synchrony

Setup Instructions

Select the type of equipment you have to setup:

PC

Setup instructions

Mac

Setup instructions

Mobile

Setup instructions

To return the equipment follow the instructions below:

Computer



Any kind of computer. Chromebooks, PC or Mac.



Mobile



Instructions on how to return a mobile device.



Need technology assistance or missing equipment? Call 1-800-754-0385 or click here.

synchrony

Mac Setup Instructions

The following 10 pages will guide you through setting up your Synchrony Macbook. Please read and follow the directions carefully.

For Existing Employees

To **return your Synchrony equipment**, please see step 10 for instructions.

Table of content

1. Mac initial logon
2. Extending Beyond Identity Passkey
3. Zscaler
4. Password reset
5. Open Email, Word, Excel, OneNote
6. Login to One Drive
7. Open Teams
8. Confirm Carbonite is running
9. Load PST file (if applicable)
10. Equipment return instructions

Need technology assistance or missing equipment? Call 1-800-754-0385 or click here.

Back

Go to 1. Mac initial lo...

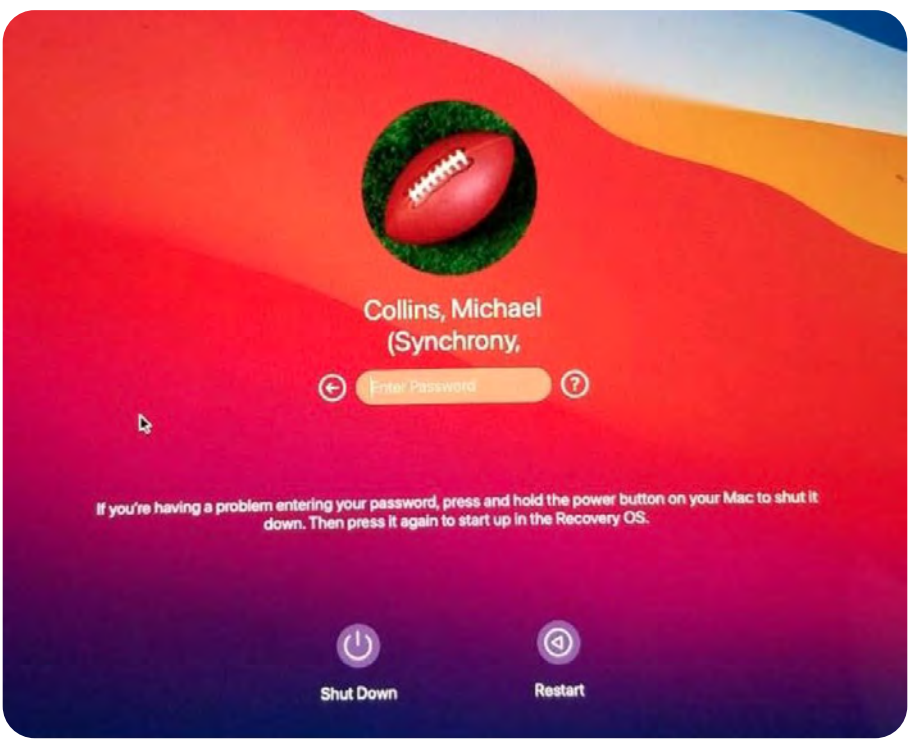
synchrony

Mac initial logon

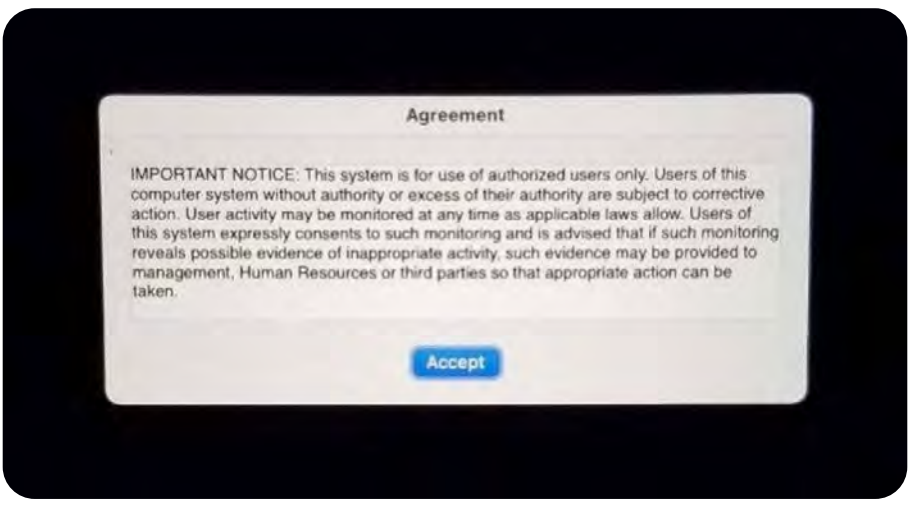
1. Power on the Mac.
2. Upon boot up, a logon screen should appear.
3. Select your profile (picture is an example).



4. Enter ADSYF password then press the `return` key.



5. Read the Agreement then click accept or `return` key.



Go to 2. Extending Beyon...

Back to table of content

synchrony

Extending Beyond Identity Passkey

Beyond identity

Beyond Identity is typically already installed on SYF Laptops and pre-enrolled with passkey.
If you need to extend the passkeys, follow these instructions:

1. Open Beyond Identity software on your primary device and follow the instructions below.
2. Now, click **"Set up other devices"** > Beyond Identity will enforce for OS verification **"Enter your AD password"** to view the QR code or 9-digit registration code to enroll the new device.



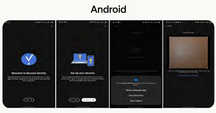
3. Steps to extend the passkey on secondary computer device.
4. Open Beyond Identity app, click **"Next"** > select **"Enroll with existing device"** > select **"Enter the 9-digit code"** > now, type the code generated on primary device.
5. As soon as the 9-digit code is entered, passkey set up successfully.



Steps to extend the passkey to mobile devices

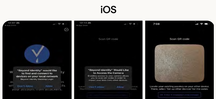
6. Follow the instructions given below for Android and iOS devices.
   a. Open the Beyond identity app on your android and click **Next**, allow notifications and click **Get started** and allow notification access to the camera.

Android



   b. Open Beyond identity app on iOS device and click allow notifications and click **Next** and allow access to the camera.

iOS



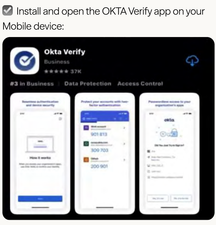
   c. Now, you can either scan the QR code (method 1) or type in the 9-digit code (method 2) to enroll the passkey.



Registration Guide to Set up OKTA Verify – Beyond Identity Users (w/o YubiKey)

Steps to Set up OKTA Verify on your Mobile

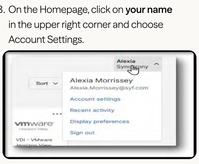
☑ Install and open the OKTA Verify app on your Mobile device:



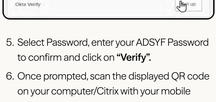
1. Open the app, click on **"Get Started"** and then select **"Next"** to add account.
2. Under **"Choose Account Type"** select **"Organization"**, then click **"Skip"** and choose **"Yes, Ready to Scan"**.
3. Allow/Enable all the prompts: Enable Face ID/Biometrics or password confirmation, then enable Bluetooth, Camera and Push Notifications.

To get the QR Code:

1. On your laptop or in Citrix, open a browser and type sso.synchronyfinancial.com
2. Enter your SSO and complete Beyond Identity Authentication as usual.
3. On the Homepage, click on **your name** in the upper right corner and choose Account Settings.



