



Authentication Commands

This chapter describes the commands used to configure both AAA and non-AAA authentication methods. Authentication identifies users before they are allowed access to the network and network services. Basically, the Cisco IOS software implementation of authentication is divided into two main categories:

- AAA Authentication Methods
- Non-AAA Authentication Methods

Authentication, for the most part, is implemented through the AAA security services. We recommend that, whenever possible, AAA be used to implement authentication.

For information on how to configure authentication using either AAA or non-AAA methods, refer to the “Configuring Authentication” chapter in the *Security Configuration Guide*. For configuration examples using the commands in this chapter, refer to the “Authentication Configuration Examples” section located at the end of the “Configuring Authentication” chapter in the *Security Configuration Guide*.

aaa authentication arap

To enable an AAA authentication method for AppleTalk Remote Access (ARA) users using TACACS+, use the **aaa authentication arap** global configuration command. Use the **no** form of this command to disable this authentication.

```
aaa authentication arap {default | list-name} method1 [method2...]  
no aaa authentication arap {default | list-name} method1 [method2...]
```

Syntax Description

default	Uses the listed methods that follow this argument as the default list of methods when a user logs in.
<i>list-name</i>	Character string used to name the following list of authentication methods tried when a user logs in.
<i>method</i>	One of the keywords described in Table 1.

Default

If the **default** list is not set, only the local user database is checked. This has the same effect as the following command:

```
aaa authentication arap default local
```

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.3.

The list names and default that you set with the **aaa authentication arap** command are used with the **arap authentication** command. Note that ARAP guest logins are disabled by default when you enable AAA. To allow guest logins, you must use either the **guest** or **auth-guest** method listed in Table 1. You can only use one of these methods; they are mutually exclusive.

Create a list by entering the **aaa authentication arap list-name method** command, where *list-name* is any character string used to name this list (such as *MIS-access*.) The *method* argument identifies the list of methods the authentication algorithm tries in the given sequence. See Table 1 for descriptions of method keywords.

To create a default list that is used if no list is specified in the **arap authentication** command, use the **default** keyword followed by the methods you want to be used in default situations.

The additional methods of authentication are used only if the previous method returns an error, not if it fails.

Use the **show running-config** command to view lists of authentication methods.

Table 1 **AAA Authentication ARAP Methods**

Keyword	Description
guest	Allows guest logins. This method must be the first method listed, but it can be followed by other methods if it does not succeed.
auth-guest	Allows guest logins only if the user has already logged in to EXEC. This method must be the first method listed, but can be followed by other methods if it does not succeed.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
tacacs+	Uses TACACS+ authentication.

Note This command cannot be used with TACACS or extended TACACS.

Examples

The following example creates a list called *MIS-access*, which first tries TACACS+ authentication and then none:

```
aaa authentication arap MIS-access tacacs+ none
```

The following example creates the same list, but sets it as the default list that is used for all ARA protocol authentications if no other list is specified:

```
aaa authentication arap default tacacs+ none
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

aaa authentication local-override

aaa new-model

aaa authentication enable default

To enable AAA authentication to determine if a user can access the privileged command level, use the **aaa authentication enable default** global configuration command. Use the **no** form of this command to disable this authorization method.

```
aaa authentication enable default method1 [method2...]  
no aaa authentication enable default method1 [method2...]
```

Syntax Description

method At least one of the keywords described in Table 2.

Default

If the **default** list is not set, only the enable password is checked. This has the same effect as the following command:

```
aaa authentication enable default enable
```

On the console, the enable password is used if it exists. If no password is set, the process will succeed anyway.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.3.

Use the **aaa authentication enable default** command to create a series of authentication methods that are used to determine whether a user can access the privileged command level. Method keywords are described in Table 2. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all methods return an error, specify **none** as the final method in the command line.

If a default authentication routine is not set for a function, the default is **none** and no authentication is performed. Use the **show running-config** command to view currently configured lists of authentication methods.

Table 2 AAA Authentication Enable Default Methods

Keyword	Description
enable	Uses the enable password for authentication.
line	Uses the line password for authentication.
none	Uses no authentication.
tacacs+	Uses TACACS+ authentication.
radius	Uses RADIUS authentication.

Note This command cannot be used with TACACS or extended TACACS.

Example

The following example creates an authentication list that first tries to contact a TACACS+ server. If no server can be found, AAA tries to use the enable password. If this attempt also returns an error (because no enable password is configured on the server), the user is allowed access with no authentication.

```
aaa authentication enable default tacacs+ enable none
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

aaa authentication local-override

aaa authorization

aaa new-model

enable password

aaa authentication local-override

To configure the Cisco IOS software to check the local user database for authentication before attempting another form of authentication, use the **aaa authentication local-override** global configuration command. Use the **no** form of this command to disable the override.

```
aaa authentication local-override  
no aaa authentication local-override
```

Syntax Description

This command has no arguments or keywords.

