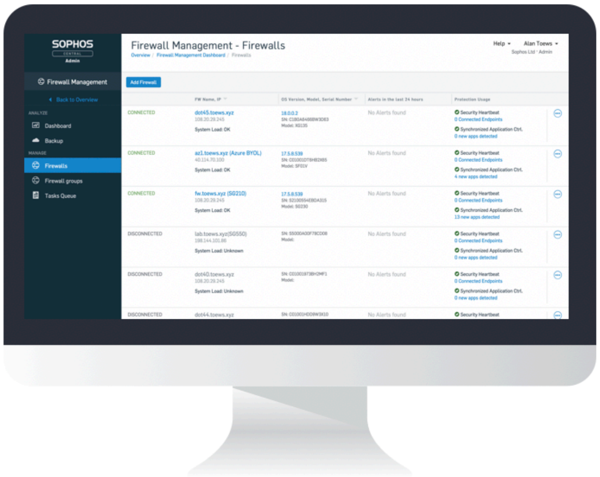
SOPHOS
Security made simple.

XG Firewall

Making the Most of New Sophos Central Management Features



Firewall Management - Firewalls

Overview / Firewall Management Dashboard / Firewalls

	FW Name, IP	OS Version, Model, Serial Number	Alerts in the last 24 hours	Protection Usage
CONNECTED	dot45.toews.xyz 108.20.29.245 System Load: OK	18.0.0.2 SN: C1B0A84668W3D63 Model: XG135	No Alerts found	✓ Security Heartbeat 0 Connected Endpoints ✓ Synchronized Application Ctrl. 0 new apps detected
CONNECTED	az1.toews.xyz (Azure BYOL) 40.114.70.100 System Load: OK	17.5.8.539 SN: C01001DT6HB2X65 Model: SFOIV	No Alerts found	✓ Security Heartbeat 0 Connected Endpoints ✓ Synchronized Application Ctrl. 4 new apps detected
CONNECTED	fw.toews.xyz (SG210) 108.20.29.245 System Load: OK	17.5.8.539 SN: S2100554EBDA315 Model: SG230	No Alerts found	✓ Security Heartbeat 0 Connected Endpoints ✓ Synchronized Application Ctrl. 13 new apps detected
DISCONNECTED	lab.toews.xyz(SG550) 198.144.101.86 System Load: Unknown	SN: S5000A00F78CD08 Model:	No Alerts found	✓ Security Heartbeat 0 Connected Endpoints ✓ Synchronized Application Ctrl. 0 new apps detected
DISCONNECTED	dot40.toews.xyz 108.20.29.245 System Load: Unknown	SN: C010019738H2MF1 Model:	No Alerts found	✓ Security Heartbeat 0 Connected Endpoints ✓ Synchronized Application Ctrl. 0 new apps detected
DISCONNECTED	dot44.toews.xyz	SN: C01001HDD9W3X10	No Alerts found	✓ Security Heartbeat

New Sophos Central Management Features Mid-2019

Since XG Firewall joined Sophos Central earlier this year, a few new helpful features have been added that make day-to-day management of XG Firewall easier than ever:

- Management and storage of scheduled backups
- Firmware update management
- Zero-touch deployment of new XG Firewall appliances

This guide provides an overview and how you can make the most of these new Sophos Central features.

