SOPHOS
Security made simple.

Cyberoam to Sophos XG Firewall migration guide: Firmware and configuration

Product: Cyberoam

Contents

Overview 4
Guidance before you upgrade CyberoamOS to SFOS 4
Migration eligibility 4
Why migrate to SFOS 4
Upgrade CyberoamOS to SFOS 6
Things to know before you upgrade 6
Rollbacks 6
Warranty 6
Licenses 7
Steps to upgrade Cyberoam firmware to SFOS 8
Appendices 15
Appendix 1. Transformation of firewall rules 15
Appendix 2. Changes in individual features 20
Licensed features 20
Wireless 20
Web Application Firewall (WAF) 20
Dynamic DNS 20
General Authentication Client 20
SSL VPN 21
Web and Application filtering 21
Identity 22
High availability (HA) 22
Certificates 22
DHCP/PPPoE 23
SNMP 23
Country host 23
Custom zones 23
HTTP redirection 23
Telnet access 24
Web proxy 24
Appendix 3. Important notes 25

Appendix 4. Renamed CR features 26
Appendix 5. Sophos partner portal 27
Appendix 6. Sophos Central Firewall Manager (For partners) 28
Copyright Notice 29

Overview

This guide helps you migrate the firmware and configuration from Cyberoam to Sophos XG Firewall. Follow the steps in these sections:

- Guidance before you upgrade CyberoamOS to Sophos Firewall OS (SFOS)
- Upgrade CyberoamOS to SFOS (with 30-day Full Guard trial license of SFOS with rollback facility)

Guidance before you upgrade CyberoamOS to SFOS

Migration eligibility

Not all Cyberoam appliances are eligible to run XG Firewall firmware. Only appliances that meet the hardware version and resource utilization requirements can run SFOS.

To check if your Cyberoam hardware supports firmware upgrade to SFOS, click here.

Why migrate to SFOS

SFOS brings to you the best of CR and SG UTM protection along with SFOS-focused enhancements. To fully leverage SFOS features, we recommend that you upgrade to an XG Firewall. Upgrading to the powerful XG hardware allows you to run the full Sophos Firewall functionality and protection.

Sophos Firewalls carry the latest industry-grade hardware and deliver the high performance required by continuously evolving networks. With enhanced user interface and powerful security features, Sophos XG Firewall offers the following advanced functionality:

- Advanced threat protection to capture zero-day threats
  - Sandstorm (Cloud-based sandboxing)
  - Advanced Threat Protection (ATP)
  - Improved TALOS IPS patterns
- Synchronized Security for endpoint protection
  - Security Heartbeat
  - Synchronized Application Control
  - Sync user ID
- Powerful web and email protection
  - Cloud Access Security Broker (CASB) to monitor data being stored in cloud storage services
  - Secure Web Gateway (SWG) enhancements
  - Full-fledged email protection: MTA, SPX encryption, DLP
  - Safe Search on each web policy
- Improved routing, logging, and reporting

    - Policy-based routing
    - Improved log viewer and reporting (raw logs, export logs, executive report)
    - DNS request route
- Enhanced remote security
    - SSL VPN (OTP feature)
    - Free IPsec VPN client
    - Two-factor authentication
    - Site-to-Site RED tunnels
    - Hotspot feature for hotels and educational institutions
    - FQDN-based login portal
- Improved UX and manageability
    - Multi-zone-based firewall rule; matching criteria-based automatic firewall rule grouping
    - Wildcard-based FQDN
    - Installation wizard and firmware upgrade directly from the appliance
    - Management from Sophos Central

Upgrade CyberoamOS to SFOS

To upgrade Cyberoam firmware to SFOS, follow these steps:

- The Cyberoam appliance must be registered and have valid support subscription, which you can verify from the Cyberoam Customer Portal.
- We recommend that you upgrade CyberoamOS to its latest firmware version before you upgrade to SFOS.

If you're a partner, you can refer to the details of registering appliances on Sophos partner portal and Sophos Central Firewall Manager.

Things to know before you upgrade

- Rollbacks
- Warranty
- Licenses
- Features

Rollbacks

When you upgrade to SFOS, you can choose the 30-day SFOS Full Guard trial. During the trial period, you can roll back to CyberoamOS. Rollback is a simple process and is as short in duration as a device reboot.

Once you reboot with CyberoamOS, the earlier configuration, reports, and subscriptions will be restored. Configuration changes made on SFOS will be lost.

Once you upgrade permanently to SFOS, you cannot rollback to CyberoamOS.

Warranty

Once you upgrade the Cyberoam appliance to SFOS, Sophos XG Firewall warranty rules will determine warranty expiry.

- Start date for SFOS warranty is based on the following:
  - Cyberoam registration date, if you have registered the appliance within 90 days of the invoice date.
  - Cyberoam invoice date, if you have registered the appliance after 90 days from the invoice date.
- Warranty expiry date is a minimum of 12 months from the warranty start date and can extend to a maximum of 5 years.
- Within this period, the expiry date of Enhanced Support subscription (which can be renewed) determines the warranty expiry date.

Note: After warranty expires, you will not be eligible for RMA (Return Merchandise Authorization).

Example:

Warranty and subscription	Dates	Details
Cyberoam invoice date	28-May-2017	With 3 years Total Value Subscription (TVS)
Upgrade to SFOS	15-Dec-2017	
Warranty start	28-May-2017	Set to Cyberoam invoice date since the device has been migrated after 90 days from the invoice date
Warranty expiry	27-May-2020	Up to subscription expiry date
Sophos XG Firewall subscription		
Start date of 3-year Full Guard subscription of XG Firewall	27-May-2020	Includes Enhanced Support subscription
Subscription expiry	27-May-2023	
Warranty expiry	27-May-2022	Extended by two years based on Full Guard subscription, which includes Enhanced Support subscription. (Capped at 5 years from Cyberoam invoice date.)

Licenses

XG Firewall's Full Guard trial includes licenses of all modules, including web, email, web server, network protection. Details of equivalent Sophos licenses for single and bundled Cyberoam licenses are in the license migration guide.

During the trial period, Cyberoam licenses will remain valid and their duration will continue to elapse.

After migration to SFOS, you need to purchase or renew SFOS subscriptions and not Cyberoam subscriptions.