Default

Override is disabled.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.3.

This command is useful when you want to configure an override to the normal authentication process for certain personnel such as system administrators.

When this override is set, the user is always prompted for the username. The system then checks to see if the entered username corresponds to a local account. If the username does not correspond to one in the local database, login proceeds with the methods configured with other **aaa** commands (such as **aaa authentication login**). Note that when using this command the Username: prompt is fixed as the first prompt.

Example

The following example enables AAA authentication override:

```
aaa authentication local-override
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

```
aaa authentication arap  
aaa authentication enable default  
aaa authentication login  
aaa authentication ppp  
aaa new-model
```

aaa authentication login

To set AAA authentication at login, use the **aaa authentication login** global configuration command. Use the **no** form of this command to disable AAA authentication.

```
aaa authentication login { default | list-name } method1 [method2...]  
no aaa authentication login { default | list-name } method1 [method2...]
```

Syntax Description

default	Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.
<i>list-name</i>	Character string used to name the following list of authentication methods activated when a user logs in.
<i>method</i>	At least one of the keywords described in Table 3.

Default

If the **default** list is not set, only the local user database is checked. This has the same effect as the following command:

```
aaa authentication login default local
```

Note On the console, login will succeed without any authentication checks if **default** is not set.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.3.

The default and optional list names that you create with the **aaa authentication login** command are used with the **login authentication** command.

Create a list by entering the **aaa authentication list-name method** command for a particular protocol, where *list-name* is any character string used to name this list (such as *MIS-access*). The *method* argument identifies the list of methods that the authentication algorithm tries, in the given sequence. Method keywords are described in Table 3.

To create a default list that is used if no list is assigned to a line, use the **login authentication** command with the default argument followed by the methods you want to use in default situations.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line.

If authentication is not specifically set for a line, the default is to deny access and no authentication is performed. Use the **show running-config** command to display currently configured lists of authentication methods.

Table 3 AAA Authentication Login Methods

Keyword	Description
enable	Uses the enable password for authentication.
krb5	Uses Kerberos 5 for authentication.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
none	Uses no authentication.
radius	Uses RADIUS authentication.
tacacs+	Uses TACACS+ authentication.
krb5-telnet	Uses Kerberos 5 Telnet authentication protocol when using Telnet to connect to the router.

Note This command cannot be used with TACACS or extended TACACS.

Examples

The following example creates an AAA authentication list called *MIS-access*. This authentication first tries to contact a TACACS+ server. If no server is found, TACACS+ returns an error and AAA tries to use the enable password. If this attempt also returns an error (because no enable password is configured on the server), the user is allowed access with no authentication.

```
aaa authentication login MIS-access tacacs+ enable none
```

The following example creates the same list, but it sets it as the default list that is used for all login authentications if no other list is specified:

```
aaa authentication login default tacacs+ enable none
```

The following example sets authentication at login to use the Kerberos 5 Telnet authentication protocol when using Telnet to connect to the router:

```
aaa authentication login default KRB5-TELNET krb5
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

aaa authentication local-override

aaa new-model

login authentication

aaa authentication nasi

To specify AAA authentication for Netware Asynchronous Services Interface (NASI) clients connecting through the access server, use the **aaa authentication nasi** global configuration command. Use the **no** form of this command to disable authentication for NASI clients.

```
aaa authentication nasi {default | list-name} method1 [method2...]  
no aaa authentication nasi {default | list-name} method1 [method2...]
```

Syntax Description

default	Makes the listed authentication methods that follow this argument the default list of methods used when a user logs in.
<i>list-name</i>	Character string used to name the following list of authentication methods activated when a user logs in.
<i>methods</i>	At least one of the methods described in Table 4.

Default

If the **default** list is not set, only the local user database is selected. This has the same effect as the following command:

```
aaa authentication nasi default local
```

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

The default and optional list names that you create with the **aaa authentication nasi** command are used with the **nasi authentication** command.

Create a list by entering the **aaa authentication nasi** command, where *list-name* is any character string that names this list (such as *MIS-access*). The *method* argument identifies the list of methods the authentication algorithm tries in the given sequence. Method keywords are described in Table 4.

To create a default list that is used if no list is assigned to a line with the **nasi authentication** command, use the default argument followed by the methods that you want to use in default situations.

The remaining methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line.

If authentication is not specifically set for a line, the default is to deny access and no authentication is performed. Use the **show running-config** command to display currently configured lists of authentication methods.

