

# redirect access-list

To associate an access control list with a Service Selection Gateway (SSG) TCP redirect server group, use the **redirect access-list** command in SSG-redirect mode. To remove the association, use the **no** form of this command.

```
redirect access-list {number | name} [to groupname]
```

```
no redirect access-list {number | name} [to groupname]
```

## Syntax Description

<i>number</i>	Specifies the access control list number.
<i>name</i>	Specifies the access control list name.
<b>to</b> <i>groupname</i>	(Optional) Defines the group name of the server group to which the access control list is redirected. If no server group is specified, the access control list is used for redirection to any server group that does not have an access control list associated with it.

## Defaults

An access control list is not associated with an SSG TCP redirect server group.

## Command Modes

SSG-redirect

## 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 associate an access control list with a TCP redirect server group. By associating an access control list with a redirect group, you can limit the kind of traffic that is redirected on the basis of the source or destination IP address and TCP ports. It can also be used to redirect different sets of users to different dashboards for unauthenticated users and unauthorized service redirection.

If a port list and an access control list are both associated with a server group, the TCP packet must match the access control list and port list. Only one access control list can be associated with a server group. Either an access control list or a port or port list should be configured with server groups for unauthorized service redirection and captivation.

If a server group is not specified, the access control list is used for redirection to any server group that does not have an access control list associated with it.

The access control list can be a simple or extended access control list. It can also be a named or numbered access control list.

## Examples

The following example redirects access control list 101 to server group “InitialCapt”:

```
redirect access-list 101 to InitialCapt
```

The following example redirects access control list 50 to server group “SESM1”:

```
redirect access-list 50 to SESM1
```

**Related Commands**

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

# redirect captive advertising default group

To configure the default captive portal group, duration, and frequency for advertising captivation, use the **redirect captive advertising default group** command in SSG-redirect configuration mode. To deselect a captive portal group as the default for advertising captivation, use the **no** form of this command.

**redirect captive advertising default group** *group-name* **duration** *seconds* **frequency** *frequency*

**no redirect captive advertising default group** *group-name* **duration** *seconds* **frequency** *frequency*

## Syntax Description

<i>group-name</i>	Name of the captive portal group.
<b>duration</b> <i>seconds</i>	The duration in seconds of the advertising captivation. The valid range is from 1 to 65536 seconds.
<b>frequency</b> <i>frequency</i>	The frequency in seconds at which TCP packets are redirected to the captive portal group. The valid range is from 1 to 65536 seconds.

## 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 select the default captive portal group for advertising captivation of users upon Account Logon. Use the *seconds* argument to configure the duration, in seconds, of the advertising captivation. Any packets arriving from the user and marked for one of the TCP ports configured in the captive portal group *group-name* are redirected to one of the captive portals defined in that captive portal group for the duration configured by the *seconds* argument.

Use the *frequency* argument to configure how often Service Selection Gateway (SSG) attempts to forward packets from the user to the captive portal.

The parameters set by this command can be overridden by the RADIUS attributes set for a user.

## Examples

The following example shows how to configure the captive portal group named “CaptiveServer” to forward packets from a user for 30 seconds at intervals of 3600 seconds:

```
server-group SSD
  server 10.0.0.253 8080
!
redirect port-list WebPorts to SSD
!
```

```

redirect unauthenticated-user to RedirectServer
redirect unauthorized-service to SSD
redirect smtp group SMTPServer all
redirect captive initial default group CaptivateServer duration 10
redirect captive advertising default group CaptivateServer duration 30 frequency 3600
    
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>redirect captive initial default group</b>	Selects a default captive portal group and duration of the initial captivation of users on Account Logon.
<b>redirect to</b>	Marks a TCP port or named TCP port list for SSG TCP redirection.
<b>redirect smtp group</b>	Selects a captive portal group for redirection of SMTP traffic.
<b>redirect unauthorized-service to</b>	Sets a list of destination IP networks that can be redirected by a specified, named captive portal group.
<b>redirect unauthenticated-user to</b>	Redirects TCP traffic from unauthenticated users to a specified captive portal group.
<b>show ssg tcp-redirect group</b>	Displays information about the captive portal groups and the networks associated with the captive portal groups.
<b>show tcp-redirect mappings</b>	Displays information about the TCP redirect mappings for hosts within your system.
<b>ssg enable</b>	Enables SSG.
<b>ssg tcp-redirect</b>	Enables SSG TCP redirect and enters SSG-redirect mode.

# redirect captivate initial default group

To select a default captive portal group and duration of the initial captivation of users on Account Logon, use the **redirect captivate initial default group** command in SSG-redirect configuration mode. To deselect a captive portal group as the default for initial captivation, use the **no** form of this command.

**redirect captivate initial default group** *group-name* **duration** *seconds*

**no redirect captivate initial default group** *group-name* **duration** *seconds*

Syntax Description	
<i>group-name</i>	Name of the captive portal group.
<b>duration</b> <i>seconds</i>	Duration in seconds of the initial captivation. The valid range is from 1 to 65536 seconds.

**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 select the default captive portal group for initial captivation of users on Account Logon. Use the *seconds* argument to configure the duration, in seconds, of the initial captivation. Any packets arriving from the user and marked for one of the TCP ports configured in the captive portal group *group-name* are redirected to one of the captive portals defined in that captive portal group for the duration configured by the *seconds* argument.

The parameters set by this command can be overridden by the RADIUS attributes set for a user.

**Examples** The following example shows that the captive portal group named “CaptivateServer” will be used to forward packets from a user for the first 10 seconds that the user is connected:

```
server-group SSD
 server 10.0.0.253 8080
!
 redirect port-list WebPorts to SSD
!
 redirect unauthenticated-user to RedirectServer
 redirect unauthorized-service to SSD
 redirect smtp group SMTPServer all
 redirect captivate initial default group CaptivateServer duration 10
 redirect captivate advertising default group CaptivateServer duration 30 frequency 3600
```

Related Commands	Command	Description
	<b>redirect captive advertising default group</b>	Configures the default captive portal group, duration, and frequency for advertising.
	<b>redirect to</b>	Marks a TCP port or named TCP port list for SSG TCP redirection.
	<b>redirect smtp group</b>	Selects a captive portal group for redirection of SMTP traffic.
	<b>redirect unauthorized-service to</b>	Sets a list of destination IP networks that can be redirected by a specified, named captive portal group.
	<b>redirect unauthenticated-user to</b>	Redirects TCP traffic from unauthenticated users to a specified captive portal group.
	<b>show ssg tcp-redirect group</b>	Displays information about the captive portal groups and the networks associated with the captive portal groups.
	<b>show tcp-redirect mappings</b>	Displays information about the TCP redirect mappings for hosts within your system.
	<b>ssg enable</b>	Enables SSG.
	<b>ssg tcp-redirect</b>	Enables SSG TCP redirect and enters SSG-redirect mode.

# redirect permanent http to

To configure SSG with permanent TCP redirection for HTTP proxy server support, use the **redirect permanent http to** command in SSG-redirect configuration mode. To disable permanent TCP redirection, use the **no** form of this command.

```
redirect permanent http {authenticated | unauthenticated} to server-group
```

```
no redirect permanent http {authenticated | unauthenticated} to server-group
```

Syntax Description		
<b>authenticated</b>	Redirects HTTP traffic to the HTTP proxy server for authenticated users.	
<b>unauthenticated</b>	Redirects HTTP traffic to the HTTP proxy server for unauthenticated users.	
<i>server-group</i>	Server group name to which HTTP traffic will be sent.	

**Defaults** Permanent TCP redirection is not configured.

**Command Modes** SSG-redirect configuration

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

**Usage Guidelines** Permanent TCP redirection enables SSG to support users whose web browsers are configured with HTTP proxy servers.

**Examples** The following example shows how to configure SSG to support permanent TCP redirection for authenticated and unauthenticated HTTP proxy users:

```
ssg tcp-redirect
 server-group unauthen-group
   server 10.76.86.90 80
 !
 server-group auth_web_group
   server 9.2.36.253 80
 !
 server-group unauth_web_group
   server 9.2.76.12 80
 !
 redirect unauthenticated-user to unauthen-group
 !
 redirect permanent http unauthenticated to unauth_web_group
 !
 redirect permanent http authenticated to auth_web_group
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>server</b>	Adds a server to a captive portal group.
<b>server-group</b>	Defines the group of one or more servers that make up a named captive portal group.
<b>show ssg host</b>	Displays information about a subscriber and current connections of the subscriber.
<b>show ssg tcp-redirect mapping</b>	Displays information about the TCP redirect mappings for hosts within your system.

# redirect prepaid-user to

To configure a captive portal group for redirection of prepaid user traffic, use the **redirect prepaid-user to** command in SSG-redirect configuration mode. To configure SSG not to redirect prepaid users to the specified captive portal group, use the **no** form of this command.

**redirect prepaid-user to** *group-name*

**no redirect prepaid-user to** *group-name*

Syntax Description	<i>group-name</i>	Name of the captive portal group
--------------------	-------------------	----------------------------------

**Defaults** If no redirect group is configured, prepaid traffic is dropped.

**Command Modes** SSG-redirect

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 configure and name a captive portal group to which prepaid user traffic is redirected. When a user that is logged on to a prepaid service runs out of quota on the billing server, the user is redirected to the configured captive portal group if the service is not configured with any specific redirect server group. Once redirected to the captive portal group, the user can refill the quota on the billing server without being disconnected from the original prepaid service.

The captive portal group is the default group for all services that are not configured with a redirect group.

**Examples** The following example shows how to configure a captive portal group called “DefaultRedirectGroup”, add two servers to “DefaultRedirectGroup”, and redirect prepaid users to the newly created captive portal:

```

ssg enable
ssg tcp-redirect
  server-group DefaultRedirectGroup
    server 10.0.0.1 8080
    server 10.0.0.20 80
  end
redirect prepaid-user to DefaultRedirectGroup

```

**Related Commands**

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

# redirect smtp group

To select a captive portal group for redirection of Simple Mail Transfer Protocol (SMTP) traffic, use the **redirect smtp group** command in SSG-redirect configuration mode. To stop redirecting SMTP traffic to a captive portal group, use the **no** form of this command.

```
redirect smtp group group-name [all | user]
```

```
no redirect smtp group group-name [all | user]
```

## Syntax Description

<i>group-name</i>	Name of the captive portal group.
<b>all</b>	(Optional) Any SMTP packets are forwarded.
<b>user</b>	(Optional) SMTP packets from users that have SMTP forwarding permission are forwarded.

## Defaults

**all**

## 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 select a captive portal group for redirection of SMTP traffic. If you select the **all** keyword, all SMTP packets (TCP port 25) from authorized users are redirected to one of the servers in the captive portal group specified by the *group-name* argument. If you select the **user** keyword, only SMTP packets from authorized users that have SMTP forwarding permission set through a RADIUS attribute are redirected. If you do not select a keyword, the default is the **all** keyword.

