Contents

Introduction 3
Interoperability and Supported Platforms 3
Pulse 5.0R3 New Features 3
  SRX Dynamic VPN Connections for Pulse for Mac 3
  Configuring a Pulse Credential Provider Connection for Password or
  Smart Card Login 4
  Updated NDIS Support 6
Problems Resolved in This Release 7
Known Issues in This Release 8
Problems Resolved in 5.0R2 9
Known Issues in Pulse 5.0R2 10
Documentation 10
Documentation Feedback 10
Technical Support 10
Revision History 10
Introduction

These release notes contain information about Pulse new features, software issues that have been resolved and new issues that affect Pulse behavior. If the information in the release notes differs from the information found in the documentation set, follow the release notes.

Note: This Pulse maintenance release introduces new features. These new features are documented in this document.

Interoperability and Supported Platforms

Please refer to the Pulse 5.0R3 Supported Platforms Guide for supported versions of browsers and operating systems in this release.

Pulse 5.0R3 New Features

SRX Dynamic VPN Connections for Pulse for Mac

Pulse for Mac OS X adds support for Dynamic VPN tunnels to a Juniper Networks SRX gateway. Mac OS X endpoints can now use Pulse client software to connect to SRX Branch series SRX100-SRX650 gateways that are running Junos OS Release 10.x or later, and that have dynamic VPN access enabled and configured. SRX gateways do not support deployment of the Mac version of the Pulse Client. For deployment options for the Mac version of the Pulse client, please read the Pulse Admin guide.

Figure 1. Pulse for Mac
Note: The Pulse Dynamic VPN functionality is compatible with SRX-Branch (SRX100-SRX650) devices only. SRX Data Center (SRX1400-SRX5800 – also called SRX HE or High End) devices do not support Pulse Dynamic VPN from either Windows or Mac clients.

Configuring a Pulse Credential Provider Connection for Password or Smart Card Login

If you allow users to log in with smart cards or with a username/password, then you can have the Pulse credential provider automatically authenticate the user based on the login method. The Pulse user sees two different credential provider tiles for the Pulse connection, one for smart card authentication and one for username/password authentication. Credential provider tiles that launch a Pulse connection include a Pulse logo. See Figure 2. The Pulse connection determines which realm to use through preferred realm settings that you specify as part of the Pulse connection preferences. If the connection succeeds, the login type is saved so that, if re-authentication is needed, (for example, the connection times out), the same login type is used.

![Figure 2. Pulse Credential Provider Tiles](image)

Before you begin:

- Before you deploy a connection that uses this feature, make sure that you have created all the authentication realms that are required. You need one realm for smart card authentication and a different one for user name/password authentication. Both realms can be mapped to the same role or you can use different roles, and include a remediation role for endpoints that do not pass Host Checker evaluation. If you use machine authentication for a connection (machine-then-user-at-credprov), you need an authentication realm for the machine.
• Make sure that all of the realms that are used in the Pulse connection are included in the sign-in policy.

• The authentication realms on the Pulse server must be configured so that the Preferred Pre-login Smartcard Realm uses certificate authentication and the Preferred Pre-login Password Realm uses username/password authentication.

The following procedure summarizes the steps to create a Pulse connection that uses credential provider authentication, and allows the user to choose either smart card login or username/password login. 0 describes the configuration options:

1. Click **Users > Pulse > Connections** and create or select a connection set.

2. Create or edit a connection. For connection type, you can select either **UAC (802.1X)** for a Layer 2 connection or **SSL VPN or UAC (L3)** for a Layer 3 connection. The **SRX** and **App Acceleration** connection types do not support credential provider authentication.

3. For the **Connection is established** option, choose one of the credential provider options:
   - **Automatically at user login**—Enables Pulse client interaction with the credential provider software on the endpoint. The user credentials are used to establish the authenticated Pulse connection to the network, login to the endpoint, and login to the domain server.
   - **Automatically when the machine starts.** Connection is authenticated again at user login—Enables Pulse client interaction with the credential provider software on the endpoint. Machine credentials are used to establish the authenticated Pulse connection to the network using the specified Machine Connection Preferences or Pre-login Connection Preferences. When the user provides user credentials, the connection is authenticated again.

4. For **SSL VPN or UAC (L3)** connections that are set to have the connection established automatically, you can define location awareness rules that enable an endpoint to connect conditionally.

5. For a Layer 2 connection that uses machine certificate authentication, make sure that the connection has an entry in the Trusted Server List. To allow any server certificate, type **ANY** as the Server certificate DN. To allow only one server certificate, specify the server certificate's full DN for example, **C=US; ST=NH; L=Kingston; O=My Company; OU=Engineering; CN=c4k1.stnh.mycompany.net; E=ausername@mycompany.com**.

