

Enhanced Interior Gateway Routing Protocol (EIGRP)

The Enhanced Interior Gateway Routing Protocol (EIGRP) is a hybrid dynamic distance-vector and link-state interior gateway routing protocol. Originally a proprietary protocol developed by Cisco, it is now an open standard defined in RFC 7868. You can configure EIGRP to manage interior routes within an autonomous system.

- Best Practices for EIGRP, on page 1
- About EIGRP, on page 2
- Guidelines for EIGRP, on page 3
- Configure the Core EIGRP Process, on page 4
- Customize the EIGRP Process, on page 7
- Monitoring EIGRP, on page 17

Best Practices for EIGRP

Following are some tips for configuring EIGRP:

- If you are inserting the device into an existing EIGRP autonomous system, examine the configuration of the other routers in the autonomous system to determine the system number and any other customizations. Ensure that you implement the same, or at least consistent, customizations on the Firewall Threat Defense device that you are adding.
- Determine whether to configure a full EIGRP process or a stub process:
  - If the Firewall Threat Defense device is in the middle of the autonomous system, where it is connected to more than one other EIGRP router, you probably need the full EIGRP process. See Configure the EIGRP Process for Full Routing, on page 4.
  - If the Firewall Threat Defense device is at the edge of the autonomous system, where it is connected to just one other EIGRP router, and otherwise hosts connected networks only, then configuring it as a stub router might make the most sense. You can configure the stub so that the Firewall Threat Defense device sends information to the EIGRP neighbor about connected routes, so that other EIGRP routers in the autonomous system can get routes to the Firewall Threat Defense device's connected networks. See Configure the EIGRP Process for Stub Routing, on page 5.

- The default settings work for most networks, so adjust them only if you have adjusted them on other EIGRP routers in the autonomous system. You can have a fully-functional EIGRP process by simply configuring the autonomous system number and specifying the networks to route.
- Configure the router ID to ensure a stable address is used to identify the router. This can help make troubleshooting routing problems easier. See Configure EIGRP Advanced Settings, on page 7.
- Do not enable automatic route summarization (the **auto-summary** command) unless you have determined that it will not create routing loops and it will provide some benefit for your network. How to determine whether auto summarization will work for your network is outside the scope of this document.

About EIGRP

The Enhanced Interior Gateway Routing Protocol (EIGRP) is a hybrid dynamic distance-vector and link-state interior gateway routing protocol. EIGRP sends routing updates to routers within the same autonomous system. Normally, EIGRP discovers neighbor routers using multicast updates, but you can configure static neighbors that are outside of a multicast boundary, and these static neighbors get unicast updates.

The convergence technology of EIGRP is based on an algorithm called the Diffusing Update Algorithm (DUAL). The algorithm guarantees loop-free operation at every instant throughout a route computation and allows all devices involved in a topology change to synchronize. Devices that are not affected by topology changes are not involved in recomputations.

To a limited extent, you can adjust routing metrics to control how routes are chosen. The following topics provide some background on these advanced concepts.



Note If you adjust these metrics, you must make the same adjustment to all routers within the autonomous system or you might get routing loops.

DUAL Finite State Machine

The DUAL finite state machine embodies the decision process for all route computations. It tracks all routes advertised by all neighbors. DUAL uses the distance information (known as the metric) to select efficient, loop-free paths.

DUAL selects routes to be inserted into a routing table based on feasible successors. A successor is a neighboring device (used for packet forwarding) that has the least-cost path to a destination that is guaranteed not to be part of a routing loop.

When a topology change occurs, DUAL will test for feasible successors. If there are feasible successors, DUAL will use any feasible successors it finds to avoid unnecessary recomputation.

When there are no feasible successors but only neighbors advertising the destination, a recomputation must occur to determine a new successor. The time required to recompute the route affects the convergence time.

EIGRP Metric Weights

EIGRP uses metric weights, known as K values, in routing and metric computations. EIGRP metric defaults have been carefully selected to provide optimal performance in most networks.

Unlike IOS routers, you cannot adjust these default K values for EIGRP running on the Firewall Threat Defense device. Because you need to use the same K values on all systems within an autonomous network, you should not change them on any routers within an autonomous system that includes Firewall Threat Defense devices.