## Examples

The following example shows how to configure all SMTP packets from authorized users to be redirected to the captive portal group named "SMTPServer":

```
server-group SSD
server 10.0.0.253 8080
!
redirect port-list WebPorts to SSD
!
redirect unauthenticated-user to RedirectServer
redirect unauthorized-service to SSD
redirect smtp group SMTPServer all
redirect captivate initial default group CaptivateServer duration 10
redirect captivate advertising default group CaptivateServer duration 30 frequency 3600
```

The following example shows how to configure SMTP packets from any authorized user with the SMTP forwarding permission set through a RADIUS attribute to be redirected to the captive portal group named “SMTPServer”:

```
redirect smtp group SMTPServer user
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>redirect captivate advertising default group</b>	Configures the default captive portal group, duration, and frequency for advertising.
<b>redirect captivate initial default group</b>	Selects a default captive portal group and duration of the initial captivation of users on Account Logon.
<b>redirect to</b>	Marks a TCP port or named TCP port list for SSG TCP redirection.
<b>redirect unauthorized-service to</b>	Sets a list of destination IP networks that can be redirected by a specified, named captive portal group.
<b>redirect unauthenticated-user to</b>	Redirects TCP traffic from unauthenticated users to a specified captive portal group.
<b>show ssg tcp-redirect group</b>	Displays information about the captive portal groups and the networks associated with the captive portal groups.
<b>show tcp-redirect mappings</b>	Displays information about the TCP redirect mappings for hosts within your system.
<b>ssg enable</b>	Enables SSG.
<b>ssg tcp-redirect</b>	Enables SSG TCP redirect and enters SSG-redirect mode.

# redirect to

To configure a TCP port or named TCP port list for Service Selection Gateway (SSG) TCP Redirect for Services, use the **redirect to** command in SSG-redirect configuration mode. To disable SSG TCP Redirect for Services on a TCP port or named TCP port list, use the **no** form of this command.

**redirect** { **port-list** *port-listname* | **port** *port-number* } **to** *group-name*

**no redirect** { **port-list** *port-listname* | **port** *port-number* } **to** *group-name*

## Syntax Description

<b>port-list</b>	Specifies the named TCP port list to mark for SSG TCP redirection.
<i>port-listname</i>	Specifies the name of the named TCP port list.
<b>port</b>	Specifies a TCP port to mark for SSG TCP redirection.
<i>port-number</i>	Specifies the incoming destination port number of the TCP port to mark for SSG TCP redirection.
<i>group-name</i>	Defines the name of the captive portal group to redirect packets to that are marked for a destination port or named TCP 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 mark a TCP port or a named TCP port list for SSG TCP Redirect for Services. 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. Packets arriving from an authorized user, or from an authorized user attempting to access an unauthorized service at a marked TCP port or named TCP port list can be redirected to a captive portal group that presents the user with an appropriate response, such as a logon screen.



### Note

You can associate only one port or port list with a portal group.

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 TCP port or named TCP port list for SSG TCP redirection.



### Note

This command replaces the **ssg http-redirect port group** command.

**Examples**

The following example marks TCP port 8080 for SSG TCP redirection. Packets with a destination port of 8080 are redirected to the captive portal group named “RedirectServer”:

```
server-group RedirectServer
  server 10.2.36.253 8080
!
  redirect port 8080 to RedirectServer
  redirect unauthorized-service destination network-list RedirectNw to RedirectServer
```

The following example marks the named TCP port “WebPorts” for SSG TCP redirection. Packets with a destination port that is one of the ports in the port list “WebPorts” are redirected to the captive portal group named “RedirectServer”:

```
server-group SSD
  server 10.0.0.253 8080
!
  redirect port-list WebPorts to RedirectServer
!
```

**Related Commands**

Command	Description
<b>port (ssg-redirect)</b>	Adds a TCP port to a named port list.
<b>port-list</b>	Defines a list of one or more TCP ports that make up a named port list and enters SSG-redirect-port configuration mode.
<b>redirect captivate advertising default group</b>	Configures the default captive portal group, duration, and frequency for advertising.
<b>redirect captivate initial default group</b>	Selects a default captive portal group and duration of the initial captivation of users on Account Logon.
<b>redirect unauthorized-service to</b>	Sets a list of destination IP networks that can be redirected by a specified, named captive portal group.
<b>server (SSG)</b>	Adds a server to a captive portal group.
<b>server-group</b>	Defines the group of one or more servers that make up a named captive portal group and enters SSG-redirect-group configuration mode.
<b>show ssg tcp-redirect group</b>	Displays information about the captive portal groups and the networks associated with the captive portal groups.
<b>show tcp-redirect mappings</b>	Displays information about the TCP redirect mappings for hosts within your system.
<b>ssg enable</b>	Enables SSG.
<b>ssg tcp-redirect</b>	Enables SSG TCP redirect and enters SSG-redirect mode.

# redirect unauthenticated-user to

To redirect TCP traffic from unauthenticated users to a specified captive portal group, use the **redirect unauthenticated-user to** command in Service Selection Gateway SSG-redirect configuration mode. To stop redirecting traffic from unauthenticated users to the specified captive portal group, use the **no** form of this command.

**redirect unauthenticated-user to** *group-name*

**no redirect unauthenticated-user to** *group-name*

## Syntax Description

<i>group-name</i>	The name of the captive portal group.
-------------------	---------------------------------------

## 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 redirect traffic from unauthenticated users to a specified captive portal group.



### Note

This command replaces the **ssg http-redirect unauthorized-user group** command.

## Examples

The following example sets redirection of traffic from unauthenticated users to the captive portal group named "RedirectServer":

```
server-group SSD
 server 10.0.0.253 8080
!
 redirect port-list WebPorts to SSD
!
 redirect unauthenticated-user to RedirectServer
 redirect unauthorized-service to SSD
 redirect smtp group SMTPServer all
 redirect captivate initial default group CaptivateServer duration 10
 redirect captivate advertising default group CaptivateServer duration 30 frequency 3600
```

Related Commands	Command	Description
	<b>redirect captivate advertising default group</b>	Configures the default captive portal group, duration, and frequency for advertising.
	<b>redirect captivate initial default group</b>	Selects a default captive portal group and duration of the initial captivation of users on Account Logon.
	<b>redirect to</b>	Marks a TCP port or named TCP port list for SSG TCP redirection.
	<b>redirect smtp group</b>	Selects a captive portal group for redirection of SMTP traffic.
	<b>redirect unauthorized-service to</b>	Sets a list of destination IP networks that can be redirected by a specified, named captive portal group.
	<b>show ssg tcp-redirect group</b>	Displays information about the captive portal groups and the networks associated with the captive portal groups.
	<b>show tcp-redirect mappings</b>	Displays information about the TCP redirect mappings for hosts within your system.
	<b>ssg enable</b>	Enables SSG.
	<b>ssg tcp-redirect</b>	Enables SSG TCP redirect and enters SSG-redirect mode.

# redirect unauthorized-service service to

To redirect traffic that is destined for an unauthorized service to a specified server group, use the **redirect unauthorized-service service to** command in SSG TCP-redirect configuration mode. To remove this redirection, use the **no** form of this command.

**redirect unauthorized-service service** *service-name* **to** *server-group*

**no redirect unauthorized-service service** *service-name* **to** *server-group*

## Syntax Description

<i>service-name</i>	Name of the unauthorized service.
<i>server-group</i>	Name of the server group to which traffic will be forwarded.

## Defaults

Users trying to access a service that they are unauthorized to access will not be redirected.

## Command Modes

SSG TCP-redirect 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

The **redirect unauthorized-service service to** command causes SSG to download the service profile from the authentication, authorization, and accounting (AAA) server and create mappings for the networks associated with the service. If traffic is received for the specified service while the service profile is being downloaded, the traffic either will be dropped or will be forwarded if Internet service is available to the user.

## Examples

In the following example, users who are trying to access the service “test\_service” but are unauthorized for that service will be forwarded to the server group “test\_group”:

```

ssg tcp-redirect
  Server-group test_group
    Server 10.10.10.1 90
  !
  !
  Port-list test_ports
    Port 777
  !
  !
  redirect port-list test_ports to test_group
  !
  redirect unauthorized-service service test_service to test_group

```

<b>Command</b>	<b>Description</b>
<b>redirect unauthenticated-user to</b>	Redirects TCP traffic from unauthenticated users to a specified captive portal group.
<b>redirect unauthorized-service to</b>	Sets a list of destination IP networks that can be redirected by a specified, named captive portal group.
<b>ssg tcp-redirect</b>	Enables SSG TCP redirect and enters SSG TCP-redirect configuration mode.

# redirect unauthorized-service to

To set a list of destination IP networks that can be redirected by a specified, named captive portal group, use the **redirect unauthorized-service to** command in SSG-redirect configuration mode. To remove the list of IP networks that can be redirected by a specified named captive portal group, use the **no** form of this command.

**redirect unauthorized-service** [**destination network-list** *network-listname*] **to** *group-name*

**no redirect unauthorized-service** [**destination network-list** *network-listname*] **to** *group-name*

Syntax Description	destination network list	(Optional) Checks incoming packets from authenticated hosts to networks that they are not authorized to access to determine if they need redirection.
	<i>network-listname</i>	(Optional) Name of the list of destination IP networks.
	<i>group-name</i>	Name of the captive portal group.

**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 set a list of destination IP networks that can be redirected by the named captive portal group specified by the *group-name* argument. Incoming packets from authenticated hosts to networks that they are not authorized to access are checked against the destination IP network list to determine if they need redirection. If you do not specify a destination IP network by configuring the optional **destination network-list** keywords, the captive portal group specified in the *group-name* argument is used as the default group for unauthorized service redirection when the IP address of the unauthorized packet does not fall into any network list associated with any captive portal group.

You can associate only one destination IP network list with a captive portal group. You can associate a destination IP network list with multiple captive portal groups.

When you associate a destination IP network list with a captive portal group, packets arriving marked with a destination IP network that matches an IP network list may be redirected via SSG TCP redirection. The incoming destination TCP port also determines whether a packet is a candidate for SSG TCP redirection.

You can associate different server groups with overlapping IP network addresses. You must configure the captive portal group associated with a more specific network group first. For example, you must configure

```
redirect 10.1.1.0/255.255.0.0 to IPTVGroup
```

before you can configure

```
redirect 10.0.0.0/255.0.0.0 to ISPGroup
```

### Examples

The following example shows how to set the captive portal group called “RedirectServer” as a possible candidate for redirection when the destination of a packet matches one of the networks in the destination IP network list named “RedirectNW”:

```
server-group RedirectServer
 server 10.2.36.253 8080
!
 redirect port 80 to RedirectServer
 redirect unauthorized-service destination network-list RedirectNw to RedirectServer
```

The following example shows how to set the captive portal group called “DefaultRedirectServer” as a possible candidate for redirection when the destination of a packet does not match any of the networks defined in any destination IP network list:

```
redirect unauthorized-service to DefaultRedirectServer
```

### Related Commands

Command	Description
<b>redirect captivate advertising default group</b>	Configures the default captive portal group, duration, and frequency for advertising.
<b>redirect captivate initial default group</b>	Selects a default captive portal group and duration of the initial captivation of users on Account Logon.
<b>redirect to</b>	Marks a TCP port or named TCP port list for SSG TCP redirection.
<b>redirect smtp group</b>	Selects a captive portal group for redirection of SMTP traffic.
<b>redirect unauthenticated-user to</b>	Redirects TCP traffic from unauthenticated users to a specified captive portal group.
<b>show ssg tcp-redirect group</b>	Displays information about the captive portal groups and the networks associated with the captive portal groups.
<b>show tcp-redirect mappings</b>	Displays information about the TCP redirect mappings for hosts within your system.
<b>ssg enable</b>	Enables SSG.
<b>ssg tcp-redirect</b>	Enables SSG TCP redirect and enters SSG-redirect mode.

## remove vsa

To allow all Third Generation Partnership Project 2 (3GPP2) vendor-specific attributes (VSAs) or all Cisco VSAs from Access-Accept packets proxied from a authentication, authorization, and accounting (AAA) server to a RADIUS client to be removed, use the **remove vsa** command in SSG-radius-proxy-client mode. To enable all 3GPP2 VSAs or Cisco VSAs to be passed transparently, use the **no** form of this command.