6. For the desired connection behavior, set the connection preferences as described in 0.

**Table 1 Configuration Options for Credential Provider Login**
### Pulse Client Credential Provider Login Behavior

<table>
<thead>
<tr>
<th>Connection is established option</th>
<th>User Connection Preferences options</th>
<th>Pre-login Connection Preferences</th>
<th>Machine Connection Preferences</th>
</tr>
</thead>
<tbody>
<tr>
<td>At user login, the user can choose from two credential provider tiles: smart card login or username/password login.</td>
<td>Preferred User Realm and Preferred User Role Set are not available if you specify values for Preferred Pre-login Password Realm Preferred Pre-login Smartcard Realm.</td>
<td>Enables Pulse credential provider tiles. The realm name appears on each tile. You must specify values for both of the following options:</td>
<td>Not available.</td>
</tr>
<tr>
<td>The credentials are then used to connect to the network, login to the endpoint, and login to the domain server.</td>
<td>• Preferred Pre-login Password Realm—The authentication realm that provides username/password authentication.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Preferred Pre-login Smartcard Realm—The authentication realm that provides smartcard authentication.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### At machine login and at user login, the user can choose from two credential provider tiles: smart card login or username/password login.

<table>
<thead>
<tr>
<th>Connection is established option</th>
<th>User Connection Preferences options</th>
<th>Pre-login Connection Preferences</th>
<th>Machine Connection Preferences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatically at user login</td>
<td>Enables Pulse credential provider tiles. The realm name appears on each tile.</td>
<td>Preferred Machine Realm and Preferred Machine Role Set are not available if you specify values for Preferred Pre-login Password Realm Preferred Pre-login Smartcard Realm.</td>
<td></td>
</tr>
<tr>
<td>Preferred Pre-login Password Realm—The authentication realm that provides username/password authentication.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Preferred Pre-login Smartcard Realm—The authentication realm that provides smartcard authentication.</td>
<td></td>
<td>Preferred Machine Realm and Preferred Machine Role Set are not available if you specify values for Preferred Pre-login Password Realm Preferred Pre-login Smartcard Realm.</td>
<td></td>
</tr>
</tbody>
</table>

### Updated NDIS Support

Pulse for Windows includes a set of drivers that interface with the Windows Network Driver Interface Specification (NDIS) driver for communications with the endpoint’s network interface. For Pulse 5.0R3, the NDIS5 compliant Pulse Secure Agent (PSA) has been replaced with the NDIS6 compliant Pulse Secure Service (PSS) to support enhanced functionality that is available in Windows Vista and later Windows versions. PSA will continue to be available on Windows XP endpoints. Pulse on all other Windows versions will use PSS. The Pulse for Windows file set changes are included in the Pulse Client Changes Guide 5.0R3.
Note: PSS does not support wired 802.1x for Odyssey Access Client (OAC). If OAC is already installed on the endpoint when you install Pulse 5.0R3, the new PSS components will be installed to support Pulse, and the required legacy PSA components will remain on the endpoint to support OAC functionality.

For more information about NDIS and upgrading to Pulse 5.0R3, see KB 28892.

## Problems Resolved in This Release

Table 2 describes issues that are resolved when you upgrade.

### Table 2 Resolved in This Release

<table>
<thead>
<tr>
<th>Problem Report Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>959763, 965819</td>
<td>On machines running Pulse 5.0r1 or 5.0r2, Pulse may freeze under certain conditions, including:</td>
</tr>
<tr>
<td></td>
<td>• When the endpoint displays the splash screen after the device resumes from sleep</td>
</tr>
<tr>
<td></td>
<td>• During the ‘Remediating’ state</td>
</tr>
<tr>
<td>959840</td>
<td>User prompted for realm selection when multiple connections are configured and the user logs in as a username password user.</td>
</tr>
<tr>
<td>971965</td>
<td>Pulse UI message displaying the presence/absence of the wireless adapter is not being updated frequently enough.</td>
</tr>
<tr>
<td>969904</td>
<td>After receiving connection information from the server, the client can fail to save the data and report the following errors:</td>
</tr>
<tr>
<td></td>
<td>'UiModel' Error getting machine::setting conn-info using conn-store client.</td>
</tr>
<tr>
<td></td>
<td>and</td>
</tr>
<tr>
<td></td>
<td>Failed CreateFile: 32 C:\Program Files (x86)\Common Files\Pulse Secure\ConnectionStore</td>
</tr>
<tr>
<td></td>
<td>This problem can happen on machines that are either very slow, or, that are running Antivirus software that substantially delays access to files</td>
</tr>
<tr>
<td>970841</td>
<td>Under very limited and intermittent conditions after upgrading to Pulse 5.0r2, Pulse may stop sending traffic through the VPN tunnel.</td>
</tr>
</tbody>
</table>

## Known Issues in This Release

Table 3 describes the open issues with Pulse.