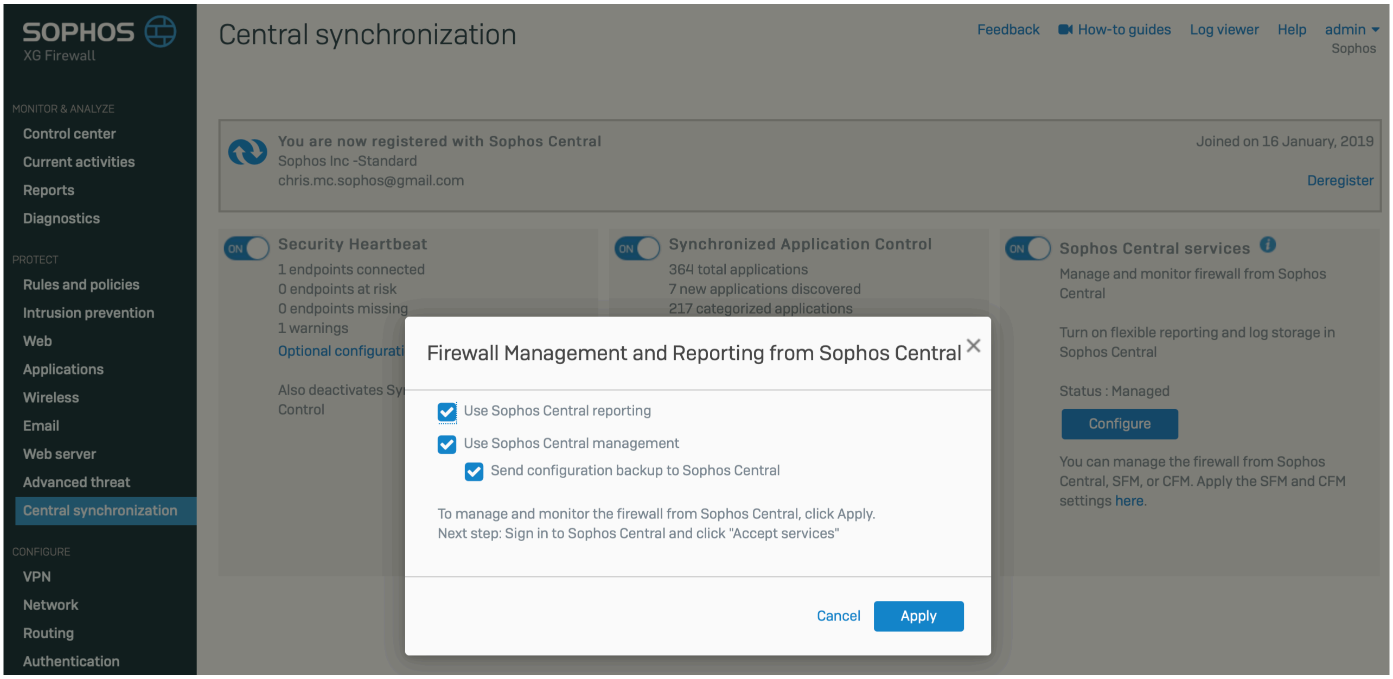
Backup Management

Sophos Central now includes a helpful new feature to centrally schedule and manage all your firewall configuration backups. XG Firewall v17.5 MR7 or later is required.

Here's how to take advantage of this great new feature:

(1) Enabling Sophos Central Backup Management

You can activate this feature in XG Firewall from the "Central Synchronization" menu. Under Sophos Central Services, click the "Configure" button, and then check the box to "Use Sophos Central Management", and "Send configuration backups to Sophos Central" as shown below:



Central synchronization

You are now registered with Sophos Central
Sophos Inc -Standard
chris.mc.sophos@gmail.com
Joined on 16 January, 2019

Security Heartbeat
1 endpoints connected
0 endpoints at risk
0 endpoints missing
1 warnings

Also deactivates Sy
Control

Synchronized Application Control
364 total applications
7 new applications discovered
217 categorized applications

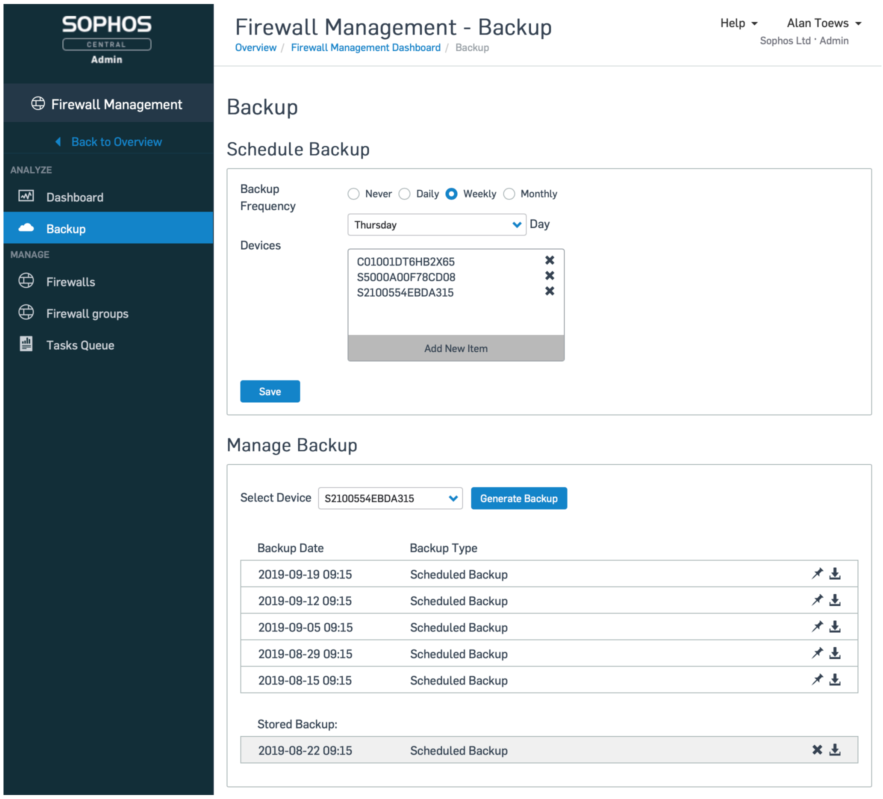
Sophos Central services
Manage and monitor firewall from Sophos Central
Turn on flexible reporting and log storage in Sophos Central
Status : Managed
You can manage the firewall from Sophos Central, SFM, or CFM. Apply the SFM and CFM settings here.

Firewall Management and Reporting from Sophos Central

☑ Use Sophos Central reporting
☑ Use Sophos Central management
☑ Send configuration backup to Sophos Central

To manage and monitor the firewall from Sophos Central, click Apply.
Next step: Sign in to Sophos Central and click "Accept services"

In Sophos Central this new feature is part of your Firewall Management Menu as shown on the screen below.



Firewall Management - Backup

Backup

Schedule Backup

Backup Frequency ○ Never ○ Daily ● Weekly ○ Monthly

Thursday Day

Devices
C01001DT6HB2X65 ✖
S5000A00F78CD08 ✖
S2100554EBDA315 ✖

Manage Backup

Select Device S2100554EBDA315

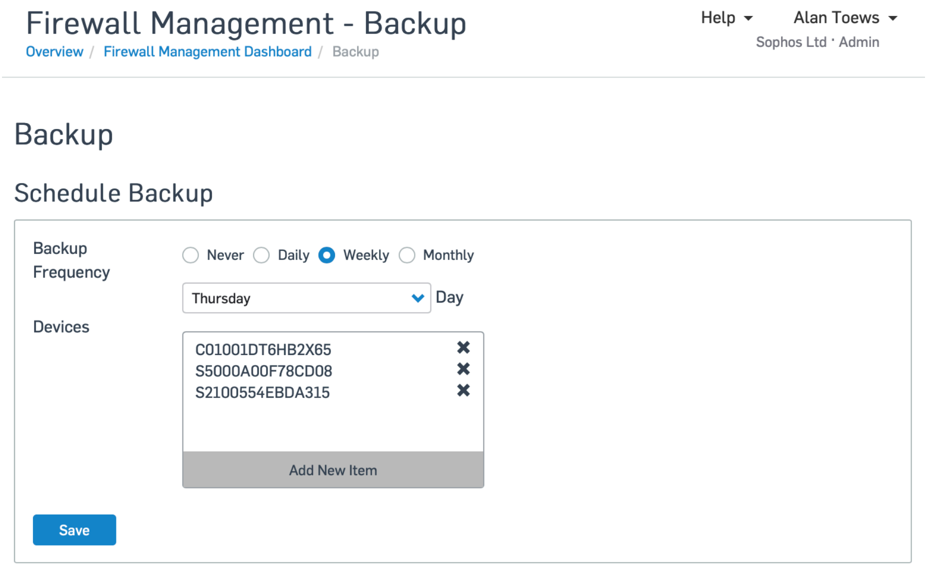
Backup Date	Backup Type
2019-09-19 09:15	Scheduled Backup
2019-09-12 09:15	Scheduled Backup
2019-09-05 09:15	Scheduled Backup
2019-08-29 09:15	Scheduled Backup
2019-08-15 09:15	Scheduled Backup

Stored Backup:

2019-08-22 09:15	Scheduled Backup

(2) Scheduling Backups

Here you can select which devices you wish to back up, when, and how often. The backup files will then be generated automatically according to the schedule and stored securely encrypted in Sophos Central.



Firewall Management - Backup

Backup

Schedule Backup

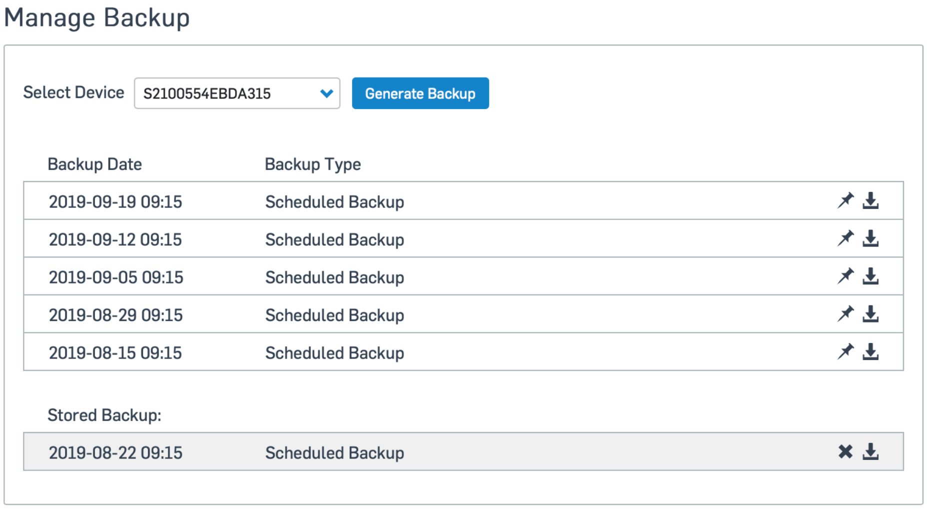
Backup Frequency ○ Never ○ Daily ● Weekly ○ Monthly

Thursday Day

Devices
C01001DT6HB2X65 ✖
S5000A00F78CD08 ✖
S2100554EBDA315 ✖

(3) Managing Backups

You manage your backup files on the same screen where you can download a backup file to restore or pin a backup to store permanently. Sophos Central stores your last five backups, replacing the oldest one with every new scheduled backup. Any backup you pin is stored permanently in a separate location from the backup file rotation.



Manage Backup

Select Device S2100554EBDA315

Backup Date	Backup Type	
2019-09-19 09:15	Scheduled Backup	📌 ⬇
2019-09-12 09:15	Scheduled Backup	📌 ⬇
2019-09-05 09:15	Scheduled Backup	📌 ⬇
2019-08-29 09:15	Scheduled Backup	📌 ⬇
2019-08-15 09:15	Scheduled Backup	📌 ⬇

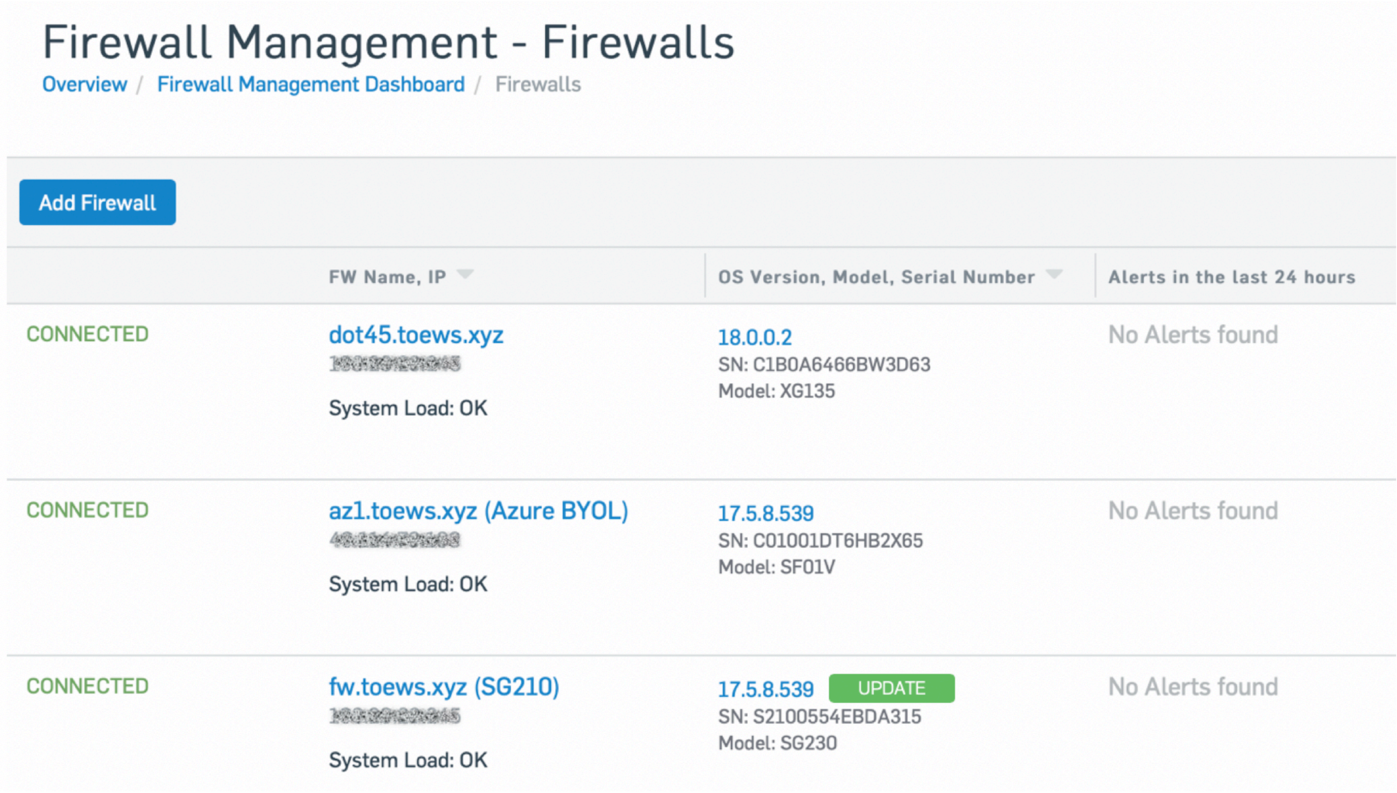
Stored Backup:

2019-08-22 09:15	Scheduled Backup	✖ ⬇

When you download a backup, the configuration file will be re-encrypted using a password of your choice to ensure it remains secure, making it easy to restore onto your XG Firewall appliance. You will be prompted for the password by Sophos Central when you download the backup file, and again by the firewall to decrypt it when you use it to restore the configuration.

Firmware Update Management

When a firmware update is available for any of your firewalls, a green “Update” button will appear next to the current firmware version in the Firewall list. As with backup management, XG Firewall v17.5 MR7 or later is required to take advantage of this new feature.



Firewall Management - Firewalls

Overview / Firewall Management Dashboard / Firewalls

Add Firewall

	FW Name, IP	OS Version, Model, Serial Number	Alerts in the last 24 hours
CONNECTED	dot45.toews.xyz [redacted] System Load: OK	18.0.0.2 SN: C1B0A6466BW3D63 Model: XG135	No Alerts found
CONNECTED	az1.toews.xyz (Azure BYOL) [redacted] System Load: OK	17.5.8.539 SN: C01001DT6HB2X65 Model: SF01V	No Alerts found
CONNECTED	fw.toews.xyz (SG210) [redacted] System Load: OK	17.5.8.539 UPDATE SN: S2100554EBDA315 Model: SG230	No Alerts found

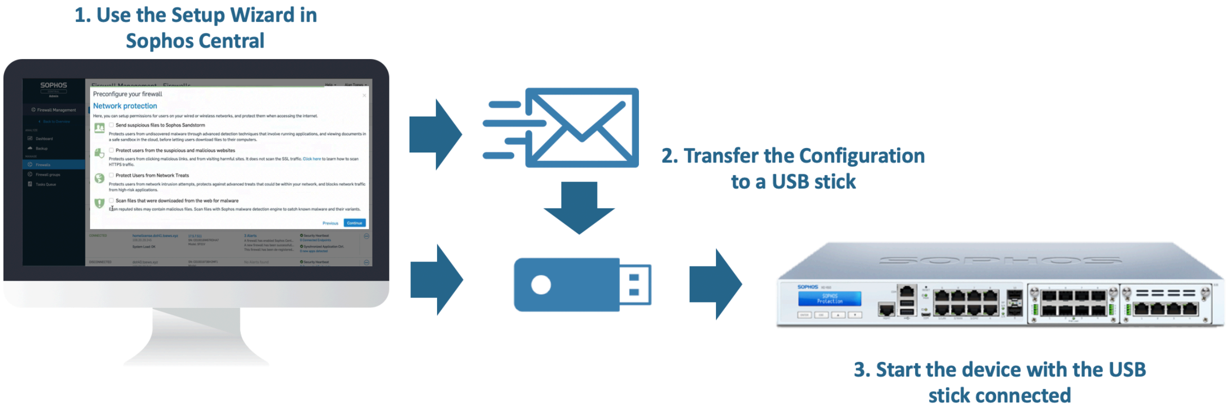
Clicking this button will provide a pop-up window highlighting the details of the new firmware and a confirmation button to proceed with the firmware update.

