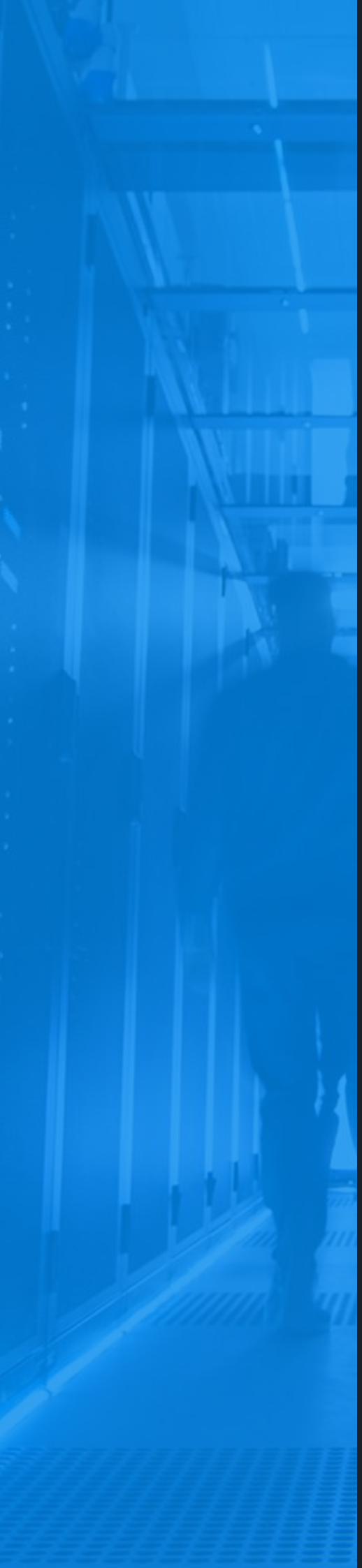
Sysnet Protect user guide

Installing and using Sysnet Protect and Endpoint Protect



Security software

As part of your subscription to your service, you have access to various cybersecurity tools to bolster your protection against cybercriminals.

This user guide will walk you through the installation steps and actions you can take to **help you stay protected.**

What's included in this guide?

Click the links below for more

Windows user guide

MAC user guide

Windows user guide

Click here for **MAC**

Windows installation guide

Downloading and installing Sysnet Protect

Step 1: Download the Sysnet Protect application

First you must download the Sysnet Protect App.

You can download the app via a link within your portal and follow the on screen instructions.

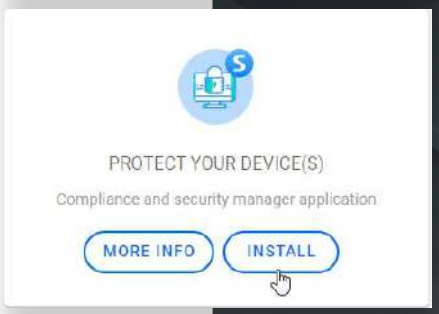
Click '**Download Sysnet Protect for Windows**'

Step 2: Save/Run the file

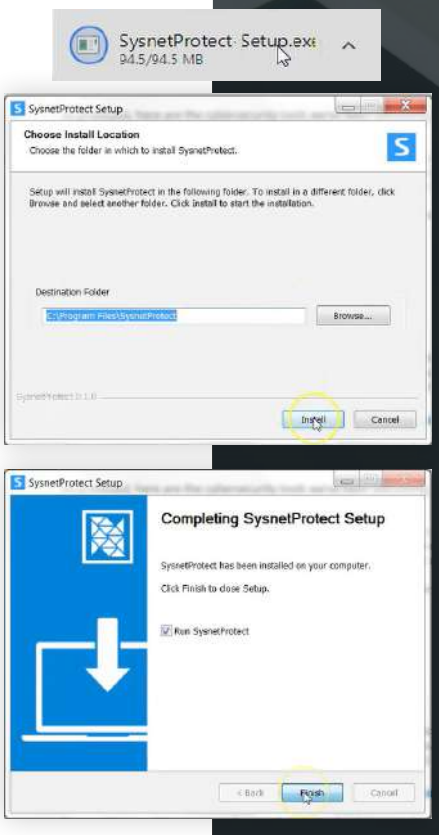
Click '**Save File**' or '**Run**' depending on your version of Windows.

If the file does not run, you may need to locate it in your '**Downloads**' folder and run it from there.

Step 1 Download from your Portal



Step 2 Save / Run the file

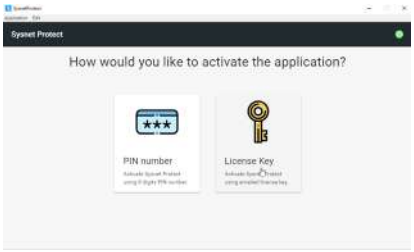


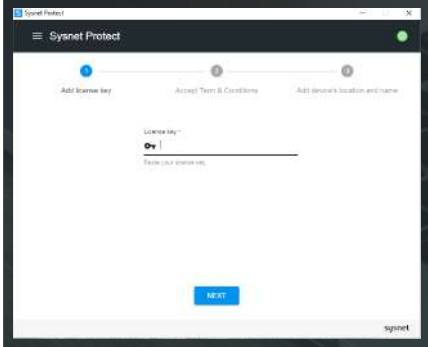
Windows installation guide

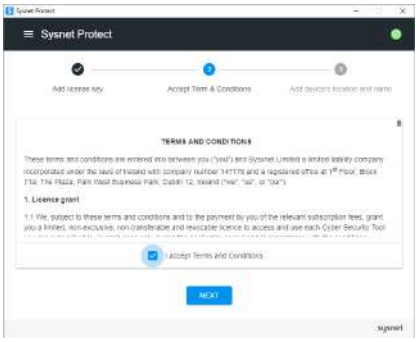
Downloading and installing Sysnet Protect

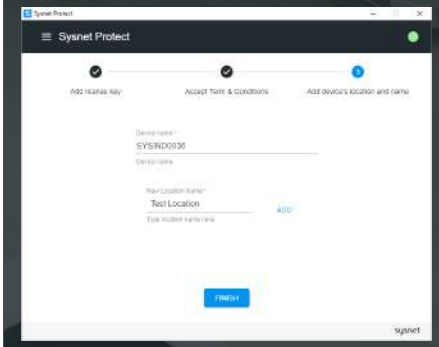
Step 3: Complete installation steps

- Select ‘Licence Key’ as your method of authentication
- Copy the licence key from your Portal and paste into the space provided
- Accept the terms and conditions
- Input the device’s name and location within your business







