# AAA Double Authentication Secured by Absolute Timeout

**Last Updated: January 17, 2012**

The AAA Double Authentication Secured by Absolute Timeout feature allows you to secure the double authentication mechanism by protecting it with a per-user session timeout. This feature optimizes the connection to the network by service providers to only connections that are authorized, and it increases the security of the overall access to the network by ensuring that no unwanted sessions are connected.



## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

## Prerequisites for AAA Double Authentication Secured by Absolute Timeout


**Americas Headquarters:**
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

- You need access to a Cisco RADIUS or TACACS+ server and should be familiar with configuring RADIUS or TACACS+.
- You should be familiar with configuring authentication, authorization, and accounting (AAA).
- You should be familiar with enabling AAA automated double authentication.

# Restrictions for AAA Double Authentication Secured by Absolute Timeout

- The AAA Double Authentication Secured by Absolute Timeout feature, like the existing double authentication feature, is for PPP connections only. Automated double authentication cannot be used with other protocols, such as X.25 or Serial Line Internet Protocol (SLIP).
- There may be a minimal impact on performance if a TACACS+ server is used. However, there is no performance impact if a RADIUS server is used.

# Information About AAA Double Authentication Secured by Absolute Timeout



## AAA Double Authentication

With the current AAA double authentication mechanism, a user must pass the first authentication using a host username and password. The second authentication, after Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP), uses a login username and password. In the first authentication, a PPP session timeout will be applied to the virtual access interface if it is configured locally or remotely. The AAA Double Authentication Secured by Absolute Timeout feature allows you to secure the double authentication mechanism by protecting it with a per-user session timeout. The per-user timeout, which can be customized, supersedes the generic absolute timeout value. This method works on the same principle as per-user access control lists (ACLs) in double authentication.

# How to Apply AAA Double Authentication Secured by Absolute Timeout



## Applying AAA Double Authentication Secured by Absolute Timeout

To apply the absolute timeout, you need to configure “Session-Timeout” in the login user profile as a link control protocol (LCP) per-user attribute. There is no new or modified command-line interface (CLI) for this feature, but before you use the **access-profile** command when enabling AAA double authentication,

you must first reauthorize LCP per-user attributes (for example, Session-Timeout) and then reauthorize Network Control Protocols (NCPs) to apply other necessary criteria, such as ACLs and routes. See the Example for AAA Double Authentication Secured by Absolute Timeout.

**Note** Timeout configuration in a TACACS+ user profile is a little different from the configuration in a RADIUS user profile. In a RADIUS profile, only one “Session-Timeout” is configured, along with the autocommand “access-profile.” The timeout will be applied to the EXEC session and to the PPP session. In TACACS+, however, the timeout must be configured under the service types “exec” and “ppp” (LCP) to apply a timeout to the EXEC session and to the PPP session. If the timeout is configured only under the service type “ppp,” the timeout value is not available while doing an EXEC authorization--and the timeout will not be applied to the EXEC session.

# Verifying AAA Double Authentication Secured by Absolute Timeout

To verify that AAA double authentication has been secured by absolute timeout and to see information about various attributes associated with the authentication, perform the following steps. These **show** and **debug** commands can be used in any order.

**Note** When idle timeout is configured on a full virtual access interface and a subvirtual access interface, the **show users** command displays the idle time for both the interfaces. However, if the idle timeout is not configured on both interfaces, then the **show users** command will display the idle time for the full virtual access interface only.

or

**debug tacacs**

### SUMMARY STEPS

1. **enable**
2. **show users**
3. **show interfaces virtual-access** *number* [**configuration**]
4. **debug aaa authentication**
5. **debug aaa authorization**
6. **debug aaa per-user**
7. **debug ppp authentication**
8. Do one of the following:
   - **debug radius**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **show users**<br><br>**Example:**<br>**enable**<br><br>**Example:**<br>`Router# show users` | Displays information about the active lines on the router. |
| **Step 3** | **show interfaces virtual-access** *number* [**configuration**]<br><br>**Example:**<br>`Router# show interfaces virtual-access 2 configuration` | Displays status, traffic data, and configuration information about a specified virtual access interface. |
| **Step 4** | **debug aaa authentication**<br><br>**Example:**<br>`Router# debug aaa authentication` | Displays information about AAA TACACS+ authentication. |
| **Step 5** | **debug aaa authorization**<br><br>**Example:**<br>`Router# debug aaa authorization` | Displays information about AAA TACACS+ authorization. |
| **Step 6** | **debug aaa per-user**<br><br>**Example:**<br>`Router# debug aaa per-user` | Displays the attributes that are applied to each user as the user authenticates. |

| Command or Action | Purpose |
|---|---|
| **Step 7** **debug ppp authentication**<br><br>**Example:**<br>`Router# debug ppp authentication` | Displays whether a user is passing authentication. |
| **Step 8** Do one of the following:<br>• **debug radius**<br><br>**Example:**<br>`Router# debug radius`<br><br>**Example:**<br><br>**Example:**<br><br>**Example:**<br><br>**debug tacacs**<br><br>**Example:**<br>`Router# debug tacacs` | Displays information associated with the RADIUS server.<br>or<br>Displays information associated with the TACACS+ server. |