4. Scroll down to **"Security Methods"** and select **"Setup"** next to Okta Verify.



5. Select Password, enter your ADSYF Password to confirm and click on **"Verify"**.
6. Once prompted, scan the displayed QR code on your computer/Citrix with your mobile phone application to complete setup on your laptop/Citrix.

FAQs

Q. Why do I need to allow Bluetooth?
A. Okta Verify uses Bluetooth primarily for device-to-device account transfers and authentication. It allows your phone and computer to securely communicate, verifying that both devices are in the immediate vicinity to prevent remote, long-distance hacking or phishing attacks.

Q. Why do I need to allow Camera Access?
A. The app will use your camera to scan a QR Code to setup your account.

Q. Why do I need to allow Push Notifications?
A. OKTA Verify requires notifications be sent to your phone when a device is attempting to use OKTA.

Q. Is using Face ID mandatory?
A. No, you can choose to enable and use Face ID or simply use your passcode.

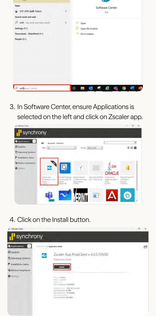
Go to 3. Zscaler

Back to table of content

Zscaler

Zscaler is typically already installed on SYF Laptops. If you need to install the Zscaler App, follow these instructions:

1. Ensure you are connected to the Synchrony network via ENGAGE, F5 VPN or wired in a Synchrony business center.
2. Go to the Start Menu and locate the Software Center icon or search for Software Center in the search bar located at the lower left of your screen.



3. In Software Center, ensure Applications is selected on the left and click on Zscaler app.



4. Click on the Install button.



5. When the installation is finished, you should see a small Z cloud symbol on your task bar or hidden icons bar.



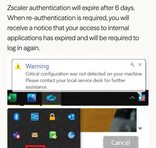
6. A login window will appear the first time you launch your Zscaler. Login using your primary Synchrony SSO or email address and your ADSYF password.



7. If you are using Zscaler for remote access you will see a second login. Login using SSO.

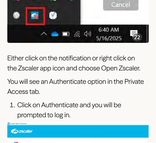


8. You will then receive identity verification screen. Since the Beyond Identity is pre-enrolled your identity will be validated with Beyond Identity Passkey.



9. When all logins are completed successfully, the window should disappear and the exclamation mark will disappear from the icon.

Note: After authentication, no need to reboot. Close and reopen apps if they are not responding.



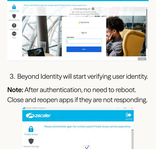
10. To check the status of your connections to the Internet Security and Private Access services:

Right click on the Zscaler app icon in the task bar and select Open Zscaler.



11. The Lock icon shows the status of your connection to internal applications.

The Authentication Status will show Authenticated if green when connected.



Re-Authenticating in Zscaler

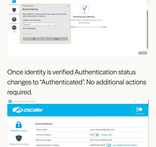
Zscaler authentication will expire after 6 days. When re-authentication is required, you will receive a notice that your access to internal applications has expired and will be required to log in again.



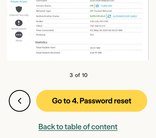
Either click on the notification or right click on the Zscaler app icon and choose Open Zscaler.

You will see an Authenticate option in the Private Access tab.

1. Click on Authenticate and you will be prompted to log in.



2. Login using SSO and password.



3. Beyond Identity will start verifying user identity.

Note: After authentication, no need to reboot. Close and reopen apps if they are not responding.



4. Beyond Identity will enforce for OS verification as per the Organizations' security policy, enter your AD password to complete the authentication process.

Once identity is verified Authentication status changes to "Authenticated." No additional actions required.

Go to 4. Password reset

Back to table of content

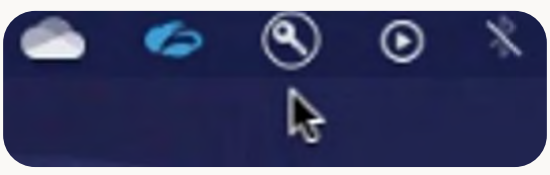
synchrony

Password Reset

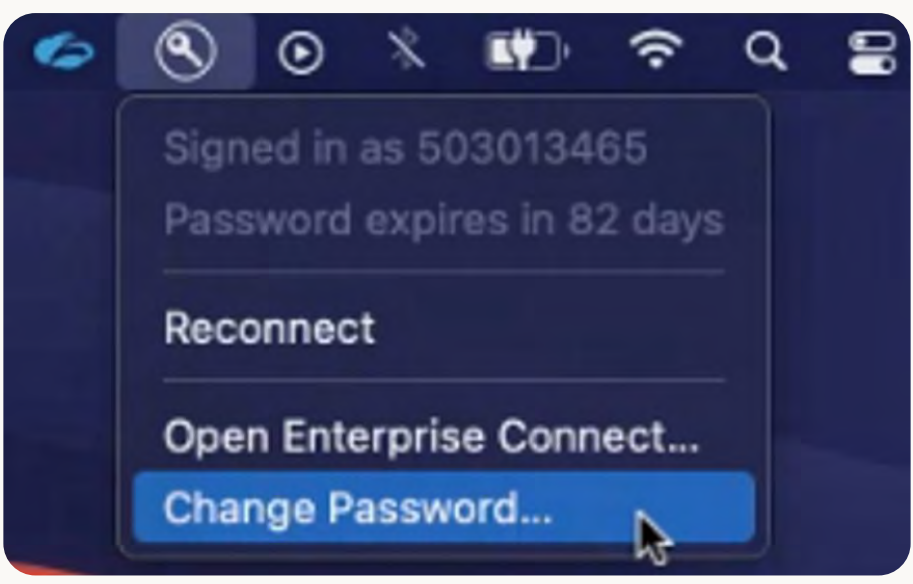
If you received your password from any source, you are required to change your password at the first opportunity to a unique password only you know.

To change your password, do the following:

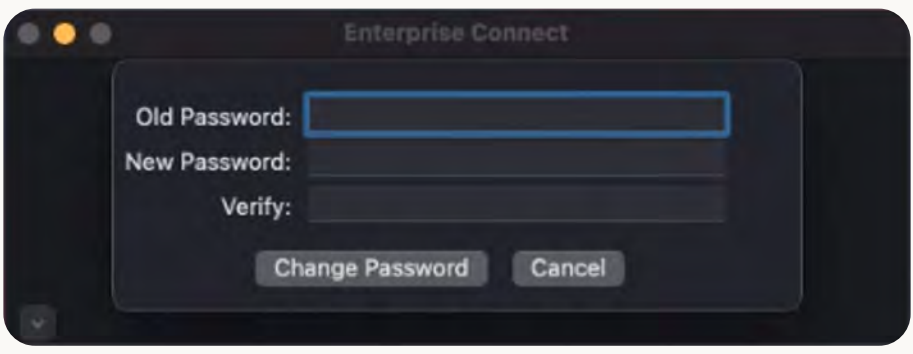
1. Click on **Enterprise Connect** icon on the menu bar, typically at the top of your desktop screen.



2. Click on **Change Password**.



3. Type in your old password followed by a new password and verify that they are the same.



4. Click on Change password – if password is accepted, this change is complete.

Notes: Synchrony Password Requirements:

- Your password must contain a Capital letter.
- Your password must contain two ② embedded numbers.
- Your password must contain one ① special character.
- Your password must start and end with either a letter or a special character.
- Your password must contain no fewer than 12 characters.
- Your password must not match one of your last 10 passwords.
- Your password must not include your display name.

synchrony

Open Email, Word, Excel, OneNote

To access Microsoft Outlook, Word or Excel, you can access it from the **'Dock'** or via **Applications**.



Click on the **Outlook, Excel, Word** or **OneNote** button which will appear in the Dock menu.

