



Service Selection Gateway Commands

This chapter presents the commands for configuring and maintaining Cisco IOS Service Selection Gateway (SSG) applications. The commands are presented in alphabetical order.

address-pool

To define local IP pools that are to be used by Service Selection Gateway (SSG) to assign IP addresses to users for which SSG is acting as a RADIUS client, use the **address-pool** command in SSG-radius-proxy configuration mode. To remove a local IP pool, use the **no** form of this command.

address-pool *start-ip end-ip* [**domain** *domain-name*]

no address-pool *start-ip end-ip* [**domain** *domain-name*]

Syntax Description

| | |
|--------------------|---|
| <i>start-ip</i> | First IP address of the local IP address pool. |
| <i>end-ip</i> | Last IP address of the local IP address pool. |
| domain | (Optional) IP address pool for a specific domain. |
| <i>domain-name</i> | (Optional) Name of the domain. |

Defaults

SSG does not assign IP addresses from a local IP pool.

Command Modes

SSG-radius-proxy configuration

Command History

| Release | Modification |
|-----------|--|
| 12.2(4)B | This command was introduced. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2 T. |

Usage Guidelines

Use this command to configure SSG to assign an IP address taken from a local pool to a user for which SSG is acting as a RADIUS client. SSG assigns an IP address from a local pool only when one has not been assigned by one of the following methods:

- Assignment in the Access-Accept from the AAA server
- Assignment in the Access-Request received from the client
- Assignment from an Autodomain service (tunnel or proxy) that does not have the **auto-domain nat user-address** configuration enabled



Note

You must have SSG Autodomain configured in order for an IP address to be assigned from an Autodomain tunnel. See [SSG AutoDomain](#) for more information about configuring SSG Autodomain.

You can use this command to define a global local IP address pool or an IP address pool for a specific domain by using the **domain** keyword. You cannot create pools with more than 20,000 addresses.



Note

Using IP address pools within SSG is completely standalone and unrelated to Cisco IOS IP local pools.

Examples

The following example shows how to configure a local IP address pool for SSG:

```
address-pool 172.16.16.0 172.16.20.0
```

The following example shows how to configure a local IP address pool for the domain named “cisco”.

```
address-pool 172.21.21.0 172.21.25.0 domain cisco
```

Related Commands

| Command | Description |
|--|---|
| clear ssg radius-proxy client-address | Clears all hosts connected to a specific RADIUS client. |
| clear ssg radius-proxy nas-address | Clears all hosts connected to a specific NAS. |
| forward accounting-start-stop | Proxies accounting start, stop, and update packets generated by any RADIUS clients to the AAA server. |
| idle-timeout (SSG) | Configures a host object timeout value. |
| server-port | Defines the ports for the SSG RADIUS proxy. |
| show ssg tcp-redirect group | Displays the pool of IP addresses configured for a router or a specific domain. |
| ssg enable | Enables SSG. |
| ssg radius-proxy | Enables SSG RADIUS Proxy. |
| ssg tcp-redirect | Configures the RADIUS proxy IP address and shared secret. |

attribute

To configure an attribute in a local service profile, use the **attribute** command in profile configuration mode. To delete an attribute from a service profile, use the **no** form of this command.

attribute *radius-attribute-id* [*vendor-id*] [*cisco-vsa-type*] *attribute-value*

no attribute *radius-attribute-id* [*vendor-id*] [*cisco-vsa-type*] *attribute-value*

Syntax Description

| | |
|----------------------------|--|
| <i>radius-attribute-id</i> | RADIUS attribute ID to be configured. |
| <i>vendor-id</i> | (Optional) Vendor ID. Required if the RADIUS attribute ID is 26, indicating a vendor-specific attribute (VSA). The Cisco vendor ID is 9. |
| <i>cisco-vsa-type</i> | (Optional) Cisco VSA type. Required if the vendor ID is 9, indicating a Cisco VSA. |
| <i>attribute-value</i> | Attribute value. The following optional attribute values are also supported: <ul style="list-style-type: none"> Linterval—Required to change an interim accounting interval. Specifies the new accounting interval in seconds. Q—Configures the token bucket parameters for the Service Selection Gateway (SSG) Hierarchical Policing feature. |

Defaults

For the **Linterval** option: If the L option is not defined, the accounting records for a service profile will be sent at the interval configured by the **ssg accounting interval** command. If the **ssg accounting interval** command is not set, the accounting records are sent every 600 seconds.

Otherwise, no default behavior or values are set.

Command Modes

Profile configuration

Command History

| Release | Modification |
|-----------|---|
| 12.0(3)DC | This command was introduced on the Cisco 6400 NRP. |
| 12.2(4)B | The L and Q attributes were introduced as an <i>attribute-value</i> . |
| 12.2(8)T | This command was integrated into Cisco IOS Release 12.2(8)T. |
| 12.2(13)T | This command was modified for Cisco IOS Release 12.2(13)T. |

Usage Guidelines

Use this command to configure attributes in local service profiles.

For the SSG Open Garden feature, use this command to configure the Service Route, DNS Server Address, and Domain Name attributes in a local service profile before adding the service to the open garden.

To change the SSG accounting interval for a service profile, use the *Linterval* option in the **attribute** command. For example, if L80 is entered as the attribute value, the service profile sends accounting information every 80 seconds. Interim accounting can be disabled by entering the value (in seconds) as 0 (for instance, L0). When interim accounting is disabled, the normal accounting stops and starts are still sent.

For the SSG Hierarchical Policing feature, use the Q option to configure the token bucket parameters (token rate, normal burst, and excess burst). The syntax for the Q option is as follows:

```
Router(config-prof)# attribute radius-attribute-id vendor-id cisco-vs-a-type
"QU;upstream-committed-rate;upstream-normal-burst;
[upstream-excess-burst];D;downstream-committed-rate;
downstream-normal-burst;[downstream-excess-burst]"
```

The variables are used to configure upstream (U) and downstream (D) policing. The upstream traffic is the traffic that travels from the subscriber to the network, and the downstream traffic is the traffic that travels from the network to the subscriber.

Examples

In the following example, the Cisco AV pair Upstream Access Control List (inacl) attribute is configured in the local service profile called "cisco.com":

```
Router(config)# local-profile cisco.com
Router(config-prof)# attribute 26 9 1 "ip:inacl#101=deny tcp 10.2.1.0 0.0.0.255 any eq 21"
```

In the following example, the Session-Timeout attribute is deleted from the local service profile called "cisco.com":

```
Router(config)# local-profile cisco.com
Router(config-prof)# no attribute 27 600
```

In the following example, the local profile cisco.com is configured to send an interim accounting update every 90 seconds:

```
Router(config)# local-profile cisco.com
Router(config-prof)# attribute 26 9 1 "L90"
```

In the following example, the SSG Hierarchical Policing parameters are set for upstream and downstream traffic:

```
Router(config)# local-profile cisco.com
Router(config-prof)# attribute 26 9 251 "QU:8000:16000:20000:D10000:20000:30000"
```

In the following example, an open garden service called "opencisco.com" is defined.

```
Router(config)# local-profile opencisco.com
Router(config-prof)# attribute 26 9 251 "Oopengarden1.com"
Router(config-prof)# attribute 26 9 251 "D10.13.1.5"
Router(config-prof)# attribute 26 9 251 "R10.1.1.0;255.255.255.0"
Router(config-prof)# exit
Router(config)# ssg open-garden opencisco.com
```

Related Commands

| Command | Description |
|----------------------------|--|
| debug ssg data | Displays SSG QoS information. |
| local-profile | Configures a local service profile. |
| show ssg connection | Displays information about a particular SSG connection, including the policing parameters. |

| Command | Description |
|--------------------------------|---|
| show ssg host | Displays information about an SSG host, including whether policing is enabled or disabled and the policing configurations of a particular host. |
| show ssg open-garden | Displays a list of all configured open garden services. |
| ssg accounting interval | Specifies the interval at which accounting updates are sent to the server. |
| ssg open-garden | Designates a service, defined in a local service profile, to be an open garden service. |
| ssg qos police | Enables SSG Hierarchical Policing on a router. |

clear ssg connection

To remove the connections of a given host and a service name, use the **clear ssg connection** command in privileged EXEC mode.

```
clear ssg connection ip-address service-name [interface]
```

Syntax Description

| | |
|---------------------|---|
| <i>ip-address</i> | IP address of an active Service Selection Gateway (SSG) connection. |
| <i>service-name</i> | Name of an active SSG connection. |
| <i>interface</i> | (Optional) Interface to which the host is connected. |

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|-----------|---|
| 12.0(3)DC | This command was introduced on the Cisco 6400 node route processor. |
| 12.2(2)B | The <i>interface</i> argument was added. |
| 12.2(4)B | This command was integrated into Cisco IOS Release 12.2(4)B. |
| 12.2(8)T | This command was integrated into Cisco IOS Release 12.2(8)T. |

Examples

The following example shows how to remove the service connection for “Service1” to host 192.168.1.1, connected through Fast Ethernet:

```
Router# clear ssg connection 192.168.1.1 fastethernet Service1
```

Related Commands

| Command | Description |
|----------------------------|--|
| show ssg connection | Displays the connections of a given host and a service name. |

clear ssg host

To remove a Service Selection Gateway (SSG) host object or a range of host objects, use the **clear ssg host** command in privileged EXEC mode. The command syntax of the **clear ssg host** command depends on whether the SSG port-bundle host key has been enabled with the **ssg port-map** global configuration command.

SSG Host Key Is Not Enabled

```
clear ssg host {all | range start-ip-address end-ip-address}
```

SSG Host Key Is Enabled

```
clear ssg host {all | ip-address | range [start-ip-address end-ip-address [interface]]}
```

Syntax Description

| | |
|-------------------------|---|
| all | Clears all SSG host objects. |
| <i>ip-address</i> | Clears the specified SSG host object. This option is available only when SSG host key functionality is enabled. |
| range | Clears a specified range of SSG host objects. |
| <i>start-ip-address</i> | Host IP address. This argument specifies the beginning of an IP address range if you follow it with an <i>end-ip-address</i> value. |
| <i>end-ip-address</i> | (Optional) Host IP address that is used with the <i>ip-address</i> argument to specify a range of host objects. |
| <i>interface</i> | (Optional) SSG downlink interface through which the host or subscriber is connected, such as ATM, Fast Ethernet, or Virtual-Access. For more information, use the question mark (?) online help function. |

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|-----------|---|
| 12.0(3)DC | This command was introduced on the Cisco 6400 node route processor. |
| 12.2(2)B | The <i>interface</i> argument was added for the SSG Host Key feature. |
| 12.2(8)T | This command was integrated into Cisco IOS Release 12.2(8)T. |
| 12.2(15)B | This command was modified by the introduction of <ul style="list-style-type: none"> • Syntax dependence on SSG host key • The <i>start-ip-address</i> and <i>end-ip-address</i> arguments • The all keyword |
| 12.2(15)T | The modifications made in release 12.2(15)B were integrated into Cisco IOS Release 12.2(15)T. |

Usage Guidelines

Use this command to remove one, all, or a range of SSG host objects. You can specify the host objects to remove by entering the host IP addresses or the SSG downlink interface through which the subscriber is connected.

