



Configuring SSG for MAC-Address-Based Authentication

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 MAC-Address-Based Authentication for SSG feature allows a service provider to authorize subscriber access to services by the subscriber's MAC address, thus eliminating the need for explicit user logins between client power cycles. This module describes how the Cisco Service Selection Gateway (SSG) recognizes and manages MAC-address-based subscribers.

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 for MAC-Address-Based Authentication” section on page 10](#).

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 MAC-Address-Based Authentication for SSG, page 2](#)
- [Restrictions for MAC-Address-Based Authentication for SSG, page 2](#)
- [Information About MAC-Address-Based Authentication for SSG, page 2](#)
- [How to Configure MAC-Address-Based Authentication for SSG, page 6](#)



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

- [Additional References, page 9](#)
- [Feature Information for Configuring SSG for MAC-Address-Based Authentication, page 10](#)

Prerequisites for MAC-Address-Based Authentication for SSG

- SSG must be enabled before MAC-address-based authentication for SSG can be configured.
- The SSG Transparent Autologon (TAL) feature must be configured.
- Dynamic Host Configuration Protocol (DHCP) lease query functionality is required when the subscriber's MAC address is not available in the Address Resolution Protocol (ARP) table, or when the DHCP call flows between the subscriber and the DHCP server bypass the SSG.

Restrictions for MAC-Address-Based Authentication for SSG

Because subscribers can share a MAC address (for instance, users of the same computer), the activity of an individual subscriber cannot be tracked when the MAC address is used to authorize access to services.

Information About MAC-Address-Based Authentication for SSG

To configure the MAC-Address-Based Authentication for SSG feature, you should understand the following concepts:

- [Overview of MAC-Address-Based Authentication for SSG, page 2](#)
- [Subscriber Login with MAC-Address-Based Authentication for SSG, page 3](#)
- [Benefits of MAC-Address-Based Authentication for SSG, page 6](#)

Overview of MAC-Address-Based Authentication for SSG

The MAC-Address-Based Authentication for SSG feature gives service providers the option to authenticate subscribers on the basis of their MAC address rather than their IP address.

When a subscriber first logs in through the explicit login process, a subscriber profile containing the subscriber's MAC address is created by the authentication, authorization, and accounting (AAA) and Lightweight Directory Access Protocol (LDAP) applications and is stored on the LDAP server. Subsequent logins will be authorized through the implicit login process because the AAA and LDAP servers authenticate the subscriber in response to the access request from SSG, which contains the subscriber's MAC address. Because a previously authenticated subscriber need not self-identify and log in to previously authorized services, a service provider can offer an "always-on" service.

MAC Address as Username for Transparent Autologon

By default, the TAL feature identifies subscribers by their IP addresses. When MAC-address-based authentication is configured, service providers can use a subscriber's MAC address instead.

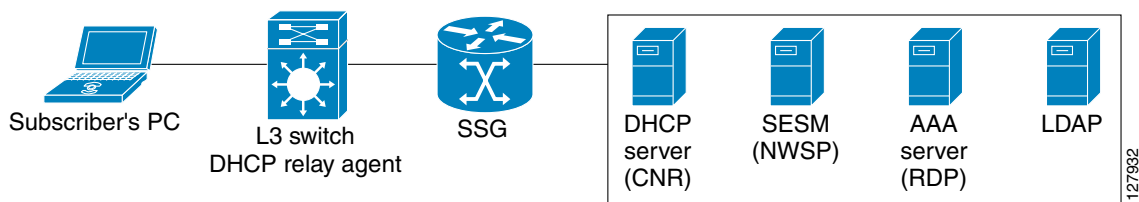
SSG obtains a subscriber's MAC address from a DHCP server by sending a DHCP lease query request containing the subscriber's IP address. This process is explained in further detail in the [“Explicit Login Call Flow” section on page 3](#). Once a subscriber's MAC address has been authenticated, the subscriber can gain access to services through transparent autologon. This process is explained in further detail in the [“Implicit Login Call Flow” section on page 5](#).

