

# SSG AutoDomain

---

## Feature History

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

This document describes the SSG AutoDomain feature. It contains the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 6](#)
- [Supported Standards, MIBs, and RFCs, page 6](#)
- [Configuration Tasks, page 7](#)
- [Monitoring and Maintaining SSG AutoDomain, page 8](#)
- [Configuration Examples, page 9](#)
- [Command Reference, page 9](#)
- [Glossary, page 25](#)

## Feature Overview

When you configure SSG AutoDomain, users can automatically connect to a service based on either Access Point Name (APN) or the domain part of the structured username specified in an Access-Request. When SSG AutoDomain is configured, user authentication is not performed at the Network Access Server (NAS), but instead at the service (for example, at an authentication, authorization, and accounting (AAA) server within a corporate network).

### SSG

Service Selection Gateway (SSG) is a switching solution for service providers who offer intranet, extranet, and Internet connections to subscribers using broadband access technology such as xDSL, cable modems, or wireless to allow simultaneous access to network services.

SSG with Web Selection works in conjunction with the Cisco Service Selection Dashboard (SSD) or its successor product, the Cisco Subscriber Edge Services Manager (SESM). Together with the SESM or SSD, SSG provides subscriber authentication, service selection, and service connection capabilities to subscribers of Internet services. Subscribers interact with an SESM or SSD web application using a standard Internet browser.

SSG acts as a central control point for Layer 2 and Layer 3 services. This can include services available through ATM virtual circuits (VCs), virtual private dial-up networks (VPDNs), or normal routing methods.

SSG communicates with the AAA management network where Remote Access Dial-In User Service (RADIUS), Dynamic Host Configuration Protocol (DHCP), and Simple Network Management Protocol (SNMP) servers reside. The SSG also communicates with the Internet service provider (ISP) network, which may connect to the Internet, corporate networks, and value-added services.

A licensed version of SSG works with SESM or SSD to present to subscribers a menu of network services that can be selected from a single graphical user interface (GUI). This functionality improves flexibility and convenience for subscribers, and enables service providers to bill subscribers based on connect time and services used, rather than charging a flat rate.

The user opens an HTML browser and accesses the URL of the SESM or SSD web server application. SESM or SSD forwards user login information to SSG, which forwards the information to the AAA server.

- If the user is not valid, the AAA server sends an Access-Reject message.
- If the user is valid, the AAA server sends an Access-Accept message with information specific to the user profile about which services the user is authorized to use. SSG logs the user in, creates a host object in memory, and sends the response to SESM or SSD.

Based on the contents of the Access-Accept response, SESM or SSD presents a dashboard menu of services that the user is authorized to use, and the user selects one or more of the services. SSG then creates an appropriate connection for the user and starts RADIUS accounting for the connection.

Note that when a non-Point-to-Point Protocol (non-PPP) user, such as in a bridged-networking environment, disconnects from a service without logging off, the connection remains open and the user can reaccess the service without going through the login procedure. This is because no direct connection (PPP) exists between the subscribers and SSG. To prevent non-PPP users from being logged in to services indefinitely, be sure to configure the Session-Timeout and/or Idle-Timeout RADIUS attributes.

### Access Point Names

An APN identifies a Packet Data Network (PDN) that is configured on and accessible from a Gateway GPRS Support Node (GGSN). An access point is identified by its APN name. The Global System for Mobile Communication (GSM) standard 03.03 defines the following two parts of an APN:

- APN Network Identifier
- APN Operator Identifier

The APN Network Identifier is mandatory. The name of an access point in the form of an APN Network Identifier must correspond to the fully-qualified name in the Domain Name System (DNS) configuration for that network, and it must also match the name specified for the access point in the GGSN configuration. The GGSN also uniquely identifies an APN by an index number. The APN Operator Identifier is an optional name that consists of the fully-qualified DNS name, with the ending “.gprs.”

The access points that are supported by the GGSN are preconfigured on the GGSN. When a user requests a connection in the GPRS network, the APN is included in the Create Packet Data Protocol (PDP) Request message. The Create PDP Request message is a GPRS Tunneling Protocol (GTP) message that establishes a connection between the Serving GPRS Support Node (SGSN) and the GGSN.