**Note**

The system deletes the specified host objects that exist *at the time* that you enter this command. The system may not delete host objects that are created *after* you enter the command or while the system is executing the command. Enter the **show ssg host** command to confirm that all specified host objects have been deleted.

You can specify the SSG downlink interface only when the SSG Host Key feature is enabled. To enable the host key, enter the **ssg port-map** command in global configuration mode. To disable the host key, enter the **no ssg port-map** command.

**Note**

The **ssg port-map** command does not take effect until after the router is reloaded.

Examples**SSG Port-Bundle Host Key Is Not Enabled**

The following example shows how to delete host objects for a range of IP addresses:

```
Router# clear ssg host range 10.0.0.2 10.0.0.20
```

The following example shows how to delete all host objects:

```
Router# clear ssg host all
```

SSG Port-Bundle Host Key Is Enabled

The following example shows how to delete all host objects:

```
Router# clear ssg host all
```

The following example shows how to delete all host objects for subscribers connected through IP address 10.0.0.2:

```
Router# clear ssg host 10.0.0.2
```

The following example shows how to delete host objects for a specific range of IP addresses:

```
Router# clear ssg host range 10.0.0.2 10.0.0.20
```

The following example shows how to delete host objects for a specific IP address range and interface:

```
Router# clear ssg host range 10.0.0.2 10.0.0.20 FastEthernet 0/0
```

Related Commands

| Command | Description |
|----------------------|--|
| show ssg host | Displays information about a subscriber and current connections of the subscriber. |
| ssg port-map | Enables the SSG port-bundle host key. |

clear ssg next-hop

To remove a next-hop table, use the **clear ssg next-hop** command in privileged EXEC mode.

```
clear ssg next-hop
```

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 12.0(3)DC | This command was introduced on the Cisco 6400 node route processor. |
| | 12.2(4)B | This command was integrated into Cisco IOS Release 12.2(4)B. |
| | 12.2(8)T | This command was integrated into Cisco IOS Release 12.2(8)T. |

Usage Guidelines If you use this command to clear the next-hop table, nothing appears when you use the **show ssg next-hop** command. However, the next-hop table will still appear in the running configuration. To remove the next-hop table from the running configuration, use the **no** form of the **ssg next-hop download** command.

Examples The following example shows how to remove the next-hop table:

```
Router# clear ssg next-hop
```

| Related Commands | Command | Description |
|------------------|------------------------------|--|
| | show ssg next-hop | Displays the next-hop table. |
| | ssg next-hop download | Downloads the next-hop table from a RADIUS server. |

clear ssg open-garden

To remove open garden configurations and all open garden service objects, use the **clear ssg open-garden** command in privileged EXEC mode.

```
clear ssg open-garden
```

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|-----------|--|
| 12.1(5)DC | This command was introduced on the Cisco 6400 series node route processor. |
| 12.2(4)B | This command was integrated into Cisco IOS Release 12.2(4)B. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |

Usage Guidelines

This command removes the open garden configuration by deleting all instances of the **ssg open-garden** global configuration command. This command also removes the service object of all the open garden services. The local service profiles of the open garden services are not deleted from the configuration.

Examples

In the following example, all open garden services are displayed and then removed:

```
Router# show ssg open-garden
```

```
nrp1-nrp2_og1
nrp1-nrp2_og2
nrp1-nrp2_og3
nrp1-nrp2_og4
```

```
Router# clear ssg open-garden
Router# show ssg open-garden
Router#
```

Related Commands

| Command | Description |
|-----------------------------|--|
| local-profile | Configures a local service profile. |
| show ssg open-garden | Displays a list of all configured open garden services. |
| ssg open-garden | Designates a service, defined in a local service profile, as an open garden service. |

clear ssg pass-through-filter

To remove the downloaded filter for transparent pass-through, use the **clear ssg pass-through-filter** command in privileged EXEC mode.

clear ssg pass-through-filter

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 12.0(3)DC | This command was introduced on the Cisco 6400 node route processor. |
| | 12.2(4)B | This command was integrated into Cisco IOS Release 12.2(4)B. |
| | 12.2(8)T | This command was integrated into Cisco IOS Release 12.2(8)T. |

Usage Guidelines Removing the filter allows unauthenticated traffic to pass through the Service Selection Gateway in either direction without modification. If you use this command to clear the downloaded transparent pass-through filter, nothing will be displayed when you use the **show ssg pass-through-filter** command. However, the transparent pass-through filter will still appear in the running configuration. To remove the transparent pass-through filter from the running configuration, use the **no** form of the **ssg pass-through** command.

Examples The following example shows how to remove the downloaded transparent pass-through filter:

```
Router# clear ssg pass-through-filter
```

| Related Commands | Command | Description |
|------------------|-------------------------------------|--|
| | show ssg pass-through-filter | Displays the downloaded filter for transparent pass-through. |
| | ssg pass-through | Enables transparent pass-through. |

clear ssg pending-command

To remove all pending commands, use the **clear ssg pending-command** command in privileged EXEC mode.

```
clear ssg pending-command
```

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 12.0(3)DC | This command was introduced on the Cisco 6400 node route processor. |
| | 12.2(4)B | This command was integrated into Cisco IOS Release 12.2(4)B. |
| | 12.2(8)T | This command was integrated into Cisco IOS Release 12.2(8)T. |

Usage Guidelines Use this command to clear pending commands.

Examples The following example shows how to clear pending commands:

```
Router# clear ssg pending-command
```

| Related Commands | Command | Description |
|------------------|---------------------------------|------------------------------------|
| | show ssg pending-command | Displays current pending commands. |

clear ssg prepaid default-quota

To clear the Service Selection Gateway (SSG) prepaid default quota counters, use the **clear ssg prepaid default-quota** command in privileged EXEC mode.

clear ssg prepaid default-quota

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|-----------|------------------------------|
| | 12.3(11)T | This command was introduced. |

Usage Guidelines SSG maintains two counters to keep track of the number of times the SSG prepaid default quota has been allotted. One counter is for the total number of default quotas allotted by SSG (irrespective of how many times the prepaid server has become available and unavailable). The other counter keeps track of the number of default quotas allotted by SSG during the latest instance of prepaid server unavailability. The **clear ssg prepaid default-quota** command clears the SSG default quota counters.

The **show ssg prepaid default-quota** command displays the number of default quotas that SSG has allocated since the last time the **clear ssg prepaid default-quota** command was entered.

Examples The following example shows how to clear the default quota counter for all quotas allocated by SSG:

```
Router# clear ssg prepaid default-quota
```

| Related Commands | Command | Description |
|------------------|---------------------------------------|--|
| | show ssg prepaid default-quota | Displays the values of the SSG prepaid default quota counters. |

clear ssg radius-proxy client-address

To clear all hosts connected to a specific RADIUS client, use the **clear ssg radius-proxy client-address** command in privileged EXEC mode.

```
client ssg radius-proxy client-address ip-address
```

Syntax Description

| | |
|-------------------|--------------------------------|
| <i>ip-address</i> | IP address of a RADIUS client. |
|-------------------|--------------------------------|

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|-----------|---|
| 12.2(4)B | This command was introduced. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |

Usage Guidelines

Use this command to clear all hosts connected to a specific RADIUS client. This command deactivates and destroys all host objects associated with the specified RADIUS client.

Examples

The following example shows how to clear all hosts connected to the RADIUS client that has the IP address 172.16.0.0:

```
clear ssg radius-proxy client-address 172.16.0.0
```

Related Commands

| Command | Description |
|---|--|
| address-pool | Defines local IP pools to be used by SSG to assign IP addresses to users for which SSG is acting as a RADIUS client. |
| clear ssg radius-proxy nas-address | Clears all hosts connected to a specific NAS. |
| idle-timeout (SSG) | Configures a host object timeout value. |
| show ssg tcp-redirect group | Displays the pool of IP addresses configured for a router or for a specific domain. |
| ssg enable | Enables SSG. |
| ssg radius-proxy | Enables SSG RADIUS Proxy. |
| ssg tcp-redirect | Configures the RADIUS proxy IP address and shared secret. |

clear ssg radius-proxy nas-address

To clear all hosts connected to a specific network access server (NAS), use the **clear ssg radius-proxy nas-address** command in privileged EXEC mode.

client ssg radius-proxy nas-address *ip-address*

Syntax Description

| | |
|-------------------|--------------------------------|
| <i>ip-address</i> | IP address of a RADIUS client. |
|-------------------|--------------------------------|

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|-----------|---|
| 12.2(4)B | This command was introduced. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |

Usage Guidelines

Use this command to clear all hosts connected to a specific NAS. This command deactivates and destroys all host objects associated with the specified NAS client.



Note

Service Selection Gateway (SSG) does not currently notify RADIUS clients when a host object is removed from the SSG.

Examples

The following example shows how to clear all hosts connected to the NAS with IP address 172.16.0.0:

```
clear ssg radius-proxy nas-address 172.16.0.0
```

Related Commands

| Command | Description |
|---|--|
| address-pool | Defines local IP pools to be used by SSG to assign IP addresses to users for which SSG is acting as a RADIUS client. |
| clear ssg radius-proxy nas-address | Clears all hosts connected to a specific RADIUS client. |
| forward accounting-start-stop | Proxies accounting start, stop, and update packets generated by any RADIUS clients to the AAA server. |
| idle-timeout (SSG) | Configures a host object timeout value. |
| server-port | Defines the ports for the SSG RADIUS proxy. |
| show ssg tcp-redirect group | Displays the pool of IP addresses configured for a router or for a specific domain. |
| ssg enable | Enables SSG. |
| ssg radius-proxy | Enables SSG RADIUS Proxy. |
| ssg tcp-redirect | Configures the RADIUS proxy IP address and shared secret. |

clear ssg service

To remove a service object and all connection objects of the service, use the **clear ssg service** command in privileged EXEC mode.

```
clear ssg service {service-name | all}
```

Syntax Description

| | |
|---------------------|-----------------------------|
| <i>service-name</i> | Service name. |
| all | Clears all service objects. |

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|-----------|---|
| 12.0(3)DC | This command was introduced on the Cisco 6400 node route processor. |
| 12.2(4)B | This command was integrated into Cisco IOS Release 12.2(4)B. |
| 12.2(8)T | This command was integrated into Cisco IOS Release 12.2(8)T. |
| 12.2(15)B | The all keyword was added. |
| 12.2(15)T | The all keyword was integrated into Cisco IOS Release 12.2(15)T. |

Usage Guidelines

Use this command to remove one or all service objects and all connection objects of the services.



Note

When you use the **all** keyword, the system deletes all service objects that exist *at the time* that you enter this command. The system may not delete service objects that are created *after* you enter the command or while the system is executing the command. Enter the **show ssg service** command to confirm that all service objects have been deleted.

Examples

The following example show how to remove all service objects and connections:

```
Router# clear ssg service all
```

The following example shows how to remove a service called “Perftest”:

```
Router# clear ssg service Perftest
```

Related Commands

| Command | Description |
|-------------------------|---|
| show ssg binding | Displays service names that have been bound to interfaces and the interfaces to which they have been bound. |
| show ssg service | Displays the information for a service. |
| ssg bind service | Specifies the interface for a service. |

clear ssg user transparent all

To delete all Service Selection Gateway (SSG) transparent autologon transparent pass-through (TP), suspect (SP), unidentified (NR), and authorizing (WA) users, use the **clear ssg user transparent all** command in privileged EXEC mode.

clear ssg user transparent all

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|------------|--|
| | 12.3(1a)BW | This command was introduced. |
| | 12.3(3)B | This command was integrated into Cisco IOS Release 12.3(3)B. |
| | 12.3(7)T | This command was integrated into Cisco IOS Release 12.3(7)T. |

Usage Guidelines Use this command to clear all SSG transparent autologon users, including pass-through (TP), suspect (SP), unidentified (NR), and authorizing (WA) users.

Examples The following example deletes all TP, SP, NR, and WA users:

```
Router# clear ssg user transparent all
```

| Related Commands | Command | Description |
|------------------|------------------------------|--|
| | ssg login transparent | Enables the SSG Transparent Autologon feature. |

clear ssg user transparent passthrough

To delete Service Selection Gateway (SSG) transparent autologon transparent pass-through (TP) users, use the **clear ssg user transparent passthrough** command in privileged EXEC mode.

```
clear ssg user transparent passthrough {all | ip-address}
```

Syntax Description

| | |
|-------------------|---|
| all | Deletes all pass-through user entries. |
| <i>ip-address</i> | Deletes the entry for the specified IP address. |

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|------------|--|
| 12.3(1a)BW | This command was introduced. |
| 12.3(3)B | This command was integrated into Cisco IOS Release 12.3(3)B. |
| 12.3(7)T | This command was integrated into Cisco IOS Release 12.3(7)T. |

Examples

The following example deletes all pass-through user entries:

```
Router# clear ssg user transparent passthrough all
```

Related Commands

| Command | Description |
|------------------------------|--|
| ssg login transparent | Enables the SSG Transparent Autologon feature. |

clear ssg user transparent suspect

To delete Service Selection Gateway (SSG) transparent autologon suspect (SP) user entries, use the **clear ssg user transparent suspect** command in privileged EXEC mode.

```
clear ssg user transparent suspect {all | ip-address}
```

Syntax Description

| | |
|-------------------|---|
| all | Deletes all suspect user entries. |
| <i>ip-address</i> | Deletes the entry for the specified IP address. |

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|------------|--|
| 12.3(1a)BW | This command was introduced. |
| 12.3(3)B | This command was integrated into Cisco IOS Release 12.3(3)B. |
| 12.3(7)T | This command was integrated into Cisco IOS Release 12.3(7)T. |

Usage Guidelines

An SSG transparent autologon suspect (SP) user is a user whose authentication, authorization, and accounting (AAA) authorization resulted in an Access Reject.

Examples

The following example deletes all suspect user entries:

```
Router# clear ssg user transparent suspect
```

Related Commands

| Command | Description |
|------------------------------|--|
| ssg login transparent | Enables the SSG Transparent Autologon feature. |

clear ssg user transparent unidentified

To delete all Service Selection Gateway (SSG) transparent autologon unidentified user (NR) entries, use the **clear ssg user transparent unidentified** command in privileged EXEC mode.

```
clear ssg user transparent unidentified {all | ip-address}
```

Syntax Description

| | |
|-------------------|---|
| all | Deletes all unidentified user entries. |
| <i>ip-address</i> | Deletes the entry for the specified IP address. |

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|------------|--|
| 12.3(1a)BW | This command was introduced. |
| 12.3(3)B | This command was integrated into Cisco IOS Release 12.3(3)B. |
| 12.3(7)T | This command was integrated into Cisco IOS Release 12.3(7)T. |

Examples

The following example clears all unidentified user entries:

```
Router# clear ssg user transparent unidentified all
```

Related Commands

| Command | Description |
|------------------------------|--|
| ssg login transparent | Enables the SSG Transparent Autologon feature. |

client-address

To configure a RADIUS client to proxy requests from a specified IP address to a RADIUS server and to enter SSG-radius-proxy-client configuration mode, use the **client-address** command in SSG-radius-proxy configuration mode. To remove a client from the client list, use the **no** form of this command.

client-address *ip-address* [**vrf** *vrf-name*]

no client-address *ip-address*

Syntax Description

| | |
|----------------------------|--|
| <i>ip-address</i> | IP address of a RADIUS client. |
| vrf <i>vrf-name</i> | (Optional) Associates a configured VRF with a RADIUS client. |

Defaults

No default behavior or values.

Command Modes

SSG-radius-proxy configuration

Command History

| Release | Modification |
|-----------|---|
| 12.2(4)B | This command was introduced. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |
| 12.2(15)B | This command was modified to enter SSG-radius-proxy-client mode. |
| 12.3(4)T | The modifications from 12.2(15)B were integrated into Cisco IOS Release 12.3(4)T. |
| 12.3(11)T | The vrf <i>vrf-name</i> option was introduced. |

Usage Guidelines

Use this command to configure the RADIUS client to proxy requests from a specified IP address to a RADIUS server. You can also use this command to enter SSG-radius-proxy-client mode.

Examples

The following example shows how to enter SSG-radius-proxy-client mode:

```
client-address 172.16.0.0
```

The following example shows how to configure a RADIUS client to proxy all requests from IP address 172.16.0.0 to the RADIUS server and assigns the shared secret "cisco" to the client:

```
client-address 172.16.0.0
key cisco
```

The following example defines a RADIUS client that is connected to SSG through a VRF called "BLUE":

```
ip vrf BLUE
```

```

rd 1:1
!
ssg radius-proxy
  client-address 10.1.1.1 vrf BLUE
  key cisco
!

```

Related Commands

| Command | Description |
|---|---|
| address-pool | Defines local IP pools to be used by SSG to assign IP addresses to users for whom SSG is acting as a RADIUS client. |
| clear ssg radius-proxy client-address | Clears all hosts connected to a specific RADIUS client. |
| host-route insert | Inserts a host route via the RADIUS client address into the VRF configured for the RADIUS client. |
| key (SSG-radius-proxy-client) | Configures the shared secret between SSG and a RADIUS client. |
| server-port | Configures the ports on which SSG listens for RADIUS-requests from configured RADIUS clients. |
| session-identifier (SSG-radius-proxy-client) | Overrides SSG's automatic RADIUS client session identification. |
| show ssg radius-proxy | Displays the pool of IP addresses configured for a router or for a specific domain. |
| ssg radius-proxy | Enables SSG RADIUS Proxy and enters SSG-radius-proxy mode. |

destination access-list

To specify packets for port-mapping by specifying an access list to compare against the subscriber traffic, use the **destination access-list** command in SSG portmap configuration mode. To remove this specification, use the **no** form of this command.

destination access-list *access-list-number*

no destination access-list *access-list-number*

Syntax Description

access-list-number Integer from 100 to 199 that is the number or name of an extended access list.

Defaults

SSG does not use an access list when port-mapping subscriber traffic.

Command Modes

SSG portmap configuration

Command History

| Release | Modification |
|-----------|---|
| 12.2(16)B | This command was introduced. This command replaces the ssg port-map destination access-list command. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T. |

Usage Guidelines

When the **destination access-list** command is configured, any traffic going to the default network and matching the access list will be port-mapped.



Note A default network must be configured and routable from SSG in order for this command to be effective.

You can use multiple entries of the **destination access-list** command. The access lists are checked against the subscriber traffic in the order in which they are defined.

Examples

In the following example, SSG will port-map packets that are permitted by access list 100:

```
ssg port-map
 destination access-list 100
 source ip Ethernet0/0/0
 !
 .
 .
 !
 access-list 100 permit ip 10.0.0.0 0.255.255.255 host 70.13.6.100
 access-list 100 deny ip any any
```

Related Commands

| Command | Description |
|---------------------|---|
| destination range | Identifies packets for port-mapping by specifying the TCP port range to compare against the subscriber traffic. |
| ssg port-map | Enables the SSG port-bundle host key and enters SSG portmap configuration mode. |

destination range

To identify packets for port-mapping by specifying the TCP port range to compare against the subscriber traffic, use the **destination range** command in SSG portmap configuration mode. To remove this specification, use the **no** form of this command.

destination range *port-range-start to port-range-end* [**ip** *ip-address*]

no destination range *port-range-start to port-range-end* [**ip** *ip-address*]

Syntax Description

| | |
|-----------------------------|---|
| <i>port-range-start</i> | Port number at the start of the TCP port range. |
| <i>to</i> | Specifies higher end of TCP port range. |
| <i>port-range-end</i> | Port number at the end of TCP port range. |
| ip <i>ip-address</i> | (Optional) Destination IP address in the packets. |

Defaults

A TCP port range is not used in port-mapping subscriber traffic.

Command Modes

SSG portmap configuration

Command History

| Release | Modification |
|-----------|---|
| 12.2(16)B | This command was introduced. This command replaces the ssg port-map destination range command. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T. |

Usage Guidelines

If a destination IP address is not configured, a default network must be configured and routable from SSG in order for this command to be effective.

If the destination IP address is not configured, any traffic going to the default network whose destination port falls within the destination port range will be port-mapped.

You can use multiple entries of the **destination range** command. The port ranges are checked against the subscriber traffic in the order in which they were defined.

Examples

In the following example, SSG will port-map any packets that are going to the default network and have a destination port within the range from 8080 to 8081:

```
ssg port-map
 destination range 8080 to 8081
```

Related Commands

| Command | Description |
|-------------------------|--|
| destination access-list | Specifies packets for port-mapping by specifying an access list to compare against the subscriber traffic. |
| ssg port-map | Enables the SSG port-bundle host key and enters SSG portmap configuration mode. |

dnis-prefix all service

To configure the dial-out global service, use the **dnis-prefix all service** command in SSG dial-out configuration mode. To remove a service name and prevent further connections to the specified service, use the **no** form of this command.

dnis-prefix all service *service-name*

no dnis-prefix all service [*service-name*]

Syntax Description

| | |
|---------------------|--------------------------------------|
| <i>service-name</i> | Name of the dial-out global service. |
|---------------------|--------------------------------------|

Defaults

Dial-out global service is not configured.