Subscriber Login with MAC-Address-Based Authentication for SSG

The first time a subscriber attempts to access the service provider network, SSG redirects the subscriber's HTTP session to the Cisco Subscriber Edge Services Manager (SESM), which then prompts the subscriber for a username and password. This process is called *explicit login*. During the explicit login process, SSG acquires and authorizes the subscriber's MAC address. When the subscriber logs off and logs in again, the session will be created through TAL, since the subscriber's MAC address is already known and authenticated. This process is called *implicit login*.

[Figure 1](#) is a diagram of the network topology when the MAC-Address-Based Authentication for SSG feature is enabled. In this sample configuration, the router running SSG also acts as the DHCP relay agent, while the DHCP server, SESM, AAA, and Lightweight Directory Access Protocol (LDAP) services run on separate platforms.

Figure 1 MAC-Address-Based Authentication for SSG Network Topology



Explicit Login Call Flow

In the explicit login process, the following events occur:

1. On bootup, a subscriber's computer sends a DHCPDISCOVER request packet to the DHCP relay agent. The DHCP relay agent forwards the DHCPDISCOVER request packet to the DHCP server.
2. The DHCP server assigns the subscriber an IP address from the private address pool in a DHCPOFFER response packet, which is passed through SSG to the subscriber.
3. The subscriber's computer sends a DHCPREQUEST packet to the DHCP server.
4. The DHCP server acknowledges the subscriber's IP assignment by returning a DHCPACK packet.
5. SSG receives an HTTP IP packet from the subscriber and sends a DHCP lease query request packet, based on the subscriber's IP and Virtual Private Network (VPN) information, before attempting a TAL request. The DHCP relay agent sends the DHCP lease query request packet to all that were servers configured using the `ip dhcp-server` command. If no DHCP servers are configured, the DHCP lease query request packet will be broadcast on all interfaces.
6. SSG receives the subscriber's MAC address in the DHCP lease query response packet from the DHCP server that has assigned the IP address to the subscriber.
7. SSG sends a TAL Authorization-Request packet to the AAA server. The TAL authorization request packet contains the following attributes relevant to the MAC-Address-Based Authentication for SSG feature:

- User-Name (attribute 1): The subscriber’s IP address, in dotted decimal notation.
 - Password (attribute 2): The global service password configured on SSG.
 - Calling-station-id (attribute 31): The subscriber’s MAC address. Note that this attribute will be present only when SSG receives a valid MAC address in the DHCP lease query response packet.
 - Framed-ip (attribute 8): The subscriber’s IP address.
 - Service-type (attribute 6): “outbound” (value 5).
8. The AAA server sends a query based on the subscriber’s MAC address to the LDAP application.
 9. The LDAP application sends a “no entry” response.
 10. The AAA server sends an Access-Reject packet to SSG.
 11. SSG redirects the subscriber’s HTTP session to SESM.
 12. SESM presents an accounting logon page to the subscriber, asking for the username and password. The subscriber enters this information and clicks the “logon” button.
 13. SESM sends an Account-Logon request packet containing the subscriber’s username and password to SSG.
 14. SSG sends a DHCP lease query request packet for the subscriber to the DHCP server and sends an authentication request packet to the AAA server. If no DHCP servers have been configured using the **ip dhcp-server** command, the DHCP lease query request packet is broadcast on all interfaces.
 15. The DHCP server returns the subscriber’s MAC address to SSG.
 16. SSG sends an Access-Request packet to the AAA server to authenticate the subscriber. Along with other attributes, the Access-Request packet includes the following:
 - User-Name (attribute 1): The username entered by the subscriber on the SESM accounting logon page.
 - Password (attribute 2): The password entered by the subscriber on the SESM accounting logon page.
 - Calling-station-id (attribute 31): The subscriber’s MAC address. Note that this attribute will be present only when SSG receives a valid MAC address in the DHCP lease query response packet.
 - Framed-ip (attribute 8): The subscriber’s IP address.
 17. The AAA server sends a query to the LDAP application to verify the subscriber’s username.
 18. The LDAP application finds an entry for the subscriber and sends the subscriber’s profile to the AAA server.
 19. The AAA server sends an Access-Accept packet to SSG.
 20. SSG creates a host object for the subscriber based on the contents of the Access-Accept packet and forwards the access-accept packet to SESM. Along with other attributes, the Access-Accept packet includes the following:
 - Calling-station-id (attribute 31): The subscriber’s MAC address. Note that this attribute will be present only when SSG receives a valid MAC address in the DHCP lease query response packet.
 - Framed-ip (attribute 8): The subscriber’s IP address.
 21. SESM adds the subscriber’s MAC address to the subscriber’s record.
 22. SSG sends an Accounting-Start packet to the AAA server. Along with other attributes, the Accounting-Start packet includes the following:
 - Username (attribute 1): The username of the subscriber as received in the Access-Accept packet.

