



Configuring AAA

This chapter contains the following sections:

- [Information About AAA, page 1](#)
- [Prerequisites for AAA, page 4](#)
- [Guidelines and Limitations, page 4](#)
- [AAA Default Settings, page 4](#)
- [Configuring AAA, page 5](#)
- [Verifying the AAA Configuration, page 6](#)
- [Configuration Examples for AAA, page 7](#)
- [Feature History for AAA, page 7](#)

Information About AAA

AAA Security Services

Based on a user ID and password combination, AAA is used to authenticate and authorize users. A key secures communication with AAA servers.

In many circumstances, AAA uses protocols such as RADIUS or TACACS+, to administer its security functions. If your router or access server is acting as a network access server, AAA is the means through which you establish communication between your network access server and your RADIUS or TACACS+, security server.

Although AAA is the primary (and recommended) method for access control, additional features for simple access control are available outside the scope of AAA, such as local username authentication, line password authentication, and enable password authentication. However, these features do not provide the same degree of access control that is possible by using AAA.

Separate AAA configurations are made for the following services:

- User Telnet or Secure Shell (SSH) login authentication
- Console login authentication

- User management session accounting

AAA Service Configuration Option	Related Command
Telnet or SSH login	aaa authentication login default
Console login	aaa authentication login console

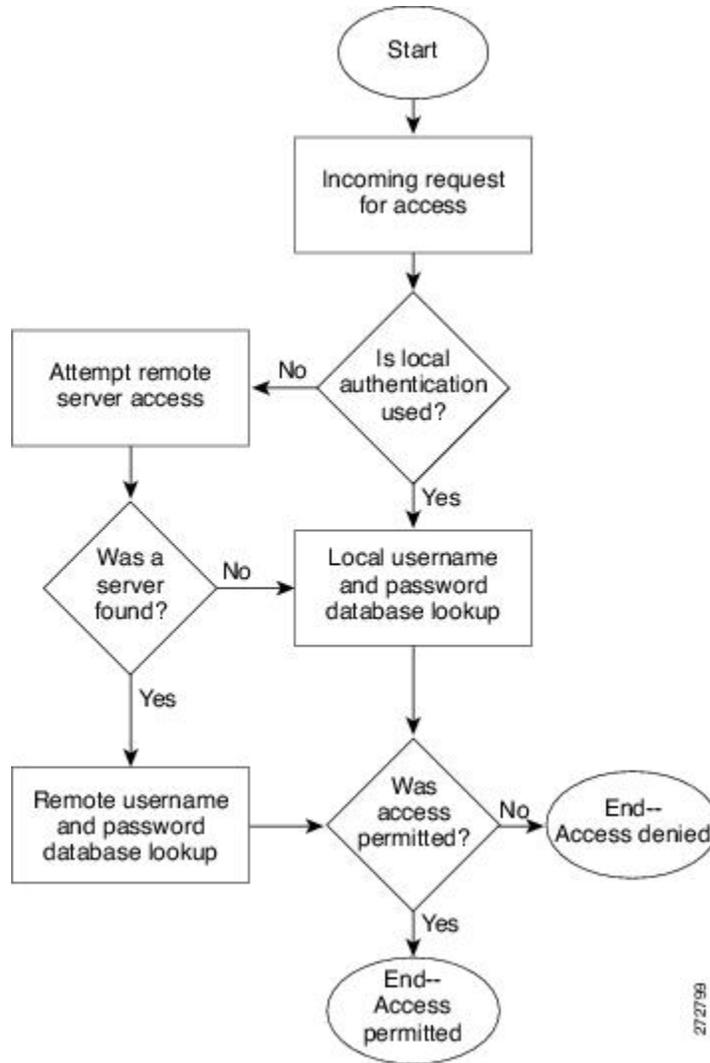
Authentication

Authentication provides the method of identifying users, including login and password dialog, challenge and response, messaging support, and, depending on the security protocol that you select, encryption. Authentication is the way a user is identified prior to being allowed access to the network and network services. You configure AAA authentication by defining a named list of authentication methods and then applying that list to various interfaces.

Authentication is accomplished as follows:

Authentication Method	Description
Local database	Authenticates the following with a local lookup database of usernames or passwords <ul style="list-style-type: none"> • Console login authentication • User login authentication • User management session accounting
Remote RADIUS or TACACS+ server	Authenticates the following with a local lookup database of usernames or passwords <ul style="list-style-type: none"> • Console login authentication • User login authentication • User management session accounting
None	Authenticates the following with only a username. <ul style="list-style-type: none"> • Console login authentication • User login authentication • User management session accounting

Figure 1: Authenticating User Login



Authorization

Authorization restricts the actions that a user is allowed to perform. It provides the method for remote access control, including one-time authorization or authorization for each service, per-user account list and profile, user group support, and support of IP, IPX, ARA, and Telnet.

