Windows NPS RADIUS Event ID Errors

This knowledge base article discusses common configuration errors when implementing WPA2 Enterprise with PEAP-MSCHAPv2, using a Windows 2008 NPS environment for error codes. This article addresses Windows event log messages, possible causes for the error events, and recommended solutions.

Windows Event Viewer can be found by navigating to Start > All Programs > Administrative Tools > Event Viewer. The 2 logs that will be referenced are Network Policy and Access Services logs and Security logs, see the image below:

Common Configuration Errors

The following common configuration errors may result in RADIUS authentication failing. Though the error codes outlined below are specific to Windows NPS, the following configuration check should be made regardless of RADIUS server vendor:

1. No certificate installed on the RADIUS Server or the certificate has expired.

2. Cisco Meraki Access Points are not added as a RADIUS Client or are Configured for DHCP

3. Incorrect Secret on the Dashboard

4. Network Policy is Misconfigured

5. Connection Request Policy is Misconfigured
6. Mismatch in Authentication Settings

7. Incorrect Username or Password

8. Root Certificate is not added to the client Device

**Event ID 6273 with reason code 23 (bad/missing certificate)**

Often times connection issues occur because a digital certificate is not installed on the RADIUS Server or the certificate has expired. If this is the case, you will see Event ID 6273 with Reason Code 23 in the Network Policy and Access Services logs, shown below.

To resolve this, a certificate will need to be installed or renewed on your NPS server, in order to establish TLS.

**Event ID 13: A RADIUS message was received from the invalid RADIUS client (APs not added as clients)**

WPA2 Enterprise authentication requires your Cisco Meraki Access Points be added as RADIUS Clients on your NPS Server. Because of this, it is imperative that a static IP assignment or a DHCP fixed IP assignment be used on your APs. If your AP is not added as a RADIUS Client you will see Event ID 13 in the Network Policy and Access Services logs, as shown below.

To resolve, see the below KB articles on adding a RADIUS client and setting static IP addresses on access points.

- Adding a Gateway AP as a RADIUS Client in NPS
Event ID 18: An Access-Request message was received from RADIUS client x.x.x.x with a Message-Authenticator attribute that is not valid (bad shared secret)

On the Dashboard, Configure > Access Control, you must enter a secret when specifying your RADIUS server. This secret must match the shared secret you enter when you adding the MR Access Points as RADIUS clients. When the Secrets do no match, you will see Event ID 18 in the Network Policy and Access Services logs as shown below.

To resolve, ensure when Adding a Gateway AP as a RADIUS Client in NPS that the Shared Secret matches the Secret on Configure > Access Control on the Dashboard.
Event ID 6273 Reason Code 48 (bad network policy)

If you receive Event ID 6273 with Reason Code 48 when testing with the RADIUS Test feature on Dashboard, this is usually indicative of an incorrectly configured **Network Policy** on your NPS server.

To resolve please refer to our documentation on [creating an NPS policy for PEAP MSCHAPv2](#).

If the Dashboard test passes and you receive this error when testing with a Windows 7 client ensure the client's WPA-2 Enterprise settings are correct.
Event ID 6273 Reason Code 49 (bad request policy)

If you receive Event ID 6273 with Reason Code 49 when testing with the RADIUS Test feature on Dashboard, this is usually indicative of an incorrectly configured Connection Request Policy on your NPS server.

To resolve visit our KB on Creating a Policy in NPS to Support PEAP-MSCHAPv2 Authentication.
**Event ID 6273 Reason Code 66 (auth settings mismatch)**

If you receive **Event ID 6273 with Reason Code 66** when testing with the RADIUS Test feature on Dashboard, this is usually indicative of the authentication settings incorrectly configured the **Network Policy** on your NPS server.

If the Dashboard test passes and you receive this error when testing with a Windows 7 client ensure the client's authentication settings are correct by viewing our KB on [Pushing a PEAP Wireless Profile to a Windows 7 domain computer via GPO](#).

![Event Log Example](image)

**Event ID 6273 Reason Code 8 (bad username or password)**

When testing RADIUS authentication it is possible that the username may be incorrect or may not be located in the Windows group specified in the Network Policy. If this is the case, you will see **Event ID 6273 with Reason Code 8** in the **Network Policy and Access Services** logs, see the image below.

To resolve, ensure the username is correct and is present in the Windows group specified on your network policy. Please refer to our documentation regarding [NPS policy configuration](#).
When testing RADIUS authentication it is possible that the user password may be incorrect. If this is the case, you will see Event ID 4625 in the Windows Security logs, shown below.

To resolve, confirm the users password and/or perform a password reset in Active Directory.

---

Event 6273, Microsoft Windows security auditing.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Session Identifier</td>
<td>-</td>
</tr>
<tr>
<td>Logging Results</td>
<td>Accounting information was written to the local log file.</td>
</tr>
<tr>
<td>Reason Code</td>
<td>8</td>
</tr>
<tr>
<td>Reason</td>
<td>The specified user account does not exist.</td>
</tr>
</tbody>
</table>

Log Name: Security
Source: Microsoft Windows security
Logged: 6/5/2013 3:30:37 PM
Event ID: 6273
Task Category: Network Policy Server
Level: Information
Keywords: Audit Failure
User: N/A
Computer: WIN-SK3KB0U0NOP.test.local
OpCode: Info
More Information: Event Log Online Help

---

Event 4625, Microsoft Windows security auditing.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure Information</td>
<td>Unknown user name or bad password.</td>
</tr>
<tr>
<td>Failure Reason</td>
<td>0xc000006d</td>
</tr>
<tr>
<td>Status</td>
<td>0xc000006a</td>
</tr>
</tbody>
</table>

Log Name: Security
Source: Microsoft Windows security
Event ID: 4625
Task Category: Logon
Level: Information
Keywords: Audit Failure
User: N/A
Computer: WIN-SK3KB0U0NOP.test.local
OpCode: Info
More Information: Event Log Online Help
**Event ID 6273 Reason Code 265 (untrusted CA)**

On Windows end-user devices you have the option to validate the server certificate presented by the server when using WPA-2 Enterprise, which is strongly recommended for RADIUS. If this option is selected, the Certificate Authority must be added to the client's list of Trusted Root Certification Authorities. If the Certificate Authority is not added to the Windows Client you may see Event 6273 Reason Code 265 in the Network Policy and Access Services logs: