RADIUS Authentication for Cisco SPS

You can configure Cisco SPS to send RADIUS Access-Request packets to a RADIUS server that correspond to the SIP REGISTER and SIP INVITE requests that the RADIUS server receives. Access-Request packets are as defined in RFC 2865, with the additional syntax and semantics defined in RADIUS Extension for Digest Authentication (Cisco Systems draft-sterman-aaa-sip-01.txt). Based on the responses received from the RADIUS server for the Access-Request packets, the SIP requests are either accepted or rejected by Cisco SPS.

The authentication scheme used by Cisco SPS may be either HTTP Digest or HTTP Basic, as defined in RFC 2617 and RFC 3261; however, the use of HTTP Basic as a SIP authentication mechanism has been deprecated by RFC 3261. Only HTTP Digest is described in this document. SIP messaging that is associated with the authentication occurs between Cisco SPS and the originator of the SIP request; but the actual validation of the user’s identification and password may occur at Cisco SPS or at a RADIUS server. The configuration which occurs at the RADIUS server is the only configuration within the scope of this document.

RADIUS Authentication for Cisco SPS Overview

Cisco SPS can generate Access-Request packets for REGISTER and INVITE requests as a means of authenticating any request that has not yet passed the configured access-control mechanisms. The high-level diagram in Figure 7 shows a SIP REGISTER which is assumed to contain the user’s credentials from a SIP phone to Cisco SPS, as well as the corresponding RADIUS Access-Request packet sent by Cisco SPS to the RADIUS server. In this example, the RADIUS server queries an external database to retrieve the user’s password and validate the credentials. Further processing of the REGISTER by Cisco SPS is dependant on the response Cisco SPS receives from the RADIUS server.
A user password is stored in the RADIUS server, or in some database that is accessible by the RADIUS server. The user identification, as found in the Authorization header (for REGISTER requests) or the Proxy-Authorization header (for INVITE requests), is passed as one of the attribute value pairs from the Cisco SPS to the RADIUS server in an Access-Request. You can configure Cisco SPS to add any SIP headers as VSAs in the authentication request to the RADIUS server.

The username can be expanded by Cisco SPS before being passed to the RADIUS server. This enables phone numbers to be expanded to fully expanded E.164 numbers before processing.

If the virtual proxy host feature is enabled, the username@domain (username found in the Authorization/Proxy-Authorization header and the domain name found in either the Authorization/Proxy-Authorization header if present, otherwise in the From header) can be passed as one of the attribute value pairs from Cisco SPS to the RADIUS server. This attribute value pair can then be used as the key for the user.

**RADIUS Access-Request Format**

The following summary describes the format of the RADIUS data packet. The data fields defined in the format for the Access-Request packet are transmitted from left to right.

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

---

**Code**

The Code field is one octet and identifies the type of RADIUS packet. RADIUS access codes (decimal) are assigned as follows:

1. Access-Request code (request sent by Cisco SPS)
2. Access-Accept code (returned by the RADIUS server if the SIP request is accepted)
3. Access-Reject code (returned by the RADIUS server if the SIP request is rejected)

Upon receipt of an Access-Request packet, the RADIUS server must transmit an Access-Accept or Access-Reject reply. If all Attribute values received in an Access-Request packet are acceptable then the RADIUS server must transmit a packet with the Code field set to 2 (Access-Accept). If any value of the received Attributes is not acceptable, then the RADIUS server must transmit a packet with the Code field set to 3 (Access-Reject).

**Identifier**

The Identifier field is one octet and aids in matching requests and replies. The RADIUS server can detect a duplicate request if the server sees the same client source IP address and source UDP port and Identifier field within a short span of time. Cisco SPS changes the Identifier field whenever the content of the Attributes field change and whenever a valid reply has been received for a previous request. For retransmissions where the contents are identical, the Identifier field remains unchanged. Cisco SPS uses monotonically increasing identifiers that wrap around to 1 once they reach 254.

