Junos® Pulse

Windows In-Box Junos Pulse Client Quick Start Guide

Published: 2013-10-18

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Junos Pulse Windows In-Box Junos Pulse Client Quick Start

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement (“EULA”) posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

PART 1

Introducing the Windows In-Box Junos Pulse Client

CHAPTER 1

Introducing the Windows In-Box Junos Pulse Client

Microsoft Windows In-Box Junos Pulse Client Overview

Microsoft Windows 8.1 introduced Junos Pulse client as part of the Windows operating system. (Microsoft calls this an “in-box” application.) The Windows in-box Pulse client appears as a VPN Provider network option within Windows 8.1 and later endpoints, including Windows RT endpoints. The user can establish a Layer 3 VPN connection to Junos Pulse Secure Access Service. You can create, manage, and remove Pulse VPN connections on the Windows endpoint through Windows PowerShell scripts. The user can also create connections manually on the endpoint. The Windows in-box Pulse client provides a subset of the features that are available through the Junos Pulse for Windows client.

Windows PowerShell is a command-line shell and scripting language for Windows system administration. For more information about PowerShell, see the PowerShell documentation on Microsoft Tech Net. PowerShell commands are called *cmdlets*. For information about the VPN Client cmdlets, see the Microsoft Tech Net topic on VPN Client cmdlets.

Configuration on the Pulse server to support the Windows in-box Pulse client is the same as for the Pulse for Windows client. You create sign-in, realm, role, VPN tunnel, and Host Checker policies. You can use the same roles and connection profiles for the Windows in-box Pulse client as you use for the Pulse for Windows client. However, Host Checker functionality for the in-box client is not fully implemented on Pulse Secure Access Service. The client supports Statement of Health (SoH) as a Host Checker rule. Statement of Health is a component of Network Access Protection (NAP), a Microsoft policy enforcement platform built into Windows 8, Windows 7, Windows Vista, and Windows Server 2008 operating systems. NAP SoH lets you enforce system health compliance.

Microsoft Windows In-Box Junos Pulse Client Supported Platforms

The Windows in-box Pulse client is supported on Pulse Secure Access Service R7.4 and later.

NOTE: **The Statement of Health rule is the only Host Checker rule supported by the Windows in-box Pulse client, and the Statement of Health rule is not fully implemented on Pulse Secure Access Service. If you are using Pulse Secure Access Service R7.4, then Host Checker rule functions are not available.**

Microsoft Windows In-Box Junos Pulse Client Supported Features

The following list describes the supported features for the Windows in-box Pulse client.

- The Windows in-box Pulse client supports connections to Junos Pulse Secure Access Service. Only one connection at a time can be active.
- The user can manually connect and disconnect. The Pulse administrator can also configure a Pulse VPN connection to connect automatically when the user starts a particular app.
- The Windows in-box Pulse client supports the following authentication functions:
  - Username and password or token code.
  - Authentication server prompts for changing the password, creating a PIN, changing a PIN, and specifying the next token code.
  - Realm and role selection and preferred realm and role.
  - Sign-in notification messages.
  - Secondary authentication.
- Cached credentials.
- SSL-VPN connections.
- Split tunneling enabled or disabled.
- Primary and secondary DNS and domain suffix list:
  - DNS search order as defined on Pulse server (redirects all DNS traffic to specified primary or secondary servers).
  - DNS suffixes added to endpoint DNS lookup.
- Proxy server and Proxy Automatic Configuration (PAC).
- Host Checker (Statement of Health rule only).
- Automatic tunnel connection application launch.

Microsoft Windows In-Box Junos Pulse Client Limitations

The Windows in-box Pulse client supports connections to Pulse Secure Access Service only.