Command Modes

SSG dial-out configuration

Command History

| Release | Modification |
|-----------|--|
| 12.2(15)B | This command was introduced. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T. |

Usage Guidelines

Use this command to configure the dial-out global service used for users who are doing account logon with a structured username (*user@DNIS*). The service profile is downloaded when the user connects to the dial-out service. You can specify only one dial-out global service. If you configure this command more than once and use different service names each time, the previously configured service name is removed from the configuration.

If SSG is operating in SSG Autodomain basic mode, you should configure the dial-out tunnel service profile as the dial-out global service. If SSG is operating in SSG Autodomain extended mode, you should configure the virtual-user profile as the dial-out global service and configure dial-out tunnel service as an Autologon service within SSG Autodomain extended mode.

Examples

The following example shows how to configure a global dial-out service profile named “profile1” as the global dial-out service profile:

```
dnis-prefix all service profile1
```

The following example shows how to configure a global dial-out service profile when SSG is operating in SSG Autodomain basic mode:

```
dnis-prefix all service dialout_tunnel
```

The following example shows how to configure a global dial-out service profile when SSG is operating in SSG Autodomain extended mode:

```
dnis-prefix all service virtual-user
```

Related Commands

| Command | Purpose |
|--|---|
| download exclude-profile (ssg dial-out) | Downloads the DNIS exclusion list locally or from a AAA server. |
| exclude dnis-prefix | Configures the DNIS filter by adding a DNIS prefix to the DNIS exclusion list. |
| show ssg dial-out exclude-list | Displays information about the DNIS prefix profile and the DNIS exclusion list. |
| ssg dial-out | Enters SSG dial-out configuration mode. |

download exclude-profile (SSG dial-out)

To download the Dialed Number Identification Service (DNIS) exclusion list locally or from a authentication, authorization, and accounting (AAA) server, use the **download exclude-profile** command in SSG dial-out configuration mode. To remove the DNIS exclusion list from the configuration, use the **no** form of this command.

download exclude-profile *profile-name* [*password*]

no download exclude-profile *profile-name* [*password*]

Syntax Description

| | |
|---------------------|---|
| <i>profile-name</i> | Name of the DNIS exclusion list. |
| <i>password</i> | (Optional) Password of the DNIS exclusion list. |

Defaults

A DNIS exclusion list is not downloaded.

Command Modes

SSG dial-out configuration

Command History

| Release | Modification |
|-----------|---|
| 12.2(15)B | This command was introduced. |
| 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |

Usage Guidelines

Use this command to download a DNIS exclusion list from the local profile configured in Service Selection Gateway (SSG) or from a AAA server. If you do not specify a profile name and password, SSG attempts to download the profile with the previously configured profile name and password. If there is no previously configured profile name and password, the DNIS exclusion list is not downloaded.

You can download only one DNIS exclusion list. If you attempt to use the **download exclude-profile** command more than once with different profile names, only the last profile name is downloaded, and the previously downloaded profiles are removed from the configuration.

Use the **no download exclude-profile** command to remove the downloaded DNIS exclusion list from the configuration.

You can configure the order in which SSG searches for the DNIS exclusion list using the **ssg service-search-order** command.

Examples

The following example shows how to download a DNIS exclusion list with a profile name of “dnisprofile1” and a password of “abc”:

```
download exclude-profile dnisprofile1 abc
```

Related Commands

| Command | Description |
|---------------------------------------|--|
| dnis-prefix all service | Configures the dial-out global service. |
| exclude dnis-prefix | Configures the DNIS filter by adding a DNIS prefix to the DNIS exclusion list. |
| show ssg dial-out exclude-list | Displays information about the DNIS exclusion list. |
| ssg dial-out | Enters SSG dial-out configuration mode. |
| ssg service-search-order | Specifies the order in which SSG searches for a service profile. |

download exclude-profile (SSG PTA-MD)

To download a PPP Termination Aggregation-Multidomain (PTA-MD) exclusion list from the authentication, authorization, and accounting (AAA) server to the router, use the **download exclude-profile** command in SSG PTA-MD configuration mode. To remove all domains in the specified PTA-MD exclusion list, use the **no** form of this command.

download exclude-profile *profile-name* [*password*]

no download exclude-profile *profile-name* [*password*]

Syntax Description

| | |
|---------------------|---|
| <i>profile-name</i> | Name of the exclusion list to download. |
| <i>password</i> | (Optional) Password required to download the PTA-MD exclusion list from the AAA server. If no password is entered, the password used in the previous exclusion list download will be used to download the exclusion list. |

Defaults

A PTA-MD exclusion list is not downloaded.

Command Modes

SSG PTA-MD configuration

Command History

| Release | Modification |
|-----------|---|
| 12.2(15)B | This command was introduced. |
| 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |

Usage Guidelines

A PTA-MD exclusion list provides the option of passing the entire structured username in the form *user@service* to PPP for authenticating an SSG request. The entire structured username can be passed to PPP through the use of a PTA-MD exclusion list; if an entire structured username should be passed to PPP, the domain (the *@service* portion of the structured username) should be added to a PTA-MD exclusion list. The **download exclude-profile** command is used to download an exclusion list from the AAA server as part of the process for adding domains to an exclusion list using the router command-line interface (CLI).

PTA-MD exclusion lists can also be configured directly on the AAA server.

Examples

Adding Domains to an Existing PTA-MD Exclusion List

In the following example, a PTA-MD exclusion list that already includes “cisco”, “motorola”, “nokia”, and “voice-stream” is downloaded from the AAA server. After the exclusion list is downloaded, “microsoft” and “sun” are added to the exclusion list.

The exclusion list currently on the AAA server includes “cisco”, “motorola”, “nokia”, and “voice-stream”:

```

user = pta_md{
profile_id = 119
profile_cycle = 2
member = SSG-DEV
radius=6510-SSG-v1.1 {
check_items= {
2=cisco
}
reply_attributes= {
9,253="XPcisco"
9,253="XPmotorola"
9,253="XPnokia"
9,253="XPvoice-stream"
}
}

```

The PTA-MD exclusion list is then downloaded to the router from the AAA server. The password to download the exclusion list is “cisco”. After the PTA-MD exclusion list is downloaded, “microsoft” and “sun” are added to the list using the router CLI:

```

ssg multidomain ppp
download exclude-profile pta_md cisco
exclude domain microsoft
exclude domain sun

```

The enhancements to the exclusion list are then verified:

```
Router# show ssg multidomain ppp exclude-list
```

```

Profile name :pta_md
1  cisco
2  motorola
3  nokia
4  voice-stream

Domains added via CLI :
1  microsoft
2  sun

```

Related Commands

| Command | Description |
|---------------------------------------|---|
| exclude (SSG PTA-MD) | Adds a domain name to the existing PTA-MD exclusion list. |
| show ssg multidomain ppp exclude-list | Displays the contents of the PTA-MD exclusion list. |
| ssg multidomain ppp | Enters PTA-MD configuration mode. |

download exclude-profile (SSG-auto-domain)

To add domain names or Access Point Names (APNs) to the Service Selection Gateway (SSG) Autodomain exclusion list, use the **download exclude-profile** command in SSG-auto-domain configuration mode. To remove a name from the Autodomain exclusion list, use the **no** form of this command.

download exclude-profile *profile-name password*

no download exclude-profile *profile-name password*

Syntax Description

| | |
|---------------------|---|
| <i>profile-name</i> | Name for a list of excluded names that may be downloaded from the authentication, authorization, and accounting (AAA) server. |
| <i>password</i> | Password for a list of excluded names that may be downloaded from the AAA server. |

Defaults

No default behavior or values.

Command Modes

SSG-auto-domain configuration

Command History

| Release | Modification |
|-----------|---|
| 12.2(4)B | This command was introduced. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |

Usage Guidelines

Use the **download exclude-profile** command to specify the name and password for a list of names that are excluded from being downloaded from the AAA server. Downloads from the AAA server occur at the time of entering the configuration and also on subsequent Route Processor reloads. By reentering the configuration command, you can synchronize with a modified table on the AAA server by forcing a new download. For every successful exclude-profile download, Service Selection Gateway (SSG) deletes the exclude entries added by the previous exclude-profile download and adds the new downloaded entries to the Autodomain exclusion list. The excluded name list introduces the following new attributes to the SSG Control-Info vendor-specific attributes (VSAs):

X—Excluded name list entry.

A—Add this name to the APN exclusion list.

D—Add this name to the domain name exclusion list.

The following is an example profile using the new exclusion list attributes:

```
abc Password = "cisco" Service-Type = Outbound
Control-Info = XAapn1.gprs
Control-Info = XAapn2.com
Control-Info = XDcisco.com
Control-Info = XDcompany.com
```

Examples

The following example shows how to add a list of names called “abc” with the password “cisco” to the Autodomain exclusion list:

```
download exclude-profile abc cisco
```

Related Commands

| Command | Description |
|---|--|
| exclude | Configures the Autodomain exclusion list. |
| mode extended | Enables extended mode for SSG Autodomain. |
| nat user-address | Enables Network Address Translation (NAT) on Autodomain tunnel service. |
| select | Configures the Autodomain selection mode. |
| show ssg auto-domain exclude-profile | Displays the contents of an Autodomain exclude-profile downloaded from the AAA server. |
| ssg enable | Enables SSG functionality. |

exclude

To add Access Point Names (APNs) and domain names to a Service Selection Gateway (SSG) Autodomain exclusion list, use the **exclude** command in SSG-auto-domain mode. To remove an APN or domain name from the Autodomain exclusion list, use the **no** form of this command.

```
exclude {apn | domain} name
```

```
no exclude {apn | domain} name
```

Syntax Description

| | |
|---------------|--|
| apn | Adds an APN to the exclusion list. |
| domain | Adds a domain to the exclusion list. |
| <i>name</i> | Name of the APN or domain to be added to the exclusion list. |

Defaults

No default behavior or values

Command Modes

SSG-auto-domain

Command History

| Release | Modification |
|-----------|---|
| 12.2(4)B | This command was introduced. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |

Usage Guidelines

Use the **exclude** command to add an APN or a domain to the Autodomain exclusion list. APN and domain names that are not on an exclusion list are used to perform Autodomain for a user. You can use the **no download exclude-profile** command to remove a domain or APN name that is downloaded from the AAA server.