- Calling-station-id (attribute 31): The subscriber's MAC address. Note that this attribute will be present only when SSG receives a valid MAC address in the DHCP lease query response packet.
 - Framed-ip (attribute 8): The subscriber's IP address.
23. The AAA server sends an Accounting-Response packet to SSG.
 24. When the subscriber logs out, SSG deletes the host object for that subscriber.

Implicit Login Call Flow

When a subscriber has logged in once through the explicit login call flow, subsequent logins proceed more quickly. The subscriber is not required to re-enter login information, because the subscriber's MAC address is already known and authenticated. In the implicit login process, the following events occur:

1. On bootup, a subscriber's computer sends a DHCPDISCOVER request packet to the DHCP relay agent. The DHCP relay agent forwards the DHCPDISCOVER request packet to the DHCP server.
2. The DHCP server assigns the subscriber an IP address from the private address pool in a DHCPOFFER response packet, which is passed through SSG to the subscriber.
3. The subscriber's computer sends a DHCPREQUEST packet to the DHCP server.
4. The DHCP server acknowledges the subscriber's IP assignment by returning a DHCPACK packet.
5. SSG receives an HTTP IP packet from the subscriber and sends a DHCP lease query packet request, based on the subscriber's IP and VPN information, before attempting a transparent autologon (TAL) request. The DHCP relay agent sends the DHCP lease query request packet to all servers that were configured using the **ip dhcp-server** command. If no DHCP servers are configured, the DHCP lease query request packet will be broadcast on all interfaces.
6. SSG receives the MAC address for the provided IP address in the DHCP lease query response packet from the DHCP server that has assigned the IP address to the subscriber.
7. SSG sends a TAL authorization request packet to the AAA server. The TAL Authorization-Request packet contains the following attributes relevant to the MAC-Address-Based Authentication for SSG feature:
 - User-Name (attribute 1): The subscriber's IP address, in dotted decimal notation.
 - Password (attribute 2): The global service password configured on SSG.
 - Calling-station-id (attribute 31): The subscriber's MAC address. Note that this attribute will be present only when SSG receives a valid MAC address in the DHCP lease query response packet.
 - Framed-ip (attribute 8): The subscriber's IP address.
 - Service-type (attribute 6): "outbound" (value 5).
8. The AAA server sends a query based on the subscriber's MAC address to the LDAP server.
9. The LDAP application finds the profile for the subscriber's MAC address and sends this profile to the AAA server.
10. The AAA server sends the subscriber profile in an Access-Accept packet to SSG. SSG creates a host object for the subscriber based on the contents of the Access-Accept packet and forwards the Access-Accept packet to SESM. Along with other attributes, the Access-Accept packet includes the following:
 - Calling-station-id (attribute 31): The subscriber's MAC address. Note that this attribute will be present only when SSG receives a valid MAC address in the DHCP lease query response packet.
 - Framed-ip (attribute 8): The subscriber's IP address.

11. SSG sends an Accounting-Start packet to the AAA server. Along with other attributes, the Accounting-Start packet includes the following:
 - Username (attribute 1): The username of the subscriber as received in the Access-Accept packet.
 - Calling-station-id (attribute 31): The subscriber's MAC address. Note that this attribute will be present only when SSG receives a valid MAC address in the DHCP lease query response packet.
 - Framed-ip (attribute 8): The subscriber's IP address.
12. The AAA server sends an Accounting-Response packet to SSG.
13. When the subscriber logs out, SSG deletes the host object for that subscriber.

Benefits of MAC-Address-Based Authentication for SSG

The MAC-Address-Based Authentication for SSG feature allows service providers to offer subscribers an “always on” experience when accessing services for which the subscriber has already been authenticated.