```
remove vsa {3gpp2 | cisco}
```

```
no remove vsa {3gpp2 | cisco}
```

### Syntax Description

<b>3gpp2</b>	Removes all 3GPP2 VSAs.
<b>cisco</b>	Removes all Cisco VSAs.

### Defaults

By default, Service Selection Gateway (SSG) removes all Cisco VSAs from Access-Accept packets proxied from the AAA server to the client device. All 3GPP2 VSAs are, by default, passed transparently.

### 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 remove all 3GPP2 VSAs or Cisco VSAs from a RADIUS client.

By default, SSG removes all Cisco VSAs from Access-Accept packets proxied from the AAA server to the client device. This is because the client device is unlikely to understand the VSAs, and their presence may cause interoperation difficulties. The **no remove vsa cisco** command may be used to allow these attributes to be passed transparently.

You can use this command to remove all 3GPP2 VSAs in addition to Cisco VSAs by using the **3gpp2** keyword. 3GPP2 VSAs are not filtered by default, whereas Cisco VSAs are filtered by default. SSG VSAs (a subset of Cisco VSAs) are always removed, irrespective of any configuration.

### Examples

The following example shows how to remove all 3GPP2 VSAs from an Accept-Accept packet proxied from the AAA server to the client device:

```
remove vsa 3gpp2
```

The following example shows how to transparently pass all Cisco VSAs in an Accept-Accept packet proxied from the AAA server to the client device:

```
remove vsa cisco
```

```
no remove vsa cisco
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>client-address</b>	Configures a RADIUS client to proxy requests from the specified IP address to a RADIUS server and enters SSG-radius-proxy-client mode.

# select

To override the default Autodomain selection algorithm, use the **select** command in SSG-auto-domain mode. To reenable the default algorithm for selecting the Autodomain, use the **no** form of this command.

```
select {username | called-station-id}
```

```
no select {username | called-station-id}
```

## Syntax Description

<b>username</b>	Configures the algorithm to use only the username to select the Autodomain.
<b>called-station-id</b>	Configures the algorithm to use only the Access Point Name (APN) Called-Station-ID.

## Defaults

The algorithm attempts to find a valid Autodomain based on the APN Called-Station-ID and then by username.

## 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 **select** command to override the default algorithm for selecting the Autodomain. By default, the algorithm attempts to find a valid Autodomain based on APN Called-Station-ID and then by username. Using this command, you can configure the algorithm to use only the APN or only the username.



### Note

The Autodomain exclusion list is applied even if the mode is selected using the **select** command.

## Examples

The following example shows how to configure the algorithm to search for a valid Autodomain based only on the username:

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

The following example shows how to configure the algorithm to search for a valid Autodomain based only on the APN:

```
select called-station-id
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>download exclude-profile</b>	Adds to the Autodomain download exclusion list.
<b>exclude</b>	Configures the Autodomain exclusion list.
<b>mode extended</b>	Enables extended mode for SSG Autodomain.
<b>nat user-address</b>	Enables NAT on Autodomain tunnel service.
<b>show ssg auto-domain exclude-profile</b>	Displays the contents of an Autodomain exclude-profile downloaded from the AAA server.
<b>ssg auto-domain</b>	Enables SSG Autodomain.
<b>ssg enable</b>	Enables SSG functionality.

## server (SSG)

To add a server to a captive portal group, use the **server** command in SSG-redirect-group configuration mode. To remove a server from a captive portal group, use the **no** form of this command.

```
server ip-address port
```

```
no server ip-address port
```

Syntax Description	<i>ip-address</i>	IP address of the server to be added to the captive portal group.
	<i>port</i>	TCP port of the server to be added to the captive portal group.

Defaults	No default behavior or values
----------	-------------------------------

Command Modes	SSG-redirect-group 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 <b>server</b> command in SSG-redirect-group configuration mode to add a server, defined by its IP address and TCP port, to a captive portal group.
------------------	--

Service Selection Gateway (SSG) TCP Redirect for Services provides nonauthorized users access to controlled services within an SSG. Packets sent upstream from an unauthenticated user are forwarded to the captive portal that deals with the packets in a suitable manner, such as routing them to a logon page. You can also use captive portals to handle requests from authorized users who request access to services into which they are not logged.

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 captive portal group. Use the **server-group** command in SSG-redirect configuration mode to create and name a captive portal group before using the **server** command to add servers to the captive portal group.

Examples	The following example adds a server at IP address 10.0.0.0 and TCP port 8080 and a server at IP address 10.1.2.3 and TCP port 8081 to a captive portal group named “RedirectServer”:
----------	--

```
ssg enable
ssg tcp-redirect
server-group RedirectServer
server 10.0.0.0 8080
server 10.1.2.3 8081
```

**Related Commands**

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

# server-group

To define a group of one or more servers that make up a named captive portal group and enter SSG-redirect-group configuration mode, use the **server-group** command in SSG-redirect configuration mode. To remove a captive portal group and any servers configured within that portal group, use the **no** form of this command.

**server-group** *group-name*

**no server-group** *group-name*

## Syntax Description

<i>group-name</i>	The name of the captive portal group.
-------------------	---------------------------------------

## 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 and name a captive portal group. Service Selection Gateway (SSG) TCP Redirect for Services provides nonauthorized users access to controlled services within an SSG. Packets sent upstream from an unauthenticated user are forwarded to the captive portal that deals with the packets in a suitable manner, such as routing them to a logon page. You can also use captive portals to handle requests from authorized users who request access to services into which they are not logged.

After defining a captive portal group with the **server-group** command, identify individual servers for inclusion in the captive portal group using the **server** *ip-address port* command in SSG-redirect-group configuration mode.

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 captive portal group.



### Note

This command, along with the **server** command, replaces the **ssg http-redirect group** *group-name* **server** *ip-address port* command.

## Examples

The following example defines a captive portal group named “RedirectServer”:

```
ssg enable
ssg tcp-redirect
server-group RedirectServer
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>server (SSG)</b>	Adds a server to a captive portal group.
<b>show ssg tcp-redirect group</b>	Displays information about the captive portal groups and the networks associated with the captive portal groups.
<b>show tcp-redirect mappings</b>	Displays information about the TCP redirect mappings for hosts within your system.
<b>ssg enable</b>	Enables SSG.
<b>ssg tcp-redirect</b>	Enables SSG TCP redirect and enters SSG-redirect mode.

# server-port

To configure the ports on which Service Selection Gateway (SSG) listens for RADIUS-requests from configured RADIUS clients, use the **server-port** command in SSG-radius-proxy configuration mode. To stop SSG from listening for RADIUS requests from configured RADIUS clients on a port, use the **no** form of this command.

**server-port** [**auth** *auth-port*] [**acct** *acct-port*]

**no server-port** [**auth** *auth-port*] [**acct** *acct-port*]

## Syntax Description

<b>auth</b>	(Optional) RADIUS authentication port.
<i>auth-port</i>	(Optional) Port number to be used for RADIUS authentication. The default is 1645.
<b>acct</b>	(Optional) RADIUS accounting port.
<i>acct-port</i>	(Optional) Port number to be used for RADIUS accounting. The default is 1646.

## Defaults

Port 1645 is the default RADIUS authentication port.  
Port 1646 is the default RADIUS accounting port.

## 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 configure the authentication and accounting ports for the SSG Autologon Using Proxy RADIUS feature. Ports configured with this command are global parameters that apply to all proxy clients in the SSG.

## Examples

The following example shows how to configure port 23 as the RADIUS authentication port and port 45 as the RADIUS accounting port:

```
server-port auth 23 acct 45
```

**Related Commands**

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

# session-identifier

To override Service Selection Gateway (SSG) automatic RADIUS client session identification and to configure SSG to identify the specified client session by a specific type of ID attribute, use the **session-identifier** command in SSG-radius-proxy-client mode. To configure SSG to perform user identification only by the username without using a session identification, use the **no** form of this command.

**session-identifier** [auto | msid | correlation-id | acct-sess-id]

**no session-identifier** [auto | msid | correlation-id | acct-sess-id]

## Syntax Description

<b>auto</b>	Automatically determines the session identifier.
<b>msid</b>	Uses the MSID as the client session identifier.
<b>correlation-id</b>	Uses the Correlation-ID as the client session identifier.
<b>acct-sess-id</b>	Uses the Accounting-Session-ID as a client session identifier.

## Defaults

SSG selects the attribute used for session identification according to the type of client device.

## 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

By default, SSG automatically selects the attribute to use for session identification according to the type of RADIUS client device. This attribute is used in the SSG Proxy RADIUS logon table. SSG assigns the following vendor-specific attributes (VSAs) to identify client sessions:

- 3GPP2-Correlation-ID for Packet Data Serving Nodes (PDSNs)
- Accounting-Session-ID for Home Agents (HAs)
- Calling-Station-ID (MSID) for non-CDMA2000 devices such as a general packet radio system (GPRS)

Use the **session-identifier** command to override the automatic session identification. Use the **auto** keyword to return to automatic session identification.

## Examples

The following example shows how to configure SSG to use the Correlation-ID to identify the specified client session:

```
session-identifier correlation-id
```

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, to assign the shared secret “cisco” to the client, and to use the Accounting-Session-ID attribute to identify the specified client session:

```
client-address 172.16.0.0
  key cisco
  session-identifier acct-session-id
```

**Related Commands**

Command	Description
<b>client-address</b>	Configures the RADIUS client to proxy requests from the specified IP address to the RADIUS server and enters SSG-radius-proxy-client mode.
<b>key (SSG-radius-proxy-client)</b>	Configures a shared secret between SSG and a RADIUS client.

# sessions auto cleanup

To configure an aggregation device to attempt to recover PPP over Ethernet (PPPoE) sessions that failed after reload by notifying customer premises equipment (CPE) devices about the PPPoE session failures, use the **sessions auto cleanup** command in BBA group configuration mode. To disable PPPoE session recovery after reload, use the **no** form of this command.

**sessions auto cleanup**

**no sessions auto cleanup**

**Syntax Description** This command has no arguments or keywords.

**Defaults** PPPoE session recovery after reload is not enabled.

**Command Modes** BBA group configuration

Command History	Release	Modification
	12.3(2)T	This command was introduced.

**Usage Guidelines** If the PPP keepalive mechanism is disabled on a CPE device, the CPE device has no way to detect link or peer device failures over PPPoE connections. When an aggregation device that serves as the PPPoE session endpoint reloads, the CPE will assume that the link is up and will continue to send traffic to the aggregation device. The aggregation device will drop the traffic for the failed PPPoE session.

