Pulse Connect Secure

Network Connect to Pulse Desktop Client Migration Guide

Release Number	9.1R2
Published Date	August 2019
Document Version	3.1

Pulse Secure, LLC

2700 Zanker Road, Suite 200
San Jose, CA 95134

http://www.pulsesecure.net

Products made or sold by Pulse Secure or components thereof might be covered by one or more of the following patents that are owned by or licensed to Pulse Secure: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

Pulse Connect Secure Network Connect to Pulse Desktop Migration Guide

Printed in USA.

Revision History

The following table lists the revision history for this document.

Revision	Date	Document Version	Description
9.1R2	August 2019	3.1	9.1R2 Updates
9.1R1	June 2019	3.0	9.1R1 Updates

Contents

Introduction

This document highlights the measures needed for a migration from the Network Connect client to the Pulse Secure Desktop Client.

Follow the steps below to migrate from Network Connect to the Pulse Secure Desktop Client.

Note: This document covers only the migration from Network Connect. This document does not cover client migration in environments where Pulse Secure's NAC (Pulse Policy Secure) and/or 802.1x offerings (Odyssey Access Client) are in use. For migration assistance in such an environment, contact your authorized **Pulse Secure support representative**.

Understanding Product Versioning

This document makes references to various Pulse Connect Secure versions (for example, 9.1R2 which is the latest version of the PCS gateway as of this writing). Network Connect shares the same versioning scheme as the Pulse Connect Secure gateway (e.g., 9.0 PCS contains 9.0 NC, 8.3 PCS contains 8.3 NC, 8.2 PCS contains 8.2 NC, and 8.1 PCS contains 8.1 NC).

The versioning scheme for the Pulse Secure Desktop Client and Pulse Connect Secure is the same in PCS 9.1R2 which contains 9.1R2 PDC. The versioning is different in PCS 8.3 which contains 5.3 PDC, and PCS 8.2 which contains 5.2 PDC.

Understanding Client Differences

Before moving from Network Connect to the Pulse Secure Desktop Client, it is worthwhile to familiarize yourself with feature sets of each. The Pulse Secure Desktop Client is more feature-rich than Network Connect. For more information on feature comparison between NC and PDC refer to Table "Network Connect and Pulse Secure Client Feature Comparison" in the **Pulse Secure Desktop Client Administration Guide**.

Contact your **authorized Pulse Secure support representative** if you have questions about the feature sets of either the Pulse Secure Desktop Client of the Pulse Secure Universal App for Windows.

Creating a Pilot Program with a Test PCS Gateway

For a seamless migration from Network Connect to the Pulse Secure Desktop Client, it is recommended that you designate a pilot group of users and create a test user role which gives these users the option of using the Pulse Secure Desktop Client. Ideally, you will have a staging or test PCS gateway that can be used for testing with a pilot group of users before upgrading a production PCS device.

If the tests go well, you can migrate all the users to the Pulse Secure Desktop Client.

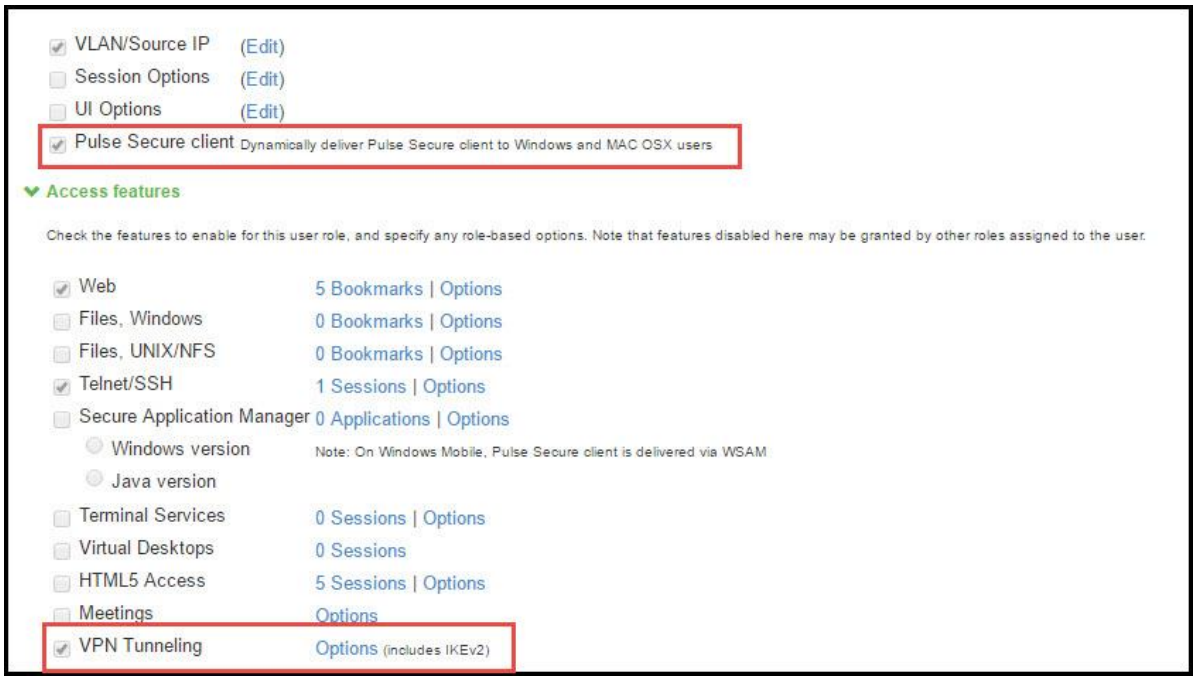
PCS Gateway Configuration: Creating a Pilot Role