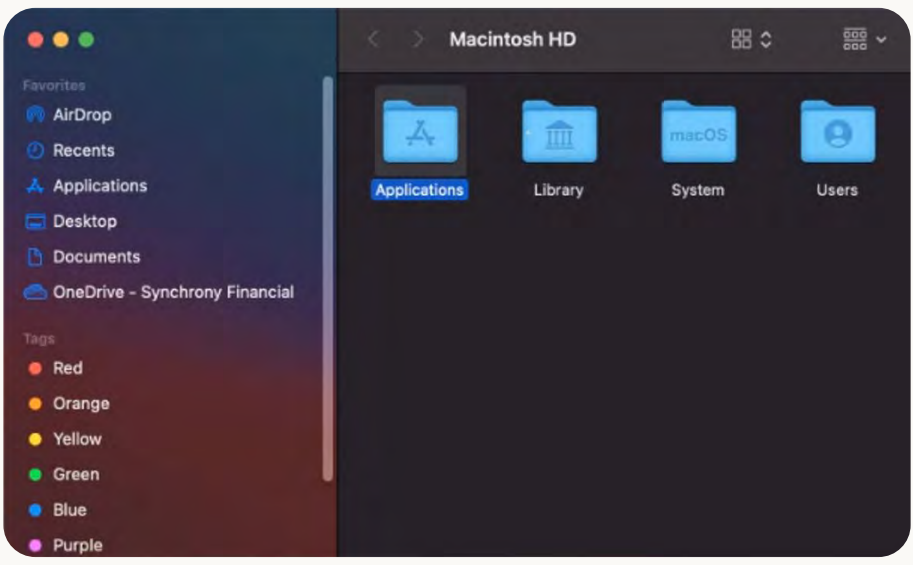


Or access all applications by doing the following:

From your desktop screen, click on **Macintosh HD**.



Double click on **Applications**, then find the application you wish to open and double click on it.







Carbonite Endpoint.app

Go to 6. Login to One Drive

Back to table of content

synchrony

Login to One Drive

To access Microsoft OneDrive, you can access it from the **'Dock'** or via **Applications**.



Click on the **OneDrive** button which will appear in the Dock menu.



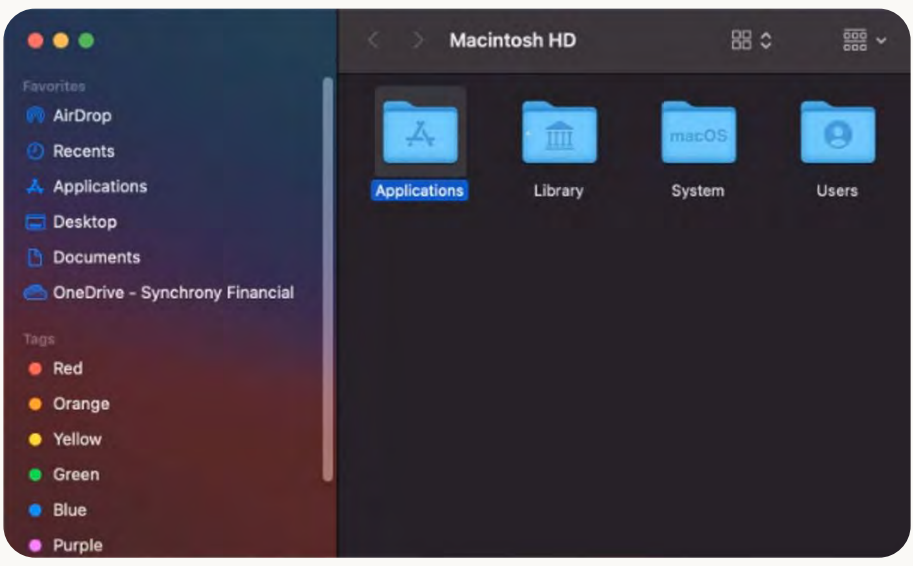
Microsoft OneDrive.app

Or access all applications by doing the following:

From your desktop screen, click on **Macintosh HD.**



Double click on **Applications**, then find the application you wish to open and double click on it.





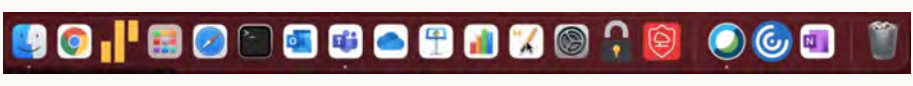
*** If prompted to log in – use your ADSYF SSO/ Password.**

Go to 7. Open Teams

Back to table of content

Open Teams

To access Microsoft Teams, you can access it from the **'Dock'** or via **Applications**.



Click on the **Teams** button which will appear in the Dock menu.



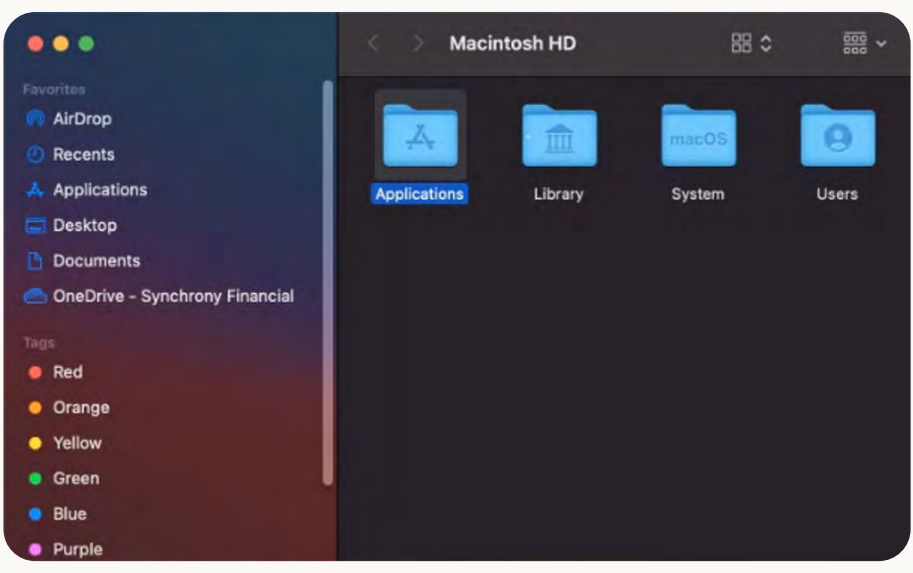
Microsoft Teams.app

Or access all applications by doing the following:

From your desktop screen, click on **Macintosh HD**.



