



# SSG Transparent Autologon

---

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. Depending on how the feature is deployed, SSG will allow the coexistence of the SSG Transparent Autologon feature with other login methods such as Subscriber Edge Services Manager (SESM), RADIUS proxy, and PPP session termination.

## Feature History for the SSG Transparent Autologon Feature

Release	Modification
12.3(1a)BW	This feature was introduced.
12.3(3)B	This feature was integrated into Cisco IOS Release 12.3(3)B and implemented on the Cisco 7200 series, Cisco 7301, and Cisco 7400 series routers.
12.3(7)T	This feature was integrated into Cisco IOS Release 12.3(7)T.

## 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 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](#)
- [Configuration Examples for SSG Transparent Autologon, page 10](#)
- [Additional References, page 12](#)
- [Command Reference, page 13](#)



---

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

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

## Prerequisites for SSG Transparent Autologon

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

## Restrictions for SSG Transparent Autologon

Hosts with overlapping IP addresses are not supported.

Idle timeouts and session timeouts are the only features that can be applied to transparent pass-through users. Other features, such as quality of service and accounting, can be applied to users that have host objects only.

## Information About SSG Transparent Autologon

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

- [SSG Transparent Autologon User-to-Service Packet Flow, page 2](#)
- [States of SSG Transparent Autologon Users, page 4](#)
- [Switching Between Pay-per-Use and Flat-Rate Use, page 5](#)
- [Benefits of SSG Transparent Autologon, page 6](#)

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

The SSG Transparent Autologon feature enables SSG to authenticate and authorize users on the basis of the source IP address of packets received on an SSG downlink interface, without any previous authentication phase. SSG authorizes users by using information from the AAA server when the first IP packet is received from the user.

An SSG transparent autologon user will be in one of the following states.

- User with host object
- Waiting for authorization (WA)
- Transparent pass-through (TP)
- Suspect user (SP)
- Unidentified user (NR)

Information about these states is provided in the user-to-service packet flow description that follows 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. The process is illustrated in the following steps:

1. SSG receives the first packet from a user and initiates an authorization request.
2. SSG sends an access request 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). WA user traffic is forwarded on the basis of the command-line interface (CLI) configuration.
3. SSG receives an answer (either an Access Accept or Access Reject) or no response from the AAA server.

**Access Accept**—If the user profile received as part of the Access Accept has a Transparent User (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 full host object 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 (flat-rate user)—Traffic from the user will be allowed to access all services routable from the SSG device.
- Host object user (pay-per-use user)—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.

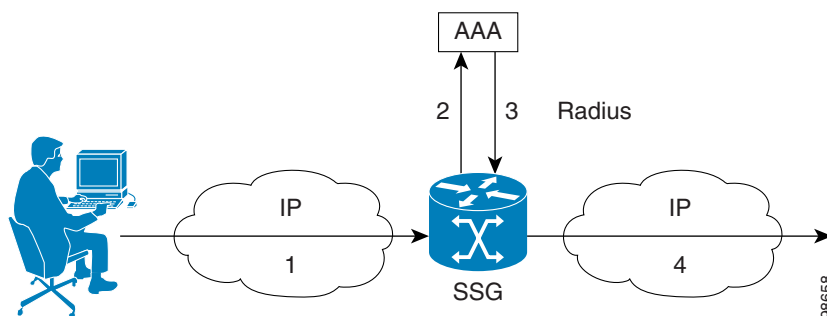
If there is no response from the AAA server, traffic will be handled as follows:

- 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.

5. WA user traffic is allowed.

**Waiting for authorization (WA) user**—User traffic will be allowed on the basis of the CLI configuration. The user will be in the WA state until SSG receives a response from the AAA server or the AAA request times out.

**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 Object](#), page 4
- [Transparent Pass-Through User \(TP\)](#), page 4
- [User Waiting for Authorization \(WA\)](#), page 5
- [Suspect User \(SP\)](#), page 5
- [Unidentified User \(NR\)](#), page 5

### User with Host Object

Using SSG transparent autologon, the host object user can be logged on in one of three ways:

1. An Access Accept is received from the AAA server for an 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 into 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. The AAA server has a profile with the username, but the username is not the IP address in decimal dotted notation. In this case, when SSG sends an authorization request with the username as an IP address in dotted decimal notation, the AAA server returns an Access Reject, and the user is marked 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.
3. For pay-per-use users, data is forwarded to the service network on the basis of the service binding configuration.