For an explanation of how the K values are used, see EIGRP Cost Metrics, on page 3.

EIGRP Cost Metrics

EIGRP uses metric weights (K values) in addition to link characteristics to compute a composite cost metric. To avoid churn in the network as a result of a change in the link characteristics, you can tune some of the values used in this computation.

The actual computation is quite complex, using five K values (as multipliers) and five vector attributes. However, three K values are 0 by default, and because you cannot change the K value defaults, the actual computation is greatly simplified:

cost metric = 256 * (bandwidth + delay)

What you can change is the bandwidth and delay values for routes redistributed from or to the EIGRP process. Specifically, you can adjust these values in the **default-metric** command (to set a default for all types of redistributed routes) or in the **redistribute metric** command (to set the metrics for a specific type of route). Note the following:

- Bandwidth is the minimum bandwidth of the route, in kilobits per second. It can be 1 to 4294967295 Kilobytes per second. The bandwidth for the formula is scaled and inverted by the following formula:

  $(10^7$/minimum bandwidth in kilobits per second)

- Delay is the route delay, in tens of microseconds.

The other characteristics, which are not used by Firewall Threat Defense, are the delay reliability, the effective load on the route, and the minimum MTU (maximum transmission unit) on the route. Even though the values are not used, you must configure them if you adjust these commands.

For more detailed information on how EIGRP calculates the cost metric, see *IP Routing: EIGRP Configuration Guide*. For example, https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_eigrp/configuration/xe-16-7/ire-xe-16-8-book/ire-enhanced-igrp.html.

Guidelines for EIGRP

IPv6 Guidelines

Does not support IPv6.

Additional Guidelines

- A maximum of one EIGRP process is supported.
- You cannot change the autonomous system number for an EIGRP process. Instead, delete the process, deploy your changes, then configure a new process using the new autonomous system number.
- You cannot include a network in the EIGRP process that belongs to a Bridge Virtual Interface (BVI).

- EIGRP adjacency flap occurs whenever a configuration change is applied which results in modifying the routing information (sent or received) from neighbors especially in distribute lists, offset lists, and changes to summarization. After the routers are synchronized, EIGRP reestablishes the adjacency between neighbors. When an adjacency is torn down and reestablished, all learned routes between the neighbors are erased and the entire synchronization between the neighbors is performed newly with the new distribute list.

Configure the Core EIGRP Process

The following topics explain how to get EIGRP up and running on the device. You can either configure the full routing process, or configure it as a stub process for systems that should not fully participate in the autonomous network as an EIGRP router.

Configure the EIGRP Process for Full Routing

You can configure one EIGRP process. If you configure multiple virtual routers, EIGRP is supported in the global virtual router only.

The following procedure sets up basic EIGRP routing for a set of networks using all default values for EIGRP routing. Completing this procedure is sufficient to enable EIGRP on the device. You can complete the other procedures to fine-tune the EIGRP process as needed.

Before you begin

Determine what autonomous system number you are using for EIGRP in your network.

Create network objects that define each of the networks that you want to route within the EIGRP autonomous system. For example, if you want to use EIGRP for the 192.168.1.0/24 and 192.168.2.0/24 networks, create two network objects, one for each network.

Procedure

Step 1 Click **Device**, then click the **Routing** summary.

Step 2 If you enabled virtual routers, click the view icon ( ) for the global virtual router.

Step 3 Click the **EIGRP** tab.

Step 4 Do one of the following:

- To create a new process, click **+** or click the **Create EIGRP Object** button.
- Click the edit icon ( ) for the object you want to edit. Note that when you edit an object, you might see lines that you did not directly configure. These lines are exposed to show you the default values that are being configured.

If you no longer need a process, click the trash can icon for the object to delete it.

Step 5 Enter a **Name** for the Smart CLI object and optionally, a description.

Step 6 Configure the basic process properties:

router eigrp *autonomous-system*

Click the variable and enter a number from 1-65535. Use the same autonomous system number used on the other routers in the network that should operate within the same routing domain as this device.

Step 7 Configure the networks and interfaces that should be routed within the EIGRP autonomous system.

a) Click the **Show Disabled** link above the object body to add all other possible configuration lines.

b) Click the + to the left of the **network** *network-object* line.

c) In the **network** command, click the variable and select the object that defines a network that should be included in this autonomous system.