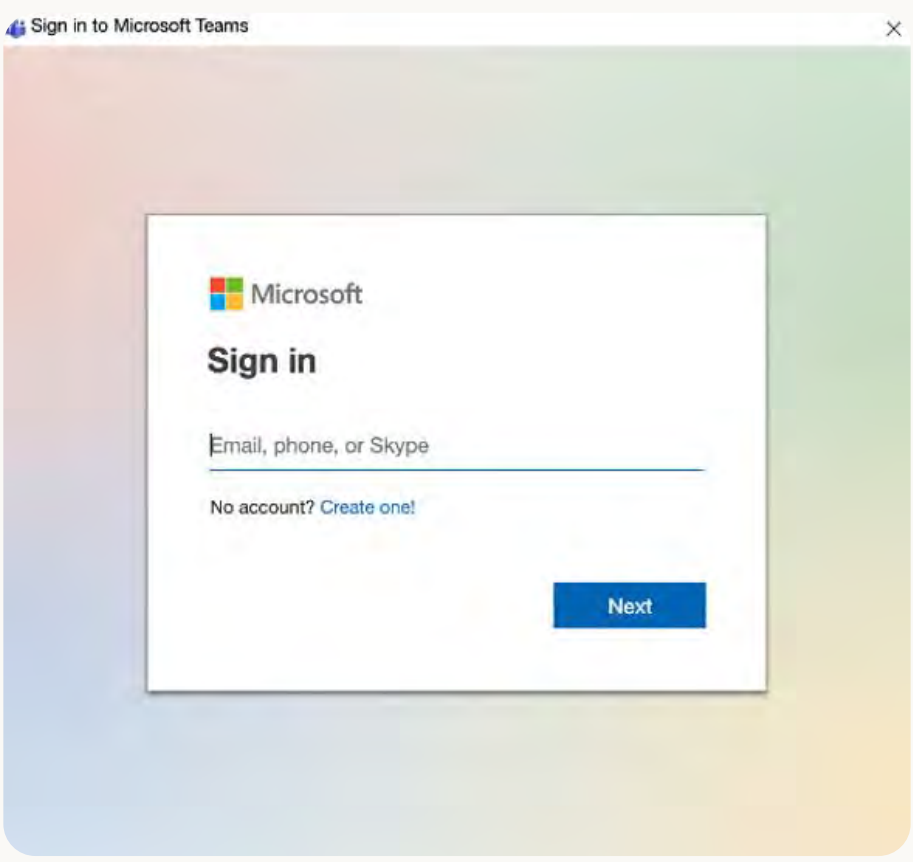
Double click on **Applications**, then find the application you wish to open and double click on it.



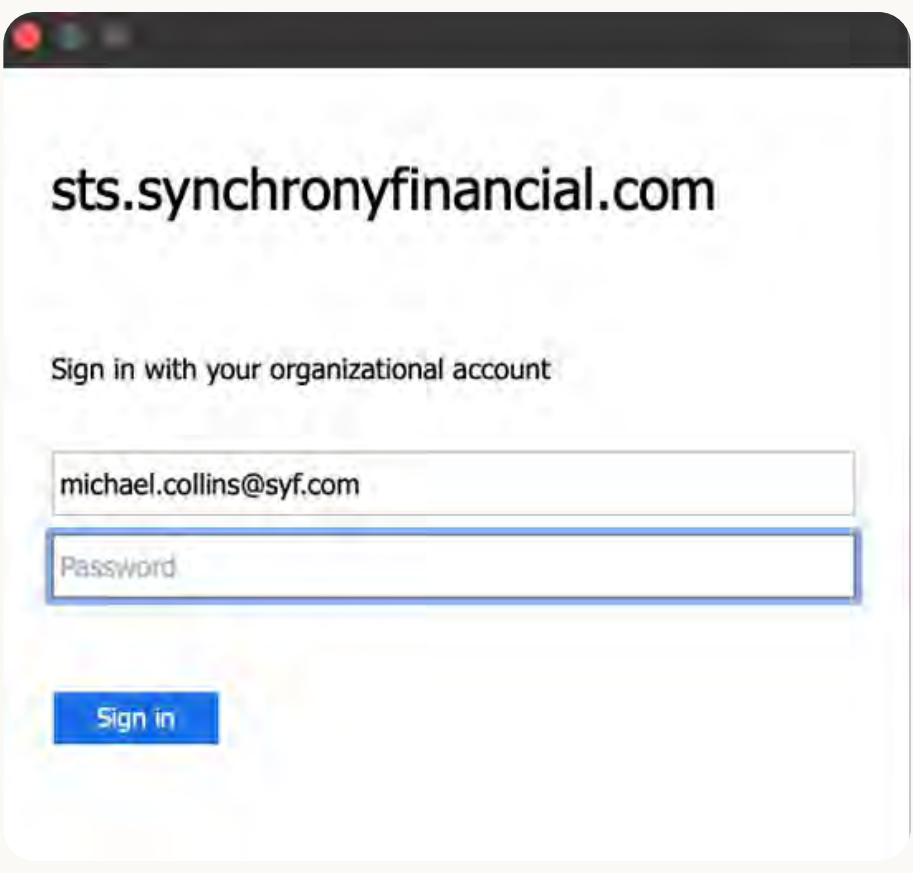


* If prompted to sign in

Type in your Synchrony email address (example: Firstname.Lastname@syf.com) then click **Next**.



Enter your ADSYF Password then click Sign in.



Go to 8. Confirm Carbon...

Back to table of content

synchrony

Confirm Carbonite is running

To access Carbonite, you can access it via **Applications** by doing the following:

From your desktop screen, click on **Macintosh HD**.

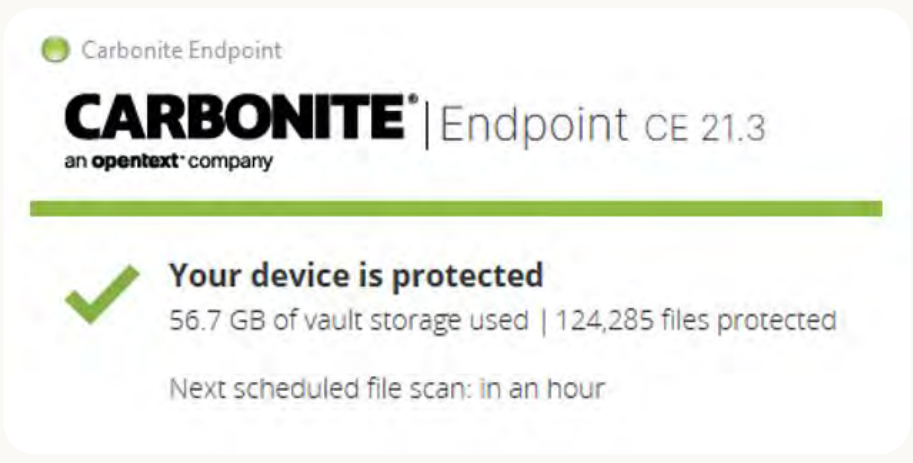


Double click on **Applications**, then find the application you wish to open and double click on it.

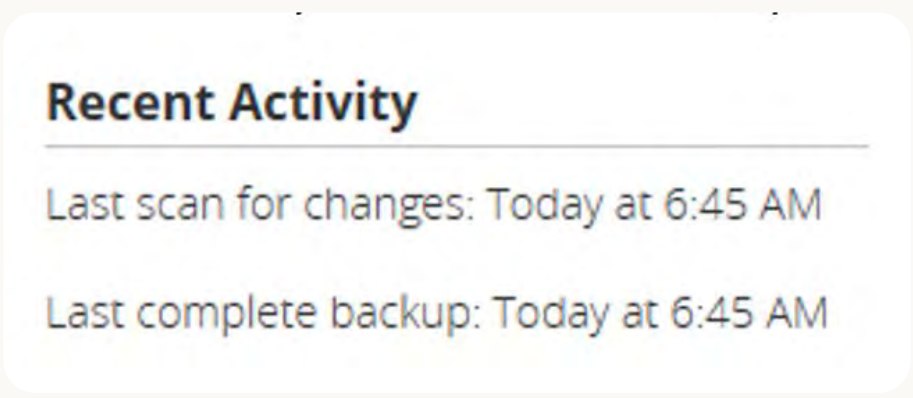


Carbonite Endpoint.app

Look for green check mark showing your device is connected.