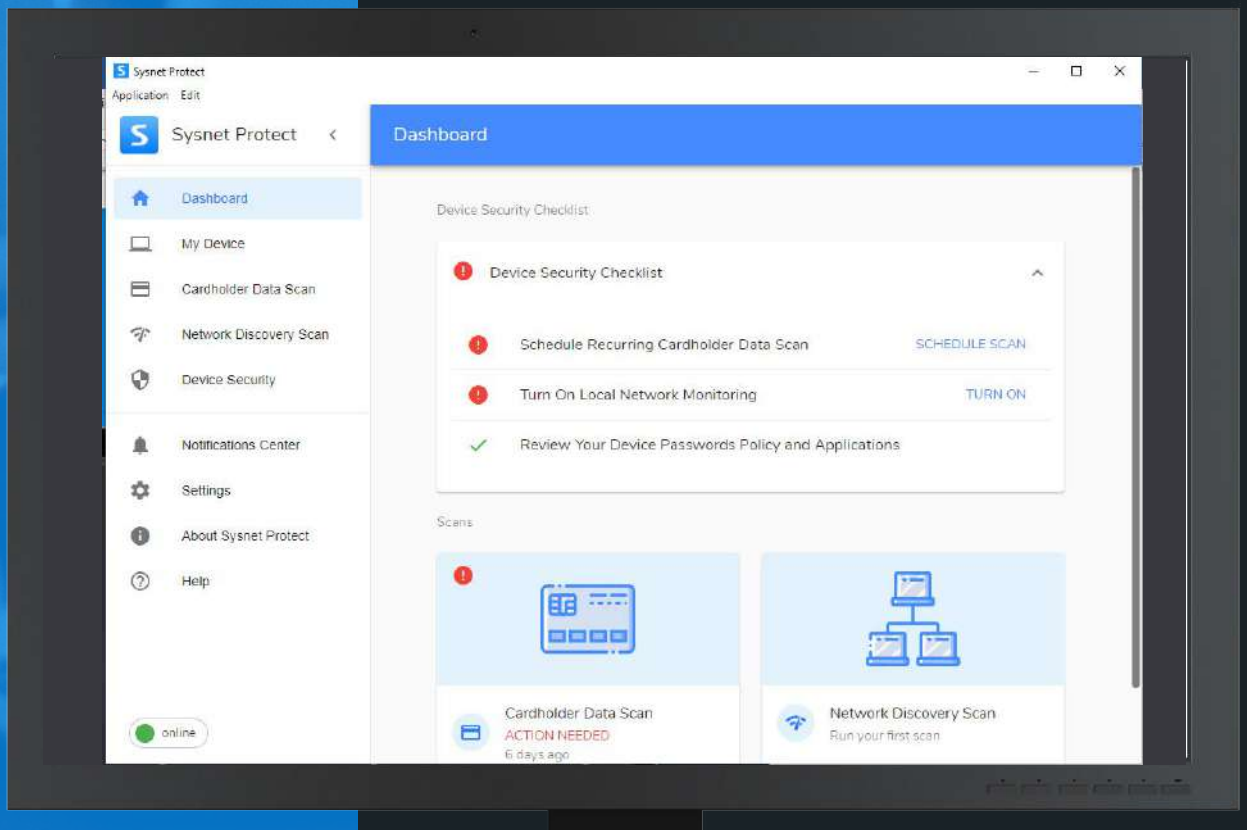


Go to MAC guide

Overview - Sysnet Protect

Sysnet Protect allows us to assist you with managing your compliance.

You can also conduct scanning and perform an array of different tasks (see next page).



Sysnet Protect

The main interface

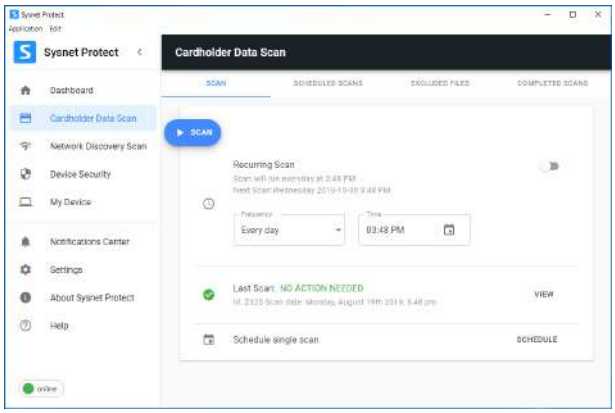
From the main interface you can navigate through your software to perform an array of security tasks.

NOTE: the features available on Sysnet Protect depend on your subscription type. All features may not be available on your version of the software.

Cardholder data scan

Allows you to scan for unencrypted cardholder data that may be stored on your device(s).

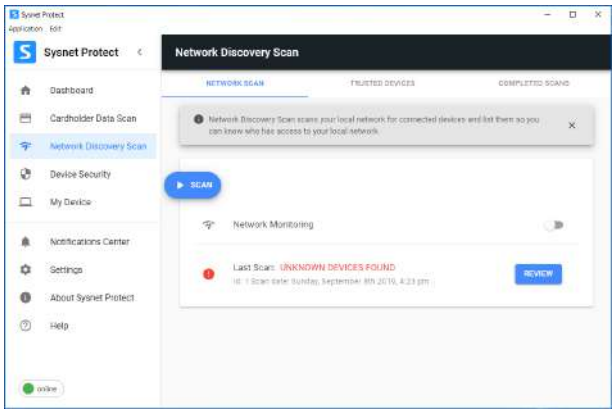
Click here for more on this scan.



Network discovery scan

This scan allows you to view all devices visible and connected to your network. You can see devices that may be accessing your network that shouldn't be.

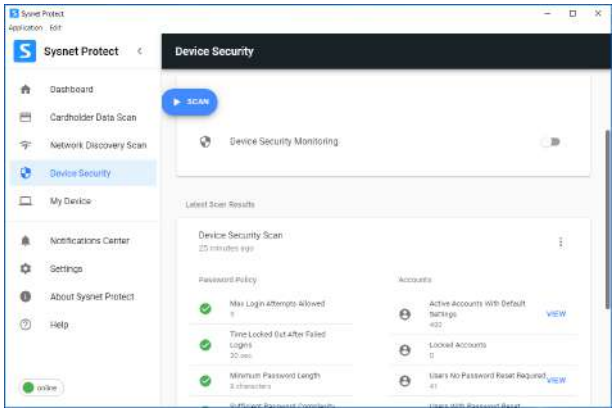
Click here for more on this scan.



Device security

This scan allows you to view all devices visible and connected to your network. You can see devices that may be accessing your network that shouldn't be.

Click here for more on this scan.



I want to... scan for unencrypted cardholder data

Discover and remove unencrypted credit card numbers

About the cardholder data scan

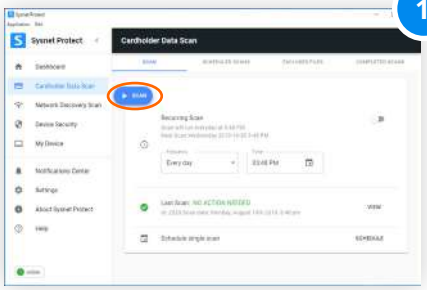
Cardholder data refers to unencrypted credit card long numbers (e.g. the 16 digit card number) belonging to you, your customers or a third party. As part of the PCI DSS, you are required to refrain from storing unencrypted cardholder data on your systems to help protect against the risk of fraud. This scan will scan your systems for unencrypted cardholder data.

About scan results

If the scan finds files/folders that potentially contain payment card numbers, they will be displayed in a list for you to review.

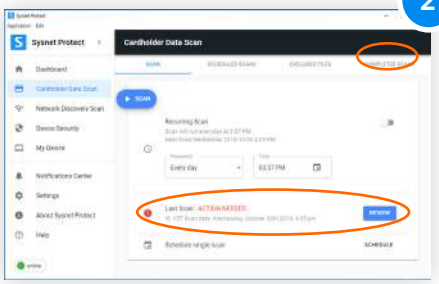
The best way to protect your customer's cardholder data and your business is not to store this data. If such data has been found and you don't need to store it, please securely delete it. If it is necessary to retain this data, ask your payment solution provider about available technologies you can employ to store this data securely.
If the results display files that, upon investigation, do not actually contain cardholder data, you can exclude this file/folder from the scan. See overleaf for more details on excluding files.

1



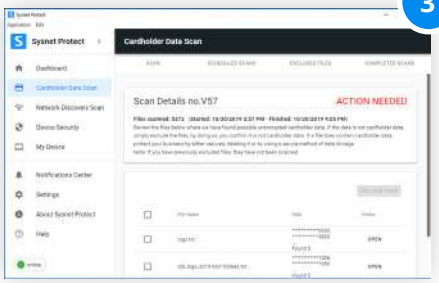
Under the 'Cardholder data scan' tab on the Sysnet Protect app, click '**Scan**.'

2



Once complete, a **'Last Scan'** box will open on the main screen. Click **'Review'** to see the results. Alternatively, navigate to the **'Completed Scans'** tab in the top right to see all previous scans.

3



If suspected card data is found you will be able to review the details of the files/folders here.

I want to... scan **regularly** for unencrypted cardholder data

Run regular checks that cardholder data is not being stored on your system

Set up a scan to run automatically on a regular basis

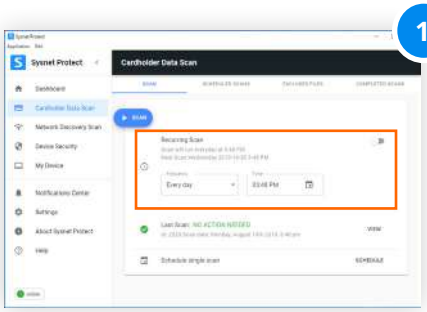
Sometimes running a scan on one isolated occasion is not enough. You can set up the cardholder data scan to run on a regular basis on your system.

This is an effective way to protect against the threat of cardholder data being stored without your knowledge or consent.

You can run the scan on a daily, weekly or monthly basis and specify the time of day the scan should run.

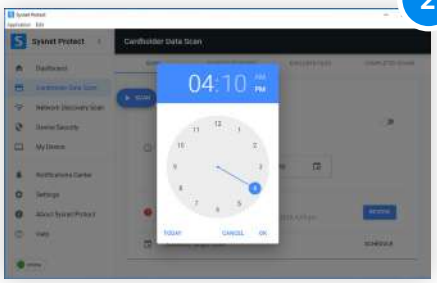
See overleaf for dealing with scan results.

1



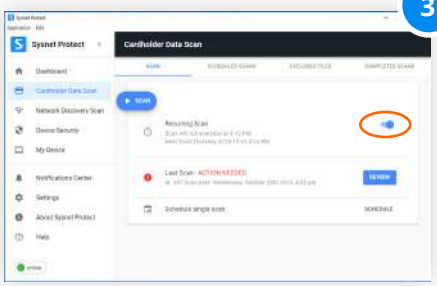
Under the **'Cardholder data scan'** tab on the Sysnet Protect app, navigate to the **'Recurring Scan'** box.

2



Select how often you want the scan to run (Daily, Weekly or Monthly) from the dropdown menu and then the time of the day you wish it to run, click **'OK'**.

3

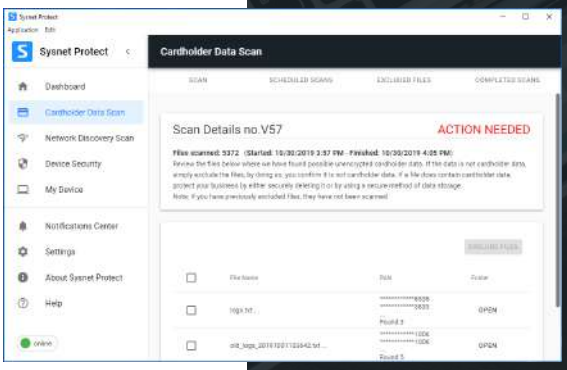


Once you've selected the frequency and time, click the slider to the right to activate the regular scan.