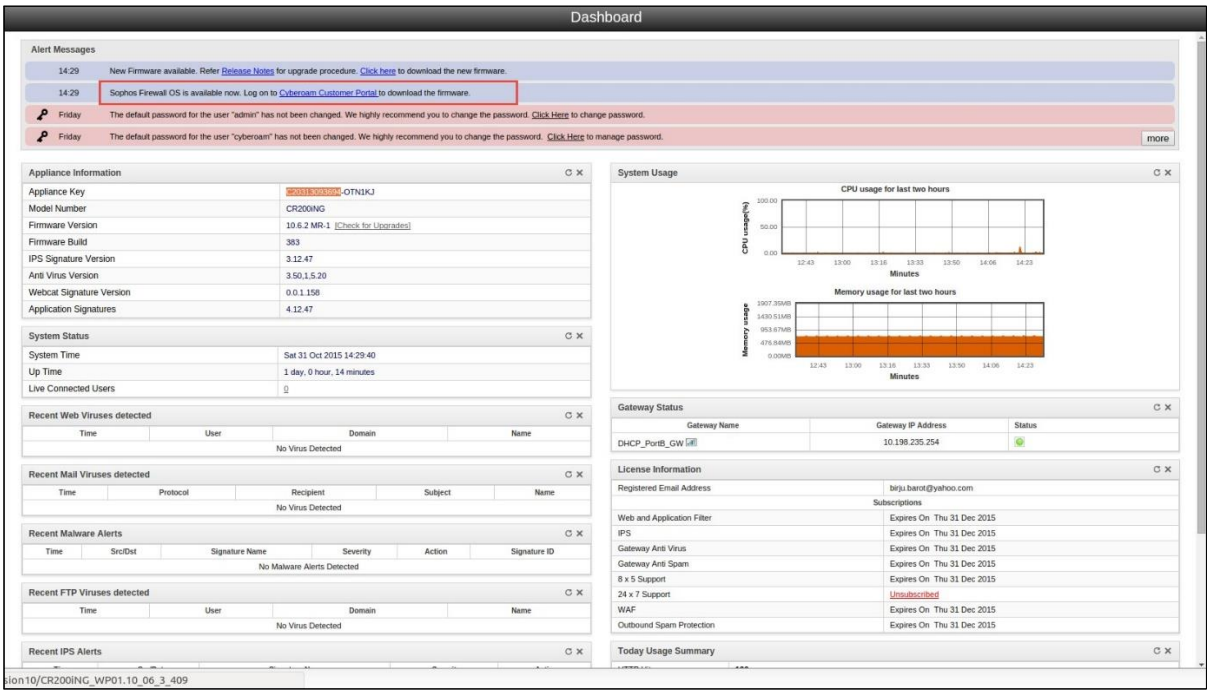
Activate SFOS license keys after migration: To activate the license keys, the firmware must be permanently migrated to SFOS. For details of permanent migration, click here.

Steps to upgrade Cyberoam firmware to SFOS

Step 1

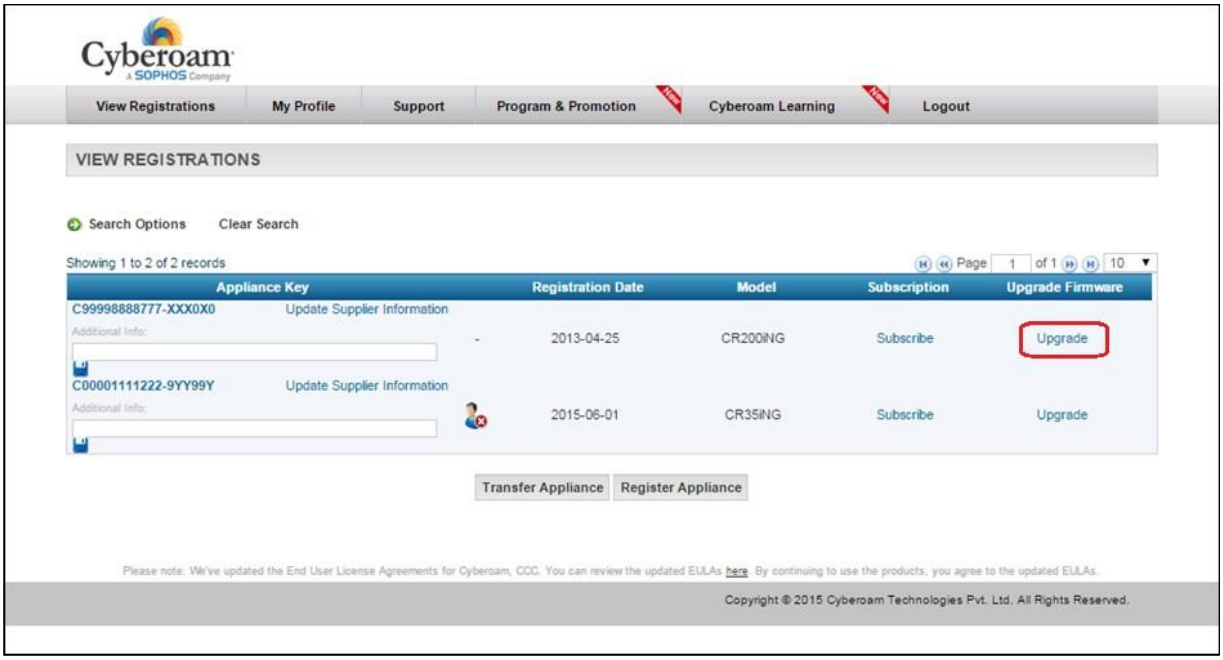
When SFOS upgrade is available, an alert appears on your Cyberoam dashboard. Click **Cyberoam Customer Portal** and log in.

Note: You need to activate unused Cyberoam license keys, if any. You cannot activate these after firmware upgrade to SFOS.



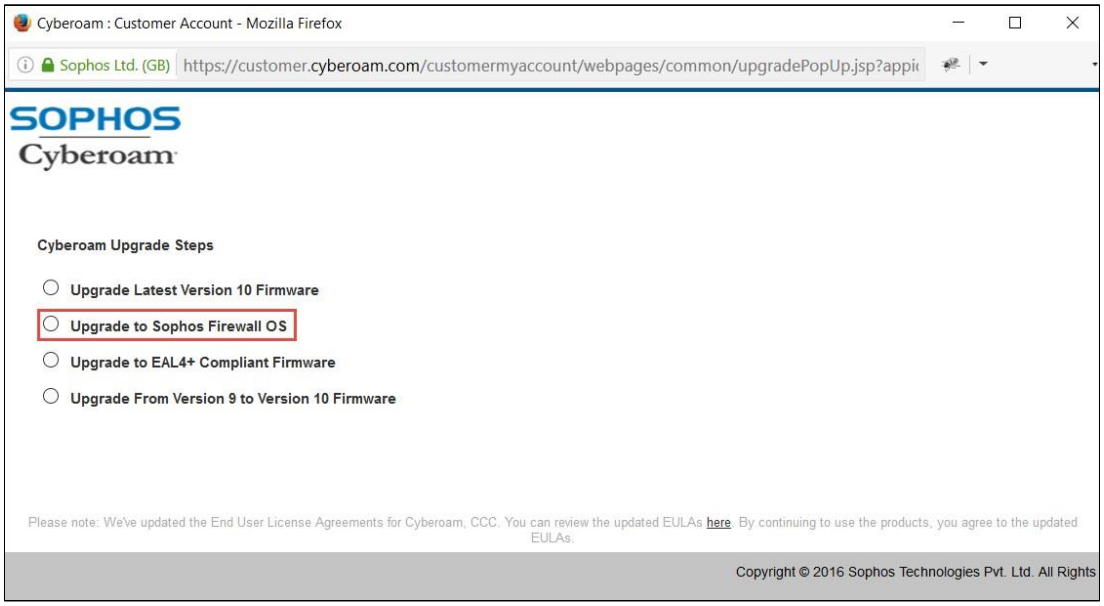
Step 2

Click **Upgrade** against the appliance you want to upgrade.