**Note**

---

The pay-per-use user requires accounting; therefore, the user profile should not have the TP attribute in the Access Accept packet. The user needs a full host object and other SSG features. Accounting records for host object users are sent on the basis of the CLI configuration.

---

### Transparent Pass-Through User (TP)

If the response to the AAA authorization results in an Access Accept, the user is treated as either a host object or a transparent pass-through user. A transparent pass-through user (TP) is a user who has the TP attribute configured in his user profile. SSG does not create host objects for TP users; instead the user is added to the TP user cache.

For TP users, SSG honors only idle timeout and session timeout attributes. If other attributes are present, they are ignored.

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 device.

For flat-rate users, data is forwarded to the service network on the basis of global Cisco IOS routing.

**Note**

User profiles for flat-rate users must include the TP attribute. Transparent pass-through user profiles are configured with a username equal to the IP address; user profiles of users that have host objects are configured with the same username that is configured in SESM.

Idle timeouts and session timeouts can be configured in the user profiles for transparent pass-through users 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 request for authorization, the user is treated 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 access requests waiting for authorization exceeds a configured value, any packet that causes SSG to send an authorization request is dropped in the CEF path. This packet drop reduces the number of packets in the process path that will trigger user authorization.

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 is reached, a syslog message is generated.

## Suspect User (SP)

If the response to the AAA server authorization request causes an Access Reject, the user is marked as a suspect user (SP). Packets received from an SP user are dropped or TCP-redirection. The user remains marked as SP for one hour (by default) or for a length of time configured in the CLI.

Too many SP users can cause SSG to consume all its memory maintaining the SP cache. To counter this, 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 new SP users to the SP user cache.

## Unidentified User (NR)

If there is no response from the AAA server for an authorization request and the authorization request times out, the user 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 dropped, TCP-redirection, or forwarded using Cisco IOS routing, depending on the CLI configuration. By default, packets received from NR users are dropped or TCP-redirection.

## Switching Between Pay-per-Use and Flat-Rate Use

### Transition from Flat-Rate User to Pay-per-Use User

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

### Transition from Pay-per-Use User to Flat-Rate User

An external device sends an account logoff request to SSG. After account logoff, 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 the SESM

## How to Configure SSG Transparent Autologon

This section contains the following procedures:

- [Configuring SSG Transparent Autologon, page 6](#)
- [Monitoring and Maintaining SSG Transparent Autologon, page 8](#)

## Configuring SSG Transparent Autologon

Perform this task to configure SSG transparent autologon.

### SUMMARY STEPS

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

## 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>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ssg enable</b>  <b>Example:</b> Router(config)# ssg enable	Enables SSG.
Step 4	<b>ssg login transparent</b>  <b>Example:</b> Router(config)# ssg login transparent	Enables SSG transparent autologon and enters transparent auto-logon configuration mode.
Step 5	<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.</li> <li>If a server group is specified, SSG sends a transparent authorization request to that server group.</li> </ul>
Step 6	<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 transparent autologon 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>
Step 7	<b>authorization rate-limit</b> <i>number</i>  <b>Example:</b> Router(config-login-transparent)# authorization rate-limit 100	(Optional) Specifies the number of SSG transparent autologon authorization requests sent per second. <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, the SSG logs a syslog message. The syslog message is logged only once for each time the rate limit value is reached.</li> </ul>
Step 8	<b>packet drop during-authorization</b>  <b>Example:</b> Router(config-login-transparent)# packet drop during-authorization	(Optional) Specifies that packets received from the user during SSG transparent autologon authorization will be dropped.

