Junos Pulse Access Control Service Release Notes

5.0 R3.2 Build 25137
April 2014
Revision 00

Contents

Introduction

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

This is an incremental release notes document that describes the changes made from 5.0R1 release to 5.0R3. The 5.0R1 release notes still apply except for the changes mentioned in this document. Please refer to 5.0R1 release notes for the complete version.

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

Interoperability and Supported Platforms

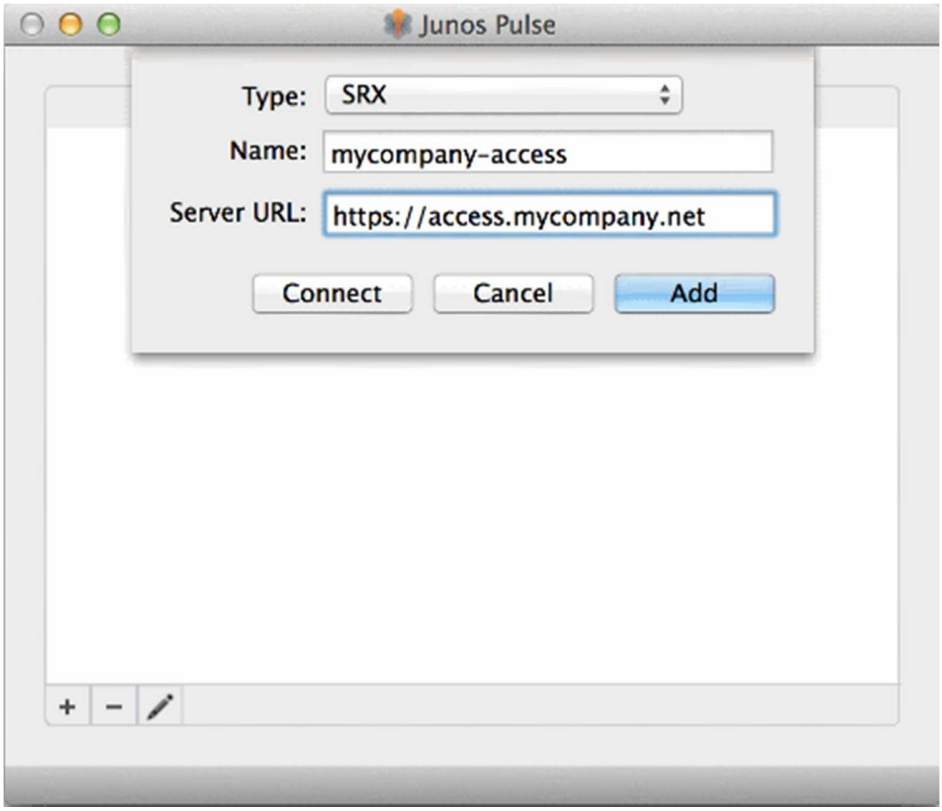
Please refer to the *Junos Pulse Access Control Service Supported Platforms Guide* for supported versions of browsers and operating systems in this release.

Junos Pulse Access Control Service 5.0R3 and Junos Pulse 5.0R3 New Features

SRX Dynamic VPN Connections for Junos Pulse for Mac

Junos Pulse for Mac OS X adds support for Dynamic VPN tunnels to a Juniper Networks SRX gateway. Mac OS X endpoints can now use Junos 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 Junos Pulse Client. For deployment options for the Mac version of the Junos Pulse client, please read the Junos Pulse Admin guide.