Table 4 AAA Authentication NASI Methods

Keyword	Description
enable	Uses the enable password for authentication.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
none	Uses no authentication.
tacacs+	Uses TACACS+ authentication.

Note This command cannot be used with TACACS or Extended TACACS.

Examples

The following example creates an AAA authentication list called *list1*. This authentication first tries to contact a TACACS+ server. If no server is found, TACACS+ returns an error and AAA tries to use the enable password. If this attempt also returns an error (because no enable password is configured on the server), the user is allowed access with no authentication.

```
aaa authentication nasi list1 tacacs+ enable none
```

The following example creates the same list, but sets it as the default list that is used for all login authentications if no other list is specified:

```
aaa authentication nasi default tacacs+ enable none
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ipx nasi-server enable
login authentication
show ipx nasi connections
show ipx spx-protocol

aaa authentication password-prompt

To change the text displayed when users are prompted for a password, use the **aaa authentication password-prompt** global configuration command. Use the **no** form of this command to return to the default password prompt text.

```
aaa authentication password-prompt text-string  
no aaa authentication password-prompt text-string
```

Syntax Description

<i>text-string</i>	String of text that will be displayed when the user is prompted to enter a password. If this text-string contains spaces or unusual characters, it must be enclosed in double-quotes (for example, "Enter your password:").
--------------------	---

Default

This command is disabled by default.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

Use the **aaa authentication password-prompt** command to change the default text that the Cisco IOS software displays when prompting a user to enter a password. This command changes the password prompt for the enable password as well as for login passwords that are not supplied by remote security servers. The **no** form of this command returns the password prompt to the default value:

```
Password:
```

The **aaa authentication password-prompt** command does not change any dialog that is supplied by a remote TACACS+ server.

The **aaa authentication password-prompt** command works when using RADIUS as the login method. You will be able to see the password prompt defined in the command shown even when the RADIUS server is unreachable. The **aaa authentication password-prompt** command does not work with TACACS+. TACACS+ supplies the NAS the password prompt to display to the users. If the TACACS+ server is reachable, the NAS gets the password prompt from the server and uses that prompt instead of the one defined in the **aaa authentication password-prompt** command. If the TACACS+ server is not reachable, the password prompt defined in the **aaa authentication password-prompt** command may be used.

Example

The following example changes the text for the password prompt:

```
aaa authentication password-prompt "Enter your password now:"
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

aaa authentication username-prompt

aaa new-model

enable password

aaa authentication ppp

To specify one or more AAA authentication methods for use on serial interfaces running Point-to-Point Protocol (PPP), use the **aaa authentication ppp** global configuration command. Use the **no** form of this command to disable authentication.

```
aaa authentication ppp {default | list-name} method1 [method2...]
no aaa authentication ppp {default | list-name} method1 [method2...]
```

Syntax Description

default	Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.
<i>list-name</i>	Character string used to name the following list of authentication methods tried when a user logs in.
<i>method</i>	At least one of the keywords described in Table 5.

Default

If the **default** list is not set, only the local user database is checked. This has the same effect as the following command:

```
aaa authentication ppp default local
```

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.3.

The lists that you create with the **aaa authentication ppp** command are used with the **ppp authentication** command. These lists contain up to four authentication methods that are used when a user tries to log in to the serial interface.

Create a list by entering the **aaa authentication ppp** *list-name* *method* command, where *list-name* is any character string used to name this list (such as *MIS-access*). The *method* argument identifies the list of methods that the authentication algorithm tries in the given sequence. You can enter up to four methods. Method keywords are described in Table 5.

The additional methods of authentication are only used if the previous method returns an error, not if it fails. Specify **none** as the final method in the command line to have authentication succeed even if all methods return an error.

If authentication is not specifically set for a function, the default is **none** and no authentication is performed. Use the **show running-config** command to display lists of authentication methods.

Table 5 AAA Authentication PPP Methods

Keyword	Description
if-needed	Does not authenticate if user has already been authenticated on a TTY line.
krb5	Uses Kerberos 5 for authentication (can only be used for PAP authentication).
local	Uses the local username database for authentication.
none	Uses no authentication.
radius	Uses RADIUS authentication.
tacacs+	Uses TACACS+ authentication.

Note This command cannot be used with TACACS or Extended TACACS.

Example

The following example creates an AAA authentication list called *MIS-access* for serial lines that use PPP. This authentication first tries to contact a TACACS+ server. If this action returns an error, the user is allowed access with no authentication.

```
aaa authentication ppp MIS-access tacacs+ none
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

aaa authentication local-override

aaa new-model

ppp authentication

aaa authentication username-prompt

To change the text displayed when users are prompted to enter a username, use the **aaa authentication username-prompt** global configuration command. Use the **no** form of this command to return to the default username prompt text.

