Addendum to Product Guide

McAfee® Firewall Enterprise Control Center

version 5.2.1

LICENSE INFORMATION

License Agreement
NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANTOR PURCHASE ORDER DOCUMENTS THAT ACCOMPANIES YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

License Attributions
For license attributions, access the McAfee® Firewall Enterprise Control Center Management Server from the command line, enter the following command, then press **Y** at the prompt. (To scroll, press **Page Down**. To quit, press **Q**.)

```
less /usr/share/doc/ControlCenter/LICENSE.txt
```

Contents

Contents

About this guide

This addendum explains the new features and enhancements included in McAfee® Firewall Enterprise Control Center (hereinafter Control Center) version 5.2.1. Use this addendum to supplement the information in the *McAfee Firewall Enterprise Control Center Product Guide*, version 5.2.0.

Conventions

The following text conventions are used in this guide.

Table i-1 Conventions

Convention	Description
Monotype bold	Identifies commands and key words that you type at a system prompt. Note: A backslash (\) indicates a command that does not fit on the same line. Type the command as shown, ignoring the backslash.
<placeholder> *nnn.nnn.nnn.nnn*	Indicates a placeholder for text that you specify. Indicates a placeholder for an IP address that you specify.
Monotype plain	Indicates text that is displayed on a computer screen.
Plain text italic	Indicates the names of files and directories. Also used for emphasis (for example, when introducing a new term)
Plain text bold	Identifies buttons, field names, and tabs that require user interaction
[ ]	Indicates conditional or optional text and instructions (for example, instructions that pertain only to a specific configuration).
Caution:	Indicates that you must be careful. In this situation, you might do something that might result in the loss of data or in an unpredictable outcome.
Note:	Indicates a helpful suggestion or a reference to material that is not covered elsewhere in this documentation.
Security Alert:	Indicates information that is critical for maintaining product integrity or security.
Tip:	Indicates time-saving actions. It might also help you solve a problem.

Note: The IP addresses, screen captures, and graphics used within this document are for illustration purposes only. They are not intended to represent a complete or appropriate configuration for your specific needs. Features might be enabled in screen captures to make them clear; however, not all features are appropriate or desirable for your setup.

Find product information

You can find additional information at the following locations.

Table i-2 Locations of product information

Information	Location
User documentation	**1** Go to the McAfee Technical Support ServicePortal at mysupport.mcafee.com. **2** Under **Self Service**, click **Product Documentation**. **3** Select a **Product**, then select a **Version**. **4** Select a product document.
KnowledgeBase	Go to the McAfee Technical Support ServicePortal at mysupport.mcafee.com. • Click **Search the KnowledgeBase** for answers to your product questions. • Click **Browse the KnowledgeBase** for articles listed by product and version.
Help	Help is built into Control Center Client application programs and the Control Center Initialization Tool. Click the Help icon in the title bar of the main window or press **F1** to access context-sensitive Help.
Product updates	Visit go.mcafee.com/goto/updates to download the latest McAfee Firewall Enterprise Control Center patches.

1 ePolicy Orchestrator and managed firewalls

McAfee® Firewall Enterprise Control Center version 5.2.1 supports McAfee® Firewall Enterprise ePolicy Orchestrator® Extension version 5.2.1. You can use Control Center to configure managed firewalls so that firewall details can be viewed in ePolicy Orchestrator dashboards.

Contents

Using ePolicy Orchestrator to monitor firewalls

ePolicy Orchestrator is a management platform that enables centralized policy management and enforcement of your security products and the systems on which they reside. ePolicy Orchestrator uses firewall data to more accurately assess the risk levels of the traffic flowing through your network. With insight into the risk-level of the traffic on your network, you can tailor your policy to limit or eliminate traffic that might be carrying viruses, spyware, or malware.

See the *McAfee Firewall Enterprise ePolicy Orchestrator Extension Integration Guide*, version 5.2.1 for instructions on installing and configuring the extension.

Configure managed firewalls for ePolicy Orchestrator reporting

Use the Control Center Client application to set up a managed firewall to pass information to ePolicy Orchestrator.

Note: Only firewalls at version 8.2.1 and later can be configured to send information directly to ePolicy Orchestrator.

1 Create an ePolicy Orchestrator settings object.

   a From the Control Center Client application, click **Policy**. The Policy icon page appears.

   b On the Firewall Settings tab, right-click **ePolicy Orchestrator**, then select **Add Object**. The ePolicy Orchestrator window appears.

   c Enter a name and description for the ePolicy Orchestrator settings object.

   d Select **Enabled**.

   e Enter the IP address of the ePolicy Orchestrator server.

   f Enter the user name and password used to communicate with the ePolicy Orchestrator server.

   g Click **Retrieve ePO root certificate**. The ePolicy Orchestrator root certificate is added to and selected in the CA certificate list.

   h Click **OK**.

   The new ePolicy Orchestrator settings object appears on the Firewall Settings tab under the ePolicy Orchestrator node.

2 Apply the ePolicy Orchestrator settings object to a managed firewall.

   a In the Policy area, double-click the firewall. The Firewall window appears.

   b Click **Offbox**. The Offbox area appears.

   c In the ePolicy Orchestrator section, from the Configuration drop-down list, select the ePolicy Orchestrator settings object you created in step 1.

   d Click **OK**. The Firewall window closes.

   e Click **Apply**. The Apply Configuration window appears.

   f Select the firewall, then click **OK**. The ePolicy Orchestrator settings are applied to the firewall.