**Length**

The Length field is two octets and indicates the length of the packet including the Code, Identifier, Length, Authenticator and Attribute fields. Octets outside the range of the Length field are treated as padding and ignored on reception. If a packet is shorter than the Length field indicates, the packet must be silently discarded. The minimum Length field value is 20 and maximum is 4095. If Cisco SPS is configured to include more headers than fit within the maximum length, the Access-Request packet is truncated.

**Authenticator**

The Authenticator field is 16 octets. The most significant octet is transmitted first. The Authenticator field value is used to authenticate the messages between the client and the RADIUS access server.

**Request Authenticator**

In Access-Request packets, the Authenticator value is a 16-octet random number, which is called the Request Authenticator. The value is unpredictable and unique over the lifetime of a shared secret between the Cisco SPS and the RADIUS server because repetition of a request value with the same secret permits an attacker to reply with a previously intercepted response. The shared secret is configured on Cisco SPS as described in the “Authentication Module Directives” section on page 30.

**Response Authenticator**

The Authenticator field in an Access-Accept and Access-Reject packet is called the Response Authenticator and contains a one-way MD5 hash that is calculated over a stream of octets, consisting of the RADIUS packet, beginning with the Code field, including the Identifier, the Length, the Request Authenticator field from the Access-Request packet, and the response Attributes, followed by the shared
secret. That is, $\text{ResponseAuth} = \text{MD5 (Code+ID+Length+RequestAuth+Attributes+Secret)}$ where $+$ denotes concatenation. The shared secret configured that is on the RADIUS server must match the one configured on Cisco SPS.

On reception of an Access-Accept, the Response Authenticator field must contain the correct response for the pending access request. Invalid packets are discarded by Cisco SPS, and an error is logged in the error_log file.

### Attributes

The Attributes field is variable in length and contains a list of attributes. Attributes may have multiple instances. The end of the list of attributes is indicated by the Length field of the RADIUS packet. The following is a summary of the attribute format. The fields are transmitted from left to right.

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |  Value ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

#### Standard Attributes

The standard RADIUS attributes in RFC 2865 that are included in Access-Request packets from Cisco SPS are listed in Table 6. The Attribute column is for illustrative purposes only because it is not a field in the actual attributes included in the request. The Length field is in octets and is 1 (for the Type field) + 1 (for the Length field) + length of the Value field.

---

Table 6  **Standard Attributes for Access-Request Packets**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Type</th>
<th>Length (octets)</th>
<th>Value</th>
</tr>
</thead>
</table>
| User Name | 1    | 3-254           | User part of the URL in the “From” SIP header or user in “Proxy-Authorization” SIP header, if present. This value is controlled by a configuration directive (OrigUserNameSource). If the RadiusUserNameAttrAddDomain directive is On, the domain in the “From” header will be appended to the User Name and the User Name attribute will be in the name@domain format.
|           |      |                 | The User Name can be expanded to a fully expanded E164 number. If the user name is taken from the “From” header, the expansion is dependent on the user type and the NumericUserNameInterpretation directive. If the user name is taken from the “Proxy-Authorization” header, the expansion is dependent on the NumExpandAuthUserName directive. The expansion is based on the number expansion rules, which are defined in the number expansion module. Example: “5000” Example: “+1xxxyyy1212” Example: “bob@foo.com” |
| NAS IP    | 4    | 6               | IP address of Cisco SPS. Example: a.22.76.1 |
| Vendor-Specific | 26   | 7-254           | See Table 2 on page 10 for the complete set. |
The following is a summary of the VSA format:

```
+---------------------------------+-------+-----------------+-----------------+---------------------------------+-------+-----------------+-----------------+
| Type     | Length          | Vendor-ID          | Vendor-Type      | Vendor-Length     | Value                           |
+---------------------------------+-------+-----------------+-----------------+---------------------------------+-------+-----------------+-----------------+
| 26       | 7 to 254 octets | 9                |                 |                  |                                |
+---------------------------------+-------+-----------------+-----------------+---------------------------------+-------+-----------------+-----------------+
```

The values of these fields for Accounting-Requests from Cisco SPS are:

- Type = 26 (indicating Vendor-Specific)
- Length = 7 to 254 octets
- Vendor-ID = 9 (Cisco’s Vendor-ID for all VSAs used by Cisco SPS)
- Vendor-Type, Vendor-Length, and Vendor-Data take various values as summarized in Table 2 on page 10.