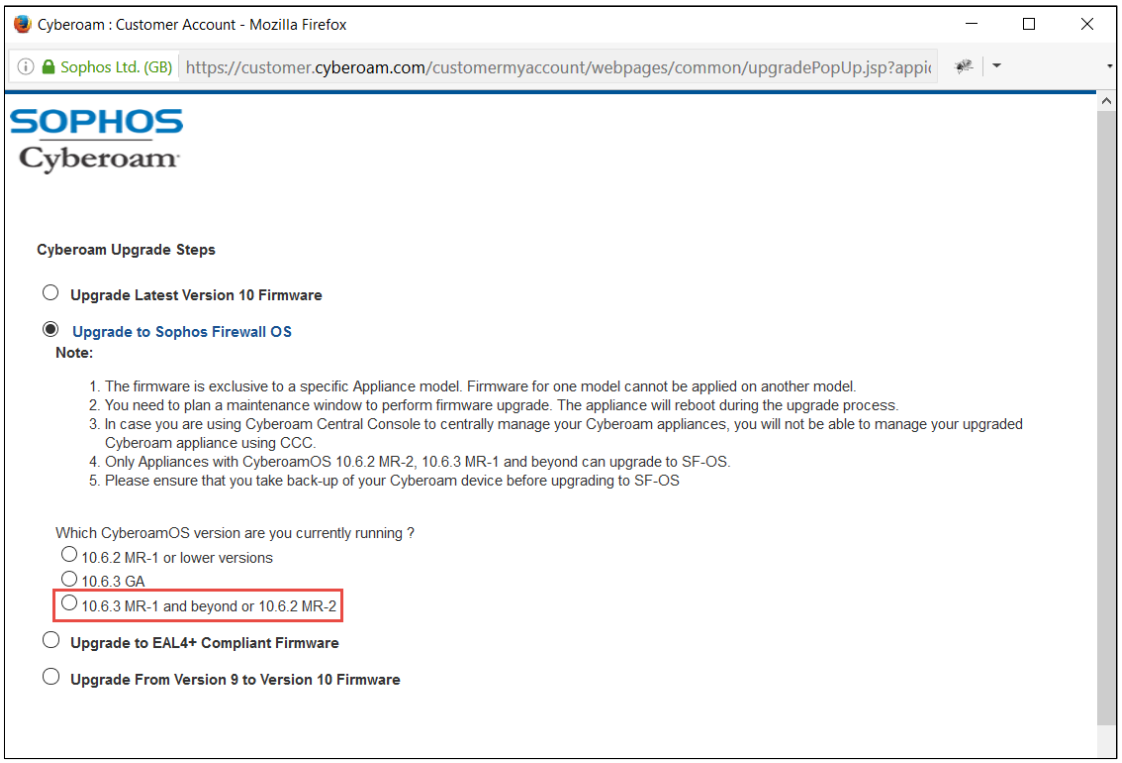
Step 3

Select **Upgrade to Sophos Firewall OS.**



Step 4

Select your current CyberoamOS firmware version. Click **Next**.

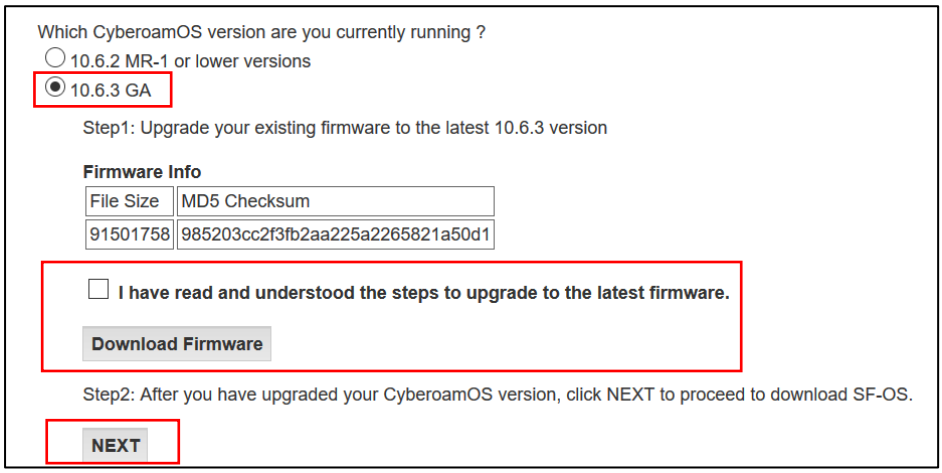


Step 5

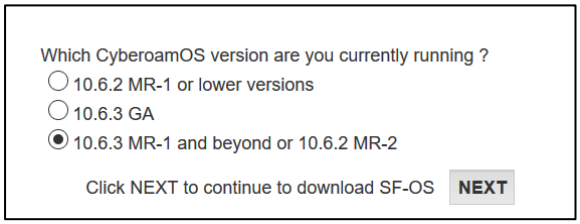
Select the current CyberoamOS version.

Options:

For 10.6.2 MR-1 or lower versions and 10.6.3 GA, click **Download firmware** to upgrade to the latest version of 10.6.3. Click **Next** to download SFOS.

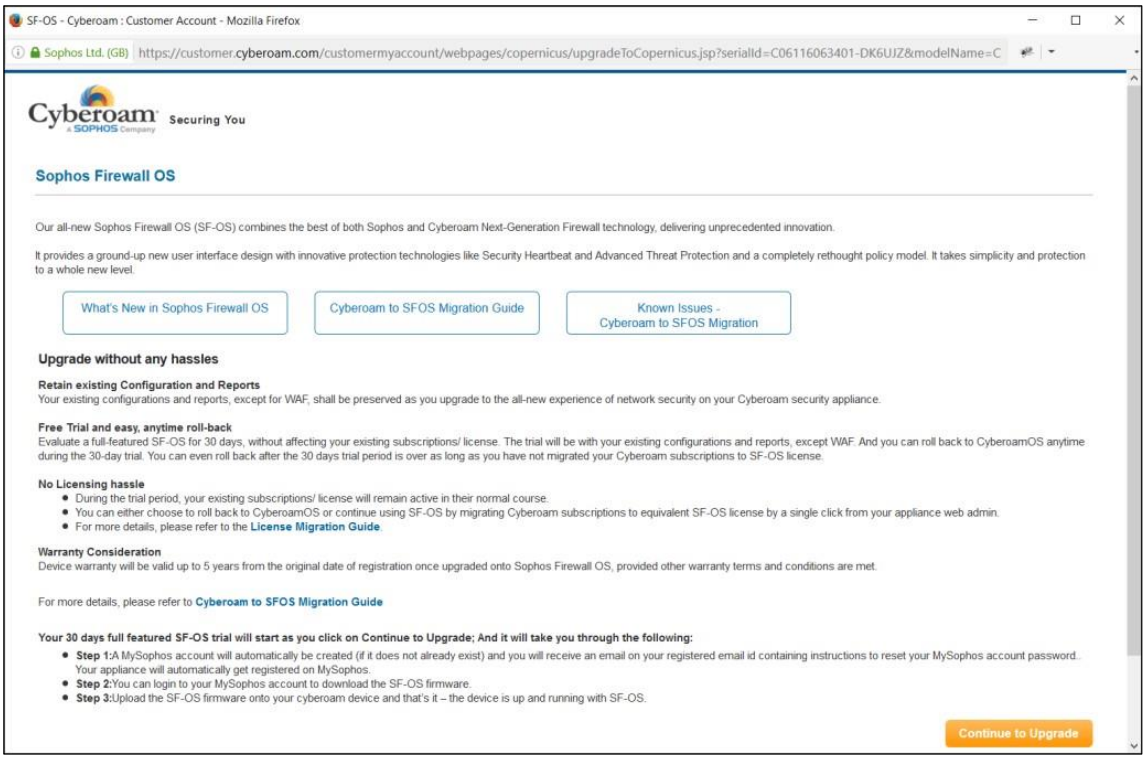


For 10.6.3 MR-1 and beyond or 10.6.2 MR-2, click **Next**.



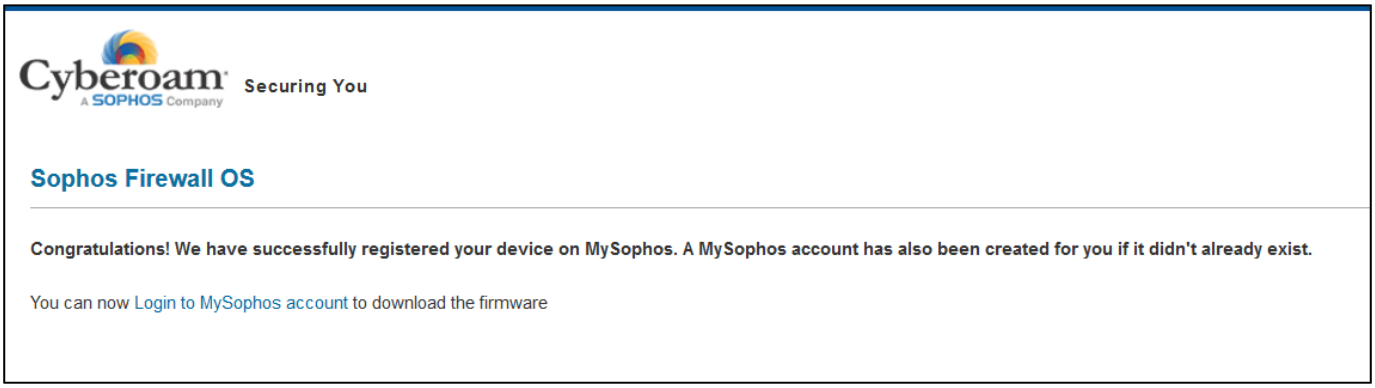
Step 6

Click **Continue to upgrade**.



Step 7

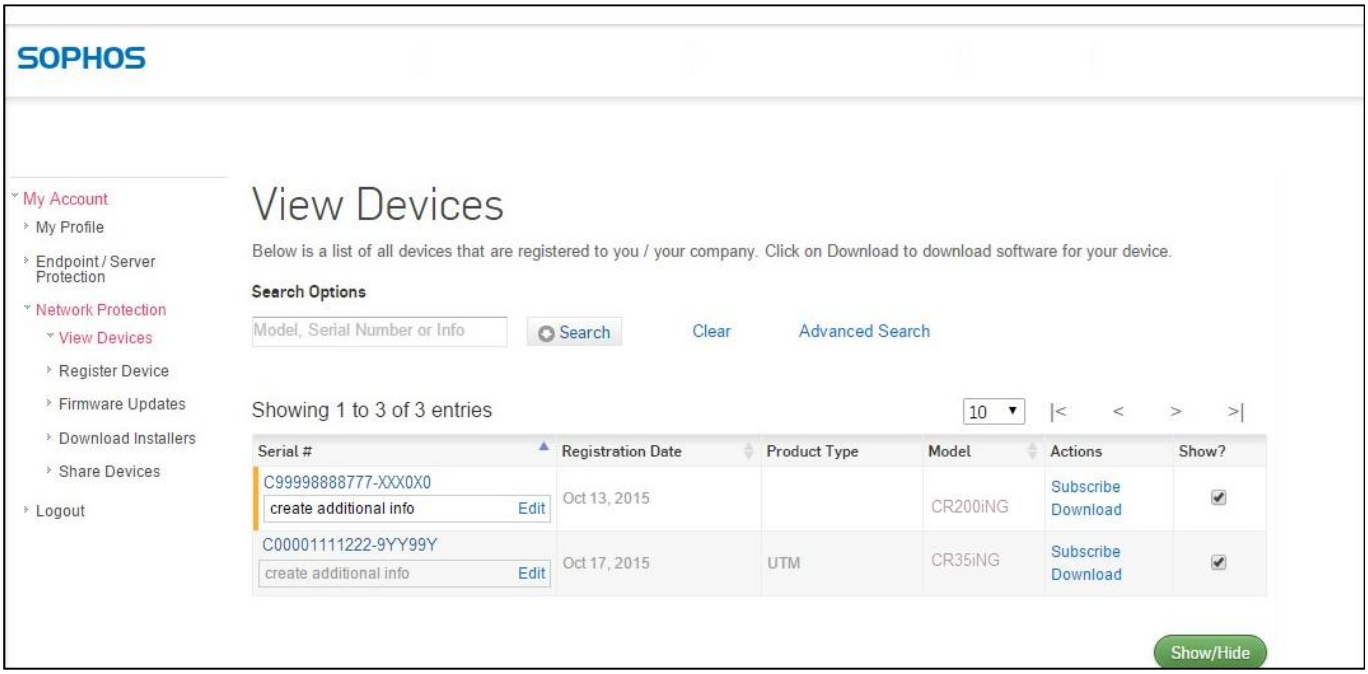
Your Sophos ID and MySophos account will be created automatically (if you don't have one already) with instructions to reset the password.



Cyberoam Customer Portal

Step 8

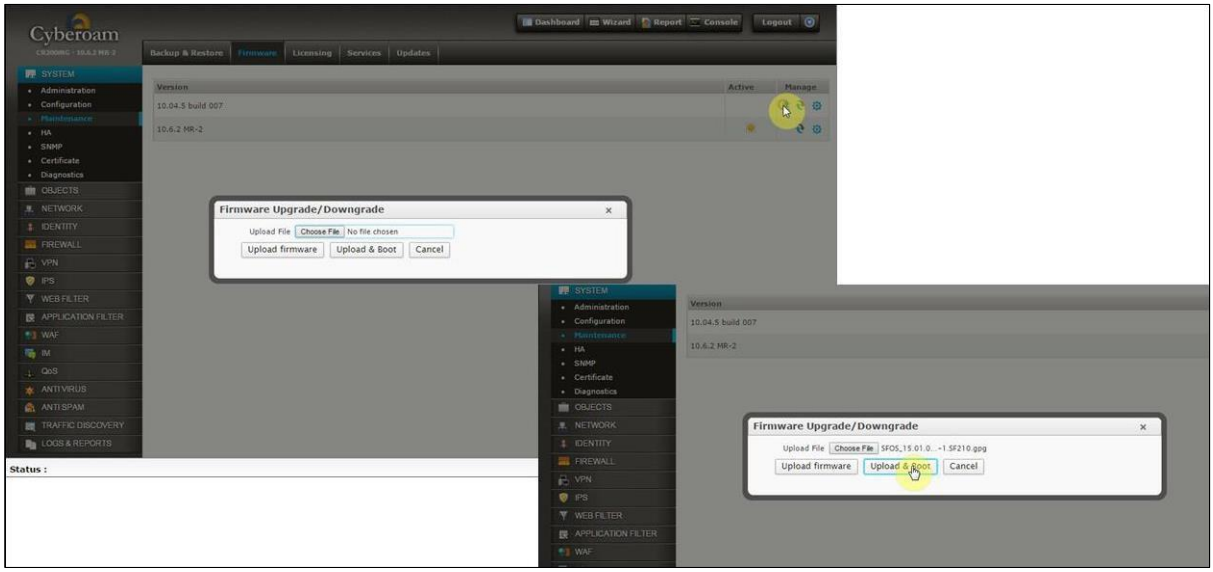
Log in to your MySophos account and Click **Download** against the Cyberoam appliance to download SFOS firmware.