	Command or Action	Purpose
Step 9	<pre>user suspect maximum <i>number</i></pre> <p><b>Example:</b> Router(config-login-transparent)# user suspect maximum 1000</p>	(Optional) Specifies the maximum number of SSG transparent autologon suspect (SP) users that can be added to the suspect user list.
Step 10	<pre>user suspect timeout <i>minutes</i></pre> <p><b>Example:</b> Router(config-login-transparent)# user suspect timeout 600</p>	(Optional) Specifies the maximum length of time an SSG transparent autologon suspect (SP) user remains in the suspect user list. <ul style="list-style-type: none"> <li>By default, packets to or from a suspect user are dropped or TCP-redirected for a period of 60 minutes.</li> </ul>
Step 11	<pre>user unidentified timeout <i>minutes</i></pre> <p><b>Example:</b> Router(config-login-transparent)# user unidentified timeout 600</p>	(Optional) Specifies the maximum length of time an unidentified user remains has the status “no response” (NR). <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 logon procedure.</li> </ul>
Step 12	<pre>user unidentified traffic permit</pre> <p><b>Example:</b> Router(config-login-transparent)# user unidentified traffic permit</p>	(Optional) Specifies that packets received by an unidentified (NR) user are to be forwarded or received.
Step 13	<pre>exit</pre> <p><b>Example:</b> Router(config-login-transparent)# exit</p>	(Optional) Returns to global configuration mode.

## Monitoring and Maintaining SSG Transparent Autologon

Perform this task to monitor and maintain SSG transparent autologon. Step 1 is required. Steps 2 through 11 are optional and need not be performed in any particular order.

### SUMMARY STEPS

- enable
- show ssg user transparent
- clear ssg user transparent all
- show ssg user transparent authorizing [count]
- show ssg user transparent passthrough [*ipaddress* | count]
- clear ssg user transparent passthrough {all | *ipaddress*}
- show ssg user transparent suspect [count]
- clear ssg user transparent suspect {all | *ipaddress*}

9. `show ssg user transparent unidentified [count]`
10. `clear ssg user transparent unidentified {all | ipaddress}`
11. `debug ssg transparent login {errors | events} [ipaddress]`

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><code>enable</code></p> <p><b>Example:</b> Router&gt; <code>enable</code></p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<p><code>show ssg user transparent</code></p> <p><b>Example:</b> Router# <code>show ssg user transparent</code></p>	<p>Displays all users (pass-through, suspect, unidentified, or waiting for authorization), IP addresses, and user types.</p>
Step 3	<p><code>clear ssg user transparent all</code></p> <p><b>Example:</b> Router# <code>clear ssg user transparent all</code></p>	<p>Deletes all pass-through, suspect, unidentified, and authorizing users.</p>
Step 4	<p><code>show ssg user transparent authorizing [count]</code></p> <p><b>Example:</b> Router# <code>show ssg user transparent authorizing</code></p>	<p>Displays a list of users for whom authorization is in progress, waiting for AAA response (WA users).</p>
Step 5	<p><code>show ssg user transparent passthrough [ipaddress   count]</code></p> <p><b>Example:</b> Router# <code>show ssg user transparent passthrough</code></p>	<p>Displays a list of transparent (TP) users.</p>
Step 6	<p><code>clear ssg user transparent passthrough {all   ipaddress}</code></p> <p><b>Example:</b> Router# <code>clear ssg user transparent passthrough all</code></p>	<p>Deletes pass-through user entries.</p>
Step 7	<p><code>show ssg user transparent suspect [count]</code></p> <p><b>Example:</b> Router# <code>show ssg user transparent suspect count</code></p>	<p>Displays a list of all suspect (SP) user IP addresses.</p>
Step 8	<p><code>clear ssg user transparent suspect {all   ipaddress}</code></p> <p><b>Example:</b> Router# <code>clear ssg user transparent suspect all</code></p>	<p>Deletes suspect (SP) user entries.</p>

	Command or Action	Purpose
Step 9	<code>show ssg user transparent unidentified [count]</code>  <b>Example:</b> Router# <code>show ssg user transparent unidentified</code>	Displays a list of all users for whom there is no response from AAA to the authorization request (NR users).
Step 10	<code>clear ssg user transparent unidentified {all   ipaddress}</code>  <b>Example:</b> Router# <code>clear ssg user transparent unidentified all</code>	Deletes users for whom there is no response from AAA to the authorization request (NR users).
Step 11	<code>debug ssg transparent login {errors   events} [ipaddress]</code>  <b>Example:</b> Router# <code>debug ssg transparent login</code>	Displays transparent login control events or errors.