The **sessions auto cleanup** command enables an aggregation device to attempt to recover PPPoE sessions that existed before a reload. When the aggregation device detects a PPPoE packet for a “half-active” PPPoE session (a PPPoE session that is active on the CPE end only), the device notifies the CPE of the PPPoE session failure by sending a PPPoE active discovery terminate (PADT) packet. The CPE device is expected to respond to the PADT packet by taking failure recovery action.

The **sessions auto cleanup** command must be configured in a PPPoE profile. This command enables PPPoE session recovery after reload on all ingress ports that use the PPPoE profile.

**Examples** In the following example, PPPoE session recovery after reload is configured in PPPoE profile “group1”.

```
bba-group pppoe group1
 virtual-template 1
  sessions auto cleanup
```

Related Commands	Command	Description
	<b>bba-group pppoe</b>	Creates a PPPoE profile.

# show ssg auto-domain exclude-profile

To display the contents of an Autodomain exclude profile downloaded from the AAA server, use the **show ssg auto-domain exclude-profile** command in global configuration mode.

```
show ssg auto-domain exclude-profile
```

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Global 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 in global configuration mode to display the contents of an Autodomain exclude-profile downloaded from the AAA server. If any exclude entries downloaded from the AAA server are removed by the **no exclude {apn | domain} name** command, these entries will not be displayed by the **show ssg auto-domain exclude-profile** command.

**Examples** The following sample displays the contents of an Autodomain exclude profile downloaded from the AAA server. The report is self-explanatory.

```
Router# show ssg auto-domain exclude-profile

Exclude APN Entries Downloaded:

apn1.gprs   apr2.com

Exclude Domain Entries Downloaded:

cisco.com   abcd.com
```

Related Commands	Command	Description
	<b>exclude</b>	Configures the Autodomain exclusion list.
	<b>mode extended</b>	Enables extended mode for SSG Autodomain.
	<b>nat user-address</b>	Enables NAT on Autodomain tunnel service.
	<b>select</b>	Configures the Autodomain selection mode.
	<b>show ssg auto-domain exclude-profile</b>	Adds to the Autodomain download exclusion list.
	<b>ssg enable</b>	Enables SSG functionality.

# show ssg binding

To display service names that have been bound to interfaces and the IP addresses to which they have been bound, use the **show ssg binding** command in privileged EXEC mode.

```
show ssg binding [begin expression | exclude expression | include expression]
```

Syntax Description	begin	(Optional) Begin with the line that contains <i>expression</i> .
	<i>expression</i>	(Optional) Word or phrase used to determine what lines will be shown.
	<b>exclude</b>	(Optional) Exclude lines that contain <i>expression</i> .
	<b>include</b>	(Optional) Include lines that contain <i>expression</i> .

**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 display services and the interfaces to which they have been bound.

**Examples** The following example shows all service names that have been bound to interfaces:

```
Router# show ssg binding

WhipitNet          -> 192.168.1.1 (NHT)
Service1.com       -> 192.168.1.2 (NHT)
Service2.com       -> 192.168.1.3 (NHT)
Service3.com       -> 192.168.1.4 (NHT)
GoodNet            -> 192.168.2.1
Perftest           -> 192.168.1.6
```

Related Commands	Command	Description
	<b>clear ssg service</b>	Removes a service.
	<b>show ssg service</b>	Displays the information for a service.
	<b>ssg bind service</b>	Specifies the interface for a service.

# show ssg connection

To display the connections of a given Service Selection Gateway (SSG) host and a service name, use the **show ssg connection** command in privileged EXEC mode.

```
show ssg connection {ip-address | network-id subnet-mask} service-name [interface]
```

## Syntax Description

<i>ip-address</i>	The IP address of an active SSG connection. This is always a subscribed host.
<i>network-id</i>	The IP network ID of an active SSG connection. This is always a subscribed host.
<i>subnet-mask</i>	The IP subnet mask of the subnet-based subscribed host.
<i>service-name</i>	Name of an active SSG connection.
<i>interface</i>	(Optional) IP address through 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 for the SSG Host Key feature.
12.2(4)B	This command was modified to display information about SSG prepaid billing.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(13)T	The modifications from Release 12.2(4)B were integrated into Cisco IOS Release 12.2(13)T.
12.3(1a)BW	This command was modified to display the MSISDN (Calling Station ID) used for service logon.
12.3(3)B	The modifications from Release 12.3(1a)BW were integrated into Cisco IOS Release 12.3(3)B.
12.3(7)T	The modifications from Release 12.3(1a)BW were integrated into Cisco IOS Release 12.3(7)T.
12.3(14)T	The <i>network-id</i> and <i>subnet-mask</i> arguments were added.

## Examples

### Prepaid Service Based on Volume: Example

The following example displays the SSG connection for a prepaid service that uses a volume-based quota:

```
Router# show ssg connection 10.10.1.1 InstMsg
```

```
-----ConnectionObject Content -----
```

```
User Name:
Owner Host:10.10.1.1
Associated Service:InstMsg
```

```

Connection State:0 (UP)
Connection Started since:*00:25:58.000 UTC Tue Oct 23 2001
User last activity at:*00:25:59.000 UTC Tue Oct 23 2001
Connection Traffic Statistics:
    Input Bytes = 0, Input packets = 0
    Output Bytes = 0, Output packets = 0
    Quota Type = 'VOLUME', Quota Value = 100
Session policing disabled

```

### Prepaid Service Based on Time: Example

The following example displays the SSG connection for a prepaid service that uses a time-based quota:

```
Router# show ssg connection 10.10.1.2 Prepaid-internet
```

```

-----ConnectionObject Content -----
User Name:Host
Owner Host:10.10.1.2
Associated Service:Prepaid-internet
Connection State:0 (UP)
Connection Started since:*00:34:06.000 UTC Tue Oct 23 2001
User last activity at:*00:34:07.000 UTC Tue Oct 23 2001
Connection Traffic Statistics:
    Input Bytes = 0, Input packets = 0
    Output Bytes = 0, Output packets = 0
    Quota Type = 'TIME', Quota Value = 100
Session policing disabled

```

### Autologin Service: Example

The following example shows the service connection for the autologon service to host 10.3.6.1:

```
Router# show ssg connection 10.3.6.1 autologin
```

```

----- ConnectionObject Content -----
User Name:autologin
Owner Host:10.3.6.1
Associated Service:autologin
Connection State:0 (UP)
Connection Started since:
*20:41:26.000 UTC Fri Jul 27 2001
User last activity at:*20:41:26.000 UTC Fri Jul 27 2001
Connection Traffic Statistics:
    Input Bytes = 0 (HI = 0), Input packets = 0
    Output Bytes = 0 (HI = 0), Output packets = 0

```

### MSISDN: Example

The following sample output for the **show ssg connection** command shows the MSISDN that is used for service logon:

```
Router# show ssg connection 10.0.1.1 proxy2
```

```

-----ConnectionObject Content -----
User Name: dev-user2
Owner Host: 10.0.1.1
Associated Service: proxy2
Calling station id: 12345
Connection State: 0 (UP)
Connection Started since: *17:44:59.000 GMT Sun Jul 6 2003
User last activity at: *17:44:59.000 GMT Sun Jul 6 2003
Connection Traffic Statistics:
    Input Bytes = 0, Input packets = 0
    Output Bytes = 0, Output packets = 0
Session policing disabled

```

**Subnet-Based Subscriber: Example**

The following sample output for the **show ssg connection** command shows the subnet mask of the subscribed host:

```
Router# show ssg connection 10.0.1.1 255.255.255.0 passthru

-----ConnectionObject Content -----
User Name: dev-user2
Owner Host: 10.0.1.1 (Mask : 255.255.255.0)
Associated Service: passthru1
Calling station id: 00d0.792f.8054
Connection State: 0 (UP)
Connection Started since: *17:44:59.000 GMT Sun Jul 6 2004
User last activity at: *17:44:59.000 GMT Sun Jul 6 2004
Connection Traffic Statistics:
    Input Bytes = 0, Input packets = 0
    Output Bytes = 0, Output packets = 0
```

Table 2 describes the significant fields shown in the displays.

**Table 2** *show ssg connection Field Descriptions*

Field	Description
User Name	Subscriber name supplied at authentication.
Owner Host	IP address and subnet mask of the subscribed host.
Associated Service	Service name of the connected service.
Calling station id	MSISDN used for service logon.
Connection State	State of activation (active or inactive).
Connection Started since	Time of host connection to the associated service.
User last activity at	Time of last data packet sent over this connection.
Input Bytes	Number of bytes received on this connection.
Input packets	Number of packets received on this connection.
Output Bytes	Number of bytes sent on this connection.
Output packets	Number of packets sent on this connection.
Quota Type	Form in which the quota value is expressed (time or volume).
Quota Value	Value of the quota (in bytes for volume or seconds for time).

**Related Commands**

Command	Description
<b>clear ssg connection</b>	Removes the connections of a given host and a service name.

# show ssg dial-out exclude-list

To display information about the Dialed Number Identification Service (DNIS) prefix profile and the DNIS exclusion list, use the **show ssg dial-out exclude-list** command in privileged EXEC mode.

**show ssg dial-out exclude-list**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

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 display the DNIS profile name and all DNIS entries configured via CLI or downloaded from a authentication, authorization, and accounting (AAA) server.

**Examples** The following example shows sample output for the **show ssg dial-out exclude-list** command:

```
Router# show ssg dial-out exclude-list
Exclude DNIS prefixes downloaded from profile exclude_dnis_aaa
```

Related Commands	Command	Description
	<b>dnis-prefix all service</b>	Configures the dial-out global service.
	<b>download exclude-profile (ssg dial-out)</b>	Downloads the DNIS exclusion list locally or from a AAA server.
	<b>exclude dnis-prefix</b>	Configures the DNIS filter by adding a DNIS prefix to the DNIS exclusion list.
	<b>ssg dial-out</b>	Enters SSG dial-out configuration mode.

# show ssg direction

To display the direction of all interfaces for which a direction has been specified, use the **show ssg direction** command in privileged EXEC mode.

```
show ssg direction [begin expression | exclude expression | include expression]
```

Syntax Description	begin	(Optional) Begin with the line that contains <i>expression</i> .
	<i>expression</i>	(Optional) Word or phrase used to determine what lines will be shown.
	<b>exclude</b>	(Optional) Exclude lines that contain <i>expression</i> .
	<b>include</b>	(Optional) Include lines that contain <i>expression</i> .

**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 show all interfaces that have been specified as uplinks or downlinks.

**Examples** The following example shows the direction of all interfaces that have been specified as uplinks or downlinks.

```
Router# show ssg direction

ATM0/0/0.10: Uplink
BVI1: Downlink
FastEthernet0/0/0: Uplink
```

Related Commands	Command	Description
	<b>ssg bind direction</b>	Specifies an interface as a downlink or uplink interface.

# show ssg host

To display information about a Service Selection Gateway (SSG) subscriber and the current connections of the subscriber, use the **show ssg host** command in privileged EXEC mode. The command syntax of the **show ssg host** command depends on whether the SSG Port-Bundle Host Key feature is enabled.

