job-related client data files should not be retained in e-mails.
- Incoming client files for conventional jobs should be sent directly to CSRs via SFTP for our most efficient workflows.
- Retention of e-mail attachments creates storage problems in our e-mail system.
- **Organizing Your Emails**
- To understand the storage size of your mailbox and which folders are taking up the most storage space, go to the File tab on the top of your Outlook. Through the info panel, select Tools and a dropdown menu will appear, select Mailbox Cleanup. This will prompt a pop-up menu for you to select View Mailbox Size. After a brief wait, this will show your subfolder storage sizes (in kb).

- To delete emails, go to the folder which you want to clean up.
Within any folder you can sort e-mails by the column headers:
 - By clicking on the “Size” column header, you can sort to put the largest on top.
(Click again to sort the largest to the bottom.)
 - By clicking on the “Received” column header, you can sort to the oldest on top.
(Click again to sort the oldest on the bottom.)

How to Select Groups of Emails for Deletion

There are several tactics to use in deleting e-mails. One tactic is deleting e-mails by age and getting rid of your oldest e-mails. Another tactic is focusing on the messages with the largest attachments and deleting e-mails by size.

1. Select multiple individual e-mails by using the Ctrl + Click function.
2. Select a group of e-mail messages, from your first selection to your next by using the Shift + Click function.

Permanently Deleting Emails Can Be a One-Step or Two-Step Process

One-Step Process

After selecting a group of messages to delete, the one-Step process uses the (Shift + Delete) function on your keyboard. This may prompt a pop-up window asking, “Are you sure you want to permanently delete the selected items?” or it may instantly delete all.

Two-Step Process

After selecting a group of messages to delete, the two-step process starts by right clicking on your selected e-mails and choosing Delete at the bottom of the dropdown menu. This will send the selected e-mails to the Deleted Items folder. You will then need to select and delete these same items from the Deleted Items folder in order to clear storage space.

How to Access Email Remotely (Web Mail)

Certain ENPOINTE employees will be given access to Web Mail (also known as Outlook Web Access or OWA). This allows a user to access their email from any web browser with internet access.

To access OWA simply open a web browser and enter the URL <https://www.outlook.com/owa/> and hit enter. Enter your email address which is usually first.last@alwaysevenpointe.com and then your current password. This is the same password you use when you log into your desktop computer.

How to Access Email on a Mobile Device

1. Install the Outlook app from the app store.
2. Open the Outlook App and go to Settings, tap your profile picture or the gear icon in the top-left corner to access Settings.
3. Add Account, scroll down and tap Add Mail Account or Add Account and Select Exchange.
4. Enter Your Email Address and password.
5. Complete MFA process
6. Accept permissions if prompted
7. The app will then begin to sync your account to your device.

Note that adding ENPOINTE email to your mobile device will require certain security features on your phone to be enabled. For example, you will be required to have a PIN that you will need to enter every time you unlock your phone unless your phone has biometric features such as fingerprint or facial recognition.

Phone System (Mitel)

How to Set Up Your Voicemail Greeting

Note that it is required that you set this up within the first 7 days of hire.

1. Pick up the handset on your phone and then press the voicemail button on your keypad.
2. Enter your 6-digit password followed by # key
3. Press 7 and then press 1
4. Record your greeting and save

How to View Directory

You can access the directory from the phone directly or via the Mitel Connect application on your PC.

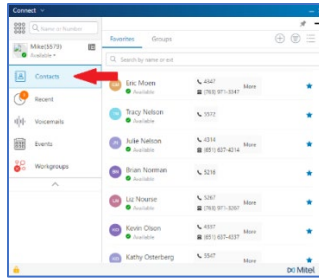
From Phone

Push the 'Directory' button and then start typing the person's first name on the number pad until you see them. You can also scroll through list using the up down button next to the display.



From Mitel Connect

Open the application either from your start menu or your system tray. From there click on Contacts. You can scroll through the list or type in a name to quickly search.



How to Access Voicemail

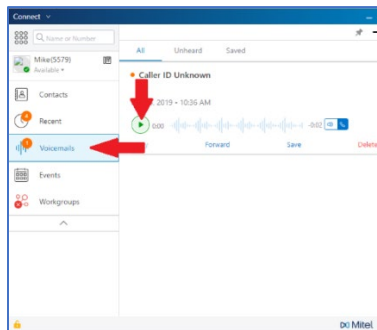
You can access your voicemail directly from the phone or from Mitel Connect.