Typically, this would be a directly-connected network. For example, if the IP address of the inside interface is 192.168.1.1/24, the associated network object for this command would contain 192.168.1.0/24. If the object does not already exist, click **Create New Network** and create it now.

Directly connected and static networks that fall within the defined network are advertised by the process. Additionally, only interfaces with an IP address that fall within the defined network participate in the EIGRP routing process.

If you have an interface that you do not want to have participate in EIGRP routing, but that is attached to a network that you want advertised, see Configure EIGRP Passive Routing Interfaces, on page 10.

d) If you have additional networks to route, click **...** > **Duplicate** to the left of the **network** command to add a new one. Keep adding **network** lines until you have configured all the networks to route.

Step 8 (Optional.) If necessary, adjust settings for the other initially disabled commands. See Customize the EIGRP Process, on page 7.

Step 9 Click **OK**.

Configure the EIGRP Process for Stub Routing

You can configure the device to be an EIGRP stub router. Stub routing decreases memory and processing requirements on the system. As a stub router, the system does not need to maintain a complete EIGRP routing table because it forwards all non-local traffic to a distribution router. Generally, the distribution router need not send anything more than a default route to the stub router.

Only specified routes are propagated from the stub router to the distribution router. As a stub router, the system responds to all queries for summaries, connected routes, redistributed static routes, external routes, and internal routes with the message “inaccessible.” The system sends a special peer information packet to all neighboring routers to report its status as a stub router. Any neighbor that receives a packet informing it of the stub status will not query the stub router for any routes, and a router that has a stub peer will not query that peer. The stub router depends on the distribution router to send the correct updates to all peers.

Before you begin

Determine what autonomous system number you are using for EIGRP in your network.

Create network objects that define each of the networks that you want to route within the EIGRP autonomous system. For example, if you want to use EIGRP for the 192.168.1.0/24 and 192.168.2.0/24 networks, create two network objects, one for each network.

Procedure

Step 1 Click **Device**, then click the **Routing** summary.

Step 2 If you enabled virtual routers, click the view icon ( ) for the global virtual router.

Step 3 Click the **EIGRP** tab.

Step 4 Do one of the following:

- To create a new process, click + or click the **Create EIGRP Object** button.
- Click the edit icon ( ) for the object you want to edit. Note that when you edit an object, you might see lines that you did not directly configure. These lines are exposed to show you the default values that are being configured.

If you no longer need a process, click the trash can icon for the object to delete it.

Step 5 Enter a **Name** for the Smart CLI object and optionally, a description.

Step 6 Configure the basic process properties:

router eigrp *autonomous-system*

Click the variable and enter a number from 1-65535. Use the same autonomous system number used on the other routers in the network that should operate within the same routing domain as this device.

Step 7 Configure the networks and interfaces that should be routed within the EIGRP autonomous system.

a) Click the **Show Disabled** link above the object body to add all other possible configuration lines.
b) Click the + to the left of the **network** *network-object* line.
c) In the **network** command, click the variable and select the object that defines a network that should be included in this autonomous system.

   Typically, this would be a directly-connected network. For example, if the IP address of the inside interface is 192.168.1.1/24, the associated network object for this command would contain 192.168.1.0/24. If the object does not already exist, click **Create New Network** and create it now.

   Directly connected and static networks that fall within the defined network are advertised by the process. Additionally, only interfaces with an IP address that fall within the defined network participate in the EIGRP routing process.

   If you have an interface that you do not want to have participate in EIGRP routing, but that is attached to a network that you want advertised, see Configure EIGRP Passive Routing Interfaces, on page 10.

d) If you have additional networks to route, click **...** > **Duplicate** to the left of the **network** command to add a new one. Keep adding **network** lines until you have configured all the networks to route.

Step 8 Configure the stub settings.

a) Click the + to the left of the **setup eigrp** *configuration* line.
b) Click the variable and select **advanced**.
c) Click the + to the left of the **setup eigrp stub** *stub-options* command.
d) To restrict the device from sharing any of its routes with any other router in the autonomous system, so that it only receives updates from the EIGRP neighbor router, click *stub-options* and select **receive**. Then, configure the following command:

eigrp stub *stub-parameters*

Click the variable and select **receive-only**.

e) To allow the device to advertise routes to EIGRP neighbor routers, click *stub-options* and select **other**. Then, configure the following command to select the types of route that should be advertised.

eigrp stub *connected-parameter redistributed-parameter static-parameter summary-parameter*

Click the variables to make your selection. You must select at least one route type, but you can select all or any combination.