## Configuration Examples for SSG Transparent Autologon

This section provides the following configuration examples:

- [SSG Transparent Autologon Configuration with AAA and RADIUS: Example, page 10](#)
- [AAA User Profile Configuration for Transparent Pass-Through \(Flat-Rate\) Users: Example, page 11](#)
- [AAA User Profile Configuration for Users with Host Objects \(Pay-per-Use\): Example, page 12](#)

### SSG Transparent Autologon Configuration with AAA and RADIUS: Example

The following example shows the configuration of SSG transparent autologon.

```
!
aaa new-model
!
!
aaa group server radius TEST1
  server 23.0.0.100 auth-port 1646 acct-port 1646
!
aaa authentication ppp default group TEST1
aaa authorization network default group radius
!
ip cef
!
ssg enable
ssg accounting interval 1800
ssg accounting stop rate-limit 100
ssg default-network 23.0.0.0 255.0.0.0
ssg service-password cisco
ssg radius-helper auth-port 1812 acct-port 1813
ssg radius-helper key cisco
ssg maxservice 20
ssg service-cache refresh-interval 10
ssg bind service SURF 22.0.0.1
ssg bind service CORP 22.0.0.1
```

```

ssg bind service pass-through 24.0.0.1
ssg bind service pass-through1 22.0.0.1
ssg bind service SURF101 22.0.0.1
!
ssg radius-proxy
  server-port auth 1812 acct 1813
  client-address 21.0.0.1
  key cisco
!
  forward accounting-start-stop
!
ssg tcp-redirect
  server-group group-name
  server 1.1.1.1 100
!
  redirect access-list 101 to group-name
!
! The following commands configure SSG transparent autologon.
ssg login transparent
  authorization list TEST1
  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
!
!
ssg service-search-order remote local
!
!
interface FastEthernet2/0
  ip address 21.0.0.2 255.0.0.0
  duplex full
  ssg direction downlink
!
interface FastEthernet3/0
  ip address 24.0.0.2 255.0.0.0
  duplex auto
  speed auto
  ssg direction uplink
!
interface FastEthernet4/0
  ip address 22.0.0.2 255.0.0.0
  duplex full
  ssg direction uplink
!
!
radius-server host 23.0.0.1 auth-port 1812 acct-port 1813 key cisco
!

```

## AAA User Profile Configuration for Transparent Pass-Through (Flat-Rate) 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 Host Objects (Pay-per-Use): 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
```

## Additional References

The following sections provide references related to the SSG Transparent Autologon feature.

### Related Documents

Related Topic	Document Title
SSG commands	<i>Cisco IOS Wide-Area Networking Command Reference, Release 12.3 T</i>
SSG configuration tasks	<i>Service Selection Gateway, Release 12.3(4)T new-feature document</i> <i>SSG TCP Redirect for Services, Release 12.2(13)T new-feature document</i>
SESM	<i>Cisco Subscriber Edge Services Manager</i> <i>Cisco Service Selection Dashboard</i>
RADIUS commands	<i>Cisco IOS Security Command Reference, Release 12.3 T</i>
RADIUS configuration tasks	<i>Cisco IOS Security Configuration Guide</i>

### Standards

Standards	Title
No new or modified standards are supported by this feature.	—

## MIBs

MIBs	MIBs Link
No new or modified MIBs are supported 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.	—

## 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 the following new commands:

- [authorization list](#)
- [authorization pending maximum](#)
- [authorization rate-limit](#)
- [clear ssg user transparent all](#)
- [clear ssg user transparent passthrough](#)
- [clear ssg user transparent suspect](#)
- [clear ssg user transparent unidentified](#)
- [debug ssg transparent login](#)
- [packet drop during-authorization](#)
- [show ssg user transparent](#)
- [show ssg user transparent authorizing](#)
- [show ssg user transparent passthrough](#)
- [show ssg user transparent suspect](#)

- **show ssg user transparent unidentified**
- **ssg login transparent**
- **user suspect maximum**
- **user suspect timeout**
- **user unidentified timeout**
- **user unidentified traffic permit**

# authorization list

To specify the server group that Service Selection Gateway (SSG) uses for authorization of transparent autologon users, use the **authorization list** command in transparent auto-logon configuration mode. To remove the server group specification, use the **no** form of this command.

**authorization list** *list-name*

**no authorization list** *list-name*

## Syntax Description

<i>list-name</i>	Name of the server group that will be used for authorization of transparent autologon users.
------------------	--

## Defaults

If no server group is specified, or if the server group configuration is removed with the **no** form of the command, SSG uses the default server group for user authorization.

## Command Modes

Transparent auto-logon configuration

## Command History

Release	Modification
12.3(1a)BW	This command was introduced.
12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

## Usage Guidelines

The server group must be configured using authentication, authorization, and accounting (AAA) commands.

## Examples

The following example configures SSG to use the server group named “alpha” for authorization of transparent autologon users:

```
Router(config-login-transparent)# authorization list alpha
```

## Related Commands

Command	Description
<b>ssg login transparent</b>	Enables the SSG Transparent Autologon feature.

# authorization pending maximum

To specify the maximum number of Service Selection Gateway (SSG) transparent autologon access requests that can be pending at a given time, use the **authorization pending maximum** command in transparent auto-logon configuration mode. To remove the specification, use the **no** form of this command.

**authorization pending maximum** *number*

**no authorization pending maximum** *number*

<b>Syntax Description</b>	<i>number</i>	Maximum number of access requests that can be pending at a given time. Range is 1 to 5000.
---------------------------	---------------	--

<b>Defaults</b>	No maximum limit
-----------------	------------------

<b>Command Modes</b>	Transparent auto-logon configuration
----------------------	--------------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.3(1a)BW	This command was introduced.
12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.	
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.	

<b>Usage Guidelines</b>	When the number of SSG transparent autologon access requests reaches the configured maximum, SSG issues a syslog message. Any received packets that cause SSG to send a new RADIUS request are dropped at the Cisco Express Forwarding (CEF) path.
-------------------------	--

<b>Examples</b>	The following example specifies that the maximum number of access requests that can be pending is 10:
-----------------	---

```
Router(config-login-transparent)# authorization pending maximum 10
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ssg login transparent</b>	Enables the SSG Transparent Autologon feature.

# authorization rate-limit

To specify the maximum number of Service Selection Gateway (SSG) transparent autologon authorization requests sent per second to the authentication, authorization, and accounting (AAA) server, use the **authorization rate-limit** command in transparent auto-logon configuration mode. To remove the specification, use the **no** form of this command.

**authorization rate-limit** *number*

**no authorization rate-limit** *number*

<b>Syntax Description</b>	<i>number</i>	Maximum number of authorization requests sent per second. Range is from 1 to 10000.
---------------------------	---------------	---

<b>Defaults</b>	No rate limit
-----------------	---------------

<b>Command Modes</b>	Transparent auto-logon configuration
----------------------	--------------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.3(1a)BW	This command was introduced.
	12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
	12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

<b>Usage Guidelines</b>	This command must be configured on the basis of the number of requests that the AAA server can handle per second. When the number of authorization requests per second reaches the configured rate limit, SSG issues a syslog message. A syslog message is generated only once for each time the rate-limit value is reached.
-------------------------	---

<b>Examples</b>	The following example specifies that the maximum number of authorization requests is 10:
-----------------	--

```
Router(config-login-transparent)# authorization rate-limit 10
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ssg login transparent</b>	Enables the SSG Transparent Autologon feature.

# clear ssg user transparent all

To delete all Service Selection Gateway (SSG) transparent autologon transparent pass-through (TP), suspect (SP), unidentified (NR), and authorizing (WA) users, use the **clear ssg user transparent all** command in privileged EXEC mode.

**clear ssg user transparent all**

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.3(1a)BW	This command was introduced.
	12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
	12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

**Usage Guidelines** Use this command to clear all SSG transparent autologon users, including pass-through (TP), suspect (SP), unidentified (NR), and authorizing (WA) users.

**Examples** The following example deletes all TP, SP, NR, and WA users:

```
Router# clear ssg user transparent all
```

Related Commands	Command	Description
	ssg login transparent	Enables the SSG Transparent Autologon feature.

# clear ssg user transparent passthrough

To delete Service Selection Gateway (SSG) transparent autologon transparent pass-through (TP) users, use the **clear ssg user transparent passthrough** command in privileged EXEC mode.

