



# Configuring SSG to Authenticate Subscribers with Transparent Autologon

---

**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 Transparent Autologon feature enables Service Selection Gateway (SSG) to authenticate and authorize a user on the basis of the source IP address of packets received from the user. This document describes the SSG Transparent Autologon feature and how to configure SSG to authenticate subscribers by using transparent autologon.

## 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 with Transparent Autologon”](#) section on page 16.

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 Transparent Autologon, page 2](#)
- [Restrictions for SSG Transparent Autologon, page 2](#)
- [Information About SSG Transparent Autologon, page 2](#)
- [How to Configure SSG Transparent Autologon, page 6](#)



---

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

- [Configuration Examples for SSG Transparent Autologon, page 13](#)
- [Where to Go Next, page 14](#)
- [Additional References, page 15](#)
- [Feature Information for Configuring SSG to Authenticate Subscribers with Transparent Autologon, page 16](#)

## Prerequisites for SSG Transparent Autologon

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](#).

SSG authorizes the transparent autologon (TAL) user by using the IP address of the user in dotted notation as a string. Therefore, subscriber profiles must be configured with the IP addresses in dotted decimal notation as the username on the authentication, authorization, and accounting (AAA) server. Additionally, all of the subscriber profiles must all be configured with the same password.

## Restrictions for SSG Transparent Autologon

- Hosts with overlapping IP addresses are not supported.
- 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, Release*. Refer to “[Configuring Authorization](#)” section in the Part 1: Authentication, Authorization, and Accounting (AAA).

## Information About SSG Transparent Autologon

Before you configure this feature, you should understand the following concepts:

- [Overview of SSG Transparent Autologon, page 2](#)
- [SSG Transparent Autologon User-to-Service Packet Flow, page 3](#)
- [States of SSG Transparent Autologon Users, page 4](#)
- [Switching Between TP and Host User States, page 6](#)
- [Benefits of SSG Transparent Autologon, page 6](#)

## Overview of SSG Transparent Autologon

The SSG Transparent Autologon feature enables SSG to authenticate subscribers on the basis of the source IP address of packets received on an SSG downlink interface. Depending on how the feature is deployed, SSG allows the coexistence of SSG transparent autologon with other logon methods such as Subscriber Edge Services Manager (SESM) authentication, RADIUS proxy, and PPP session termination.

When transparent autologon is configured, SSG first creates a temporary entry when it receives the first IP packet from the unauthenticated user. SSG then sends an authorization request to the AAA server with the username as the IP address in dotted string format, along with the MAC address (if available) as the calling-station-id (attribute 31) and the user's IP address in framed-ip (attribute 8). If the AAA server finds a valid entry for the user, it authenticates the user and sends an Access-Accept packet. On receiving the Access-Accept packet, SSG creates a user session on SSG. The functionality of this feature does not depend on any specific access technology.

Without this feature, SSG always creates a host object for an active user session. With this feature enabled, an active user in SSG can be of two types:

- User session with host.
- User session without host (known as a transparent pass-through user, or TP).

The type of user session created is determined by the Transparent Pass-Through User (TP) SSG Account-Info attribute in the subscriber's profile.

The new user session type (TP user) is useful in situations in which subscribers have a flat-rate access and there is no need of service selection, accounting, quality of service, prepaid, and so on. The user session representation of TP requires much less memory than a user session represented with the host object.

**Note**

Transparent autologon functionality is not applied to packets destined to the default network or SSG's IP address.