From Phone

Press the Voice Mail button on your phone, enter your PIN, and follow the prompts. If you do not know your PIN please put in a TrackIt ticket and we will reset it for you.

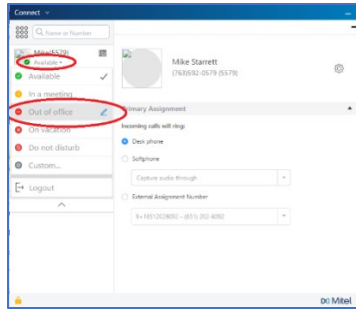
From Mitel Connect

Click voicemails and then click play on the message. You can then delete, forward, or save the message as needed.



How to Set Status When Out of Office

You can easily set your Out of Office status on your phone from the Mitel Connect application. Click on “Available” and then choose the appropriate status from the list. You can also click the pencil icon.



How to Reset Your Voicemail PIN

If you forgot your voicemail PIN you should submit a TrackIt ticket to IT Support and we will reset it for you.

How to transfer your extension to another phone temporarily

1. Press the Voice Mail button on the phone.
2. When the automated voicemail starts, press the '#' button, and your extension number.
3. Enter the password you normally use for your voicemail.
4. Dial 7, 3, 1

When you are done, follow the below instructions to remove your extension from the phone.

1. Press the Voice Mail button.
2. Enter the password you normally use to check your voicemail.
3. Dial 7, 3, 2, and your extension will revert to your primary phone.

How to Access Your Voicemail From an External Phone

1. From an outside phone you can access your Mitel voicemail. To do so just call your phone number and when your voice recording starts to play press *.
2. Enter your extension
3. Enter your vmail PIN
4. Follow the prompts to access voice messages.

OR

1. Dial 763-971-3300 and follow the prompts for extension and PIN code.

Internet Access

ENPOINTE provides internet access to most workstations throughout the company. This access is closely monitored, and certain websites are blocked, and all activity is logged.

Browsers

ENPOINTE has standardized two web browser options for all workstations. For PCs the standard is Google Chrome and Edge. For Mac users the browsers are Apple Safari and Google Chrome.

Web Filtering

ENPOINTE employs several policies to restrict what websites users can visit from its corporate network. Depending on your role these restrictions will be different. In most areas websites that allow for file uploads/downloads are restricted.

If there is a business use case for needing access to a site that you find is blocked, you will need to complete a request form

Appropriate Use

ENPOINTE provides internet access to its employees to allow them to do their jobs and is not intended to be used for personal use, however during breaks it is permissible for users to access the internet for personal use. Note that ENPOINTE logs and monitors all internet activity and actively blocks access to sites deemed to be inappropriate for a business setting.

Wi-Fi Internet Access

There are two wi-fi networks at ENPOINTE. One is called CORPORATE and the other is called GUEST. The CORPORATE network is only to be used by corporate owned devices and allows users wireless access various parts of the corporate network based on the user's login.

Guest Wi-Fi Network

The GUEST wi-fi network is open and free for anyone to use while they are on-site. Note however that all activity is logged and monitored, and any abuse or inappropriate use could lead to disciplinary action.

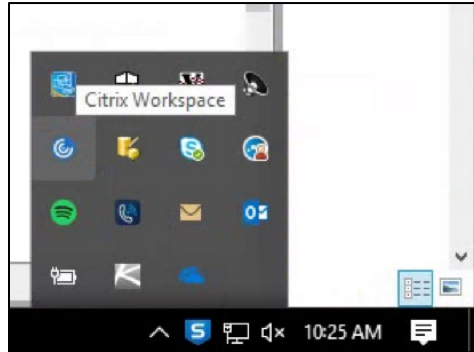
How to Access

On your device, scan the wireless networks available to you and choose the one named GUEST. It will prompt you for a password and you will need to enter “**Minnesota123**” without the quotes.

Citrix

ENPOINTE utilizes Citrix Virtual Apps to deploy the PrintStream MIS throughout the company. This includes the PrintStream Executor toolbar, Shopfloor applications, Job Tickets, and several other applications.