Examples

The following example shows how to add the APN named “abc” to the exclusion list:

```
exclude apn abc
```

The following example shows how to add the domain named “xyz” to the exclusion list:

```
exclude domain xyz
```

Related Commands

| Command | Description |
|-------------------------|---|
| exclude | Adds to the Autodomain download exclusion list. |
| mode extended | Enables extended mode for SSG Autodomain. |
| nat user-address | Enables NAT on Autodomain tunnel service. |
| select | Configures the Autodomain selection mode. |

| Command | Description |
|---|---|
| show ssg auto-domain exclude-profile | Displays the contents of an Autodomain exclude-profile downloaded from the AAA server. |
| ssg enable | Enables SSG functionality. |

exclude (SSG PTA-MD)

To add a domain to a PPP Termination Aggregation-Multidomain (PTA-MD) exclusion list, use the **exclude** command in SSG PTA-MD configuration mode. To remove a domain from the PTA-MD exclusion list, use the **no** form of this command.

exclude [*domain name* | **all-domains**]

no exclude [*domain name* | **all-domains**]

Syntax Description

| | |
|--------------------|--|
| domain | Adds a domain to the exclusion list. |
| <i>name</i> | Name of the domain to be added to the exclusion list. |
| all-domains | Excludes all domains; in effect, disables parsing of PPP structured usernames. |

Defaults

A domain is not included in a PTA-MD exclusion list.

Command Modes

SSG PTA-MD configuration

Command History

| Release | Modification |
|-----------|---|
| 12.2(15)B | This command was introduced in PTA-MD configuration mode. |
| 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |

Usage Guidelines

A PTA-MD exclusion list provides the option of passing an entire structured username in the form *user@service* to PPP for authenticating a Service Selection Gateway (SSG) request. The entire structured username can be passed to PPP through the use of a PTA-MD exclusion list; if an entire structured username should be passed to PPP, the domain (the *@service* portion of the structured username) should be added to a PTA-MD exclusion list. The **exclude** command is used to add a domain to the exclusion list as part of the process for adding domains to an exclusion list using the router command-line interface (CLI).

PTA-MD exclusion lists can also be configured directly on the authentication, authorization, and accounting (AAA) server.

To disable all parsing of PPP structured usernames during authentication, use the **exclude all-domains** command.

Examples

Adding Domains to an Existing PTA-MD Exclusion List

In the following example, a PTA-MD exclusion list that already includes “cisco”, “motorola”, “nokia”, and “voice-stream” is downloaded from the AAA server. After the exclusion list is downloaded, “microsoft” and “sun” are added to the exclusion list.

The exclusion list currently on the AAA server includes “cisco”, “motorola”, “nokia”, and “voice-stream”:

```

user = pta_md{
profile_id = 119
profile_cycle = 2
member = SSG-DEV
radius=6510-SSG-v1.1 {
check_items= {
2=cisco
}
reply_attributes= {
9,253="XPcisco"
9,253="XPmotorola"
9,253="XPnokia"
9,253="XPvoice-stream"
}
}

```

In the following example, the PTA-MD exclusion list is downloaded to the router from the AAA server. The password to download the exclusion list is “cisco”. After the PTA-MD exclusion list is downloaded, “microsoft” and “sun” are added to the list using the router CLI:

```

ssg multidomain ppp
download exclude-profile pta_md cisco
exclude domain microsoft
exclude domain sun

```

The enhancements to the exclusion list are then verified:

```
Router# show ssg multidomain ppp exclude-list
```

```

Profile name :pta_md
1  cisco
2  motorola
3  nokia
4  voice-stream

Domains added via CLI :
1  microsoft
2  sun

```

Disabling Parsing of PPP Structured Usernames

In the following example, parsing of PPP structured usernames is disabled:

```
exclude all-domains
```

| Related Commands | Command | Description |
|------------------|--|--|
| | download exclude-profile (SSG PTA-MD) | Downloads the PTA-MD exclusion list from the AAA server to the router. |
| | show ssg multidomain ppp exclude-list | Displays the contents of the PTA-MD exclusion list. |
| | ssg multidomain ppp | Enters PTA-MD configuration mode. |

exclude dnis-prefix

To configure the Dialed Number Identification Service (DNIS) filter by adding a DNIS prefix to the DNIS exclusion list, use the **exclude dnis-prefix** command in SSG dial-out configuration mode. To remove a DNIS prefix from the DNIS exclusion list, use the **no** form of this command.

exclude dnis-prefix *dnis-prefix*

no exclude dnis-prefix *dnis-prefix*

Syntax Description

| | |
|--------------------|---|
| <i>dnis-prefix</i> | DNIS prefix to be added to the DNIS exclusion list. |
|--------------------|---|

Defaults

No prefix is added

Command Modes

SSG dial-out configuration

Command History

| Release | Modification |
|-----------|---|
| 12.2(15)B | This command was introduced. |
| 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |

Usage Guidelines

Use this command to add a DNIS prefix to the DNIS exclusion list. You can use this command to add multiple DNIS prefixes to the DNIS exclusion list. When a user dials with a DNIS whose prefix is in the DNIS exclusion list, the service logon for that user is rejected.

Examples

The following example adds the DNIS prefix “1122334455” to the DNIS exclusion list:

```
exclude dnis-prefix 1122334455
```

Related Commands

| Command | Description |
|--|---|
| dnis-prefix all service | Configures the dial-out global service. |
| download exclude-profile (SSG dial-out) | Downloads the DNIS exclusion list locally or from a AAA server. |
| show ssg dial-out exclude-list | Displays information about the DNIS prefix profile and the DNIS exclusion list. |
| ssg dial-out | Enters SSG dial-out configuration mode. |

forward accounting-start-stop

To proxy accounting start, stop, and update packets generated by any RADIUS clients to the authentication, authorization, and accounting (AAA) server, use the **forward accounting-start-stop** command in SSG-radius-proxy configuration mode. To stop forwarding accounting start, stop, and update packets, use the **no** form of this command.

forward accounting-start-stop

no forward accounting-start-stop

Syntax Description This command has no arguments or keywords.

Defaults Forward accounting-start-stop is disabled by default.

Command Modes SSG-radius-proxy configuration

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 12.2(4)B | This command was introduced. |
| | 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |

Usage Guidelines Use this command to proxy accounting start, stop, and update packets generated by all RADIUS clients to the AAA server. Disabling this command reduces RADIUS packet traffic and processing for deployments where the billing server is not using these packets for billing purposes.



Note

The **forward accounting-start-stop** command does not affect accounting on and off packets, which are forwarded regardless of this command.

Examples The following example shows how to proxy accounting packets generated by all RADIUS clients to the AAA server:

```
ssg radius-proxy
 server-port auth 1645 acct 1646
 client-address 10.1.2.2 key secret1
 client-address 10.2.25.90 key secret2
 client-address 10.0.0.1 key secret3
 client-address 10.23.3.2 key secret4
 idle-timeout 30
 forward accounting-start-stop
 address-pool 10.1.1.1 10.1.40.250
 address-pool 10.1.5.1 10.1.5.30 domain ssg.com
```

| Related Commands | Command | Description |
|-------------------------|--|--|
| | address-pool | Defines local IP pools to be used by SSG to assign IP addresses to users for which SSG is acting as a RADIUS client. |
| | clear ssg radius-proxy client-address | Clears all hosts connected to a specific RADIUS client. |
| | clear ssg radius-proxy nas-address | Clears all hosts connected to a specific NAS. |
| | idle-timeout (SSG) | Configures a host object timeout value. |
| | server-port | Defines the ports for the SSG RADIUS proxy. |
| | show ssg tcp-redirect group | Displays the pool of IP addresses configured for a router or for a specific domain. |
| | ssg enable | Enables SSG. |
| | ssg radius-proxy | Enables SSG RADIUS Proxy. |

hand-off

To configure a Service Selection Gateway (SSG) RADIUS proxy handoff timeout, use the **hand-off** command in SSG-radius-proxy-timers configuration mode. To disable the handoff timeout, use the **no** form of this command.

hand-off *timeout*

no hand-off *timeout*

| | | |
|---------------------------|----------------|--|
| Syntax Description | <i>timeout</i> | Timeout value, in seconds. Valid range is 1 to 30 seconds. The default is 5 seconds. |
|---------------------------|----------------|--|

Defaults The handoff timeout is set to 5 seconds.

Command Modes SSG-radius-proxy-timers

| Command History | Release | Modification |
|------------------------|----------------|--|
| | 12.2(15)B | |
| | 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T. |

Usage Guidelines Use this command to configure an SSG RADIUS proxy handoff timeout. You can use this command when a PPP session is not disabled and the host object remains active after a base station controller (BSC) handoff.

A Session-Continue vendor-specific attribute (VSA) with a value of 1 in an Accounting-Stop packet indicates that a BSC/packet control function (PCF) handoff is in progress. When SSG detects the BSC/PCF handoff, it keeps the host object and begins the configured handoff timeout. If SSG does not receive an Accounting-Start for this host object before the handoff timeout expires, it deletes the host object.

Examples The following example shows how to configure a handoff timeout value of 25 seconds:

```
ssg radius-proxy
 ssg timeouts
 hand-off 25
```

| Related Commands | Command | Description |
|-------------------------|--|--|
| | | idle (SSG-radius-proxy-timers) |
| | ip-address (SSG-radius-proxy-timers) | Configures an SSG RADIUS proxy IP address timeout. |

| Command | Description |
|------------------------------------|---|
| key (SSG-radius-proxy-client) | Configures a shared secret between SSG and a RADIUS client. |
| ssg radius-proxy | Enables SSG RADIUS Proxy and enters SSG-radius-proxy mode. |
| timeouts (SSG-radius-proxy) | Enters SSG-radius-proxy-timeouts mode. |

home-agent (SSG-radius-proxy)

To configure an IP address or domain for a Home Agent (HA) in a CDMA2000 network, use the **home-agent** command in SSG-radius-proxy configuration mode. To remove an HA address or domain, use the **no** form of this command.

```
home-agent {address HA-ip-address | domain domain-name [address domain-ip-address]}
```

```
no home-agent {address HA-ip-address | domain domain-name [address domain-ip-address]}
```

Syntax Description

| | |
|----------------------------------|--|
| address <i>ip-address</i> | IP address of the local Home Agent. |
| domain <i>domain-name</i> | Domain of the local Home Agent. |
| address <i>ip-address</i> | (Optional) IP address of the domain of the Home Agent. |

Defaults

No default behavior or values.

Command Modes

SSG-radius-proxy configuration

Command History

| Release | Modification |
|-----------|--|
| 12.2(15)B | This command was introduced. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T. |

Usage Guidelines

Use the **home-agent** command to configure a list of domain names for which dynamic Home Agent (HA) IP address assignment is applicable. You can configure each domain name with an HA address. You should also configure the IP address of a default local HA.