Remote security servers, such as RADIUS and TACACS+, authorize users for specific rights by associating attribute-value (AV) pairs, which define those rights, with the appropriate user. AAA authorization works by assembling a set of attributes that describe what the user is authorized to perform. These attributes are compared with the information contained in a database for a given user, and the result is returned to AAA to determine the user’s actual capabilities and restrictions.

Accounting

Accounting provides the method for collecting and sending security server information used for billing, auditing, and reporting, such as user identities, start and stop times, executed commands (such as PPP), number of packets, and number of bytes. Accounting enables you to track the services that users are accessing, as well as the amount of network resources that they are consuming.

Accounting tracks and maintains a log of every SVS management session. You can use this information to generate reports for troubleshooting and auditing purposes. You can store accounting logs locally or send them to remote AAA servers.

AAA Server Groups

Remote AAA server groups can provide failovers if one remote AAA server fails to respond, which means that if the first server in the group fails, the next server in the group is tried until a server responds. Multiple server groups can provide failovers for each other in this same way.

If all remote server groups fail, the local database is used for authentication.

Prerequisites for AAA

- At least one TACACS+ or RADIUS server is IP reachable
- The VSM is configured as an AAA server client.
- A shared secret key is configured on the VSM and the remote AAA server.

Guidelines and Limitations

The Cisco Nexus 1000V does not support usernames that have all numeric characters and does not create local usernames that have all numeric characters. If a username that has all numeric characters already exists on an AAA server and is entered during login, the Cisco Nexus 1000V does authenticate the user.

AAA Default Settings

Parameters	Default
Console authentication method	local
Default authentication method	local
Login authentication failure messages	Disabled

Configuring AAA

Configuring a Login Authentication Method

If authentication is to be done with TACACS+ server group(s), you must have already added the group(s).

Before You Begin

Log in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# aaa authentication login {console default} {group <i>group-list</i> [none] local none}	Configures the console or default login authentication method. The keywords and arguments are as follows: <ul style="list-style-type: none"> • group—Specifies that authentication is done by server group(s). • <i>group-list</i>—List of server group names separated by spaces. • none— Specifies no authentication. • local—Specifies that the local database is used for authentication. <p>Note Local is the default and is used when no methods are configured or when all the configured methods fail to respond.</p> <ul style="list-style-type: none"> • none—Specifies that authentication is done by username.
Step 3	switch(config)# exit	Exits the global configuration mode and returns you to EXEC mode.
Step 4	switch# show aaa authentication	(Optional) Displays the configured login authentication method.
Step 5	switch# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

This example shows how to configure a login authentication method:

```
switch# configure terminal
switch(config)# aaa authentication login console group tacgroup
switch(config)# exit
switch# show aaa authentication
      default: group tacgroup
```

```

        console: group tacgroup
switch# copy running-config startup-config
switch#
switch# configure terminal
switch(config)# aaa authentication login default group tacacs
switch(config)# aaa authentication login console group tacacs

```

Enabling Login Authentication Failure Messages

You can enable the login authentication failure message to display if the remote AAA servers do not respond.

The following is the Login Authentication Failure message:

```

Remote AAA servers unreachable; local authentication done.
Remote AAA servers unreachable; local authentication failed.

```

Before You Begin

Log in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# aaa authentication login error-enable	Enables login authentication failure messages. The default is disabled.
Step 3	switch(config)# exit	Exits global configuration mode and returns you to EXEC mode.
Step 4	switch# show aaa authentication login error-enable	(Optional) Displays the login failure message configuration.
Step 5	switch# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

This example shows how to enable login authentication failure messages:

```

switch# configure terminal
switch(config)# aaa authentication login error-enable
switch(config)# exit
switch# show aaa authentication login error-enable
enabled

```

Verifying the AAA Configuration

Use the following commands to verify the configuration:

Command	Purpose
show aaa authentication [login {error-enable mschap}]	Displays AAA authentication information.

Command	Purpose
show aaa groups	Displays the AAA server group configuration.
show running-config aaa [all]	Displays the AAA configuration in the running configuration.
show startup-config aaa	Displays the AAA configuration in the startup configuration.

Example: show aaa authentication

```
switch# show aaa authentication login error-enable
disabled
switch#
```

Example: show running config aaa

```
switch# show running-config aaa all
version 4.0(1)
aaa authentication login default local
aaa accounting default local
no aaa authentication login error-enable
no aaa authentication login mschap enable
no radius-server directed-request
no snmp-server enable traps aaa server-state-change
no tacacs-server directed-request
switch#
```

Example: show startup-config aaa

```
switch# show startup-config aaa
version 4.0(1)
```

Configuration Examples for AAA

The following is an AAA configuration example:

```
aaa authentication login default group tacacs
aaa authentication login console group tacacs
```

Feature History for AAA

This table includes only the updates for those releases that have resulted in additions or changes to the feature.

Feature Name	Releases	Feature Information
AAA	4.0(4)SV1(1)	This feature was introduced.