With Citrix all the MIS applications run on a centralized group of servers and not locally on your computer. The component users will interact with primarily is called Citrix Workspace which is installed locally.



When you log in to your computer, your Citrix Workspace application is automatically launched in the background and authenticates using your windows login credentials. Based on your login role, you will receive access to the appropriate applications you will need. Most applications will be shown as shortcuts on your desktop, but they can also be accessed by opening the Citrix Workspace application which is located at the bottom right-hand corner of your screen or in your Windows menu.

PrintStream MIS

ENPOINTE has the PrintStream MIS which was purchased from a vendor named EFI. ENPOINTE has been running PrintStream since 2009 and it is the core system that runs our business. It manages accounting, inventory, estimating, shopfloor data collection, order fulfillment and more.

Shopfloor – What is it?

Hourly employees are required to log their time into PrintStream so that we can track labor as well as the status of jobs being produced.

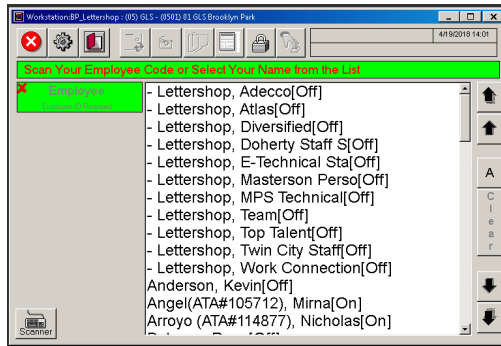
Shopfloor – How to Access?

There are Shopfloor workstations strategically placed around the buildings to allow for hourly employees to easily log their time in PrintStream. The Shopfloor applications are shared out via Citrix Workspace.

If the Shopfloor application is not running, you can launch it simply by double clicking on the desktop shortcut named with your department and has an icon of a clock. See below.

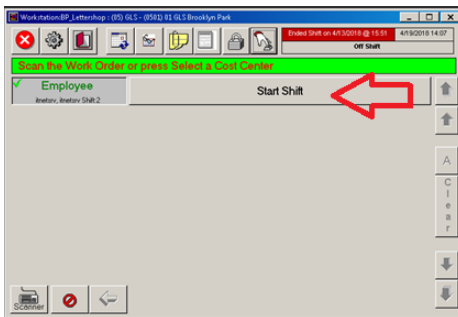


Once you double click on the shortcut, Citrix will open and launch the application. It should look like below once it is up.

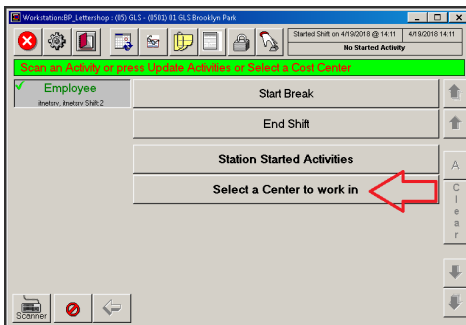


Shopfloor – How to punch in and out?

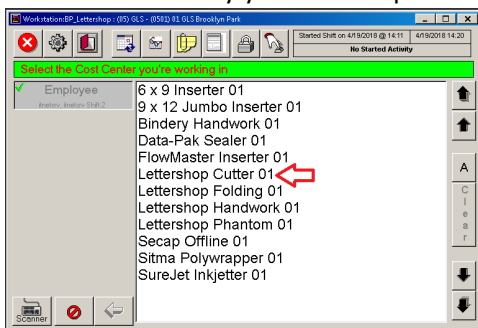
1. Find your name in the list of employees in the shopfloor for your department and then click on it.
2. Click Start Shift



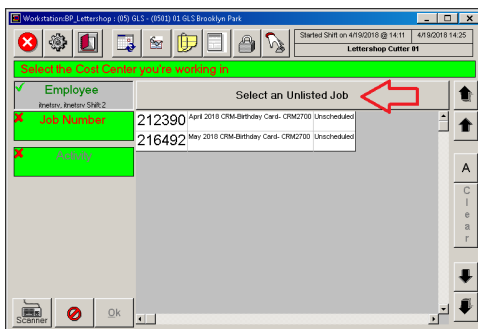
3. Click the “Select a Center to work in” button