## SSG Transparent Autologon User-to-Service Packet Flow

When SSG Transparent Autologon is configured, a user will be in one of the following states:

- Waiting for authorization (WA)
- Transparent pass-through (TP)
- With host created
- Suspect (SP)
- Unidentified (NR)

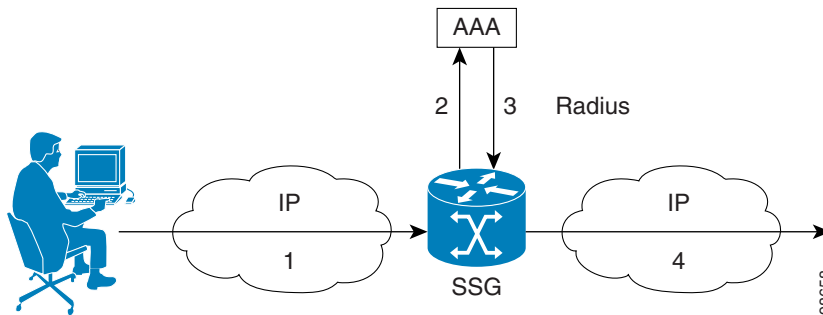
These states are described in the following user-to-service packet flow description and in the [“States of SSG Transparent Autologon Users”](#) section on page 4.

[Figure 1](#) is a diagram of the user-to-service packet flow when SSG Transparent Autologon is enabled. In this sample process, the following events occur:

1. SSG receives the first packet from a user and initiates an authorization request.
2. SSG sends an Access-Request packet to the AAA server with the user's IP address (in dotted decimal notation) as the username and a global service password as the password. The user is marked as waiting for authorization (WA). If the user in WA state continues to send traffic, it is forwarded or dropped on the basis of the command-line interface (CLI) configuration.
3. SSG receives an answer (either an Access-Accept packet or Access-Reject packet) or no response from the AAA server. SSG responds to the answer with the following actions:
  - Access Accept—If the user profile received as part of the Access-Accept packet has a Transparent Passthrough (TP) attribute, the user is added to the list of valid users as a transparent pass-through user (TP), and the user state is changed from WA to TP. If there is no TP attribute in the user profile, a host is created.

- Access Reject—The user is marked as a suspect user (SP), and the user state is changed from WA to SP.
  - Unidentified User—If there is no response (NR) to the access request from the AAA server, the user is marked as unidentified (NR).
4. User traffic is allowed, depending on the response from the AAA server and the CLI configuration.
- If the AAA server responds with an Access Accept, traffic will be handled as follows:
    - TP user—Traffic from the user will be allowed to access all routable destinations.
    - Host—Traffic from the user is allowed according to the services to which the user is logged in.
  - If the AAA server responds with an Access Reject, traffic will be handled as follows:
    - SP user—Traffic from the user will be allowed to access open garden services and the default network or it will be TCP-redirected. SP user entries will be deleted after a specified timeout.
  - If there is no response from the AAA server, traffic will be handled as follows:
    - NR user—Traffic from the user will be allowed on the basis of the CLI configuration. NR user entries will be deleted after a specified timeout.

**Figure 1** *User-to-Service Packet Flow*



## States of SSG Transparent Autologon Users

The following sections describe the SSG transparent autologon user states:

- [User with Host](#), page 5
- [Transparent Pass-Through User \(TP\)](#), page 5
- [User Waiting for Authorization \(WA\)](#), page 5
- [Suspect User \(SP\)](#), page 6
- [Unidentified User \(NR\)](#), page 6

## User with Host

When the SSG Transparent Autologon feature is configured, the host object user can be logged on in one of two ways:

1. An Access-Accept packet is received from the AAA server for the TAL authorization request by SSG, and the response does not have the TP attribute. SSG creates a host object for this user, and if there are any autoservices in the profile, it logs the user in to the autoservices. (Autoservices are services that a user can log onto as soon as SSG account logon is complete.) This type of logon is useful if the user's access to a service is static and authentication is required from the user.
2. An Access-Reject packet is received from the AAA server for the TAL authorization request, and SSG marks the subscriber as an SP user. When the next packet is received from the same user, SSG attempts a TCP-redirect (if configured) to SESM, and SESM displays a logon page for the user. If the user account logon through SESM is successful, SSG creates a host object. The user is removed from the SP list.

## Transparent Pass-Through User (TP)

An Access-Accept packet is received from the AAA server for the TAL authorization request and the user profile response has the Transparent Pass-Through (TP) attribute configured. In this case, SSG does not create hosts; instead, SSG adds the user to the TP user table.

