



Tokenless Call Authorization

The Tokenless Call Authorization feature provides a statically configured access list of authorized H.323 endpoints for the Cisco IOS gatekeeper. The gatekeeper accepts calls from endpoints on the list. This security feature is an alternative to Interzone ClearTokens (IZCTs) and Cisco Access Tokens (CATs), and can be used with Cisco CallManager (CCM).

Feature Specifications for the Tokenless Call Authorization Feature

Feature History

| Release | Modification |
|-----------|------------------------------|
| 12.2(15)T | This feature was introduced. |

Supported Platforms

Cisco 2610, Cisco 2611, Cisco 2611XM, Cisco 2613, Cisco 2620, Cisco 2620XM, Cisco 2621, Cisco 2621XM, Cisco 2650, Cisco 2650XM, Cisco 2651, Cisco 2651XM, Cisco 3620, Cisco 3640, Cisco 3660, Cisco 3725

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 Tokenless Call Authorization, page 2](#)
- [Information About Tokenless Call Authorization, page 2](#)
- [How to Configure Tokenless Call Authorization, page 3](#)
- [Configuration Examples for Tokenless Call Authorization, page 6](#)
- [Additional References, page 7](#)
- [Command Reference, page 9](#)

Prerequisites for Tokenless Call Authorization

- Cisco IOS Release 12.2(106)T installed on the Cisco IOS gatekeeper
- Working H.323 network

Information About Tokenless Call Authorization

To configure the Tokenless Call Authorization feature, you must understand the following concepts:

- [Gatekeeper Security Using Tokens, page 2](#)
- [Gatekeeper Security Using Access Lists, page 2](#)
- [Benefits of Tokenless Call Authorization, page 3](#)

Gatekeeper Security Using Tokens

Cisco provides two methods that Internet Telephony Service Providers (ITSPs) can use to provide gatekeeper security between administrative domains in their H.323 voice network. IZCTs are generated in the originating gatekeeper and sent to other gatekeepers in the domain. Each gatekeeper stamps the IZCT's destination gatekeeper with its own ID before the IZCT is sent back to the originating gateway in the location confirm (LCF) message. The originating gateway passes the IZCT to the terminating gateway in the SETUP message. The terminating gatekeeper forwards the IZCT in the admission request (ARQ) answerCall field to the terminating gatekeeper, which then validates it.

IZCTs are used for per-call authorization; CATs are used for gatekeeper-to-gatekeeper authentication. CATs are configured on a per-zone basis and provide a gatekeeper ID and a password. Gatekeepers in each domain check the CAT's password and reject it if the wrong password is used.

IZCT and CAT security requires Cisco software on all gatekeepers in the ITSP's H.323 voice network. These security features do not work with Cisco CallManager as of Cisco IOS Release 12.2(106)T.

Gatekeeper Security Using Access Lists

The Tokenless Call Authorization feature is an alternative to using IZCTs and CATs to provide gatekeeper security in an H.323 voice network. ITSPs may not control gatekeepers in other domains to which they connect; for example, if these domains do not have Cisco software installed on the gatekeepers, tokens cannot be used. Additionally, the Tokenless Call Authorization feature can be used with Cisco Call Manager; tokens cannot.

With the Tokenless Call Authorization feature, an access list of all known endpoints is configured on the gatekeeper. The gatekeeper is configured to use the access list when processing calls. Rather than rejecting all calls that do not contain IZCTs or CATs, gatekeepers reject only calls that do not have tokens and are not from endpoints on the access list.

Benefits of Tokenless Call Authorization

- Provides an alternative to token-based gatekeeper security
- Provides security for gatekeepers in domains not using Cisco software
- Works with Cisco CallManager

How to Configure Tokenless Call Authorization

This section contains the following procedures:

- [Configuring the IP Access List, page 3](#) (required)
- [Configuring IP Access List Security on the Gatekeeper, page 5](#) (required)

Configuring the IP Access List

Perform this task to create a list of endpoints known to the gatekeeper. Calls from these endpoints will be accepted by the gatekeeper even if the endpoints are located in a different domain.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**permit** | **deny** | **remark**} *source* [*source-wildcard*] [*log*]

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|--|
| Step 1 | <p>enable</p> <p>Example: Router> enable</p> | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted. |
| Step 2 | <p>configure terminal</p> <p>Example: Router# configure terminal</p> | <p>Enters global configuration mode.</p> |
| Step 3 | <p>access-list <i>access-list-number</i> {permit deny remark} <i>source</i> [<i>source-wildcard</i>] [<i>log</i>]</p> <p>Example: Router(config)# access-list 20 permit 172.16.10.190</p> | <p>Configures the access list mechanism for filtering frames by protocol type or vendor code.</p> <ul style="list-style-type: none"> <i>access-list-number</i>—Number of an access list. This is a decimal number from 1 to 99 (standard) or from 1300 to 1999 (extended). Only standard IP access lists numbered 1 through 99 are supported for the Tokenless Call Authorization feature. permit—Permits access if the conditions are matched. deny—Denies access when there is an address match. remark—Comment that describes the access list entry, up to 100 characters long. <i>source</i>—Number of the network or host from which the packet is being sent. There are three ways to specify the source: <ul style="list-style-type: none"> <i>hostname</i>—Use the name of the host machine. <i>A.B.C.D</i>—Use 32-bit quantity in four-part, dotted-decimal format. <i>any</i>—Use the <i>any</i> keyword as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255. <i>source-wildcard</i>—(Optional) Wildcard bits to be applied to the source. There are two alternative ways to specify the source wildcard: <ul style="list-style-type: none"> Use a 32-bit quantity in four-part, dotted-decimal format. Place 1s in the bit positions you want to ignore. Use the <i>any</i> keyword as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255. <i>log</i>—(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the logging console command.) |