The firewall sends information to the ePolicy Orchestrator server. Firewall details can be viewed on ePolicy Orchestrator dashboards.

ePolicy Orchestrator window

Use this window to create an ePolicy Orchestrator settings object to apply to managed firewalls.

Option	Definition
Name	Specifies a name for the ePolicy Orchestrator server settings object.
Description	Provides additional information about the ePolicy Orchestrator settings object.
Enabled	Allows the firewall to send information to the ePolicy Orchestrator server.
IP address	Specifies the ePolicy Orchestrator server IP address.
Username	Specifies the user name required for ePolicy Orchestrator server access.
Password	Specifies the ePolicy Orchestrator server password.
Confirm password	Confirms the ePolicy Orchestrator server password.
CA certificate	Specifies the CA certificate to use to authenticate to the ePolicy Orchestrator server.
Edit	Opens the CA Certificate Details window for the selected certificate.
Add	Opens the CA Certificate Import wizard.
Retrieve ePO root certificate	Adds the ePolicy Orchestrator server certificate to the CA certificate drop-down list. The ePolicy Orchestrator server certificate is selected in the lit.
OK	Closes the window and saves your changes. New ePolicy Orchestrator settings objects appear beneath the ePolicy Orchestrator node.
Cancel	Closes the window and discards your changes.

2 Dynamic routing on Crossbeam X-Series Platforms

McAfee® Firewall Enterprise Control Center version 5.2.1 supports dynamic routing for managed firewalls on Crossbeam X-Series platforms.

Contents

Benefits of dynamic routing

Dynamic routing protocols facilitate the exchange of routing information between routers. Routers acquire the network topology by communicating and updating the routing tables accordingly.

The benefits of dynamic routing include the following:

- You do not have to manually configure and maintain routing information.
- The network can quickly adapt to changes such as the addition, removal, or failure of network devices.

Network performance improves because routers select the best path for connections between network devices.

See the *McAfee Firewall Enterprise Product Guide* for more information about dynamic routing.

Configure dynamic routing for firewalls on Crossbeam X-Series Platforms

Modify the dynamic routing configuration file from the Control Center Client application.

Note: Editing configuration files associated with dynamic routing protocols and applications requires advanced knowledge.

1. In the navigation bar, click **Policy**.
2. In the Firewalls tree, click the **Firewalls** node. Double-click the firewall to configure dynamic routing for. The Firewall window is displayed.
3. In the tree on the left, click **Dynamic Routing**. The Dynamic Routing area is displayed.

   Tip: For option descriptions, press **F1**.
4. From the drop-down list, select the appropriate dynamic routing configuration file. The configuration file appears.
5. Modify the configuration file as needed.
6. Click **OK**.

The configuration file is updated the next time you apply changes to the firewall.

3 Client application windows

This release simplifies the configuration of cluster interfaces, static routes, and host and adaptive endpoints, and improves the dashboard for members of High Availability (HA) pairs.

Contents

Cluster window

The Cluster window contains updates. Use this window to configure cluster-specific settings for the selected cluster object.

General area (Cluster window)

Use the General area to specify cluster parameters such as the management IP address, management port, and cluster properties.

Option	Definition
Cluster Name	Specifies the name of the cluster as it appears in the list of clusters in the Clusters node of the Policy tree.
Description	Specifies a description about the cluster.
Firewall Management Address	
Node	Displays the cluster node.
Address	Specifies the IP address or host name of the network interface on the firewall that the Control Center uses to manage the cluster.
Port	Specifies the port number the cluster uses to communicate with the Control Center. The value in this field must match the value on the cluster by using its native user interface. If you change the value on this window and apply the change, it does not change the value on the cluster. The default management port is 9005.
Configuration	
Version	[Read-only] Displays the version of software that is installed on the cluster.
Time Zone	Specifies the time zone where the cluster is located.
Location	Specifies user-defined location information.

Option	Definition
Contact	Specifies contact information for the cluster. The administrator email address will be displayed in this field. This is the email address that was configured on and retrieved from the firewall. Note: If you are using Control Center to manage sendmail files, this email address will be used to define the alias for the root user in the firewall sendmail aliases file.
Enable IPv6	[Read-only; firewall clusters on X-series Platforms at version 8.1.2 and earlier] When selected, IPv6 is enabled on the cluster.
Mail Configuration	
SMTP Mode	Specifies settings for the cluster's mail configuration. The following options are available: • **Secure Split SMTP** — When selected, the firewall-hosted sendmail servers are used. If selected, you can take advantage of such sendmail features as header stripping, spam and fraud control, and mail routing. • **Transparent** — When selected, mail is passed by proxy through the firewall. If selected, only the files that are necessary to send administrative messages will be configured. These include firewall-generated alerts, messages, and logs.
Internal SMTP Zone	Specifies the zone that your site's SMTP server resides in.
Management Servers	

Management Servers table	Lists Control Center Management Servers. The following columns are available:
	• *Edit* — Identifies the edit status of the row in the table. The following icons can be displayed:
	  • **Pencil** — Indicates that this row is the one that is being edited.
	  • **Right-arrow** — Indicates that this row is currently selected and it contains previously specified values.
	• **Host Name** — [Read-only] Displays the fully qualified host name of the Management Server.
	• **IP address** — Specifies the IP address of the Management Server.
	Note: Specify the IP address that the firewall uses to reach the Management Server. It might be different from the IP address that is configured for the server if there is a NAT device between the firewall and the server.