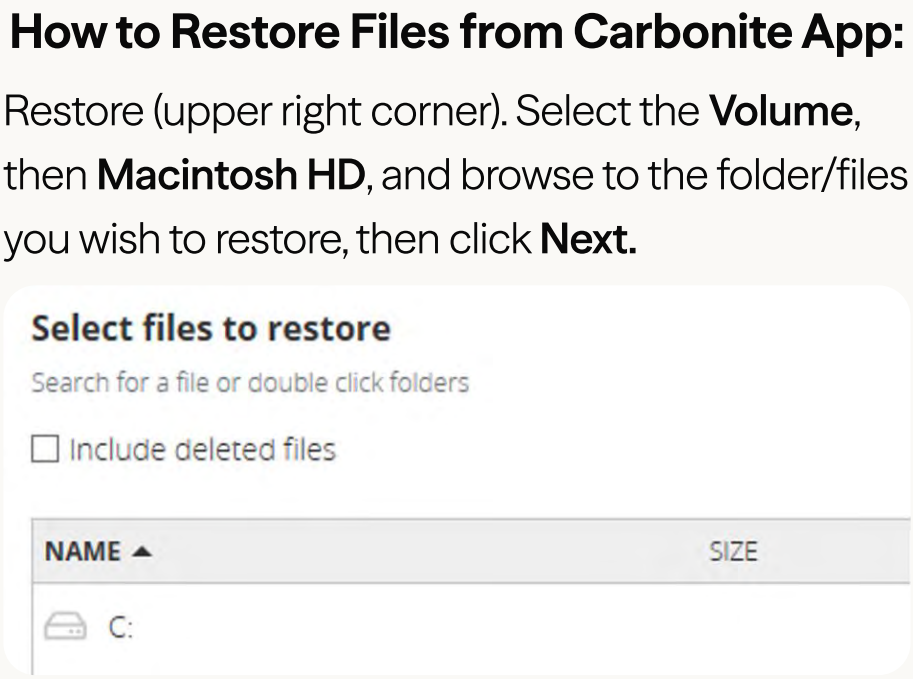
Review Activity to confirm recent activity.



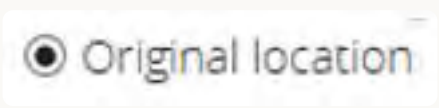
If you believe Carbonite is not working, please open a helpdesk incident https://syf.service-now.com/techcompass

How to Restore Files from Carbonite App:

Restore (upper right corner). Select the **Volume**, then **Macintosh HD**, and browse to the folder/files you wish to restore, then click **Next.**



To restore files to original location – select



Click Restore to continue – Cancel if needed.



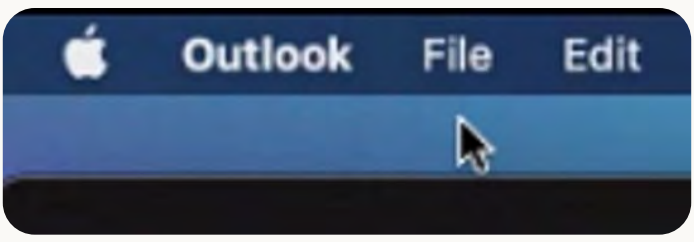
Go to 9. Load PST file

Back to table of content

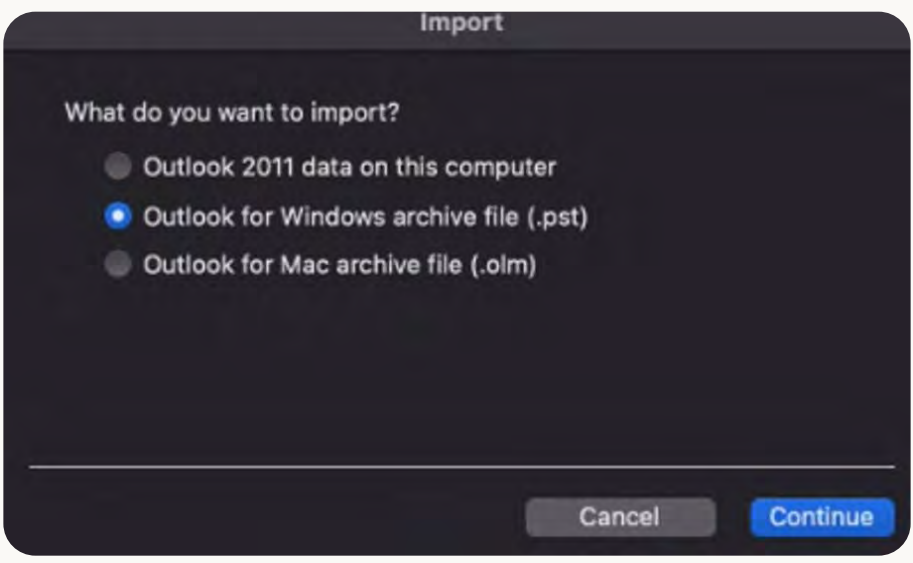
synchrony

Load PST file (if applicable)

1. Open **Outlook**
2. Click on **File** in upper left menu.



3. Click on **Import** then check **"Outlook for Windows Archive file (.pst)"**, then **Continue**.



4. Browse to file location then select target file, then click **Import**.

Data file (PST) will open and be available by clicking on that **file** in the left view pane.

5. When the import process is complete, select **Done**.

The imported items appear in the navigation pane under **On My Computer** in Outlook.

6. Once completed, save user's .pst to the local **Documents** folder as an .OLM file.

* Synchrony does not recommend the use of PST or OLM files. Each SYF O365 account comes standard with a large capacity. If you wish to stop using PST files, you can upload your files to O365 and discontinue using PST files by disconnecting them from your Outlook profile.

synchrony

Equipment Return Instructions

Synchrony box for Suspension box (Packing has built in foam or suspends asset in middle of box)

- Using the same Packing material / wrapping provide with the delivery of your new device
  - Please Laptop / Chromebook in the Synchrony Box with foam or in between the plastic sleeve for the suspension box.
  - Use extra room for any peripherals, cords, cables, power supplies, etc.
  - Synchrony box – please insert Synchrony box into provided sleeve

Standard Box with bubble wrap

- Using the same Packing material / wrapping provide with the delivery of your new device
  - Boxes and/or bubble wrap have been provided for the return of electronic assets to Synchrony
  - Please use the bubble wrap provided to wrap equipment being returned
  - Laptops, Chromebooks, MACs, Avaya phones, should have 2-3" of bubble wrap on all sides.
  - For surplus open space, please use any extra bubble wrap + clean wadded up newspaper to fill these open areas.

All – Continued

- Tape box shut:
  - Please secure the box openings with 2" or 3" wide packing tape.
  - Optional: Most staffed FedEx locations can tape the box shut for you if you do not have tape.
- Return label
  - Secure the provided return FedEx shipping label to the top of the box or on to SYF box sleave.
  - Ensure original TO: label is covered or marked out
  - Optional: Provide label to the shipping agent, who can assist you with applying it.

* Please do not ship any personal belongings to Synchrony

synchrony

PC Setup Instructions

The following 11 steps will guide you through setting up your Synchrony PC. Please read and follow the directions carefully.

For Existing Employees

To **return your Synchrony equipment**, please see step 11 for instructions.

Table of content

1. Checkpoint Encryption Login
2. Extending Beyond Identity Passkey
3. Zscaler
4. Password Reset
5. Open Email
6. Login to OneDrive
7. Open Teams
8. Confirm Carbonite is running
9. Load PST file (if applicable)
10. SEE Self-Recovery Setup
11. Equipment Return Instructions

Need technology assistance or missing equipment? Call 1-800-754-0385 or click here.

Back

Go to 1. Checkpoint...

Checkpoint Encryption Login

1. Power on PC.
2. Pre-boot screen will appear.



3. Press any key to continue.



4. Enter your username and ADSYF password then press the Enter key.

- Press F3 : Show the password being typed.
- Press tab or shift + tab to toggle between username, password and domain.

If your username and password is accepted, the PC will boot into the Windows Operating system.

Because Checkpoint Encryption caches your password, your PC should boot directly into your Windows profile after you click to pass the SYF user acceptance message.

