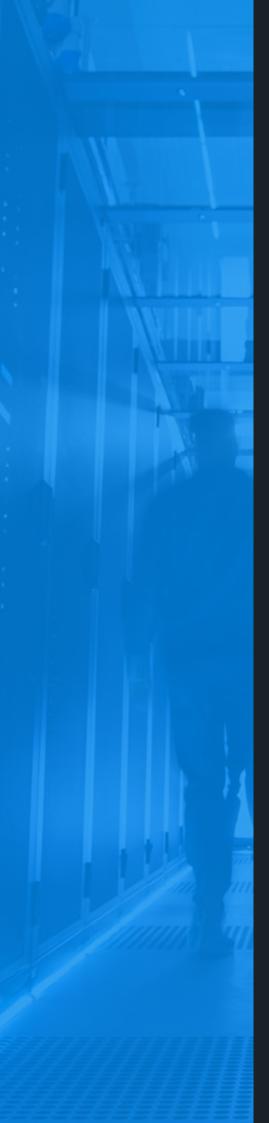


Sysnet Protect user guide

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

Installation guide Overview

I want to...

Scan for cardholder data Regularly scan for cardholder data Deal with cardholder data Find what's accessing my network Check my security configuration Communicate my IP address Uninstall Sysnet Protect

MAC user guide

Installation guide Overview I want to... Scan for cardholder data Regularly scan for cardholder data Deal with cardholder data Find what's accessing my network Check my security configuration Communicate my IP address Uninstall Sysnet Protect S

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.



Go to MAC guide

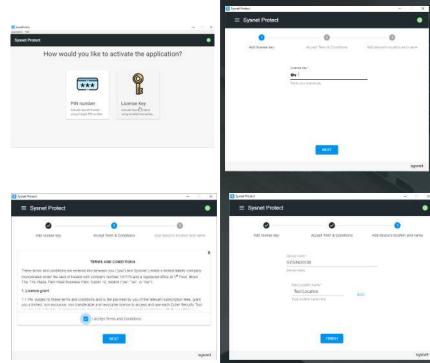
Windows installation guide



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



Step 3 Complete installation

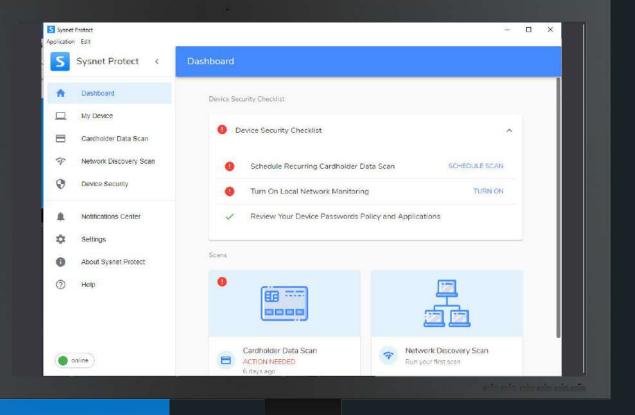
Go to MAC guide



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

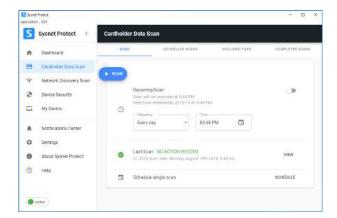
This scan allows you to view all devices visible and connected to your network. You can see devices that may be accessing your network that shouldn't be.

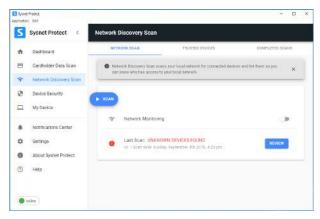
Click here for more on this scan.

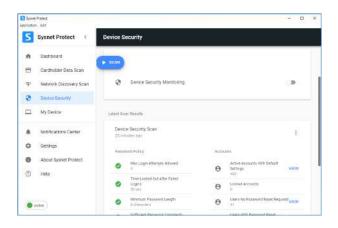
Device security

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

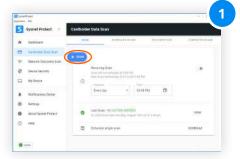
Cardholder data refers to unencrypted credit card long numbers (e.g. the 16 digit card number) belonging to you, your customers or a third party. As part of the PCI DSS, you are required to refrain from storing unencrypted cardholder data on your systems to help protect against the risk of fraud. This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

About scan results

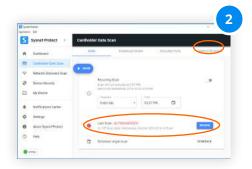
If the scan finds files/folders that potentially contain payment card numbers, they will be displayed in a list for you to review.