Configuring IP Access List Security on the Gatekeeper

Perform this task to enable a gatekeeper to use an IP access list to perform tokenless call authorization.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **gatekeeper**
4. **security acl answerarq *access-list-number***

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|---|
| Step 1 | enable Example: Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted. |
| Step 2 | configure terminal Example: Router# configure terminal | Enters global configuration mode. |
| Step 3 | gatekeeper Example: Router(config)# gatekeeper | Enters gatekeeper configuration mode. |
| Step 4 | security acl answerarq <i>access-list-number</i> Example: Router(config-gk)# security acl answerarq 20 | Instructs the gatekeeper to use an IP access list (also known as an access control list [ACL]) to verify calls. <ul style="list-style-type: none">• Calls received from endpoints listed in the ACL are processed by the gatekeeper regardless of whether they contain IZCTs or CATs in the ARQ message from the endpoint. Rather than sending a Location Reject (LRJ) message for calls without tokens from these endpoints, the gatekeeper sends an admission confirm (ACF) message and accepts the calls. |

Configuration Examples for Tokenless Call Authorization

This section provides the following configuration guidelines:

- [Configuring Tokenless Call Authorization Example, page 6](#)
- [Verifying Tokenless Call Authorization Example, page 6](#)

Configuring Tokenless Call Authorization Example

The following example shows how to configure tokenless call authorization. You create an IP ACL containing endpoints from which the gatekeeper should accept calls. After the router enters gatekeeper configuration mode, you instruct the gatekeeper to check the ACL before processing the call.

```
Router# enable
Router# configure terminal
  Router(config)# access-list 20 permit 172.16.10.190
  Router(config)# access-list 20 permit 192.16.18.2
  Router(config)# access-list 20 permit 192.16.10.12
  Router(config)# access-list 20 permit 192.16.12.1
  Router(config)# gatekeeper
  Router(config-gk)# security acl answerarq 20
```

Verifying Tokenless Call Authorization Example

The following example shows how to verify the IP access lists and that the gatekeeper has been configured to use them:

```
Router# show running-config
Building configuration...
.
.
.
ip access-list standard WORD
!
access-list 20 permit 172.16.10.190
access-list 20 permit 192.16.18.2
access-list 20 permit 192.16.10.12
access-list 20 permit 192.16.12.1
.
.
.
gatekeeper
zone local herndon.cisco.com cisco.com
security acl answerarq 20
no shutdown
.
.
.
end
```

Additional References

For additional information related to Tokenless Call Authorization, see the following sections:

- [Related Documents, page 7](#)
- [Standards, page 7](#)
- [MIBs, page 8](#)
- [RFCs, page 8](#)
- [Technical Assistance, page 8](#)

Related Documents

| Related Topic | Document Title |
|--|---|
| Gatekeeper security and Interzone ClearTokens (IZCTs) | Inter-Domain Gatekeeper Security Enhancement |
| Gatekeeper-to-gatekeeper authentication and Cisco access tokens (CATs) | Gatekeeper-to-Gatekeeper Authentication |
| Voice configuration documentation | Cisco IOS Voice, Video, and Fax Configuration Guide, Release 12.2 |
| Voice command reference | Cisco IOS Voice, Video, and Fax Command Reference, Release 12.2 T |
| Platform documentation | <ul style="list-style-type: none"> • Cisco 2600 series product documentation • Cisco 3600 series product documentation • Cisco 3700 series product documentation |
| Platform release notes | <ul style="list-style-type: none"> • Release Notes for Cisco 2600 Series Routers • Release Notes for Cisco 3600 Series Routers • Release Notes for Cisco 3700 Series Routers |

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 obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml |

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

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. | http://www.cisco.com/public/support/tac/home.shtml |

Command Reference

This section documents the **security acl answerarq** new command. All other commands used with this feature are documented in the Cisco IOS Release 12.2T command reference publications.

security acl answerarq

To configure the gatekeeper to use tokenless call authorization, use the **security acl answerarq** command in gatekeeper configuration mode. To disable tokenless call authorization, use the **no** form of this command.

security acl answerarq *access-list-number*

no security acl answerarq *access-list-number*

Syntax Description

| | |
|---------------------------|--|
| <i>access-list-number</i> | Number of an access list that was configured using the access-list command. This is a decimal number from 1 to 99 (standard) or from 1300 to 1999 (extended). Only standard IP access lists numbered 1 through 99 are supported for the Tokenless Call Authorization feature. |
|---------------------------|--|

Defaults

Tokenless call authorization is not configured.

Command Modes

Gatekeeper configuration

Command History

| Release | Modification |
|-----------|------------------------------|
| 12.2(15)T | This command was introduced. |

Usage Guidelines

Use this command in conjunction with the **access-list** command to configure tokenless call authorization on a gatekeeper. The IP access list contains endpoints that are not in the gatekeeper's administrative domain, but from which calls should be accepted. This command configures the gatekeeper to use the IP access list for security.

Examples

The following example shows how to configure a gatekeeper to use a previously configured IP access list with an IP access list number of 20 for call authorization:

```
Router(config-gk)# security acl answerarq 20
```

Related Commands

| Command | Description |
|--------------------|--|
| access-list | Configures the access list mechanism for filtering frames by protocol type or vendor code. |