How to Configure MAC-Address-Based Authentication for SSG

This section contains the following tasks:

- [Configuring a DHCP Lease Query Request for MAC-Address-Based Authentication, page 6](#) (required)
- [Configuring an IP DHCP Lease Query Request, page 7](#) (optional)

Configuring a DHCP Lease Query Request for MAC-Address-Based Authentication

This task explains how to configure a DHCP lease query request for MAC-address-based authentication for SSG.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ssg query mac dhcp**
4. **username mac**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ssg query mac dhcp Example: Router(config)# ssg query mac dhcp	Enables SSG to send a DHCP lease query request to determine the subscriber's MAC address.
Step 4	username mac Example: Router(config)# username mac	Configures SSG to send a subscriber's MAC address as the username in TAL authorization requests.

Configuring an IP DHCP Lease Query Request

This task explains how to configure a DHCP lease query request for MAC-address-based authentication for SSG when no IP address is received in the accounting-start record.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ssg radius-proxy**
4. **client-address *ip-address* [vrf *vrf-name*]**
5. **query ip dhcp**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<code>ssg radius-proxy</code> Example: Router(config)# ssg radius proxy	Enables the SSG RADIUS proxy.
Step 4	<code>client-address ip-address [vrf vrf-name]</code> Example: Router(config-radius-proxy)# client-address 10.0.0.0	Configures the RADIUS client to proxy requests from a specified IP address to a RADIUS server.
Step 5	<code>query ip dhcp</code> Example: Router(config-radproxy-client)# query ip dhcp	Enables DHCP lease query requests for a RADIUS proxy client.

Configuration Examples for SSG MAC-Address-Based Authentication

This section contains the following configuration examples:

- [Configuring SSG for MAC-Address-Based Authentication: Example, page 8](#)
- [Configuring an IP DHCP Lease Query Request: Example, page 8](#)

Configuring SSG for MAC-Address-Based Authentication: Example

The following example shows a simple configuration to enable SSG to support MAC-address-based authentication:

```
enable
configure terminal
ssg query mac dhcp
username mac
```

Configuring an IP DHCP Lease Query Request: Example

The following example shows a simple configuration to configure a DHCP lease query request for MAC-address-based authentication for SSG when no IP address is received in the accounting-start record:

```
enable
configure terminal
ssg radius-proxy
client-address 10.0.0.0
query ip dhcp
```

Additional References

The following sections provide references related to the MAC-Address-Based Authentication for SSG feature.

Related Documents

Related Topic	Document Title
Configuring DHCP	“DHCP” section in the <i>Cisco IOS IP Addressing and Services Configuration Guide</i>
DHCP Lease Query Support	<i>DHCP Enhancement for Edge-Session Management</i> feature module
SSG commands	<i>Cisco IOS Service Selection Gateway Command Reference</i>
RADIUS commands	<i>Cisco IOS Security Command Reference</i>
RADIUS configuration tasks	“Configuring RADIUS” chapter in the <i>Cisco IOS Security Configuration Guide</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>	<p>http://www.cisco.com/techsupport</p>

Feature Information for Configuring SSG for MAC-Address-Based Authentication

[Table 1](#) lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.3(14)T or a later release appear in the table.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, 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 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 SSG On-Demand IP Address Renewal

Feature Name	Releases	Feature Configuration Information
Configuring SSG for MAC-Address-Based Authentication	12.3(14)T 12.4 15.0(1)M	<p>The MAC-Address-Based Authentication for SSG feature allows a service provider to authorize subscriber access to services by the subscriber's MAC address, thus eliminating the need for explicit user logins between client power cycles.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Overview of MAC-Address-Based Authentication for SSG, page 2 • Subscriber Login with MAC-Address-Based Authentication for SSG, page 3 • Benefits of MAC-Address-Based Authentication for SSG, page 6 • Configuring a DHCP Lease Query Request for MAC-Address-Based Authentication, page 6 • Configuring an IP DHCP Lease Query Request, page 7 • Configuring SSG for MAC-Address-Based Authentication: Example, page 8 • Configuring an IP DHCP Lease Query Request: Example, page 8 <p>The following commands were introduced by this feature: query ip dhcp, ssg query mac dhcp, username mac</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.