MySophos Account

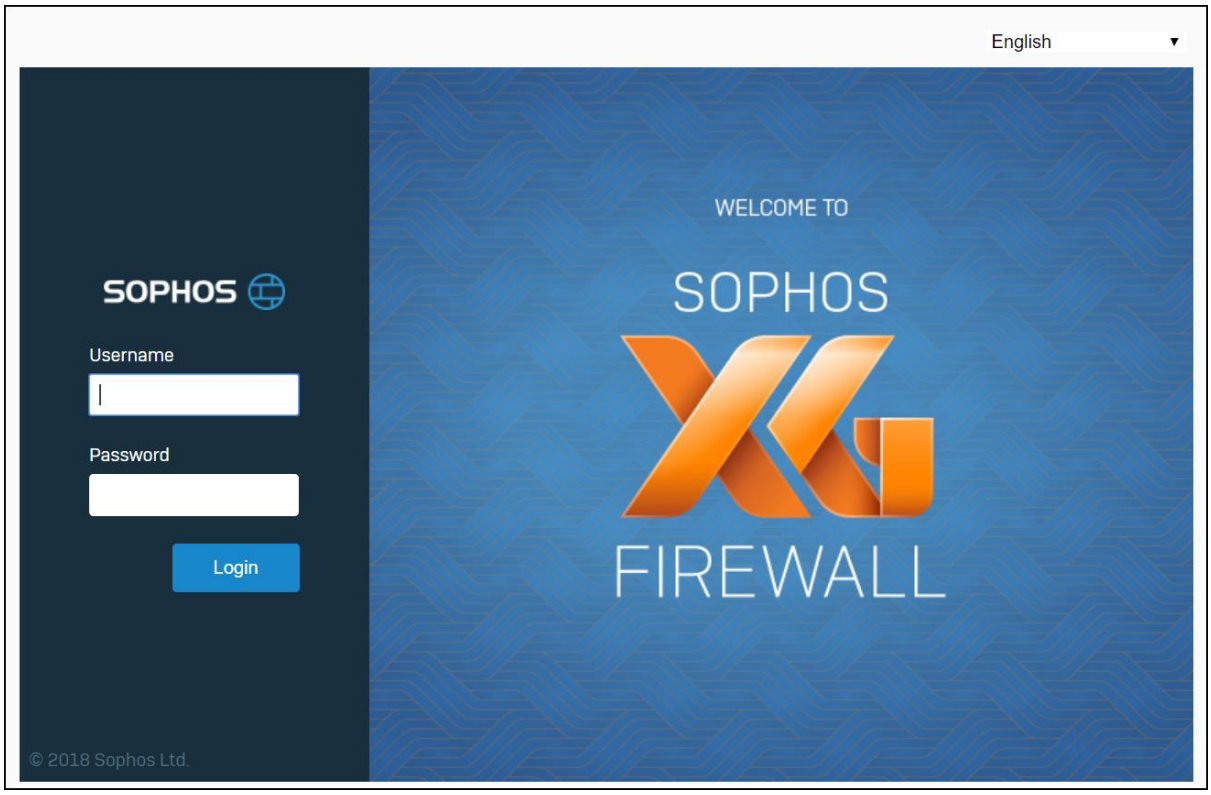
Step 9

Log in to Cyberoam web admin console and go to **System > Maintenance > Firmware**. Click the **Upload** button. Select the downloaded firmware (.gpg file) and click **Upload and Boot**.

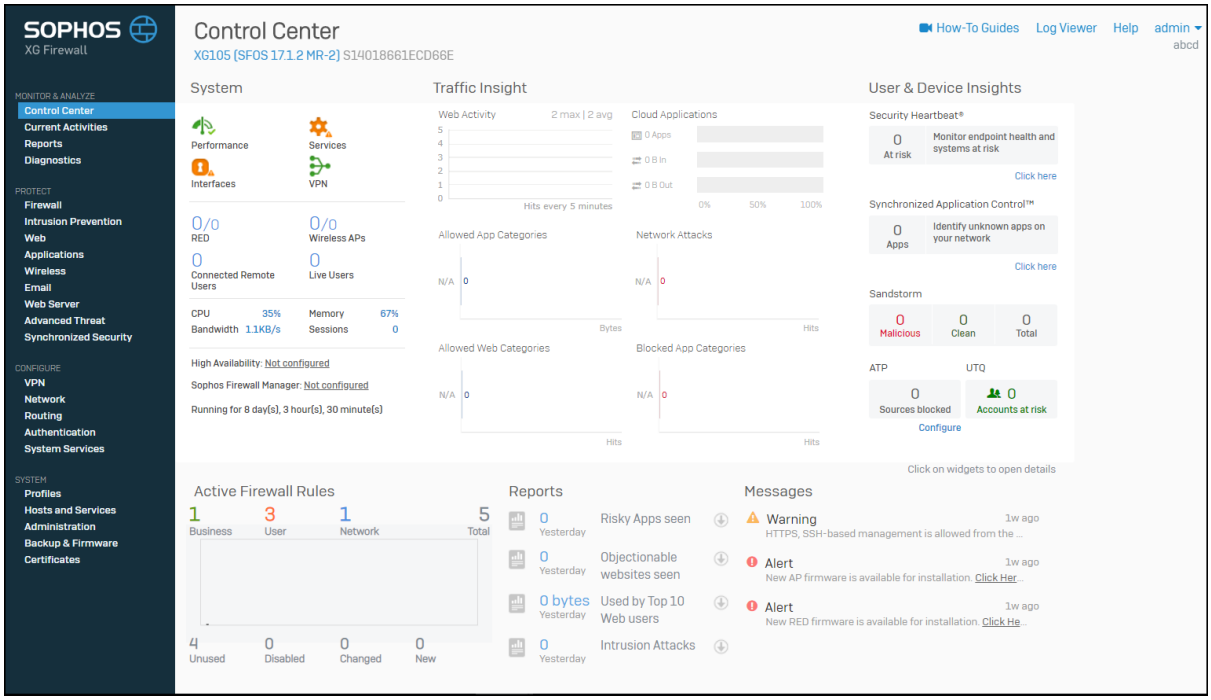


Step 10

After the device starts, log in with your administrator credentials (admin/admin).



Note: The Cyberoam appliance's model number and serial key will not change. Virtual appliances will be renamed with the corresponding XG model numbers.



Results

CyberoamOS has been migrated to SFOS with 30-day Full Guard trial license.

Appendices

Appendix 1. Transformation of firewall rules

Firewall rules will be migrated to SFOS in the following manner:

1. WAF-related rules will not be migrated.
2. For rules related to LOCAL Zone:
    a. If Action in the source rule is marked Reject or Drop, Action in the migrated rule will be Drop.
    b. Log Firewall Traffic parameter will be disabled for all migrated rules.
    c. Identity will be disabled for all migrated rules.
    d. Destination Host will always be "Any" in the migrated rule. Rules with specific Destination Host will not be migrated.
    e. All service–specific rules will be migrated as they are. However, if the service specified in the Cyberoam rule is not present in SFOS, the rule will not be migrated.
3. Non–identity-based rules:
    a. Rules with Identity disabled will be migrated to SFOS as Network rules.
    b. Rules that have Email Scanning enabled will be migrated to SFOS as Business application rules. Rules with SMTP and/or SMTPS Scanning enabled will be migrated as policy with Email server template. Rules with POP, POPS and/or IMAP will be migrated as policy with Email client template.
    c. For rules with Email Scanning and HTTP/HTTPS/FTP scanning enabled, two corresponding rules will be created in SFOS:
        a. A Business application rule with Email client or Email server template, as applicable.
        b. A Network rule with the corresponding Web filter, Application filter and HTTP/HTTPS/FTP scanning configuration, if any.
4. Virtual Host-based rules:
    a. Rules with Action set to "Drop" or "Reject" will be migrated as the respective User/Network rule, containing external information of the source rule.
    b. Rules with Action set to "Accept" will be migrated to SFOS as Business application rules with non-HTTP-based template. The corresponding Web filter, Application filter, Multi-link management (MLM) and HTTP/HTTPS/FTP/IMAP/POP scanning configuration, if any, will not be carried over.
    c. Loopback rules will be migrated to SFOS as Business application rules with non-HTTP-based template. The corresponding Web filter, Application filter, Multi-link management (MLM) and HTTP/HTTPS/FTP/IMAP/POP scanning configuration, if any, will not be carried over.