Upon initiating a firmware update from Sophos Central, the device will download the firmware update file if it has not done so previously, apply the new firmware, and reboot. It may take several minutes for this process to complete and for the firewall to re-appear in the management list in Sophos Central.

Zero-Touch Deployment

Sophos Central now enables you to set up a new XG Firewall appliance in Sophos Central without having to touch the device yourself. It's done in three easy steps:

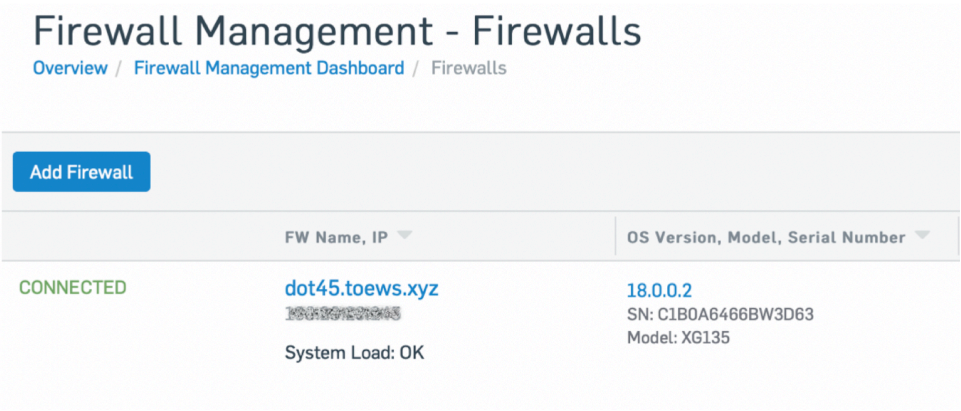
1. Perform the initial setup in Sophos Central
2. Put the configuration file on a USB stick
3. Connect the USB stick to the firewall and start up the device


1. Use the Setup Wizard in Sophos Central
2. Transfer the Configuration to a USB stick
3. Start the device with the USB stick connected

Note: This new feature only works with hardware appliance deployments. Virtual and software firewall deployments are not supported at this time. All firewalls with v17.5 MR3 or later support zero-touch deployment which should include any firewall ordered today.

(1) Initial Configuration in Sophos Central

From your "Firewalls" Management List in Sophos Central, click the "Add Firewall" button at the top of the list and select "Add a New Firewall".

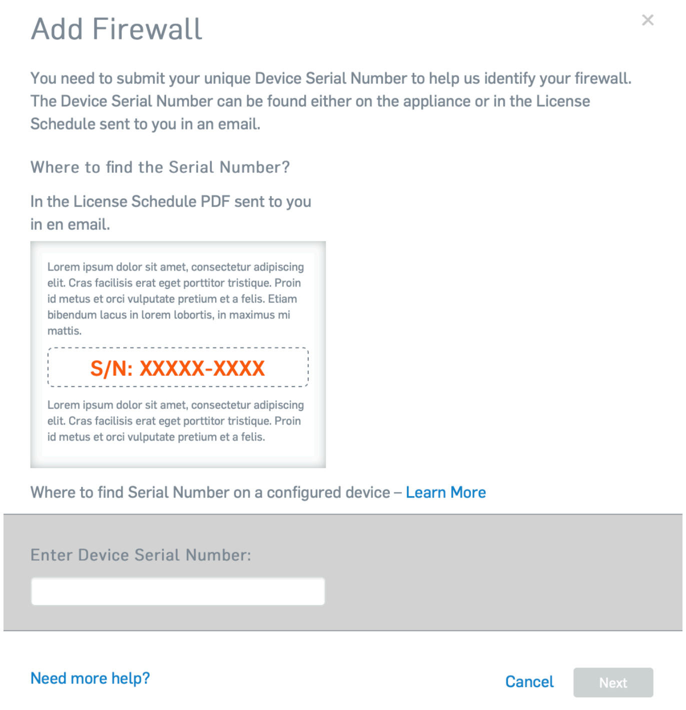


Firewall Management - Firewalls

Overview / Firewall Management Dashboard / Firewalls

	FW Name, IP	OS Version, Model, Serial Number
CONNECTED	dot45.toews.xyz [redacted] System Load: OK	18.0.0.2 SN: C1B0A6466BW3D63 Model: XG135

You will then be prompted for the device serial number which can be found on the License Schedule, the outside of the cardboard box, or on the underside of the appliance itself:



Add Firewall

You need to submit your unique Device Serial Number to help us identify your firewall. The Device Serial Number can be found either on the appliance or in the License Schedule sent to you in an email.