Extending Beyond Identity Passkey

Beyond identity

Beyond Identity is typically already installed on SYF Laptops and pre-enrolled with passkey. If you need to extend the passkeys, follow these instructions:

1. Open Beyond Identity software on your primary device and follow the instructions below.
2. Now, click **"Set up other devices"** > Beyond Identity will enforce for OS verification **"Enter your AD password"** to view the QR code or 9-digit registration code to enroll the new device.



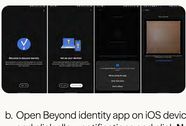
3. Steps to extend the passkey on secondary computer device.
4. Open Beyond Identity app, click **"Next"** > Select **"Enroll with existing device"** > Select **"Enter the 9-digit code"** > Now, type the code generated on primary device.
5. As soon as the 9-digit code is entered, passkey set up successfully.



Steps to extend the passkey to mobile devices

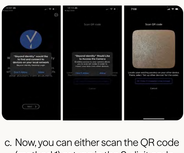
6. Follow the instructions given below for Android and iOS devices.
   a. Open the Beyond identity app on your android and click **Next,** allow notifications and click **Get started** and allow notification & access to the camera.

Android:

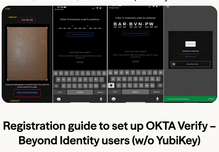


   b. Open Beyond identity app on iOS device and click allow notifications and click **Next** and allow access to the camera.

iOS:



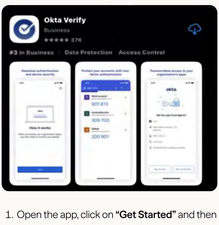
   c. Now, you can either scan the QR code (method 1) or type in the 9-digit code (method 2) to enroll the passkey.



Registration guide to set up OKTA Verify – Beyond Identity users (w/o YubiKey)

Steps to Set up OKTA Verify on your Mobile

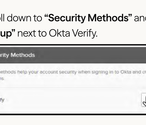
☑ Install and open the OKTA Verify app on your Mobile device:



1. Open the app, click on **"Get Started"** and then select **"Next"** to add account.
2. Under **"Choose Account Type"** select **"Organization"**, then click **"Skip"** and choose **"Yes, ready to scan"**.
3. **Allow/Enable** all the prompts: Enable Face ID/ Biometrics or password confirmation, then enable Bluetooth, Camera and Push Notifications.

To get the QR Code:

1. On your laptop or in Citrix, open a browser and type sso.synchronyfinancial.com
2. Enter your SSO and complete Beyond Identity Authentication as usual.
3. On the Homepage, click on your Name in the upper right corner and choose Account Settings.



4. Scroll down to **"Security Methods"** and select **"Setup"** next to Okta Verify.



5. Select Password, enter your ADSYF Password to confirm and click on "Verify".
6. Once prompted, scan the displayed QR code on your computer/Citrix with your mobile phone application to complete setup on your laptop/Citrix.

FAQs

Q. Why do I need to allow Bluetooth?

A. Okta Verify uses Bluetooth primarily for device-to-device account transfers and authentication. It allows your phone and computer to securely communicate, verifying that both devices are in the immediate vicinity to prevent remote, long-distance hacking or phishing attacks.

Q. Why do I need to allow Camera Access?

A. The app will use your camera to scan a QR Code to setup your account.

Q. Why do I need to allow Push Notifications?

A. OKTA Verify requires notifications be sent to your phone when a device is attempting to use OKTA.

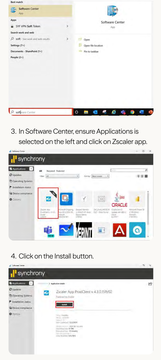
Q. Is using Face ID mandatory?

A. No, you can choose to enable and use Face ID or simply use your passcode.

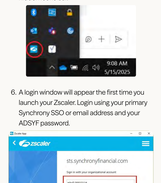
Zscaler

Zscaler is typically already installed on SYF Laptops. If you need to install the Zscaler App, follow these instructions:

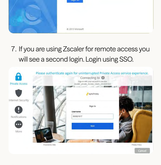
1. Ensure you are connected to the Synchrony network via ENGAGE, F5 VPN or wired in a Synchrony business center.
2. Go to the Start Menu and locate the Software Center icon or search for Software Center in the search bar located at the lower left of your screen.



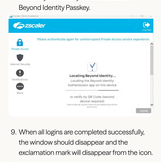
3. In Software Center, ensure Applications is selected on the left and click on Zscaler app.



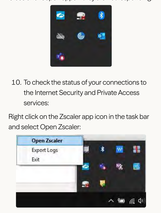
4. Click on the Install button.



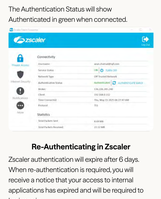
5. When the installation is finished, you should see a small Z cloud symbol on your task bar or hidden icons bar.



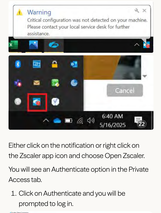
6. A login window will appear the first time you launch your Zscaler. Login using your primary Synchrony SSO or email address and your AD/LDAP password.



7. If you are using Zscaler for remote access you will see a second login. Login using SSO.

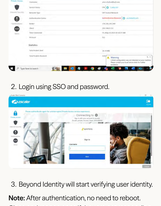


8. You will then receive identity verification screen. Since the Beyond identity is pre-enrolled your identity will be validated with Beyond Identity Passkey.



9. When all logins are completed successfully, the window should disappear and the exclamation mark will disappear from the icon.

Note: After authentication, no need to reboot. Close and reopen apps if they are not responding.



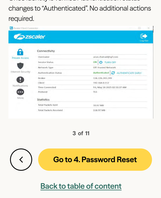
10. To check the status of your connections to the Internet Security and Private Access services:

Right click on the Zscaler app icon in the task bar and select Open Zscaler:



11. The Lock icon shows the status of your connection to internal applications.

The Authentication Status will show Authenticated in green when connected.



Re-Authenticating in Zscaler

Zscaler authentication will expire after 6 days. When re-authentication is required, you will receive a notice that your access to internal applications has expired and will be required to log in again.



Either click on the notification or right click on the Zscaler app icon and choose Open Zscaler.

You will see an Authenticate option in the Private Access tab.

1. Click on Authenticate and you will be prompted to log in.

2. Login using SSO and password.

3. Beyond Identity will start verifying user identity.

Note: After authentication, no need to reboot. Close and reopen apps if they are not responding.

4. Beyond Identity will enforce for OS verification as per the Organizations' security policy, enter your AD password to complete the authentication process.

Once identity is verified Authentication status changes to "Authenticated". No additional actions required.

Go to 4. Password Reset

Back to table of content

Password Reset

If you received your password from any source, you are required to change your password at the first opportunity to a unique password only you know.

To change your password, do the following:

1. On your keyboard, press the CTRL ALT Delete keys simultaneously.

2. Click on **Change a password**.



Your ADSYF should already be populated with your SSO.

3. Follow instructions then click the → to the right of the Confirm password box.



Go to 5. Open Email

Back to table of content

synchrony

Open Email

Click on the **Outlook** button which will appear in the start menu.



Outlook will open.

***If prompted to log in – use your ADSYF SSO/Password**

Go to 6. Login to OneDrive

Back to table of content

synchrony

Login to OneDrive

Click on the start windows logo on the Start Bar.

Click on the **OneDrive** button which will appear in the start menu.



OneDrive will open.

***If prompted to log in – use your ADSYF SSO/Password**

Go to 7. Open Teams

Back to table of content

Open Teams

Click on the start windows logo on the Start Bar.