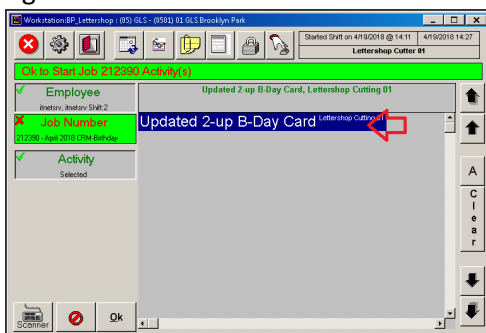
- Click on the activity you want to punch into



- If the job you want to punch into is listed you can click on it, otherwise click on the 'Select an unlisted job' button.



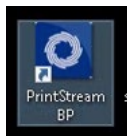
- Next click on the component you are working on. The job may have one or several components listed. Make sure you pick the right one.



- Click OK. You are now logged into the job and can begin work.

How to Access PrintStream

If you are an office employee or are in management, you will likely be using PrintStream to perform various job tasks. The PrintStream Executor is a toolbar application that will be at the top of your screen and will provide access to PrintStream applications depending on your role. This is what your desktop icon looks like.



Please see your individual department's training documentation for instructions on use of individual PrintStream applications.

How to Get Support with PrintStream Issues

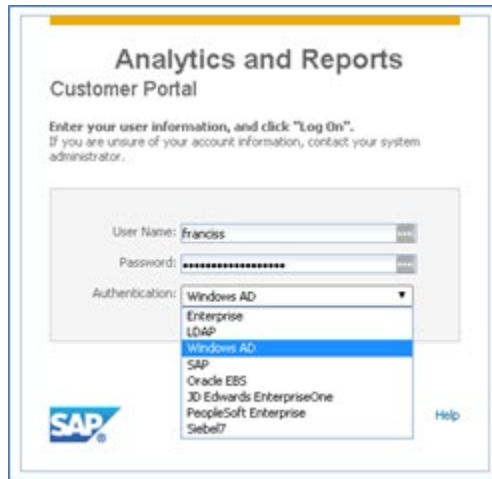
If you have any difficulty using the PrintStream MIS suite, the first thing to do is reboot your system. This will refresh your OS as well as log you out of your Citrix session which will start a new one when you log back in. If your issue persists after the reboot, please submit a TrackIt ticket and provide enough detail about your problem to aid IT in resolving it for you quickly.

Crystal Reports

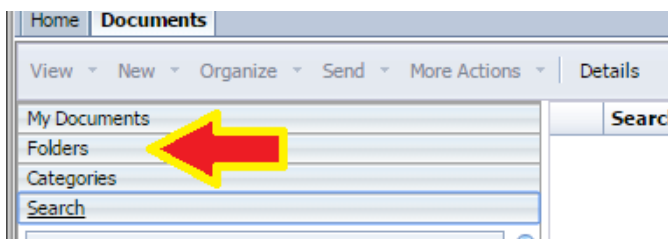
ENPOINTE uses a business intelligence application called Crystal Reports (from SAP Business Objects) to create custom reports from PrintStream and other data sources. Reports can be run manually but some may be scheduled to run automatically and delivered to users via email attachment.

How to Access Crystal Reports

1. Go to this URL: <https://webreports.Alwaysenpointe.com/BOE/BI>
2. Log in using the same login as your computer
 - a. Set the “Authentication” to “Windows AD”
 - b. Enter your username and password
 - c. Click “Log On”
3. Here is a screen shot of what the login screen should look like



4. In the left pane, click the “Folders” bar if the folder view is not shown to you



5. When you browse the folders, you will only see reports which you have been granted access to.
6. Simply double click on the report you want to view. Depending on the report you run, you may be prompted to enter several parameters from drop down menus.

Remote Access - LogMeIn

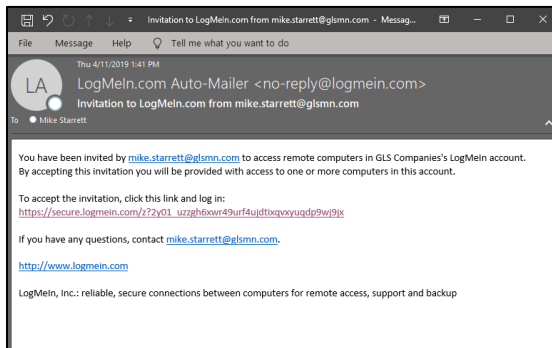
What is It?