- *connected-parameter*. Select **connected** to advertise connected routes. If the connected routes are not covered by a **network** statement, it might be necessary to configure redistribution for the connected routes in the EIGRP process.
- *redistributed-parameter*. Select **redistributed** to advertise routes redistributed into the EIGRP routing process from other routing protocols.
- *static-parameter*. Select **static** to advertise static routes. You must also enable the **configure redistribution** command and configure the redistribution of static routes.
- *summary-parameter*. Select **summary** to advertise summary routes.

Step 9 (Optional.) If necessary, adjust settings for the other initially disabled commands. See Customize the EIGRP Process, on page 7.

Step 10 Click **OK**.

Customize the EIGRP Process

EIGRP includes many options that have default values. These values work well for many networks. However, you might need to adjust one or more settings to get the precise behavior you need. The following topics explain the various ways you can customize your EIGRP routing process.

Configure EIGRP Advanced Settings

You can configure several settings that control the overall behavior of an EIGRP process, including automatic route summarization, distance metrics, logging. and the router ID used for sending link state advertisements and other routing updates. Many of these settings have defaults that are appropriate for most networks.

Before you begin

This procedure assumes you have already configured the EIGRP process; see Configure the Core EIGRP Process, on page 4.

When you create the process, certain advanced options are enabled by default. You will see these enabled options when you edit the EIGRP object.

Procedure

Step 1 Click **Device**, then click the **Routing** summary.

Step 2 If you enabled virtual routers, click the view icon ( ) for the global virtual router.

Step 3 Click the **EIGRP** tab.

Step 4 Click the edit icon ( ) for the EIGRP object.

Note that when you edit an object, you might see lines that you did not directly configure. These lines are exposed to show you the default values that are being configured.

Step 5 Click **Show Disabled** above the object body to add all other possible configuration lines.

Step 6 The **setup eigrp** *configuration* line should already be enabled as **setup eigrp advanced**. If it is not, click the + to the left of the line to enable it, then click the variable and select **advanced**.

Step 7 (Optional; not recommended.) To automatically summarize routes on network number boundaries, click + next to the **auto-summary** command.

This can cause routing problems if you have noncontiguous networks.

For example, if you have a router with the networks 172.16.1.0, 172.16.2.0, and 172.16.3.0 connected to it, and those networks all participate in EIGRP, the EIGRP routing process creates the summary address 172.16.0.0 for those routes. If an additional router is added to the network with the networks 172.16.10.0 and 172.16.11.0, and those networks participate in EIGRP, they will also be summarized as 172.16.0.0. Thus, automatically summarizing the routes leads to traffic being routed to the wrong router.

Step 8 (Optional; recommended.) Configure the router ID.

Click + to enable the **router-id** command, then click the variable and enter the IPv4 address that should be used when sending any router updates from this device. No two routers in an EIGRP autonomous system can have the same router ID, so ensure that it is unique in the system.

If you do not explicitly specify a router ID for the process, the system uses the highest IP address assigned to an active interface. Thus, the router ID can change if you disable the selected interface, or you change its addresses. By assigning a router ID explicitly, you ensure consistency for your process.

Step 9 (Optional.) Configure the administrative distances for internal and external EIGRP routes.

The following command is enabled by default when you configure the process. If you are configuring a new object, you might need to click + to enable the command.

distance eigrp 90 170

Because every routing protocol has metrics based on algorithms that are different from the other routing protocols, it is not always possible to determine the “best path” for two routes to the same destination that were generated by different routing protocols. Administrative distance is a route parameter that the system uses to select the best path when there are two or more different routes to the same destination from two different routing protocols.

Administrative distances for EIGRP are from 1 to 255. These numbers are relative to the administrative values assigned to other routing processes when the system chooses the best routes. In general, the higher the value, the lower the trust rating. The default values should work for most networks. Adjust them it you want to either give preference to EIGRP routes, or if you want to reduce the likelihood of EIGRP routes being used.