```
clear ssg user transparent passthrough {all | ip-address}
```

Syntax Description	all	Deletes all pass-through user entries.
	<i>ip-address</i>	Deletes the entry for the specified IP address.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.3(1a)BW	This command was introduced.
	12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
	12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

**Examples** The following example deletes all pass-through user entries:

```
Router# clear ssg user transparent passthrough all
```

Related Commands	Command	Description
	<b>ssg login transparent</b>	Enables the SSG Transparent Autologon feature.

# clear ssg user transparent suspect

To delete Service Selection Gateway (SSG) transparent autologon suspect (SP) user entries, use the **clear ssg user transparent suspect** command in privileged EXEC mode.

```
clear ssg user transparent suspect {all | ip-address}
```

Syntax Description		
	<b>all</b>	Deletes all suspect user entries.
	<i>ip-address</i>	Deletes the entry for the specified IP address.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.3(1a)BW	This command was introduced.
	12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
	12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

**Usage Guidelines** An SSG transparent autologon suspect (SP) user is a user whose authentication, authorization, and accounting (AAA) authorization resulted in an Access Reject.

**Examples** The following example deletes all suspect user entries:

```
Router# clear ssg user transparent suspect
```

Related Commands	Command	Description
	<b>ssg login transparent</b>	Enables the SSG Transparent Autologon feature.

# debug ssg transparent login

To display all the Service Selection Gateway (SSG) transparent login control events or errors, use the **debug ssg transparent login** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

```
debug ssg transparent login {errors | events} [ip-address]
```

```
no debug ssg transparent login {errors | events} [ip-address]
```

## Syntax Description

<b>errors</b>	Displays any SSG transparent login errors.
<b>events</b>	Displays significant SSG transparent login events or state changes.
<i>ip-address</i>	(Optional) Displays events or errors for a specified IP address.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.3(1a)BW	This command was introduced.
12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

## Usage Guidelines

Use this command when troubleshooting SSG for problems related to transparent autologon users.

## Examples

The examples in this section show sample output for the **debug ssg transparent login** 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 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
```

### Related Commands

Command	Description
<b>ssg login transparent</b>	Enables the SSG Transparent Autologon feature.

# packet drop during-authorization

To specify that packets received from the user during authorization will be dropped, use the **packet drop during-authorization** command in transparent auto-logon configuration mode. To remove the configuration, use the **no** form of this command.

**packet drop during-authorization**

**no packet drop during-authorization**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Packet drop during authorization is disabled, and packets from the authorizing user are forwarded.

## Command Modes

Transparent auto-logon configuration

## Command History

Release	Modification
12.3(1a)BW	This command was introduced.
12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

## Usage Guidelines

Use this command for configuring data traffic packet drop for users that are waiting for authorization (WA).

## Examples

The following example specifies that packets received from the user during authorization will be dropped:

```
Router(config-login-transparent)# packet drop during-authorization
```

## Related Commands

Command	Description
<b>ssg login transparent</b>	Enables the SSG Transparent Autologon feature.

# show ssg user transparent

To display a list of all the Service Selection Gateway (SSG) transparent autologon users, use the **show ssg user transparent** command in privileged EXEC mode.

**show ssg user transparent**

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.3(1a)BW	This command was introduced.
	12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
	12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

**Usage Guidelines** Use this command to display the IP addresses and the states of all transparent autologon users that are active on SSG. The transparent autologon user states are passthrough (TP), suspect (SP), unidentified (NR), and waiting for authorization (WA).

**Examples** 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
```

Related Commands	Command	Description
	<b>ssg login transparent</b>	Enables the SSG Transparent Autologon feature.

# show ssg user transparent authorizing

To display a list of all Service Selection Gateway (SSG) transparent autologon users for whom authorization is in progress and who are waiting for authentication, authorization, and accounting (AAA) server response, use the **show ssg user transparent authorizing** command in privileged EXEC mode.

**show ssg user transparent authorizing [count]**

Syntax Description	count	(Optional) Displays the number of authorizing users.
--------------------	-------	--

Command Modes	Privileged EXEC
---------------	-----------------

Command History	Release	Modification
	12.3(1a)BW	This command was introduced.
	12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
	12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines	Use this command to display all Service Selection Gateway (SSG) transparent autologon users that are waiting for authorization (WA).
------------------	--

Examples	The following is sample output from the <b>show ssg user transparent authorizing</b> command with the <b>count</b> keyword:
----------	---

```
Router# show ssg user transparent authorizing count
```

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

Related Commands	Command	Description
	<b>ssg login transparent</b>	Enables the SSG Transparent Autologon feature.

# show ssg user transparent passthrough

To display information about Service Selection Gateway (SSG) transparent autologon pass-through users, use the **show ssg user transparent passthrough** command in privileged EXEC mode.

