



AAA Double Authentication Secured by Absolute Timeout

Last Updated: July 9, 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 connections to the network that are authorized by service providers and increases the security of the overall access to the network by ensuring that no unwanted sessions are connected.

- [Finding Feature Information, page 1](#)
- [Prerequisites for AAA Double Authentication Secured by Absolute Timeout, page 1](#)
- [Restrictions for AAA Double Authentication Secured by Absolute Timeout, page 2](#)
- [Information About AAA Double Authentication Secured by Absolute Timeout, page 2](#)
- [How to Apply AAA Double Authentication Secured by Absolute Timeout, page 2](#)
- [Configuration Examples for AAA Double Authentication Secured by Absolute Timeout, page 5](#)
- [Additional References, page 8](#)
- [Feature Information for AAA Double Authentication Secured by Absolute Timeout, page 9](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and 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 module.

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

- You need access to a Cisco RADIUS or TACACS+ server and should be familiar with configuring RADIUS or TACACS+.



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

- You should be familiar with configuring authentication, authorization, and accounting (AAA) and enabling AAA automated double authentication.

Restrictions for AAA Double Authentication Secured by Absolute Timeout

- The AAA Double Authentication Secured by Absolute Timeout 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, page 2](#)

AAA Double Authentication

Use the AAA double authentication mechanism to pass the first authentication using a host username and password. The second authentication, after the Challenge Handshake Authentication Protocol (CHAP) or the Password Authentication Protocol (PAP) authentication, uses a login username and password. In the first authentication, a PPP session timeout is 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 session 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, page 2](#)
- [Verifying AAA Double Authentication Secured by Absolute Timeout, page 3](#)

Applying AAA Double Authentication Secured by Absolute Timeout

To apply the absolute timeout, you must configure session-timeout in the login user profile as a link control protocol (LCP) per-user attribute. Use the **access-profile** command to enable AAA double authentication. This command is used to apply your per-user authorization attributes to an interface during a PPP session. Before you use the **access-profile** command, 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 section “Examples for AAA Double Authentication Secured by Absolute Timeout.”

**Note**

The Timeout configuration in a TACACS+ user profile is 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 is applied to the EXEC session and to the PPP session respectively. 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 will not be available during 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**

If 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 interfaces. However, if the idle timeout is not configured on both interfaces, the **show users** command will display the idle time for the full virtual access interface only.

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. Enter one of the following:
 - **debug radius**
or
debug tacacs

DETAILED STEPS

Command or Action	Purpose
<p>Step 1 <code>enable</code></p> <p>Example:</p> <pre>Device> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
<p>Step 2 <code>show users</code></p> <p>Example:</p> <pre>Device# show users</pre>	<p>Displays information about active lines on the device.</p>
<p>Step 3 <code>show interfaces virtual-access <i>number</i> [configuration]</code></p> <p>Example:</p> <pre>Device# show interfaces virtual-access 2 configuration</pre>	<p>Displays status, traffic data, and configuration information about a specified virtual access interface.</p>
<p>Step 4 <code>debug aaa authentication</code></p> <p>Example:</p> <pre>Device# debug aaa authentication</pre>	<p>Displays information about AAA TACACS+ authentication.</p>
<p>Step 5 <code>debug aaa authorization</code></p> <p>Example:</p> <pre>Device# debug aaa authorization</pre>	<p>Displays information about AAA TACACS+ authorization.</p>
<p>Step 6 <code>debug aaa per-user</code></p> <p>Example:</p> <pre>Device# debug aaa per-user</pre>	<p>Displays the attributes that are applied to each user as the user gets authenticated.</p>
<p>Step 7 <code>debug ppp authentication</code></p> <p>Example:</p> <pre>Device# debug ppp authentication</pre>	<p>Displays whether a user is passing authentication.</p>

Command or Action	Purpose
<p>Step 8 Enter one of the following:</p> <ul style="list-style-type: none"> • debug radius or debug tacacs <p>Example:</p> <pre>Device# debug radius</pre> <p>Example:</p> <pre>Device# debug tacacs</pre>	<p>Displays the debug information associated with the RADIUS server.</p> <p>or</p> <p>Displays the debug information associated with the TACACS+ server.</p>

Examples

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

```
Device# 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:

```
Device# 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.
```

Configuration Examples for AAA Double Authentication Secured by Absolute Timeout

Example: RADIUS User Profile

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"

```

Example: TACACS User Profile

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 Authentication

The following example shows how to allow the remote host to be authenticated by the local host during the 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

```

Using the 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)!

```

Using the access-profile Command with the merge Keyword

The **merge** keyword in the **access-profile** command is used to remove all old access lists, and any attribute-value (AV) pair is allowed to be uploaded and installed. The use of the **merge** keyword will allow for the uploading of any custom static routes, Service Advertisement Protocol (SAP) filters, and other requirements that users may need in their profiles. Configure the **merge** keyword 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)!

```

Using the access-profile Command with the replace Keyword

If you use the **access-profile** command with the **replace** keyword, any old configurations are removed and a new configuration is installed.

**Note**

When the **access-profile** command is configured, the new configuration is checked for address pools and address-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**

The Timeout configuration in a TACACS+ user profile is 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 the TACACS+ user profile, 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 respectively. If the timeout is configured only under the service type “ppp,” the timeout value will not be available during an EXEC authorization, and the timeout will not be applied to the EXEC session.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Master Command List, All Releases

Related Topic	Document Title
Security commands	<ul style="list-style-type: none"> • <i>Security Command Reference: Commands A to C</i> • <i>Security Command Reference: Commands D to L</i> • <i>Security Command Reference: Commands M to R</i> • <i>Security Command Reference: Commands S to Z</i>

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

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	12.3(7)T 12.2(28)SB 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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2012 Cisco Systems, Inc. All rights reserved.