### Examples

The following sample output is from the **show users** command:

```
Router# show users
     Line       User        Host(s      Idle       Location
  *  0 con 0    aaapbx2     idle        00:00:00   aaacon2 10
     8 vty 0    broker_def  idle        00:00:08   192.168.1.8
     Interface  User            Mode        Idle       Peer Address
     Vi2        broker_default  VDP         00:00:01   192.168.1.8 <=========
     Se0:22     aaapbx2         Sync PPP    00:00:23
```

The following sample output is from the **show interfaces virtual-access** command:

```
Router# show interfaces virtual-access 2 configuration
Virtual-Access2 is a Virtual Profile (sub)interface
Derived configuration: 150 bytes
!
interface Virtual-Access2
```

```
  ip unnumbered Serial0:23
  no ip route-cache
  timeout absolute 3 0
! The above line shows that the per-user session timeout has been applied.
  ppp authentication chap
  ppp timeout idle 180000
! The above line shows that the absolute timeout has been applied.
```

# Examples for AAA Double Authentication Secured by Absolute Timeout



## RADIUS User Profile Example

The following sample output shows that a RADIUS user profile has been applied and that AAA double authentication has been secured by an absolute timeout:

```
aaapbx2 Password = "password1",
 Service-Type = Framed,
 Framed-Protocol = PPP,
 Session-Timeout = 180,
 Idle-Timeout = 180000,
 cisco-avpair = "ip:inacl#1=permit tcp any any eq telnet"
 cisco-avpair = "ip:inacl#2=permit icmp any any"
broker_default Password = "password1",
 Service-Type = Administrative,
 cisco-avpair = "shell:autocmd=access-profile",
 Session-Timeout = 360,
 cisco-avpair = "ip:inacl#1=permit tcp any any"
 cisco-avpair = "ip:inacl#2=permit icmp any any"
broker_merge Password = "password1",
 Service-Type = Administrative,
 cisco-avpair = "shell:autocmd=access-profile merge",
 Session-Timeout = 360,
 cisco-avpair = "ip:inacl#1=permit tcp any any"
 cisco-avpair = "ip:inacl#2=permit icmp any any"
 cisco-avpair = "ip:route#3=10.4.0.0 255.0.0.0"
 cisco-avpair = "ip:route#4=10.5.0.0 255.0.0.0"
 cisco-avpair = "ip:route#5=10.6.0.0 255.0.0.0"
broker_replace Password = "password1",
 Service-Type = Administrative,
 cisco-avpair = "shell:autocmd=access-profile replace",
 Session-Timeout = 360,
 cisco-avpair = "ip:inacl#1=permit tcp any any"
 cisco-avpair = "ip:inacl#2=permit icmp any any"
 cisco-avpair = "ip:route#3=10.4.0.0 255.0.0.0"
 cisco-avpair = "ip:route#4=10.5.0.0 255.0.0.0"
 cisco-avpair = "ip:route#5=10.6.0.0 255.0.0.0"
```

## TACACS User Profile Example

The following sample output shows that a TACACS+ user profile has been applied and that AAA double authentication has been secured by an absolute timeout.

### Remote Host

The following allows the remote host to be authenticated by the local host during first-stage authentication and provides the remote host authorization profile.

```
user = aaapbx2
 chap = cleartext Cisco
 pap = cleartext cisco
 login = cleartext cisco
 service = ppp protocol = lcp
  idletime = 3000
  timeout = 3
 service = ppp protocol = ip
  inacl#1="permit tcp any any eq telnet"
 service = ppp protocol = ipx
```

### access-profile Command Without Any Arguments

Using the **access-profile** command without any arguments causes the removal of any access lists that are found in the old configuration (both per-user and per-interface) and ensures that the new profile contains only access-list definitions.

```
user = broker_default
 login = cleartext Cisco
 chap = cleartext "cisco"
 service = exec
  autocmd = "access-profile"
! This is the autocommand that executes when broker_default logs in.
  timeout = 6
 service = ppp protocol = lcp
  timeout = 6
 service = ppp protocol = ip
! Put access lists, static routes, and other requirements that are
! needed here. Read the software specifications for details. If you leave
! this blank, the user will have no access lists (not even the ones that were
! installed prior to the creation of this user profile)!
  inacl#1="permit tcp any any"
  inacl#2="permit icmp host 10.0.0.0 any"
 service = ppp protocol = ipx
! Put access lists, static routes, and other requirements that are
! needed here. Read the software specifications for details. If you leave
! this blank, the user will have no access lists (not even the ones that were
! installed prior to the creation of this user profile)!
```

