

Early Access Program (EAP1) Evaluation Guide for Firewall Group Management

Firewall Group Management EAP1 Feature List

#	Features	Exceptions – Not supported tabs/pages
1	Join to cloud of SFOS v18 Firewall device to Firewall Group Management	
2	Groups management in Central	
3	Group based management of Firewall devices in Central	
4	Configure and manage Web policies from Central	<ul style="list-style-type: none"> • General Settings • User Notifications
5	Configure and manage Advanced Threat policies from Central	
6	Configure and manage Authentication policies from Central	<ul style="list-style-type: none"> • Web Authentication
7	Configure and manage Host and Services from Central	<ul style="list-style-type: none"> • IP Host Group • Country
8	Configure and manage System services from Central	<ul style="list-style-type: none"> • Log Settings
9	Connection and Config States	
10	Tasks Queue	
11	Configure and manage Firewall Rules & Policies from Central	<ul style="list-style-type: none"> • Filters • Dynamic objects to select Zones, Network interface, Host-System Hosts in SSL/TLS rules and apply this configurations on different Firewall devices together

Firewall Group Management EAP1 Feature List

#	Features	Exceptions – Not supported tabs/pages
12	Configure and manage NAT Rules from Central	<ul style="list-style-type: none"> • Filters • Dynamic objects to select Zones, Network interface, Host-System Hosts in SSL/TLS rules and apply this configurations on diff. Firewall devices together
13	Configure and manage SSL/TLS inspection rules from Central	<ul style="list-style-type: none"> • Dynamic objects to select Zones, Network interface, Host-System Hosts in SSL/TLS rules and apply this configurations on diff. Firewall devices together • Synchronized security applications selection in SSL/TLS rules
14	Configure and manage Certificates from Central	<ul style="list-style-type: none"> • Certificate Revocation Lists • Generate self-signed certificate • Generate certificate signing request (CSR)
15	Initiation of firewall management Migration to Firewall Group Management	<p>Supports only below functions as of now:</p> <ul style="list-style-type: none"> • Open Firewall from Central via RP-SSO • Accept firewall from Central for Central management • Connection and Config states
16	Configure and manage Wireless from Central	<ul style="list-style-type: none"> • Mesh Networks • Rogue SP Scan • Hotspots • Wireless Settings • Hotspot Settings

Firewall Group Management EAP1 Evaluation Guide

Feature List	Brief Introduction	Task List (Week1 to Week2)	Feedback	Worked (Y/N/Free Text)
Join to cloud of SFOS v18 Firewall device to Firewall Group Management	As an admin, you can now choose to enable "Central Management" option when registering an XG firewall with Central.	<p>Task: Register SFOS v18 with Central and enable Sophos Central services.</p> <p>We'd like you to explore the different options available under Sophos Central Services like:</p> <ul style="list-style-type: none"> • Enable Central management only • Enable Central Reporting only • Enable both • Disable one-by-one 	<ul style="list-style-type: none"> • Were you able to register the device to Central? • Were you able to enable/disable Central Management via Sophos Central services along with different combination options of Central reporting? • Did you see firewall devices connected in Central? • If not, what problems did you face? • Please provide additional feedback on the overall experience, considering ease of use, intuitiveness, configuration choice, etc. <free text field> 	

Notes:

Firewall Group Management EAP1 Evaluation Guide

Feature List	Brief Introduction	Task List (Week1 to Week2)	Feedback	Worked (Y/N/Free Text)
<p>Group based management of Firewall devices in Central</p>	<p>Now we have Group based management of Firewall devices in Firewall Group Management.</p> <p>As an admin, you can now configure group of firewalls as a single entity. To do so, you need to create a group, and then assign firewalls to this group</p>	<p>Task: We'd like you to explore the creation and management of Groups based on your requirements:</p> <p>add/update/delete groups.</p> <p>We would like you to explore the user experience of Firewall groups by Edit Group option against any group.</p> <p>Also explore Group based management by add/remove firewall devices from and to groups.</p>	<ul style="list-style-type: none"> • Were you able to create/update and delete groups according to your requirements? • Were you able to add/remove firewalls into groups and switch firewalls from one group to another group according to your requirements? • What problems and difficulties did you face? • Please provide feedback on the overall user experience of Firewall groups page, considering ease of use, intuitiveness, configuration choice, different options of Firewall groups page etc. <free text field> 	