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.



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



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.

Sysnet Protect	Cardholder D	ete Scen			
Dashboard	. 66pm	And Allowed Dy Advisory	explanate resta	DOMESTIC CASE	
B Contrast Cara Low					
Network Discovery Scari	Scan Details no.V57 ACTION NEEDED				
Demo Security	 His special 1272 (Harrid Techner's EV NV Available scenary Actives) Special to Harrison scenario from any first accide activity part of tables and if the data is not conference on 				
		the Press, by desting and proceeding of an April 5			
MyDese	probard pays byte	channes for pathone processing, indealining of our log with a synthesizable analysis of these theory three south the	ong is service method of Arts (\$1)		
Notifications Carter	probard pays byte	many by faller participal Adding it in by its	ong is service method of Arts (\$1)		
	probard pays byte	many by faller participal Adding it in by its	ong is service method of Arts (\$1)		
Netifications Center	probard pays byte	many by faller participal Adding it in by its	ong is service method of Arts (\$1)		
Notifications Cartai Settinge	protect loss has	name by Alber sample, Adatoget as by an generality with all the Bary bary new reds	eng san ya nahad at tera ini ala inanad		
 Realizations Cartes Settings 	protect loss has	And the differ and only defining the by an provide state of the difference of the the transmission of the difference of the Angle state.	eng taking nahad at tips line an ing tak		

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.

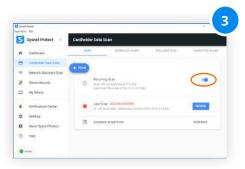
See overleaf for dealing with scan results.

Synnet P	rotect d Card	holde	Deta Scan	
a Destored		-	- 000 (152.23 10 mil) (161.0023 732	0.00493270040444
S Grinne	hus Xa-	-		
P. Metwork 1	lacowy tran	-	auronteo c	
ð Devins Se	owthy		Recurring Scills. Incoment care overcomental Academics	
Wy Davies		0	And the standard in 2019 (4:30) 40 PM	
horitage	and the second se		Energian + 2248.PM	
a server	in the second			2
	and Protect		LANTRON: NO ACTION INVERT	2010
	set Platect		or 2023 has one torong a good 144 (114.) at you	
D test			Schulain ample inter	10+10A.8

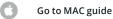
Under the **'Cardholder data** scan' tab on the Sysnet Protect app, navigate to the **'Recurring** Scan' box.



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'**.



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



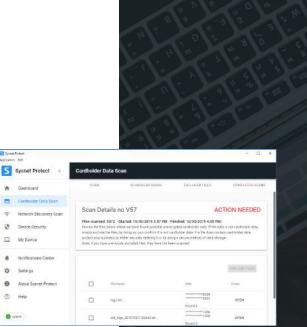
Dealing with the results of your cardholder data scan



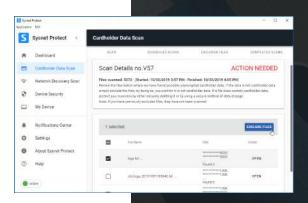
Reviewing results and taking action

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



p matter	Protect:				- 0
s	Sysnet Protect <	Cardholder Dat	a Scan		
ń	Dashboard	30AN	DEHEDULED SEAAN	Listonen (kus	COMPLETED STATE
=	Cambolder Data Scan	Completed :	Scans		
*	Network Discovery Scan Device Security	No. 1	Nerge	Declempent	Delpin
-	My Device	457	ACTION MEEDED	3819-10 (0.2.05.PM	view C
	Notifications Genter	8210	NO ACTION NEEDED	2010-08-10 3 48 PM	VIEW
\$	Settings	8258	NO ACTION NEEDED	2019/08/15 2 47 PM	VIEW
0	About Sysnet Protect	Case	NO ACTION NEEDED	2019-06-14 2 47-PM	VIEW
0	Help	8406	NO ACTION NEEDED	3019-08-12-0-40-914	VIEW
_	citive .	ETFC .	NO ACTION NEEDED	2019-30-09 3:23 PM	siew.



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.

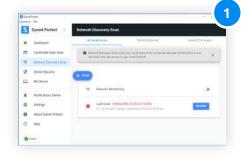
For your cybersecurity, it's important that only trusted devices can access your network.

About scan results

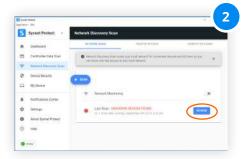
If you see a device listed that you do not recognise, you will need to investigate as to how unrecognised devices gained access to your network and should consider changing your access passwords as soon as possible.

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.



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



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

Sysnet Protect +	Network	Discovery Scan				
Destinant		NHC 1244	1297	TEC BYFRIDE	eperantestate	
Candheriner Dates Scan	Scan n	o. 1 - Unknown	Devices			
National Discours South	Thi.4.75	cast of sciences and	uie or \$96 rath	10A.		
Durks Security	1 years	theat				
My Device		1442 (0.00 miles)	I	and a	. more from	0
Notifications Contar		-	101114	84	3100	¥.
Settep:	0	residential	1641(4		340W	÷.
Most Saleri Porst	n	000 0100 0010		Linna Creanshina	1100	¥2
Hill	0	021333387112	antes.	darat taldiderati. Techning	5468	
104	D	MINTERPORT	MAINT	man and the same lost	and at	

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.

Spotel Potenti promine Effe		D
Sysnet Protect +	Device Security	
n Darittoard	(Tan)	
E Cartholder Data Non		
P Network Discovery Scien	Ø Desce Descript Macazing	
Ø Denie Security		
My Delice	Called State Decide	
R Treshcators Center	Device Security Stars 22 million and	1
Ø Getege	Austral Printy	Accounts
 Atout Sympet Prozect 	O Declays analysis and well	e anna konome deri briadi
(2) Hep	Non-Lodget flat After Factor Non-Lodget flat After Factor	e benefacture
	C Annual Pressent (mgR	e internet to the based and
the second second	A Real Provide August	in the second

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

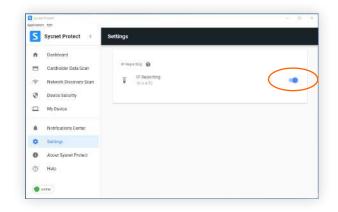


IP Reporting facilitates smoother scanning and compliance

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.

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.



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

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

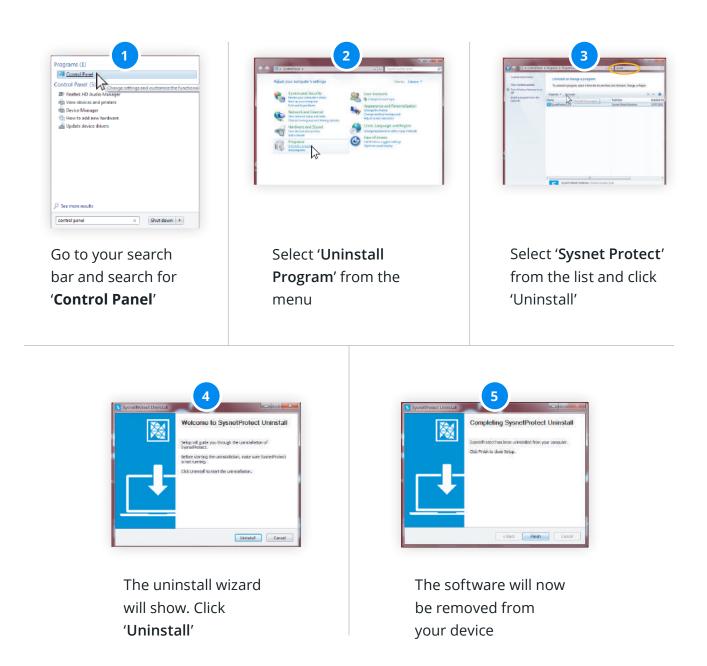
By checking this box, your payment provider will be able to run these scans on your behalf without the need to call you to confirm the IP address every time.

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





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.