ENPOINTE offers the ability to access your workstation from home using LogMeIn. If your job role requires you to have remote access talk to your manager and they can open a TrackIt ticket requesting IT Support to set up access.

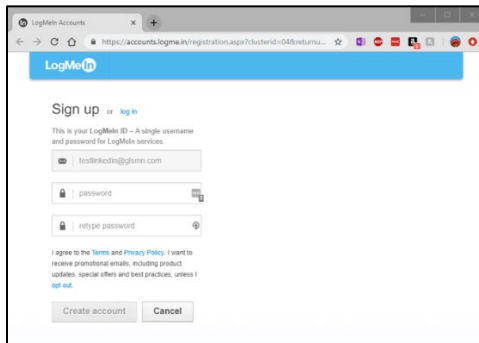
How to Set Up

How to set up your LogMeIn remote access user account

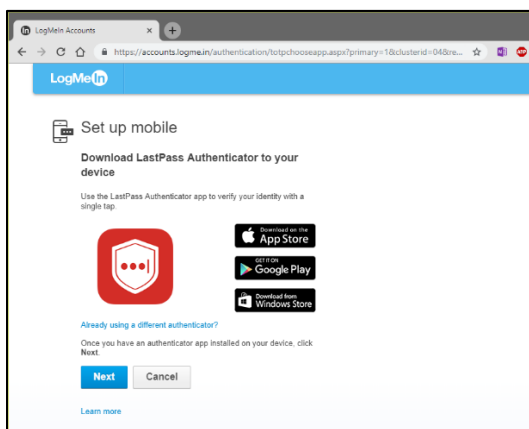
1. Your IT Support representative will generate an automated email from the LogMeIn system which will be sent to your ENPOINTE email box.



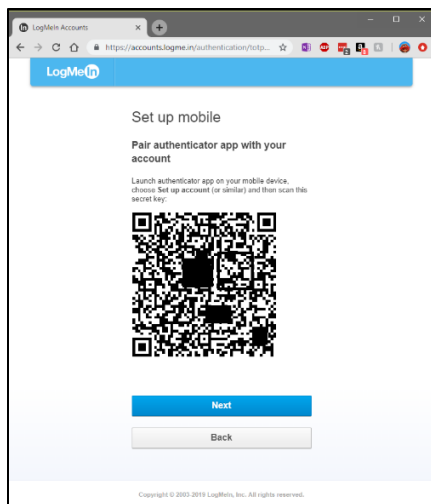
2. Click the link in the email to accept the invitation.



3. Enter in a password of your choosing and then click **Create account**.
4. It will bring you to the login screen where you will now log in with your new account.
5. After logging in it will prompt you to set up two-step verification (2 factor authentication). Click the **Get Started** button.
6. ENPOINTE requires you to use a mobile app for two factor authentication, DO NOT USE the TEXT MESSAGE OPTION. Click the **Set up mobile app** button.
7. ENPOINTE recommends you use the LastPass Authenticator app which you can download for free from the Apple or Google app store. If you already use Google Authenticator or Windows authenticator you may use those instead.
8. After installing the app on your phone, click the **NEXT** button on the web page.



9. Open your Authenticator app on your phone and then add a new site and then use the scan barcode option and then scan the barcode on your computer screen.



10. Once the site is added on your phone go back to the website and click NEXT. You will then be prompted to enter the 6 digit code from your phone to complete the setup.
11. Install LogMeIn client on your home computer.
 - PC - <https://secure.logmein.com/LogMeInIgnition.msi>
 - Mac - <https://secure.logmein.com/LogMeInClientMac.dmg>

If you have trouble getting this to work, please contact ENPOINTE IT Support at x5911 or via email at itsupport@alwaysenpointe.com

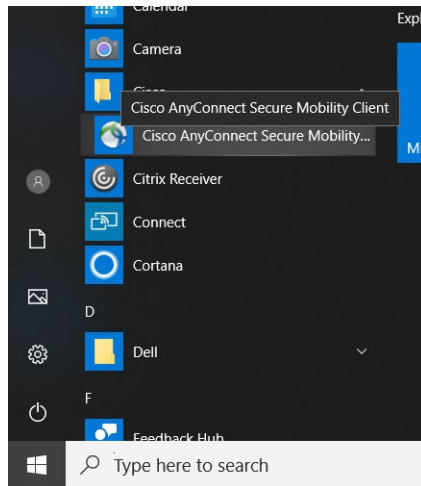
Remote Access - VPN

What is It?