An APN has several attributes associated with its configuration that define how users can access the network at that entry point. For more information about configuring APNs, see the [APN Manager Application Programming Guide](#).

**Note**

If the Access-Request received from the radius-client does not contain the Called-Station-ID (Attribute 30), then the NAS-Identifier (Attribute 32), if provided, is treated as the APN name.

**SSG AutoDomain**

Using SSG AutoDomain, you can automatically log in a user to a service based on either the APN or the domain portion of the structured username. The domain portion of the structured username is the portion after the @ in the username. For example, the domain in the username “abc@cisco.com” is “cisco.com”. Users can bypass the Service Selection Dashboard (SSD) and access a service, such as a corporate intranet. SSG AutoDomain is also supported for users logging in from an SESM or SSD.

SSG AutoDomain makes it possible to log in a user to either Layer 2 Tunnel Protocol (L2TP) or proxy services. The username and password used to log in a user with Autodomain is the username and password provided by the user when logging into the General Packet Radio Service (GPRS) network. This password can be a dynamically generated password.

SSG AutoDomain does not require SSG Vendor Specific Attributes (VSAs) when using a domain name as a means to determine which service to log in the user. Autodomain uses a heuristic to determine the service into which the user is logged. When using Autodomain, the host object is not activated until successfully authenticated with the service. If the autoservice connection fails for any reason, the user login is rejected and an Access-Reject is returned to the Gateway GPRS Support Node (GGSN).

By default, Autodomain service first checks for an APN (Called-Station-ID) and then for a structured username.

If Autodomain is enabled and the received Access-Request specifies an APN, then this APN is used for Autodomain selection unless it is a member of the APN Autodomain exclusion list. If an Autodomain is not selected based on APN, then the structured username is used. If a structured username is not supplied, or the supplied structured username is a member of the domain name exclusion list, then no Autodomain is selected and normal SSG user login proceeds. You can override these Autodomain selection defaults by configuring the **select** command in SSG-auto-domain mode. You can define the APN Autodomain exclusion list and the domain name exclusion list with the **exclude** command in SSG-auto-domain mode.

When Autodomain is enabled, an Autodomain profile is downloaded from the local AAA server. This profile is specified as an outbound service and the password is the globally configured service password.

Host objects are assigned an IP address by one of the following methods:

- Specified in the Access-Request
- Returned for an Autodomain tunnel, VPDN, or proxy service. If an IP address is assigned from an Autodomain tunnel, VPDN or proxy service, it does not have NAT enabled and must be non-overlapped and routable in the inside network. You can enable NAT at the tunnel by configuring the **nat user-address** command.
- Assigned from a previously configured IP local pool.

You can configure SSG AutoDomain in basic or extended mode. In basic mode, the Autodomain profile downloaded from the AAA server is a service profile. In extended Autodomain mode the profile downloaded from the AAA server is a “virtual user” profile that contains one autoservice to an authenticated service such as a proxy, VPDN, or a tunnel. The “virtual user” profile defines the Autodomain service. Connection to this autoservice occurs as it does for basic Autodomain, where the host object is not activated until the user is authenticated at the proxy, VPDN, or tunnel service. The presence of the SSD in extended Autodomain mode enables the user to access any other service in the specified user profile. If the “virtual user” profile does not have exactly one autoservice or the autoservice is not authenticated, the Autodomain login is rejected.

The Autodomain service profile can be a proxy, VPDN, or tunnel service. If the downloaded Autodomain service profile is a proxy service, then SSG authenticates the user to the appropriate domain AAA server with the authentication information found in the Access-Request received from the radius-client. If the downloaded Autodomain service profile is a tunnel service, a PPP session is regenerated into an L2TP tunnel for the selected service. If no SSG-specific attributes are returned indicating the type of service required, the SSG treats this service as a VPDN service and adds the following attributes to the service profile;

- Service network (R) as 0.0.0.0;0.0.0.0
- Service mode as concurrent (MC)
- Service type as tunnel (TT)

SSG then regenerates the PPP session for the specified service.

