



# Configuring SSG for MAC-Address-Based Authentication

---

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.

## History for MAC-Address-Based Authentication for SSG Feature

Release	Modification
12.3(14)T	This feature was introduced.

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## 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](#)
- [Additional References, page 9](#)
- [Command Reference, page 10](#)



---

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

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

## 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.

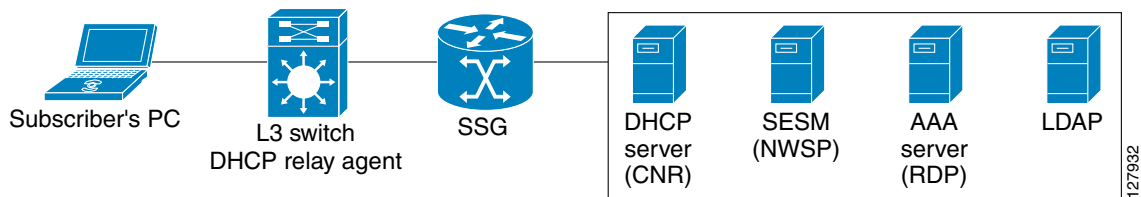
SSG obtains a subscriber's MAC address from a DHCP server by sending a DHCP lease query request containing the subscriber's IP address. This process is explained in further detail in the "[Explicit Login Call Flow](#)" section on page 3. Once a subscriber's MAC address has been authenticated, the subscriber 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 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	<code>enable</code>  <b>Example:</b> Router> <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# <code>configure terminal</code>	Enters global configuration mode.

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

	Command or Action	Purpose
Step 4	<b>client-address</b> <i>ip-address</i> [ <b>vrf</b> <i>vrf-name</i> ]  <b>Example:</b> 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	<b>query ip dhcp</b>  <b>Example:</b> 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	“Configuring DHCP” chapter in the <i>Cisco IOS IP Configuration Guide</i> , Release 12.3
DHCP Lease Query Support	<i>DHCP Enhancement for Edge-Session Management</i> , feature module for Cisco IOS Release 12.3(14)T.
Configuring RADIUS	“Configuring RADIUS” chapter in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.2

### Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

### MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

### RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

## Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	<a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a>

## Command Reference

This section documents new commands only.

- [query ip dhcp](#)
- [ssg query mac dhcp](#)
- [username mac](#)

## query ip dhcp

To configure the Service Selection Gateway (SSG) to send a Dynamic Host Configuration Protocol (DHCP) lease query request for the subscriber session created under a RADIUS proxy client when no IP address appears in the accounting-start record, use the **query ip dhcp** command in the client-address submode of SSG-radius-proxy mode. To disable the sending of the lease query request, use the **no** form of this command.

**query ip dhcp**

**no query ip dhcp**

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

**Command Default** SSG sends the subscriber's IP address as the username (RADIUS attribute 1).

**Command Modes** Client-address submode of SSG-radius-proxy mode

Command History	Release	Modification
	12.3(14)T	This command was introduced.

**Usage Guidelines** Use the **query ip dhcp** command to send DHCP lease query requests for a subscriber session under a specified RADIUS proxy client when no IP address is received in the accounting start record.

**Examples** The following example enables DHCP lease query requests for RADIUS proxy client 10.0.0.0:

```
Router(config)# ssg enable
Router(config)# ssg radius-proxy
Router(config-radius-proxy)# client-address 10.0.0.0
Router(config-radproxy-client) # query ip dhcp
```

Related Commands	Command	Description
	<b>ssg query mac dhcp</b>	Sends a DHCP lease query request to the DHCP server when a subscriber's MAC address is not known.
	<b>username mac</b>	Sends a subscriber's MAC address as RADIUS attribute 1 in TAL requests.

## ssg query mac dhcp

To configure the Service Selection Gateway (SSG) to send a Dynamic Host Control Protocol (DHCP) lease query request to the configured DHCP server when a subscriber's Media Access Control (MAC) address is not already known, use the **ssg query mac dhcp** command in global configuration mode. To disable the sending of DHCP lease query requests, use the **no** form of this command.

**ssg query mac dhcp**

**no ssg query mac dhcp**

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

**Command Default** SSG does not send DHCP lease query requests.

**Command Modes** Global configuration

Command History	Release	Modification
	12.3(14)T	This command was introduced.

**Usage Guidelines** SSG can be configured to authenticate a subscriber on the basis of the subscriber's MAC address. Use the **ssg query mac dhcp** command to configure SSG to request a subscriber's MAC address when the MAC address is not already present in a subscriber's user profile.

**Examples** The following example enables SSG to send a DHCP lease query request to determine the MAC address of a subscriber:

```
Router(config)# ssg query mac dhcp
```

Related Commands	Command	Description
	<b>query ip dhcp</b>	Sends DHCP lease query requests for the subscriber session when no IP address is received in the accounting start record.
	<b>username mac</b>	Sends a subscriber's MAC address as RADIUS attribute 1 in TAL requests.

## username mac

To configure the Service Selection Gateway (SSG) to send a subscriber's MAC address as the username (RADIUS attribute 1) in transparent autologon (TAL) authorization requests, use the **username mac** command in SSG login transparent submode. To disable the sending of the subscriber's MAC address and send the subscriber's IP address instead, use the **no** form of this command.

**username mac**

**no username mac**

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

**Command Default** SSG sends the subscriber's IP address as the username (RADIUS attribute 1).

**Command Modes** SSG login transparent submode

Command History	Release	Modification
	12.3(14)T	This command was introduced.

**Usage Guidelines** Use the **username mac** command to configure SSG to send a subscriber's MAC address as the username in TAL authorization requests.

**Examples** The following example enables SSG to send a subscriber's MAC address as the username in TAL authorization requests:

```
Router(config-login-transparent)# username mac
```

Related Commands	Command	Description
	<b>query ip dhcp</b>	Sends DHCP lease query requests for the subscriber session when no IP address is received in the accounting start record.
	<b>ssg query mac dhcp</b>	Sends a DHCP lease query request to the DHCP server when a subscriber's MAC address is not known.

---

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0711R)

Copyright © 2005 Cisco Systems, Inc. All rights reserved.