With Synchronized Security, Sophos products share threat, health, and security information in real time via the Security Heartbeat™ and respond automatically to threats.

This quick start guide walks you through enabling Synchronized Security between Sophos XG Firewall and Sophos endpoint and server protection managed through Sophos Central (including Sophos Intercept X and Sophos Intercept X for Server).

By following the steps in this guide you will be able to:

- Manage your XG Firewall in Sophos Central 5
- Automatically block compromised devices from accessing corporate data 8
- Block worm-like lateral movement on your network 11
- See which unclassified apps and processes are using your bandwidth 13
- Easily enable user-based firewall rules 17
1. Register your XG Firewall in Sophos Central

To enable Synchronized Security you first need to register your XG Firewall in Sophos Central.

1. Sign in to XG Firewall and go to Central Synchronization in the left-hand navigation
2. Click on Register in the top right corner.
3. In the pop-up box add the email address and password for the Sophos Central account you want to sync with. Click Register.
2. Enable firewall management via Sophos Central

1. If you wish to manage this XG Firewall from Sophos Central, switch **Manage from Sophos Central** to **On**. In the pop-up box click **Apply**.
2. You now need to approve managing this XG Firewall from Sophos Central. Sign in to the Sophos Central Admin account that is synchronized with the XG Firewall.

3. Go to Firewall Management in the left-hand navigation.
4. In the **Firewalls** section, find your recently registered firewall and click **Accept services**.

5. Go back to the **Central Synchronization** page in XG Firewall. In the **Managed from Sophos Central** section check that the status is now **Managed**.
3. Automatically block compromised devices from accessing corporate data

Synchronized Security uses a simple Red – Yellow - Green traffic light system to show the health status of each device. The health status (color) is identified automatically:

- Red: Compromised device e.g. running malware detected on the device, or Sophos protection is not functioning correctly
- Yellow: Dormant malware detected
- Green: Healthy device e.g. no malware detected, Sophos protection is functioning correctly

Connected devices communicate their health status via the Security Heartbeat. To automatically block compromised machines from accessing corporate data, enable XG Firewall to block traffic from unhealthy devices.

1. In XG Firewall select Firewall in the left-hand navigation. Click Add firewall rule and then select User/network rule.
2. Set up your rule to access your corporate data

3. Scroll down to the **Advanced** section at the bottom of the page until you get to the Synchronized Security section.

   - **Minimum source HB [Heartbeat] permitted** controls which devices traffic can come from, based on health status.
   - **Minimum destination HB [Heartbeat] permitted** controls which devices traffic can be sent to, based on health status.
4. Select GREEN or YELLOW based on your requirements:
   - GREEN – blocks traffic from devices/destinations with Red or Yellow health status.
   - YELLOW – blocks traffic from devices/destinations with Red health status.
   We recommend you select YELLOW for both, so you are only blocking traffic from devices with red health status.

5. Leave both Block .. no heartbeat boxes unchecked.
Checking the Block ... no heartbeat boxes will block connections from all devices that do not have a Heartbeat, including devices that are unable to have a Heartbeat such as printers or endpoints not protected by Sophos. We recommend you leave both boxes unchecked as you get started.
4. **Block worm-like lateral movement on your network**

With Synchronized Security, Sophos products can work together to stop threats moving laterally across your network.

1. In Sophos Central go to **Global Settings** in the left-hand navigation.

2. In the **General** section, select **Reject Network Connections**.
3. Under **Reject connections from other devices**, switch on **Allow devices to reject connections from other devices with red health**.
5. See which unclassified apps and processes are using your bandwidth

Synchronized Application Control lets you see all unclassified apps and processes on your network. It lets you identify malicious and unwanted apps that may be hiding in your network traffic.

Synchronized Application Control is on by default; however, you can switch it on manually if needed.

1. In XG Firewall, select Central Synchronization in the left-hand navigation

2. Switch Synchronized Application Control to On. You will be prompted that Security Heartbeat is required for this feature. Click OK.
3. See your unclassified apps and processes. There are a couple of ways to do this:

A) In the XG Firewall control panel, click on the **Synchronized Application Control** widget on the right-hand side of the screen.

![Synchronized Application Control widget](image)

B) In the XG Firewall control panel, select **Applications** in the left-hand navigation, and then select the **Synchronized Application Control** tab.

![Applications tab](image)
4. XG Firewall will automatically classify many applications based on information provided by Sophos endpoint protection.

5. To manually classify an application, for example a custom application built for your organization, click on the application to open the **Customize application** box and then select your desired category. The application will then be subject to the same application control rules as all other application in that category.

![Customize application](image-url)
6. For full reporting on unclassified apps and processes, in XG Firewall select **Reports** from the left-hand navigation, and then select the **Applications & web** tab.
6. Easily enable user-based firewall rules

With Synchronized Security, Sophos endpoint protection can automatically tell XG Firewall which user is sending traffic, making it very easy to create user-based policies. First, synchronize your XG Firewall with Active Directory (AD), and then add the User ID information to your rules.

1. In XG Firewall select Authentication in the left-hand navigation, select the Servers tab, then click Add.
2. Enter the details of the Active Directory server with which you want to synchronize, then click Save.
3. In XG Firewall select Firewall in the left-hand navigation. Click Add firewall rule and then select User/network rule.
4. In the **Identity** section, check the box for **Match known users** then specify who the policy should apply to in **Users or groups**.

Thank you for choosing Sophos to secure your organization.