## When SSG Port-Bundle Host Key Is Not Enabled

```
show ssg host [ip-address | count | username [subnet-mask]]
```

## When SSG Port-Bundle Host Key Is Enabled

```
show ssg host [ip-address | count | username] [interface [username] [subnet-mask]]
```

Syntax	Description
<i>ip-address</i>	(Optional) Host IP address.
count	(Optional) Displays host object count, including inactive hosts.
username	(Optional) Displays all host usernames and IP addresses.
<i>interface</i>	(Optional) 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.
<i>subnet-mask</i>	(Optional) The IP subnet mask of the subnet-based subscribed host.

## Defaults

If no argument is provided, all current connections are displayed.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 Node Route Processor (NRP).
12.2(2)B	The <i>interface</i> argument was added.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(15)B	This command was modified as follows: <ul style="list-style-type: none"> <li>Introduced syntax dependence on SSG host key.</li> <li>Introduced <b>count</b> keyword.</li> <li>Added fields to the output to display additional information about the status of hosts.</li> </ul>
12.2(15)T	The modifications made in Cisco IOS Release 12.2(15)B were integrated into Cisco IOS Release 12.2(15)T.
12.3(11)T	The output was enhanced to show information about the VPN routing/forwarding instance (VRF) that is associated with a host.
12.3(14)T	The <i>subnet-mask</i> argument was added.

**Usage Guidelines**

You can specify the Service Selection Gateway (SSG) downlink interface only when the SSG Port-Bundle 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.

**Examples****Display All Active Hosts: Example**

The following example shows all active hosts:

```
Router# show ssg host

1:10.3.1.1          [Host-Key 70.13.60.3:64]
2:10.3.6.1          [Host-Key 70.13.60.3:65]

### Active HostObject Count:2
```

**Simple IP Host: Example**

The following example shows information about a simple IP host with an IP address of 10.0.0.0:

```
Router# show ssg host 10.0.0.0

----- HostObject Content -----
Activated: TRUE
Interface:
User Name: user1
Owner Host: 10.0.0.0
Msg IP: 0.0.0.0 (0)
Host DNS IP: 0.0.0.0
Proxy logon from client IP: 10.0.48.3
  Device: PDSN (Simple IP)
  NASIP : 10.0.48.3
  SessID: 12345678
  APN   :
  MSID  : 5551000
  Timer : None
Maximum Session Timeout: 0 seconds
Host Idle Timeout: 60000 seconds
Class Attr: NONE
User policing disabled
User logged on since: *05:59:46.000 UTC Fri May 3 2002
User last activity at: *05:59:52.000 UTC Fri May 3 2002
SMTP Forwarding: NO
Initial TCP captivate: NO
TCP Advertisement captivate: NO
Default Service: NONE
DNS Default Service: NONE
Active Services: internet-blue;
AutoService: internet-blue;
Subscribed Services: internet-blue; iptv; games; distlearn; corporate; shop; banking;
vidconf;
Subscribed Service Groups: NONE
```

**Mobile IP Host: Example**

The following example shows information about a mobile IP host with an IP address of 10.0.0.0:

```
Router# show ssg host 10.0.0.0

----- HostObject Content -----
Activated: TRUE
Interface:
User Name: user1
Owner Host: 10.0.0.0
```

```

Msg IP: 0.0.0.0 (0)
Host DNS IP: 0.0.0.0
Proxy logon from client IP: 10.0.48.4
  Device: HA
  NASIP : 10.0.48.4
  SessID: 44444445
  APN   :
  MSID  : 5551001
  Timer : None
Maximum Session Timeout: 0 seconds
Host Idle Timeout: 60000 seconds
Class Attr: NONE
User policing disabled
User logged on since: *06:01:02.000 UTC Fri May 3 2002
User last activity at: *06:01:09.000 UTC Fri May 3 2002
SMTP Forwarding: NO
Initial TCP captivate: NO
TCP Advertisement captivate: NO
Default Service: NONE
DNS Default Service: NONE
Active Services: internet-blue;
AutoService: internet-blue;
Subscribed Services: internet-blue; iptv; games; distlearn; corporate; shop; banking;
vidconf;
Subscribed Service Groups: NONE

```

### Two Hosts with the Same IP Address: Examples

The following example shows two host objects with the same IP address:

```
Router# show ssg host 10.3.1.1
```

```
SSG:Overlapping hosts for IP 10.3.1.1 at interfaces:FastEthernet0/0/0
Virtual-Access1
```

In this case, use the *interface* argument to uniquely identify the host:

```
Router# show ssg host 10.3.1.1 FastEthernet0/0/0
```

```
.
.
.
```



#### Note

Note that the output produced by this command is the same as that produced by the command without the *interface* argument. The *interface* argument is used to uniquely identify a host only when there are overlapping host IP addresses.

The following example shows the usernames logged in to the active hosts:

```
Router# show ssg host username
```

```

1:10.3.1.1      (active) Host name:pppoauser
2:10.3.6.1      (active) Host name:ssguser2

```

```
### Total HostObject Count(including inactive hosts):2
```

### Host Associated with a VRF: Example

The following sample output for the **show ssg host** command shows a VRF called “BLUE” associated with a host that has the IP address 10.0.0.2:

```
Router# show ssg host 10.0.0.2
```

```
----- HostObject Content -----
```

```
Activated: TRUE
Interface: Ethernet1/0   VRF Name: BLUE
User Name: prep-user1
Owner Host: 10.0.0.2
```

**Subnet-Based Subscriber: Example**

The following example shows information about a subnet-based subscriber with an IP address of 10.0.0.0 and a subnet mask of 255.255.255.0:

```
Router# show ssg host 10.0.0.0 255.255.255.0

----- HostObject Content -----
Activated: TRUE
Interface:
User Name: user1
Host IP : 10.0.0.0
Mask : 255.255.255.0
Msg IP: 0.0.0.0 (0)
Host DNS IP: 0.0.0.0
Maximum Session Timeout: 0 seconds
Host Idle Timeout: 60000 seconds
Class Attr: NONE
User policing disabled
User logged on since: *05:59:46.000 UTC Fri May 3 2004
User last activity at: *05:59:52.000 UTC Fri May 3 2004
SMTP Forwarding: NO
Initial TCP captivate: NO
TCP Advertisement captivate: NO
Default Service: NONE
DNS Default Service: NONE
Active Services: NONE
AutoService: NONE
Subscribed Services: passthru1; proxynat1; tunnel1; proxy1
Subscribed Service Groups: NONE
```

Table 3 describes the significant fields shown in the displays.

**Table 3 show ssg host Field Descriptions**

Field	Description
Activated:	State of host object. Can be activated or inactivated. Activated—IP address has been assigned to the host, and the host object was created successfully Inactivated—A host is inactivated in the following situations: <ul style="list-style-type: none"> <li>When SSG, acting as a RADIUS proxy, is waiting for the IP address of the host, the host object is created, but the state is inactive.</li> <li>If a host that is using PPP logs off from SSG, but the virtual-access interface of that PPP host is still up, SSG moves the host object to the inactivated state.</li> </ul>
Interface:	The interface on the SSG device from which the SSG host is routable.
User Name:	Username that is used to authenticate the host at the authentication, authorization, and accounting (AAA) server.

**Table 3** show ssg host Field Descriptions (continued)

Field	Description
VRF Name:	VRF associated with the interface for the host.
Owner Host:	IP address and subnet mask assigned to host object.
Msg IP:	IP address of the messaging server. SSG notifies the messaging server of events such as the logging off of a host, an idle-timeout expiration, and a session-timeout expiration. The default messaging server is Subscriber Edge Services Manager (SESM).
Host DNS IP:	IP address of the Domain Name System (DNS) server of the host. This server will be used only if DNS queries cannot be forwarded to a DNS server for the services that are subscribed to by the host.
Device:	Type of device. Device types can be a home agent (HA), Packet Data Serving Node (PDSN), or Generic (for non-CDMA2000 devices).
SessID:	A numeric string derived from the attribute specified as the Session-Identifier.
Timer:	Timer type can be None, Wait for IP, Hand-off, or Wait for MSID.
Maximum Session Timeout:	Session timeout value (RADIUS attribute 27) defined in the user profile. The session timeout value is the amount of time for which the user will stay active after logging on. After this timer expires, the host object is deleted.
Host Idle Timeout:	Maximum amount of time that a host can stay idle (not forwarding any traffic) before the host is deleted from SSG.
Class Attr:	Class attribute (RADIUS attribute 25) defined in the user profile. The class attribute is sent in all host accounting records. This attribute is used by some accounting servers.
User logged on since:	Time at which the user logged on to SSG.
User last activity at:	Last time the user forwarded traffic via SSG.
Default Service:	This field is not currently supported.
DNS Default Service:	This field is not currently supported.
Active Services:	List of services to which the host has logged on.
AutoService:	List of services to which the host logged on at the time of SSG host logon. These services are defined in the user profile, and the user can access these services after logging on to SSG.
Subscribed Services:	List of services to which the host is able to log on.

**Related Commands**

Command	Description
<b>clear ssg host</b>	Removes a host object or a range of host objects.
<b>ssg port-map</b>	Enables the SSG port-bundle host key.

# show ssg interface

To display information about Service Selection Gateway (SSG) interfaces, use the **show ssg interface** command in user EXEC or privileged EXEC mode.

**show ssg interface** [*interface* | **brief**]

Syntax Description		
<i>interface</i>	(Optional)	Specific interface for which to display information.
<b>brief</b>	(Optional)	Gives brief information about each of the SSG interfaces and their usage.

Command Modes	
	User EXEC
	Privileged EXEC

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 this command without any keywords or arguments to display information about all SSG interfaces.

**Examples** The following example shows the **show ssg interface brief** command:

```
Router# show ssg interface brief
```

```
Interface   Direction           bindingtype   Status
ATM3/0.1    Uplink              Dynamic       Up
ATM3/0.2    Downlink            Static        Down
```

Related Commands	Command	Description
	<b>show ssg binding</b>	Displays service names that have been bound to interfaces and the IP addresses to which they have been bound.
	<b>show ssg direction</b>	Displays the direction of all interfaces for which a direction has been specified.
	<b>show ssg summary</b>	Displays a summary of the SSG configuration.

# show ssg multidomain ppp exclude-list

To display the contents of a PPP Termination Aggregation-Multidomain (PTA-MD) exclusion list, use the **show ssg multidomain ppp exclude-list** command in privileged EXEC mode.

**show ssg multidomain ppp exclude-list**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

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** This command is used to verify the contents of a PTA-MD exclusion list.

## 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 authentication, authorization, and accounting (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 command-line interface (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
<b>download exclude-profile (SSG PTA-MD)</b>	Downloads the PTA-MD exclusion list from the AAA server to the router.
<b>exclude (SSG PTA-MD)</b>	Adds a domain name to the existing PTA-MD exclusion list.
<b>ssg multidomain ppp</b>	Enters PTA-MD configuration mode.

# show ssg next-hop

To display the next-hop table, use the **show ssg next-hop** command in privileged EXEC mode.