```
aaa authentication username-prompt text-string  
no aaa authentication username-prompt text-string
```

Syntax Description

<i>text-string</i>	String of text that will be displayed when the user is prompted to enter a username. If this text-string contains spaces or unusual characters, it must be enclosed in double-quotes (for example, "Enter your name:").
--------------------	---

Default

There is no user-defined *text-string*, and the username prompt appears as "Username."

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

Use the **aaa authentication username-prompt** command to change the default text that the Cisco IOS software displays when prompting a user to enter a username. The **no** form of this command returns the username prompt to the default value:

```
Username:
```

Some protocols (for example, TACACS+) have the ability to override the use of local username prompt information. Using the **aaa authentication username-prompt** command will not change the username prompt text in these instances.

Note The **aaa authentication username-prompt** command does not change any dialog that is supplied by a remote TACACS+ server.

Example

The following example changes the text for the username prompt:

```
aaa authentication username-prompt "Enter your name here:"
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

```
aaa authentication password-prompt  
aaa new-model  
enable password
```

aaa new-model

To enable the AAA access control model, issue the **aaa new-model** global configuration command. Use the **no** form of this command to disable this functionality.

aaa new-model
no aaa new-model

Syntax Description

This command has no arguments or keywords.

Default

AAA is not enabled.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

This command enables the AAA access control system. After you have enabled AAA, TACACS and Extended TACACS commands are no longer available. If you initialize AAA functionality and later decide to use TACACS or Extended TACACS, issue the **no** version of this command, and then enable the version of TACACS that you want to use.

Example

The following example initializes AAA:

```
aaa new-model
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

aaa accounting
aaa authentication arap
aaa authentication enable default
aaa authentication local-override
aaa authentication login
aaa authentication ppp
aaa authorization
tacacs-server key

access-profile

To apply your per-user authorization attributes to an interface during a PPP session, use the **access-profile EXEC** command. Use the default form of the command (no keywords) to cause existing access control lists (ACLs) to be removed, and ACLs defined in your per-user configuration to be installed. Refer to the “Usage Guidelines” section that follows to learn what each form of the command specifically accomplishes.

access-profile [**merge** | **replace**] [**ignore-sanity-checks**]

Syntax Description

- | | |
|-----------------------------|---|
| merge | <p>(Optional) Like the default form of the command, this option removes existing ACLs while retaining other existing authorization attributes for the interface.</p> <p>However, using this option also installs per-user authorization attributes in addition to the existing attributes. (The default form of the command installs only new ACLs.) The per-user authorization attributes come from all AV pairs defined in the AAA per-user configuration (the user’s authorization profile).</p> <p>The interface’s resulting authorization attributes are a combination of the previous and new configurations.</p> |
| replace | <p>(Optional) This option removes existing ACLs <i>and</i> all other existing authorization attributes for the interface.</p> <p>A complete new authorization configuration is then installed, using all AV pairs defined in the AAA per-user configuration.</p> <p>This option is not normally recommended because it initially deletes <i>all</i> existing configuration, including static routes. This could be detrimental if the new user profile does not reinstall appropriate static routes and other critical information.</p> |
| ignore-sanity-checks | <p>(Optional) Enables you to use any AV pairs, whether or not they are valid.</p> |

Command Mode

User EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2 F.

Remote users can use this command to activate Double Authentication for a PPP session. Double Authentication must be correctly configured for this command to have the desired effect.

You should use this command when you are a remote user and are establishing a PPP link to gain local network access.

After you have been authenticated with CHAP (or PAP), you will have limited authorization. To activate Double Authentication and gain your appropriate user network authorization, you must Telnet to the NAS and execute the **access-profile** command. (This command could also be set up as an autocommand, which would eliminate the need to manually enter the command.)

This command causes all subsequent network authorizations to be made in *your* username, instead of in the remote *host*'s username.

Any changes to the interface caused by this command will stay in effect for as long as the interface stays up. These changes will be removed when the interface goes down. This command does not affect the normal operation of the router or the interface.

The default form of the command, **access-profile**, causes existing ACLs to be unconfigured (removed), and new ACLs to be installed. The new ACLs come from your per-user configuration on an AAA server (such as a TACACS+ server). The ACL replacement constitutes a reauthorization of your network privileges.

The default form of the command can fail if your per-user configuration contains statements other than ACL AV pairs. Any protocols with non-ACL statements will be deconfigured, and no traffic for that protocol can pass over the PPP link.

The **access-profile merge** form of the command causes existing ACLs to be unconfigured (removed) and new authorization information (including new ACLs) to be added to the interface. This new authorization information consists of your complete per-user configuration on an AAA server. If any of the new authorization statements conflict with existing statements, the new statements could “override” the old statements or be ignored, depending on the statement and applicable parser rules. The resulting interface configuration is a combination of the original configuration and the newly installed per-user configuration.



Caution The new user authorization profile (per-user configuration) must *not* contain any invalid mandatory AV pairs, otherwise the command will fail and the PPP protocol (containing the invalid pair) will be dropped. If invalid AV pairs are included as *optional* in the user profile, the command will succeed, but the invalid AV pair will be ignored. Invalid AV pair types are listed later in this section.

The **access-profile replace** form of the command causes the entire existing authorization configuration to be removed from the interface, and the complete per-user authorization configuration to be added. This per-user authorization consists of your complete per-user configuration on an AAA server. The caution of the previous paragraph applies.



Caution Use extreme caution when using the **access-profile replace** form of the command. It might have detrimental and unexpected results, because this option deletes *all* authorization configuration information (including static routes) before reinstalling the new authorization configuration.

Invalid AV pair types:

- addr
- addr-pool
- zonelist
- tunnel-id
- ip-addresses
- x25-addresses

- frame-relay
- source-ip

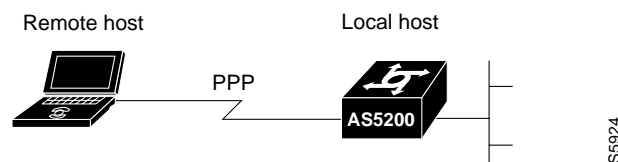
Note These AV pair types are only “invalid” when used with Double Authentication, in the user-specific authorization profile—they cause the **access-profile** command to fail. However, these AV pair types can be appropriate when used in other contexts.

Example

This example activates Double Authentication for a remote user. This example assumes that the **access-profile** command was *not* configured as an autocommand.

The remote user connects to the corporate headquarters network per Figure 2.

Figure 2 Network Topology for Activating Double Authentication (Example)



The remote user runs a terminal emulation application to Telnet to the corporate NAS, an AS5200 local host named “hqnas.” The remote user, named Bob, has the username “BobUser.”

This example replaces ACLs on the local host PPP interface. The ACLs previously applied to the interface during PPP authorization are replaced with ACLs defined in the per-user configuration AV pairs.

The remote user Telnets to the local host and logs in:

```

login: BobUser
Password: <welcome>
hqnas> access-profile
  
```

Bob is reauthenticated when he logs in to hqnas, because hqnas is configured for login AAA authentication using the corporate RADIUS server. When Bob enters the **access-profile** command, he is reauthorized with his per-user configuration privileges. This causes the access lists and filters in his per-user configuration to be applied to the NAS interface.

After the reauthorization is complete, Bob is automatically logged out of the AS5200 local host.

Related Commands

You can use the master indexes or search online to find documentation of related commands.

connect
telnet

arap authentication

To enable AAA authentication for ARA on a line, use the **arap authentication** line configuration command. Use the **no** form of the command to disable authentication for an ARA line.

arap authentication { **default** | *list-name* } [**one-time**]
no arap authentication { **default** | *list-name* }



Caution If you use a *list-name* value that was not configured with the **aaa authentication arap** command, ARA protocol will be disabled on this line.

Syntax Description

default	Default list created with the aaa authentication arap command.
<i>list-name</i>	Indicated list created with the aaa authentication arap command.
one-time	(Optional) Accepts the username and password in the username field.

Default

ARA protocol authentication uses the default set with **aaa authentication arap** command. If no default is set, the local user database is checked.

Command Mode

Line configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

This command is a per-line command that specifies the name of a list of AAA authentication methods to try at login. If no list is specified, the default list is used (whether or not it is specified in the command line). You create defaults and lists with the **aaa authentication arap** command. Entering the **no** version of **arap authentication** has the same effect as entering the command with the **default** argument.

Before issuing this command, create a list of authentication processes by using the **aaa authentication arap** global configuration command.

Example

The following example specifies that the TACACS+ authentication list called *MIS-access* is used on ARA line 7:

```
line 7
 arap authentication MIS-access
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

aaa authentication arap

login authentication

To enable AAA authentication for logins, use the **login authentication** line configuration command. Use the **no** form of this command to either disable TACACS+ authentication for logins or to return to the default.

```
login authentication { default | list-name }  
no login authentication { default | list-name }
```

Syntax Description

default	Uses the default list created with the aaa authentication login command.
<i>list-name</i>	Uses the indicated list created with the aaa authentication login command.

Default

Uses the default set with **aaa authentication login**.

Command Mode

Line configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.3.

This command is a per-line command used with AAA that specifies the name of a list of AAA authentication methods to try at login. If no list is specified, the default list is used (whether or not it is specified in the command line).