Where to find the Serial Number?

In the License Schedule PDF sent to you in en email.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras facilisis erat eget porttitor tristique. Proin id metus et orci vulputate pretium et a felis. Etiam bibendum lacus in lorem lobortis, in maximus mi mattis.

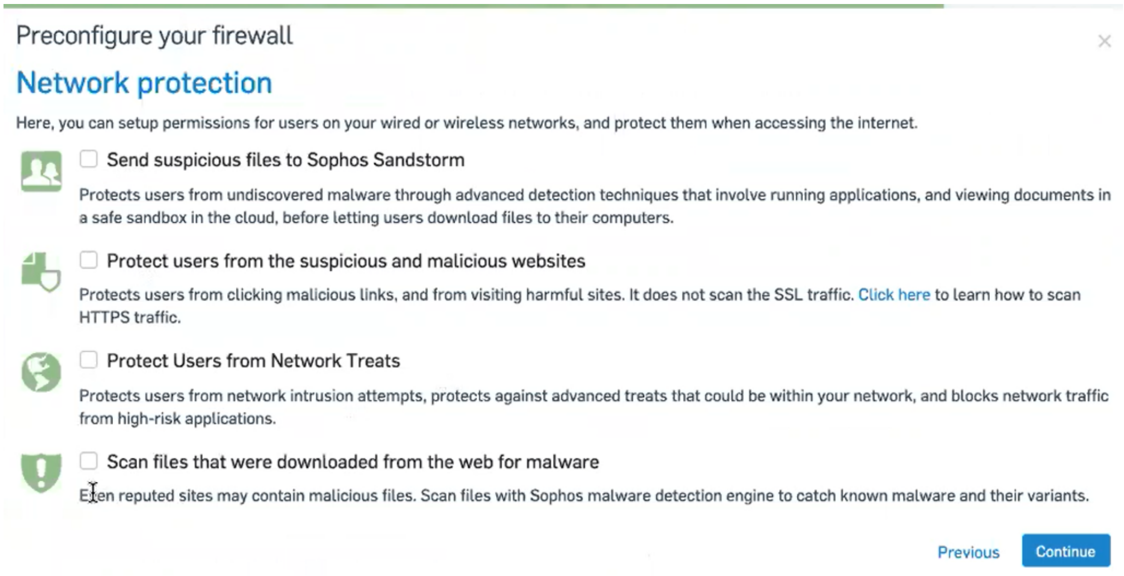
S/N: XXXXX-XXXX

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras facilisis erat eget porttitor tristique. Proin id metus et orci vulputate pretium et a felis.

Where to find Serial Number on a configured device – Learn More

Enter Device Serial Number:

You will then go through the normal Firewall Setup Wizard to configure the firewall…



Preconfigure your firewall

Network protection

Here, you can setup permissions for users on your wired or wireless networks, and protect them when accessing the internet.

□ Send suspicious files to Sophos Sandstorm

Protects users from undiscovered malware through advanced detection techniques that involve running applications, and viewing documents in a safe sandbox in the cloud, before letting users download files to their computers.

□ Protect users from the suspicious and malicious websites

Protects users from clicking malicious links, and from visiting harmful sites. It does not scan the SSL traffic. Click here to learn how to scan HTTPS traffic.

□ Protect Users from Network Treats

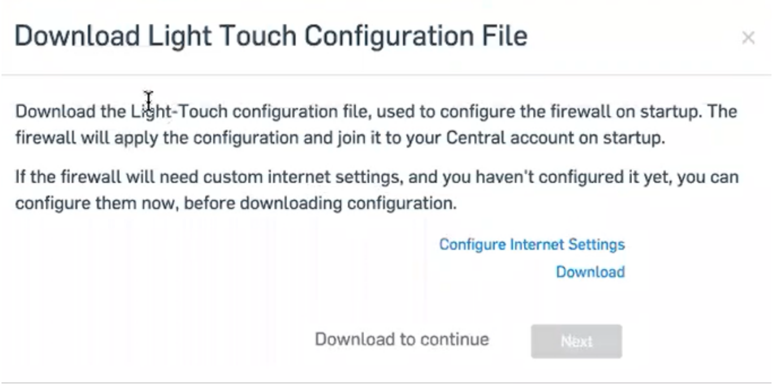
Protects users from network intrusion attempts, protects against advanced treats that could be within your network, and blocks network traffic from high-risk applications.