Notes:

Firewall Group Management EAP1 Evaluation Guide

Feature List	Brief Introduction	Task List (Week1 to Week2)	Feedback	Worked (Y/N/Free Text)
<p>Configure and manage Web feature & policies from Central</p>	<p>This feature provides configuration of Web feature & policies on group of devices together from Central at one go.</p> <p>It allows Admin to configure different Firewall devices from Central by configuring Web</p> <ul style="list-style-type: none"> • Policies • User Activities • Categories • URL Group • Exceptions • File Type • Surfing Quota 	<p>Task: We'd like you to explore creation of different Web Policies like:</p> <ul style="list-style-type: none"> • Policies • User Activities • Categories • URL Group • Exceptions • File Type • Surfing Quota <p>Update & remove the above configured policies as per your need.</p>	<ul style="list-style-type: none"> • Were you able to configure these policies in different Firewall devices together? • Confirm from those Firewall devices, expected policies applied successfully or not? • Confirm from those Firewall devices, expected policies are updated & removed successfully or not? • What problems and difficulty did you face? • Please provide additional feedback on the overall experience, considering ease of use, intuitiveness, configuration choice, etc. <free text field> 	
<p>Notes:</p>				

Firewall Group Management EAP1 Evaluation Guide

Feature List	Brief Introduction	Task List (Week1 to Week2)	Feedback	Worked (Y/N/Free Text)
<p>Configure and manage Advanced Threat policies from Central</p>	<p>This feature provides configuration of Advance Threat feature & polices on group of devices together from Central at one go.</p> <p>It allows an admin to configure different Firewall devices from Central by configuring Advanced Threat policies like:</p> <ul style="list-style-type: none"> • Advanced Threat Protection • Sandstorm Settings 	<p>Task: We'd like you to explore creation of different Advanced Threat Policies like:</p> <ul style="list-style-type: none"> • Advanced Threat Protection • Sandstorm Settings <p>Update and remove the above configured policies as per your need.</p>	<ul style="list-style-type: none"> • Were you able to configure these policies in different Firewall devices together? • Confirm from those Firewall devices, expected policies are applied successfully or not? • Confirm from those Firewall devices, expected policies are updated & removed successfully or not? • What problems and difficulty did you face? • Please provide additional feedback on the overall experience, considering ease of use, intuitiveness, configuration choice, etc. <free text field> 	

Notes:

Firewall Group Management EAP1 Evaluation Guide

Feature List	Brief Introduction	Task List (Week1 to Week2)	Feedback	Worked (Y/N/Free Text)
<p>Configure and manage Authentication feature & policies from Central</p>	<p>This feature provides configuration of Authentication feature & policies on group of devices together from Central at one go.</p> <p>It allows Admin to configure his different Firewall devices from Central by configuring: Authentication</p> <ul style="list-style-type: none"> • Server • Services • Groups • Users • One-Time Password • Clientless Users • STAS • Guest User Settings 	<p>Task: We'd like you to explore creation of Authentication feature & policies like:</p> <ul style="list-style-type: none"> • Server • Services • Groups • Users • One-Time Password • Clientless Users • STAS • Guest User Settings <p>Update & remove above configured feature & policies as per your need.</p>	<ul style="list-style-type: none"> • Were you able to configure Authentication feature and policies in different Firewall devices together? • Confirm from those Firewall devices, expected configuration are applied successfully or not? • Confirm from those Firewall devices, expected policies are updated & removed successfully or not? • What problems and difficulty did you face? • Please provide additional feedback on the overall experience, considering ease of use, intuitiveness, configuration choice, etc. <free text field> 	

Notes:

Firewall Group Management EAP1 Evaluation Guide

Feature List	Brief Introduction	Task List (Week1 to Week2)	Feedback	Worked (Y/N/Free Text)
<p>Configure and manage Host sand Services from Central</p>	<p>This feature provides configuration of different types of Hosts and Services on group of devices together from Central at one go. It allows Admin to configure his different Firewall devices from Central by configuring: Host and Services</p> <ul style="list-style-type: none"> • IP Host • IP Host Group • MAC Host • FQDN Host • FQDN Host Group • Country • Country Group • Services • Service Group 	<p><u>Task:</u> We'd like you to explore creation of different hosts and services:</p> <ul style="list-style-type: none"> • IP Host • IP Host Group • MAC Host • FQDN Host • FQDN Host Group • Country • Country Group • Services • Service Group <p>Update & remove above configured feature & policies as per your need.</p>	<ul style="list-style-type: none"> • Were you able to configure Host and Services in different Firewall devices together? • Confirm from those Firewall devices, expected configuration are applied successfully or not? • Confirm from those Firewall devices, expected policies are updated & removed successfully or not? • What problems and difficulty did you face? • Please provide additional feedback on the overall experience, considering ease of use, intuitiveness, configuration choice, etc. <free text field> 	

Notes:

Firewall Group Management EAP1 Evaluation Guide

Feature List	Brief Introduction	Task List (Week1 to Week2)	Feedback	Worked (Y/N/Free Text)
<p>Configure and manage System Services from Central</p>	<p>This feature provides configuration of different types of System services on group of devices together from Central at one go.</p> <p>Admin can use System services to configure below functionalities on different Firewall devices from Central</p> <ul style="list-style-type: none"> • Traffic Shaping Settings • Malware Protection • Traffic Shaping policies 	<p>Task: We'd like you to configure</p> <ul style="list-style-type: none"> • Traffic Shaping Settings • Malware Protection • Traffic Shaping policies <p>as per your business need from Central.</p> <p>Update/Remove, Set/Unset and Disable/Enable above configured functionalities based on your requirement.</p>	<ul style="list-style-type: none"> • Were you able to configure and set different System services like Traffic Shaping Settings, Malware protection, Traffic Shaping policies in different Firewall devices together? • Confirm from those Firewall devices, expected System services like Traffic Shaping Settings, Malware Protection, Traffic Shaping policies are configured and enabled successfully or not? • What problems and difficulty did you face? • Please provide additional feedback on the overall experience, considering ease of use, intuitiveness, configuration choice, etc. <free text field> 	

Notes:

Firewall Group Management EAP1 Evaluation Guide

Feature List	Brief Introduction	Task List (Week1 to Week2)	Feedback	Worked (Y/N/Free Text)
Connection and Config States	<p>With this feature, admin would know about the firewall's connection and configuration states in Central</p> <p>Connection States:</p> <ul style="list-style-type: none"> • Connected: It suggests that firewall is sending heartbeats to Central • Disconnected: It suggests that firewall's heartbeat is not coming to Central • Suspended: It suggests that firewall is disconnected since last 30 days <p>Configuration States:</p> <ul style="list-style-type: none"> • Synchronized: When firewall group configuration is synchronized with firewall • Synchronizing: When firewall group configuration is synchronizing in firewall, firewall executing the opcodes • Error needs attention: When any group configuration is failed to apply in firewall. 	<p>Task: We'd like you to see different Connection and Configuration States of Firewall devices while different actions performed on Firewall devices.</p> <p>We'd like you to explore below scenarios</p> <ul style="list-style-type: none"> • Register the firewall with central, add into Firewall group and observe connection state • Disconnect firewall device from central and observe connection state. • Apply correct configurations, apply wrong configurations and then correct that configurations and observe that all firewalls belong to one firewall group should be synchronised. • Add/remove firewalls into the firewall group • Switch device to another group • Reboot/Shutdown the Firewall device 	<ul style="list-style-type: none"> • Were you able to connect your firewall in Central, add into the firewall group and synchronised with firewall group configurations ? • Did you see expected States while different actions are performed at Firewall group level. • Was it easy to understand the different States of Firewall devices? • What problems and difficulty did you face while looking into the States? • Please provide additional feedback on the overall experience, considering ease of use, intuitiveness, configuration choice, etc. <free text field> 	

Notes:

Firewall Group Management EAP1 Evaluation Guide

Feature List	Brief Introduction	Task List (Week1 to Week2)	Feedback	Worked (Y/N/Free Text)
<p>Tasks Queue Verify the transactions status in Task queue and perform actions if needed.</p>	<p>This feature provides to see whether the configuration is applied in all firewall devices or not.</p> <p>We will find the transaction as below:</p> <ul style="list-style-type: none"> • Pending: It suggests that configuration is saved in firewall group and opcode generated but it is not yet fetched by firewall. • InProgress: It suggests that firewall fetched the configuration and executing it. • Success: It suggests that firewall successfully applied the group configurations • Failed: It suggests that firewall is failed to apply the group configuration. <p>Actions on Failed Transaction:</p> <ul style="list-style-type: none"> • Retry: Analyze the failure and retry with same configuration. • Skip: Analyze the failure and skip the failed configuration 	<p>Task: We'd like you to apply different configurations on groups of Firewall devices and see success and failed transactions.</p> <p>We'd like you to explore to do group configurations and see whether it applied in firewall or not.</p> <p>In case your configuration is failed in firewall. Are you able to retrieve the error reason from failed transaction in Task Queue. If yes, then we are good.</p> <p>You can also perform the actions, analyse your error from task queue, fix it then retry the same operation or you can skip that configuration and continue.</p>	<ul style="list-style-type: none"> • Were you able to apply different configurations on groups of Firewall devices and see success and failed transactions? • Were you able to see success & failed transactions and able to retried failed transactions? • What problems and difficulty did you face? • Please provide additional feedback on the overall experience, considering ease of use, intuitiveness, configuration choice, etc. <free text field> 	
<p>Notes:</p>				

Firewall Group Management EAP1 Evaluation Guide

Feature List	Brief Introduction	Task List (Week1 to Week2)	Feedback	Worked (Y/N/Free Text)
<p>Configure and manage Firewall Rules and Policies from Central</p>	<p>This feature provides configuration of Rules & Policies on group of devices together from Central at one go.</p> <p>It allows Admin to configure different Firewall devices from Central by configuring Rules and Policies</p> <ul style="list-style-type: none"> • Add Firewall Rule • Edit Firewall Rule • Delete Firewall Rule • Enable/Disable Firewall Rule (On/Off) • Add rule Above/Below • Clone Rule Above/Below 	<p>Task: On group of Firewall devices from Central, we'd like you to configure firewall Rules and Policies.</p> <p>Do this operations on configured Firewall rules based on your requirement</p> <ul style="list-style-type: none"> • Edit/Delete • Disable/Enable • Add rule Above/Below • Clone rule Above/Below 	<ul style="list-style-type: none"> • Were you able to configure Firewall Rules and Policies in different Firewall devices together? • Were you able to Enable/Disable, Edit/Delete and Clone Firewall Rules in different Firewall devices together? • Confirm from those Firewall devices, expected Firewall rules configured successfully • Confirm from those Firewall devices expected Firewall rules Enabled/Disable, Edit/Delete and Cloned successfully • What problems and difficulty did you face? • Please provide additional feedback on the overall experience, considering ease of use, intuitiveness, configuration choice, etc. <free text field> 	

Notes:

Firewall Group Management EAP1 Evaluation Guide

Feature List	Brief Introduction	Task List (Week1 to Week2)	Feedback	Worked (Y/N/Free Text)
<p>Configure and manage NAT rules from Central</p>	<p>This feature provides configuration of NAT rules on group of devices together from Central at one go.</p> <p>It allows Admin to configure different Firewall devices from Central by configuring NAT</p> <ul style="list-style-type: none"> • Add NAT Rule • Edit NAT Rule • Delete NAT Rule • Enable/Disable NAT Rule (On/Off) • Add rule Above/Below 	<p>Task: On group of Firewall devices together, we'd like you to configure the firewall rules along with the new NAT policies.</p> <p>Do this operations on above configured NAT rules</p> <ul style="list-style-type: none"> • Edit NAT Rule • Delete NAT Rule • Enable/Disable NAT Rule (On/Off) • Add rule Above/Below 	<ul style="list-style-type: none"> • Were you able to configure NAT rules in different Firewall devices together? • Were you able to Edit/Delete and Enable/Disable NAT rules in different Firewall devices together? • Confirm from those Firewall devices, expected NAT rules configured successfully • Confirm from those Firewall devices, expected NAT rules Edit/Delete and Enable/Disable successfully. • What problems and difficulty did you face? • Please provide additional feedback on the overall experience, considering ease of use, intuitiveness, configuration choice, etc. <free text field> 	

Notes:

Firewall Group Management EAP1 Evaluation Guide

Feature List	Brief Introduction	Task List (Week1 to Week2)	Feedback	Worked (Y/N/Free Text)
<p>Configure and manage SSL/TLS inspection rules from Central</p>	<p>With this feature, an admin can enable and configure below SSL/TLS inspection rules on group of devices together from Central at one go</p> <p>It allows Admin to configure different Firewall devices from Central by configuring</p> <ul style="list-style-type: none"> • SSL/TLS inspection rules • SSL/TLS inspection settings 	<p>Task: On group of Firewall devices together from Central, we'd like you to explore</p> <ul style="list-style-type: none"> • SL/TLS inspection rules • SSL/TLS inspection settings. <p>Do this operation on above configured SSL/TLS rules</p> <ul style="list-style-type: none"> • Edit/Delete • On/Off • Add rule Above/Below • Clone Rule Above/Below 	<ul style="list-style-type: none"> • Were you able to configure SSL/TLS inspection rules in different Firewall devices together? • Were you able to Edit/Delete, On/Off and Clone SSL/TLS rules in different Firewall devices together? • Confirm from those Firewall devices, expected SSL/TLS inspection rules configured successfully • Confirm from those Firewall devices, expected SSL/TLS inspection rules Edit/Delete, On/Off and Clone successfully • What problems and difficulty did you face? • Please provide additional feedback on the overall experience, considering ease of use, intuitiveness, configuration choice, etc. <free text field> 	

Notes:

Firewall Group Management EAP1 Evaluation Guide

Feature List	Brief Introduction	Task List (Week1 to Week2)	Feedback	Worked (Y/N/Free Text)
<p>Configure and manage Certificates from Central</p>	<p>This feature provides configuration of Certificates on group of devices together from Central at one go.</p> <p>It allows Admin to configure his different Firewall devices from Central by configuring: Certificates</p> <ul style="list-style-type: none"> • Certificate • Certificate authority 	<p>Task: We'd like you to explore and upload new certificate and CA's:</p> <ul style="list-style-type: none"> • Certificate • Certificate authority <p>Upload valid/invalid certificate, delete the certificate at group level.</p>	<ul style="list-style-type: none"> • Were you able to upload valid Certificate and Certificate Authority in different Firewall devices together? • Were you able to update/remove Certificate and Certificate Authority in different Firewall devices together? • Confirm from those Firewall devices, expected Certificate and Certificate Authority update/remove successfully 	
<p>firewall management Migration to Firewall Group Management</p>	<p>If you are existing user of firewall management and managing your firewalls in Central, then now you can manage the firewalls in Group also.</p> <p>All the firewalls which is listed in Firewall Page will come under in Ungrouped section at Firewall Groups page</p>	<p>We'd like you to explore working of below firewall management functionalities in Firewall Group page:</p> <ul style="list-style-type: none"> • Open Firewall from Central via RP-SSO • Accept Services • Remove firewall from Central 	<ul style="list-style-type: none"> • Confirm firewall management Firewalls functionalities are working properly in Firewall Group Management Firewall groups as well? • Did you face any difficulty in using existing firewall management functionalities in Firewall Group Management Firewall groups • Please provide additional feedback on the overall experience, considering ease of use, intuitiveness, configuration choice, etc. <free text field> 	

Notes:

Firewall Group Management EAP1 Evaluation Guide

Feature List	Brief Introduction	Task List (Week1 to Week2)	Feedback	Worked (Y/N/Free Text)
<p>Configure and manage Wireless from Central</p>	<p>This feature provides configuration of Wireless on group of devices together from Central at one go.</p> <p>It allows Admin to configure his different Firewall devices from Central by configuring:</p> <p>Wireless</p> <ul style="list-style-type: none"> • Wireless Networks • Access Point Groups • Hotspots • Hotspot Voucher Definition • Wireless Settings • Hotspot Settings 	<p>Task: We'd like you to explore and configure different Wireless configurations:</p> <ul style="list-style-type: none"> • Wireless Networks • Access Point Groups • Hotspots • Hotspot Voucher Definition • Wireless Settings • Hotspot Settings <p>Update/Remove wireless configurations based on your requirement on group</p>	<ul style="list-style-type: none"> • Were you able to configure Wireless Networks, Access Point Groups, Hotspot Voucher Definition in different Firewall devices together? • Were you able to update/remove Wireless Networks, Access Point Groups, Hotspot Voucher Definition in different Firewall devices together? • Verify in Firewall, whether your configuration is successfully pushed or not? • What problems and difficulty did you face? • Please provide additional feedback on the overall experience, considering ease of use, intuitiveness, configuration choice, etc. <free text field> 	

Notes:

SOPHOS
Security made simple.