



Configuring SSG to Authenticate Subscribers Automatically in the Service Domain

First Published: May 2, 2005
Last Updated: October 2, 2009



Note

Effective with Cisco IOS Release 15.0(1)M, this feature is not available in Cisco IOS software.

The SSG AutoDomain feature allows Service Selection Gateway (SSG) to authenticate subscribers automatically in the service domain. The AutoDomain feature allows a user to be connected to a service automatically on the basis of either the access point name (APN) or the domain part of a structured username, which is specified in an Access-Request packet. In this mode, authentication of the user is not performed at the network access provider (NAP) authentication, authorization, and accounting (AAA) server but instead in the service domain (for example, the AAA server within a corporate network).

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for Configuring SSG to Authenticate Subscribers Automatically in the Service Domain”](#) section on page 14.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for SSG AutoDomain, page 2](#)
- [Restrictions for SSG AutoDomain, page 2](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

- [Information About SSG AutoDomain, page 2](#)
- [How to Configure SSG AutoDomain, page 7](#)
- [Configuration Examples for SSG AutoDomain, page 11](#)
- [Where to Go Next, page 12](#)
- [Additional References, page 12](#)
- [Feature Information for Configuring SSG to Authenticate Subscribers Automatically in the Service Domain, page 14](#)

Prerequisites for SSG AutoDomain

Before you configure SSG AutoDomain, SSG must be enabled.

If SSG is configured to work with SESM in RADIUS mode, service profiles, subscriber profiles, and control profiles must be configured on the AAA server before SSG will work. See the “RADIUS Profiles and Attributes for SSG” document for information about RADIUS profiles and attributes for SSG.

Subscriber Edge Services Manager (SESM) and the AAA server must be configured to support SSG AutoDomain.

Restrictions for SSG AutoDomain

- Loose coupling of hosts objects and Packet Data Protocol (PDP) contexts (when Gateway GPRS Support Node (GGSN) is a RADIUS client) can cause some error conditions that cannot be cleanly recovered without end-user intervention (such as reconnecting).
- In the event of a server failure, SSG ignores configured **server group** *group-name* commands and, instead, will failover to the server that is specified by the next **radius-server host** command in the configuration; no matter how these servers are partitioned into groups by **server group** *group-name* command(s).

For more information about the **radius-server host** command, see the *Cisco IOS Security Configuration Guide*. Refer to “[Configuring Authorization](#)” section in the Part 1: Authentication, Authorization, and Accounting (AAA).

Information About SSG AutoDomain

The SSG AutoDomain feature allows SSG to provide subscriber authentication for services. To configure SSG AutoDomain, you need to understand the following concepts:

- [Overview of SSG AutoDomain, page 3](#)
- [IP Address Assignment, page 4](#)
- [SSG AutoDomain Basic and Extended Modes, page 4](#)
- [SSG AutoDomain Service Types, page 4](#)
- [Access Point Names, page 5](#)
- [AutoDomain Name Selection, page 5](#)
- [Multiple Local IP Pools, page 6](#)

- [Primary AutoDomain Service Termination, page 6](#)
- [SSG AutoDomain and NAT, page 6](#)
- [Benefits of SSG AutoDomain, page 7](#)

Overview of SSG AutoDomain

The SSG AutoDomain feature allows SSG to authenticate subscribers in the service domain.

The SSG AutoDomain feature enables users to connect to a service automatically on the basis of either access point name (APN) or the domain part of the structured username specified in an Access-Request packet. When SSG AutoDomain is configured, user authentication is not performed by the Network Access Provider (NAP), but instead in the service domain (for example, at an authentication, authorization, and accounting (AAA) server within a corporate network).

Using SSG AutoDomain, you can automatically log a user on to a service on the basis of 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, in the username abc@cisco.com, cisco.com is the domain name.

Users can bypass SESM and access a service, such as a corporate intranet. SSG AutoDomain is also supported for users logging in from SESM.

SSG AutoDomain makes it possible to log a user on to either Layer 2 Tunnel Protocol (L2TP) or proxy services. The username and password used to log a user on with AutoDomain are the same username and password provided by the end-user device when the end user originally logged into the network. The username and password may be entered manually by the end user or preconfigured on the end-user device. The password may also be dynamically generated.

