



Configuring SSG to Authenticate Web Logon Subscribers

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.

This module describes how SSG can be configured to authenticate Web logon subscribers.

SSG works in conjunction with SESM, which provides a user interface for subscribers to SSG services. SESM is a specialized web server that allows users to connect to and disconnect from various services offered by the service provider. SESM provides subscriber authentication, service selection, and service connection capabilities.

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 Web Logon Subscribers” section on page 9](#).

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 Configuring SSG to Authenticate Web Logon Subscribers, page 2](#)
- [Restrictions for Configuring SSG to Authenticate Web Logon Subscribers, page 2](#)
- [Information About Web Logon Subscribers, page 2](#)



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

- [How to Configure SSG to Authenticate Web Logon Subscribers, page 4](#)
- [Where to Go Next, page 7](#)
- [Additional References, page 8](#)
- [Feature Information for Configuring SSG to Authenticate Web Logon Subscribers, page 9](#)

Prerequisites for Configuring SSG to Authenticate Web Logon Subscribers

- Before you can perform the tasks in this process, you must enable SSG. See the *Cisco IOS Security Configuration Guide*. Refer to [Implementing SSG: Initial Tasks](#).
- Before you can configure SSG to authenticate subscribers you must first configure SESM and the RADIUS server to support the logon method.
- Before you configure SSG to authenticate web logon subscribers, you should perform the tasks described in [Configuring SSG Interface Direction](#), [Configuring SSG-SESM API Communication](#), and [Configuring SSG to AAA Server Interaction](#). See the *Cisco IOS Security Configuration Guide*. Refer to [Implementing SSG: Initial Tasks](#).
- In order to use the SSG TCP Redirect feature, you must install Cisco SESM Release 3.1(1) or higher.

Restrictions for Configuring SSG to Authenticate Web Logon Subscribers

- Only subscribers with a unique IP address can be configured for Web logon.
- 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 Web Logon Subscribers

Before you configure SSG authentication of web logon subscribers, you should understand the following concepts:

- [Web Logon, page 3](#)
- [TCP Redirection of Unauthenticated Users, page 3](#)
- [SSG 3-Key Authentication, page 4](#)

Web Logon

SSG works in conjunction with SESM, which provides a user interface for subscribers to SSG services. SESM is a specialized web server that allows users to connect to and disconnect from various services offered by the service provider. SESM provides subscriber authentication, service selection, and service connection capabilities. Web service selection enables subscribers to concurrently access multiple on-demand services from a list of personalized services.

SESM provides subscriber authentication, service selection, and service connection capabilities to subscribers. Subscribers interact with SESM using a standard Internet browser. They do not need to download any software or plug-ins to use SESM. After a subscriber successfully authenticates, SESM presents a list of services that the subscriber is currently authorized to use. The subscriber can gain access to one or more of those services by selecting them from a web page.

SESM works in conjunction with other network components to provide extremely robust, highly scalable connection management to Internet services. Internet service providers (ISPs) and network access providers (NAPs) deploy SESM to provide their subscribers with a web interface for accessing multiple Internet services. The ISPs and NAPs can customize and brand the content of the web pages and thereby control the user experience for different categories of subscribers.

TCP Redirection of Unauthenticated Users

The SSG TCP Redirect feature redirects certain subscriber traffic to an alternative location that can handle the packets in a suitable manner. This feature works in conjunction with the SESM captive portal and web interface. SSG forces subscribers to authenticate before accessing the network or specific services, and ensures that subscribers are only allowed to access services authorized by the service provider.

In TCP redirection, the following events occur:

1. An unauthenticated user opens a browser and attempts to send traffic.
2. SSG determines that the traffic is coming from an unauthenticated user. If SSG is configured for TCP redirection, the TCP redirection process begins. Otherwise, the traffic is dropped.
3. SSG selects a captive portal server (a server configured to respond to redirected packets) from the captive portal group configured in SESM to handle traffic from unauthenticated users.
4. SSG redirects the user's traffic to the captive portal server by changing the packet's destination IP address and TCP port to those of the captive portal server.
5. The captive portal server responds to the redirected traffic with an http-redirect packet in the application layer.
6. SSG applies reverse TCP redirection to forward the http-redirect packet back to the unauthenticated user.
7. The http-redirect packet redirects the unauthenticated user's browser to the SESM logon page.
8. Once the user is authenticated as a subscriber, the captive portal server can present the subscriber with a personalized home page, the service provider's home page, or the URL originally requested before the subscriber was authenticated.