d. Reflexive rules will be migrated as they are to User/Network rules. Rules with SMTP and/or SMTPS scanning enabled will be migrated as rules with Email server template. Rules with POP, POPS and/or IMAP will be migrated as rules with Email client template.
e. Virtual host rules using #vhost as a service will be migrated as they are.
f. For rules with destination set to "Any" and no Virtual Host rules, a corresponding Virtual host rule will be created along with a Network rule based on the source and destination zones.
g. Rules that have destination host set to "Any" will be migrated to SFOS as Business application rules with non-HTTP-based template. Rules with SMTP and/or SMTPS scanning enabled will be migrated as rules with Email server template. Rules with POP, POPS and/or IMAP will be migrated as rules with Email client template. The corresponding Web filter, Application filter, Multi-link management (MLM) and HTTP/HTTPS/FTP scanning configuration, if any, will be carried over in a separate Network rule.

5. Identity-based rules (applicable when migrated from CR 10.6.3 MR3 or earlier to SFOS):
   a. Rules in which Web and Application Filter policies are defined, are migrated as they are to User rules. If the destination zone in the rule is a zone other than WAN, the Web and Application Filter values are not carried over to the migrated rule.
   b. Rules in which specific users are specified, are migrated as User rules. The user-specific Web and Application Filter policies are carried over with the corresponding configuration in the rule. However, if the CR rule has Web and Application Filter parameters defined, the rule is migrated as it is.
   c. Group-specific Web and Application Filter policies are carried over as the corresponding configuration in the rule. However, if the CR rule has Web and Application Filter parameters defined, the rule is migrated as it is.
   d. Rules in which specific groups or "Any" are specified, are migrated as User rules.
   e. If user-specific policies differ from those in the group, a separate User rule is created for the user-specific policies based on the method described in point 5b.
   f. If Email Scanning is enabled in the CR Rule, a corresponding Business application rule with Email client template is created along with this rule.
6. Identity-based rules (applicable when migrated from CR 10.6.3 MR4 to SFOS):

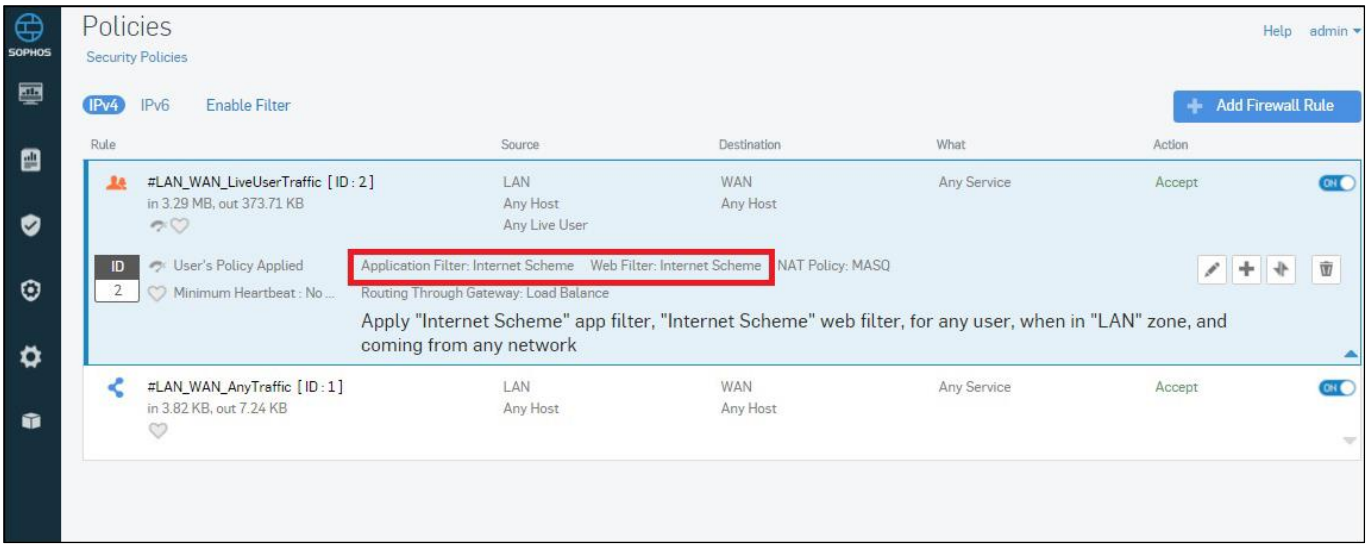
a. Rules in which User's Policy has been applied to the web/app filter are migrated with "Internet Scheme" applied to the migrated rules. In the Internet scheme* page in SFOS (Web > Internet scheme), all the users/groups from Cyberoam are listed along with the specific web and app filter policies that have been applied to each.
b. User or Group-based rules in which a User's Policy has been applied to the web/app filter, are migrated with "Internet scheme" applied to the migrated policies. In the Internet scheme* page in SFOS (Web > Internet scheme), users/groups affected by the rule are listed along with the specific web and app filter policies that have been applied to each.
c. User or Group-based rules in which the app filter is set to User's Policy and web filter is set to CIPA are migrated with app filter set to "Internet scheme" and web filter set to CIPA.
d. User or Group-based rules in which app filter is set to Custom Policy and web filter is set to User's Policy are migrated with app filter set to Custom policy and web filter set to Internet scheme.
e. If the user or group is not present in the Internet scheme* page, the default web and app filter policies are applied to users.

7. Rules containing Discover (TAP) zone will not be migrated.
8. Default firewall rule groups will be migrated as SFOS firewall rule groups based on the zones. For example, firewall rules with source zone WAN and destination zone LAN will be migrated to the automatically created group named WAN to LAN IPv4 traffic or WAN to LAN IPv6 traffic.