Figure 1. Pulse for Mac

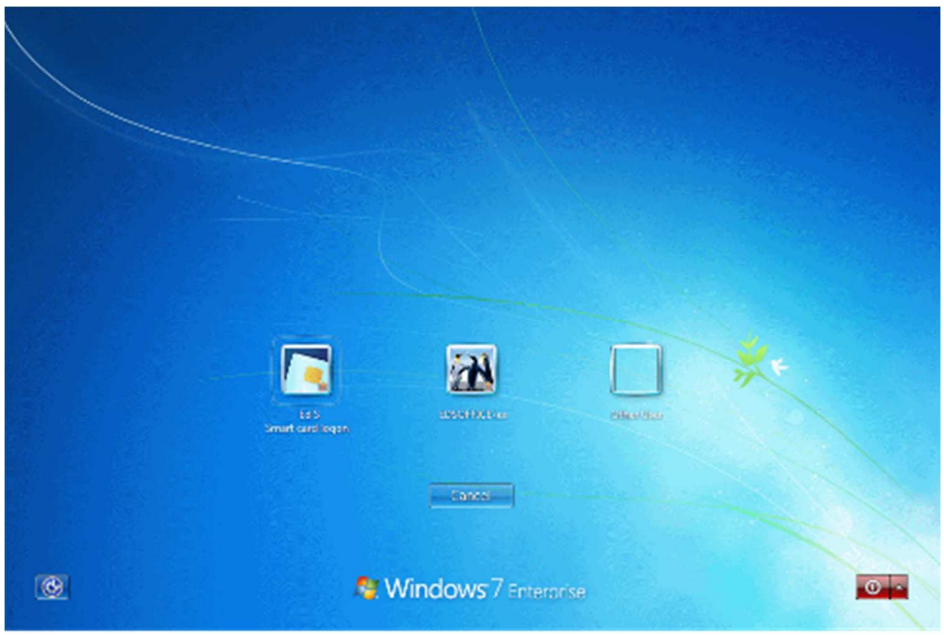


NOTE: The Junos Pulse Dynamic VPN functionality is compatible with SRX-Branch (SRX100-SRX650) devices only. SRX Data Center (SRX1400-SRX5800 – also called SRX HE or High End) devices do not support Junos Pulse Dynamic VPN from either Windows or Mac clients. For more details, please see the KB http://kb.juniper.net/InfoCenter/index?page=content&id=KB17436&smlogin=true.

Configuring a Junos 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



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 Junos 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 > Junos 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	**Connection is established option**	**User Connection Preferences options**	**Pre-login Connection Preferences**	**Machine Connection Preferences**
At user login, the user can choose from two credential provider tiles: smart card login or username/password login. The credentials are then used to connect to the network, login to the endpoint, and login to the domain server.	Automatically at user login	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.	Enables Pulse credential provider tiles. The realm name appears on each tile. You must specify values for both of the following options: • Preferred Pre-login Password Realm—The authentication realm that provides username/password authentication. • Preferred Pre-login Smartcard Realm—The authentication realm that provides smartcard authentication.	Not available.
At machine login and at user login, the user can choose from two credential provider tiles: smart card login or username/password login.	Automatically when machine starts. Connection is authenticated again at user login.		Enables Pulse credential provider tiles. The realm name appears on each tile. • Preferred Pre-login Password Realm—The authentication realm that provides username/password authentication. • Preferred Pre-login Smartcard Realm—The authentication realm that provides smartcard authentication.	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.

Updated NDIS Support

Junos 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 Juniper Network Agent (JNPRNA) has been replaced with the NDIS6 compliant Juniper Network Service (JNPRNS) to support enhanced functionality that is available in Windows Vista and later Windows versions. JNPRNA will continue to be available on Windows XP endpoints. Pulse on all other Windows versions will use JNPRNS. The Pulse for Windows file set changes are included in the *Junos Pulse Client Changes Guide 5.0R3.*

NOTE: JNPRNS 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 JNPRNS components will be installed to support Pulse, and the required legacy JNPRNA 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 C5.0R3.2 release

Table 3 describes issues that are resolved when you upgrade.

Table 2 Resolved in This Release

Problem Report Number	Description
981148	This release fixes the issue described in JSA10623. For more detailed info please refer KB29007

Problems Resolved in C5.0R3 Release

Table 33 describes issues that are resolved when you upgrade.

Table 3 Resolved in This Release

Problem Report Number	Description
928667	If a RADIUS Client is configured with Support Disconnect Message [x] The following message may appear in the Events log: RADIUS: Invalid Message-Authenticator from RADIUS client CLIENT, discarding. Incorrect shared secret? Here CLIENT will be localhost2 or the name of a node of the appliance's cluster.
948953	CHAP authentication for users authenticating to SQL authentication server fails.

Known Issues

Table 44 describes the open issues with Junos Pulse.

Table 4 Known Issues

Problem Report Number	Description
	There are no new issues to report in this release.

Problems Resolved in 5.0R2

Table 55 describes the open issues with Junos Pulse.

Table 5 Resolved in 5.0R2

Problem Report Number	Description
935842	OAC failed to populate the correct encryption details during a network scan for a new network when the wireless access point is configured for WPA2/TKIP or WPA/AES Encryption.
851224	IP allocation fails for the IPSEC clients connected to IC A/A cluster configured with DNS load balancer.
952715	Gateman crashes when there are multiple dot1x sessions for same IP and MAC address but different users. The dot1x session is using non-JUAC protocol and the IP is updated on IC by publishing IP-MAC link.
921463	Log messages like "Warning: Duplicate Request in Cache with mismatched message authenticator, rejecting." observed in SBR logs.
923625	Secure Access users sending PAP authentication requests fails to get connected to the UAC device having certificate restriction enabled on the realm.
947021	RADIUS process memory leak when client sends EAP-NAK indicating it has no supported protocols.

Known Issues in C5.0R2

Table 66 describes the open issues with Junos Pulse.

Table 6 Known Issues

Problem Report Number	Description
	There are no new issues to report in this release.

Documentation

Junos Pulse documentation is available at http://www.juniper.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@juniper.net.

Technical Support

When you need additional information or assistance, you can contact Juniper Networks Technical Assistance Center (JTAC):

http://www.juniper.net/support/requesting-support.html
support@juniper.net
1-888-314-JTAC within the United States
1-408-745-9500 from outside the United States

For more technical support resources, browse the support website (http://www.juniper.net/customers/support/#task).

Revision History

Table 77 lists the revision history for this document.

Table 7 Revision History

Revision	Description
25 March 2014	Initial publication.