 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
- You'll then need to drag the new app into your applications as shown

Finally - Complete the installation

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





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

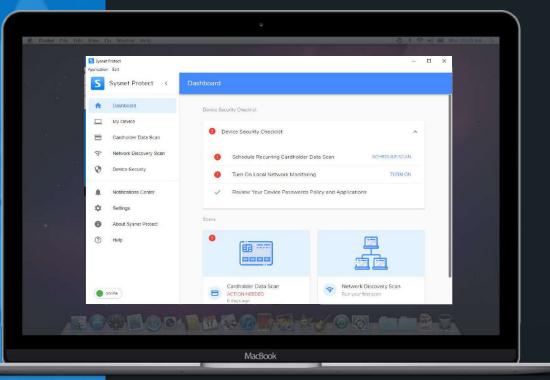
View all devices visible and connected to your network. You can see devices that may be accessing your network that shouldn't be.

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

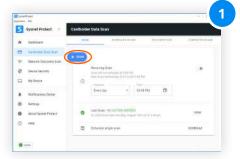
Cardholder data refers to unencrypted credit card long numbers (e.g. the 16 digit card number) belonging to you, your customers or a third party. As part of the PCI DSS, you are required to refrain from storing unencrypted cardholder data on your systems to help protect against the risk of fraud. This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

About scan results

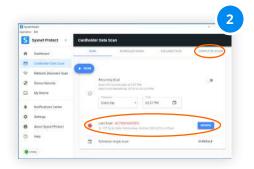
If the scan finds files/folders that potentially contain payment card numbers, they will be displayed in a list for you to review.

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.



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



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.

Sysnet Protect	Cardholder D	ete Scen			
Dashboard	. 66pm	And Allowed Dy Advisory	explanate resta	DOMESTIC CASE	
B Contrast Cara Low					
Network Discovery Scari	Scan Details no.V57 ACTION NEEDED				
Demo Security	 His special 1272 (Harrid Techner's EV NV Available scenary Actives) Special to Harrison scenario from any first accide activity part of tables and if the data is not conference on 				
		the Press, by desting and proceeding of an April 5			
MyDese	probard pays byte	channes for pathow processing in the second se	ong is service method of Arts (\$1)		
Notifications Carter	probard pays byte	many by faller participal Adding it in by its	ong is service method of Arts (\$1)		
	probard pays byte	many by faller participal Adding it in by its	ong is service method of Arts (\$1)		
Netifications Center	probard pays byte	many by faller participal Adding it in by its	ong is service method of Arts (\$1)		
Notifications Cartai Settinge	protect loss has	name by Alber sample, Adatoget as by an generality with all the Bary bary new reds	eng san ya nahad at tera ini ala inanad		
 Realizations Cartes Settings 	protect loss has	And the differ and only defining the by an provide state of the difference of the the transmission of the difference of the Angle state.	eng taking nahad at tips line an ing tak		

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.

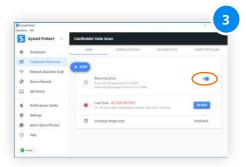
See overleaf for dealing with scan results.

5	Symet Protect	Cardholder Data	Scan		
•	Textorer	(Binney	0.0194235.02000	decourses and	0100012730.00000
3	Cardiona Itala Nati	-			
8	Network Decovery Scan	B 1040			
8	Device Security	in an a	ng Scan Liun Aniyolad at Acad Pitt		
1	My Device	0	er verdenneller 2000-in 2014-il Pr		
ł	Notifications Dentar		day • 214		
	Suffrage	1.000			
	About System Protect		IN NO FETON HUTFU		- 1000
		* 200	Searcher Inchis sugar 1811	111.141.04	
2	1403	2 3tes	in angle is an		60×804.8

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



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'**.



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



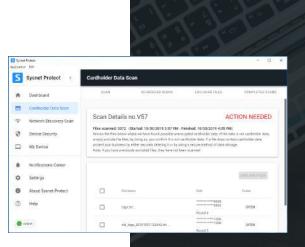
Dealing with the results of your cardholder data scan