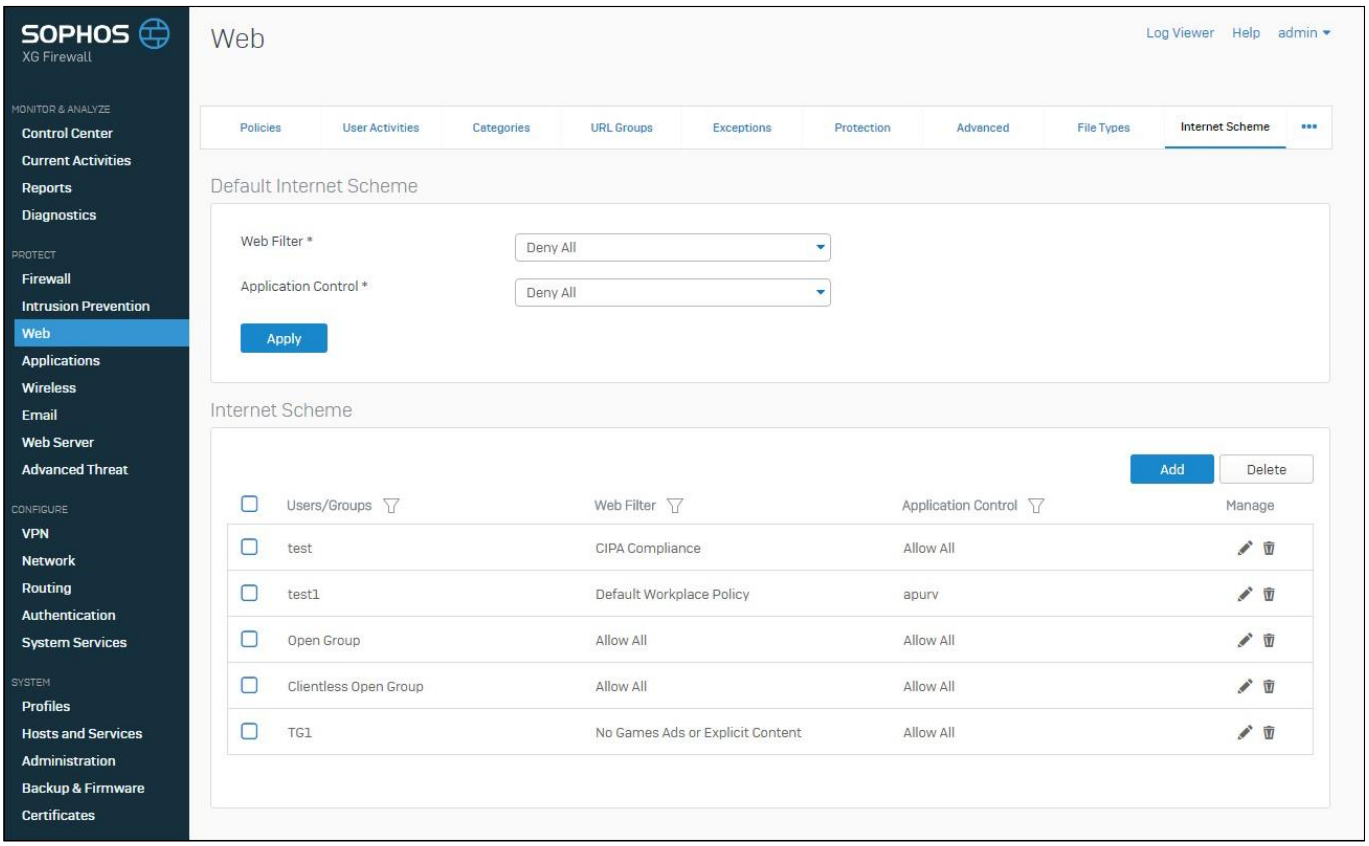
Internet scheme page

*The Internet scheme page is displayed after migration from CR 10.6.3 MR4 to SFOS. It displays the list of all users and groups affected by the migrated firewall rules, listing the corresponding web and app filter policies applied to them.

For example, Cyberoam Firewall Rules in which User's Policy has been applied to the web/app filter are migrated with "Internet scheme" applied to the migrated Firewall rules.



In the Internet scheme* page in SFOS (Web > Internet scheme), all the users/groups from Cyberoam are listed along with the specific web and app filter policies that have been applied to each.



Behavior difference

Difference in behavior between Cyberoam firewall rules and SFOS firewall rules after migration:

- You will not be able to configure Email scanning, WAF, and Virtual host on User/Network rules.
- Web and Application filter policies are not associated with individual users or groups. They will have to be applied using Firewall rules.
- AV/AS scanning, Web/Application filter policy and MLM are not available in non-HTTP (Virtual host) Business application rules.
- Web/Application filter policies are not available in Email client and Email server templates.
- Multi-Link Management is not available on Email server template.
- Destination host "Any" will not cover all the virtual hosts.
- For Business application rules, the corresponding reflexive firewall rules will be created but will not be visible on the Firewall rule page. The reflexive rule inherits its properties from the rule with which it is associated.

Appendix 2. Changes in individual features

Licensed features

For features related to Web, Email and Network protection, if you haven't subscribed to the respective licenses, SFOS will allow you to configure the feature, but will not perform the corresponding scanning and logging. For example, if you haven't subscribed to the Network Protection module, SFOS will allow you to create custom IPS signatures and policies but will not scan or log the traffic.

Similarly, if a license expires, SFOS will stop scanning and logging traffic related to the module without disrupting network traffic.

However, for security reasons, this behavior does not hold true for Web server protection module. You need a valid license of the module for SFOS to allow any traffic from your Web servers.

Wireless

If the Security mode of a wireless network is set to WEP Open, after migration, the Wi-Fi key of the network will be regenerated. This is applicable to Cyberoam firmware version 10.6.3 MR4 and later versions.

If Wireless Protection in Cyberoam is disabled, Access point and DHCP configuration is not carried over to SFOS.

Web Application Firewall (WAF)

WAF configuration of the Cyberoam appliance will not be migrated to SFOS firmware. You need to reconfigure WAF-related policies in SFOS firmware.

Dynamic DNS

If you've used Cyberoam (<host name>. ddns.cyberoam.com) as your Dynamic DNS service provider, it will be migrated to SFOS as a non-editable entity. To continue using DDNS services smoothly, we recommend that you either register with and use a third-party DDNS service provider, or use Sophos (<host name>.myfirewall.co) as your provider.

General Authentication Client

- Users will not be able to log in to SFOS using Cyberoam General Authentication Client (GAC). They need to download and install new instances called Client Authentication Agents (CAA) from the User portal.
- User-MAC binding will not be supported after migration to SFOS.

- After migration, each agent will be bound to the XG Firewall through the appliance certificate and communication will take place over a secure channel. Hence, an agent authenticating to one XG Firewall cannot be bound to another XG Firewall.
- In SFOS, users will be logged out from CAA once they connect to the device using VPN.

SSL VPN

- SSL VPN users will not be able to connect to SFOS using Cyberoam SSL VPN Client. They need to install new instances of SSL VPN Client for SFOS, which can be obtained from the User portal.
- SSL VPN portal (accessed from https://<Cyberoam WAN IP Address>:8443) will be part of the SFOS User portal. After migration, users can access the User portal from https://< Cyberoam LAN IP Address>:8443.
- SSL VPN port cannot be configured in SFOS.
- SSL VPN Bookmarks of Type IBM Server Terminal will be converted to Telnet bookmark type after migration.
- If you have customized the Simultaneous Login SSL VPN Users, after migration, reset the limit to unlimited to prevent the "Maximum Login Limit" error being displayed to users.
- If you have configured per user certificate for SSL VPN, after migration, you need to delete the user certificates from your appliance. Users will then need to download and import a new SSL VPN Client bundle for SFOS from the User portal.

We've discontinued the following SSL VPN-related commands:

console> set sslvpn proxy-sslv3

console> set sslvpn web-access

console> show sslvpn log

console> show sslvpn proxy-sslv3

console> show sslvpn web-access

Web and Application filtering

The Web categorization database in SFOS will contain a different set of categories from those of Cyberoam.

If you haven't subscribed to the Web protection license, you will be allowed to configure web and application settings, but the traffic will not be scanned or logged.

The Web filter policy page (**Web > Policies**) has been revamped to allow inline configuration of policies.