Caution If you use a *list-name* value that was not configured with the **aaa authentication login** command, you will disable login on this line.

Entering the **no** version of **login authentication** has the same effect as entering the command with the **default** argument.

Before issuing this command, create a list of authentication processes by using the global configuration **aaa authentication login** command.

Examples

The following example specifies that the default AAA authentication is to be used on line 4:

```
line 4  
login authentication default
```

The following example specifies that the AAA authentication list called *list1* is to be used on line 7:

```
line 7
 login authentication list1
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

aaa authentication login

login tacacs

To configure your router to use TACACS user authentication, use the **login tacacs** line configuration command. Use the **no** form of this command to disable TACACS user authentication for a line.

login tacacs
no login tacacs

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Line configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

You can use TACACS security if you have configured a TACACS server and you have a command control language (CCL) script that allows you to use TACACS security. For information about using files provided by Cisco Systems to modify CCL scripts to support TACACS user authentication, refer to the “Configuring AppleTalk Remote Access” chapter in the *Dial Solutions Configuration Guide*.

Note This command cannot be used with AAA. Use the **login authentication** command instead.

Example

In the following example, lines 1 through 16 are configured for TACACS user authentication:

```
line 1 16
 login tacacs
```

nasi authentication

To enable AAA authentication for NetWare Asynchronous Services Interface (NASI) clients connecting to a router, use the **nasi authentication** line configuration command. Use the **no** form of the command to return to the default, as specified by the **aaa authentication nasi** command.

```
nasi authentication { default | list-name }  
no login authentication { default | list-name }
```

Syntax Description

default Uses the default list created with the **aaa authentication nasi** command.

list-name Uses the list created with the **aaa authentication nasi** command.

Default

Uses the default set with the **aaa authentication nasi** command.

Command Mode

Line configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

This command is a per-line command used with AAA authentication that specifies the name of a list of authentication methods to try at login. If no list is specified, the default list is used, even if it is specified in the command line. (You create defaults and lists with the **aaa authentication nasi** command.) Entering the **no** form of this command has the same effect as entering the command with the **default** argument.



Caution If you use a *list-name* value that was not configured with the **aaa authentication nasi** command, you will disable login on this line.

Before issuing this command, create a list of authentication processes by using the **aaa authentication nasi** global configuration command.

Examples

The following example specifies that the default AAA authentication be used on line 4:

```
line 4  
nasi authentication default
```

The following example specifies that the AAA authentication list called *list1* be used on line 7:

```
line 7  
nasi authentication list1
```


Related Commands

You can use the master indexes or search online to find documentation of related commands.

aaa authentication nasi

ipx nasi-server enable

show ipx nasi connections

show ipx spx-protocol

ppp authentication

To enable CHAP or PAP or both and to specify the order in which CHAP and PAP authentication are selected on the interface, use the **ppp authentication** interface configuration command. Use the **no** form of this command to disable this authentication.

```
ppp authentication {chap | chap pap | pap chap | pap} [if-needed] [list-name | default]
[callin] [one-time]
no ppp authentication
```

Syntax Description

chap	Enables CHAP on a serial interface.
pap	Enables PAP on a serial interface.
chap pap	Enables both CHAP and PAP, and performs CHAP authentication before PAP.
pap chap	Enables both CHAP and PAP, and performs PAP authentication before CHAP.
if-needed	(Optional) Used with TACACS and extended TACACS. Does not perform CHAP or PAP authentication if the user has already provided authentication. This option is available only on asynchronous interfaces.
<i>list-name</i>	(Optional) Used with AAA. Specifies the name of a list of methods of authentication to use. If no list name is specified, the system uses the default. The list is created with the aaa authentication ppp command.
default	The name of the method list is created with the aaa authentication ppp command.
callin	Specifies authentication on incoming (received) calls only.
one-time	(Optional) Accepts the username and password in the username field.



Caution If you use a *list-name* value that was not configured with the **aaa authentication ppp** command, you will disable PPP on this interface.

Default

PPP authentication is not enabled.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

When you enable CHAP or PAP authentication (or both), the local router requires the remote device to prove its identity before allowing data traffic to flow. PAP authentication requires the remote device to send a name and a password, which is checked against a matching entry in the local username database or in the remote security server database. CHAP authentication sends a Challenge to the remote device. The remote device encrypts the challenge value with a shared secret

and returns the encrypted value and its name to the local router in a Response message. The local router attempts to match the remote device's name with an associated secret stored in the local username or remote security server database; it uses the stored secret to encrypt the original challenge and verify that the encrypted values match.

You can enable PAP or CHAP (or both) in either order. If you enable both methods, the first method specified is requested during link negotiation. If the peer suggests using the second method, or refuses the first method, the second method is tried. Some remote devices support only CHAP and some support only PAP. Base the order in which you specify methods on the remote device's ability to correctly negotiate the appropriate method, and on the level of data line security you require. PAP usernames and passwords are sent as clear text strings, which can be intercepted and reused. CHAP has eliminated most of the known security holes.

Enabling or disabling PPP authentication does not affect the local router's willingness to authenticate itself to the remote device.

If you are using autoselect on a TTY line, you probably want to use the `ppp authentication` command to turn on PPP authentication for the corresponding interface.

Example

The following example enables CHAP on asynchronous interface 4 and uses the authentication list MIS-access:

```
interface async 4
 encapsulation ppp
 ppp authentication chap MIS-access
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

aaa authentication ppp

aaa new-model

autoselect

encapsulation ppp

ppp-use-tacacs

username

ppp chap hostname

To create a pool of dialup routers that all appear to be the same host when authenticating with CHAP, use the **ppp chap hostname** interface configuration command. To disable this function, use the **no** form of the command.

```
ppp chap hostname hostname  
no ppp chap hostname hostname
```

Syntax Description

hostname The name sent in the CHAP challenge.

Default

Disabled. The router name is sent in any CHAP challenges.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

Currently, a router dialing a pool of access routers requires a username entry for each possible router in the pool because each router challenges with its hostname. If a router is added to the dialup rotary pool, all connecting routers must be updated. The **ppp chap hostname** command allows you to specify a common alias for all routers in a rotary group to use so that only one username must be configured on the dialing routers.

This command is normally used with local CHAP authentication (when the router authenticates to the peer), but it can also be used for remote CHAP authentication.

Example

The commands in the following example identify dialer interface 0 as the dialer rotary group leader and specifies ppp as the encapsulation method used by all member interfaces. This example shows that CHAP authentication is used on received calls only and the username *ISPCorp* will be sent in all CHAP challenges and responses:

```
interface dialer 0  
  encapsulation ppp  
  ppp authentication chap callin  
  ppp chap hostname ISPCorp
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

```
aaa authentication ppp  
ppp authentication  
ppp chap password  
ppp chap refuse  
ppp chap wait
```

ppp chap password

To enable a router calling a collection of routers that do not support this command (such as routers running older Cisco IOS software images) to configure a common CHAP secret password to use in response to challenges from an unknown peer, use the **ppp chap password** interface configuration command. To disable this function, use the **no** form of this command.

```
ppp chap password secret  
no ppp chap password secret
```

Syntax Description

<i>secret</i>	The secret used to compute the response value for any CHAP challenge from an unknown peer.
---------------	--

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

This command allows you to replace several username and password configuration commands with a single copy of this command on any dialer interface or asynchronous group interface.

This command is used for remote CHAP authentication only (when routers authenticate to the peer) and does not affect local CHAP authentication.

Example

The commands in the following example specify ISDN Basic Rate Interface (BRI) number 0. The method of encapsulation on the interface is PPP. If a CHAP challenge is received from a peer whose name is not found in the global list of usernames, the encrypted secret 7 1267234591 is decrypted and used to create a CHAP response value.

```
interface bri 0  
  encapsulation ppp  
  ppp chap password 7 1234567891
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

aaa authentication ppp
ppp authentication
ppp chap hostname
ppp chap refuse
ppp chap wait

ppp chap refuse

To refuse CHAP authentication from peers requesting it, use the **ppp chap refuse** interface configuration command. To disable this function, use the **no** form of this command.

ppp chap refuse [callin]
no ppp chap refuse [callin]

Syntax Description

callin (Optional) This keyword specifies that the router will refuse to answer CHAP authentication challenges received from the peer, but will still require the peer to answer any CHAP challenges the router sends.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.3.

This command specifies that CHAP authentication is disabled for all calls, meaning that all attempts by the peer to force the user to authenticate using CHAP will be refused. If the **callin** keyword is used, CHAP authentication is disabled for incoming calls from the peer, but will still be performed on outgoing calls to the peer.

If outbound PAP has been enabled (using the **ppp pap sent-username** command), PAP will be suggested as the authentication method in the refusal packet.

Example

The commands in the following example specify ISDN Basic Rate Interface (BRI) number 0. The method of encapsulation on the interface is PPP. This example disables CHAP authentication from occurring if a peer calls in requesting CHAP authentication:

```
interface bri 0
 encapsulation ppp
 ppp chap refuse
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

aaa authentication ppp
ppp authentication
ppp chap hostname
ppp chap password
ppp chap wait

ppp chap wait

To specify that the router will not authenticate to a peer requesting CHAP authentication until after the peer has authenticated itself to the router, use the **ppp chap wait** interface configuration command. To disable this function, use the **no** form of this command.