**show ssg next-hop** [**begin** *expression* | **exclude** *expression* | **include** *expression*]

Syntax Description	begin	(Optional) Displays lines beginning with the line that contains <i>expression</i> .
	<i>expression</i>	(Optional) Word or phrase used to determine what lines will be shown.
	<b>exclude</b>	(Optional) Excludes lines that contain <i>expression</i> .
	<b>include</b>	(Optional) Includes lines that contain <i>expression</i> .

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 display all next-hop IP addresses.
------------------	--

**Examples** The following example shows the next-hop table:

```
Router# show ssg next-hop

Next hop table loaded from profile prof-nhg:
  WhipitNet          -> 192.168.1.6
  Service1.com       -> 192.168.1.3
  Service2.com       -> 192.168.1.2
  Service3.com       -> 192.168.1.1
  GoodNet            -> 192.168.1.2
  Perfctest          -> 192.168.1.5
End of next hop table.
```

Related Commands	Command	Description
	<b>clear ssg next-hop</b>	Removes the next-hop table.
	<b>ssg next-hop download</b>	Downloads the next-hop table from a RADIUS server.

# show ssg open-garden

To display a list of all configured open garden services, use the **show ssg open-garden** command in privileged EXEC mode.

```
show ssg open-garden
```

**Syntax Description** This command has no keywords or arguments.

**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.

**Examples** In the following example, all configured open garden services are displayed:

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

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

Related Commands	Command	Description
	<b>local-profile</b>	Configures a local service profile.
	<b>ssg open-garden</b>	Designates a service, defined in a local service profile, as an open garden service.
	<b>ssg service-search-order</b>	Specifies the order in which SSG searches for a service profile.

# show ssg pass-through-filter

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

```
show ssg pass-through-filter [begin expression | exclude expression | include expression]
```

Syntax Description	begin	(Optional) Begin with the line that contains <i>expression</i> .
	<i>expression</i>	(Optional) Word or phrase used to determine what lines will be shown.
	<b>exclude</b>	(Optional) Exclude lines that contain <i>expression</i> .
	<b>include</b>	(Optional) Include lines that contain <i>expression</i> .

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 display the downloaded transparent pass-through filter. The filter prevents pass-through traffic from accessing the specified IP address and subnet mask combinations. The filter is set using the **ssg pass-through** command.

To display a filter defined on the command line, use the **show running-config** command.

**Examples**

The following example shows the pass-through filter:

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

Service name: filter01
Password: cisco

Direction: Uplink

Extended IP access list (SSG ACL)
 permit tcp 172.16.6.0 0.0.0.255 any eq telnet
 permit tcp 172.16.6.0 0.0.0.255 192.168.250.0 0.0.0.255 eq ftp
```

Related Commands	Command	Description
	<b>clear ssg pass-through-filter</b>	Removes the downloaded filter for transparent pass-through.
	<b>ssg pass-through</b>	Enables transparent pass-through.

# show ssg pending-command

To display current pending commands, such as next-hop or filters, use the **show ssg pending-command** command in privileged EXEC mode.

**show ssg pending-command**

**Syntax Description** This command has no keywords or arguments.

**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 display the current pending commands.

**Examples** The following example shows the pending commands:

```
Router# show ssg pending-command

SSG pending command list:
  ssg bind service Service1.com 192.168.103.1
  ssg bind service Perfctest206 192.168.104.5
```

Related Commands	Command	Description
	<b>clear ssg pending-command</b>	Removes all pending commands.

# show ssg port-map ip

To display information about a particular port bundle, use the **show ssg port-map ip** command in privileged EXEC mode.

```
show ssg port-map ip ip-address port port-number
```

## Syntax Description

<i>ip-address</i>	IP address used to identify the port bundle.
<b>port</b> <i>port-number</i>	TCP port number used to identify the port bundle.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(2)B	This command was introduced on the Cisco 6400 series.
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.
12.3(11)T	This command was modified to display the downlink VRF associated with the port bundle.

## Usage Guidelines

This command displays the following information about a port bundle:

- Port maps in the port bundle
- IP address of the subscriber
- Interface through which the subscriber is connected
- Downlink VRF

## Examples

The following is sample output for the **show ssg port-map ip** command:

```
Router# show ssg port-map ip 25.0.0.1 port 64

State = RESERVED
Subscriber Address = 10.1.1.1
Downlink Interface = Ethernet1/0
Downlink VRF = BLUE

Port-mappings:-

Subscriber Port: 1           Mapped Port: 1039
```

[Table 4](#) describes the significant fields shown in the display.

**Table 4** *show ssg port-map ip Field Descriptions*

<b>Field</b>	<b>Description</b>
State	Port bundle status.
Subscriber Address	Subscriber IP address.
Downlink Interface	Interface through which the subscriber is connected.
Downlink VRF	VRF associated with the port bundle.
Port-mappings	Port maps in the port bundle.
Subscriber Port	Subscriber port number.
Mapped Port	Port assigned by SSG.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show ssg port-map status</b>	Displays information on port bundles.

# show ssg port-map status

To display information on port bundles, use the **show ssg port-map status** command in privileged EXEC mode.

**show ssg port-map status** [**free** | **reserved** | **inuse**]

Syntax Description	free	(Optional) Lists the port bundles that are in the “free” state for each bundle group.
	reserved	(Optional) Lists the port bundles that are in the “reserved” state for each bundle group. Also displays the associated subscriber IP address and interface for each port bundle.
	inuse	(Optional) Lists the port bundles that are in the “inuse” state for each bundle group. Also displays the associated subscriber IP address and interface for each port bundle.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(2)B	This command was introduced on the Cisco 6400 series.
	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** Entered without any keywords, the command displays a summary of all port-bundle groups, including the following information:

- A list of port-bundle groups
- Port-bundle length
- Number of free, reserved, and in-use port bundles in each group

## Examples

### Display All Bundles Example

The following example shows output for the **show ssg port-map status** command with no keywords:

```
Router# show ssg port-map status
```

```
Bundle-length = 4
```

```
Bundle-groups:-
```

```
IP Address           Free Bundles      Reserved Bundles  In-use Bundles
10.13.60.2           4032              0                  0
```

[Table 5](#) describes the significant fields shown in the display.

**Table 5** *show ssg port-map status Field Descriptions*

Field	Description
Bundle-length	The bundle-length value indicates the number of ports per bundle and the number of bundles per bundle group.
Bundle-groups	List of bundle groups.
IP Address	IP address of a bundle group.
Free Bundles	Number of free bundles in the specified bundle group.
Reserved Bundles	Number of reserved bundles in the specified bundle group.
In-use Bundles	Number of in-use bundles in the specified bundle group.

**Display In-Use Bundles Example**

The following example shows output for the **show ssg port-map status** command with the **inuse** keyword:

```
Router# show ssg port-map status inuse
Bundle-group 70.13.60.2 has the following in-use port-bundles:-
Port-bundle          Subscriber Address      Interface
64                   10.10.3.1              Virtual-Access2
```

Table 6 describes the significant fields shown in the display.

**Table 6** *show ssg port-map status inuse Field Descriptions*

Field	Description
Port-bundle	Port-bundle number.
Subscriber Address	Subscriber IP address of the subscriber.
Interface	Interface through which the subscriber is connected.

**Related Commands**

Command	Description
<b>show ssg port-map ip</b>	Displays information on a particular port bundle.

# show ssg prepaid default-quota

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

## show 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.

Note that the value of the counter for currently allocated default quotas will be zero when the prepaid billing server is available. The counter for currently allocated default quotas restarts at 1 each time the prepaid billing server becomes unavailable.

The **clear ssg prepaid default-quota** command clears the SSG default quota counters.

**Examples** The following example shows sample output for the **show ssg prepaid default-quota** command:

```
Router# show ssg prepaid default-quota

### Total default quotas allocated since this counter was last cleared:10

      Default Quota Threshold:100
      Currently allocated Default Quotas:4
```

[Table 7](#) describes the significant fields shown in the display.

**Table 7** *show ssg prepaid default-quota Field Descriptions*

Field	Description
Total default quotas allocated since this counter was last cleared	Total number of default quotas allocated by SSG since the last time the <b>clear ssg prepaid default-quota</b> command was entered.

**Table 7** *show ssg prepaid default-quota Field Descriptions (continued)*

<b>Field</b>	<b>Description</b>
Default Quota Threshold	The maximum number of default quotas that SSG will allocate each time the prepaid billing server is unavailable. This value can be configured by using the <b>ssg prepaid threshold</b> command.
Currently allocated Default Quotas	Number of default quotas allocated by SSG during the current instance of prepaid billing server unavailability.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>clear ssg prepaid default-quota</b>	Clears the SSG prepaid default quota counters.
<b>ssg prepaid threshold</b>	Configures an SSG prepaid threshold value.

## show ssg radius-proxy

To display a list of all RADIUS proxy clients, details of a particular RADIUS proxy client, or the pool of IP addresses configured for a router or for a specific domain, use the **show ssg radius-proxy** command in privileged EXEC mode.

```
show ssg radius-proxy [ip-address [vrf vrf-name]] | [address-pool [domain domain-name] [free | inuse]]
```

Syntax Description		
<i>ip-address</i>	(Optional)	Details for the RADIUS proxy client at this IP address.
<b>vrf</b> <i>vrf-name</i>	(Optional)	Details for the RADIUS proxy client associated with the specified VRF.
address-pool	(Optional)	IP addresses configured in an IP pool.
<b>domain</b>	(Optional)	IP addresses configured for a specific domain.
<i>domain-name</i>	(Optional)	Name of the domain to display.
<b>free</b>	(Optional)	IP addresses currently available in the free pool.
<b>inuse</b>	(Optional)	IP addresses currently in use.

**Defaults** Displays a list of RADIUS proxy clients.

**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.
	12.2(15)B	This command was enhanced to allow display of a list of RADIUS proxy clients.
	12.3(4)T	The enhancements from Cisco IOS Release 12.2(15)B were integrated into Cisco IOS Release 12.3(4)T.
	12.3(11)T	This command was enhanced to display information about VRFs associated with RADIUS proxy clients.

**Usage Guidelines** Use the **show ssg radius-proxy** command without any keywords or arguments to display a list of RADIUS proxy clients. This command also displays the IP addresses, device types, timers, and the number of proxy users for each proxy client. Use the *ip-address* argument to display the full list of proxy users for the specified RADIUS proxy client.

Use the **address-pool** keyword to display the IP address pools configured for a router or for a specific domain. You can also display which IP addresses are available or are in use.

**Examples**

The following example shows how to display a list of RADIUS proxy clients:

```
Router# show ssg radius-proxy

::: SSG RADIUS CLIENT TABLE :::

Client IP      VRF          Device type  Users
100.0.0.2     Global       PDSN         2
10.1.1.1      BLUE         HA           1
```

The following example shows how to display details about the RADIUS proxy client at IP address 172.16.0.0:

```
Router# show ssg radius-proxy 172.16.0.0

::: SSG RADIUS PROXY LOGON TABLE :::

User           SessionID    Host IP      Timer      IP Tech
user1          12345678    50.0.0.100  None      Simple
user1          12345679    (no host)   None      Mobile
```

The following example shows how to display information for IP addresses in the IP address pool:

```
Router# show ssg radius-proxy address-pool

Global Pool:  Free Addresses= 10234  Inuse Addresses= 0
```

The following example shows how to display information about the IP addresses in the IP address pool in the domain called "ssg.com":