The numbers mean the following:

- First value (90): **Internal Distance**. The administrative distance for EIGRP internal routes. Internal routes are those that are learned from another entity within the same autonomous system.
- Second value (170): **External Distance**. The administrative distance for EIGRP external routes. External routes are those for which the best path is learned from a neighbor external to the autonomous system

Step 10 The **default-metric** command is used when redistributing routes from other routing processes. Configure it only if you also configure redistribution. For details, see Configure EIGRP Route Redistribution, on page 15.

Step 11 Configure neighbor logging.

The following commands are enabled by default when you configure the process. If you are configuring a new object, you might need to click + to enable the command. If you want to disable logging, click - to disable the commands.

- **eigrp log-neighbor-changes** enables the logging of EIGRP neighbor adjacency changes.
- **eigrp log-neighbor-warnings 10** enables the logging of EIGRP neighbor warning messages. The number is the time interval between repeated neighbor warning messages, from 1 to 65535 seconds. Repeated warnings are not logged if they occur during this interval.

Step 12 If you want to configure the **setup stub** command, see Configure the EIGRP Process for Stub Routing, on page 5.

Step 13 Click **OK**.

Configure the Networks for EIGRP to Advertise

Use the **network** command to identify the networks, and by implication, interfaces that should be included in EIGRP routing. For an interface to participate in EIGRP routing, it must fall within the range of addresses defined by the network entries. For directly connected and static networks to be advertised, they must also fall within the range of the network entries.

Before you begin

This procedure assumes you have already configured the EIGRP process; see Configure the Core EIGRP Process, on page 4.

Create the network objects that define the networks to advertise.

Procedure

Step 1 Click **Device**, then click the **Routing** summary.

Step 2 If you enabled virtual routers, click the view icon ( ) for the global virtual router.

Step 3 Click the **EIGRP** tab.

Step 4 Click the edit icon ( ) for the EIGRP object.

Note that when you edit an object, you might see lines that you did not directly configure. These lines are exposed to show you the default values that are being configured.

Step 5 Click **Show Disabled** above the object body to add all other possible configuration lines.

Step 6 Assuming you already configured a network, click **...** > **Duplicate** next to a **network** line to create a new empty command.

If you have defined no networks yet, click + next to the empty **network** *network-object* line.

Step 7 In the **network** command, click the variable and select the object that defines a network that should be included in this autonomous system.

Typically, this would be a directly-connected network. For example, if the IP address of the inside interface is 192.168.1.1/24, the associated network object for this command would contain 192.168.1.0/24. If the object does not already exist, click **Create New Network** and create it now.

Directly connected and static networks that fall within the defined network are advertised by the process. Additionally, only interfaces with an IP address that fall within the defined network participate in the EIGRP routing process.

If you have an interface that you do not want to have participate in EIGRP routing, but that is attached to a network that you want advertised, see Configure EIGRP Passive Routing Interfaces, on page 10.

Step 8 If you have additional networks to route, click **...** > **Duplicate** to the left of the **network** command to add a new one. Keep adding **network** lines until you have configured all the networks to route.

Step 9 Click **OK**.

Configure EIGRP Passive Routing Interfaces

If you have an interface that you do not want to have participate in EIGRP routing, but that is attached to a network that you want advertised, you can configure a **network** command that includes the network to which the interface is attached, and use the **passive-interface** command to prevent that interface from sending or receiving EIGRP updates.

By default, the system enables the **no passive-interface default** command, which sets all interfaces to be active, sending and receiving EIGRP updates.

The following procedure explains how to change an interface to be passive.

Before you begin

This procedure assumes you have already configured the EIGRP process; see Configure the Core EIGRP Process, on page 4.

When you create the process, you add the **network** commands to indicate which networks should be routed using EIGRP. To configure additional networks to route, see Configure the Networks for EIGRP to Advertise, on page 9.

Procedure

Step 1 Click **Device**, then click the **Routing** summary.

Step 2 If you enabled virtual routers, click the view icon ( ) for the global virtual router.

Step 3 Click the **EIGRP** tab.

Step 4 Click the edit icon () for the EIGRP object.

Note that when you edit an object, you might see lines that you did not directly configure. These lines are exposed to show you the default values that are being configured.

Step 5 Click **Show Disabled** above the object body to add all other possible configuration lines.