SSG AutoDomain does not require SSG vendor specific attributes (VSAs) when using a domain name as a means to determine which service the user is to be logged on to. AutoDomain uses a heuristic to determine the service onto which the user is to be logged. When AutoDomain is used, the host object is not activated until the user has been successfully authenticated with the service. If the autoservice connection fails for any reason, the user logon is rejected, and an Access-Reject packet is returned to the client device.

By default, SSG first checks for an AutoDomain name using the APN. The APN is normally conveyed in the Called-Station-ID attribute. If the AutoDomain name is not in the Called-Station-ID attribute, SSG looks for the name in the NAS-Identifier attribute. If the AutoDomain name cannot be extracted from the APN, SSG attempts to extract it from the structured username.

If AutoDomain is enabled and the received Access-Request packet specifies an APN, SSG uses this APN for AutoDomain selection unless it is a member of the APN AutoDomain exclusion list. If an AutoDomain is not selected based on the APN, SSG uses the structured username. If a structured username is not supplied, or the supplied structured username is a member of the domain name exclusion list, no AutoDomain is selected, and normal SSG user logon 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. The AutoDomain profile can be a service profile or a virtual user profile, depending on whether you configure AutoDomain in basic or extended mode. This profile is specified as an outbound service, and the password is the globally configured service password.

IP Address Assignment

Host objects created as a result of AutoDomain logon are assigned an IP address from one of the following sources:

- From the client device. If the IP address is assigned by the client device before authentication, each Access-Request packet received from the client device has an IP address in the Framed-IP field. If after authentication, the client device uses DHCP to assign an IP address to the user once the user has been successfully authenticated. This IP address is signaled to SSG in the Accounting start packet.
- From the Gateway GPRS Support Node (GGSN). Each Access-Request packet received from GGSN has an IP address in the Framed-IP field.
- From the Corporate Network: The AAA server in the corporate network authenticates the user and sends an Access-Accept packet. In the Access-Accept packet, the AAA server sends an IP address in the Framed-IP field.
- From the SSG local pool: In RADIUS-proxy mode you can configure IP address pools. If an IP address is not assigned from any of the above sources, the IP address is allocated from the SSG local pool.

SSG AutoDomain Basic and Extended Modes

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 primary service to an authenticated service such as a proxy or tunnel. The virtual user profile defines the AutoDomain service as a primary service. Connection to this primary service occurs as it does for basic AutoDomain; that is, the host object is not activated until the user has been authenticated at the proxy or tunnel service. The virtual user profile can also have other auto-logon services along with the primary service. Extended mode is for deployments in which the extra functionality introduced by SESM is to be utilized. The presence of SESM allows the user to switch among the services in the virtual user profile. If the virtual user profile does not have a primary service or if the autoservice is not authenticated, the AutoDomain logon is rejected.

SSG AutoDomain Service Types

The AutoDomain service profile can be a proxy, VPDN, tunnel service, or pass-through. If the downloaded AutoDomain service profile is a proxy service, SSG authenticates the user to the appropriate domain AAA server with the authentication information found in the Access-Request packet 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, SSG treats the service as a virtual private dialup network (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 selection of the AutoDomain is based on the realm part of the username, 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.

It is possible to configure an unauthenticated service as the AutoDomain service in basic mode or the primary service in extended mode AutoDomain. However, in these cases no user authentication occurs because in AutoDomain authentication at the NAP, the AAA server is bypassed.

Access Point Names

An APN identifies a packet data network (PDN) that is configured on and accessible from a GGSN. An access point is identified by its APN name. The Global System for Mobile Communications (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 a specified entry point. For more information about configuring APNs, see the [APN Manager Application Programming Guide](#).



Note

If the Access-Request packet 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.

AutoDomain Name Selection

When AutoDomain is enabled, SSG uses the following algorithm to determine the AutoDomain name:

- If the received Access-Request packet contains an APN (attribute 30), this APN is used for AutoDomain selection unless it is a member of the APN AutoDomain exclusion list.
- If APN is not selected using attribute 30, the NAS-Identifier (attribute 32) is used, unless it is a member of the APN AutoDomain exclusion list.
- If an AutoDomain is not selected based on APN, the structured username is used (attribute 1).
- If a valid AutoDomain is not found in one of these attributes, AutoDomain is not selected, and normal SSG user logon proceeds.