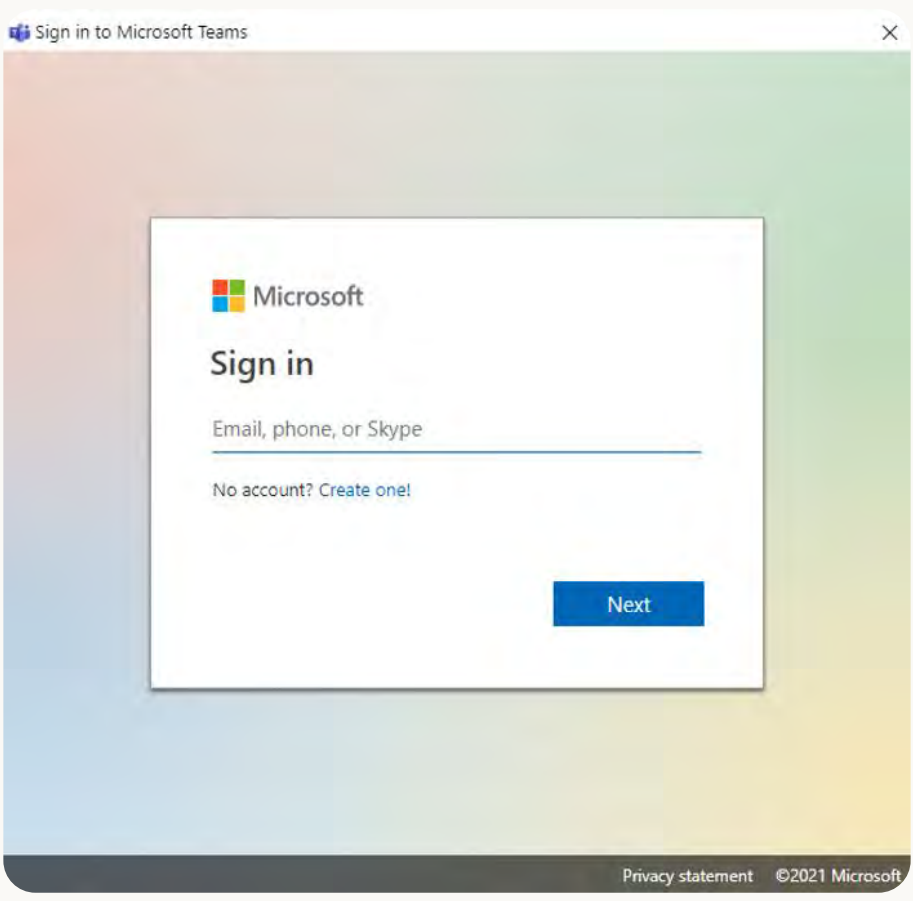
Click on the **Teams** button which will appear in the start menu.



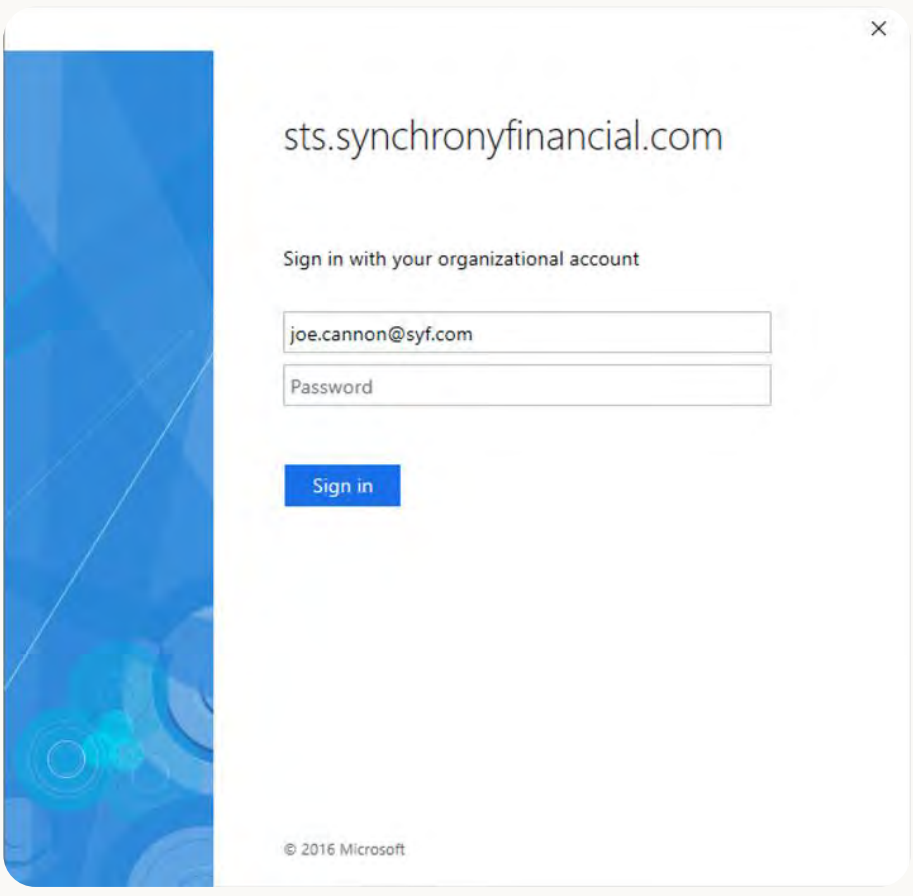
Teams will open.

***If prompted to sign in:**

Type in your Synchrony email address (example: Firstname.Lastname@syf.com) then click Next.



Enter your ADSYF Password then click **Sign in**.



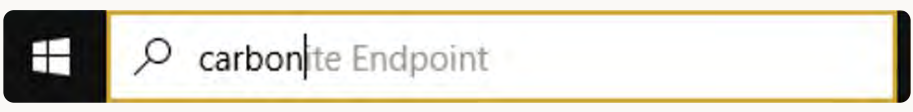
Go to 8. Confirm Carbon...

Back to table of content

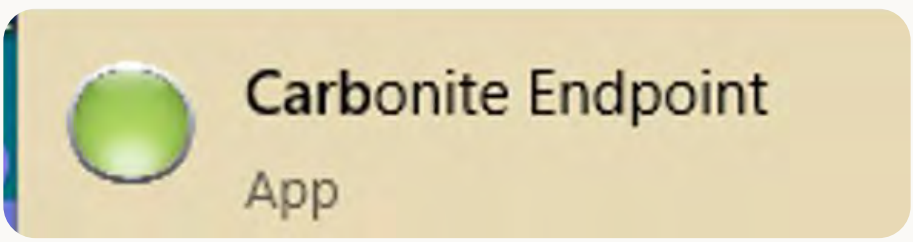
synchrony

Confirm Carbonite is running

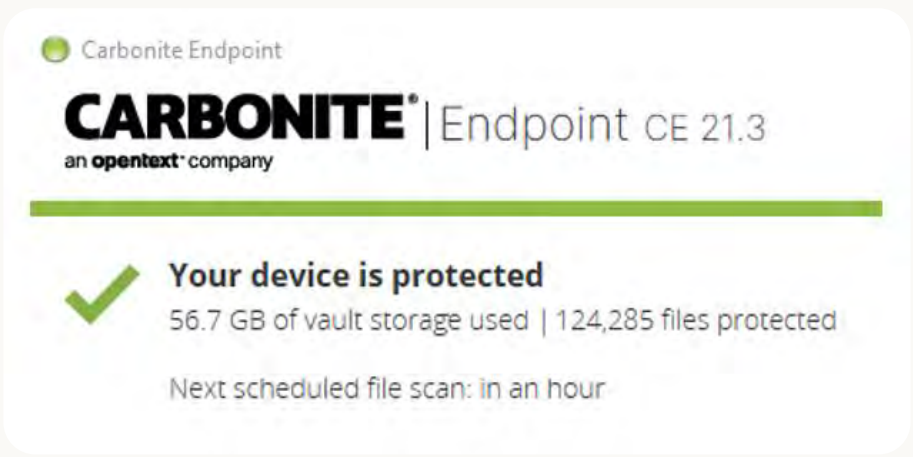
In the Windows Search bar – type in **"Carbonite Endpoint."**