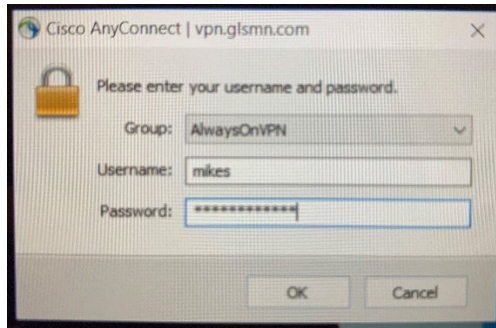
For users who are issued a corporate laptop, we allow remote access to our internal network via a secure VPN connection. This essentially connects your laptop to the corporate network as if you were on site.

How to Set Up

1. Connect your laptop to your internet via wifi or ethernet connection.
2. In your Windows Menu launch “Cisco AnyConnect Secure Mobility Client”



3. Type in the VPN URL if not already populated
 - a. vpn.alwaysenpointe.com
4. Enter your domain username which is your first name and first letter of your last name (FirstL) and then your current password.



5. Read and accept the notice on screen.
6. You are now securely connected to the corporate network and can access all file shares and systems.

Notes

- You will not be able to access any network printers you may have at home while connected to the VPN.
- Opening and accessing large files across the VPN connection will be slower than it would be if you were on site.

FTP System

ENPOINTE hosts its own FTP site on premises to allow secure inbound and outbound transfer of customer files.

How our FTP works

ENPOINTE creates individual user accounts for customer users to allow them access to a private FTP folder on our system. When a customer uploads files to our FTP, it auto-generates an email to the internal CSR group confirming the transfer.

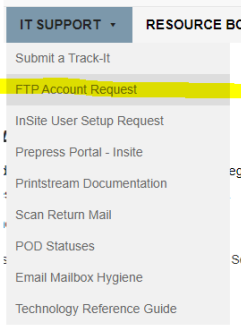
How is FTP access organized and granted?

ENPOINTE organizes all FTP accounts into two basic groups.

- **Open Access:** All CSRs, Premedia, and Data Processing have access to all customer data. This is the default level of security for new FTP account requests.
- **Explicit Access:** This is a more secure section of the FTP system. Client folder access is strictly managed to ensure that only those who need access to the data get access. Customers that do any PHI or SPII work with ENPOINTE will default to being placed into this group. If a client approaches ENPOINTE about other security concerns, ENPOINTE will place the customers FTP into this folder.

Requesting New External FTP User Setup

If you are a CSR or Sales Rep and would like a new FTP user account created, please fill out the online account request form located on our Intranet underneath the IT Support menu.



How an External FTP User Can Reset Their Password

If a customer comes to you saying they have forgotten their password, they can simply reset their password by going to the FTP site and clicking the Recover Password link. They will be prompted to enter their user ID. User IDs are usually the customer name or their email address. This will trigger an email to them with a link to reset their password.



How to Get Help With FTP Issues

If you or your customer has trouble accessing the ENPOINTE FTP system, please submit a TrackIt ticket with adequate detail and someone will assist you as soon as possible.

Xerox Copiers

Locations

ENPOINTE has Xerox copiers strategically located throughout the business. There are copiers in the Sales/Client Services areas at both locations, as well as in Accounting, Purchasing, Distribution, and Shipping areas at the Brooklyn Park location.

Desktop Printers

Paper and Toner Replenishment

If your workstation is equipped with a desktop printer, you can attain replacement toner by contacting the front desk at Brooklyn Park.

Order toner by calling

x5200

Getting help

If your printer isn't functioning correctly and you have already cleared all the paper jams and restarted it, you should open a TrackIt ticket to get support.

Resource Board

Purpose

ENPOINTE has written a custom application which allows all employees to easily view other employee's availability status. All office staff are required to log in and out of the Resource Board when they are in and out of the building. It is also utilized to indicate if a user is working at another physical location or currently on vacation.