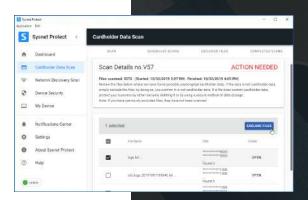
Reviewing results and taking action

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



System Product.					- 0
S Sysne	t Protect	Cardholder Dat	a Scan		
n Dashb	card	30AN	SCHEDILETI SCANS	LYPLOUGH OLES	ODMPLATED STARS
Caralha	older Data Scan	Completed	Scans		
	rk Discovery Scan				
Device	Security	Dist B	Bergit	heritagent	Delain
💷 My De	vice	467	activities weepers	3319-10 (0.4.55 PM	VIEW
		2228	NO ACTION NEEDED	2119-10-19-245-996	VIEW
Notific	ations Center	M208	NO ACTION NEEDED	2219-08-16 3 43 PM	VIEW
🗘 Settini	24	8258	NO ACTION NEEDED	2019/08/15 2:47 PM	VIEW
O About	Sysnet Protect	6488	NO ACTION NEEDED	2019-08-12.2.37.PM	VIEW
🐑 нар		8406	NU 40TION NEEDED	2019-06-12-0-40-914	VIEW
		BARE .	NO ACTION NEEDED	2010-0003-0094	SIEW



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.

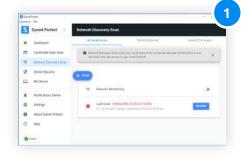
For your cybersecurity, it's important that only trusted devices can access your network.

About scan results

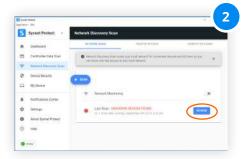
If you see a device listed that you do not recognise, you will need to investigate as to how unrecognised devices gained access to your network and should consider changing your access passwords as soon as possible.

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.



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



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

star honge star blo Sysnet Protect	Network	Discovery Scan			1.5.1
Instant		TAINE STAN	.797	the level of	(paraticita)
Cantheriner Dates	scan	no. 1 - Uniknowi	Devices		
P. Hatarah Darrow	April 14 4	revisit of unintered pine		ww.	
ð Duice Security		whet			ar hi haatsin javassi
T My Device		MAL BADRON		Juny .	- C
Red Frailing Core	- 8		10110	24	3100 V
Ø Settep:	0	. restances	144164	*	sion 🖌
Next Saleet Pro	ad D	10001-01103-00110		Linna Creanshina	1000 w
2 нар	10	02134448.1112	and the	darat taldiderati. Techning	
C atta	D	SATISTICS	MAINT	man and the same and	-

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.

Spond Portant Feature Effe		
Syanet Protect	Device Security	
Desitions		
Circletolder Data Base		
9 Network Discovery Scien	O Destar Destarty Manufacery	
O Desire Security		
Wy Deelca	Labor Star Density	
Noticatore Gener	Device Records Stars	1
¢ Grege	Associat Policy	A111000
Atout System Protect	O Berrage analysi advest	e active Accounts with Ballacil
0 ***	Contraction of the Artist Factor	e lover and a
Q	O Memory Pressent (mg/h	e in the formation from the state
Contraction of the second seco	A Real Provide Street	in the second

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

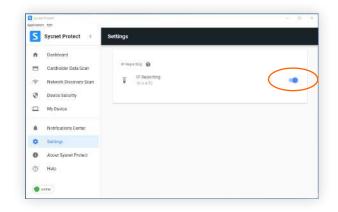


IP Reporting facilitates smoother scanning and compliance

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.

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.



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

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

C 5		😻 🔹 👻 🔍 Search
Favorites	Name	 Date Modified
Setapp	Setapp	20 Jun 2018 at 17:19
	Siri	18 Apr 2018 at 17:43
Dropbox	Skype	18 Jun 2018 at 16:47
Desktop	Skype for Business	9 Apr 2018 at 11:24
Gobbler	🕨 🛅 Slate Digital	2 5ep 2017 at 14:21
	SonicWall Mobile Connect	9 Apr 2018 at 11:06
(iii) AirDrop	🚍 Sarios	12 Apr 2018 at 00:45
E Recents	Splice	11 Jul 2018 at 19:02
A	Spotify	29 Jun 2016 at 2010
Applications	Stickies	14 Jun 2018 at 18:33
O Downloads	5 SysnetProtect	29 Jun 2018 at 13:34
I Creative Cloud Files	System Preferences	14 Jun 2018 at 18:33
100 million (100 m	TextEdit	14 Jun 2018 at 18:33
Splice	The Unarchiver	14 Jun 2018 at 18:19
Tage	Time Machine	18 Apr 2018 at 17:43
O Work	🕨 💼 Toast 16 Titanium	6 Jun 2018 at 21:51
	Trigger Instrument Editor	27 Jul 2017 at 18:05
Red	Universal Piper	28 Apr 2018 at 16:32
Purple	Utilities	11 Jul 2018 at 07:09

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.