Firewall Properties	

Category/Value table	Lists the category or value pairs for sorting clusters.
	Use these categories and values to create cluster views on the Firewall Sorting window. The following columns are available:
	• *Edit* — Identifies the edit status of the row in the table. The following icons can be displayed:
	  • **Blank** — Indicates an existing line with associated values that is not the currently selected line.
	  • **Pencil** — Indicates that this row is the one that is being edited.
	  • **Asterisk (*)** — Indicates that you are creating a new row or entry.
	  • **Right-arrow** — Indicates that this row is currently selected and it contains previously specified values.
	• **Category** — Specifies a name for the category.
	• **Value** — Specifies a value for the category.

Appliance Address	
Hostname/IP address	[Available for clusters on X-Series Platforms only] Specifies the host name or IP address of the firewall cluster on X-Series Platform. It is also known as the Control Processor Module (CPM), where configuration occurs on the firewalls on X-Series Platforms. This value will then be used as the value to launch the Launch UI page. Note: You must configure the SSH connection in the Secure Shell window to access this page.

High Availability area (Cluster window)

Use this area to configure High Availability settings.

Option	Definition
High Availability Idenitifcation	
Cluster ID	Specifies the cluster ID.
Multicast Group Address	Specifies the multicast group address.
Heartbeat zone	Specifies the zone for heartbeat communications.
Heartbeat verification zone	Specifies an optional backup heartbeat zone.
HA Status	
HA Node	Displays the cluster node.
Status	Displays the status of the cluster node.
Refresh	Refreshes the HA status.
Status area	Displays Control Center progress for determining HA status.
IPsec Authentication	
Password	Specifies the password for IPsec authentication.
Interface Test	
Auto-Recover on Reconnect	When selected, a firewall is automatically rejoined to an HA cluster if a monitored interface or a heartbeat interface fails and recovers.
Type	
Cluster Type	Specifies the cluster type: • Primary/Standby • Load-sharing • Peer to Peer • [X-Series Platforms only] Load Balancing
Cluster Primary	Specifies which cluster node is the primary. Note: This can only be modified when the cluster type is Primary/Standby. For all other High Availability types, this option is read-only.
Cluster Takeover Time	Specifies the time the secondary will wait before initiating a failover.

Interfaces area (Cluster window)

Use this area to modify cluster IP addresses, NICs, and NIC groups.

Note: As of Control Center 5.2.1, all firewall IP addresses can be configured in the same window.

Tab	Description
Cluster Interfaces	Use the Cluster Interfaces tab to modify interface settings.
NICs/NIC Groups	Use the NICs/NIC Groups tab to modify NIC and NIC Group settings.

Cluster Interfaces tab (Interfaces area)

Use this tab to add or modify interfaces.

Option	Definition
Add	Opens the Interface Properties window.
Modify	Opens the Interface Properties window for the selected interface.
Delete	Removes the selected interface.
Find field	Searches for a specific element in the list of interfaces.
Name	Displays the interface name.
Zone	Displays the zone the interface resides in.
Addresses	Displays the IP addresses assigned to that interface.
Summary area	Displays all information for the selected interface in list form.

See also

Interface Properties tab (Interface Properties window)

Advanced tab (Interface Properties window)

NICs/NIC Groups tab (Interfaces area)

Use this tab to configure NICs and NIC groups.

Option	Definition
Node	Specifies the firewall node to configure.
NICs	
Name	Displays the name of the NIC.
MAC Address	Displays the MAC address of the NIC.
Speed Mode	Specifies the speed and duplex settings.
Capabilities	Enables media capabilities: • rxcsum • txcsum • jumbo_mtu
Description	Modifies the description of the NIC.
NIC Groups	
Add	Opens the NIC Group window.
Modify	Opens the NIC Group window for the selected NIC group.
Delete	Removes the selected NIC group.
Name	Displays the name of the NIC group.
NICs	Displays the member NICs in the group.
Type	Displays the NIC group type.
Description	Displays the description of the NIC group.

See also

NIC Group window (NICs/NIC Groups tab)

NIC Group window (NICs/NIC Groups tab)

Use this window to configure aggregate and redundant NIC groups.

Option	Definition
Name	Displays the name of the NIC group.
NIC group type	Specifies whether the group is an aggregate or redundant group.
Description	Modifies the description of the NIC group.
Available NICs	Displays the list of available NICs.
Selected NICs	Displays the list of NICs currently in the group.
Move Right	Moves a NIC from the Available NICs column to the Selected NICs column.
Move Left	Moves a NIC from the Selected NICs column to the Available NICs column.
Move Up	Moves a NIC up in the Selected NICs column.
Move Down	Moves a NIC down in the Selected NICs column.

Interface Properties window for clusters

The Interface Properties window contains updates. Use this window to configure interface properties such as IP addresses, zones, and interface monitoring.

Interface Properties tab (Interface Properties window)

Use this tab to configure interface and IP address settings.

Option	Definition
Interface Name	Defines the interface name.
Description	Adds a description to the interface.
NIC or NIC Groups	
Enabled	Enables the interface.
Cluster Node	Displays the cluster node.
NIC	Specifies the NIC or NIC group to use.
VLAN	Specifies whether the interface is standard or VLAN.
VLAN ID	Specifies the VLAN ID.
MTU Size	Selects the MTU size in bytes: • Standard (1500) • Jumbo (9000) Note: Jumbo can only be selected when the jumbo_mtu capability is enabled on the NIC or all members of the NIC group. • Custom(576-9000) Note: If the jumbo_mtu capability is not enabled, the maximum size that can be selected is 1500. If IPv6 is enabled, the minimum size that can be selected is 1280.
Address Configuration	
Zone	Selects the zone to associate with the interface.
Edit	Opens the Zones window for the selected zone.
Add	Opens the Zones window.
Obtain IPv4 address automatically via DHCP	Determines if the interface's IP address will be assigned using DHCP. Note: This option is disabled for clusters.
Enable IPv6	Enables IPv6. Note: For clusters at 8.1.x or lower, this option is read-only and cannot be configured.
IPv6 stateless auto address configuration	Specifies whether Static or Router mode is used when IPv6 is enabled.

Option	Definition
IPv4 Addresses	
Add	Opens the Interface Address window.
Modify	Opens the Interface Address window for the selected address.
Delete	Removes an IPv4 address.
Move Up	Moves an IPv4 address up in the list.
Move Down	Moves an IPv4 address down in the list.
Find field	Searches for a specific element in the list of IPv4 addresses.
Node	Displays the node. Double-clicking opens the Interface Address window for the selected interface.
Address	Specifies the IPv4 addresses.
Mask	Specifies the masks for the IPv4 addresses.
IPv6 Addresses	
Add	Opens the Interface Address window.
Modify	Opens the Interface Address window for the selected address.
Delete	Removes the selected interface.
Move Up	Moves an IPv6 address up in the list.
Move Down	Moves an IPv6 address down in the list.
Find field	Searches for a specific element in the list of IPv6 addresses.
Node	Displays the node. Double-clicking opens the Interface Address window for the selected interface.
Address	Specifies the IPv6 addresses.
Prefix	Specifies the prefixes for the IPv6 addresses.
Quality of Service (QoS) Profile	
Quality of Service (QoS) Profile	Specifies the Quality of Service profile to use.
Modify	Opens the Quality of Service window for the selected profile.
Add	Opens the Quality of Service window.

See Also

Interface Address window for IPv4 addresses

Interface Address window for IPv6 addresses

Interface Address window for IPv4 addresses

Use this window to add or modify IPv4 addresses.

Option	Definition
Node	Specifies the cluster node.
Address	Specifies the address.
Mask	Specifies the mask.

Interface Address window for IPv6 addresses

Use this window to add or modify IPv6 addresses.

Option	Definition
Node	Specifies the cluster node.
Address	Specifies the address.
Prefix	Specifies the prefix.

Advanced tab (Interface Properties window)

Use this tab to configure interface monitoring and advanced High Availability interface options.

Option	Definition
Interface IDs	
Override	Allows the interface ID to be modified manually.
Member	Displays the cluster node.
Interface ID	Specifies the interface ID.
Interface test	
Monitor link status	Detects if the interface has link.
Add	Adds a remote ping test address.
Delete	Deletes a remote ping test address.
Ping interval	Specifies the amount of time to perform a remote ping test.
Failures allowed	Specifies the number of remote ping test failures allowed.
Force ARP reset	
Add	Add an address to ping during a failover. Note: Force ARP reset is not available for Load-sharing clusters.
Delete	Removes an address to ping during a failover.
Load sharing parameters	
L2 Mode	[Load-sharing only] Specifies the layer 2 mode: • Multicast no IGMP • Unicast - Mirrored • Unicast - Flooded
Cluster MAC	[Load-sharing only] Specifies the shared cluster MAC address.
Force NDP reset	
Add	Adds an address to reissue Neighbor Detection Protocol (NDP) commands. Note: Force NDP reset is only available when IPv6 is enabled. This option is not available for Load-sharing clusters.
Delete	Removes an address to reissue NDP commands.
Float addresses	
Add	[Firewalls on Crossbeam X-Series Platforms only] Adds a float address.
Delete	[Firewalls on Crossbeam X-Series Platforms only] Removes a float address.

Firewall window

The Firewall window contains updates. Use this window to configure firewall-specific settings for the selected firewall object.

General area (Firewall window)

Use the General area to specify firewall parameters such as the management IP address, management port, and firewall properties.

Option	Definition
Name	Specifies the name of the firewall object as it appears in the list of firewalls in the Firewalls tree.
Description	Specifies a description about the firewall.
Node Name	[Read-only] Displays the host name by which the system identifies itself during network and logon connections.
Firewall Management Address	