You can configure SSG to override the default AutoDomain selection rules—that is, force it to be based on any available attribute.

Note that for AutoDomain selection based on username, SSG expects the username to be a structured username and attempts to extract the domain from it. When SSG looks for the domain name and the username is unstructured (that is, it does not contain @), the AutoDomain selection is deemed to have failed, and SSG does not use the unstructured name. Note also that SSG does not attempt to extract a domain from any other attribute.

Multiple Local IP Pools

By default for AutoDomain, SSG assigns the IP address to a host object for the primary AutoDomain service (unless the IP address has already been assigned by some other mechanism). You can override the default by using a CLI command instructing SSG to use Network Address Translation (NAT). In this case SSG assigns an IP address from a locally configured pool and performs NAT on the service. You can override the NAT/no-NAT behavior, on a per-AutoDomain service basis.

You can configure multiple local SSG IP pools for the same domain name, and also multiple global pools; for example:

```
ssg radius-proxy
address-pool 1.1.1.1 1.1.2.2
address-pool 1.1.2.3 1.1.3.3
address-pool 1.1.3.4 1.1.4.4 acme.com
address-pool 1.1.4.5 1.1.5.5 acme.com
!
```

This functionality does not allow overlapping ranges within the same domain or global set. However, no restrictions are imposed on pools in one domain overlapping with those in another domain.

Primary AutoDomain Service Termination

By default, if the connection to the primary AutoDomain service is terminated, SSG terminates the session by destroying the host object. You can override this default behavior by using the **no auto-session-terminate** command. When you configure this command, SSG does not necessarily terminate the session when it loses the primary connection. If the host object IP address originated from the primary AutoDomain service, and the connection to this service is lost, the IP address is no longer valid. Because SSG has no mechanism to reassign a host object IP address during an active session, SSG terminates the session at this point.

SSG AutoDomain and NAT

By default, the IP address assigned to a host object is that received from the primary AutoDomain service (unless the IP address has already been assigned by some other mechanism). You can override the default by configuring SSG to use NAT. In this case SSG assigns an IP address from a local pool (if configured) and performs NAT on the service. If NAT is configured but no suitable local pool is configured, SSG assumes that the IP address is being assigned by the client device via the Accounting start packet. Again NAT will be performed between the IP addresses provided by the service domain and the client device. You can override the NAT/no-NAT behavior as needed, on a per-AutoDomain service basis.

You can enable NAT for an AutoDomain service using the **nat user-address** command. When this command is in effect, SSG either attempts to allocate an IP address for an AutoDomain host from a local SSG pool or waits for one to be assigned by the client device; NAT then takes place toward the AutoDomain service. However, this configuration is global; that is, you either *always* or *never* perform NAT to all AutoDomain services.

[Table 1](#) describes the Service-Info attribute that can be used in the AutoDomain service profile to configure NAT behavior on a per-AutoDomain basis. This VSA allows the NAT configuration for a given auto-domain service to override the global configuration.

Table 1 Service-Info Vendor-Specific Attribute

Attribute ID	Vendor ID	Subattribute ID and Type	Attribute Name	Subattribute Data
26	9	251 Service-Info	NAT user address	C—Service-Info code for NAT user address. 0 or 1—Disable or enable NAT of user address respectively.

The value of attribute C can be 0 or 1 depending on whether NAT mode is being disabled or enabled, respectively. Any value received for this attribute in a service profile takes precedence over the globally configured value.

Benefits of SSG AutoDomain

SSG AutoDomain provides the following benefits:

- Eliminates the need for users to be authenticated by SSG before connecting to a service. Users do not have 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 virtual private networks (VPNs) based on APN alone.
- Enables users to access both simultaneous and sequential services without having to log off and log back on to access different services.
- Supports overlapping host IP addresses.

How to Configure SSG AutoDomain

To configure SSG subscriber authentication for services, perform the following tasks:

- [Configuring SSG AutoDomain, page 8](#)
- [Monitoring and Maintaining SSG AutoDomain, page 10](#)
- [Troubleshooting SSG AutoDomain, page 11](#)

Configuring SSG AutoDomain

Perform this task to configure the SSG AutoDomain feature.

SUMMARY STEPS

1. `ssg auto-domain`
2. `mode extended`
3. `select {username | called-station-id calling-station-id | nas-identifier | attribute number}`
4. `exclude {apn | domain} name`
5. `download exclude-profile profile-name password`
6. `session-auto-terminate`
7. `nat user-address`
8. `end`
9. Configure NAT in the service profile for the AutoDomain service.

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>ssg auto-domain</code> Example: Router(config)# <code>ssg auto-domain</code>	Enables SSG AutoDomain and enters SSG-auto-domain configuration mode.
Step 2	<code>mode extended</code> Example: Router(config-auto-domain)# <code>mode extended</code>	(Optional) Selects extended AutoDomain.

	Command or Action	Purpose
Step 3	<pre>select {username called-station-id calling-station-id nas-identifier attribute number}</pre> <p>Example: Router(config-auto-domain)# select calling-station-id</p>	<p>(Optional) Configures the AutoDomain selection method.</p> <ul style="list-style-type: none"> • username—Configures the algorithm to use only the domain portion of the username to select the AutoDomain. • called-station-id—Configures the algorithm to use only the APN (Called-Station-ID). • calling-station-id—Configures the algorithm to use only the Calling Station ID. • nas-identifier—Configures the algorithm to use only the NAS-Identifier. • attribute number—Configures any attribute to be specified as the source for the AutoDomain name. Specify the appropriate attribute number in the range from 1 to 255. SSG does not limit the range of allowed values. <p>By default, AutoDomain attempts to find a valid AutoDomain based on APN (either Called-Station-ID or NAS-Identifier) followed by the domain portion of the username.</p>
Step 4	<pre>exclude {apn domain} name</pre> <p>Example: Router(config-auto-domain)# exclude domain xyz</p>	<p>(Optional) Adds names to the AutoDomain exclusion list.</p> <ul style="list-style-type: none"> • apn—Adds an APN to the exclusion list. • domain—Adds a domain to the exclusion list. • name—Name of the APN or domain to be added to the exclusion list.
Step 5	<pre>download exclude-profile profile-name password</pre> <p>Example: Router(config-auto-domain)# download exclude-profile abc cisco</p>	<p>(Optional) Adds names to the AutoDomain download exclusion list.</p> <ul style="list-style-type: none"> • profile-name—Specifies the name for a list of excluded names that may be downloaded from the AAA server. • password—Password for a list of excluded names that may be downloaded from the AAA server.
Step 6	<pre>session auto-terminate</pre> <p>Example: Router(config-auto-domain)# session auto-terminate</p>	<p>Terminates the session when the connection to the primary auto-domain service terminates.</p>
Step 7	<pre>nat user-address</pre> <p>Example: Router(config-auto-domain)# nat user-address</p>	<p>(Optional) Configures NAT to be applied toward AutoDomain services.</p>

	Command or Action	Purpose
Step 8	<code>end</code> Example: Router(config-auto-domain)# end	(Optional) Returns to privileged EXEC mode.
Step 9	Configure NAT in the service profile for the AutoDomain service.	Defines a Service-Info attribute in the service profile for the AutoDomain service.

Monitoring and Maintaining SSG AutoDomain

Perform this task to monitor and maintain SSG AutoDomain. The steps are all optional and may be performed in any order.

SUMMARY STEPS

1. `clear ssg radius-proxy client-address ip-address`
2. `clear ssg radius-proxy nas-address ip-address`
3. `show ssg auto-domain exclude-profile`
4. `show ssg binding`
5. `show ssg connection ip-address service-name`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>clear ssg radius-proxy client-address ip-address</code> Example: Router# clear ssg radius-proxy client-address 172.16.0.0	(Optional) Clears all hosts connected to a specific RADIUS client. <ul style="list-style-type: none"> • <i>ip-address</i>—IP address of a RADIUS client.
Step 2	<code>clear ssg radius-proxy nas-address ip-address</code> Example: Router# clear ssg radius-proxy nas-address 172.16.0.0	(Optional) Clears all hosts connected to a specific Network Access Server (NAS). <ul style="list-style-type: none"> • <i>ip-address</i>—IP address of a RADIUS client.
Step 3	<code>show ssg auto-domain exclude-profile</code> Example: Router# show ssg auto-domain exclude-profile	(Optional) Displays the contents of an AutoDomain exclusion profile downloaded from the AAA server. <ul style="list-style-type: none"> • Only AutoDomain exclude entries entered via CLI are displayed.