The Attribute column is for illustrative purposes only because it is not a field in the actual attributes that are included in the request. The Vendor-Length field is in octets and is 1 (for the Vendor-Type field) + 1 (for the Vendor-Length field) + length of the Vendor-Data field. Table 7 presents the relevant Cisco VSA.

For additional details on all Cisco VSAs, see http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/vapp_dev/vsaig3.htm#27593.
Configuring RADIUS Authentication

You can configure Cisco SPS to send Access-Request packets to two RADIUS servers. For initial testing, it may be more convenient to set-up a single RADIUS server only; but in a production environment, using a pair of RADIUS servers for redundancy is strongly recommended.

Cisco SPS has multiple SIP message-handling processes (sipds); each process handles individual SIP messages. In the event the given SIP message is one that requires authentication, it is the responsibility of the sipd handling the message to send the corresponding Access-Request packet. The Access-Request packet is generated and sent prior to accepting the SIP request as a valid request, and if no response is received, the request will simply time-out. This means that SIP-request processing is dependent on RADIUS authentication.

The algorithm by which the sipd selects a RADIUS server to which to send the Access-Request packet is the same as for the Accounting-Request.

The values of the various retransmission timers and counters, as well as the configuration of the primary and the secondary RADIUS servers, are described in the “Authentication Module Directives” section on page 30 and in the “Authentication-Related SIP Server Core Directives” section on page 32.

Table 7  Cisco VSAs for Access-Request Packets

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Vendor Type</th>
<th>Vendor Length (octets)</th>
<th>Vendor Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>sip-hdr</td>
<td>1</td>
<td>Less than or equal to 247</td>
<td>An arbitrary SIP header found in the SIP request received by Cisco SPS (complete header line). Inclusion of any given header is controlled by a configuration directive AcctIncludeSIPHeader. Example: “sip-hdr=CSeq: 101 INVITE” Example: “sip-hdr=Via: SIP/2.0/UDP b.19.174.99:5060;branch=363e586d-e1529570-dad25df7-49a3df73-1,SIP/2.0/UDP a.22.76.38:5060;received=a.22.76.38”</td>
</tr>
</tbody>
</table>

Authentication Module Directives

The following directives are specific to the authentication module for Cisco SPS. Reasonable default values are assigned when possible; however, it is advisable to carefully set and review the values of all these directives. The mechanisms for viewing and editing these directives are described in Cisco SIP Proxy Server Administrator Guide. See the following URL:

The follow describes how each directive is used and how to choose appropriate values:

- Authentication—Specifies whether users must be authenticated before their transactions are processed. Valid values are On (authentication required) and Off (authentication not required). The default is Off. For authentication to occur, this directive must be set to On.

User authentication does not occur in the following case because access control is already satisfied:
- Access Control is set to On
- Host name or IP address of the sender is covered by a corresponding Allow from the directive
- Satisfy directive is set to Any instead of All

For additional information on Access Control, see Cisco SIP Proxy Server Administrator Guide at the following location:


- **AuthRealm**—Realm used in authentication response headers. The default is CISCO.
- **AuthServer**—Server on which user authentication takes place. Valid values are Radius and Proxy. The default is Proxy. For Access-Request packets to be sent to the RADIUS server, this must be set to Radius.
- **AuthScheme**—Type of authentication method to be used when users are required to obtain authentication before receiving service from the Cisco SPS. Valid values are HTTP_Digest and HTTP_Basic. The default is HTTP_Digest. HTTP_Basic for use with SIP has been deprecated in RFC 3261, so HTTP_Digest is all that is covered in this document.
- **AuthDigestQop**—QOP value for digest authentication challenge. Indicates the quality of protection supported. Valid values are Auth (qop= “auth”, authentication only), Auth-Int (qop= “auth-int”, authentication and integrity), and Both (qop= “auth, auth-int”, allows the client to choose). The default is Auth.

The use of the value Both results in value “auth, auth-int” being sent in the challenge to the SIP client. The client then responds with either “auth” or “auth-int”, and this is the value included in the QOP subattribute of the Digest-Attributes attribute.
- **AuthDigestAlgorithm**—Value of the algorithm value to be included in a Digest Challenge to the user. This value is used in Authentication Response headers. Valid values are MD5 (algorithm="MD5") and MD5-sess (algorithm="MD5-sess"). The default is MD5.
- **AuthConsumeProxyAuth**—Enables Cisco SPS to consume the Proxy-Authorization header before the request is forwarded downstream to the next hop. Valid values are On (consume header) and Off (pass header downstream). The default is On.
- **AuthAllow3rdPartyRegistration**—Allows unauthorized redirection of calls by a third-party registration. If the value of this directive is set to Off, the username in the To header is matched with the username in the From or Authorization header. If the user names in these two headers do not match, registration is rejected. If the value is On, third-party registrations are allowed. This is independent of the authentication scheme. The default is Off.
- **AuthAllow3rdPartyInvite**— Allows third-party INVITEs. Valid values are On (user in the From header can differ from user used for authentication) and Off (user in the From header must match user used for authentication). The default is On.
- **RadiusAuthSkew**—Time (in seconds) for which a nonce included by Cisco SPS in a digest challenge is valid. The default is 30.
- **PrimaryRadiusAuthIp**—IP address or host name of the primary RADIUS server to be used for authentication. By default it is set to 127.0.0.1. For authentication to work properly, this value must be set to the IP address of a functioning RADIUS server.
- **PrimaryRadiusAuthPort**—Destination port number of the primary RADIUS server to be used for authentication. The well known RADIUS server port for authentication is 1812. By default it is set to 0. For authentication to work properly, this value must be set to the port on which the primary RADIUS server is listening for Access-Request packets.
- **PrimaryRadiusAuthSecret**—Secret text string shared between Cisco SPS and the primary RADIUS authentication server. This attribute is used to compute the Authenticator field of the Access-Request packets as described in the “Response Authenticator” section on page 27. For authentication to work properly, this value must be set to the same value configured on the RADIUS server.
• SecondaryRadiusAuthIp—IP address or host name of the secondary RADIUS server to be used for authentication. By default it is set to 127.0.0.1. For authentication to work properly, this value must be set to IP address of a functioning RADIUS server.

• SecondaryRadiusAuthPort—Destination port number of the secondary RADIUS server to be used for authentication. The well known RADIUS server port for authentication is 1812. By default it is set to 0. For authentication to work properly, this value must be set to the port on which the secondary RADIUS server is listening for Access-Request packets.

• SecondaryRadiusAuthSecret—Secret text string shared between Cisco SPS and the secondary RADIUS authentication server. This is used to compute the Authenticator field of the Access-Request packets as described in the “Response Authenticator” section on page 27. For authentication to work properly, this value must be set to the same value configured on the RADIUS server.

• AuthIncludeSIPHeader—SIP header to be sent as a sip-hdr VSA (see Table 7 on page 30) within RADIUS Access-Request packets. You can configure a maximum of 50 headers.

**Authentication-Related SIP Server Core Directives**

The following directives reside in the SIP Server Core module, but they affect the authentication operation of Cisco SPS. These directives are shared across the accounting, authentication, and pre-authentication modules. Reasonable default values are assigned when possible; however, it is advisable to carefully set and/or review the values of all these directives.

---

**Note**

Complete details regarding viewing and editing Cisco SPS directives are beyond the scope of *RADIUS Interface for Cisco SPS*. Please refer to the *Cisco SIP Proxy Server Administrator Guide* for comprehensive configuration information. See the following URL:


---

The following notes summarize how directives are used and how to choose appropriate values for each within the context of a RADIUS-based environment:

• **StatefulServer**—Determines whether Cisco SPS is a transaction-stateful or transaction-stateless server. A transaction includes the following: received request, request or requests (if forked) forwarded downstream, responses received from downstream hosts, and best response returned upstream. Valid values are as follows:
  - On (stateful)—Cisco SPS remembers incoming and outgoing requests, provides reliable retransmission of proxied requests, and returns the best final responses.
  - Off (stateless)—Cisco SPS forgets all information once a request or response has been processed. Cisco SPS forwards requests and responses.

• **OrigUserNameSource**—Origin of the User Name attribute (see Table 6 on page 28) in Accounting-Request packets. Valid values are From and Auth. If the value is From, the user part of the URL in the From SIP header is used to populate the User Name attribute. If the value is Auth, the user provided for authentication in the Authorization or Proxy-Authorization header is used instead. If no Proxy-Authorization header is present, the user is taken from the From header regardless of the setting of this directive. The default is Auth. A relevant configuration for this directive is one where all the IP phones authenticating themselves to Cisco SPS share a common user and password for authentication purposes. For example, Bob and Mary both work for Cisco and populate the From header with Bob and Mary respectively. However, they authenticate themselves
to Cisco SPS by using a common username of cisco and a common password. The OrigUserNameSource provides the ability to choose whether to have Bob or Mary versus cisco as the User-Name in Accounting-Request packets.

- RadiusRetransmissionInterval—Time (in milliseconds) between retransmissions to the RADIUS server. The default is 2000.
- RadiusRetransmissionCount—Number of times to retransmit the current RADIUS request before deciding that a given RADIUS server is unreachable and trying the other RADIUS server. The default is 2.
- RadiusRetransmissionAfterFailure—Number of times to try the entire procedure for sending a RADIUS request if all attempts to send the previous request failed. The default is 0.
- RadiusRetryTime—Time (in seconds) before retrying the primary RADIUS server if it is out of service, or before trying to send requests to any RADIUS server. The default is 300 (5 minutes).

Configuration Example and Call Flows with Debugging Enabled

The following sections illustrate various call scenarios and the associated SIP and RADIUS messaging for each scenario:

- REGISTER-Accepted Scenario, page 33
- REGISTER Rejected Scenario, page 35
- INVITE-Accepted Scenario, page 36
- INVITE Rejected, page 37

The components involved in the scenarios are listed in Table 8:

Table 8 Call-Scenario Components

<table>
<thead>
<tr>
<th>Component</th>
<th>Name</th>
<th>IP Address</th>
<th>Hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco SIP Proxy Server</td>
<td>Cisco SPS</td>
<td>b.19.174.239</td>
<td>vvs-vitra</td>
</tr>
<tr>
<td>FreeRADIUS Server</td>
<td>FreeRADIUS</td>
<td>b.19.174.128</td>
<td>n/a</td>
</tr>
<tr>
<td>IP Phone (Cisco 7905)</td>
<td>Cisco 7905</td>
<td>a.22.76.101</td>
<td>n/a</td>
</tr>
<tr>
<td>IP Phone (Cisco 7963)</td>
<td>Cisco 7963</td>
<td>a.22.77.248</td>
<td>n/a</td>
</tr>
</tbody>
</table>

REGISTER-Accepted Scenario

In this scenario, Cisco 7905 is registering with Cisco SPS. The credentials provided by Cisco 7905 match those at the RADIUS server, so the registration is accepted.

Configuring the REGISTER-Accepted Scenario

Cisco SPS is configured with authentication via RADIUS enabled for a single RADIUS server. This is accomplished by modifying the default configuration with which Cisco SPS was initially installed. Table 9 provides a summary of the required modifications to the default configuration. Please refer to the “Cisco SPS Interface Reference Appendix” for screen examples showing configuration options for RADIUS-implementation.
### Table 9  
Cisco SPS Directives Modifications for RADIUS-based Implementation for the REGISTER-Accepted Scenario

<table>
<thead>
<tr>
<th>Cisco SPS Configuration Option Screen</th>
<th>Cisco SPS Directive</th>
<th>Default Value</th>
<th>Modified Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authentication</strong></td>
<td>Authentication</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td></td>
<td>AuthenticationServer</td>
<td>Proxy</td>
<td>Radius</td>
</tr>
<tr>
<td></td>
<td>PrimaryRadiusServer</td>
<td>Not Set</td>
<td>Set IP address, port, and secret of FreeRADIUS server</td>
</tr>
<tr>
<td></td>
<td>SecondaryRadiusServer</td>
<td>Not Set</td>
<td>Set IP address, port, and secret of FreeRADIUS server</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>In the scenario presented, this could have been left with the default values, but instead the same values were used as for the primary server.</td>
</tr>
<tr>
<td></td>
<td>AuthSIPHeaders</td>
<td>Not Set</td>
<td>For this scenario, From, Proxy-Authorization, and Authorization were added.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The addition of these values are optional and was done for illustrative purposes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>According to the RADIUS Extension for Digest Authentication, these headers are legal but will be ignored by the RADIUS server.</td>
</tr>
<tr>
<td><strong>Debugs and Logs</strong></td>
<td>StateMachine</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td></td>
<td>Radius</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td></td>
<td>Authentication</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td></td>
<td>LogLevel</td>
<td>warn</td>
<td>debug</td>
</tr>
</tbody>
</table>


Call Flow

The call flow is shown in Figure 8.

**Figure 8** REGISTER Accepted

For complete listings of records, debug output and error logs related to the RADIUS interface Cisco SPS implementation, please refer to “RADIUS Interface for Cisco SPS Scenario Output Appendix”.

**REGISTER Rejected Scenario**

In this example, Cisco 7905 is registering with Cisco SPS. The credentials provided by Cisco 7905 do not match those at the RADIUS server, so the registration is rejected.

**Configuring the REGISTER-Rejected Scenario**

Same as the “Configuring the REGISTER-Accepted Scenario” section on page 33.

**Call Flow**

The call flow is shown in Figure 9.
**INVITE-Accepted Scenario**

In this example, Cisco 7963 is calling Cisco 7905 through Cisco SPS. The credentials provided by Cisco 7963 match those at the FreeRADIUS server, so the INVITE is accepted and the call succeeds.

**Configuring the INVITE-Accepted Scenario**

Same as the “Configuring the REGISTER-Accepted Scenario” section on page 33.

**Call Flow**

The call flow is shown in Figure 10.
**INVITE Accepted**

In this example, Cisco 7905 is calling Cisco 7963 through Cisco SPS. The credentials provided by Cisco 7905 do not match those at the FreeRADIUS server, so the INVITE is rejected.

**INVITE Rejected**

In this example, Cisco 7905 is calling Cisco 7963 through Cisco SPS. The credentials provided by Cisco 7905 do not match those at the FreeRADIUS server, so the INVITE is rejected.

**Configuration**

Same as the “Configuring the REGISTER-Accepted Scenario” section on page 33.

**Call Flow**

The call flow is shown in Figure 11.
Figure 11  INVITE Rejected

For complete listings of records, debug output and error logs related to the RADIUS interface Cisco SPS implementation, please refer to “RADIUS Interface for Cisco SPS Scenario Output Appendix”.