SSG AutoDomain attempts to log the user onto the remote service using the username and password specified in the original Access-Request. If the Autodomain is selected based on the realm part of the username, then only the “user” part of the name is used unless the “X” attribute is present in the service profile. For VPDN-only type services (where no SSG attributes are present), it is not possible to specify use of the full structured username.

If you configure basic SSG AutoDomain with a nonauthenticated service type such as passthrough, SSG rejects the login request because Autodomain bypasses user authentication at the local AAA server and requires that authentication be performed elsewhere.

If Autodomain proxy service responds with any RADIUS attributes, these attributes are added to the host profile. In Autodomain extended mode, the host profile is a “virtual user” profile. In Autodomain in basic mode, the host profile is a synthesized profile.

## Benefits

SSG AutoDomain provides the following benefits:

- Eliminates the need for users to be authenticated to SSG before connecting to a service. Users do not need to be authenticated multiple times.
- Eliminates the need for service providers to make changes to existing AAA servers for virtual private dialup network (VPDN) services.
- Provides an enhanced user experience.
- Provides subscribers with access to corporate VPNs based on APN alone.
- Enables users to access both simultaneous and sequential services without having to log out and log back in to access different services.
- Overlapping host IP addresses are supported.

## Restrictions

SSG AutoDomain has the following restrictions:

- Restricted support for DHCP. If DHCP is used for IP address assignment, it must be done prior to RADIUS negotiation.
- Passthrough services. Because local authentication at the Network Access Server (NAS) is being bypassed, Autodomain is available only for services where authentication is performed, such as proxy, VPDN, or tunnel services.

- “Virtual-user” profiles can contain only one AutoLogon service.
- If an Access-Request does not contain an IP address, a local per-domain or global IP address pool must be configured.
- Loose coupling of hosts objects and PDP contexts (when GGSN is a radius-client) can cause some error conditions not to be cleanly recovered without end-user intervention (such as reconnecting).

## Related Features and Technologies

- Cisco Subscriber Edge Services Manager
- HTTP Redirect-Login in Cisco IOS Release 12.1(5)DC on 6400 series routers. See the “Service Selection Gateway” chapter of the *Cisco 6400 Feature Guide* for Releases 12.1(5)DB and 12.1(5)DC for more information.
- Hierarchical Policing in SSG
- PPPoA/PPPoE Autosense for ATM PVCs
- SSG Accounting Update Interval Per Service
- SSG Autologoff and MAC Address in Accounting Records
- SSG AutoLogon Using Proxy Radius
- SSG Host Key Port Bundle
- SSG Open Garden
- SSG Prepaid
- SSG TCP Redirect for Services

## Related Documents

- *APN Manager Application Programming Guide*
- *Cisco 6400 Software Configuration Guide and Command Reference*
- *Cisco Subscriber Edge Services Documentation*
- *Cisco IOS Voice, Video, and Fax Command Reference*, Release 12.2
- *Cisco IOS Voice, Video, and Fax Configuration Guide*, Release 12.2
- *Configuring RADIUS*
- *Service Selection Gateway Hierarchical Policing*
- *Service Selection Gateway*
- *SSG AutoDomain*
- *SSG Autologoff*
- *SSG AutoLogon using Proxy RADIUS*
- *SSG Open Garden*
- *SSG Port-Bundle Host Key*
- *SSG Prepaid Billing*
- *SSG TCP Redirect for Services*

# Supported Platforms

- Cisco 6400 series
- Cisco 7200 series
- Cisco 7401ASR

## Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or Cisco Feature Navigator.

# Supported Standards, MIBs, and RFCs

## Standards

No new or modified standards are supported by this feature.

## MIBs

No new or modified MIBs are supported by this feature.

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

## RFCs

No new or modified RFCs are supported by this feature.

# Prerequisites

You must enable Cisco Express Forwarding (CEF) on the router before SSG functionality can be enabled. If CEF is not enabled and you attempt to configure SSG, the following error message is displayed:

```
SSG: Please enable ip cef first
```



---

**Note** You can disable CEF at the individual interface level without affecting SSG.

---

# Configuration Tasks

See the following sections for configuration tasks for the SSG AutoDomain feature. Each task in the list is identified as either required or optional.