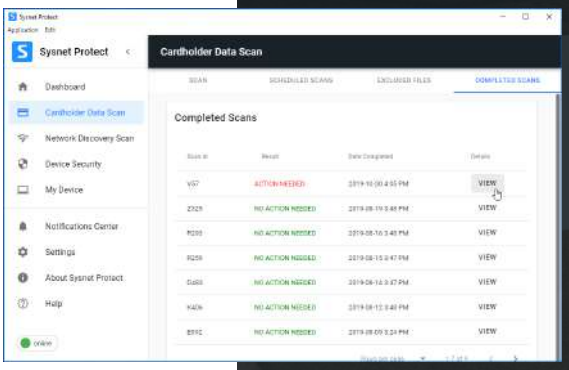
Dealing with the results of your cardholder data scan

Reviewing results and taking action

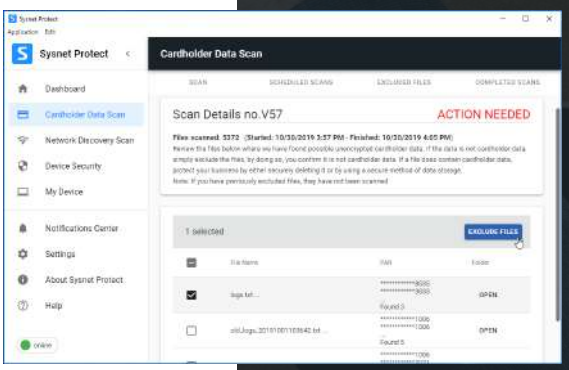
To review the results



- Click '**Review**' from the main cardholder data scan screen to view the results of the scan. Alternatively, select the **'Completed Scans'** tab at the top right. The results will be displayed



- From the list of previously ran scans, select the one you wish to review by clicking **'View.'**
- A list of the files and folders that contain suspected cardholder data will be displayed. Click **'Open'** to view the file/folder
- If you are satisfied the folder does not contain cardholder data, you can exclude it from future scans by selecting the item via the checkbox and then clicking '**Exclude files.**' If it does contain cardholder data, you'll need to securely delete it



- You will then need to rerun the scan. If you have dealt with the files properly, the scan should now pass and will display as **'Last Scan: NO ACTION NEEDED'**
- You can review the files you have excluded by clicking the '**Excluded files**' tab. You will be presented with a list of all files that are not being scanned

I want to... find what devices are accessing my network

Gain visibility on the devices that have access to your network

About the network discovery scan

Scan the network that you are connected to and view a list of all other devices that are visible and using the same network. This will allow you to identify if any unauthorised devices are connected and take action.
For your cybersecurity, it's important that only trusted devices can access your network.

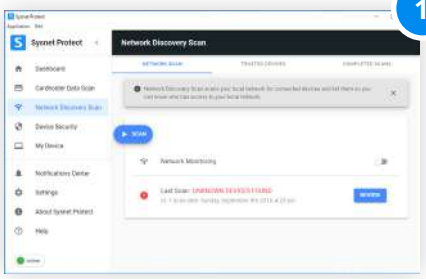
About scan results

If you see a device listed that you do not recognise, you will need to investigate as to how unrecognised devices gained access to your network and should consider changing your access passwords as soon as possible.

The scan does not have the ability to exclude, block or remove these devices, you must do this separately.

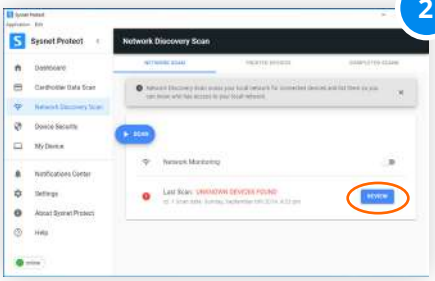
If you recognise a device, you can add it to your trusted device list. To do this, select the checkbox to the left of the device details and click **'Add to trusted devices'.** This will exclude it from future scans to save time next time you run it.

1



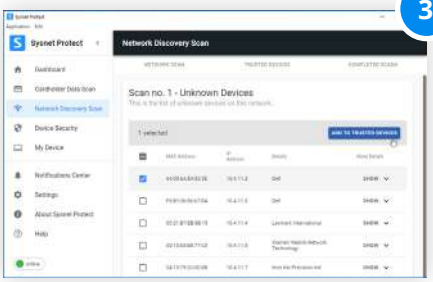
Navigate to the **'Network Discovery Scan'** tab and click **'Scan.'** The scan will now run on your network.

2



When complete, the scan will be listed under **'Completed Network Discovery Scans.'** Click **'Review'** to see the results.

3



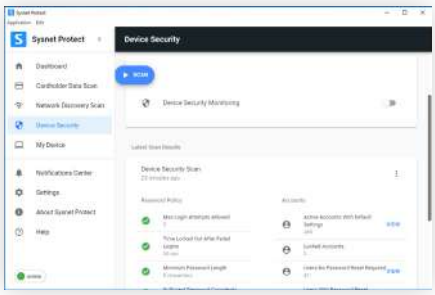
You can add devices to your trusted device list. Select the checkbox next to the device and click **'Add to trusted devices'**

I want to... check my security configuration

Check your device's settings to see if they meet minimum recommended requirements

Device Security

The Device Security Scan examines your device for common defensive measures.
It returns a list showing how well your device is configured in terms of security best practice.
You can then review your results to improve the security of your device.



From the 'Device Security' tab, select 'Scan.' The scan will run and the results will display onscreen.

Understanding the results

Password Policy

Max login attempts allowed - no of times a user is permitted to log in with the wrong password before being locked out. More than 5 is not recommended.

Time locked out after failed logins - mimumum for a pass is 30 seconds.

Minimum password length - password must be a minimum of 8 characters to pass.

Sufficient password complexity - password must contain both numeric and alphabetic characters at a minimum to pass.

Max password age allowed - how often user is prompted to change their password. Every 30 days is recommended.

Unique passwords needed before reuse - amount of times a user has to change a password before one can be reused. Minimum of 6 resets is recommended, ideally no password reuse should be permitted.

Accounts

Active accounts with default settings - checks if your device is using default user accounts (e.g. admin). Using default accounts is not advised.

