

# SIP Inbound Authentication

The Session Border Controller (SBC) supports two modes of Session Initiation Protocol (SIP) inbound authentication to challenge inbound SIP requests: local and remote. You must select the mode of authentication to configure the SBC according to the level of support present in the Remote Authentication Dial-In User Service (RADIUS) servers. If the RADIUS servers are compliant with only draft-sterman-aaa-sip-00 to 01, then select the local mode. If the RADIUS servers are compliant with only RFC 4590, then use the remote authentication mode.



**Note**

This feature is optional and you can configure the SBC not to challenge the inbound requests.



**Note**

For ACE SBC Release 3.0.00, this feature is supported in the unified model only.

## Feature History for SIP Inbound Authentication

Release	Modification
ACE SBC Release 3.0.00	This feature was introduced on the Cisco 7600 series router along with support for the SBC unified model.

## Contents

This module contains the following sections:

- [Prerequisites for Implementing SIP Inbound Authentication, page 27-1](#)
- [Restrictions for Implementing SIP Inbound Authentication, page 27-2](#)
- [Information About SIP Inbound Authentication, page 27-2](#)
- [How to Configure SIP Inbound Authentication, page 27-5](#)
- [Examples of Show Commands, page 27-7](#)

## Prerequisites for Implementing SIP Inbound Authentication

The following prerequisites are required to implement SIP inbound authentication:

- Configure a SIP adjacency with the intended mode of authentication before you configure the SBC to authenticate inbound calls.
- Configure the RADIUS server to specify which mode of inbound authentication is selected.

## Restrictions for Implementing SIP Inbound Authentication

The following restrictions and limitations apply to implement SIP inbound authentication:

- The SBC supports only one inbound authentication realm per adjacency.
- The SBC does not check the validity of nonces generated by a RADIUS server; the RADIUS server must be configured to perform this check.
- The SBC does not designate a particular RADIUS server group on an adjacency for inbound authentication.
- Since trust-transference of calls does not occur between inbound authentication, outbound authentication, and Transport Layer Security (TLS) connections, a successful inbound authentication does not ensure that the SBC marks the call as secure or implement outbound authentication. Users can, however, configure inbound authentication, outbound authentication, and TLS independently on the same adjacency.

## Information About SIP Inbound Authentication

This section contains the following subsections:

- [Local Inbound Authentication, page 27-2](#)
- [Remote Inbound Authentication, page 27-2](#)
- [Interaction with Outbound Authentication, page 27-3](#)
- [Failure Modes for Inbound Authentication, page 27-3](#)

### Local Inbound Authentication

When configured to perform local inbound authentication, the SBC is responsible for challenging an unauthorized request from the remote peer first. Therefore, to be able to challenge the request from the remote peer, the adjacency must already be configured with an authentication realm. After the remote peer has validated the request, it is forwarded to the RADIUS server, which then decides whether to permit the call to pass through or not.

### Remote Inbound Authentication

When configured to perform remote inbound authentication, the SBC relies on the RADIUS server to challenge an authorized request from the remote peer. The SBC forwards the challenge request generated by the RADIUS server to the remote peer, and also forwards the remote peer's authentication request to the RADIUS server.

## Interaction with Outbound Authentication

If an adjacency is configured for inbound authentication, then after it successfully authenticates an inbound request, the authorization headers matching the realm for that adjacency are stripped out and not propagated to the outbound signal. Authorization headers for other realms, however, are passed through to the outbound request.

## Failure Modes for Inbound Authentication

When the inbound authentication is configured, the following failure modes may occur (in addition to the standard SIP signal failure modes):

### Unacceptable Parameters

If the endpoint or RADIUS server specifies a quality of protection parameter other than **auth** or **auth-int**, then the inbound request is rejected and a 403 response is generated. Similarly, the SBC generates a 403 response when algorithms other than MD5 and MD5-sess are used.

### Access-Request Rejection

If the RADIUS server rejects the Access-Request signal with an Access-Reject response, the SBC sends a 403 response to the endpoint.

### Insufficient Memory

If the SBC does not have sufficient memory to process an inbound authentication request, it rejects the request and sends a 503 response.

### No Match on Authentication Realm

If the peer does not return any authentication headers that specify the authentication realm contained in the adjacency's configuration, then the SBC rechallenges the request with 401 response.

### No Match on Nonce

If the peer's nonce does not match the one generated by the SBC, then the SBC rejects the authentication request and sends a 403 response.

### Nonce Timed Out

If the peer's nonce has timed out, then the SBC challenges the nonce by sending a 401 response and a new nonce.

## No Acceptable RADIUS Servers

If there is no RADIUS server to support a mode configured on the adjacency, then the SBC rejects the authentication request with a 501 response and creates a log to alert the user of the inconsistent configuration.

# How to Configure SIP Inbound Authentication

This section contains the steps for configuring SIP local inbound authentication a RADIUS server.