- [Configuring SSG AutoDomain, page 7](#) (required)

## Configuring SSG AutoDomain

To configure SSG AutoDomain, issue the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# <b>ip cef</b>	Enables CEF.
Step 2	Router(config)# <b>ssg enable</b>	Enables SSG functionality.
Step 3	Router(config)# <b>ssg auto-domain</b>	Enables SSG AutoDomain and enters SSG-auto-domain configuration mode.
Step 4	Router(config-auto-domain)# <b>mode extended</b>	(Optional) Selects extended Autodomain.
Step 5	Router(config-auto-domain)# <b>select</b> { <b>username</b>   <b>called-station-id</b> }	(Optional) Configures the Autodomain selection method. <ul style="list-style-type: none"> <li>• <b>username</b>—Configures the algorithm to use only the domain portion of the username to select the Autodomain.</li> <li>• <b>called-station-id</b>—Configures the algorithm to use only the APN (Called-Station-ID).</li> </ul> <p>By default, Autodomain attempts to find a valid Autodomain based on APN (Called-Station-ID) followed by the domain portion of the username.</p>
Step 6	Router(config-auto-domain)# <b>exclude</b> { <b>apn</b>   <b>domain</b> } <i>name</i>	(Optional) Adds names to the Autodomain exclusion list. <ul style="list-style-type: none"> <li>• <b>apn</b>—Adds an APN to the exclusion list.</li> <li>• <b>domain</b>—Adds a domain to the exclusion list.</li> <li>• <i>name</i>—Name of the APN or domain to be added to the exclusion list.</li> </ul>
Step 7	Router(config-auto-domain)# <b>download</b> <b>exclude-profile</b> <i>profile-name password</i>	(Optional) Adds names to the Autodomain download exclusion list. <ul style="list-style-type: none"> <li>• <i>profile-name</i>—Specifies the name for a list of excluded names that may be downloaded from the AAA server.</li> <li>• <i>password</i>—Specifies the name for a list of excluded names that may be downloaded from the AAA server.</li> </ul>
Step 8	Router(config-auto-domain)# <b>nat</b> <b>user-address</b>	(Optional) Configures Network Address Translation (NAT) to be applied towards Autodomain services.

## Verifying SSG AutoDomain

Enter the **show running-config** command to verify configuration of SSG Autodomain:

```
Router# show running-config
```

```

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

```

## Monitoring and Maintaining SSG AutoDomain

Use the following commands to monitor and maintain SSG AutoDomain:

Command	Purpose
Router# <b>clear ssg radius-proxy client-address</b> <i>ip-address</i>	Clears all hosts connected to a specific RADIUS client. <ul style="list-style-type: none"> <li><i>ip-address</i>—IP address of a RADIUS client.</li> </ul>
Router# <b>clear ssg radius-proxy nas-address</b> <i>ip-address</i>	Clears all hosts connected to a specific Network Access Server (NAS). <ul style="list-style-type: none"> <li><i>ip-address</i>—IP address of a RADIUS client.</li> </ul>
Router# <b>debug ssg port-map events</b>	Displays port mapping event messages.
Router# <b>debug ssg port-map packets</b>	Displays port mapping packet contents.
Router# <b>show ssg auto-domain exclude-profile</b>	Displays the contents of an Autodomain exclusion profile downloaded from the AAA server. Only Autodomain exclude entries entered via CLI are displayed.
Router# <b>show ssg binding</b>	Displays service names that have been bound to interfaces and the interfaces to which they have been bound.
Router# <b>show ssg connection</b> <i>ip-address</i> <i>service-name</i>	Displays the connections of a given host and service name. <ul style="list-style-type: none"> <li><i>ip-address</i>—IP address of an active SSG connection. This is always a subscribed host.</li> <li><i>service-name</i>—The name of an active SSG connection.</li> </ul>
Router# <b>show ssg direction</b>	Displays the direction of all interfaces for which a direction has been specified.
Router# <b>show ssg host</b> [ <i>ip-address</i> ] [ <b>count</b> ] [ <b>username</b> ]	Displays the information about a subscriber and the current connections of the subscriber. <ul style="list-style-type: none"> <li><i>ip-address</i>—(Optional) IP address of the host.</li> <li><b>count</b>—(Optional) Displays the host object count, including inactive hosts.</li> <li><b>username</b>—(Optional) Displays the usernames logged into the active hosts.</li> </ul>
Router# <b>show ssg next-hop</b>	Displays the next-hop table.
Router# <b>show ssg pending-command</b>	Displays current pending commands.