Option	Definition
Address	Specifies the IP address or host name of the network interface on the firewall that the Control Center uses to manage the firewall.
Port	Specifies the port number the firewall uses to communicate with the Control Center. The value in this field must match the value on the firewall by using its native user interface. If you change the value on this window and apply the change, it does not change the value on the firewall. The default management port is 9005.
Configuration	
Version	[Read-only] Displays the version of software installed on the firewall.
Time Zone	Specifies the time zone where the firewall is located.
Location	Specifies user-defined location information.
Contact	Specifies the contact information for the firewall. The administrator email address will be displayed in this field. This is the email address that was configured on and retrieved from the firewall. Note: If you are using Control Center to manage sendmail files, this email address will be used to define the alias for the root user in the firewall sendmail aliases file.
Enable IPv6	[Firewall versions 8.1.x and earlier] Enables IPv6 on the firewall.
Mail Configuration	
SMTP Mode	Specifies settings for the firewall's mail configuration. The following options are available: • **Secure Split SMTP** — When selected, the firewall-hosted sendmail servers are used. If selected, you can take advantage of such sendmail features as header stripping, spam and fraud control, and mail routing. • **Transparent** — When selected, mail is passed by proxy through the firewall. If selected, only the files that are necessary to send administrative messages will be configured. These include firewall-generated alerts, messages, and logs.
Internal SMTP Zone	Specifies the zone that your site's SMTP server resides in.
Management Servers	

Management Servers table	Lists Control Center Management Servers. The following columns are available:
	• *Edit* — Identifies the edit status of the row in the table. The following icons can be displayed:
	  • **Pencil** — Indicates that this row is the one that is being edited.
	  • **Right-arrow** — Indicates that this row is currently selected and it contains previously specified values.
	• **Host Name** — [Read-only] Displays the fully qualified host name of the Management Server.
	• **IP address** — Specifies the IP address of the Management Server.
	Note: Specify the IP address that the firewall uses to reach the Management Server. It might be different from the IP address that is configured for the server if there is a NAT device between the firewall and the server.

Firewall Properties	

Category/Value table	Lists the category or value pairs for sorting firewalls.
	Use categories to create firewall views on the Firewall Sorting window. The following columns are available:
	• *Edit* — Identifies the edit status of the row in the table. The following icons can be displayed:
	  • **Blank** — Indicates an existing line with associated values that is not the currently selected line.
	  • **Pencil** — Indicates that this row is the one that is being edited.
	  • **Asterisk (*)** — Indicates that you are creating a new row or entry.
	  • **Right-arrow** — Indicates that this row is currently selected and it contains previously specified values.
	• **Category** — Specifies a name for the category.
	• **Value** — Specifies a value for the category.

Interfaces area (Firewall window)

Use this area to modify cluster and firewall IP addresses, NICs, and NIC groups.

Tab	Description
Firewall Interfaces	Use the Firewall Interfaces tab to modify interface settings.
NICs/NIC Groups	Use the NICs/NIC Groups tab to modify NIC and NIC Group settings.

Firewall Interfaces tab (Interfaces area)

Use this tab to add or modify interfaces.

Option	Definition
Add	Adds a standard or transparent interface, then opens the Interface Properties window.
Modify	Opens the Interface properties window for the selected interface.
Delete	Removes the selected interface.
Find field	Searches for a specific element in the list of interfaces.
Name	Displays the interface name.
Zone	Displays the zone the interface resides in.
NIC/NIC Group	Displays the NIC or NIC group the interface uses.
VLAN	Displays the VLAN ID if applicable.
Addresses	Displays the IP addresses assigned to that interface.
Summary area	Displays all information for the selected interface in list form.

See also

Interface Properties tab (Interface Properties window) for standard interfaces

Interface Properties tab (Interface Properties window) for transparent parent interfaces

Advanced tab (Interface Properties window) for standard interfaces

Advanced tab (Interface Properties window) for transparent interfaces

NICs/NIC Groups tab (Interfaces area)

Use this tab to configure NICs and NIC groups.

Option	Definition
NICs	
Name	Displays the name of the NIC.
MAC Address	Displays the MAC address of the NIC.
Speed Mode	Specifies the speed and duplex settings.
Capabilities	Enables media capabilities: • rxcsum • txcsum • jumbo_mtu
Description	Modifies the description of the NIC.
NIC Groups	
Add	Opens the NIC Group window.
Modify	Opens the NIC Group window for the selected NIC group.
Delete	Removes the selected NIC group.
Name	Displays the name of the NIC group.
NICs	Displays the member NICs in the group.
Type	Displays the NIC group type.
Description	Displays the description of the NIC group.

See also

NIC Group window (NICs/NIC Groups tab)

NIC Group window (NICs/NIC Groups tab)

Use this window to configure aggregate and redundant NIC groups.

Option	Definition
Name	Displays the name of the NIC group.
NIC group type	Specifies whether the group is an aggregate or redundant group.
Description	Modifies the description of the NIC group.
Available NICs	Displays the list of available NICs.
Selected NICs	Displays the list of NICs currently in the group.
Move Right	Moves a NIC from the Available NICs column to the Selected NICs column.
Move Left	Moves a NIC from the Selected NICs column to the Available NICs column.
Move Up	Moves a NIC up in the Selected NICs column.
Move Down	Moves a NIC down in the Selected NICs column.

Interface Properties window for firewalls

The Interface Properties window contains updates. Use this window to configure interface properties such as IP addresses, zones, and interface monitoring.

Tab	Description
Interface Properties tab	Use this tab to configure interface and IP address settings for a standard interface. The version of the Interface Properties tab displayed depends on whether the interface is a standard interface or a transparent parent or member interface.
NICs/NIC Groups	Use the NICs/NIC Groups tab to modify NIC and NIC Group settings.

Interface Properties tab (Interface Properties window) for standard interfaces

Use this tab to configure interface and IP address settings for a standard interface.

Option	Definition
Interface Name	Defines the interface name.
Description	Adds a description to the interface.
NIC or NIC Groups	
Enabled	Enables the interface.
NIC / NIC Group	Specifies which NIC or NIC group to use.
VLAN	Specifies whether the interface is standard or VLAN, configures the VLAN ID.
MTU Size	Selects the Maximum Transmission Unit (MTU) size in bytes: • Standard (1500) • Jumbo (9000) Note: Jumbo can only be selected when the jumbo_mtu capability is enabled on the NIC or all members of the NIC group. • Custom(576-9000) Note: If the jumbo_mtu capability is not enabled, the maximum size that can be selected is 1500. If IPv6 is enabled, the minimum size that can be selected is 1280.
Address Configuration	
Zone	Selects the zone to associate with the interface.
Edit	Opens the Zones window for the selected zone.
Add	Opens the Zones window.
Obtain IPv4 address automatically via DHCP	Determines if the interface's IP address will be assigned using the Dynamic Host Configuration Protocol (DHCP).
Enable IPv6	Enables IPv6.
IPv6 stateless auto address configuration	Specifies whether Static, Router, or Host mode is used when IPv6 is enabled.
IPv4 Addresses	
Add	Opens the Interface Address window.
Modify	Opens the Interface Address window for the selected address.
Delete	Removes an IPv4 address.
Move Up	Moves an IPv4 address up in the list.
Move Down	Moves an IPv4 address down in the list.
Find field	Searches for a specific element in the list of IPv4 addresses.
Address	Specifies the IPv4 addresses.
Mask	Specifies the masks for the IPv4 addresses.
IPv6 Addresses	
Add	Opens the Interface Address window.

Option	Definition
Modify	Opens the Interface Address window for the selected address.
Delete	Removes the selected interface.
Move Up	Moves an IPv6 address up in the list.
Move Down	Moves an IPv6 address down in the list.
Find field	Searches for a specific element in the list of IPv6 addresses.
Address	Specifies the IPv6 addresses.
Prefix	Specifies the prefixes for the IPv6 addresses.
Quality of Service (QoS) Profile	
Quality of Service (QoS) Profile	Selects the Quality of Service profile to use.
Modify	Opens the Quality of Service window for the selected profile.
Add	Opens the Quality of Service window.

See also

Interface Address window for IPv4 addresses

Interface Address window for IPv6 addresses

Interface Properties tab (Interface Properties window) for transparent parent interfaces

Use this tab to configure interface and IP address settings for a transparent parent interface.

Option	Definition
Interface name	Defines the interface name.
Description	Adds a description to the interface.
Enabled	Enables the interface.
Bridged interfaces	
Add	Opens the Interface Properties tab for transparent member interfaces.
Edit	Opens the Interface Properties tab for transparent member interfaces for the selected interface.
Find field	Searches for a specific element in the interface list.
Use	Selects the interface to use for the bridge.
Interface	Displays the interface name.
Zone	Displays the zone assigned to the interface.
NIC/NIC Group	Displays the NIC or NIC Group used by the interface.
VLAN	Displays the VLAN ID.
MTU Size	Selects the Maximum Transmission Unit (MTU) size in bytes: • Standard (1500) • Jumbo (9000) Note: Jumbo can only be selected when the jumbo_mtu capability is enabled on the NIC or all members of the NIC group. • Custom(576-9000) Note: If the jumbo_mtu capability is not enabled, the maximum size that can be selected is 1500.
Address Configuration	
Zone	[Read only] Displays the Firewall zone.
Obtain IPv4 address automatically via DHCP	This option is disabled for transparent interfaces.
Enable IPv6	This option is disabled for transparent interfaces.
IPv4 Addresses	
Add	Opens the Interface Address window.
Modify	Opens the Interface Address window for the selected address.
Delete	Removes an IPv4 address.
Move Up	Moves an IPv4 address up in the list.
Move Down	Moves an IPv4 address down in the list.
Find field	Searches for a specific element in the list of IPv4 addresses.
Address	Specifies the IPv4 addresses.
Mask	Specifies the masks for the IPv4 addresses.
Quality of Service (Qos) Profile	
Quality of Service (QoS) Profile	This option must be configured on the transparent member interface.

See also

Interface Properties tab (Interface Properties window) for transparent member interfaces

Interface Address window for IPv4 addresses

Interface Properties tab (Interface Properties window) for transparent member interfaces

Use this tab to configure transparent member interfaces.

Option	Definition
Interface Name	Defines the interface name.
Description	Adds a description to the interface.
NIC or NIC Groups	
Enabled	Enables the interface.
NIC / NIC Group	Specifies which NIC or NIC group to use.
VLAN id	Specifies whether the interface is standard or VLAN, configures the VLAN ID.
MTU Size	This option must be configured on the transparent parent interface.
Address Configuration	
Zone	Selects the zone to associate with the interface.
Edit	Opens the Zones window for the selected zone.
Add	Opens the Zones window.
Obtain IPv4 address automatically via DHCP	This option is disabled for transparent interfaces.
Enable IPv6	This option is disabled for transparent interfaces.
IPv4 Addresses	
IPv4 Addresses	This option must be configured on the transparent parent interface.
Address	[Read only] Displays the IPv4 addresses.
Mask	[Read only] Displays the masks for the IPv4 addresses.
Quality of Service (QoS) Profile	
Quality of Service (QoS) Profile	Selects the Quality of Service profile to use.
Modify	Opens the Quality of Service window for the selected profile.
Add	Opens the Quality of Service window.

Interface Address window for IPv4 addresses

Use this window to add or modify IPv4 addresses.

Option	Definition
Address	Specifies the address.
Mask	Specifies the mask.

Interface Address window for IPv6 addresses

Use this window to add or modify IPv6 addresses.

Option	Definition
Address	Specifies the address.
Prefix	Specifies the prefix.

Advanced tab (Interface Properties window) for standard interfaces

Use this tab to override the interface ID when IPv6 is enabled.

Option	Definition
Override	Allows the interface ID to be modified manually.
Interface ID	Specifies the interface ID.

Advanced tab (Interface Properties window) for transparent interfaces

Use this tab to configure the ARP table cache size.

Option	Definition
Interface IDs	This option is disabled for transparent interfaces.
ARP table cache size	Specifies the size of the ARP table cache.

Static Routing window

The Static Routing window contains updates. Use this window to add, remove, and manage routes.

Option	Definition
IPv4	
Configure default route failover	Configures an alternate route if the primary default route fails.

Default Route or Primary Default Route	Specifies the default route traffic is directed to. If you choose have chosen to configure an alternate default route, this route is referred to as a primary default route.
	• **IP address** — Specifies the default IPv4 address. This value is usually the IP address of a router that forwards packets to your Internet Service Provider (ISP).
	• **Description** — Provides information about the default route.
	• **Ping addresses** — Lists the IP addresses used to determine the route status. The default route is considered working if one of the addresses can be reached.
	  • **Add ping address** — Adds a row to add an IP address to the list of ping addresses.
	  • **Delete ping address** — Deletes a row from the list of ping addresses.
	  • **IP address** — Displays a list of IP addresses that are to be contacted to determine route status.
	• **Ping interval(s)** — Specifies the number of seconds the firewall waits between pings before sending configured IP addresses to check default route accessibility.
	• **Failures allowed** — Specifies the number of failed ping attempts that must occur before the alternate default route is enabled as the primary default route.

Alternate Default Route	Specifies the alternate route data is directed to.
	• **IP address** — Specifies the IPv4 address for the alternate gateway. This value is the IP address of a device that forwards traffic with no known route to its destination address.
	• **Description** — Provides information about the alternate default route.
	• **Ping addresses** — Lists the IP addresses used to determine the route status. The default route is considered working when one address can be reached.
	  • **Add ping address** — Adds a row to add an IP address to the list of ping addresses.
	  • **Delete ping address** — Deletes a row from the list of ping addresses.
	  • **IP address** — Displays a list of IP addresses that are to be contacted to determine route status.
	• **Ping interval(s)** — Specifies the number of seconds the firewall waits between pings before sending configured IP addresses to check default route accessibility.
	• **Failures allowed** — Specifies the number of failed ping attempts that must occur before the alternate default route is considered inaccessible.

Option	Definition
Static Routes	Displays static routes that are not specified as the primary default route along with the alternate default route. • **Add route** — Adds a row to the list of static routes. • **Delete route** — Deletes a row from the list of static routes. • **Replace** — Finds and replaces a value in the list. • **Destination** — Specifies the IPv4 address of the host or network route. This value must be a valid IPv4 address in dot decimal notation. • **Netmask** — Specifies the netmask assigned to the route destination. This value must be a valid IPv4 address in dotted quad format. • **Gateway** — Specifies the IPv4 address of the route gateway. • **[Version 8.2.1 and later firewalls only] Distance** — Specifies the metric value of the routing configuration. • **Description** — Provides information about the route.
IPv6	
Default Route	Specifies the default route IPv6 traffic is directed to. • **IP address** — Specifies the default IPv6 route. • **Description** — Provides information about the route.
Add route	Adds a row to the list.
Delete route	Deletes a row from the list.
Replace	Finds and replaces a value in the list.
Search	Searches for the specified value within the list of static routes.
Destination	Specifies the IPv6 address of the host or network route.
Prefix	Specifies the mask length for the destination IP address. Valid values range from 0-128.
Gateway	Specifies the IPv6 address of the route gateway.
Distance	Specifies the metric value of the routing configuration.
Description	Provides information about the route.

Host window

The Host window contains updates. Use this window to add a fully qualified host name or IP address to configure an endpoint.

Option	Definition
Name	Specifies a unique name for the host object.
Privileged	When selected, the object is created as a privileged object, which is a special object classification. Note: This checkbox is deselected by default. To create a privileged object, the user must be assigned a role that allows access to privileged objects. Tip: Use the Actions tab on the Role window in the Control Center icon to assign the privileged object action to a role.
Description	Specifies information about the host object.