Locked accounts - lists accounts that are in use on the device that are currently locked out. It is best to remove these accounts if not in use.

Users no password reset required - users who are not required to reset their password on a periodic basis. These are a security risk.

Users with password reset required - lists users required to reset their password.

System

System automatic update - checks automatic updates are turned on (recommended).

Antivirus installed - view antivirus in use.

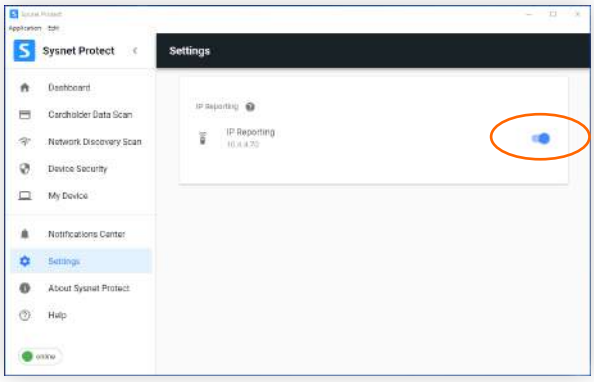
Payment applications installed - view payment apps in use.

I want to... communicate my IP address

IP Reporting facilitates smoother scanning and compliance

How IP reporting works

As part of maintaining your compliance with the Payment Card Industry Data Security Standard (PCI DSS), you may be required to conduct a scan on your network every 90 days.



View via the 'Settings' menu in Sysnet Protect. Click the checkbox to turn on IP Reporting.

These scans check your internet router to make sure that your card terminal is processing over a secure connection, reducing the risk of fraud. In order to run this scan on your behalf your payment provider will need your public IP address. This is a series of numbers and dots that is in effect, your address on the internet.

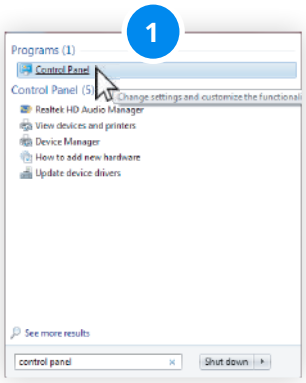
Without this address they will be unable to ensure that they are running the scan on the correct network.

By checking this box, your payment provider will be able to run these scans on your behalf without the need to call you to confirm the IP address every time.

This feature is only effective if this device is permanently located at your primary address and connected to the same internet connection as your card payment terminal. If you are unsure whether this is necessary, speak to your payment provider for more information.

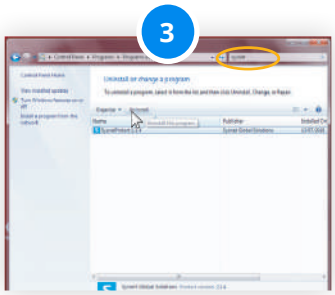
Uninstall Sysnet Protect

Removing Sysnet Protect from your Windows device

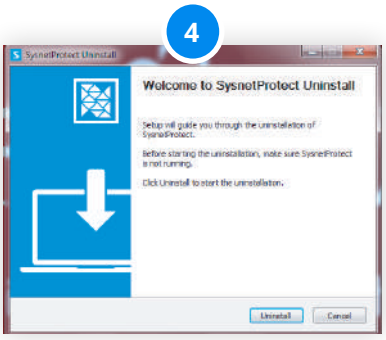


Go to your search bar and search for '**Control Panel**'

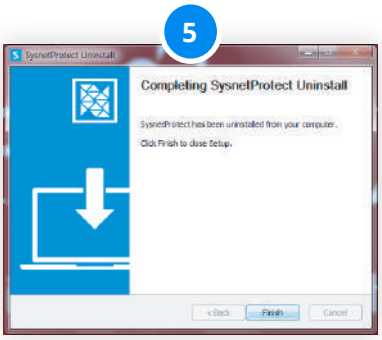
Select '**Uninstall Program**' from the menu



Select '**Sysnet Protect**' from the list and click 'Uninstall'



The uninstall wizard will show. Click '**Uninstall**'



The software will now be removed from your device

Mac user guide

Click here for **Windows**

Mac installation guide

Downloading and installing

First - Download Sysnet Protect

You can download the app via a link within your portal and follow the on screen instructions.

1. Click 'Download Sysnet Protect for Mac.' The file will begin saving onto your device via a box in the bottom left of the screen

Next - Save and run the file

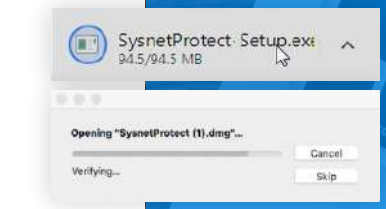
2. When the file has downloaded, you'll need to click the download box
3. You'll then need to drag the new app into your applications as shown

Finally - Complete the installation

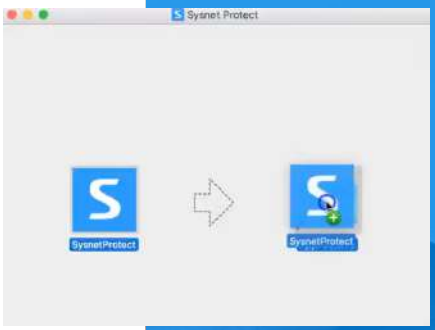
4. The application will then install. From here you will need to paste the licence key into the application from your portal when prompted
5. Complete the installation by accepting the terms and conditions and naming your device

Step 1 Download from your Portal

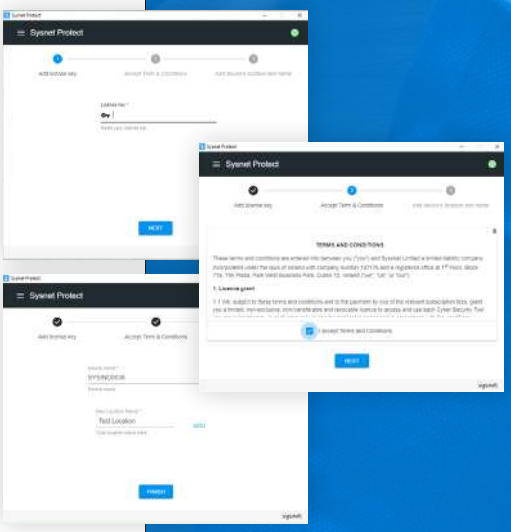
Step 2 Save / Run the file



Step 3 Drag into your applications



Step 4 Complete installation steps



Go to Windows guide

Overview - Sysnet Protect

From the main interface you can perform an array of security tasks.

Cardholder data scan

Scan for unencrypted cardholder data that may be stored on your device(s).

Click here for more on this scan.

Network discovery scan

View all devices visible and connected to your network. You can see devices that may be accessing your network that shouldn't be.

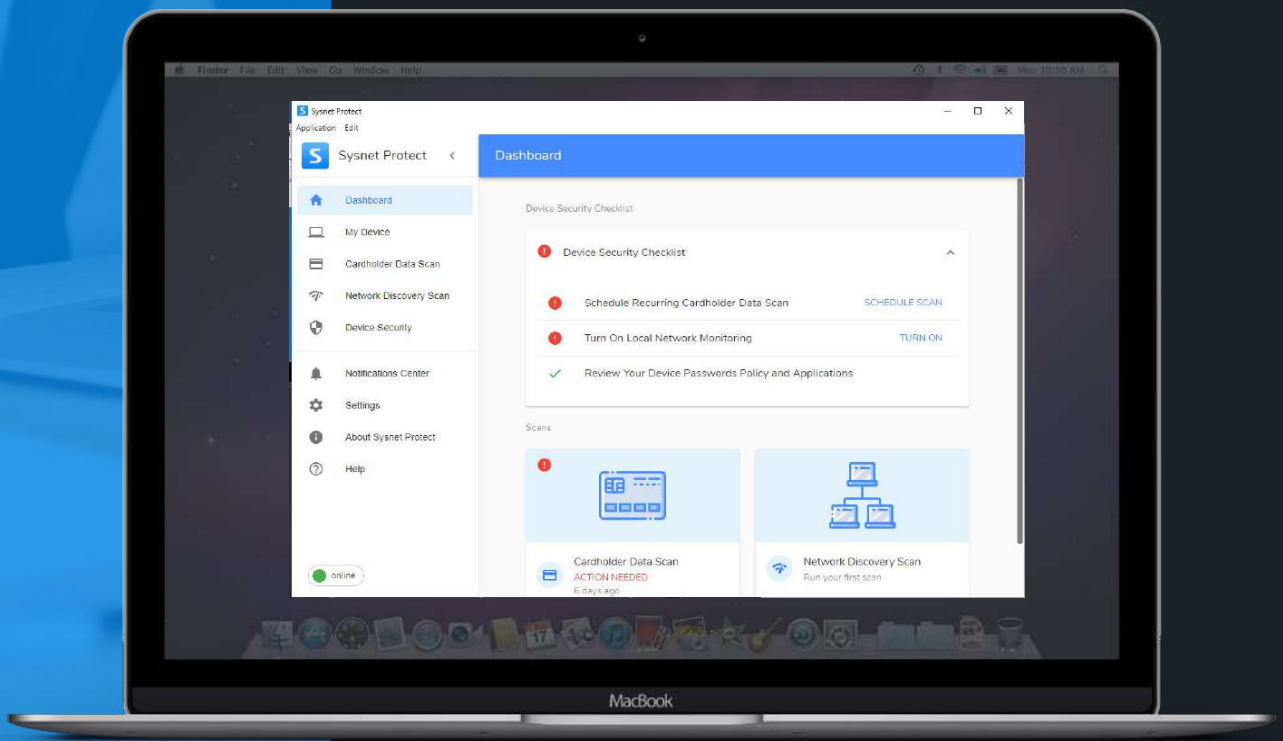
Click here for more on this scan.

Device security

This scan allows you to view all devices visible and connected to your network. You can see devices that may be accessing your network that shouldn't be.

Click here for more on this scan.

Note: the features available on Sysnet Protect are dependent on your subscription type. You may not have access to all elements listed in this guide.



I want to... scan for unencrypted cardholder data

Discover and remove unencrypted credit card numbers

About the cardholder data scan

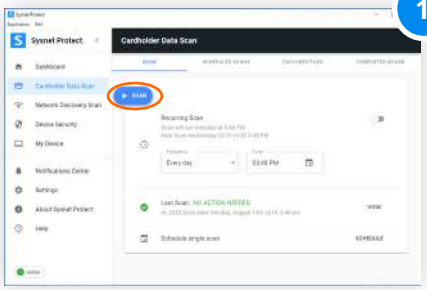
Cardholder data refers to unencrypted credit card long numbers (e.g. the 16 digit card number) belonging to you, your customers or a third party. As part of the PCI DSS, you are required to refrain from storing unencrypted cardholder data on your systems to help protect against the risk of fraud. This scan will scan your systems for unencrypted cardholder data.

About scan results

If the scan finds files/folders that potentially contain payment card numbers, they will be displayed in a list for you to review.

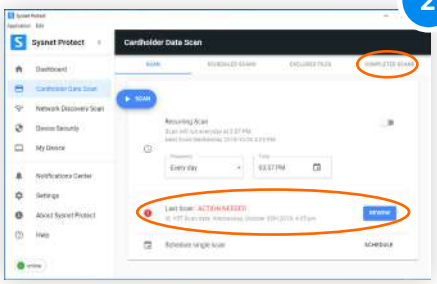
The best way to protect your customer's cardholder data and your business is not to store this data. If such data has been found and you don't need to store it, please securely delete it. If it is necessary to retain this data, ask your payment solution provider about available technologies you can employ to store this data securely.
If the results display files that, upon investigation, do not actually contain cardholder data, you can exclude this file/folder from the scan. See overleaf for more details on excluding files.

1



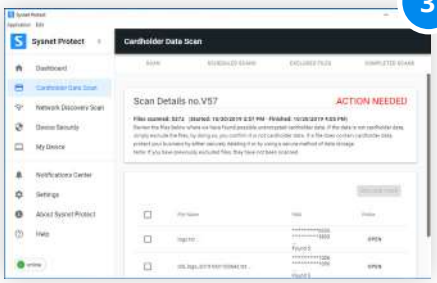
Under the 'Cardholder data scan' tab on the Sysnet Protect app, click '**Scan**.'