For more information about TCP redirection for services, refer to [Configuring Subscriber Experience Features](#).

Restrictions for TCP Redirection of Unauthenticated Users

- SSG uses the same captive portal server for each redirection if multiple TCP sessions are redirected from the same unauthenticated user.
- SSG creates translation entries with the first packet of a TCP session is redirected to a captive portal server. These translations are cleared when the TCP session terminates or is idle for more than 60 seconds.
- In port-bundle host-key mode with overlapping user IP addresses, TCP redirection only works for host-keyed servers.
- The traffic that needs to be redirected to the captive portal group is controlled on SSG by specifying the relevant TCP ports or access lists. Only packets matching these ports and/or access lists are redirected to the server group.
- TCP redirection only applies to non-PPP users. For more information about PPP subscriber authentication, see [Configuring SSG to Authenticate PPP Subscribers](#).

SSG 3-Key Authentication

The SSG 3-Key Authentication feature enables SSG to authenticate SESM users on the basis of three keys: username, password, and Mobile Station Integrated Services digital network (MSISDN) number. Before the introduction of this feature, users logging into SESM were authenticated on the basis of username and password only (2-key authentication).

When SSG 3-key authentication feature is used, users are required to provide their MSISDN number (which is typically their phone number), in addition to username and password, at the SESM logon page. RADIUS attribute 31 (calling-station ID) is used to communicate the MSISDN number in account logon requests sent from SESM to SSG and in access requests sent from SSG to a AAA server. When 3-key authentication is used, all host and connection accounting packets for the user contain the MSISDN number.

How to Configure SSG to Authenticate Web Logon Subscribers

The following sections describe how to configure SSG to authenticate web logon subscribers:

- [Configuring TCP Redirection for Unauthenticated Subscribers, page 4](#)
- [Troubleshooting SSG TCP Redirection for Unauthenticated Subscribers, page 5](#)

Configuring TCP Redirection for Unauthenticated Subscribers

Configuring unauthenticated TCP redirection is an optional task. You could just configure SESM and AAA server for web logon authentication; refer to SESM documentation for details.

SUMMARY STEPS

1. `ssg tcp-redirect`
2. `server-group group-name`
3. `server ip-address port`
4. `exit`

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	ssg tcp-redirect Example: Router(config)# ssg tcp-redirect	Enables SSG TCP redirect.
Step 2	server-group <i>group-name</i> Example: Router(config-ssg-redirect)# server-group RedirectServer	Defines the group of one or more servers that make up a named captive portal group and enables ssg-redirect-group configuration mode. <ul style="list-style-type: none"> <i>group-name</i>—Name of the captive portal group.
Step 3	server <i>ip-address port</i> Example: Router(config-ssg-redirect-group)# server 10.0.0.0 8080	Adds a server to a captive portal group. <ul style="list-style-type: none"> <i>ip-address</i>—IP address of the server to add to the captive portal group. <i>port</i>—TCP port of the server to add to the captive portal group.
Step 4	exit Example: Router(config-ssg-redirect-group)# exit	Exits ssg-redirect-group configuration mode.
Step 5	redirect unauthenticated-user to <i>group-name</i> Example: Router(config-ssg-redirect)# redirect unauthenticated-user to RedirectServer	Selects a captive portal group for redirection of traffic from unauthenticated users. <ul style="list-style-type: none"> <i>group-name</i>—Name of the captive portal group.

Troubleshooting SSG TCP Redirection for Unauthenticated Subscribers

Use the following commands to troubleshoot SSG TCP Redirection for Unauthenticated Subscribers.