Further, SFOS does not support the following:

- Selective upstream proxy (CLI Command: console> set service-param HTTPS ssl_upstream_tunnel)
- ICAP (CLI Command: console> set icap edit)
- Proxy DoS Settings (CLI Command: set http_proxy dos)

Identity

For integration with an Active Directory (AD) server, Integration Type "Loose Integration" has been discontinued. By default, XG Firewall will integrate with an AD Server with Tight integration. If you have configured your AD Server with Loose Integration, it will be converted to Tight integration.

In SFOS, Web and Application filter policies cannot be assigned to users/groups directly. If you want to apply Web or Application filter policies to a user/group, use firewall rules.

High availability (HA)

In SFOS, specification of a passphrase is compulsory for HA configuration. Existing Cyberoam HA setups will be migrated to SFOS with a unique random passphrase. In SFOS, you can check and update the HA configuration from **Configure > System services > High availability**.

Certificates

Cyberoam Certificates will be carried over to SFOS firmware with the following changes:

- Default CA will be unchanged.
- Cyberoam Self-signed CA will be renamed as SecurityApplianceSelfSIgnedCA. Contents will remain the same.
- Cyberoam_SSL_CA will be renamed as SecurityAppliance_SSL_CA and will be regenerated with default values.
- Appliance certificate will remain the same and will remain signed by SecurityApplianceSelfSIgnedCA.
- Behavior of SSLVPN per user certificate will remain the same as in Cyberoam.

DHCP/PPPoE

In SFOS, DHCP and PPPoE can be configured on interfaces of all zones except of VPN. In Cyberoam, it was available only in WAN Zone.

If two Cyberoam appliances in HA mode are migrated to SFOS, DHCP service in the auxiliary appliance may stop running. You need to remove the existing DHCP configuration to restart the DHCP service.

SNMP

You don't need to create a firewall rule in SFOS to allow SNMP traffic when SNMP is configured. The related Firewall Rule created in Cyberoam will not be migrated as it is.

Country host

- Country hosts will be migrated to SFOS as Country names. You don't need to create a Country host explicitly. You can directly use the list of countries that are available for the creation of a Country group.
- IP Hosts with Country name set to Hostname will be migrated to SFOS as Country name_Custom.

Custom zones

By default, the following services will be enabled for migrated custom zones on **System > Administration > Device access**:

- SNMP service will be enabled for custom LAN and DMZ zone.
- SMTP relay service will be enabled for custom LAN zone.

HTTP redirection

SFOS web admin console will be accessible only through HTTPS after migration, even if you had configured Device access through HTTP. HTTP requests will be redirected to HTTPS automatically. In SFOS, you will be allowed to enable and configure admin access only through HTTPS.

HTTP-related Local service ACL exception rules with Drop action will be deleted. Those with Accept action will be converted to HTTPS rules.

Telnet access

CR appliances that have Telnet access enabled for any zone will be converted to SSH access. In SFOS, if you enable Telnet access, a warning message will be displayed, advising you to switch to SSH access.

Web proxy

Web proxy section has been moved to **Web > Advanced**. The parameter “Trusted Ports” has been renamed “Allowed destination ports”.

Appendix 3. Important notes

1. You can't access the SFOS admin console over HTTP.
    a. In SFOS, HTTP setting has been removed from the Device access page.
    b. If HTTP access was enabled before upgrade, the admin port settings for HTTP will be preserved and HTTP requests for device access will be redirected to HTTPS.
    c. In case of fresh installation, factory reset configuration, or if HTTP was disabled before upgrade, HTTP admin port settings will be removed.
2. You can't access SFOS over Telnet.
    a. All Telnet requests will be converted to SSH.
    b. A warning message will be displayed on the Device access page if admin enables Telnet access for any zone.
3. ICAP will not be supported.
4. Web Proxy DOS Setting will not be available.
5. AV scanning on Virtual host will not be supported without active Webserver protection (WAF) subscription.
6. SFOS will not create "All" service-based rule for ACL (local) rule.
7. FTP scanning will be supported only for User/Network rule.
8. JavaScript emulation for URLs/cookies will not be supported in Webserver protection (WAF).
9. Auto-learning of added exceptions in WAF will not be supported.
10. Instant Messaging (IM) will not be supported.
11. Route-based VPN will not be supported.
12. Nested Group Support in NTLM will not be supported.
13. Overriding organizational Web filter policy restrictions will not be available.
14. User-MAC binding will not be supported.
15. SSLVPN Port Configuration will not be supported.
16. All Self-signed certificates and Certificate authorities will be regenerated on upgrade. You will have to re-import the certificate for all services that use them.
17. Reflexive rule for Business application rules will not be displayed on the Firewall page. All the policies of the Reflexive rule will be inherited from the Business application rule (including SNAT).
18. In Cyberoam, AV scanning of Web Servers (Virtual Hosts) is allowed if AV Module is subscribed and WAF module is not subscribed. In SFOS, admin needs an active Web server protection subscription for AV scanning of Web servers.

Appendix 4. Renamed CR features

1. My Account has been renamed User portal. User portal displays user information and facilitates SSL VPN, Hotspot, and download of clients. It is accessible from https://<SF IP Address> and is enabled by default from the WAN zone.
2. QoS has been renamed Traffic shaping.
3. Network > Gateway has been renamed WAN link manager.
4. Parent Proxy has been renamed Upstream proxy.
5. Appliance Access has been renamed Device access.
6. 4-eye Authentication has been renamed Data anonymization.
7. Data Transfer Policies has been renamed Network traffic quota.
8. Country Host Group has been renamed Country group.
9. Wireless WAN has been renamed Cellular WAN.
10. In **Web > Protection**, Deny Unknown Protocols has been renamed Block unrecognized SSL protocols.
11. In **Web > Protection**, Allow Invalid Certificates has been renamed Block invalid certificates (with the behavior change suggested by the name).

Appendix 5. Sophos partner portal

As a partner, you can upgrade Cyberoam appliances to SFOS and manage them through the Sophos partner portal. You cannot manage these devices from the Cyberoam partner portal.

1. Ensure that the Cyberoam appliances have valid, permanent (not trial) licenses. You can add only these appliances to the Sophos partner portal.
2. Upgrade CyberoamOS to SFOS.
3. To add the devices to the Sophos partner portal, write to GlobalSEDesk@sophos.com with the following device and partner details:
    a. Serial numbers of devices
    b. Your registered email address
    c. Your company name
    d. Partner portal username

    Global SE Desk will coordinate with the licensing team to add the migrated devices to Sophos partner portal.

Appendix 6. Sophos Central Firewall Manager (For partners)

As a partner, you can manage the upgraded Cyberoam appliances through the Sophos Central Firewall Manager (CFM). You cannot manage these appliances through Cyberoam's on-Cloud Management Service (CCMS).

1. Refer to the CFM guide for partners to ensure that Cyberoam appliances appear on the Sophos Central partner dashboard. Click here for the CFM Partner dashboard help.
2. If the upgraded appliances do not appear on the Sophos Central partner dashboard, write to GlobalSEDesk@sophos.com with the following device and partner details:
    a. Serial numbers of devices
    b. Registered email address
    c. Partner's company name
    d. Partner portal username

    Global SE Desk will coordinate with the licensing team to add the migrated devices to the Sophos Central partner dashboard.

Copyright Notice

Copyright 2019 Sophos Limited. All rights reserved.

Sophos is a registered trademark of Sophos Limited and Sophos Group. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the license terms or you otherwise have the prior permission in writing of the copyright owner.