For TP users, SSG honors only idle timeout and session timeout attributes from the user-profile. If other attributes are present, SSG ignores them.

The TP user model is useful for flat-rate users, where no accounting or differentiated services are required. Accounting records are not sent for the transparent pass-through users, even if accounting is enabled on the SSG. Traffic is forwarded to the service network on the basis of global routing table.

For TP users, idle timeouts and session timeouts can be configured either in the user profiles or globally through the CLI. The idle timeout and session timeout values configured in the user profile take precedence over the values configured globally.

## User Waiting for Authorization (WA)

While SSG is waiting for the AAA server's response to the TAL request, the user is treated in a state known as waiting for authorization (WA). If a user is marked as WA, packets received from the user are dropped or forwarded, depending on the CLI configuration. By default, packets are forwarded.

The number of WA users increases if the AAA server response is very slow or the rate of authorization is high.

If the number of WA users exceeds a configured value, no new WA users are added, and any packet that causes SSG to send an authorization request is dropped in the Cisco Express Forwarding (CEF) path. This also means that any new user will not undergo transparent autologon unless the number of WA users falls below the configured threshold.

To protect the AAA server from processing too many requests per second, SSG can be configured to throttle the number of access requests per second. If the maximum throttle rate is reached, a syslog message is generated.

## Suspect User (SP)

If an Access-Reject packet is received from the AAA server for the TAL authorization request, that user is marked as a suspect user (SP). Packets received from an SP user are TCP-redirectioned or dropped (if TCP-redirection is not enabled). The user remains marked as SP for a configurable length of time (one hour by default).

Too many SP users can cause SSG to consume all of its memory in maintaining the SP cache. To counter this situation, SSG provides a CLI command to configure the maximum number of SP users maintained by SSG. If the SP user count exceeds this maximum value, a syslog message is generated and SSG does not add any new SP users.

## Unidentified User (NR)

If there is no response from the AAA server for the TAL authorization request and the request times out, the user's state is changed from WA to no response (NR). SSG logs a syslog message when there is no response from the AAA server.

Packets received from NR users are either TCP-redirectioned or forwarded using global routing table, or dropped depending on the CLI configuration. By default, packets received from NR users are TCP-redirectioned and/or dropped (if TCP-redirection is not configured).

## Switching Between TP and Host User States

A TP (flat-rate) user can log on through SESM or some external device. When this occurs, SSG creates the host object for this user and removes the entry from the TP user list.

In the event that an external device sends an account logoff request to SSG, SSG will log the user as a transparent pass-through user when SSG receives the next IP packet from this user.

## Benefits of SSG Transparent Autologon

With the SSG Transparent Autologon feature, SSG provides the following functionality:

- Always-on access to network services for specific classes of users.
- Pay-per-use access to network services that are subject to explicit sign-on and authentication procedures managed by SSG and SESM.

## How to Configure SSG Transparent Autologon

This section contains the following tasks:

- [Configuring SSG Transparent Autologon, page 7](#)
- [Configuring the AAA Subscriber Profile for SSG Transparent Autologon Subscribers, page 9](#)
- [Monitoring and Maintaining SSG Transparent Autologon, page 9](#)
- [Troubleshooting SSG Transparent Autologon, page 12](#)

# Configuring SSG Transparent Autologon

Perform this task to configure SSG Transparent Autologon.