```
show ssg user transparent passthrough [ip-address | count]
```

Syntax Description	
<i>ip-address</i>	(Optional) Display details for specified user IP address.
<b>count</b>	(Optional) Displays the number of pass-through users.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.3(1a)BW	This command was introduced.
	12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
	12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

**Usage Guidelines** Use this command to display all SSG transparent autologon pass-through (TP) users that are active on SSG.

**Examples** 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
```

Related Commands	Command	Description
	<b>ssg login transparent</b>	Enables the SSG Transparent Autologon feature.

# show ssg user transparent suspect

To display a list of all Service Selection Gateway (SSG) transparent autologon suspect (SP) user IP addresses, use the **show ssg user transparent suspect** command in privileged EXEC mode.

**show ssg user transparent suspect [count]**

## Syntax Description

**count** (Optional) Displays the number of suspect users.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.3(1a)BW	This command was introduced.
12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

## Usage Guidelines

An SSG transparent autologon suspect user is a user whose authentication, authorization, and accounting (AAA) authorization resulted in an Access Reject.

## Examples

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
```

```
Router#
```

## Related Commands

Command	Description
<b>ssg login transparent</b>	Enables the SSG Transparent Autologon feature.

# show ssg user transparent unidentified

To display a list of Service Selection Gateway (SSG) transparent autologon users for whom there is no response from the authentication, authorization, and accounting (AAA) server to an authorization request (unidentified users), use the **show ssg user transparent unidentified** command in privileged EXEC mode.

**show ssg user transparent unidentified [count]**

## Syntax Description

<b>count</b>	(Optional) Displays the number of unidentified (NR) users.
--------------	--

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.3(1a)BW	This command was introduced.
12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

## Usage Guidelines

Use this command to display all SSG transparent autologon unidentified (NR) users that are active on the SSG.

## Examples

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
```

```
Router#
```

## Related Commands

Command	Description
<b>ssg login transparent</b>	Enables the SSG Transparent Autologon feature.

# ssg login transparent

To enable the SSG Transparent Autologon feature and enable transparent auto-logout configuration mode, use the **ssg login transparent** command in global configuration mode. To disable the Transparent Autologon feature, remove all the commands that were configured under transparent auto-logout mode, log off all the transparent autologon users, and refuse new logons, use the **no** form of this command.

**ssg login transparent**

**no ssg login transparent**

## Syntax Description

This command has no arguments or keywords.

## Defaults

The SSG Transparent Autologon feature is disabled by default.

## Command Modes

Global configuration

## Command History

Release	Modification
12.3(1a)BW	This command was introduced.
12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

## Examples

The following example enables the SSG Transparent Autologon feature:

```
Router(config)# ssg login transparent
```

## Related Commands

Command	Description
<b>show ssg user transparent</b>	Displays a list of all the SSG transparent autologon users.

# user suspect maximum

To specify the maximum number of Service Selection Gateway (SSG) transparent autologon suspect (SP) users that can be added to the suspect user list, use the **user suspect maximum** command in transparent auto-logon configuration mode. To remove the specification, use the **no** form of this command.

**user suspect maximum** *value*

**no user suspect maximum** *value*

## Syntax Description

<i>value</i>	Maximum number of suspect users that can be added to the SP list. Valid range is from 10 to 5000. The default is 5000.
--------------	--

## Defaults

The default maximum number of suspect users that can be added to the suspect user list is 5000.

## Command Modes

Transparent auto-logon configuration

## Command History

Release	Modification
12.3(1a)BW	This command was introduced.
12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

## Usage Guidelines

An SSG transparent autologon suspect user is a user whose authentication, authorization, and accounting (AAA) authorization resulted in an access reject.