The following Pulse features are not available with the Windows in-box Pulse client:

- Host Checker rules (Supported on the client; not fully implemented on the Pulse server.)
- Save realm or role preference.
- Machine authentication.
- Location awareness rules.
- Logon and logoff scripts.
- WINS server tunnel parameter.
- UDP-ESP tunnel (SSL mode only).
- Certificate trust override prompt.
- Proxied HTTPS connections.
- Generalized URI connection addresses. (You can use **port** and **uri** options in the network connection schema instead).
- Preconfigured Pulse settings (**.jnprpreconfig**).
- RSA soft-token integration.
- Session extension.
- Suspend/resume tunnel.

Related Documentation

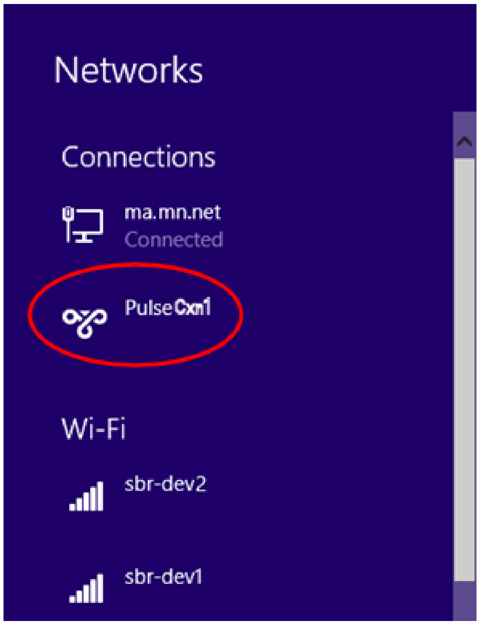
- Microsoft Windows In-box Junos Pulse Client User Interface on page 5
- Windows PowerShell Script Examples for Microsoft Windows In-box Junos Pulse Client on page 8

Microsoft Windows In-Box Junos Pulse Client User Interface

Microsoft Windows 8.1 introduced Junos Pulse client as part of the Windows operating system. (Microsoft calls this an “in-box” application.) The Windows in-box Pulse client uses Windows operating system dialogs. In addition, there is no user assistance provided with the Windows in-box Pulse client. Pulse connections appear as Windows network connections.

Users can create, manage, and delete Pulse connections by using PC Settings > Networks to create VPN connections. Pulse connections appear as VPN connections in the Networks list. Figure 1 on page 6 shows a Pulse VPN connection labeled PulseCxn1.