### access-profile Command with merge Keyword

With the “merge” option, all old access lists are removed (as before), but then almost any AV pair is allowed to be uploaded and installed. This merge will allow for the uploading of any custom static routes, Service Advertisement Protocol (SAP) filters, and other requirements that the user may need in his or her profile. This merge must be used with care because it leaves everything open in terms of conflicting configurations.

```
user = broker_merge
 login = cleartext Cisco
 chap = cleartext "cisco"
 service = exec
  autocmd = "access-profile merge"
! This is the autocommand that executes when broker_merge logs in.
  timeout = 6
 service = ppp protocol = lcp
 timeout = 6
 service = ppp protocol = ip
! Put access lists, static routes, and other requirements that are
! needed here. Read the software specifications for details. If you leave
! this blank, the user will have no access lists (not even the ones that were
! installed prior to the creation of this user profile)!
```

```
  route#1="10.4.0.0 255.0.0.0"
  route#2="10.5.0.0 255.0.0.0"
  route#3="10.6.0.0 255.0.0.0"
  inacl#5="permit tcp any any"
  inacl#6="permit icmp host 10.60.0.0 any"
 service = ppp protocol = ipx
! Put access lists, static routes, and other requirements that are
! needed here. Read the software specifications for details. If you leave
! this blank, the user will have no access lists (not even the ones that were
! installed prior to the creation of this user profile)!
```

### access-profile Command with the replace Keyword

If you use the **access-profile** command with the **replace** keyword, the command works as it does currently; that is, any old configuration is removed and any new configuration is installed.

**Note** When the **access-profile** command is configured, the new configuration is checked for address pools and address attribute-value (AV) pairs. Because addresses cannot be renegotiated at this point, the command will fail to work when it encounters such an address AV pair.

```
user = broker_replace
 login = cleartext Cisco
 chap = cleartext "cisco"
 service = exec
  autocmd = "access-profile replace"
! This is the autocommand that executes when broker_replace logs in.
  timeout = 6
 service = ppp protocol = lcp
  timeout = 6
 service = ppp protocol = ip
! Put access lists, static routes, and other requirements that are
! needed here. Read the software specifications for details. If you leave
! this blank, the user will have no access lists (not even the ones that were
! installed prior to the creation of this user profile)!
  route#1="10.7.0.0 255.0.0.0"
  route#2="10.8.0.0 255.0.0.0"
  route#3="10.9.0.0 255.0.0.0"
  inacl#4="permit tcp any any"
 service = ppp protocol = ipx
! Put access lists, static routes, and other requirements that are
! needed here. Read the software specifications for details. If you leave
! this blank, the user will have no access lists (not even the ones that were
! installed prior to the creation of this user profile)!
```

**Note** Timeout configuration in a TACACS+ user profile is a little different from the configuration in a RADIUS user profile. In a RADIUS profile, only one “Session-Timeout” is configured, along with the autocommand **access-profile**. The timeout will be applied to the EXEC session and to the PPP session. In TACACS+, however, the timeout must be configured under the service types “exec” and “ppp” (LCP) to apply a timeout to the EXEC session and to the PPP session. If the timeout is configured only under the service type “ppp,” the timeout value is not available while doing an EXEC authorization--and the timeout will not be applied to the EXEC session.

# Additional References

The following sections provide references related to AAA Double Authentication Secured by Absolute Timeout.

# Related Documents

| Related Topic | Document Title |
|---|---|
| AAA configuration | Configuring Accounting, Configuring Authorization" , and Configuring Authentication in the *Cisco IOS XE Security Configuration Guide: Securing User Services* , Release 2. |
| RADIUS configuration | Configuring RADIUS in the *Cisco IOS XE Security Configuration Guide: Securing User Services* , Release 2. |
| TACACS+ configuration | Configuring TACACS in the *Cisco IOS XE Security Configuration Guide: Securing User Services* , Release 2. |
| Security Commands | *Cisco IOS Security Command Reference* |

# Standards

| Standards | Title |
|---|---|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | -- |

# MIBs

| MIBs | MIBs Link |
|---|---|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

## RFCs

| RFCs | Title |
|---|---|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | -- |

## Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.<br>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.<br>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. | http://www.cisco.com/techsupport |

# Feature Information for AAA Double Authentication Secured by Absolute Timeout

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

*Table 1 Feature Information for AAA Double Authentication Secured by Absolute Timeout*

| Feature Name | Releases | Feature Information |
|---|---|---|
| AAA Double Authentication Secured by Absolute Timeout | Cisco IOS XE Release 2.3 | The AAA Double Authentication Secured by Absolute Timeout feature allows you to secure the double authentication mechanism by protecting it with a per-user session timeout. This feature optimizes the connection to the network by service providers to only connections that are authorized, and it increases the security of the overall access to the network by ensuring that no unwanted sessions are connected.<br><br>In Cisco IOS XE Release 2.3, this feature was introduced on the Cisco ASR 1000 Aggregation Services Routers. |