## SUMMARY STEPS

1. **configure**
2. **sbc** *service-name*
3. **sbe**
4. **radius authentication**
5. **activate**
6. **server** *server-name*
7. **address**
8. **mode local**
9. **key** *password*
10. **exit**
11. **exit**
12. **adjacency sip** *adjacency-name*
13. **authentication-realm inbound** *realm*
14. **authentication mode local**
15. **authentication nonce timeout** *time*
16. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure</b>  <b>Example:</b> host1/Admin# configure	Enables global configuration mode.
Step 2	<b>sbc</b> <i>service-name</i>  <b>Example:</b> host1/Admin(config)# sbc mysbc	Enters the mode of an SBC service. <ul style="list-style-type: none"> <li>• Use the <i>service-name</i> argument to define the name of the service.</li> </ul>
Step 3	<b>sbe</b>  <b>Example:</b> host1/Admin(config-sbc) # sbe	Enters the mode of the signaling border element (SBE) function of the SBC.

	Command or Action	Purpose
Step 4	<b>radius authentication</b>  <b>Example:</b> host1/Admin(config-sbc-sbe)# radius authentication	Enters the mode for configuring a RADIUS client for authentication purposes.
Step 5	<b>activate</b>  <b>Example:</b> host1/Admin(config-sbc-sbe-auth)# activate	Activates the RADIUS client.
Step 6	<b>server server-name</b>  <b>Example:</b> host1/Admin(config-sbc-sbe-auth)#server authserv	Enters the mode for configuring the authentication server.
Step 7	<b>address ipv4 ipv4-address</b>  <b>Example:</b> host1/Admin(config-sbc-sbe-auth-ser)# address ipv4 200.200.200.122	Specifies the IPv4 address of the authentication server.
Step 8	<b>mode local</b>  <b>Example:</b> host1/Admin(config-sbc-sbe-auth-ser)#mode local	Configures the RADIUS server for local inbound authentication. By default, the mode is remote.
Step 9	<b>key password</b>  <b>Example:</b> host1/Admin(config-sbc-sbe-auth-ser)# key authpass1	Sets the authentication server key.
Step 10	<b>exit</b>  <b>Example:</b> host1/Admin(config-sbc-sbe-auth-ser)# exit	Exits the mode for configuring the authentication server.
Step 11	<b>exit</b>  <b>Example:</b> host1/Admin(config-sbc-sbe-auth)# exit	Exits the mode for configuring the RADIUS client and enters the SBE mode.
Step 12	<b>adjacency sip adjacency-name</b>  <b>Example:</b> host1/Admin(config-sbc-sbe)# adjacency sip test	Enters the mode of an SBE SIP adjacency. <ul style="list-style-type: none"> <li>Use the <i>adjacency-name</i> argument to define the name of the service.</li> </ul>
Step 13	<b>authentication-realm inbound realm</b>  <b>Example:</b> host1/Admin(config-sbc-sbe)# authentication-realm inbound cisco.com	Configures a set of authentication credentials for a specified domain on the specified SIP adjacency.  <b>Note</b> This is a mandatory parameter for local mode.

	Command or Action	Purpose
Step 14	<b>authentication mode local</b>  <b>Example:</b> host1/Admin(config-sbc-sbe-adj-sip)# authentication mode local	Configures the SIP adjacency for local inbound authentication. To configure the SIP adjacency, for remote inbound authentication, set the value to <b>remote</b> .
Step 15	<b>authentication nonce timeout time</b>  <b>Example:</b> host1/Admin(config-sbc-sbe-adj-sip)# authentication nonce timeout 10000	Configures the value of the authentication nonce timeout in seconds. The range of acceptable values is 0 to 65535 seconds. The default value is 300 seconds.
Step 16	<b>exit</b>  <b>Example:</b> host1/Admin(config-sbc-sbe-adj-sip)# exit	Exits the adj-sip mode and returns to the SBE mode.

## Examples of Show Commands

```

host1/Admin# show services sbc mySbc sbe adjacencies SipToIsp42 detail
SBC server mySbc
Adjacency SipToIsp42
Status: Attached
Signaling address: 10.2.0.122:5060
Signaling-peer:    200.200.200.179:8888
Force next hop:   No
Account:         core
Group:           None
In Header Profile:  Default
Out Header Profile: Default
In method profile:  Default
Out method profile: Default
In UA option profile: Default
Out UA option profile: Default
In proxy option profile: Default
Priority set name:  Default
Local-id:         None
Rewrite REGISTER: Off
Target address:   None
NAT Status:       Auto-Detect
Reg-min-expiry:   3000 seconds
Fast-register:    Enabled
Fast-register-int: 30 seconds
Authenticated mode: Local
Authenticated realm: Cisco.com
Authenticated nonce life time: 300 seconds
IMS visited NetID: None
Inherit profile:  Default
Force next hop:   No
Home network ID:  None
UnEncrypt key data: None
SIPpassthrough:  No
Rewrite from domain: Yes
Rewrite to header: Yes
Media passthrough: No
Preferred transport: UDP
Hunting Triggers: Global Triggers

```

```
Redirect mode:      Passthrough
```