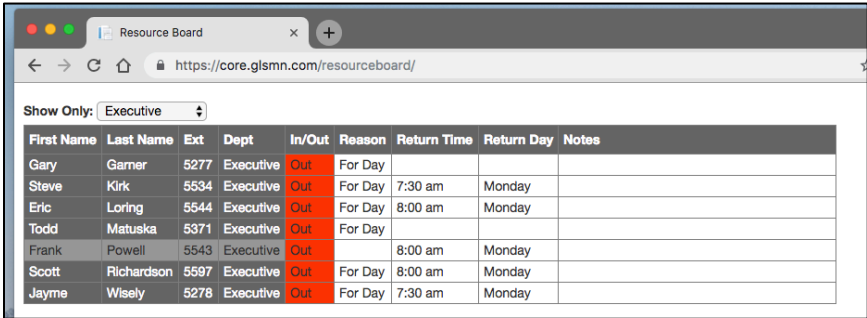
How to Access

The Resource Board is a web-based application that can be accessed both inside and outside the ENPOINTE corporate network. Below is the link.

<https://core.alwaysenpointe.com/resourceboard/>

If you access it internally on your office computer, it will automatically log you in. If you access it from outside the corporate network, it will require you to enter your desktop login credentials. For example, GaryG as the username and then your current password.

How to Use



The screenshot shows a web browser window with the address bar displaying "https://core.glsmn.com/resourceboard/". Below the address bar is a search bar labeled "Show Only:" with a dropdown menu set to "Executive". Below this is a table with the following columns: First Name, Last Name, Ext, Dept, In/Out, Reason, Return Time, Return Day, and Notes. The table contains 10 rows of employee data, all of whom are in the "Executive" department and have a status of "Out".

First Name	Last Name	Ext	Dept	In/Out	Reason	Return Time	Return Day	Notes
Gary	Garner	5277	Executive	Out	For Day			
Steve	Kirk	5534	Executive	Out	For Day	7:30 am	Monday	
Eric	Loring	5544	Executive	Out	For Day	8:00 am	Monday	
Todd	Matuska	5371	Executive	Out	For Day			
Frank	Powell	5543	Executive	Out		8:00 am	Monday	
Scott	Richardson	5597	Executive	Out	For Day	8:00 am	Monday	
Jayne	Wisely	5278	Executive	Out	For Day	7:30 am	Monday	

- Once logged in to Resource Board you can select the department you want to view from the drop down at the top.
- To log in or out simply double click on your name.
- Another way to change your status is to right click on your name and then select an option from the list.
- You can specify a Reason, Return Time, Return Day by right clicking on the field and choosing a value.
- You may enter a note by right clicking on the Notes field. This is often used to indicate which physical location you are working at or comment about return date if on vacation.
- You can access the Resource Board on any mobile device by accessing the URL in your device's browser and logging in.

InSite Proofing Portal

Purpose

ENPOINTE utilizes a tool from Kodak called InSite Proofing to allow users internally and externally to view Premedia production files in real time.

These are files that are currently in production in the Prinergy Workflow system.

How to Access

You will need a login in order to access InSite. You can contact the Premedia Manager or submit a TrackIt ticket to IT to get set up if you have not already been given a login at time of hire.

<https://insite.alwaysenpointe.com>

How to Use

If you need information on how to use the InSite portal, please contact the Premedia Manager and they will provide you with a training guide.

Getting Help

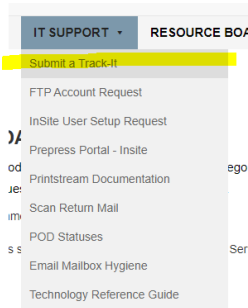
You can contact the Premedia Manager for user or workflow questions, otherwise contact IT via TrackIt if you have system access issues.

Contact IT Support

Always use TrackIt as your primary method of requesting support. If you need immediate IT assistance, however, please contact the phone number or email below.

Submit a TrackIt

Go to the Intranet and click IT Support and then Submit a TrackIt.



OR

<http://10.0.0.131/TrackItWeb/SelfService/Account/Login>

Phone Numbers

Internal Phone: **5911**

External Phone: **763-592-0591**

Email: ITSupport@alwaysenpointe.com