2



Once complete, a **'Last Scan'** box will open on the main screen. Click **'Review'** to see the results. Alternatively, navigate to the **'Completed Scans'** tab in the top right to see all previous scans.

3



If suspected card data is found you will be able to review the details of the files/folders here.

I want to... scan **regularly** for unencrypted cardholder data

Run regular checks that cardholder data is not being stored on your system

Set up a scan to run automatically on a regular basis

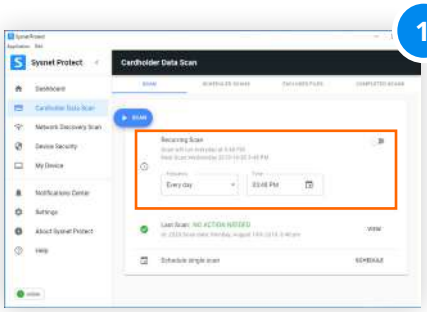
Sometimes running a scan on one isolated occasion is not enough. You can set up the cardholder data scan to run on a regular basis on your system.

This is an effective way to protect against the threat of cardholder data being stored without your knowledge or consent.

You can run the scan on a daily, weekly or monthly basis and specify the time of day the scan should run.

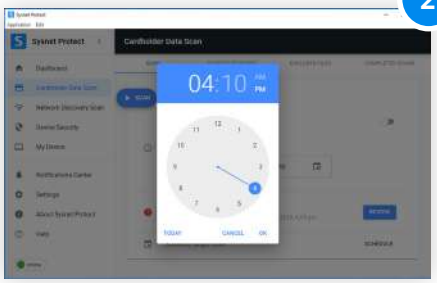
See overleaf for dealing with scan results.

1



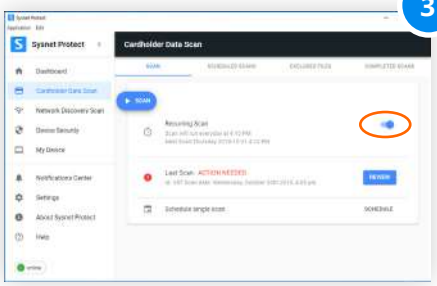
Under the **'Cardholder data scan'** tab on the Sysnet Protect app, navigate to the **'Recurring Scan'** box.

2



Select how often you want the scan to run (Daily, Weekly or Monthly) from the dropdown menu and then the time of the day you wish it to run, click **'OK'**.

3

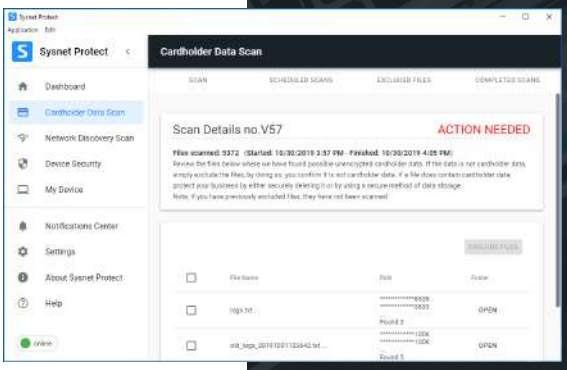


Once you've selected the frequency and time, click the slider to the right to activate the regular scan.

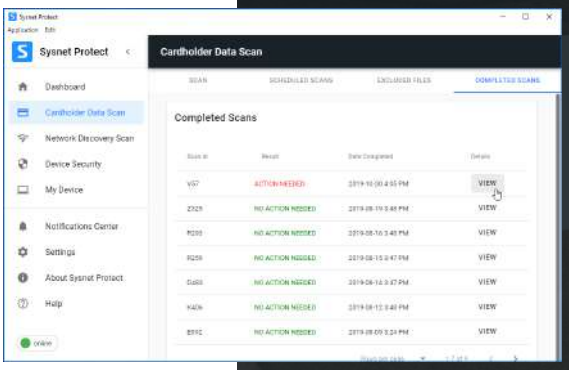
Dealing with the results of your cardholder data scan

Reviewing results and taking action

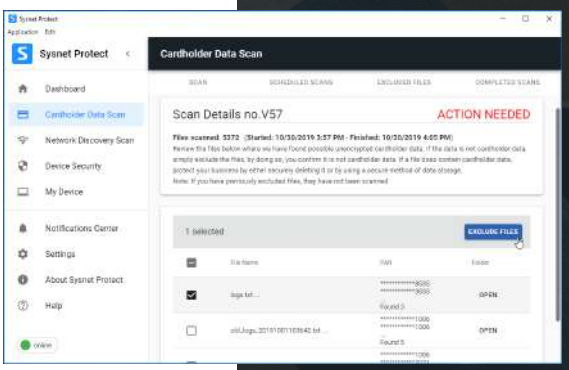
To review the results



- Click '**Review**' from the main cardholder data scan screen to view the results of the scan. Alternatively, select the **'Completed Scans'** tab at the top right. The results will be displayed



- From the list of previously ran scans, select the one you wish to review by clicking **'View.'**
- A list of the files and folders that contain suspected cardholder data will be displayed. Click **'Open'** to view the file/folder
- If you are satisfied the folder does not contain cardholder data, you can exclude it from future scans by selecting the item via the checkbox and then clicking '**Exclude files.**' If it does contain cardholder data, you'll need to securely delete it



- You will then need to rerun the scan. If you have dealt with the files properly, the scan should now pass and will display as **'Last Scan: NO ACTION NEEDED'**
- You can review the files you have excluded by clicking the '**Excluded files**' tab. You will be presented with a list of all files that are not being scanned

I want to... find what devices are accessing my network

Gain visibility on the devices that have access to your network

About the network discovery scan

Scan the network that you are connected to and view a list of all other devices that are visible and using the same network. This will allow you to identify if any unauthorised devices are connected and take action.
For your cybersecurity, it's important that only trusted devices can access your network.

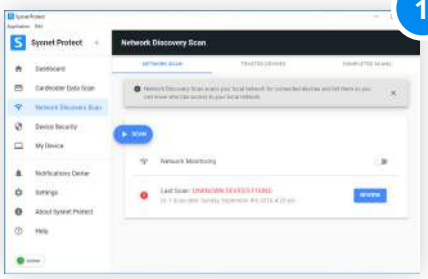
About scan results

If you see a device listed that you do not recognise, you will need to investigate as to how unrecognised devices gained access to your network and should consider changing your access passwords as soon as possible.