Step 6 If you are editing an object, the **configure interface passive** command and its child, **no passive-interface default**, are enabled.

For a new object, click **+** to enable the **configure routing-interface** *parameters* command.

Step 7 To configure interfaces to be active by default, and then selectively make interfaces passive:

a) In the **configure routing-interface** command, click the variable and select **passive**.

This action enables the **no passive-interface default** command, which makes EIGRP interfaces active by default.

b) Click **+** next to the **passive-interface** *interface* command, click the variable, and select the interface that should be passive and not participate in EIGRP routing updates.

c) Click **...** > **Duplicate** next to the **passive-interface** *interface* command if you need to configure additional passive interfaces. Continue until you have a **passive-interface** command for each interface that should be passive.

Step 8 To configure interfaces to be passive by default, and then selectively make interfaces active:

a) In the **configure routing-interface** command, click the variable and select **active**.

This action enables the **passive-interface default** command, which makes EIGRP interfaces passive by default.

b) Click **+** next to the **no passive-interface** *interface* command, click the variable, and select the interface that should actively participate in EIGRP routing updates.

c) Click **...** > **Duplicate** next to the **no passive-interface** *interface* command if you need to configure additional active interfaces. Continue until you have a **no passive-interface** command for each interface that should be active.

Step 9 To switch an interface back to the default behavior (either passive or active), click **-** next to the command that makes that specific interface passive or active. This deletes the exception and makes the interface behave according to the default action you set.

Step 10 Click **OK**.

Configure Static EIGRP Neighbors

EIGRP hello packets are sent as multicast packets. If an EIGRP neighbor is located across a non broadcast network, such as a VPN tunnel, you must manually define that neighbor. When you manually define an EIGRP neighbor, hello packets are sent to that neighbor as unicast messages.

You do not need to define static neighbors that are on regular broadcast networks, as these routers can form adjacencies themselves.

Before you begin

This procedure assumes you have already configured the EIGRP process; see Configure the Core EIGRP Process, on page 4.

Determine the interface through which the system should reach the neighbor.

You can also configure logging settings for neighbors, as explained in Configure EIGRP Advanced Settings, on page 7.

Procedure

Step 1 Click **Device**, then click the **Routing** summary.

Step 2 If you enabled virtual routers, click the view icon ( ) for the global virtual router.

Step 3 Click the **EIGRP** tab.

Step 4 Click the edit icon ( ) for the EIGRP object.

Note that when you edit an object, you might see lines that you did not directly configure. These lines are exposed to show you the default values that are being configured.

Step 5 Click **Show Disabled** to expose all commands, then click **+** to enable the **neighbor** command.

Step 6 Configure the neighbor address.

neighbor *ip-address* **interface** *interface*

- Click *ip-address* and enter the IP address of the neighbor router.
- Click *interface* and select the interface through which the system can reach the router.

Step 7 If necessary, configure a static route for the neighbor router.

If the IP address of the router is on the same network as the selected interface, a static route is not necessary. For example, if you select an interface whose IP address is 10.100.10.1/24, and the neighbor address is 10.100.10.2/24, you do not need a static route.

Step 8 You can click **...** > **Duplicate** next to the **neighbor** command to define another static neighbor. Define as many as you require.

Step 9 Click **OK**.

Control EIGRP Candidate Default Route Dissemination

You can control the sending or receiving of default route candidates from the EIGRP process. By default, all candidate routes are advertised or accepted contingent on your route filtering and redistribution settings.

You cannot directly turn off the sending or receiving of a default route. If you want to prevent default route dissemination from EIGRP, configure these commands with a standard ACL that denies the any-ipv4 network.

Before you begin

This procedure assumes you have already configured the EIGRP process; see Configure the Core EIGRP Process, on page 4.

Create the Smart CLI standard access list objects you need for each filter rule. Use deny access control entries (ACEs) to filter out routes that match the entry, and permit ACEs for the routes that should be updated.

Procedure

Step 1 Click **Device**, then click the **Routing** summary.

Step 2 If you enabled virtual routers, click the view icon ( ) for the global virtual router.

Step 3 Click the **EIGRP** tab.

Step 4 Click the edit icon ( ) for the EIGRP object.