If the number of suspect users exceeds the maximum value configured, SSG sends a syslog message and does not add any further users to the SP list.

## Examples

The following example specifies that the maximum number of suspect users that can be added to the SP list is 200:

```
Router(config-login-transparent)# user suspect maximum 200
```

## Related Commands

Command	Description
<b>ssg login transparent</b>	Enables the SSG Transparent Autologon feature.

## user suspect timeout

To specify the maximum length of time for which a Service Selection Gateway (SSG) transparent autologon suspect (SP) user remains in the suspect user list, use the **user suspect timeout** command in transparent auto-logon configuration mode. To return to the default length of time, use the **no** form of this command.

**user suspect timeout** *timeout*

**no user suspect timeout** *timeout*

<b>Syntax Description</b>	<i>timeout</i>	Maximum length of time (in minutes) that a suspect user remains in the suspect user list. Range is from 1 to 34560. Default is 60 minutes.
---------------------------	----------------	--

<b>Defaults</b>	60 minutes
-----------------	------------

<b>Command Modes</b>	Transparent auto-logon configuration
----------------------	--------------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.3(1a)BW	This command was introduced.
	12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
	12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

<b>Usage Guidelines</b>	If a packet is received for a user who is marked as an SP user, packets to or from this user are dropped or TCP-redirection until the <i>timeout</i> value is reached. When the <i>timeout</i> value is reached, any new traffic received by SSG from the user triggers the transparent logon procedure.
-------------------------	--

<b>Examples</b>	The following example specifies that a suspect user will remain in the suspect user list for 30 minutes:
-----------------	--

```
Router(config-login-transparent)# user suspect timeout 30
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ssg login transparent</b>	Enables the SSG Transparent Auto-Logon feature.

# user unidentified timeout

To specify the maximum length of time for which a Service Selection Gateway (SSG) transparent autologon unidentified user remains marked as no response (NR), use the **user unidentified timeout** command in transparent auto-logon configuration mode. To return to the default timeout value (10 minutes), use the **no** form of this command.

**user unidentified timeout** *timeout*

**no user unidentified timeout** *timeout*

<b>Syntax Description</b>	<i>timeout</i>	Length of time (in minutes) that a user remains marked as NR. Range is from 1 to 34560.
---------------------------	----------------	---

<b>Defaults</b>	10 minutes
-----------------	------------

<b>Command Modes</b>	Transparent auto-logon
----------------------	------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.3(1a)BW	This command was introduced.
	12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
	12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

<b>Usage Guidelines</b>	<p>An unidentified user is marked NR if there is no response from the authentication, authorization, and accounting (AAA) server to an authorization request and the authorization request times out.</p> <p>If a packet is received for a user who is marked as an NR user, packets to or from this user are dropped or TCP-redirected until the <i>timeout</i> value is reached. When the <i>timeout</i> value is reached, any new traffic received by SSG from the user triggers the transparent logon procedure.</p>
-------------------------	--

<b>Examples</b>	The following example sets the user unidentified timeout to 5 minutes:
-----------------	--

```
Router(config-login-transparent)# user unidentified timeout 5
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ssg login transparent</b>	Enables the SSG Transparent Auto-Logon feature.

# user unidentified traffic permit

To specify that packets received from a Service Selection Gateway (SSG) transparent autologon user whose authorization request has timed out will be forwarded or received, use the **user unidentified traffic permit** command in transparent auto-logon configuration mode. To return to the default (packets dropped if user authorization has timed out), use the **no** form of this command.

**user unidentified traffic permit**

**no user unidentified traffic permit**

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

**Defaults** Packets received from a user whose authorization request has timed out are dropped.

**Command Modes** Transparent auto-logon configuration

Command History	Release	Modification
	12.3(1a)BW	This command was introduced.
	12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
	12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

**Usage Guidelines** Configuring this command allows traffic flow for NR users toward the service network.

**Examples** The following example specifies that packets received from a user whose authorization request has timed out will be forwarded or received:

```
Router(config-login-transparent)# user unidentified traffic permit
```

Related Commands	Command	Description
	<b>ssg login transparent</b>	Enables the SSG Transparent Auto-Logon feature.

---

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 © 2003–2004 Cisco Systems, Inc. All rights reserved.