## SUMMARY STEPS

1. **ssg login transparent**
2. **authorization list** *list-name*
3. **authorization pending maximum** *number*
4. **authorization rate-limit** *number*
5. **packet drop during-authorization**
6. **user suspect maximum** *number*
7. **user suspect timeout** *minutes*
8. **user unidentified timeout** *minutes*
9. **user unidentified traffic permit**
10. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>ssg login transparent</b>  <b>Example:</b> Router(config)# ssg login transparent	Enables SSG Transparent Autologon and enters transparent autologon configuration mode.
Step 2	<b>authorization list</b> <i>list-name</i>  <b>Example:</b> Router(config-login-transparent)# authorization list list1	(Optional) Specifies the server group to be used for authorization of SSG transparent autologon users. <ul style="list-style-type: none"> <li>• If no server group is specified, SSG uses the default server group for authorization. The default server group is the list of RADIUS servers defined as “radius-server host...”.</li> <li>• If a server group is specified, SSG sends a transparent authorization request to that server group.</li> </ul>
Step 3	<b>authorization pending maximum</b> <i>number</i>  <b>Example:</b> Router(config-login-transparent)# authorization pending maximum 1200	(Optional) Specifies the maximum number of SSG TAL access requests that can be pending. <ul style="list-style-type: none"> <li>• When the number of access requests reaches the configured limit, any packets that would cause SSG to send a new RADIUS request are dropped at the CEF path, and SSG generates a syslog message.</li> </ul>

	Command or Action	Purpose
Step 4	<p><b>authorization rate-limit</b> <i>number</i></p> <p><b>Example:</b> Router(config-login-transparent)# authorization rate-limit 100</p>	<p>(Optional) Specifies the number of SSG new TAL authorization requests sent per second.</p> <ul style="list-style-type: none"> <li>The rate must be based on the number of requests the AAA server can handle per second.</li> <li>If the number of requests per second exceeds the configured limit, SSG logs a syslog message. The syslog message is logged only once for each time the rate limit value is reached.</li> </ul>
Step 5	<p><b>packet drop during-authorization</b></p> <p><b>Example:</b> Router(config-login-transparent)# packet drop during-authorization</p>	<p>(Optional) Specifies that packets received from the user during WA state (that is, during authorization) will be dropped.</p>
Step 6	<p><b>user suspect maximum</b> <i>number</i></p> <p><b>Example:</b> Router(config-login-transparent)# user suspect maximum 1000</p>	<p>(Optional) Specifies the maximum number of suspect users (SP) that can be added to the suspect user list.</p>
Step 7	<p><b>user suspect timeout</b> <i>minutes</i></p> <p><b>Example:</b> Router(config-login-transparent)# user suspect timeout 600</p>	<p>(Optional) Specifies the maximum length of time a suspect user (SP) remains in the suspect user list.</p> <ul style="list-style-type: none"> <li>The default timeout is 3600 seconds.</li> </ul>
Step 8	<p><b>user unidentified timeout</b> <i>minutes</i></p> <p><b>Example:</b> Router(config-login-transparent)# user unidentified timeout 600</p>	<p>(Optional) Specifies the maximum length of time a user remains in the no response (NR) state.</p> <ul style="list-style-type: none"> <li>An unidentified user is marked NR if there is no response from the AAA server to an authorization request and the authorization request times out.</li> <li>When the <i>timeout</i> value is reached, any new traffic received by SSG from the user triggers the transparent login procedure.</li> </ul>
Step 9	<p><b>user unidentified traffic permit</b></p> <p><b>Example:</b> Router(config-login-transparent)# user unidentified traffic permit</p>	<p>(Optional) Specifies that packets received by an unidentified (NR) user are to be forwarded.</p>
Step 10	<p><b>exit</b></p> <p><b>Example:</b> Router(config-login-transparent)# exit</p>	<p>(Optional) Returns to global configuration mode.</p>

## Configuring the AAA Subscriber Profile for SSG Transparent Autologon Subscribers

User-profiles for all the users that need to be authorized using TAL needs to be configured with username equal to the IP address as a dotted-notation in string format. This is true if there is no script running on the AAA server to change the usernames.

User profiles for flat-rate users must include the Transparent Passthrough User (TP) attribute.

## Monitoring and Maintaining SSG Transparent Autologon

Perform this task to monitor and maintain SSG Transparent Autologon. Step 1 is required. Steps 2 through 10 are optional and need not be performed in any particular order.

