MSCHAP Version 2

The MSCHAP Version 2 feature (introduced in Cisco IOS Release 12.2(2)XB5) allows Cisco routers to utilize Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAP V2) authentication for PPP connections between a computer using a Microsoft Windows operating system and a network access server (NAS).

For Cisco IOS Release 12.4(6)T, MSCHAP V2 now supports a new feature: AAA Support for MSCHAPv2 Password Aging. Prior to Cisco IOS Release 12.4(6)T, when Password Authentication Protocol (PAP)-based clients sent username and password values to the authentication, authorization, and accounting (AAA) subsystem, AAA generated an authentication request to the RADIUS server. If the password expired, the RADIUS server replied with an authentication failure message. The reason for the authentication failure was not passed back to AAA subsystem; thus, users were denied access because of authentication failure but were not informed why they were denied access.

The Password Aging feature, available in Cisco IOS Release 12.4(6)T, notifies crypto-based clients that the password has expired and provides a generic way for the user to change the password. The Password Aging feature supports only crypto-based clients.

- Finding Feature Information, on page 1
- Prerequisites for MSCHAP Version 2, on page 2
- Restrictions for MSCHAP Version 2, on page 2
- Information About MSCHAP Version 2, on page 2
- How to Configure MSCHAP Version 2, on page 3
- Configuration Examples, on page 6
- Additional References, on page 7
- Feature Information for MSCHAP Version 2, on 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.

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 MSCHAP Version 2

- Configure an interface type and enter interface configuration mode by using the `interface` command.
- Configure the interface for PPP encapsulation by using the `encapsulation` command.
- Be sure that the client operating system supports all MSCHAP V2 capabilities.
- For Cisco IOS Release 12.4(6)T, the Password Aging feature only supports RADIUS authentication for crypto-based clients.
- To ensure that the MSCHAP Version 2 features correctly interpret the authentication failure attributes sent by the RADIUS server, you must configure the `ppp max-bad-auth` command and set the number of authentication retries at two or more.

In addition, the `radius server vsa send authentication` command must be configured, allowing the RADIUS client to send a vendor-specific attribute to the RADIUS server. The Change Password feature is supported only for RADIUS authentication.

- The Microsoft Windows 2000, Microsoft Windows XP, and Microsoft Windows NT operating systems have a known caveat that prevents the Change Password feature from working. You must download a patch from Microsoft at the following URL:

  http://support.microsoft.com/default.aspx?scid=kb;en-us;Q326770

For more information on completing these tasks, see the section “PPP Configuration” in the *Cisco IOS Dial Technologies Configuration Guide*, Release 12.4T. The RADIUS server must be configured for authentication. Refer to vendor-specific documentation for information on configuring RADIUS authentication on the RADIUS server.

Restrictions for MSCHAP Version 2

- MSCHAP V2 authentication is not compatible with MSCHAP V1 authentication.
- The change password option is supported only for RADIUS authentication and is not available for local authentication.

Information About MSCHAP Version 2

MSCHAP V2 authentication is the default authentication method used by the Microsoft Windows 2000 operating system. Cisco routers that support this authentication method enable Microsoft Windows 2000 operating system users to establish remote PPP sessions without configuring an authentication method on the client.

MSCHAP V2 authentication introduced an additional feature not available with MSCHAP V1 or standard CHAP authentication: the Change Password feature. This features allows the client to change the account password if the RADIUS server reports that the password has expired.
MSCHAP V2 authentication is an updated version of MSCHAP that is similar to but incompatible with MSCHAP Version 1 (V1). MSCHAP V2 introduces mutual authentication between peers and a Change Password feature.

# How to Configure MSCHAP Version 2

## Configuring MSCHAP V2 Authentication

To configure the NAS to accept MSCHAP V2 authentication for local or RADIUS authentication and to allow proper interpretation of authentication failure attributes and vendor-specific RADIUS attributes for RADIUS authentication, use the following commands beginning in global configuration mode.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `radius-server vsa send authentication`
4. `interface type number`
5. `ppp max-bad-auth number`
6. `ppp authentication ms-chap-v2`
7. `end`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>radius-server vsa send authentication</code></td>
<td>Configures the NAS to recognize and use vendor-specific attributes.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# radius-server vsa send authentication</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>interface type number</code></td>
<td>Configures an interface type and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

**Command or Action**  
Device(config)# interface Gigabitethernet 1/0/1

**Step 5**  
**Command or Action**  
`ppp max-bad-auth number`  
**Example:**  
Device(config-if)# ppp max-bad-auth 2  
**Purpose**  
Configures a point-to-point interface to reset immediately after an authentication failure or within a specified number of authentication retries.  
- The default value for the `number` argument is 0 seconds (immediately).  
- The range is between 0 and 255.  
**Note**  
The `number` argument must be set to a value of at least 2 for authentication failure attributes to be interpreted by the NAS.

**Step 6**  
**Command or Action**  
`ppp authentication ms-chap-v2`  
**Example:**  
Device(config-if)# ppp authentication ms-chap-v2  
**Purpose**  
Enables MSCHAP V2 authentication on a NAS.

**Step 7**  
**Command or Action**  
`end`  
**Example:**  
Device(config-if)# end  
**Purpose**  
Returns to privileged EXEC mode.

### Verifying MSCHAP V2 Configuration

To verify that the MSCHAP Version 2 feature is configured properly, perform the following steps.

