



RSA SecurID Servers for AAA

The following topics explain how to configure RSA SecurID servers used in AAA. The RSA SecureID servers are also known as SDI servers, because SDI is the protocol used to communicate with them. You can use RSA SecurID servers for the authentication of management connections, network access, and VPN user access.

- [About RSA SecurID Servers, on page 1](#)
- [Guidelines for RSA SecurID Servers for AAA, on page 1](#)
- [Configure RSA SecurID Servers for AAA, on page 2](#)
- [Monitor RSA SecurID Servers for AAA, on page 4](#)
- [History for RSA SecurID Servers for AAA, on page 4](#)

About RSA SecurID Servers

You can use RSA SecurID servers either directly for authentication, or indirectly, as a second factor for authentication. In the latter case, you would configure the relationship to the SecurID server between the SecurID server and your RADIUS server, and configure the ASA to use the RADIUS server.

But, if you want to directly authenticate against the SecurID server, you would create a AAA server group for the SDI protocol, which is the protocol used to communicate with these servers.

When you use SDI, you need only specify the primary SecurID server when you create the AAA server group. The ASA will retrieve the `sdiconf.rec` file, which lists all of the SecurID server replicas, when it first connects to the server. The ASA can then use these replicas for authentication if the primary server does not respond.

In addition, you must register the ASA as an authentication agent in the RSA Authentication Manager. Authentication attempts will fail until you register the ASA.

Guidelines for RSA SecurID Servers for AAA

- You can have up to 100 server groups in single mode or 4 server groups per context in multiple mode.
- Each group can have up to 16 servers in single mode or 4 servers in multiple mode. When a user logs in, the servers are accessed one at a time starting with the first server you specify in the configuration, until a server responds.

Configure RSA SecurID Servers for AAA

The following topics explain how to configure RSA SecurID server groups. You can then use these groups when configuring management access or VPNs.

Configure RSA SecurID AAA Server Groups

If you want to use direct communication with an RSA SecurID server for authentication, you must first create at least one SDI server group and add one or more servers to each group. If you are using the SecurID server in a proxy relationship with a RADIUS server, you do not need to configure an SDI AAA server group on the ASA.

Procedure

Step 1 Create the SDI AAA server group and enter `aaa-server-group` configuration mode.

```
aaa-server server_group_name protocol sdi
```

Example:

```
ciscoasa(config)# aaa-server watchdog protocol sdi
```

Step 2 (Optional.) Specify the maximum number of failed AAA transactions with a AAA server in the group before trying the next server.

```
max-failed-attempts number
```

Example:

```
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
```

The *number* argument can range from 1 and 5. The default is 3.

If you configured a fallback method using the local database (for management access only), and all the servers in the group fail to respond, or their responses are invalid, then the group is considered to be unresponsive, and the fallback method is tried. The server group remains marked as unresponsive for a period of 10 minutes (by default), so that additional AAA requests within that period do not attempt to contact the server group, and the fallback method is used immediately. To change the unresponsive period from the default, see the **reactivation-mode** command in the next step.

If you do not have a fallback method, the ASA continues to retry the servers in the group.

Step 3 (Optional.) Specify the method (reactivation policy) by which failed servers in a group are reactivated.

```
reactivation-mode {depletion [deadtime minutes] | timed}
```

Example:

```
ciscoasa(config-aaa-server-group)# reactivation-mode depletion deadtime 20
```

The **depletion** keyword reactivates failed servers only after all of the servers in the group are inactive. This is the default mode.

The **deadtime** *minutes* keyword-argument pair specifies the amount of time in minutes, between 0 and 1440, that elapses between the disabling of the last server in the group and the subsequent reenabling of all servers. The default is 10 minutes.

The **timed** keyword reactivates failed servers after 30 seconds of down time.

Add RSA SecurID Servers to an SDI Server Group

Before you can use an SDI server group, you must add at least one RSA SecurID server to the group.

Servers in an SDI server group use the authentication and server management protocol (ACE) to communicate with the ASA.

Procedure

Step 1 Add the RSA SecurID server to the SDI server group.

aaa-server *server_group* [(*interface_name*)] **host** *server_ip*

Example:

```
ciscoasa(config-aaa-server-group)# aaa-server servergroup1 outside host 10.10.1.1
```

If you do not specify an interface, then the ASA uses the **inside** interface by default.

You can use an IPv4 or IPv6 address.

Step 2 Specify the timeout value for connection attempts to the server.

timeout *seconds*

Specify the timeout interval (1-300 seconds) for the server; the default is 10 seconds. For each AAA transaction the ASA retries connection attempts (based on the interval defined on the **retry-interval** command) until the timeout is reached. If the number of consecutive failed transactions reaches the limit specified on the **max-failed-attempts** command in the AAA server group, the AAA server is deactivated and the ASA starts sending requests to another AAA server if it is configured.

Example:

```
ciscoasa(config-aaa-server-host)# timeout 15
```

Step 3 Specify the retry interval, which is the time the system waits before retrying a connection request.

retry-interval *seconds*

You can specify 1-10 seconds. The default is 10.

Example:

```
ciscoasa(config-aaa-server-host)# retry-interval 6
```

- Step 4** Specify the server port if it is different from the default RSA SecurID port, which is TCP/5500. The ASA contacts the RSA SecurID server on this port.

server-port *port_number*

Example:

```
ciscoasa(config-aaa-server-host)# server-port 5555
```

Monitor RSA SecurID Servers for AAA

You can use the following commands to monitor and clear RSA SecurID-related information.

- **show aaa-server**

Shows the AAA server statistics. Use the **clear aaa-server statistics** command to clear the server statistics.

- **show running-config aaa-server**

Shows the AAA servers that are configured for the system. Use the **clear configure aaa-server** command to remove the AAA server configuration.

History for RSA SecurID Servers for AAA

| Feature Name | Platform Releases | Description |
|------------------------|-------------------|---|
| SecurID Servers | 7.2(1) | Support for SecurID servers for AAA for management authentication. SecurID was supported in previous releases for VPN authentication. |
| IPv6 addresses for AAA | 9.7(1) | You can now use either an IPv4 or IPv6 address for the AAA server. |