Command	Purpose
Router# <code>show ssg service service-name</code>	Displays the information for a service. <ul style="list-style-type: none"> <li><code>service-name</code>—(Optional) Name of an active SSG service.</li> </ul>
Router# <code>show ssg radius-proxy address-pool [domain domain-name] [free   inuse]</code>	Displays the pool of IP addresses configured for a router or for a specific domain. <ul style="list-style-type: none"> <li><code>domain</code>—(Optional) IP addresses configured for a specific domain.</li> <li><code>domain-name</code>—(Optional) Name of the domain to display.</li> <li><code>free</code>—(Optional) IP addresses currently available in the free pool.</li> <li><code>inuse</code>—(Optional) IP addresses currently in use.</li> </ul>

## Configuration Examples

This section provides the following configuration examples:

- [Configuring SSG AutoDomain Example, page 9](#)

### Configuring SSG AutoDomain Example

In the following example, extended SSG AutoDomain is enabled. The default selection mode is configured so that SSG attempts to select an Autodomain based only on the username. An APN named “excluded” and a domain named “cisco” are added to the Autodomain exclusion list. An exclude-profile named “abc” with a password “password1” is added to the Autodomain download exclusion list. NAT is applied towards Autodomain services.

```

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

```

## Command Reference

This section documents new commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications. Additional SSG commands can be found in the [SSG Commands for the Cisco 6400 NRP](#) document.

- [download exclude-profile](#)
- [exclude](#)
- [mode extended](#)
- [nat user-address](#)
- [select](#)

- [show ssg auto-domain exclude-profile](#)
- [ssg auto-domain](#)

# download exclude-profile

To add domain or APN names to the Autodomain exclusion list, use the **download exclude-profile** command in SSG-auto-domain mode. To remove a name from the Autodomain exclusion list, use the **no** form of this command.

**download exclude-profile** *profile-name password*

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

## Syntax Description

<i>profile-name</i>	Specifies the name for a list of excluded names that may be downloaded from the AAA server.
<i>password</i>	Specifies the password for a list of excluded names that may be downloaded from the AAA server.

## Defaults

No default behavior or values.

## Command Modes

SSG-auto-domain

## Command History

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

## Usage Guidelines

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

X—Excluded name list entry

A—Add this name to the APN exclusion list

D—Add this name to the domain name exclusion list

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

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

**Examples**

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

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

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#">exclude</a>	Configures the Autodomain exclusion list.
<a href="#">mode extended</a>	Enables extended mode for SSG AutoDomain.
<a href="#">nat user-address</a>	Enables Network Address Translation (NAT) on Autodomain tunnel service.
<a href="#">select</a>	Configures the Autodomain selection mode.
<a href="#">exclude</a>	Displays the contents of an Autodomain exclude-profile downloaded from the AAA server.
<a href="#">ssg auto-domain</a>	Enables SSG Autodomain.
<a href="#">ssg enable</a>	Enables SSG functionality.

# exclude

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

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

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

## Syntax Description

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

## Defaults

No default behavior or values.

## Command Modes

SSG-auto-domain

## Command History

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

## Usage Guidelines

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

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

```
exclude apn abc
```

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

```
exclude domain xyz
```

## Related Commands

Command	Description
<a href="#">download exclude-profile</a>	Adds to the Autodomain download exclusion list.
<a href="#">mode extended</a>	Enables extended mode for SSG AutoDomain.
<a href="#">nat user-address</a>	Enables NAT on Autodomain tunnel service.
<a href="#">select</a>	Configures the Autodomain selection mode.
<a href="#">exclude</a>	Displays the contents of an Autodomain exclude-profile downloaded from the AAA server.