Type	Determines the type of host object you are configuring. The following options are available:
	• **IP address** — When selected, the host object is created using the IP address. This is the default selection. If you select this value, the following field is available:
	  • **IP address** — Specifies the IP address of the host. If there is at least one firewall that is enabled with the IPv6 protocol, you can specify an IPv6 address, which is a series of seven groups of alphanumeric characters that are separated by colons (:). An example of this format is: nnaa:an:n:nana:naa:aa:aann:nana.
	  However, if there are no IPv6-enabled firewalls, you must specify an IPv4 address, which is a series of four groups of decimals in dot notation. An example of an IPv4 address is: nnn.nnn.nnn.nnn.
	  If you want to use an IPv6 address in this field, for version 7.x firewalls, you cannot specify a value in the **Hostname** field.
	• **Hostname** — When selected, the host object is created using the host name. If you select this value, the following fields are available:
	  • **Hostname** — Specifies the fully qualified host name.
	  • **Perform DNS lookup to resolve the hostname** — When selected, a DNS lookup is performed to find the IP address associated with a specified host name. If this checkbox is selected, the following fields are available.
	  • **IP address(es)** — Specifies additional addresses that the host name does not resolve to, when a DNS lookup is performed. Multiple addresses can be specified with a comma to separate entries. You may choose to leave this field blank.
	  Note: IPv6 addresses can be used only in firewall versions 8.0.0 or later.
	  • **Override default TTL (seconds)** — When selected, default time-to-live (TTL) period for caching DNS records is overridden by a specified value. The default value is 86400 seconds (one day). To override the default, select this checkbox and select a different value.
	  • **Use the following IP address(es) to resolve the hostname** — Specifies any addresses used to resolve the hostname. Multiple addresses can be specified with a comma to separate entries.
	  Note: IPv6 addresses can be used only in firewall versions 8.0.0 or later.

OK	Closes the window and saves any changes made.
Cancel	Closes the window and discards any changes made.

Adaptive window

The Adaptive window contains updates. Use this window to create an adaptive endpoint.

Option	Definition
Name	Specifies a unique name for the adaptive endpoint object.
Privileged	Identifies a privileged object, which is a special object classification. This checkbox is deselected by default. To create a privileged object, the user must be assigned a role that allows access to privileged objects. Use the Actions tab on the Role window in the Control Center icon to assign the privileged object action to a role.

Option	Definition
Description	Specifies information about the adaptive endpoint object.
Add	Opens the Adaptive Addresses window.
Edit	Opens the Adaptive Addresses window for the selected row. Tip: You can also double-click a row to edit it in the Add Adaptive Addresses window.
Delete	Removes the selected row from the firewall addresses.
Firewall addresses table	Displays the firewalls and the addresses assigned to them. • **Firewall** — Displays the name of the firewall on which the object is being used. • **Addresses** — Displays the IP address or addresses that are used to reference the endpoint object. • *Search* — Finds a host name or IP address in the list. Tip: To search, enter a host name or IP address and click the search button next to this field. The search will only display all entries that match.
Default	Displays the default address to be used for firewalls that are not specified in the Firewall field. To edit this value, click the edit button next to this field. The Adaptive Addresses window is displayed.
OK	Closes the window and saves any changes made.
Cancel	Closes the window and discards any changes made.

Adaptive addresses window

Use this window to configure combinations of firewalls and addresses for an adaptive endpoint object.

Option	Definition
<firewall_name>	Displays the name of the firewall that was selected in the Adaptive window. This field is viewable only when you are editing an existing address.
Firewall	Specifies the name of the firewall on which the object is being used. To search for objects, use the filter field to control the number of objects that are displayed. To limit the search to exact matches of a specified sequence of characters that appears anywhere in the object name, specify one or more characters and press **Enter**. To perform an advanced search for an object, click **Advanced Search**.
Add	Adds a row in the addresses table to allow you to enter an IP address, host name, network, or range.
Delete	Deletes a selected row from the addresses table.
Search	Allows you to search for an IP address, hostname, network, or range from the list.
Addresses	Specifies the IP address or addresses that are used to reference this endpoint object. You may specify IP addresses in any of the following ways: • IP address in dot notation form (for example, four decimal numbers separated by periods) • Host name • Network address/subnet mask length in bits (for example, 192.168.0.0/16) • Address range (<beginning_IP_address> - <ending_IP_address>)
OK	Closes the window and saves any changes made.
Cancel	Closes the window and discards any changes made.

Control Center Resources area (Summary page)

The Summary page contains updates. Use the this area to view information about the use of resources in each of the following conditions:

- **Standalone mode** — In this mode, Control Center displays information pertinent to only one Control Center Management Server.

- **High Availability (HA) mode** — In this mode, Control Center displays information pertinent to the Primary and Backup Control Center Management Servers. If the backup server malfunctions, Control Center displays a failure message to alert the administrator.

Option	Definition
Control Center Resources	Displays the Control Center Resources window.

Primary Server tab	Displays read-only information about Control Center Management Server resources.
	• **CPU Utilization** — Displays the current percentage of CPU that is being utilized on the Control Center Management Server.
	• **Physical Memory** — Displays the current percentage of physical memory that is being utilized on the Control Center Management Server.
	  • **Total** — Displays the total amount of physical memory on the Control Center Management Server in kilobytes.
	  • **Available** — Displays the amount of available physical memory on the Control Center Management Server in kilobytes.
	• **Audit Data Partition** — Displays the percentage of disk space that is currently being used by the audit data partition:
	  /opt/security/var/gccserver/auditlogs
	• **Backup Partition** — Displays the percentage of disk space that is currently being used by the backup partition:
	  /opt/security/var
	• **Database Partition** — Displays the percentage of disk space that is currently being used by the database partition:
	  /var/lib/pgsql
	• **Logs Partition** — Displays the percentage of disk space that is currently being used by the logs partition:
	  /

Backup Server tab	[High Availability only] Displays a failure message when the backup server malfunctions. Note: When the backup server is functioning normally, the backup server tab displays information for parameters similar to that of the primary server tab.