Use the **no home-agent address** command to remove any configured domain names. Use the **no home-agent domain** command to remove an entry for a specified domain.

Service Selection Gateway (SSG) determines that an Access-Request packet is for a new Mobile IP session when it receives a 3GPP2-Home-Agent-Attribute vendor-specific (VSA) with a value of 0.0.0.0. For authenticated users with a domain recognized by SSG that has a preconfigured HA address, the 3GPP2-Home-Agent-Attribute is changed to the per-domain HA address. For authenticated users with a domain recognized by SSG that does not have a preconfigured HA address, the 3GPP2-Home-Agent-Attribute is changed to the IP address of the default local HA.

For authenticated users with a domain that is not recognized by SSG, the 3GPP2-Home-Agent-Attribute is not changed.

Examples

The following example shows how to set the IP address of the default local HA to 172.16.0.0:

```
ssg radius-proxy
home-agent address 172.16.0.0
```

■ home-agent (SSG-radius-proxy)

The following example shows how to set the IP address of the HA to 172.16.0.0, for users in domain “home1.com”:

```
ssg radius-proxy
home-agent domain home1.com address 172.16.0.0
```

Related Commands

| Command | Description |
|-------------------------|--|
| ssg radius-proxy | Enables SSG RADIUS Proxy and enters SSG-radius-proxy mode. |

host overlap

To enable SSG to support overlapping host IP addresses, use the **host overlap** command in SSG port-map configuration mode. To disable support for overlapping host IP addresses, use the **no** form of this command.

host overlap

no host overlap

Syntax Description

This command has no arguments or keywords.

Defaults

Overlapping host IP addresses are supported by default when SSG port-bundle host key functionality is configured.

Command Modes

SSG port-map configuration

Command History

| Release | Modification |
|----------|------------------------------|
| 12.3(8)T | This command was introduced. |

Usage Guidelines

The SSG Port-Bundle Host Key feature enables subscribers to have overlapping IP addresses. To enable subscriber-side interface redundancy when SSG port-bundle host key functionality is configured, overlapping IP address support must be disabled so that interface binding is not needed. Use the **no host overlap** command to disable overlapping IP address support.

Examples

The following example shows how to disable support for overlapping hosts when the SSG Port-Bundle Host Key feature is configured:

```
Router(config)# ssg enable
Router(config)# ssg port-map
Router(ssg-port-map)# no host overlap
```

Related Commands

| Command | Description |
|---------------------|--|
| ssg port-map | Enables the SSG Port-Bundle Host Key feature and enters SSG port-map configuration mode. |

idle (SSG-radius-proxy-timers)

To configure a Service Selection Gateway (SSG) host object timeout value, use the **idle** command in SSG-radius-proxy-timers configuration mode. To disable the timeout value, use the **no** form of this command.

idle *timeout*

no idle *timeout*

Syntax Description

| | |
|----------------|---|
| <i>timeout</i> | Timeout value, in seconds. Valid range is 30 to 65536 seconds. There is no default value. |
|----------------|---|

Defaults

No idle timeout value is configured.

Command Modes

SSG-radius-proxy-timers

Command History

| Release | Modification |
|-----------|---|
| 12.2(15)B | This command was introduced to replace the idle-timeout command. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T. |

Usage Guidelines

Use this command to configure an idle timeout value for a host object. Configuring this command prevents dangling host objects on SSG. If a RADIUS client reloads and does not indicate its fault condition to SSG, SSG retains host objects that are no longer valid. This command removes all host objects from a RADIUS client that has been idle for the time specified by the *timeout* argument. When configured, this timeout value is added to the host object.



Note

Timeout values configured in the user profile that appears in the Access-Accept packet take precedence over any timeout value configured by the **timeouts** (SSG-radius-proxy) command.



Note

This command replaces the **idle-timeout** command in SSG-radius-proxy configuration mode.

Examples

The following example shows how to configure an idle timeout value of 60 seconds:

```
ssg radius-proxy
 ssg timeouts
 idle 60
```

Related Commands

| Command | Description |
|---|---|
| hand-off | Configures an SSG RADIUS proxy handoff timeout. |
| ip-address (SSG-radius-proxy-timers) | Configures an SSG RADIUS proxy IP address timeout. |
| key (SSG-radius-proxy-client) | Configures a shared secret between SSG and a RADIUS client. |
| ssg radius-proxy | Enables SSG RADIUS Proxy and enters SSG-radius-proxy mode. |
| timeouts (SSG-radius-proxy) | Enters SSG-radius-proxy-timers mode. |

idle-timeout (SSG)



Note

Effective with Cisco IOS Releases 12.2(16)B and 12.3(4)T, this command was replaced by the **idle** (SSG radius-proxy-timers) command. The **idle-timeout** command is still supported for backward compatibility, but support for this command may be removed in a future Cisco IOS release.

To configure a host object timeout value, use the **idle-timeout** command in SSG-radius-proxy configuration mode. To disable the timeout value, use the **no** form of this command.

idle-timeout *timeout*

no idle-timeout *timeout*

Syntax Description

| | |
|----------------|---|
| <i>timeout</i> | Timeout value, in seconds. Valid range is from 30 to 65536. |
|----------------|---|

Defaults

No timeout value is configured.

Command Modes

SSG-radius-proxy configuration

Command History

| Release | Modification |
|-----------|---|
| 12.2(4)B | This command was introduced. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |
| 12.2(16)B | This command was replaced by the idle (SSG radius-proxy-timers) command. |
| 12.3(4)T | This command was replaced by the idle (SSG radius-proxy-timers) command. |

Usage Guidelines

Use this command to configure a timeout value for a host object. Configuring this command prevents dangling host objects on the Service Selection Gateway (SSG). If a RADIUS client reloads and does not indicate its fault condition to the SSG, the SSG retains the host objects that are no longer valid. This command removes all host objects from a RADIUS client that has been idle for the time specified by the *timeout* argument. When configured, this timeout value is added to the host object.



Note

Timeout values configured in the user profile that appear in the Access-Accept take precedence over any timeout value configured by the **idle-timeout** command.

Examples

The following example shows how to configure a timeout value of 60 seconds:

```
ssg radius-proxy
 server-port auth 1645 acct 1646
```

```

client-address 10.1.2.2 key secret1
client-address 10.2.25.90 key secret2
client-address 10.0.0.1 key secret3
client-address 10.23.3.2 key secret4
idle-timeout 60
forward accounting-start-stop
address-pool 10.1.1.1 10.1.40.250
address-pool 10.1.5.1 10.1.5.30 domain ssg.com

```

Related Commands

| Command | Description |
|--|--|
| address-pool | Defines local IP pools to be used by SSG to assign IP addresses to users for which SSG is acting as a RADIUS client. |
| clear ssg radius-proxy client-address | Clears all hosts connected to a specific RADIUS client. |
| clear ssg radius-proxy nas-address | Clears all hosts connected to a specific NAS. |
| forward accounting-start-stop | Proxies accounting start, stop, and update packets generated by any RADIUS clients to the AAA server. |
| server-port | Defines the ports for the SSG RADIUS proxy. |
| show ssg tcp-redirect group | Displays the pool of IP addresses configured for a router or for a specific domain. |
| ssg enable | Enables SSG. |
| ssg radius-proxy | Enables SSG RADIUS Proxy. |

ip-address (SSG-radius-proxy-timers)

To configure a Service Selection Gateway (SSG) RADIUS proxy IP address timeout, use the **ip-address** command in SSG-radius-proxy-timers configuration mode. To disable the IP address timeout, use the **no** form of this command.

ip-address *timeout*

no ip-address *timeout*

Syntax Description

| | |
|----------------|--|
| <i>timeout</i> | Timeout value, in seconds. Valid range is 1 to 30 seconds. The default is 5 seconds. |
|----------------|--|

Defaults

The default value of this timeout is 5 seconds.

Command Modes

SSG-radius-proxy-timers

Command History

| Release | Modification |
|-----------|--|
| 12.2(15)B | This command was introduced. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T. |

Usage Guidelines

Use this command to configure an SSG RADIUS proxy IP address timeout.

If SSG, acting as a RADIUS proxy for a client, does not allocate an IP address in the Access-Accept packet, a dormant host object is created. The dormant host object is not activated until SSG receives an Accounting-Start packet from the client device, containing a valid IP address.

When an IP address timeout is configured, SSG starts this timer on creation of the dormant host object. If a valid IP address is not received via an Accounting-Start packet from the client device, prior to the expiration of this timeout, the dormant host object is destroyed.

Examples

The following example shows how to configure an SSG RADIUS proxy IP address timeout of 10 seconds:

```
ssg radius-proxy
 ssg timeouts
 ip-address 10
```

Related Commands

| Command | Description |
|---------------------|--|
| address-pool | Defines local IP pools to be used by SSG to assign IP addresses to users for which SSG is acting as a RADIUS client. |
| hand-off | Configures an SSG RADIUS proxy handoff timeout. |

| Command | Description |
|---------------------------------------|---|
| idle (SSG-radius-proxy-timers) | Configures a host object timeout value. |
| key (SSG-radius-proxy-client) | Configures a shared secret between SSG and a RADIUS client. |
| ssg radius-proxy | Enables SSG RADIUS Proxy and enters SSG-radius-proxy mode. |
| timeouts (SSG-radius-proxy) | Enters SSG-radius-proxy-timers mode. |

key (SSG-radius-proxy-client)

To configure a shared secret between the Service Selection Gateway (SSG) and a RADIUS client, use the **key** command in SSG-radius-proxy-client mode. To unconfigure the shared secret, use the **no** form of this command.

key *secret*

no key *secret*

Syntax Description

| | |
|---------------|-----------------------------------|
| <i>secret</i> | Description of the shared secret. |
|---------------|-----------------------------------|

Defaults

No default behavior or values.

Command Modes

SSG-radius-proxy-client

Command History

| Release | Modification |
|-----------|--|
| 12.2(15)B | This command was introduced. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T. |

Usage Guidelines

Use this command to configure a shared secret between SSG and a RADIUS client. Use the *secret* attribute to configure each client IP with a unique shared secret. This shared secret should be the same one that is configured on the RADIUS client.



Note

The **key** command in SSG-radius-proxy-client mode replaces the **client-address key** command in SSG-radius-proxy mode.