```
ppp chap wait secret  
no ppp chap wait secret
```

Syntax Description

secret The secret used to compute the response value for any CHAP challenge from an unknown peer.

Default

Enabled

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.3.

This command (which is the default) specifies that the router will not authenticate to a peer requesting CHAP authentication until the peer has authenticated itself to the router. The **no** form of this command specifies that the router will respond immediately to an authentication challenge.

Example

The commands in the following example specify ISDN Basic Rate Interface (BRI) number 0. The method of encapsulation on the interface is PPP. This example disables the default, meaning that users do not have to wait for peers to complete CHAP authentication before authenticating themselves:

```
interface bri 0  
  encapsulation ppp  
  no ppp chap wait
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

```
aaa authentication ppp  
ppp authentication  
ppp chap hostname  
ppp chap password  
ppp chap refuse
```

ppp pap sent-username

To reenable remote PAP support for an interface and use the **sent-username** and **password** in the PAP authentication request packet to the peer, use the **ppp pap sent-username** interface configuration command. Use the **no** form of this command to disable remote PAP support.

ppp pap sent-username *username* **password** *password*
no ppp pap sent-username

Syntax Description

<i>username</i>	Username sent in the PAP authentication request.
password	Password sent in the PAP authentication request.
<i>password</i>	Must contain from 1 to 25 uppercase and lowercase alphanumeric characters.

Default

Remote PAP support disabled.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

Use this command to reenable remote PAP support (for example to respond to the peer's request to authenticate with PAP) and to specify the parameters to be used when sending the PAP Authentication Request.

This is a per-interface command. You must configure this command for each interface.

Example

The commands in the following example identify dialer interface 0 as the dialer rotary group leader and specify PPP as the method of encapsulation used by the interface. Authentication is by CHAP or PAP on received calls only. *ISPCorp* is the username sent to the peer if the peer requires the router to authenticate with PAP.

```
interface dialer0
 encapsulation ppp
 ppp authentication chap pap callin
 ppp chap hostname ISPCorp
 ppp pap sent username ISPCorp password 7 fjhfeu
 ppp pap sent-username ISPCorp password 7 1123659238
```


Related Commands

You can use the master indexes or search online to find documentation of related commands.

aaa authentication ppp

ppp authentication

ppp chap hostname

ppp chap password

ppp use-tacacs

ppp use-tacacs

To enable TACACS for PPP authentication, use the **ppp use-tacacs** interface configuration command. Use the **no** form of the command to disable TACACS for PPP authentication.

ppp use-tacacs [single-line]
no ppp use-tacacs

Note This command is not used in TACACS+. It has been replaced with the **aaa authentication ppp** command.

Syntax Description

single-line (Optional) Accept the username and password in the username field. This option applies only when using CHAP authentication.

Default

TACACS is not used for PPP authentication.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.3.

This is a per-interface command. Use this command only when you have set up an extended TACACS server.

When CHAP authentication is being used, the **ppp use-tacacs** command with the **single-line** option specifies that if a username and password are specified in the username, separated by an asterisk (*), a standard TACACS login query is performed using that username and password. If the username does not contain an asterisk, then normal CHAP authentication is performed.

This feature is useful when integrating TACACS with other authentication systems that require a clear text version of the user's password. Such systems include one-time password systems, token card systems, and Kerberos.



Caution Normal CHAP authentications prevent the clear text password from being transmitted over the link. When you use the single-line option, passwords cross the link as clear text.

If the username and password are contained in the CHAP password, the CHAP secret is not used by the Cisco IOS software. Because most PPP clients require that a secret be specified, you can use any arbitrary string, and the Cisco IOS software ignores it.

Examples

In the following example, asynchronous interface 1 is configured to use TACACS for CHAP authentication:

```
interface async 1
  ppp authentication chap
  ppp use-tacacs
```

In the following example, asynchronous interface 1 is configured to use TACACS for PAP authentication:

```
interface async 1
  ppp authentication pap
  ppp use-tacacs
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ppp authentication
tacacs-server extended
tacacs-server host

timeout login response

To specify how long the system will wait for login input (such as username and password) before timing out, use the **timeout login response** line configuration command. Use the **no** form of this command to set the timeout value to 0 seconds.

timeout login response *seconds*

timeout login response *seconds*

Syntax Description

<i>seconds</i>	Integer that determines the number of seconds the system will wait for login input before timing out. Available settings are from 1 to 300 seconds.
----------------	---

Default

The default login timeout value is 30 seconds.

Command Mode

Line configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

Example

The following example changes the login timeout value to 60 seconds:

```
line 10
  timeout login response 60
```