### SUMMARY STEPS

1. **enable**
2. **show ssg user transparent**
3. **clear ssg user transparent all**
4. **show ssg user transparent authorizing [count]**
5. **show ssg user transparent passthrough [ipaddress | count]**
6. **clear ssg user transparent passthrough {all | ipaddress}**
7. **show ssg user transparent suspect [count]**
8. **clear ssg user transparent suspect {all | ipaddress}**
9. **show ssg user transparent unidentified [count]**
10. **clear ssg user transparent unidentified {all | ipaddress}**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router# enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>show ssg user transparent</b>  <b>Example:</b> Router# show ssg user transparent	Displays all users (pass-through, suspect, unidentified, or waiting for authorization) in a table of IP addresses and user types.
Step 3	<b>clear ssg user transparent all</b>  <b>Example:</b> Router# clear ssg user transparent all	Deletes all pass-through, suspect, unidentified, and authorizing users.

	Command or Action	Purpose
Step 4	<b>show ssg user transparent authorizing</b> [count]  <b>Example:</b> Router# show ssg user transparent authorizing	Displays a list of users for whom authorization is in progress and are waiting for AAA response (WA users).
Step 5	<b>show ssg user transparent passthrough</b> [ipaddress   count]  <b>Example:</b> Router# show ssg user transparent passthrough	Displays a list of transparent (TP) users.
Step 6	<b>clear ssg user transparent passthrough</b> {all   ipaddress}  <b>Example:</b> Router# clear ssg user transparent passthrough all	Deletes pass-through user entries.
Step 7	<b>show ssg user transparent suspect</b> [count]  <b>Example:</b> Router# show ssg user transparent suspect count	Displays a list of all suspect (SP) user IP addresses.
Step 8	<b>clear ssg user transparent suspect</b> {all   ipaddress}  <b>Example:</b> Router# clear ssg user transparent suspect all	Deletes suspect (SP) user entries.
Step 9	<b>show ssg user transparent unidentified</b> [count]  <b>Example:</b> Router# show ssg user transparent unidentified	Displays a list of all users for whom there is no response from AAA to the authorization request (NR users).
Step 10	<b>clear ssg user transparent unidentified</b> {all   ipaddress}  <b>Example:</b> Router# clear ssg user transparent unidentified all	Deletes users for whom there is no response from AAA to the authorization request (NR users).

## Example

The following examples show sample output for commands that can be used to monitor SSG transparent autologon:

### show ssg user transparent Output: Example

The following is sample output from the **show ssg user transparent** command:

```
Router# show ssg user transparent
10.10.10.10      Passthrough
11.11.11.11      Suspect
```

```
120.120.120.120 Authorizing
### Total number of transparent users: 3
```

#### **show ssg user transparent authorizing Output: Example**

The following is sample output from the **show ssg user transparent authorizing** command with the **count** keyword:

```
Router# show ssg user transparent authorizing count

### Total number of WA users: 1
```

#### **show ssg user transparent passthrough Output: Example**

The following is sample output from the **show ssg user transparent passthrough** command for the user having IP address 10.10.10.10:

```
Router# show ssg user transparent passthrough 10.10.10.10

User IP Address:      10.10.10.10
Session Timeout:     200 (seconds)
Idle Timeout:        100 (seconds)
User logged on since: *16:33:57.000 GMT Mon May 19 2003
User last activity at: *16:33:57.000 GMT Mon May 19 2003
Current Time: *16:35:17.000 GMT Mon May 19 2003
```

#### **show ssg user transparent suspect Output: Example**

The following is sample output from the **show ssg user transparent suspect** command with and without the **count** keyword:

```
Router# show ssg user transparent suspect count

### Total number of SP users: 1

Router# show ssg user transparent suspect

94.0.0.1

### Total number of SP users: 1
```

#### **show ssg user transparent unidentified Output: Example**

The following is sample output from the **show ssg user transparent unidentified** command with and without the **count** keyword:

```
Router# show ssg user transparent unidentified count

### Total number of NR (Unidentified) users: 1

Router# show ssg user transparent unidentified

93.0.0.1

### Total number of NR (Unidentified) users: 1
```

## Troubleshooting SSG Transparent Autologon

Perform this task to display logon control events or errors.