Figure 1: Windows Networks List



Networks

Connections

ma.mn.net
Connected

PulseCxn1

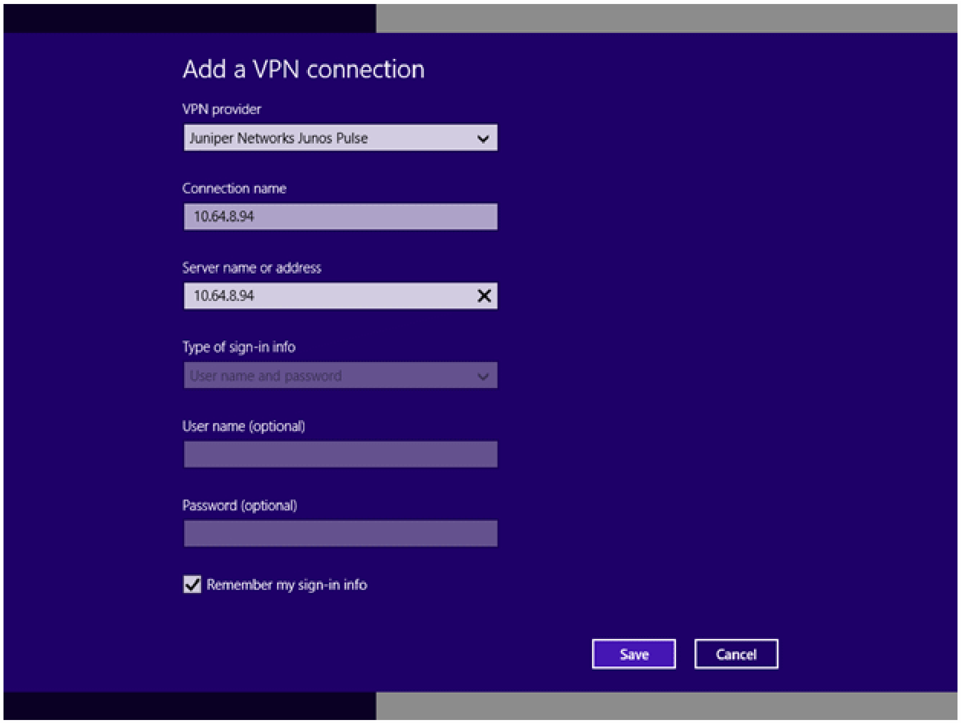
Wi-Fi

sbr-dev2

sbr-dev1

To create a new connection, the user adds a new VPN connection. Figure 2 on page 6 shows the Windows dialog.

Figure 2: Manually Adding a Pulse Connection



Add a VPN connection

VPN provider: Juniper Networks Junos Pulse

Connection name: 10.64.8.94

Server name or address: 10.64.8.94

Type of sign-in info: User name and password

User name (optional):

Password (optional):

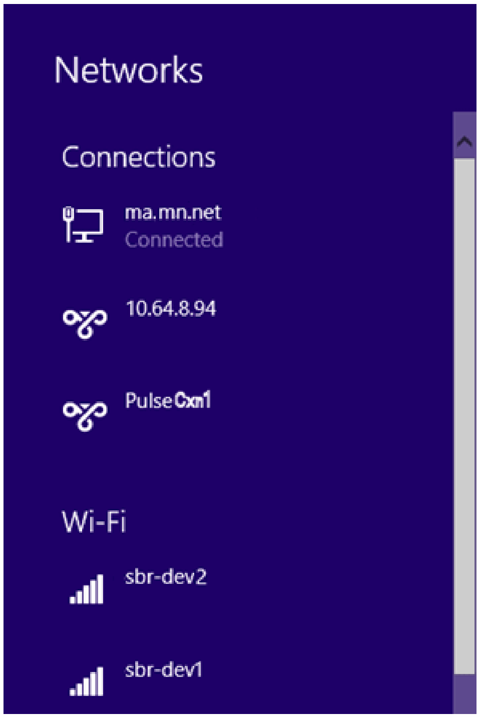
☑ Remember my sign-in info

Juniper Networks Junos Pulse appears as a selection in the **VPN provider** box. The **Connection name** can be anything the user wants but the user needs to provide either the IP address or the hostname (for example, server1.mycompany.net) of the Pulse server in the **Server name or address** box. Because credential prompts are configured on and served from the Pulse server, the **Type of sign-in info** box is not available. If the user selects **Remember my sign-in info**, Windows preserves the values the user specifies for username and password during the first logon operation.

NOTE: Users must have their server's root certificate installed on the endpoint before attempting to connect to the Pulse server to avoid the error, Server certificate is untrusted.

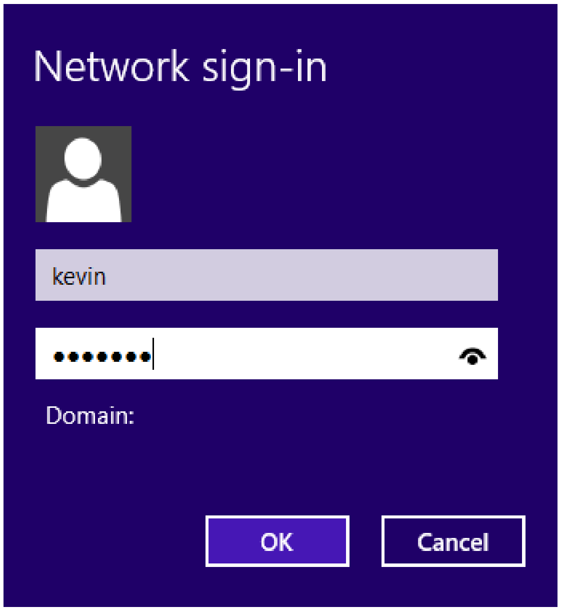
After the user saves the new connection, it appears in the Networks list as shown in Figure 3 on page 7. The user can click the connection to initiate a VPN connection.