#### SUMMARY STEPS

1. `show running-config interface type number`
2. `debug ppp negotiation`
3. `debug ppp authentication`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**  
**Command or Action**  
`show running-config interface type number`  
**Example:**  
Device# show running-config interface Asynch65  
**Purpose**  
Verifies the configuration of MSCHAP V2 as the authentication method for the specified interface. |
| **Step 2**  
**Command or Action**  
`debug ppp negotiation`  
**Example:**  
**Purpose**  
Verifies successful MSCHAP V2 negotiation. |
MSCHAP Version 2

Configuring Password Aging for Crypto-Based Clients

The AAA security services facilitate a variety of login authentication methods. Use the `aaa authentication login` command to enable AAA authentication no matter which of the supported login authentication methods you decide to use. With the `aaa authentication login` command, you create one or more lists of authentication methods that are tried at login. These lists are applied using the `login authentication` line configuration command.

After the RADIUS server requests a new password, AAA queries the crypto client, which in turn prompts the user to enter a new password.

To configure login authentication and password aging for crypto-based clients, use the following commands beginning in global configuration mode.

**Note**
The AAA Password Expiry infrastructure notifies the Easy VPN client that the password has expired and provides a generic way for the user to change the password. Please use RADIUS-server domain-stripping feature wisely in combination with AAA password expiry support.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `aaa new-model`
4. `aaa authentication login {default | list-name} passwd-expiry method1 [method2...]
5. `crypto map map-name client authentication list list-name`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
| `enable`
| Example:
| Device> enable | Enables privileged EXEC mode. |
| **Step 2**
| `configure terminal`
| Example:
<p>| Device# configure terminal | Enters global configuration mode. |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>aaa new-model</td>
<td>Enables AAA globally.</td>
</tr>
<tr>
<td>Device(config)# aaa new-model</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>aaa authentication login {default</td>
<td>list-name} passwd-expiry method1 [method2...]</td>
</tr>
<tr>
<td>Device(config)# aaa authentication login userauthen passwd-expiry group radius</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>crypto map  map-name client authentication list list-name</td>
<td>Configures user authentication (a list of authentication methods) on an existing crypto map.</td>
</tr>
<tr>
<td>Device(config)# crypto map clientmap client authentication list userauthen</td>
<td></td>
</tr>
</tbody>
</table>

### Configuration Examples

#### Configuring Local Authentication Example

The following example configures PPP on an asynchronous interface and enables MSCHAP V2 authentication locally:

```plaintext
interface Async65
  ip address 10.0.0.2 255.0.0.0
  encapsulation ppp
  async mode dedicated
  no peer default ip address
  ppp max-bad-auth 3
  ppp authentication ms-chap-v2
  username client password secret
```

#### Configuring RADIUS Authentication Example

The following example configures PPP on an asynchronous interface and enables MSCHAP V2 authentication via RADIUS:

```plaintext
interface Async65
  ip address 10.0.0.2 255.0.0.0
  encapsulation ppp
  async mode dedicated
  no peer default ip address
```
Configuring Password Aging with Crypto Authentication Example

The following example configures password aging by using AAA with a crypto-based client:

```
aaa authentication login userauthen passwd-expiry group radius
!
aaa session-id common
!
crypto isakmp policy 3
  encr 3des
  authentication pre-share
  group 2
!
crypto isakmp client configuration group 3000client
  key cisco123
  dns 10.1.1.10
  wins 10.1.1.20
  domain cisco.com
  pool ippool
  acl 153
!
crypto ipsec transform-set myset esp-3des esp-sha-hmac
!
crypto dynamic-map dynmap 10
  set transform-set myset
!
crypto map clientmap client authentication list userauthen
!
radius-server host 10.140.15.203 auth-port 1645 acct-port 1646
radius-server domain-stripping prefix-delimiter $
radius-server key cisco123
radius-server vsa send authentication
radius-server vsa send authentication 3gpp2
!
end
```

Additional References

The following sections provide references related to the MSCHAP Version 2 feature.

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring PPP interfaces</td>
<td>PPP Configuration in the <em>Cisco IOS Dial Technologies Configuration Guide</em>, Release 12.4T.</td>
</tr>
</tbody>
</table>
### Related Topic

<table>
<thead>
<tr>
<th>Description of the tasks and commands necessary to configure and maintain Cisco networking devices</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Dial Technologies Command Reference</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Lists of IOS Security Commands</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Security Command Reference</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuring PPP authentication using AAA</th>
<th>Document Title</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuring RADIUS Authentication</th>
<th>Document Title</th>
</tr>
</thead>
</table>

### Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature.</td>
<td>--</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified MIBs are supported by this feature.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

### RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 1661</td>
<td>Point-to-Point Protocol (PPP)</td>
</tr>
<tr>
<td>RFC 2548</td>
<td>Microsoft Vendor-specific RADIUS Attributes</td>
</tr>
<tr>
<td>RFC 2759</td>
<td>Microsoft PPP CHAP Extensions, Version 2</td>
</tr>
</tbody>
</table>
Technical Assistance

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

Feature Information for MSCHAP Version 2

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>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSCHAP V2</td>
<td>Cisco IOS XE</td>
<td>The MSCHAP Version 2 feature allows Cisco routers to utilize Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAP V2) authentication for PPP connections between a computer using a Microsoft Windows operating system and a network access server (NAS).</td>
</tr>
<tr>
<td></td>
<td>Release 3.9S</td>
<td>The following commands were introduced or modified: aaa authentication login, and ppp authentication ms-chap-v2.</td>
</tr>
</tbody>
</table>