	Command or Action	Purpose
Step 4	<code>show ssg binding</code> Example: Router# show ssg binding	(Optional) Displays service names that have been bound to interfaces and the interfaces to which they have been bound.
Step 5	<code>show ssg connection ip-address service-name</code> Example: Router# show ssg connection 19.1.1.19 InstMsg	(Optional) Displays the connections of a given host and service name. <ul style="list-style-type: none"> <i>ip-address</i>—IP address of an active SSG connection. This is always a subscribed host. <i>service-name</i>—The name of an active SSG connection.

Troubleshooting SSG AutoDomain

Perform the tasks in this section to display port mapping event messages or port mapping packet contents. The steps are all optional and may be performed in any order.

SUMMARY STEPS

1. `debug ssg ctrl-events`
2. `debug ssg ctrl-errors`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>debug ssg ctrl-events</code> Example: Router# debug ssg ctrl-events	Displays SSG control event messages.
Step 2	<code>debug ssg ctrl-errors</code> Example: Router# debug ssg ctrl-errors	Displays SSG control error messages.

Configuration Examples for SSG AutoDomain

This section contains the following example:

- [SSG AutoDomain: Example, page 12](#)

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 toward 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

```

Where to Go Next

To configure other methods of subscriber authentication, refer to the following modules:

- [Configuring SSG to Authenticate Subscribers Automatically in the Service Domain](#)
- [Configuring SSG Support for Subnet-Based Authentication](#)
- [Configuring SSG for MAC-Address-Based Authentication](#)
- [Configuring SSG to Authenticate PPP Subscribers](#)
- [Configuring SSG to Authenticate Subscribers with Transparent Autologon](#)

To configure SSG to authenticate RADIUS Proxy subscribers, refer to [Configuring SSG to Serve as a RADIUS Proxy](#)

Additional References

The following sections provide references related to configuring SSG to authenticate subscribers for services.

Related Documents

Related Topic	Document Title
Configuring SESM	Cisco Subscriber Edge Services Manager documentation
Configuring L2TP	<ul style="list-style-type: none"> • Cisco IOS Dial Technologies Configuration Guide • Cisco IOS Dial Technologies Command Reference
SSG commands	Cisco IOS Service Selection Gateway Command Reference
RADIUS commands	Cisco IOS Security Command Reference
RADIUS configuration tasks	“ Configuring RADIUS ” chapter in the Cisco IOS Security Configuration Guide

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/techsupport</p>

Feature Information for Configuring SSG to Authenticate Subscribers Automatically in the Service Domain

[Table 2](#) lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(1) or a later release appear in the table.

Not all commands may be available in your Cisco IOS software release. For details on when support for a specific command was introduced, see the command reference documentation.

For information on a feature in this technology that is not documented here, see the [Service Selection Gateway Features Roadmap](#).

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

**Note**

[Table 2](#) lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 2 Feature Information for Configuring SSG to Authenticate Subscribers Automatically in the Service Domain

Feature Name	Releases	Feature Configuration Information
Configuring SSG to Authenticate Subscribers Automatically in the Service Domain	12.2(4)B 12.2(13)T 12.4 15.0(1)M	<p>The SSG AutoDomain feature allows Service Selection Gateway (SSG) to authenticate subscribers automatically in the service domain.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Overview of SSG AutoDomain, page 3 • IP Address Assignment, page 4 • SSG AutoDomain Basic and Extended Modes, page 4 • SSG AutoDomain Service Types, page 4 • Access Point Names, page 5 • AutoDomain Name Selection, page 5 • Multiple Local IP Pools, page 6 • Primary AutoDomain Service Termination, page 6 • SSG AutoDomain and NAT, page 6 • Benefits of SSG AutoDomain, page 7 • Configuring SSG AutoDomain, page 8 • Monitoring and Maintaining SSG AutoDomain, page 10 • Troubleshooting SSG AutoDomain, page 11 • SSG AutoDomain: Example, page 12 <p>The following commands were introduced by this feature: exclude, mode extended, nat user-address, select, show ssg auto-domain exclude-profile, ssg auto-domain</p> <p>This feature was removed in Cisco IOS Release 15.0(1)M.</p>

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0908R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2005–2009 Cisco Systems, Inc. All rights reserved.