SUMMARY STEPS

1. **show ssg tcp-redirect group** [*group-name*]
2. **show tcp-redirect mappings** [*host-ip-address* [*interface*]]
3. **show ssg host** *ip-address*
4. **debug ssg tcp-redirect** {*packet* | *error* | *event*}
5. **debug ssg** {*ctrl-event* | *ctrl-error* | *ctrl-packets* | *event* | *error*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>show ssg tcp-redirect group [<i>group-name</i>]</p> <p>Example: Router# show ssg tcp-redirect group RedirectServer</p>	<p>Lists all configured captive portal groups and indicates which group receives redirected packets from unauthenticated users.</p> <ul style="list-style-type: none"> If the <i>group-name</i> is specified, this command displays detailed information about that captive portal group.
Step 2	<p>show tcp-redirect mappings [<i>host-ip-address</i> [<i>interface</i>]]</p> <p>Example: Router# show tcp-redirect mappings 172.16.0.0</p>	<p>Displays the redirect mappings currently stored in SSG.</p> <ul style="list-style-type: none"> If the host <i>ip-address</i> is provided, this command displays detailed redirect mapping information for the specified host. The TCP redirect mappings are removed automatically after the TCP session terminates or is idle for more than 60 seconds. The optional <i>interface</i> argument can be used to indicate the host's downlink interface.
Step 3	<p>show ssg host [<i>ip-address</i>]</p> <p>Example: Router# show ssg host 10.3.1.1</p>	<p>Displays information about a subscriber and current connections of the subscriber.</p>
Step 4	<p>debug ssg tcp-redirect {packet error event}</p> <p>Example: Router# debug ssg tcp-redirect packet</p>	<p>Use this command to turn on debug information for the SSG TCP Redirect for Services feature.</p> <ul style="list-style-type: none"> packet—Displays redirection information and any changes made to a packet when it is due for redirection. error—Displays any SSG TCP redirect errors. event—Displays any major SSG TCP redirect events or state changes. <p>Note This command replaces the debug ssg http-redirect command.</p>
Step 5	<p>debug ssg {ctrl-event ctrl-error ctrl-packets event error}</p> <p>Example: Router# debug ssg ctrl-packets</p>	<p>Use this command to turn on debug information for SSG.</p> <ul style="list-style-type: none"> ctrl-event—Displays all event messages for control modules. ctrl-error—Displays all error messages for control modules. ctrl-packets—Displays packet contents handled by control modules. event—Displays all event messages for system modules. error—Displays all error messages for system modules.

Configuration Examples for SSG Authentication for Web Logon Subscribers

The following is a sample configuration for a user with IP address 10.1.1.10 connected to SSG via interface ethernet 1/0. This example includes a basic AAA configuration on SSG (aaa new model, radius-server host) SSG-SESM communication (ssg radius-helper) and interface binding (ssg direction downlink):

```
! enable AAA on the router
aaa new-model
aaa authorization network default group radius

!
! enable SSG on the router
ssg enable
ssg radius-helper auth-port 1645 acct-port 1646
ssg radius-helper key cisco
!

! enable ssg tcp-redirection of unauthenticated users
ssg tcp-redirect
server-group group-unauthen-user
server 10.1.1.1 8090
!
redirect unauthenticated-user to group-unauthen-user
!

! bind the interface towards the user as the downlink interface
interface Ethernet 1/0
ip address 10.0.0.1 255.0.0.0
ssg direction downlink
!

! specify the RADIUS server
radius-server host 172.198.1.1 auth-port 1645 acct-port 1646 radius-server key cisco !
```

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 web logon subscribers.

Related Documents

Related Topic	Document Title
Configuring SESM	<i>Cisco Subscriber Edge Services Manager</i> documentation
RADIUS commands	<i>Cisco IOS Security Command Reference</i>
RADIUS configuration tasks	“Configuring RADIUS” chapter in the <i>Cisco IOS Security Configuration Guide</i>
SSG commands	<i>Cisco IOS Service Selection Gateway Command Reference</i>

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>	http://www.cisco.com/techsupport

Feature Information for Configuring SSG to Authenticate Web Logon Subscribers

Table 1 lists the features in this module and provides links to specific configuration information.

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

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

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 1 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 1 Feature Information for Configuring SSG to Authenticate Web Logon Subscribers

Feature Name	Releases	Feature Configuration Information
SSG TCP Redirect	12.1(5)DC 12.2(4)B 12.2(8)T 12.3T 12.4	<p>The SSG TCP Redirect feature forces subscribers to authenticate before accessing the network or specific services, and ensures that subscribers are only allowed to access services authorized by the service provider.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • TCP Redirection of Unauthenticated Users, page 3 • SSG 3-Key Authentication, page 4 • Configuring TCP Redirection for Unauthenticated Subscribers, page 4 <p>The following commands were introduced by this feature: ssg tcp-redirect, redirect unauthenticated-user to</p>
Configuring SSG to Authenticate Web Logon Subscribers	15.0(1)M	This feature was removed in Cisco IOS Release 15.0(1)M.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, 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, Flip Gift Card, and One Million Acts of Green 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 Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, 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. (0910R)

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.