### SUMMARY STEPS

1. `debug ssg transparent login {errors | events} [ipaddress]`

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>debug ssg transparent login {errors   events} [ipaddress]</code>	Displays transparent logon control events or errors.
	<b>Example:</b> Router# <code>debug ssg transparent login</code>	

### Example

The following examples show sample output for the `debug ssg transparent logon` command. The output is self-explanatory.

#### Unidentified (NR) User: Example

```
*Jan 15 12:34:47.847:SSG-TAL-EVN:100.0.0.2:Added entry successfully
*Jan 15 12:34:47.847:SSG-TAL-EVN:100.0.0.2:Attempting authorization
*Jan 15 12:34:47.847:SSG-TAL-EVN:100.0.0.2:Attempting to send authorization request
*Jan 15 12:35:09.711:SSG-TAL-EVN:100.0.0.2:Authorization response received
*Jan 15 12:35:09.711:SSG-TAL-EVN:100.0.0.2:Authorization timedout. User statechanged to
unidentified
*Jan 15 12:35:09.711:%SSG-5-SSG_TAL_NR:SSG TAL:No response from AAA server. AAA server
might be down or overloaded.
*Jan 15 12:35:09.711:SSG-TAL-EVN:100.0.0.2:Start SP/NR entry timeout timer for 10 mins
```

#### Transparent Pass-Through (TP) User: Example

```
*Jan 15 12:40:39.875:SSG-TAL-EVN:100.0.0.2:Added entry successfully
*Jan 15 12:40:39.875:SSG-TAL-EVN:100.0.0.2:Attempting authorization
*Jan 15 12:40:39.875:SSG-TAL-EVN:100.0.0.2:Attempting to send authorization request
*Jan 15 12:40:39.879:SSG-TAL-EVN:100.0.0.2:Authorization response received
*Jan 15 12:40:39.879:SSG-TAL-EVN:100.0.0.2:Parsing profile for TP attribute
*Jan 15 12:40:39.879:SSG-TAL-EVN:100.0.0.2:TP attribute found - Transparent user
*Jan 15 12:40:39.879:SSG-TAL-EVN:100.0.0.2:Stop SP/NR timer
*Jan 15 12:40:39.879:SSG-TAL-EVN:100.0.0.2:Idle timer started for 0 secs
```

```
*Jan. 15 12:40:39.879:SSG-TAL-EVN:100.0.0.2:Session timer started for 0 secs
```

### Suspect User (SP): Example

```
*Jan 15 12:43:25.363:SSG-TAL-EVN:10.10.10.10:Added entry successfully
*Jan 15 12:43:25.363:SSG-TAL-EVN:10.10.10.10:Attempting authorization
*Jan 15 12:43:25.363:SSG-TAL-EVN:10.10.10.10:Attempting to send authorization request
*Jan 15 12:43:25.939:SSG-TAL-EVN:10.10.10.10:Authorization response received
*Jan 15 12:43:25.939:SSG-TAL-EVN:10.10.10.10:Access reject from AAA server. Userstate
changed to suspect
*Jan 15 12:43:25.939:SSG-TAL-EVN:10.10.10.10:Start SP/NR entry timeout timer for 60 mins
```

### Clear All Users: Example

The following is sample output for the **debug ssg transparent login** command when it is used after all transparent autologon users have been cleared by using the **clear ssg user transparent all** command.

```
*Jan 15 12:47:08.943:SSG-TAL-EVN:10.10.10.10:Entry removed
*Jan 15 12:47:08.943:SSG-TAL-EVN:10.10.10.10:Stop SP/NR timer
*Jan 15 12:47:08.943:SSG-TAL-EVN:10.10.10.10:Stop Idle timer
*Jan 15 12:47:08.943:SSG-TAL-EVN:10.10.10.10:Stop session timer
*Jan 15 12:47:08.943:SSG-TAL-EVN:10.11.11.11:Entry removed
*Jan 15 12:47:08.943:SSG-TAL-EVN:10.11.11.11:Stop SP/NR timer
*Jan 15 12:47:08.943:SSG-TAL-EVN:10.11.11.11:Stop Idle timer
*Jan 15 12:47:08.943:SSG-TAL-EVN:10.11.11.11:Stop session timer
*Jan 15 12:47:08.943:SSG-TAL-EVN:10.0.0.2:Entry removed
*Jan 15 12:47:08.943:SSG-TAL-EVN:10.0.0.2:Stop SP/NR timer
*Jan 15 12:47:08.943:SSG-TAL-EVN:10.0.0.2:Stop Idle timer
*Jan 15 12:47:08.943:SSG-TAL-EVN:10.0.0.2:Stop session timer
```

## Configuration Examples for SSG Transparent Autologon

This section provides the following configuration examples:

- [SSG Transparent Autologon Configuration: Example, page 13](#)
- [AAA User Profile Configuration for Transparent Passthrough \(TP\) Users: Example, page 14](#)
- [AAA User Profile Configuration for Users with Hosts: Example, page 14](#)

### SSG Transparent Autologon Configuration: Example

The following example shows the how to enable and configure SSG Transparent Autologon.

```

!
aaa new-model
!
! creates aaa-list for TAL authorization
aaa group server radius TAL_LIST
  server 23.0.0.100 auth-port 1646 acct-port 1646
!
! The following commands configure SSG transparent autologon.
ssg login transparent
  authorization list TAL_LIST
  authorization pending maximum 1200
  authorization rate-limit 100
  user suspect timeout 600
  user suspect maximum 1000
  user unidentified timeout 600
  user unidentified traffic permit
  packet drop during-authorization
!

```

## AAA User Profile Configuration for Transparent Passthrough (TP) Users: Example

The following example shows the configuration of the AAA user profile for a transparent pass-through user. Note that the username is the user's IP address.

```

10.0.0.1 Password = "servicecisco"
  Cisco-SSG-Account-Info = "TP",
  Idle-Timeout = 600
  Session-Timeout = 3600

```

## AAA User Profile Configuration for Users with Hosts: Example

The following example shows the configuration of the AAA user profile for a user with a host object (pay-per-use user). Note that the username is the user's IP address.

```

10.0.0.1 Password = "servicecisco"
  Cisco-SSG-Account-Info = "Ainternet-Service",
  Idle-Timeout = 600
  Session-Timeout = 3600

```

## 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 Web Logon Subscribers](#)

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 TAL 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>	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

# Feature Information for Configuring SSG to Authenticate Subscribers with Transparent Autologon

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 Subscribers with Transparent Autologon

Feature Name	Releases	Feature Configuration Information
Configuring SSG to Authenticate Subscribers with Transparent Autologon	12.3(1a)BW 12.3(3)B 12.3(7)T 12.4 15.0(1)M	<p>The SSG Transparent Autologon feature enables Service Selection Gateway (SSG) to authenticate and authorize a user on the basis of the source IP address of packets received from the user.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Overview of SSG Transparent Autologon, page 2</a></li> <li>• <a href="#">SSG Transparent Autologon User-to-Service Packet Flow, page 3</a></li> <li>• <a href="#">States of SSG Transparent Autologon Users, page 4</a></li> <li>• <a href="#">Switching Between TP and Host User States, page 6</a></li> <li>• <a href="#">Benefits of SSG Transparent Autologon, page 6</a></li> <li>• <a href="#">Configuring SSG Transparent Autologon, page 7</a></li> <li>• <a href="#">Configuring the AAA Subscriber Profile for SSG Transparent Autologon Subscribers, page 9</a></li> <li>• <a href="#">Monitoring and Maintaining SSG Transparent Autologon, page 9</a></li> <li>• <a href="#">Troubleshooting SSG Transparent Autologon, page 12</a></li> </ul> <p>The following commands were introduced by this feature: <b>clear ssg user transparent, show ssg user transparent, ssg login transparent</b></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.