```
Router# show ssg radius-proxy address-pool domain ssg.com

Domain Pool(ssg.com):  Free Addresses= 20  Inuse Addresses= 10
```

The following example shows how to display information about the IP addresses in the IP address pool for the domain called "ssg.com" that are currently in use:

```
Router# show ssg radius-proxy address-pool domain ssg.com inuse

Inuse Addresses in Domain Pool(ssg.com):10
19.1.5.1
19.1.5.2
19.1.5.3
19.1.5.4
19.1.5.5
19.1.5.6
19.1.5.7
19.1.5.8
19.1.5.9
19.1.5.10
```

The following example shows how to display information about the IP addresses in the IP address pool for the domain called "ssg.com" that are currently available:

```
Router# show ssg radius-proxy address-pool domain ssg.com free

Free Addresses in Domain Pool(ssg.com):20
19.1.5.11
19.1.5.12
19.1.5.13
19.1.5.14
19.1.5.15
19.1.5.16
19.1.5.17
19.1.5.18
```

19.1.5.19  
 19.1.5.20  
 19.1.5.21  
 19.1.5.22  
 19.1.5.23  
 19.1.5.24  
 19.1.5.25  
 19.1.5.26  
 19.1.5.27  
 19.1.5.28  
 19.1.5.29  
 19.1.5.30

Table 8 describes significant fields shown in the displays.

**Table 8** show ssg radius-proxy Field Descriptions

Field	Description
Client IP	IP address of the client device.
VRF	Name of the VRF associated with a RADIUS proxy client. The value "Global" indicates that the client is not associated with a VRF.
Device type	Type of client device. Device types can be PDSN, HA, or Generic (for non-CDMA2000 devices).
Users	Number of users connected to client device.
User	The user name for the end user.
SessionID	A numeric string derived from the attribute specified as the "Session-Identifier".
Host IP	IP address of the user.
Timer	Timer type can be "None", "Wait for IP", "Hand-off" or "Wait for MSID".
IP Tech	IP technology: simple or mobile.

#### Related Commands

Command	Description
<b>debug radius</b>	Displays information associated with RADIUS.
<b>debug ssg ctrl-errors</b>	Displays all error messages for control modules.
<b>debug ssg ctrl-event</b>	Displays all event messages for control modules.
<b>debug ssg ctrl-packet</b>	Displays packet contents handled by control modules.
<b>debug ssg data</b>	Displays all data-path packets.
<b>show ssg binding</b>	Displays service names that have been bound to interfaces and the interfaces to which they have been bound.
<b>show ssg connection</b>	Displays the connections of a given host and a service name.
<b>show ssg service</b>	Displays the information for a service.

# show ssg service

To display the information for a Service Selection Gateway (SSG) service, use the **show ssg service** command in privileged EXEC mode.

```
show ssg service [service-name [begin expression | exclude expression | include expression]]
```

## Syntax Description

<i>service-name</i>	(Optional) Name of an active Service Selection Gateway (SSG) service.
<b>begin</b>	(Optional) Begin with the line that contains <i>expression</i> .
<i>expression</i>	(Optional) Word or phrase used to determine what lines will be shown.
<b>exclude</b>	(Optional) Exclude lines that contain <i>expression</i> .
<b>include</b>	(Optional) Include lines that contain <i>expression</i> .

## Defaults

If no service name is provided, the command displays information for all services.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.0(3) DC	This command was introduced on the Cisco 6400 node route processor.
12.1(1) DC1	The output of this command was modified on the Cisco 6400 node route processor to display the following Service-Info Attributes when they are present in the proxy RADIUS service profile: <ul style="list-style-type: none"> <li>• Service-Defined Cookie</li> <li>• Full Username Attribute</li> </ul>
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.
12.3(1a)BW	This command was modified to display the attribute filter that is set in the service profile.
12.3(3)B	The modifications in Release 12.3(1a)BW were integrated into Cisco IOS Release 12.3(3)B. The output for this command was modified to display information about default DNS redirection.
12.3(7)T	The modifications in Release 12.3(3)B were integrated into Cisco IOS Release 12.3(7)T.
12.3(8)T	The output of this command was modified to display traffic counters for open garden services.
12.4	This command was integrated into Cisco IOS Release 12.4.

## Usage Guidelines

Use this command to display connection information for a service.

**Examples****Open Garden Service: Example**

The following example show output for the **show ssg service** command for an open garden service called “dnsB-service”:

```
Router# show ssg service dnsB-service

----- ServiceInfo Content -----

Uplink IDB: ATM3/0.10
Name: dnsB-service
Binding:

ATM3/0.10 gw: 10.11.11.2 distance: 0
Type: PASS-THROUGH
Mode: CONCURRENT
DHCP pool name :
Service Session Timeout: 0 seconds
Service Idle Timeout: 0 seconds
Service refresh timeleft: 48 minutes
No Prepaid Authorization Required
Authentication Type: NONE
Session policing disabled
Reference Count: 1

DNS Server(s): Primary: 10.0.0.2 (Backup: 10.0.0.2 )
IP 10.0.0.2 : req=0 rep=0 (UP)
IP 10.0.0.2 : req=0 rep=0 (UP)

No Radius server group created. No remote Radius servers.

ConnectionCount 0
Full User Name not used

Domain List: ssg;
  OpenGarden Service:
Input Bytes = 0, Input packets = 0
Output Bytes = 0, Output packets = 0
  Included Network Segments:
10.0.0.0/255.0.0.0

Active Connections:

----- End of ServiceInfo Content -----
```

**L2TP Tunnel Service: Example**

The following example shows the information for the L2TP tunnel service called “tunnell”. The attribute filter that is set in the service profile can be seen in the output.

```
Router# show ssg service tunnell

----- ServiceInfo Content -----

Uplink IDB: gw: 0.0.0.0
Name: tunnell
Type: TUNNEL
Mode: CONCURRENT
Service Session Timeout: 0 seconds
Service Idle Timeout: 0 seconds
Service refresh timeleft: 99 minutes
No Authorization Required
Authentication Type: CHAP
Attribute Filter: 31
Session policing disabled
```

```

Reference Count: 1

DNS Server(s):
No Radius server group created. No remote Radius servers.

TunnelId: ssg1
TunnelPassword: cisco
HomeGateway Addresses: 172.0.0.1
ConnectionCount 1
Full User Name not used

Domain List: Included Network Segments:
              0.0.0.0/0.0.0.0

Active Connections:
      1      : RealIP=172.0.1.1, Subscriber=10.0.1.1

----- End of ServiceInfo Content -----

```

**Proxy Service: Example**

The following example shows information for the proxy service called “serv1-proxy”:

```

Router# show ssg service serv1-proxy

----- ServiceInfo Content -----
Uplink IDB:
Name:serv1-proxy
Type:PROXY
Mode:CONCURRENT
Service Session Timeout:0 seconds
Service Idle Timeout:0 seconds
Class Attr:NONE
Authentication Type:CHAP
Reference Count:1

Next Hop Gateway Key:my-key

DNS Server(s):Primary:10.13.1.5

Radius Server:IP=10.13.1.2, authPort=1645, acctPort=1646, secret=my-secret

Included Network Segments:
      10.13.0.0/255.255.0.0
Excluded Network Segments:
Full User Name Used
Service Defined Cookie exist

Domain List:servicel.com;

Active Connections:
      1      :Virtual=255.255.255.255, Subscriber=10.20.10.2

----- End of ServiceInfo Content -----

```

Table 9 describes the significant fields shown in the display.

**Table 9** *show ssg service Field Descriptions*

Field	Description
Uplink IDB	Interface through which the service is reachable.
Name	Service name.
Type	Type of service.
Mode	One of the following values: Concurrent—user can log into this service and other services simultaneously. Sequential—user cannot log into this service simultaneously with other services.
Service Session Timeout	Period of time after which the session (SSG connection) will be terminated.
Service Idle Timeout	If the session (SSG connection) is idle for this many seconds, the session will be terminated.
Service refresh timeleft	Amount of time after which SSG will refresh the service profile.
Authentication Type	Type of authentication that will be used for proxy or tunnel services. Values are PAP and CHAP.
Attribute Filter	RADIUS attribute that is being filtered out from user authentication.
Next Hop Gateway Key	Defines the next-hop binding. Services can be bound to the next hop using next-hop gateways. The key to next-hop-gateway mapping is present in the next-hop profile.
DNS Server(s)	DNS server used for this service.
TunnelId	ID for tunneling services.
TunnelPassword	Password for tunneling services.
HomeGateway Addresses	IP address of the LNS.
Radius Server: IP authPort acctPort secret	Information about the RADIUS server where proxy users are authenticated for service connectivity.
Input Bytes	Number of bytes sent to the open garden service.
Input packets	Number of packets sent to the open garden service.
Output Bytes	Number of bytes sent from the open garden service.
Output packets	Number of packets sent from the open garden service.
Included Network Segments	IP address subnets that form the service network.
Excluded Network Segments	IP address subnets that are excluded from the service network.

**Table 9** *show ssg service Field Descriptions (continued)*

<b>Field</b>	<b>Description</b>
Full User Name Used	Indicates that the RADIUS authentication and accounting requests use the full username (user@service).
Service Defined Cookie exist	Indicates that user-defined information is included in RADIUS authentication and accounting requests.
Domain List	List of domain names that belong to the service and can be resolved by the DNS server specified for this service.
Active Connections Virtual Subscriber	Lists the host IP address for active connections. The subscriber IP address is the IP address of the host. In cases where there is a service-defined NAT, the virtual IP address is not zero and is the IP address given by the service.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>clear ssg service</b>	Removes a service.
<b>show ssg binding</b>	Displays service names that have been bound to interfaces and the interfaces to which they have been bound.
<b>ssg bind service</b>	Specifies the interface for a service.

# show ssg summary

To display a summary of the Service Selection Gateway (SSG) configuration, use the **show ssg summary** command in user EXEC or privileged EXEC mode.

**show ssg summary**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** User EXEC  
Privileged EXEC

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 this command to display information such as which SSG features are enabled, how many users are active, how many services are active, and what filters are active.

**Examples** The following example shows the **show ssg summary** command:

```
Router# show ssg summary

SSG Features Enabled:
TCP Redirect: Unauthenticated, Service, Captive portal.
QOS: User policing, Session Policing.
Host Key: Enabled
```

Related Commands	Command	Description
	<b>show ssg binding</b>	Displays service names that have been bound to interfaces and the IP addresses to which they have been bound.
	<b>show ssg direction</b>	Displays the direction of all interfaces for which a direction has been specified.
	<b>show ssg interface</b>	Displays information about SSG interfaces.

# show ssg tcp-redirect group

To display information about the captive portal groups and the networks associated with those portal groups, use the **show ssg tcp-redirect group** command in privileged EXEC mode.

**show ssg tcp-redirect group** [*group-name*]

<b>Syntax Description</b>	<i>group-name</i>	(Optional) The previously defined name for the captive portal group.
---------------------------	-------------------	--

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(4)B	This command was introduced. This command replaced the <b>show ssg http-redirect group</b> command.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
	12.3(1a)BW	This command was modified to display the access lists that are associated with TCP redirection.
	12.3(3)B	The modifications in Release 12.3(1a)BW were integrated into Cisco IOS Release 12.3(3)B.
	12.3(103)T	The modifications in Release 12.3(3)B were integrated into Cisco IOS Release 12.3(103)T.

**Usage Guidelines** Use this command to display information about the captive portal groups and their associated networks as defined in your system.

If you omit the optional *group-name* argument, this command displays a list of all defined captive portal groups. If you specify the *group-name* argument, this command displays information about that group and its associated networks.

**Examples** The following example shows how to display a list of all of the defined captive portal groups:

```
Router# show ssg tcp-redirect group

Current TCP redirect groups:
  SESM1
  SESM2
Default access-list: 101
Default unauthenticated user redirect group: None Set
Default service redirect group: None Set
Prepaid user default redirect group: None Set
SMTP forwarding group: None Set
Default initial captivation group: None Set
Default advertising captivation group: None Set
```

[Table 10](#) describes the significant fields shown in the display.

**Table 10** show ssg tcp-redirect group Field Descriptions

Field	Description
Current TCP redirect groups	List of all TCP-redirect groups.
Default access-list	
Default unauthenticated user redirect group	
Default service redirect group	Default service redirect group.
Prepaid user default redirect group	
SMTP forwarding group	SMTP redirection settings.
Default initial captivation group	Name of the default initial captivation group and duration of captivation.
Default advertising captivation group	Name of the default advertising captivation group and duration and frequency of advertising captivation.

The following example shows how to display a detailed description of the captive portal group called “RedirectServer”:

```
Router# show ssg tcp-redirect group RedirectServer
```

```
TCP redirect group RedirectServer:
Showing all TCP servers (Address, Port):
 10.2.36.253, 8080, FastEthernet0/0
Networks to redirect to (network-list RedirectNw):
 172.16.10.0 /24
 172.20.0.0 /16
TCP port to redirect:
 80
```

Table 11 describes the significant fields shown in the display.

**Table 11** show ssg tcp-redirect group group-name Field Descriptions

Field	Description
Showing all TCP servers (Address, Port)	List of all servers.
10.2.36.253	Server IP address.
8080	Server port number.
FastEthernet0/0	Interface on which this server is reachable.
Networks to redirect to	List of networks.
(network-list RedirectNw)	Network list name.
TCP port to redirect	Name of port list (if port list is used).

**Related Commands**

Command	Description
<b>debug ssg tcp-redirect</b>	Turns on debug information for the SSG TCP Redirect for Services feature.
<b>network (ssg-redirect)</b>	Adds an IP address to a named network list.

<b>Command</b>	<b>Description</b>
<b>network-list</b>	Defines a list of one or more IP networks that make up a named network list.
<b>port (ssg-redirect)</b>	Adds a TCP port to a named port list.
<b>port-list</b>	Defines a list of one or more TCP ports that make up a named port list and enters SSG-redirect-port configuration mode.
<b>redirect captivate advertising default group</b>	Configures the default captive portal group and duration and frequency for advertising.
<b>redirect captivate initial default group duration</b>	Selects a default captive portal group and duration of the initial captivation of users on account logon.
<b>redirect port to</b>	Marks a TCP port or named TCP port list for SSG TCP redirection.
<b>redirect smtp group</b>	Selects a captive portal group for redirection of SMTP traffic.
<b>redirect unauthenticated-user to</b>	Redirects the traffic from authenticated users to a specified captive portal group.
<b>redirect unauthorized-service to</b>	Sets a list of destination IP networks that can be redirected by a specified named captive portal group.
<b>server (SSG)</b>	Adds a server to a captive portal group.
<b>server-group</b>	Defines the group of one or more servers that make up a named captive portal group and enters SSG-redirect-group configuration mode.
<b>show tcp-redirect mappings</b>	Displays information about the TCP redirect mappings for hosts within your system.
<b>ssg tcp-redirect</b>	Enables SSG TCP redirect and enters SSG-redirect mode.

# show ssg user transparent

To display a list of all the Service Selection Gateway (SSG) transparent autologon users, use the **show ssg user transparent** command in privileged EXEC mode.

**show ssg user transparent**

**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 display the IP addresses and the states of all transparent autologon users that are active on SSG. The transparent autologon user states are passthrough (TP), suspect (SP), unidentified (NR), and waiting for authorization (WA).

**Examples** The following is sample output from the **show ssg user transparent** command:

```
Router# show ssg user transparent

10.10.10.10      Passthrough
11.11.11.11     Suspect
120.120.120.120 Authorizing

### Total number of transparent users: 3
```

Related Commands	Command	Description
	<b>ssg login transparent</b>	Enables the SSG Transparent Autologon feature.

# show ssg user transparent authorizing

To display a list of all Service Selection Gateway (SSG) transparent autologon users for whom authorization is in progress and who are waiting for authentication, authorization, and accounting (AAA) server response, use the **show ssg user transparent authorizing** command in privileged EXEC mode.

**show ssg user transparent authorizing [count]**

## Syntax Description

<b>count</b>	(Optional) Displays the number of authorizing users.
--------------	--

## 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 display all Service Selection Gateway (SSG) transparent autologon users that are waiting for authorization (WA).

## Examples

The following is sample output from the **show ssg user transparent authorizing** command with the **count** keyword:

```
Router# show ssg user transparent authorizing count
```

```
### Total number of WA users : 1
```

## Related Commands

Command	Description
<b>ssg login transparent</b>	Enables the SSG Transparent Autologon feature.

# show ssg user transparent passthrough

To display information about Service Selection Gateway (SSG) transparent autologon pass-through users, use the **show ssg user transparent passthrough** command in privileged EXEC mode.

**show ssg user transparent passthrough** [*ip-address* | **count**]

Syntax Description	
<i>ip-address</i>	(Optional) Display details for specified user IP address.
<b>count</b>	(Optional) Displays the number of pass-through users.

**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 display all SSG transparent autologon pass-through (TP) users that are active on SSG.

**Examples** The following is sample output from the **show ssg user transparent passthrough** command for the user having IP address 10.10.10.10:

```
Router# show ssg user transparent passthrough 10.10.10.10

User IP Address :      10.10.10.10
Session Timeout  :      200 (seconds)
Idle Timeout    :      100 (seconds)

User logged on since : *16:33:57.000 GMT Mon May 19 2003
User last activity at : *16:33:57.000 GMT Mon May 19 2003

Current Time : *16:35:17.000 GMT Mon May 19 2003
```

Related Commands	Command	Description
	<b>ssg login transparent</b>	Enables the SSG Transparent Autologon feature.

# show ssg user transparent suspect

To display a list of all Service Selection Gateway (SSG) transparent autologon suspect (SP) user IP addresses, use the **show ssg user transparent suspect** command in privileged EXEC mode.

**show ssg user transparent suspect [count]**

<b>Syntax Description</b>	<b>count</b>	(Optional) Displays the number of suspect users.
---------------------------	--------------	--

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	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.

<b>Usage Guidelines</b>	An SSG transparent autologon suspect user is a user whose authentication, authorization, and accounting (AAA) authorization resulted in an Access Reject.
-------------------------	---

<b>Examples</b>	The following is sample output from the <b>show ssg user transparent suspect</b> command with and without the <b>count</b> keyword:
-----------------	---

```
Router# show ssg user transparent suspect count
```

```
### Total number of SP users : 1
```

```
Router# show ssg user transparent suspect
```

```
94.0.0.1
```

```
### Total number of SP users : 1
```

```
Router#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ssg login transparent</b>	Enables the SSG Transparent Autologon feature.

# show ssg user transparent unidentified

To display a list of Service Selection Gateway (SSG) transparent autologon users for whom there is no response from the authentication, authorization, and accounting (AAA) server to an authorization request (unidentified users), use the **show ssg user transparent unidentified** command in privileged EXEC mode.

**show ssg user transparent unidentified [count]**

<b>Syntax Description</b>	<b>count</b> (Optional) Displays the number of unidentified (NR) users.
---------------------------	---

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	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.

<b>Usage Guidelines</b>	Use this command to display all SSG transparent autologon unidentified (NR) users that are active on the SSG.
-------------------------	---

<b>Examples</b>	The following is sample output from the <b>show ssg user transparent unidentified</b> command with and without the <b>count</b> keyword:
-----------------	--

```
Router# show ssg user transparent unidentified count

### Total number of NR (Unidentified) users : 1

Router# show ssg user transparent unidentified

          93.0.0.1

### Total number of NR (Unidentified) users : 1

Router#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ssg login transparent</b>	Enables the SSG Transparent Autologon feature.

# show ssg vc-service-map

To display virtual circuit (VC)-to-service-name mappings, use the **show ssg vc-service-map** command in privileged EXEC mode.

**show ssg vc-service-map** [*vpi/vci* | **service** *service-name*]

Syntax Description		
<i>vpi/vci</i>	(Optional) Virtual path identifier (VPI)/virtual channel identifier (VCI) value, including the slash; for example, 3/33.	
<b>service</b>	(Optional) Displays the VCs mapped to a service name.	
<i>service-name</i>	(Optional) Service name.	

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.0(5)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 display VC-to-service-name mappings.

**Examples** The following example shows the VCs mapped to the service name “Worldwide”:

```
Router# show ssg vc-service-map service Worldwide
Interface  From      To      Service Name      Type
All        3 /33    None    Worldwide          non-exclusive
```

Related Commands	Command	Description
	<b>ssg vc-service-map</b>	Maps VCs to service names.

# source ip

To specify Service Selection Gateway (SSG) source IP addresses to which to map the destination IP addresses in subscriber traffic, use the **source ip** command in SSG portmap configuration mode. To remove this specification, use the **no** form of this command.

```
source ip {ip-address | interface}
```

```
no source ip {ip-address | interface}
```

## Syntax Description

<i>ip-address</i>	SSG source IP address.
<i>interface</i>	Interface whose main IP address is used as the SSG source IP address.

## Defaults

No default behavior or values.

## Command Modes

SSG portmap configuration

## Command History

Release	Modification
12.2(16)B	This command was introduced. This command replaces the <b>ssg port-map source ip</b> command.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

## Usage Guidelines

With the SSG Port-Bundle Host Key feature, SSG maps the destination IP addresses in subscriber traffic to specified SSG source IP addresses.

All SSG source IP addresses configured with the **source ip** command must be routable in the management network where the Cisco Service Selection Dashboard (SSD) or Subscriber Edge Services Manager (SESM) resides.

If the interface for the source IP address is deleted, the port-map translations will not work correctly.

Because a subscriber can have several simultaneous TCP sessions when accessing a web page, SSG assigns a bundle of ports to each subscriber. Because the number of available port bundles is limited, you can assign multiple SSG source IP addresses (one for each group of port bundles). By default, each group has 4032 bundles, and each bundle has 16 ports. To modify the number of bundles per group and the number of ports per bundle, use the **length** command.

## Examples

The following example shows the SSG source IP address specified with an IP address and with specific interfaces:

```
ssg port-map
source ip 10.0.50.1
source ip Ethernet 0/0/0
ssg port-map source ip Loopback 1
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>length (SSG)</b>	Modifies the port-bundle length upon the next SSG reload.
ssg port-map	Enables the SSG port-bundle host key and enters SSG portmap configuration mode.