Note that when you edit an object, you might see lines that you did not directly configure. These lines are exposed to show you the default values that are being configured.

Step 5 Click **Show Disabled** above the object body to add all other possible configuration lines.

Step 6 Click + to enable one or both of the following commands:

- **default-information in** *acl* for controlling the receiving of candidate default routes.
- **default-information out** *acl* for controlling the sending of candidate default routes.

Step 7 Click the variable and select the standard ACL that applies your filter.

Step 8 Click **OK**.

Configure EIGRP Filter Rules

You can filter incoming or outgoing routing updates based on network prefixes as defined in a standard access control list. Filtering improves your control of route distribution into an EIGRP autonomous system or outbound to other routing processes.

Before you begin

This procedure assumes you have already configured the EIGRP process; see Configure the Core EIGRP Process, on page 4.

Create the Smart CLI standard access list objects you need for each filter rule. Use deny access control entries (ACEs) to filter out routes that match the entry, and permit ACEs for the routes that should be updated.

Procedure

Step 1 Click **Device**, then click the **Routing** summary.

Step 2 If you enabled virtual routers, click the view icon ( ) for the global virtual router.

Step 3 Click the **EIGRP** tab.

Step 4 Click the edit icon () for the EIGRP object.

Note that when you edit an object, you might see lines that you did not directly configure. These lines are exposed to show you the default values that are being configured.

Step 5 Click **Show Disabled** to expose all commands, then click + to enable the **configure filter-rules** *direction* command.

Step 6 Click *direction* and select **in**, for filtering incoming updates, or **out**, for filtering outbound updates.

This action adds the **distribute-list** commands to the object.

Step 7 For inbound filters, you can optionally specify the interface on which to filter updates. If you do not specify an interface, the filter applies to all updates received on any interface. Click + to enable one of the following options:

- **distribute-list** *acl-name* **in**

  Select your standard ACL object.

- **distribute-list** *acl-name* **in interface** *interface*

  Select your standard ACL object and the interface on which to filter incoming updates.

Step 8 For outbound filters, you can optionally specify the protocol, to limit the filter to routes generated by that routing process, and the interface on which to filter updates. Click + to enable one of the following options:

- **distribute-list** *acl-name* **out**

  Select your standard ACL object.

- **distribute-list** *acl-name* **out interface** *interface*

  Select your standard ACL object and the interface on which to filter outgoing updates.

- **distribute-list** *acl-name* **out** *protocol*

  Select your standard ACL object and one of the following route types:

  - **connected**. For routes established for networks that are directly connected to the system's interfaces.
  - **static**. For static routes you manually created.
  - **rip**. For routes generated by RIP.

- **distribute-list** *acl-name* **out** *protocol identifier*

  Select your standard ACL object and one of the following route types:

  - **ospf** *process-id*. For routes generated by OSPF. Click identifier and enter the process ID for the OSPF process defined on the system.
  - **bgp** *automonous-system*. For routes generated by BGP. Click identifier and enter the autonomous system number for the BGP process defined on the system.

Step 9 You can click **...** > **Duplicate** next to the **configure filter-rules** command to define another filter rule. Define as many as you require.

Step 10 Click **OK**.

Configure EIGRP Route Redistribution

You can control the redistribution of routes into an EIGRP process from other routing protocols, connected routes, and static routes.

Before you begin

It is best practice to configure the routing process from which you will redistribute routes, and deploy your changes, before you configure redistribution into EIGRP.

If you want to apply a route map to fine-tune which routes are redistributed, create the Smart CLI route map object. Routes that match the route map are redistributed, and all non-matching routes are not redistributed.

This procedure assumes you have already configured the EIGRP process; see Configure the Core EIGRP Process, on page 4.

Procedure

Step 1 Click **Device**, then click the **Routing** summary.

Step 2 If you enabled virtual routers, click the view icon ( ) for the global virtual router.

Step 3 Click the **EIGRP** tab.

Step 4 Click the edit icon ( ) for the EIGRP object.

Note that when you edit an object, you might see lines that you did not directly configure. These lines are exposed to show you the default values that are being configured.

Step 5 Click **Show Disabled** to expose all commands.

Step 6 (Optional.) Click + to enable the **default-metric** command, which is in the **setup eigrp advanced** group of commands.