□ Scan files that were downloaded from the web for malware

Even reputed sites may contain malicious files. Scan files with Sophos malware detection engine to catch known malware and their variants.

(2) Download the Configuration and Transfer It to a USB Stick

Once you finish the initial configuration, you will be prompted to download the configuration file:

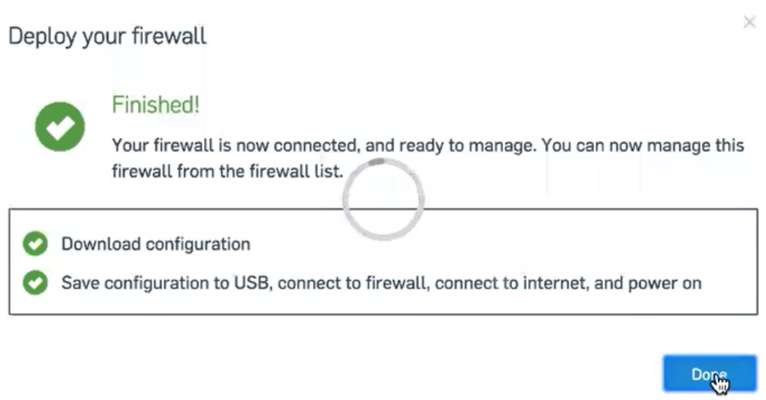


Download Light Touch Configuration File

Download the Light-Touch configuration file, used to configure the firewall on startup. The firewall will apply the configuration and join it to your Central account on startup.

If the firewall will need custom internet settings, and you haven't configured it yet, you can configure them now, before downloading configuration.

If the firewall requires customized settings to access the internet at its deployment location, you can enter those here to include them in the configuration file.



Deploy your firewall

Finished!

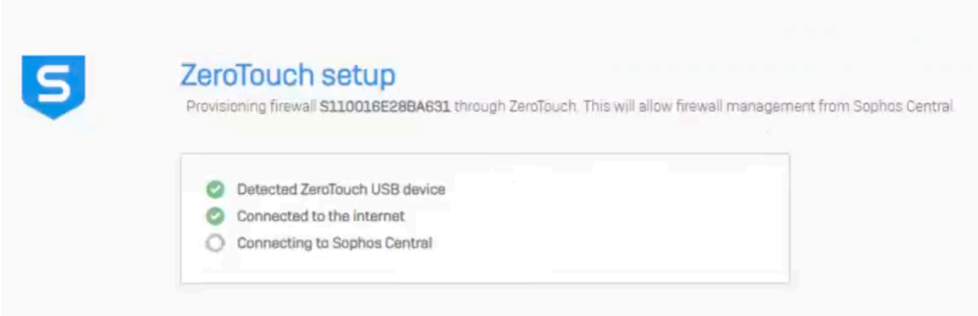
Your firewall is now connected, and ready to manage. You can now manage this firewall from the firewall list.

- ✓ Download configuration
- ✓ Save configuration to USB, connect to firewall, connect to internet, and power on

With the new firewall config file in hand you can email it to someone at the remote location to transfer to a USB stick and then insert that into the device before starting it up.

(3) Connect the USB Stick to the Device and Start It Up

At startup, the device will look for a configuration on any attached USB storage device and utilize it if present. It will then connect to the internet and connect to Sophos Central, and download any firmware updates.

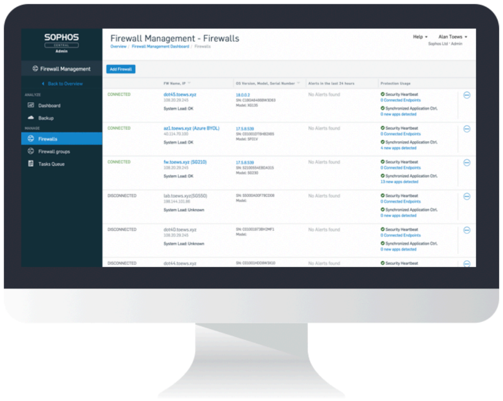


ZeroTouch setup

Provisioning firewall **S110016E28BA631** through ZeroTouch. This will allow firewall management from Sophos Central.

- ✓ Detected ZeroTouch USB device
- ✓ Connected to the internet
- ○ Connecting to Sophos Central

Once the process is complete, your new firewall will be available to manage in Sophos Central.



United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com