The scan does not have the ability to exclude, block or remove these devices, you must do this separately.

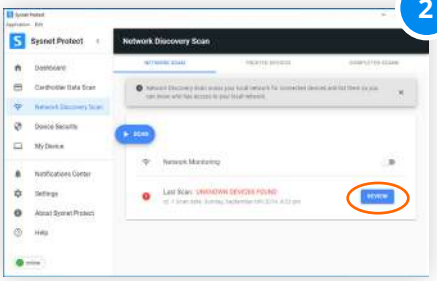
If you recognise a device, you can add it to your trusted device list. To do this, select the checkbox to the left of the device details and click **'Add to trusted devices'.** This will exclude it from future scans to save time next time you run it.

1



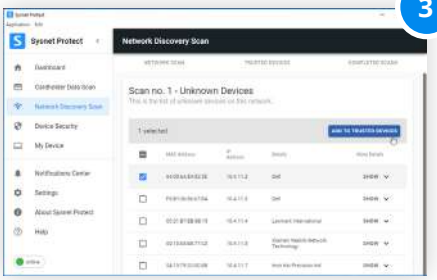
Navigate to the **'Network Discovery Scan'** tab and click **'Scan.'** The scan will now run on your network.

2



When complete, the scan will be listed under **'Completed Network Discovery Scans.'** Click **'Review'** to see the results.

3



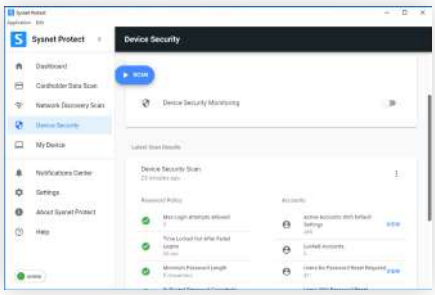
You can add devices to your trusted device list. Select the checkbox next to the device and click **'Add to trusted devices'**

I want to... check my security configuration

Check your device's settings to see if they meet minimum recommended requirements

Device Security

The Device Security Scan examines your device for common defensive measures.
It returns a list showing how well your device is configured in terms of security best practice.
You can then review your results to improve the security of your device.



From the 'Device Security' tab, select 'Scan.' The scan will run and the results will display onscreen.

Understanding the results

Password Policy

Max login attempts allowed - no of times a user is permitted to log in with the wrong password before being locked out. More than 5 is not recommended.

Time locked out after failed logins - mimumum for a pass is 30 seconds.

Minimum password length - password must be a minimum of 8 characters to pass.

Sufficient password complexity - password must contain both numeric and alphabetic characters at a minimum to pass.

Max password age allowed - how often user is prompted to change their password. Every 30 days is recommended.

Unique passwords needed before reuse - amount of times a user has to change a password before one can be reused. Minimum of 6 resets is recommended, ideally no password reuse should be permitted.

Accounts

Active accounts with default settings - checks if your device is using default user accounts (e.g. admin). Using default accounts is not advised.

Locked accounts - lists accounts that are in use on the device that are currently locked out. It is best to remove these accounts if not in use.

Users no password reset required - users who are not required to reset their password on a periodic basis. These are a security risk.

Users with password reset required - lists users required to reset their password.

System

System automatic update - checks automatic updates are turned on (recommended).

Antivirus installed - view antivirus in use.

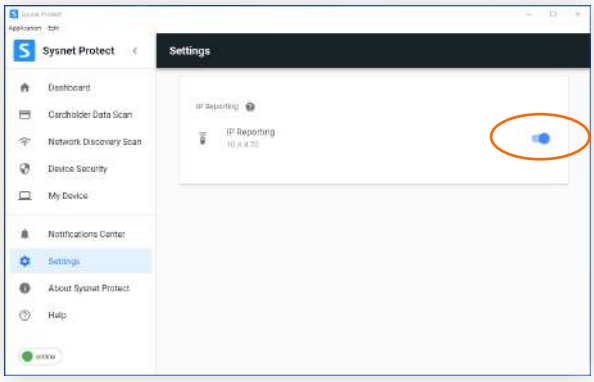
Payment applications installed - view payment apps in use.

I want to... communicate my IP address

IP Reporting facilitates smoother scanning and compliance

How IP reporting works

As part of maintaining your compliance with the Payment Card Industry Data Security Standard (PCI DSS), you may be required to conduct a scan on your network every 90 days.



View via the 'Settings' menu in Sysnet Protect. Click the checkbox to turn on IP Reporting.

These scans check your internet router to make sure that your card terminal is processing over a secure connection, reducing the risk of fraud. In order to run this scan on your behalf your payment provider will need your public IP address. This is a series of numbers and dots that is in effect, your address on the internet.

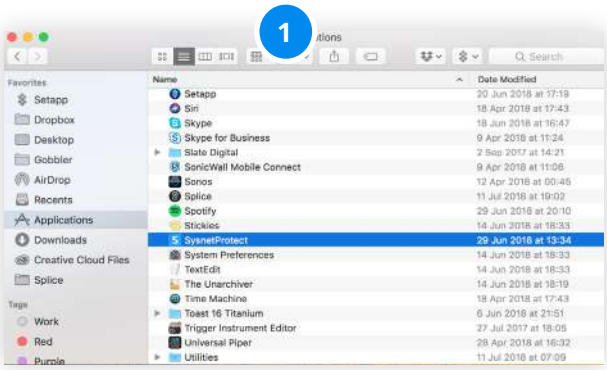
Without this address they will be unable to ensure that they are running the scan on the correct network.

By checking this box, your payment provider will be able to run these scans on your behalf without the need to call you to confirm the IP address every time.

This feature is only effective if this device is permanently located at your primary address and connected to the same internet connection as your card payment terminal. If you are unsure whether this is necessary, speak to your payment provider for more information.

Uninstall Sysnet Protect from MAC

Removing Sysnet Protect from your MAC device



Locate Sysnet Protect

Go to your applications menu, and locate ‘Sysnet Protect’ from the list.

Drag to trash

Drag the application to your trash in the bottom right of the screen.