The **default-metric** command sets the metrics to use for redistributed routes if you do not configure a specific **redistribute metric** command for a route type.

default-metric *bandwidth-metric delay-metric reliability-metric effective-bandwidth path-MTU*

Click the variables and configure the following. You must configure all metric variables.

- *bandwidth-metric*. Click the variable and enter the bandwidth for connections on this route from 1 to 4294967295 Kilobytes per second.
- *delay-metric*. Click the variable and enter the delay for connections on the route, in 10 microsecond units, from 0 to 4294967295.
- *reliability-metric*. Click the variable and enter the EIGRP reliability metric for the route, from 0 to 255, where 255 indicates 100% reliability. This metric is ignored but you still must configure it.
- *effective-bandwidth*. Click the variable and enter the EIGRP effective bandwidth for the route, from 1 to 255, where 255 indicates 100% loaded. This metric is ignored but you still must configure it.

- *path-MTU*. Click the variable and enter the mean transmission unit (MTU) of the path, from 1 to 65535. This metric is ignored but you still must configure it.

Step 7 Click **+** to enable the **configure redistribution** command.

Step 8 Click the *protocol* variable and select the source process from which you are redistributing routes. You can redistribute **connected** and **static** routes, or routes generated by **bgp**, **isis**, **ospf**, or **rip**.

Step 9 If you select a routing process, click the *identifier* variable and enter the required value:

- **bgp**. Enter the autonomous system number.
- **ospf**. Enter the process ID number.
- **connected**, **static**, **isis**, **rip**. Enter **none**. Even if you enter a different value, it will be ignored.

Step 10 (Optional; IS-IS only.) On the **redistribute isis route-level** *route-level* command, click the variable and select whether you are redistributing routes learned only within an IS-IS area (**level-1**), between IS-IS areas (**level-2**) or both (**level-1-2**).

Step 11 (Optional; all protocols.) To fine-tune which routes are redistributed based on a route map, click **+** to enable the **redistribute** *route-map* command, click the variable, and select the route map that defines your restrictions.

If you do not apply a route map, all routes for the process (that fit the other commands configured for redistribution), are redistributed.

Step 12 (Optional; all protocols.) To fine-tune the metrics for redistributed routes, click **+** to enable the following command and configure the options:

redistribute *protocol* **metric** *bandwidth-metric delay-metric reliability-metric effective-bandwidth path-MTU*

Click the variables and configure the values, which are explained under the **default-metric** command above. You must configure all metric variables.

Step 13 (Optional; OSPF only.) The following commands are enabled by default when you redistribute routes from an OSPF process. You can click **-** to disable unwanted commands.

These commands specify the criteria by which OSPF routes are redistributed into other routing domains.

- **redistribute ospf match external 1**. Routes that are external to the autonomous system, but are imported into OSPF as Type 1 external routes.
- **redistribute ospf match external 2**. Routes that are external to the autonomous system, but are imported into OSPF as Type 2 external routes.
- **redistribute ospf match internal**. Routes that are internal to a specific autonomous system.
- **redistribute ospf match nssa-external 1**. Routes that are external to the autonomous system, but are imported into OSPF as Type 1 external routes and marked as Not-So-Stubby-Area (NSSA) only.
- **redistribute ospf match nssa-external 2**. Routes that are external to the autonomous system, but are imported into OSPF as Type 2external routes and marked as Not-So-Stubby-Area (NSSA) only.

Step 14 You can click **...** > **Duplicate** next to the **configure redistribution** command to configure redistribution for another protocol. Configure redistribution for each protocol that makes sense for your network.

Step 15 Click **OK**.

Monitoring EIGRP

You can use the following commands to monitor the EIGRP routing process. For examples and descriptions of the command output, see the command reference.

- **show eigrp events** [{*start end*} | **type**]

  Displays the EIGRP event log.

- **show eigrp interfaces** [*if-name*] [**detail**]

  Displays the interfaces participating in EIGRP routing.

- **show eigrp neighbors** [**detail** | **static**] [*if-name*]

  Displays the EIGRP neighbor table.

- **show eigrp topology** [*ip-addr* [*mask*] | **active** | **all-links** | **pending** | **summary** | **zero-successors**]

  Displays the EIGRP topology table.

- **show eigrp traffic**

  Displays EIGRP traffic statistics.