Figure 3: Windows Networks List with New Pulse Connection



Pulse connection prompts (Figure 4 on page 8) and messages (Figure 5 on page 8) appear as Windows user interface elements.

Figure 4: Junos Pulse Credentials Dialog



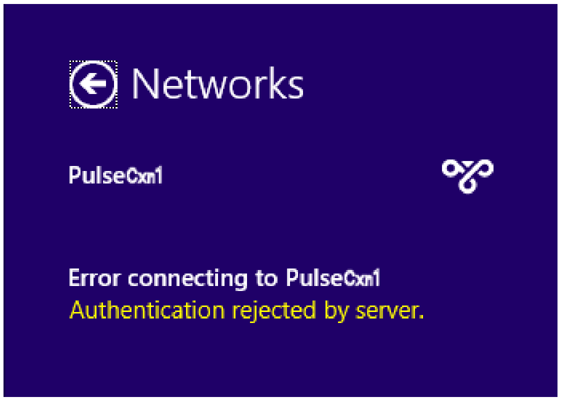
Network sign-in

kevin

•••••••

Domain:

Figure 5: Junos Pulse Message Box



Networks

PulseCxn1

Error connecting to PulseCxn1
Authentication rejected by server.

Related Documentation

- Microsoft Windows In-box Junos Pulse Client Overview on page 3
- Windows PowerShell Script Examples for Microsoft Windows In-box Junos Pulse Client on page 8

Windows PowerShell Script Examples for Microsoft Windows In-Box Junos Pulse Client

Microsoft Windows 8.1 introduced support for Junos Pulse client as part of the operating system. You can create, manage, and remove Pulse connections on the Windows endpoint by using Windows PowerShell scripts on the endpoint. PowerShell is a command-line shell and scripting language for system administration. To configure Junos Pulse connections, you should have a working knowledge of PowerShell. For detailed information on PowerShell, see the Microsoft Tech Net library.

Windows PowerShell commands are called cmdlets. To manage Pulse connections, you use the VPN Client cmdlets. For detailed information on the VPN Client cmdlets, see the VPN Client section of the Microsoft Tech Net library.

NOTE: PowerShell scripts must be signed to run on client computers that have a default PowerShell configuration. For more information, see the Microsoft Tech Net library.

NOTE: You use Windows PowerShell scripts to administer Windows in-box Pulse client connections. Pulse for Windows connections do not respond to PowerShell scripts.

The following PowerShell script examples show how to create and manage the most commonly used PowerShell cmdlets to create and mange Pulse connection configurations. Most PowerShell VPN Client cmdlets require that you specify the application ID. For Pulse, the application ID is **JuniperNetworks.JunosPulseVpn_cw5n1h2txyewy**. For a complete list of cmdlet options, see the VPN Client section of the see the Microsoft Tech Net library.

NOTE: All connections are HTTPS and use a server certificate, therefore you must install the server root CA to connect.

Add Pulse connection that uses split tunneling

This script creates a Pulse VPN connection named PulseCxn1 that connects to a Pulse server with an IP address of 10.17.1.216.

```
$xml = "<pulse-schema></pulse-schema>"
$sourceXml=New-Object System.Xml.XmlDocument
$sourceXml.LoadXml($xml)
Add-VpnConnection -Name “PulseCxn1” -ServerAddress “10.17.1.216” -SplitTunneling
-PluginApplicationID “JuniperNetworks.JunosPulseVpn_cw5n1h2txyewy”
-CustomConfiguration $sourceXml
```

NOTE:

Some VPN Client cmdlet options are not applicable to creating Pulse connections. The following Add-VpnConnection options cause an error if you use them when creating a Pulse connection:

- -AuthenticationMethod
- -EncryptionLevel
- -L2tpPsk
- -MachineCertificateEKUFilter
- -MachineCertificateIssuerFilter
- -UseWinlogonCredential

Add Pulse connection that saves the user credentials after the first login

The -RememberCredentials option applies to smart cards and certificate PINs, and to usernames and passwords.

```
$xml = "<pulse-schema ></pulse-schema>"
$sourceXml=New-Object System.Xml.XmlDocument
$sourceXml.LoadXml($xml)
Add-VpnConnection -Name “PulseCxn2” -ServerAddress “10.17.1.217”
-RememberCredential -PluginApplicationID
“JuniperNetworks.JunosPulseVpn_cw5n1h2txyewy” -CustomConfiguration $sourceXml
```

Add Pulse connection that uses a specified role and realm and a non-standard port

This script’s pulse-schema statement includes schema options that specify the realm and role that are used for this connection. If there are multiple realms or roles available to the user, and you do not specify the preferred values, then the user is prompted for selections.

```
$xml =
"<pulse-schema><port>4444</port><preferredRealm>Users</preferredRealm><preferredRole>TestRole</preferredRole><uri>/local</uri></pulse-schema>"
$sourceXml=New-Object System.Xml.XmlDocument
$sourceXml.LoadXml($xml)
Add-VpnConnection -Name “PulseCxn3” -ServerAddress “10.17.1.216” -SplitTunneling
-RememberCredential -PluginApplicationID
“JuniperNetworks.JunosPulseVpn_cw5n1h2txyewy” -CustomConfiguration $sourceXml
```

Delete Pulse connection

To delete a Pulse connection, use the following command:

```
Remove-VpnConnection -Name <connection_name>
```

Get Pulse connection information

To see the properties of a Pulse connection, use the following command:

```
Get-VpnConnection -Name <connection_name>
```

Start Pulse connection on application launch

You can associate a Pulse connection with an application. When the user starts that application, the specified Pulse VPN connection is initiated.

```
Add-VpnConnectionTriggerApplication -ConnectionName "PulseCxn1" [-ApplicationID]
<String[]>
```

Start Pulse connection when an application attempts to access a specified domain name

You can associate a Pulse connection with a specific DNS suffix to provide connectivity based on location awareness. When the user attempts to access a resource within the suffix, the specified Pulse VPN connection is initiated.

```
Add-VpnConnectionTriggerDnsConfiguration -ConnectionName "PulseCxn1" -DnsSuffix
"juniper.net" -DnsIPAddress "172.28.144.15","172.24.245.15" -PassThru
```

Table 1 on page 11 lists options that you can use in your Pulse connection PowerShell scripts.

Table 1: Schema Options

Option	Description
"port"	Use a connection port other than the standard port, 443.
"uri"	Specifies a sign on policy path override to use when connecting to the server address.
"preferredRealm"	Specify the preferred connection realm. The user must be a member of the specified authentication realm.
"preferredRole"	Specify the preferred role. The user must eligible for the role according to the role mapping rules in effect for the realm.
“optimizeForLowCostNetwork”	true/false Specifies that the connection uses a wired connection if one is available.
“isSingleSignOnCredential”	true/false Specifies that the credentials be used to access resources that require authentication after the tunnel is established.

Related Documentation

- Microsoft Windows In-box Junos Pulse Client Overview on page 3
- Microsoft Windows In-box Junos Pulse Client User Interface on page 5

Viewing Windows In-Box Junos Pulse Client Log Messages

The Windows in-box Pulse client uses the Windows Event Log for logging.

To view Windows in-box Pulse client log messages, perform the following steps:

1. Start the Windows Event Viewer.
2. On the navigation pane, open the following path:

Applications and Service Logs > Microsoft > Windows > VpnPlugInPlatform > OperationalVerbose.

Related Documentation

- Microsoft Windows In-box Junos Pulse Client User Interface on page 5
- Windows PowerShell Script Examples for Microsoft Windows In-box Junos Pulse Client on page 8

PART 2

Index

Index