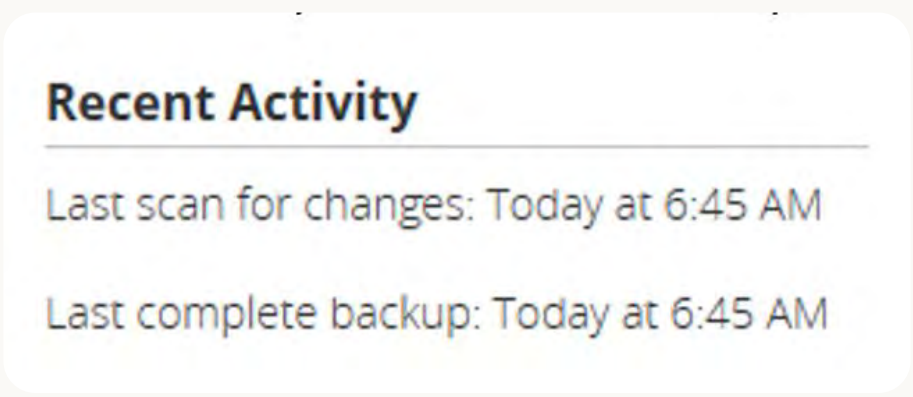
Click on the **Carbonite Endpoint App.**



Look for the green check mark showing your device is connected.



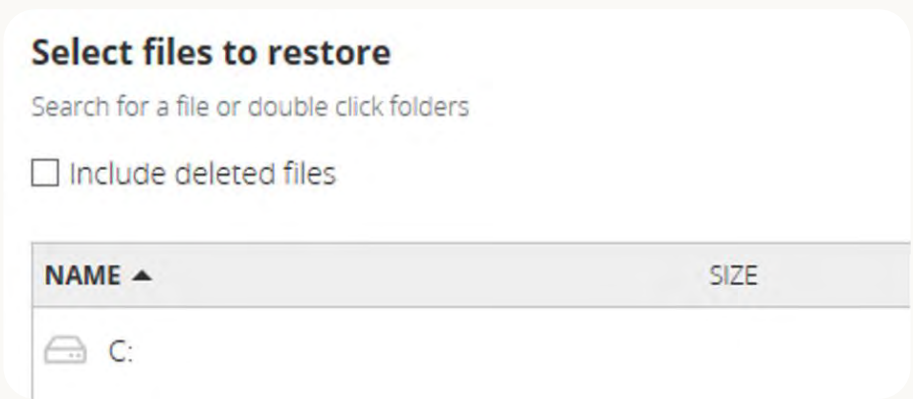
Review Activity to confirm recent activity.



If you believe Carbonite is not working, please open a helpdesk incident https://syf.service-now.com/techcompass

How to Restore Files from Carbonite App:

Restore (upper right corner). Select the **Volume,** then **Macintosh HD**, and browse to the folder/files you wish to restore, then click **Next**.



To restore files to original location – select



Click **Restore** to continue – **Cancel** if needed.



synchrony

Load PST file (if applicable)

1. Open **Outlook**
2. Click on **File** in upper left menu.



3. Click on **Open & Export**.



4. Click on **Open Outlook Data File**.



5. Browse to file location then select target file to open.
6. Click on **OK**.

Data file (PST) will open and be available by clicking on that file in the left view pane.

* Synchrony does not recommend the use of PST files. Each SYF O365 account comes standard with a large capacity. If you wish to stop using PST files, you can upload your files to O365 and discontinue using PST files by disconnecting them from your Outlook profile.

Go to 10. SEE Self-Recov...

Back to table of content

synchrony

SEE Self-Recovery Setup

Instructions on how to setup Self-Recovery Passwords for Symantec Endpoint Encryption (SEE) on a PC:

1. Click on the start windows logo on the Start Bar. Typically, this is located on the left side of the start button if the start bar is at the bottom of your screen.
2. Browse in the start menu down to **Symantec Endpoint Encryption**, then choose **SEE Management Agent**.

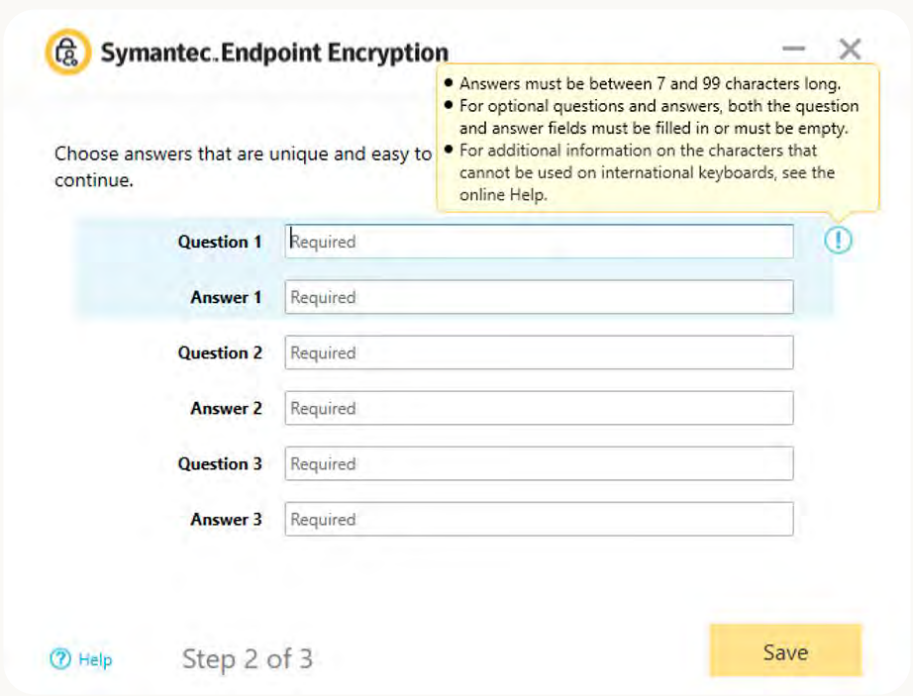




3. Enter your ADSYF Username and Password to login to this utility. Then click **Continue**.



4. Using instructions, please fill in 3 questions and answers then click **Save**.



5. Click **Finish** to complete.

Go to 11. Equipment Retu...

Back to table of content

synchrony

Equipment Return Instructions

Shipping Instructions:

Synchrony box for Suspension box – This box has built-in foam or suspends asset in the middle of the box.

- Using the same packing material/wrapping provided with the delivery of your new device:
  - Place laptop/Chromebook in the Synchrony box with foam or in-between the plastic sleeves in the suspension box.
  - Use the extra room for any peripherals, cords, cables, power supplies, etc.
  - Insert Synchrony Box into provided sleeve.

Standard box with bubble wrap

- Using the same packing material/wrapping provided with the delivery of your new device:
  - Boxes and/or bubble wrap have been provided for the return of electronic assets to Synchrony.
  - Please use the bubble wrap provided to wrap equipment being returned.
  - Laptops, Chromebooks, MACs, Avaya phones, should have 2-3” of bubble wrap on all sides.
  - For the surplus in open space, please use any extra bubble wrap and clean wadded up newspaper to fill these open areas.

All – Continued

- Tape box shut:
  - Please secure the box openings with 2” or 3” wide packing tape (most staffed FedEx locations can tape the box shut for you if you do not have tape).
  - Return label:
    - Secure the provided return FedEx shipping label to the top of the box or on to Synchrony box sleeve.
    - Ensure original TO: label is covered or marked out.
  - Optional: Provide label to the shipping agent, who can assist you with applying it.

* Please do not ship any personal belongings to Synchrony

Back to equipment selection

Back to table of content