### Table 3 Known Issues
<table>
<thead>
<tr>
<th>Problem Report Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>962446</td>
<td>Pulse running in FIPS mode on an endpoint running McAfee Application Control can cause a self-test failure. Pulse Secure Knowledgebase article KB28876 describes how to recognize this issue and how to configure McAfee Application Control to avoid this issue.</td>
</tr>
<tr>
<td>970837</td>
<td>Some 3rd party applications can lock DLLs that must be changed during a Pulse upgrade. When this happens, a reboot is required to finish the upgrade. To minimize the likelihood of being asked to reboot after a Pulse upgrade, we recommend that you close all applications prior to upgrading Pulse.</td>
</tr>
<tr>
<td>974070</td>
<td>The “Dynamic VPN to SRX” firewalls feature that was added in Pulse 5.0r3 is not supported on OSX versions 10.7 and earlier. If you attempt to establish an SRX connection on Mac OS 10.7 or earlier, you will encounter a “Failed to get HTTP response” error.</td>
</tr>
<tr>
<td>954731</td>
<td>On Mac OSX devices running 5.0r3 and later Pulse, the Advanced Connection Details screen will always report ‘Session time remaining’ as zero seconds when a Dynamic VPN connection is established to an SRX firewall. This value can be ignored.</td>
</tr>
<tr>
<td>960981</td>
<td>Users of Java 7 update 45 may see the erroneous warning message ‘This application will be blocked in a future Java security update because the JAR file manifest does not contain the Permissions attribute.’ A bug in Java 7 update 45 causes the Permissions attribute not to be read if the Trusted-Library attribute is also in the manifest. The solution to avoid this warning is to upgrade to Java 7 update 51 or later.</td>
</tr>
<tr>
<td>912652</td>
<td>On OSX 10.9 (Mavericks) and 10.8 (Mountain Lion), Safari 6.1/7’s default action of blocking Java applets prevents Pulse from being deployed from the browser.</td>
</tr>
<tr>
<td>925097</td>
<td>On Vista and greater OS, when using Pulse Collaboration, there may be two Collaboration processes (dscboxui.exe) present.</td>
</tr>
</tbody>
</table>
Problem Report Number | Description
--- | ---
932287 | If a user signs into Pulse Secure Access Services (SSL-VPN) and then migrates their session to a Pulse Access Control Service (an IC), the Federation-Wide Sessions display on the IF-MAP server (navigate to IF-MAP Federation -> This Server -> Federation-Wide Sessions) may contain two nearly identical rows for the one session.

When the user later signs out of the IC, a vestigial row may be left behind, with all cells blank except the “User” cell.

These extra rows can be ignored unless thousands of them accumulate. An accumulation might affect the IF-MAP server’s performance and storage capacity.

Workaround: to eliminate the extra rows, on the JPACS (IC) box to which the users have migrated

7. Click IF-MAP Federation -> Overview.
8. Select No IF-MAP.
9. Click Save Changes.
10. Select IF-MAP client or IF-MAP server, whichever was in effect at step 1.
11. Click Save Changes.

This workaround disrupts users’ access to protected resources, so it should be scheduled during a quiet time.

Problems Resolved in 5.0R2

Table 4 describes the issues resolved in Pulse 5.0R2.

Table 4 Resolved in 5.0R2

| Problem Report Number | Description |
--- | --- |
937818 | When there is no network/internet connection, users are unable to login to the client machine when credential provider connection is in enabled in Pulse. |
882595 | When Pulse is connected to SA via PPPOE with ‘Search the device’s DNS servers first, then client’ option enabled, the DNS resolution requests are still sent to PPPOE’s DNS server rather than IVE’s DNS Server. |
97984 | When ‘Back to my mac’ is enabled through iCloud on Mac OS X, end user cannot reach any resources through the VPN tunnel with Pulse. |
944594 | Pulse Location awareness does not work when router/DHCP server assigns primary and the secondary DNS as the same IP. |
Known Issues in Pulse 5.0R2

Table 5 describes the open issues with Pulse.

**Table 5 Known Issues**

<table>
<thead>
<tr>
<th>Problem Report Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

There are no new issues to report in this release.

Documentation

Pulse documentation is available at [http://www.pulsesecure.net/techpubs](http://www.pulsesecure.net/techpubs).

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@pulsesecure.net.

Technical Support

When you need additional information or assistance, you can contact “Pulse Secure Global Support Center (PSGSC):

- [http://www.pulsesecure.net/support](http://www.pulsesecure.net/support)
- support@pulsesecure.net
- Call us at (408) 372-9600

For more technical support resources, browse the support ([website http://www.pulsesecure.net/support](http://www.pulsesecure.net/support)).

Revision History

Table 6 lists the revision history for this document.

**Table 6 Revision History**

<table>
<thead>
<tr>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>25 March 2014</td>
<td>Initial publication.</td>
</tr>
</tbody>
</table>