Examples

The following example shows how to configure the RADIUS client to proxy all requests from IP address 172.16.0.0 to the RADIUS server and assigns the shared secret “cisco” to the client:

```
client-address 172.16.0.0
key cisco
```

Related Commands

| Command | Description |
|-----------------------|--|
| client-address | Configures the RADIUS client to proxy requests from the specified IP address to the RADIUS server and enters SSG-radius-proxy-client mode. |

length (SSG)

To modify the port-bundle length upon the next Service Selection Gateway (SSG) reload, use the **length** command in SSG portmap configuration mode. To return the port-bundle length to the default value, use the **no** form of this command.

length *bits*

no length *bits*

Syntax Description

bits Port-bundle length, in bits. The range is from 0 to 10 bits. The default is 4 bits.

Defaults

4 bits

Command Modes

SSG portmap configuration

Command History

| Release | Modification |
|-----------|---|
| 12.2(16)B | This command was introduced. This command replaces the ssg port-map destination range command. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T. |

Usage Guidelines

The port-bundle length is used to determine the number of bundles in one group and the number of ports in one bundle. By default, the port-bundle length is 4 bits. The maximum port-bundle length is 10 bits. See [Table 1](#) for available port-bundle length values and the resulting port-per-bundle and bundle-per-group values. Increasing the port-bundle length can be useful when you see frequent error messages about running out of ports in a port bundle, but note that the new value does not take effect until SSG next reloads and Cisco Service Selection Dashboard (SSD) restarts.



Note

For each Cisco SSD server, all connected SSGs must have the same port-bundle length.

Table 1 Port-Bundle Lengths and Resulting Port-per-Bundle and Bundle-per-Group Values

| Port-Bundle Length (in Bits) | Number of Ports per Bundle | Number of Bundles per Group (and per-SSG Source IP Address) |
|------------------------------|----------------------------|---|
| 0 | 1 | 64512 |
| 1 | 2 | 32256 |
| 2 | 4 | 16128 |
| 3 | 8 | 8064 |
| 4 (default) | 16 | 4032 |

Table 1 Port-Bundle Lengths and Resulting Port-per-Bundle and Bundle-per-Group Values

| Port-Bundle Length (in Bits) | Number of Ports per Bundle | Number of Bundles per Group (and per-SSG Source IP Address) |
|------------------------------|----------------------------|---|
| 5 | 32 | 2016 |
| 6 | 64 | 1008 |
| 7 | 128 | 504 |
| 8 | 256 | 252 |
| 9 | 512 | 126 |
| 10 | 1024 | 63 |

Examples

The following example results in 64 ports per bundle and 1008 bundles per group:

```
ssg port-map
length 6
```

Related Commands

| Command | Description |
|---------------------|---|
| source ip | Specifies SSG source IP addresses to which to map the destination IP addresses in subscriber traffic. |
| ssg port-map | Enables the SSG port-bundle host key and enters SSG portmap configuration mode. |

local-profile

To configure a local service profile and enter profile configuration mode, use the **local-profile** command in global configuration mode. To delete the local service profile, use the **no** form of this command.

local-profile *profile-name*

no local-profile *profile-name*

| Syntax Description | <i>profile-name</i> | Name of profile to be configured. |
|--------------------|---------------------|-----------------------------------|
|--------------------|---------------------|-----------------------------------|

Defaults No default behavior or values

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|-----------|--|
| | 12.0(3)DC | This command was introduced on the Cisco 6400 series node route processor. |
| | 12.2(4)B | This command was integrated into Cisco IOS Release 12.2(4)B. |
| | 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |

Usage Guidelines Use this command to configure local service profiles.

Examples The following example shows how to configure a RADIUS profile called “fictitiousname.com” and enter profile configuration mode:

```
Router(config)# local-profile fictitiousname.com
Router(config-prof)#
```

In the following example, two services called “og1” and “og2” are defined and added to the open garden:

```
!
ssg open-garden og1
ssg open-garden og2
!
local-profile og1
  attribute 26 9 251 "Oopengarden1.com"
  attribute 26 9 251 "D10.13.1.5"
  attribute 26 9 251 "R10.1.1.0;255.255.255.0"
local-profile og2
  attribute 26 9 251 "Oopengarden2.com"
  attribute 26 9 251 "D10.14.1.5"
  attribute 26 9 251 "R10.2.1.0;255.255.255.0"
  attribute 26 9 251 "R10.3.1.0;255.255.255.0"
!
ssg bind service og2 10.5.5.1
```

| Related Commands | Command | Description |
|------------------|---------------------------------|--|
| | attribute | Configures attributes in local RADIUS profiles. |
| | show ssg open-garden | Displays a list of all configured open garden services. |
| | ssg open-garden | Designates a service, defined in a local service profile, as an open garden service. |
| | ssg service-search-order | Specifies the order in which SSG searches for a service profile. |

max-sessions host

To set the maximum number of TCP sessions that can be established by an unauthenticated host, use the **max-sessions host** command in SSG TCP-redirect server-group configuration configuration mode. To remove this setting, use the **no** form of this command.

max-sessions host *number-of-sessions*

no max-sessions host *number-of-sessions*

Syntax Description

| | |
|---------------------------|---|
| <i>number-of-sessions</i> | Maximum number of TCP sessions per unauthenticated host. The range is from 1 to 65535. The default is |
|---------------------------|---|

Defaults

No limit on the number of TCP sessions that can be established by an unauthenticated host.

Command Modes

SSG TCP-redirect server-group configuration

Command History

| Release | Modification |
|-----------|--|
| 12.2(16)B | This command was introduced. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T. |

Usage Guidelines

Use the **max-sessions host** command to configure a per-host limit on the number of TCP sessions that can be established by unauthenticated hosts that are redirected to the server group.

The maximum number of TCP connections allowed per host, as configured by the **max-sessions host** command, should be greater than the average number of TCP connections required when a page is accessed.

Examples

The following example sets the maximum number of TCP sessions that can be established by an unauthenticated host at 20 sessions:

```
ssg tcp-redirect
server-group test_group
  Server 10.10.10.1 90
  max-sessions host 20
```

Related Commands

| Command | Description |
|-------------------------|---|
| server-group | Defines the group of one or more servers that make up a named captive portal group and enters SSG TCP-redirect server-group configuration mode. |
| ssg tcp-redirect | Enables SSG TCP redirect and enters SSG TCP-redirect configuration mode. |

mode extended

To select extended Autodomain mode, use the **mode extended** command in SSG-auto-domain configuration mode. To reenable basic Autodomain mode, use the **no** form of this command.

mode extended

no mode extended

Syntax Description This command has no arguments or keywords.

Defaults Basic Autodomain mode is selected.

Command Modes SSG-auto-domain configuration

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 12.2(4)B | This command was introduced. |
| | 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |

Usage Guidelines Use the **mode extended** command to select the extended Autodomain mode. In basic Autodomain mode, the profile downloaded from the AAA server for the selected Autodomain name is a service profile, which may or may not contain attributes specific to Service Selection Gateway (SSG). In extended Autodomain mode, the profile is a “virtual user” profile, which may contain a list of services in addition to other account attributes. The “virtual user” profile contains one autoservice to an authenticated service such as a proxy, VPDN, or tunnel. Connection to the autoservice occurs in the same way as in basic Autodomain mode. The host object is not activated until the user is authenticated at the service. The presence of SSD allows the user to access any other service in the specified user profile. Extended mode also enables users with multiple service selection to log on.

Examples The following example shows how to enable extended Autodomain mode:

```

ssg enable
ssg auto-domain
mode extended
select username
exclude apn company
exclude domain cisco
download exclude-profile abc password1
nat user-address

```

| Related Commands | Command | Description |
|------------------|---------------------------------|---|
| | download exclude-profile | Adds to the Autodomain download exclusion list. |
| | exclude | Configures the Autodomain exclusion list. |

| Command | Description |
|---|---|
| nat user-address | Enables NAT on Autodomain tunnel service. |
| select | Configures the Autodomain selection mode. |
| show ssg auto-domain exclude-profile | Displays the contents of an Autodomain exclude-profile downloaded from the AAA server. |
| ssg auto-domain | Enables SSG Autodomain mode. |
| ssg enable | Enables SSG functionality. |

msid (SSG-radius-proxy-timers)

To configure a Service Selection Gateway (SSG) RADIUS proxy mobile station ID (MSID) timeout, use the **msid** command in SSG-radius-proxy-timers configuration mode. To disable the MSID timeout, use the **no** form of this command.

msid *timeout* **retry** *retries*

no msid *timeout* **retry** *number-of-retries*

Syntax Description

| | |
|---------------------------------------|---|
| <i>timeout</i> | Timeout value in seconds. Valid range is 1 to 5 seconds. The default is 1 second. |
| retry <i>number-of-retries</i> | Maximum number of retries. Valid range is 1 to 20 retries. The default is 10 retries. |

Defaults

The default value of this timeout is 1 second, with a default retry count of 10.

Command Modes

SSG-radius-proxy-timers.

Command History

| Release | Modification |
|-----------|--|
| 12.2(15)B | This command was introduced. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T. |

Usage Guidelines

Use this command to configure an MSID timeout.

Configure the MSID timer to associate an MSID to the host object for a Mobile IP connection. The MSID is associated with a host object only after SSG receives the Accounting-Start packets from the Packet Data Serving Node (PDSN)/Foreign Agent (FA) and the Home Agent (HA). The host object address is not assigned until SSG receives the Accounting-Start packet from the HA. If the Accounting-Start packet from the PDSN/FA arrives before the Accounting-Start packet from the HA, the host object cannot be located, and the MSID is not associated with the host object. When this occurs, the retry timer is started. When the retry timer expires, the MSID is associated with the host object.

If SSG does not receive the Account-Start packet with the correct MSID from the PDSN before the timeout expires, the host object is removed.

Examples

The following example shows how to configure an SSG RADIUS proxy MSID timeout of 3 seconds with 5 retries:

```
ssg radius-proxy
 ssg timeouts
 msid 3 retry 5
```

Related Commands

| Command | Description |
|--|--|
| hand-off | Configures an SSG RADIUS proxy hand off timeout. |
| idle (SSG-radius-proxy-timers) | Configures a host object timeout value. |
| ip-address (SSG-radius-proxy-timers) | Configures an SSG RADIUS proxy IP address timeout. |
| ssg radius-proxy | Enables SSG RADIUS Proxy and enters SSG-radius-proxy mode. |
| timeouts (SSG-radius-proxy) | Enters SSG-radius-proxy-timers mode. |

nat user-address

To enable Network Address Translation (NAT) toward Autodomain service, use the **nat user-address** command in SSG-auto-domain mode. To disable NAT on Autodomain service, use the **no** form of this command.

nat user-address

no nat user-address

Syntax Description

This command has no arguments or keywords.

Defaults

NAT is not applied toward Autodomain services and IP addresses assigned at the tunnel, VPDN, or proxy service will be assigned at the host and then sent back to the RADIUS client. NAT is always applied towards the Autodomain connection regardless of the configuration of the **nat user-address** command when the Access-Request from the RADIUS client contains an IP address.

Command Modes

SSG-auto-domain

Command History

| Release | Modification |
|-----------|---|
| 12.2(4)B | This command was introduced. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |

Usage Guidelines

Use the **nat user-address** command to enable NAT toward the Autodomain connection. When a host object has not been assigned an IP address using the Access-Request from the RADIUS client, Service Selection Gateway (SSG) by default passes an IP address assigned at the tunnel, VPDN, or proxy service back to the RADIUS client and NAT does not happen toward the Autodomain connection. The **nat user-address** command overrides the default behavior and specifies that NAT should be performed towards Autodomain services. If a host has been assigned an IP address via the Access-Request, NAT happens toward the Autodomain connection regardless of the status of this command.

Examples

The following example enables NAT toward the Autodomain connection:

```

ssg enable
ssg auto-domain
mode extended
select username
exclude apn motorola
exclude domain cisco
download exclude-profile abc password1
nat user-address

```

Related Commands

| Command | Description |
|---|--|
| download exclude-profile | Adds to the Autodomain download exclusion list. |
| exclude | Configures the Autodomain exclusion list. |
| mode extended | Enables extended mode for SSG Autodomain. |
| select | Configures the Autodomain selection mode. |
| show ssg auto-domain exclude-profile | Displays the contents of an Autodomain exclude-profile downloaded from the AAA server. |
| ssg enable | Enables SSG functionality. |

network (ssg-redirect)

To add an IP address to a named network list, use the **network** command in SSG-redirect-network configuration mode. To remove an IP address from a named network list, use the **no** form of this command.

network *ip-address mask*

no network *ip-address mask*

Syntax Description

| | |
|-------------------|---|
| <i>ip-address</i> | IP address that is to be added to a named network list. |
| <i>mask</i> | Mask for the associated IP subnet. |

Defaults

No default behavior or values

Command Modes

SSG-redirect-network configuration

Command History

| Release | Modification |
|-----------|---|
| 12.2(4)B | This command was introduced. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |

Usage Guidelines

Use this command to define an individual network that is found in a named network list. Use the **network-list** command to define and name the network list and the **network** command to add an individual IP address to the named network list.

Packets arriving from an authorized user who is attempting to access an unauthorized service from an IP address that is part of a named network list can be redirected to a captive portal group that presents the user with an appropriate response, such as a logon screen. Service Selection Gateway (SSG) TCP Redirect for Services uses a marked TCP port or TCP port list in addition to the destination IP address to determine if a packet is redirected to a captive portal group.

Define a named TCP port list using the **port-list** command, and add TCP ports to the named TCP port list using the **port (ssg-redirect)** command.

You must enable SSG using the **ssg enable** command and SSG TCP Redirect for Services using the **ssg tcp-redirect** command before you can define a named network list.

Examples

The following example creates a network list named “RedirectNw” and adds IP address 10.0.0.0 255.0.0.0 and address 10.2.2.0 255.255.255.0 to the “RedirectNw” network list:

```
ssg tcp-redirect
network-list RedirectNw
network 10.0.0.0 255.0.0.0
network 10.2.2.0 255.255.255.0
```

Related Commands

| Command | Description |
|-------------------------|--|
| network-list | Defines a list of one or more IP networks that make up a named network list. |
| ssg enable | Enables SSG. |
| ssg tcp-redirect | Enables SSG TCP redirect and enters SSG-redirect mode. |

network-list

To define a list of one or more IP networks that make up a named network list and to enter SSG-redirect-network configuration mode, use the **network-list** command in SSG-redirect configuration mode. To remove a named network list, use the **no** form of this command.

network-list *network-listname*

no network-list *network-listname*

Syntax Description

| | |
|-------------------------|---------------------------------------|
| <i>network-listname</i> | Defines the name of the network list. |
|-------------------------|---------------------------------------|

Defaults

No default behavior or values

Command Modes

SSG-redirect configuration

Command History

| Release | Modification |
|-----------|---|
| 12.2(4)B | This command was introduced. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |

Usage Guidelines

Use this command to define a list of one or more IP networks that make up a named network list. Use the *network-listname* attribute to name the IP network list.

Packets arriving from an authorized user who is attempting to access an unauthorized service from an IP address that is part of a named network list can be redirected to a captive portal group that presents the user with an appropriate response, such as a logon screen. Service Selection Gateway (SSG) TCP Redirect for Services uses a marked TCP port or TCP port list in addition to the destination IP address to determine if a packet is redirected to a captive portal group.

Define a named TCP port list using the **port-list** command, and add TCP ports to the named TCP port list using the **port (ssg-redirect)** command.

You must enable SSG using the **ssg enable** command and SSG TCP Redirect for Services using the **ssg tcp-redirect** command before you can define a named network list.

Examples

The following example defines an IP network list named "RedirectNw":

```
network-list RedirectNw
```

Related Commands

| Command | Description |
|---|---|
| network (ssg-redirect) | Adds an IP address to a named network list. |
| redirect unauthorized-service to | Sets a list of destination IP networks that can be redirected by a specified, named captive portal group. |

| Command | Description |
|------------------------------------|--|
| show ssg tcp-redirect group | Displays information about the captive portal groups and the networks associated with the captive portal groups. |
| ssg enable | Enables SSG. |
| ssg tcp-redirect | Enables SSG TCP redirect and enters SSG-redirect mode. |

port (ssg-redirect)

To add a TCP port to a named port list, use the **port** command in SSG-redirect-port configuration mode. To remove a TCP port from a named port list, use the **no port** form of this command.

port *port-number*

no port *port-number*

Syntax Description

| | |
|--------------------|-----------------------------------|
| <i>port-number</i> | Incoming destination port number. |
|--------------------|-----------------------------------|

Defaults

No default behavior or values

Command Modes

SSG-redirect-port configuration

Command History

| Release | Modification |
|-----------|---|
| 12.2(4)B | This command was introduced. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |

Usage Guidelines

Use this command to add incoming destination ports to a named TCP port list. Incoming packets directed to a port in the named TCP port list can be redirected by the named captive portal group. Configure the named captive portal group using the **server-group** command, and add servers to the captive portal group using the **server** (SSG) command. Define and name the TCP port list using the **port-list** command.

You must enable Service Selection Gateway (SSG) using the **ssg enable** command and SSG TCP Redirect for Services using the **ssg tcp-redirect** command before you can define or add incoming destination ports to a named TCP port list.

Examples

The following example creates a named TCP port list named “WebPorts” and adds TCP ports 80 and 8080:

```
ssg enable
ssg tcp-redirect
  port-list WebPorts
    port 80
    port 8080
```

Related Commands

| Command | Description |
|---------------------|---|
| port-list | Defines a list of one or more TCP ports that make up a named port list and enters SSG-redirect-port configuration mode. |
| server (SSG) | Adds a server to a captive portal group. |

| Command | Description |
|------------------------------------|--|
| server-group | Defines the group of one or more servers that make up a named captive portal group and enters SSG-redirect-group configuration mode. |
| show ssg tcp-redirect group | Displays information about the captive portal groups and the networks associated with the captive portal groups. |
| show tcp-redirect mappings | Displays information about the TCP redirect mappings for hosts within your system. |
| ssg enable | Enables SSG. |
| ssg tcp-redirect | Enables SSG TCP redirect and enters SSG-redirect mode. |

port-list

To define a list of one or more TCP ports that make up a named port list and to enter SSG-redirect-port configuration mode, use the **port-list** command in SSG-redirect configuration mode. To disable a port list, use the **no** form of this command.

port-list *port-listname*

no port-list *port-listname*

Syntax Description

| | |
|----------------------|------------------------------------|
| <i>port-listname</i> | Defines the name of the port list. |
|----------------------|------------------------------------|

Defaults

No default behavior or values

Command Modes

SSG-redirect configuration

Command History

| Release | Modification |
|-----------|---|
| 12.2(4)B | This command was introduced. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |

Usage Guidelines

Use this command to define a named port list. Use this command to create a list of TCP ports that can be redirected by the captive portal group. Use the **port** (ssg-redirect) command in SSG-redirect-port configuration mode to add TCP ports to the named port list.

You must enable Service Selection Gateway (SSG) using the **ssg enable** command and SSG TCP Redirect for Services using the **ssg tcp-redirect** command before you can define a named port list.

Examples

The following example creates a port list named “WebPorts”:

```
ssg enable
ssg tcp-redirect
port-list WebPorts
```

Related Commands

| Command | Description |
|----------------------------|--|
| port (ssg-redirect) | Adds a TCP port to a named port list. |
| redirect to | Marks a TCP port or named TCP port list for SSG TCP redirection. |
| server (SSG) | Adds a server to a captive portal group. |
| server-group | Defines the group of one or more servers that make up a named captive portal group and enters SSG-redirect-group configuration mode. |

| Command | Description |
|------------------------------------|--|
| show ssg tcp-redirect group | Displays information about the captive portal groups and the networks associated with the captive portal groups. |
| show tcp-redirect mappings | Displays information about the TCP redirect mappings for hosts within your system. |
| ssg enable | Enables SSG. |
| ssg tcp-redirect | Enables SSG TCP redirect and enters SSG-redirect mode. |

query ip dhcp

To configure the Service Selection Gateway (SSG) to send a Dynamic Host Configuration Protocol (DHCP) lease query request for the subscriber session created under a RADIUS proxy client when no IP address appears in the accounting-start record, use the **query ip dhcp** command in the client-address submode of SSG-radius-proxy mode. To disable the sending of the lease query request, use the **no** form of this command.

query ip dhcp

no query ip dhcp

Syntax Description This command has no arguments or keywords.

Command Default SSG sends the subscriber's IP address as the username (RADIUS attribute 1).

Command Modes Client-address submode of SSG-radius-proxy mode

| Command History | Release | Modification |
|-----------------|-----------|------------------------------|
| | 12.3(14)T | This command was introduced. |

Usage Guidelines Use the **query ip dhcp** command to send DHCP lease query requests for a subscriber session under a specified RADIUS proxy client when no IP address is received in the accounting start record.

Examples The following example enables DHCP lease query requests for RADIUS proxy client 10.0.0.0:

```
Router(config)# ssg enable
Router(config)# ssg radius-proxy
Router(config-radius-proxy)# client-address 10.0.0.0
Router(config-radproxy-client) # query ip dhcp
```

| Related Commands | Command | Description |
|------------------|---------------------------|---|
| | ssg query mac dhcp | Sends a DHCP lease query request to the DHCP server when a subscriber's MAC address is not known. |
| | username mac | Sends a subscriber's MAC address as RADIUS attribute 1 in TAL requests. |