<b>Command</b>	<b>Description</b>
<a href="#">ssg auto-domain</a>	Enables SSG AutoDomain.
<code>ssg enable</code>	Enables SSG functionality.

# mode extended

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

**mode extended**

**no mode extended**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Basic Autodomain is selected by default.

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

## Examples

The following example shows how to enable extended Autodomain:

```
mode extended
```

## Related Commands

Command	Description
<a href="#">download exclude-profile</a>	Adds to the Autodomain download exclusion list.
<a href="#">exclude</a>	Configures the Autodomain exclusion list.
<a href="#">nat user-address</a>	Enables Network Address Translation (NAT) on Autodomain tunnel service.
<a href="#">select</a>	Configures the Autodomain selection mode.
<a href="#">exclude</a>	Displays the contents of an Autodomain exclude-profile downloaded from the AAA server.

Command	Description
<a href="#">ssg auto-domain</a>	Enables SSG AutoDomain.
<code>ssg enable</code>	Enables SSG functionality.

# nat user-address

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

**nat user-address**

**no nat user-address**

## Syntax Description

This command has no arguments or keywords.

## Defaults

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

## Command Modes

SSG-auto-domain

## Command History

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

## Usage Guidelines

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

## Examples

The following example enables Network Address Translation (NAT) towards Autodomain tunnel, VPDN, or proxy service:

```
nat user-address
```

## Related Commands

Command	Description
<a href="#">download exclude-profile</a>	Adds to the Autodomain download exclusion list.
<a href="#">exclude</a>	Configures the Autodomain exclusion list.
<a href="#">mode extended</a>	Enables extended mode for SSG AutoDomain.
<a href="#">select</a>	Configures the Autodomain selection mode.

Command	Description
<code>exclude</code>	Displays the contents of an Autodomain exclude-profile downloaded from the AAA server.
<code>ssg auto-domain</code>	Enables SSG AutoDomain.
<code>ssg enable</code>	Enables SSG functionality.

# 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 APN Called-Station-ID.

## Defaults

By default, 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 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 APN:

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

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

```
select username
```

## Related Commands

Command	Description
<a href="#">download exclude-profile</a>	Adds to the Autodomain download exclusion list.
<a href="#">exclude</a>	Configures the Autodomain exclusion list.

<b>Command</b>	<b>Description</b>
<b>mode extended</b>	Enables extended mode for SSG AutoDomain.
<b>nat user-address</b>	Enables NAT on Autodomain tunnel service.
<b>exclude</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.

# 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.

**Defaults** This command has no default behaviors or values.

**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 example enables basic SSG AutoDomain:

```
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
	<a href="#">download exclude-profile</a>	Adds to the Autodomain download exclusion list.
	<a href="#">exclude</a>	Configures the Autodomain exclusion list.
	<a href="#">mode extended</a>	Enables extended mode for SSG AutoDomain.
	<a href="#">nat user-address</a>	Enables NAT on Autodomain tunnel service.
	<a href="#">select</a>	Configures the Autodomain selection mode.

■ show ssg auto-domain exclude-profile

---

<b>ssg auto-domain</b>	Enables SSG AutoDomain.
<b>ssg enable</b>	Enables SSG functionality.

---

# ssg auto-domain

To enable SSG AutoDomain, use the **ssg auto-domain** command in global configuration mode. To remove all Autodomain configuration from the running configuration and to prevent further activation of Autodomains, use the **no** form of this command.

**ssg auto-domain**

**no ssg auto-domain**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Autodomain is disabled by default.

## 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

To enable SSG AutoDomain, use this command in global configuration mode. SSG must be enabled before the **ssg auto-domain** command can be entered.



### Note

The **ssg auto-domain** command enables basic Autodomain. In basic Autodomain, the profile downloaded from the AAA server for the Autodomain name is a service profile (either with or without SSG-specific attributes). By default, an attempt is made to find a valid service profile based on Access Point Name (APN), then by username. Use the **mode extended** command to configure Autodomain extended mode.

Use the **no ssg auto-domain** command to prevent further activations of autodomains and to remove all Autodomain configuration from the running-configuration. Subsequent reissuing of the **ssg auto-domain** command restores Autodomain to its former state.

## Examples

The following example enables basic SSG AutoDomain:

```
ssg enable
ssg auto-domain
```

## Related Commands

Command	Description
<a href="#">download exclude-profile</a>	Adds to the Autodomain download exclusion list.
<a href="#">exclude</a>	Configures the Autodomain exclusion list.

<b>Command</b>	<b>Description</b>
<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>exclude</b>	Displays the contents of an Autodomain exclude-profile downloaded from the AAA server.
<b>ssg enable</b>	Enables SSG functionality.

# Glossary

**APN**—Access Point Name. Identifies a PDN that is configured on and accessible from a GGSN in a GPRS network.

**GGSN**—Gateway GPRS Support Node. A wireless gateway that allows mobile cell phone users to access the public data network (PDN) or specified private IP networks.

**GPRS**—General Packet Radio System. Service defined and standardized by the European Telecommunication Standards Institute (ETSI). GPRS is an IP packet-based data service for Global System for Mobile Communications (GSM) networks.

**L2TP**—Layer 2 Tunneling Protocol. Layer 2 Tunnel Protocol (L2TP) is an emerging Internet Engineering Task Force (IETF) standard that combines features of two existing tunneling protocols: Cisco Layer 2 Forwarding (L2F) and Microsoft Point-to-Point Tunneling Protocol (PPTP). L2TP is an extension to the Point-to-Point Protocol (PPP), which is an important component for VPNs.

**MSISDN**—The header field type for Wireless Application Protocol (WAP).

**NAS**—Network Access Server. Cisco platform (or collection of platforms, such as an AccessPath system) that interfaces between the packet world (for example, the Internet) and the circuit world (for example, the PSTN).

**NAT**—Network Address Translation. Mechanism for reducing the need for globally unique IP addresses. NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating those addresses into globally routable address space. Also known as *Network Address Translator*.

**PDN**—Public/Private/Packet Data Network. Represents a public or private packet-based network, such as an IP or X.25 network.

**PDP**—Packet Data Protocol. Network protocol used by external packet data networks that communicate with a GPRS network. IP is an example of a PDP supported by GPRS. Refers to a set of information (such as a charging ID) that describes a mobile wireless service call or session, which is used by mobile stations and GGSNs in a GPRS network to identify the session.

**PTA-MD**—PPP Termination and Aggregation Multi-Domain. The Aggregation part of the acronym indicates that after the PPP sessions are terminated, the traffic is aggregated. For an ISP, the aggregated traffic either remains in the ISP network or routes to the Internet. For a wholesale provider, the aggregated IP traffic is forwarded to different destinations or domains depending on the service selected; thus the term PTA-Multi-Domain.

**SESM**—Cisco Subscriber Edge Services Manager. Successor product of the SSD. Cisco SESM is part of a Cisco solution that allows subscribers of DSL, cable, wireless, and dial-up to simultaneously access multiple services provided by different Internet service providers, application service providers, and Corporate Access Servers.

Cisco SESM allows a service provider to create a customized web application that provides a network portal for individual subscribers. Through the Cisco SESM web-based network portals, subscribers can have simultaneous access to the Internet, corporate intranets, gaming, and other entertainment-based services. After logging on and being authenticated to the system, subscribers access their own personalized services by pointing and clicking.

**SSD**—Service Selection Dashboard. A specialized web server that allows users to log in to and disconnect from multiple passthrough and proxy services through a standard web browser.

**SSG**—Service Selection Gateway. SSG provides subscriber authentication, service selection, and service connection capabilities to subscribers of Internet services.

**VPDN**—Virtual Private Dialup Network. Also known as virtual private dial network. A VPDN is a network that extends remote access to a private network using a shared infrastructure. VPDNs use Layer 2 tunnel technologies (L2F, L2TP, and PPTP) to extend the Layer 2 and higher parts of the network connection from a remote user across an ISP network to a private network. VPDNs are a cost effective method of establishing a long distance, point-to-point connection between remote dial users and a private network.