On either a test PCS gateway dedicated to the Pulse Desktop pilot, or, on a production PCS gateway, create a role that will enable the Pulse Secure Desktop Client. Details for this can be found in the **Pulse Secure Desktop Client Administration Guide** – especially in "Configuring Pulse Connect Secure" and "Deploying Pulse Secure Client" but here are a few pointers relevant to upgrading from NC to the Pulse Secure Desktop Client:

Generally, you will want to add parallel roles for the Pulse Secure Desktop Client to correspond to all existing roles for NC; that way you can migrate your environment and remove the old NC roles after the last NC client is removed from the endpoints.

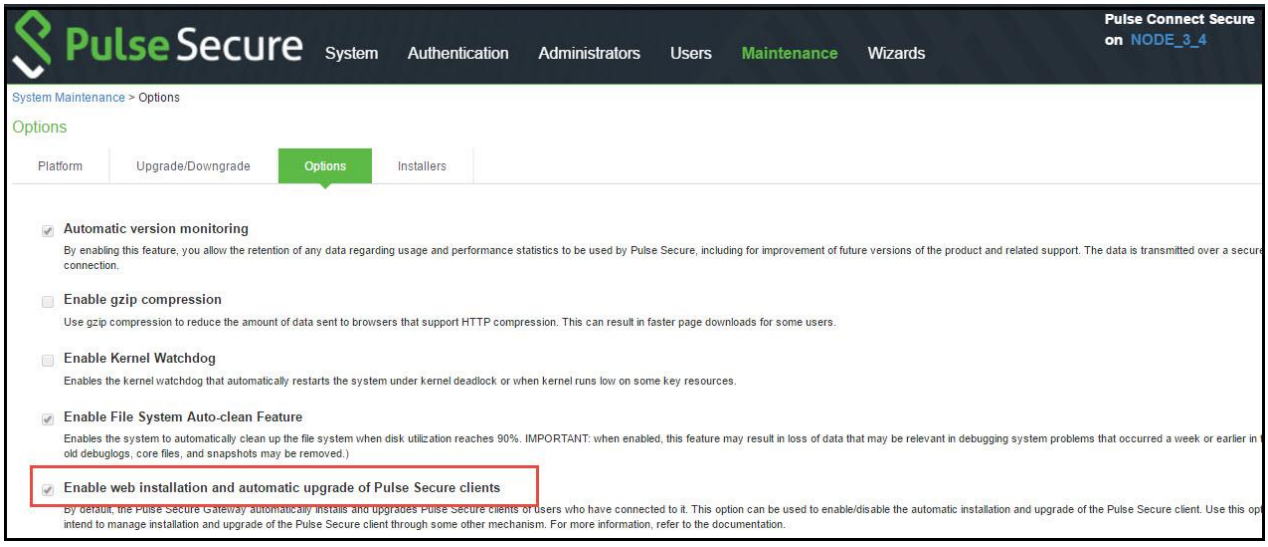
To enable Pulse Secure client for a user role, you must enable the "Pulse Secure client" and "VPN Tunneling" options under the user role, as shown in Figure 1.

Figure 1: User Role



If you will be deploying the Pulse client via a third-party tool like SMS or SCCM, then in the admin console of the PCS gateway, you may wish to uncheck the "Enable web installation and automatic upgrade of Pulse Secure Clients" option as shown in Figure 2. Generally, enterprises choosing SMS/SCCM deployments do so in part to ensure that the Pulse Secure desktop Client remains at a fixed version on all endpoints, regardless of which PCS gateway the endpoint connects to.

Figure 2: Options



Deploying Pulse Desktop Clients to Pilot Users

Once the configuration changes are made on the PCS gateway, you can deploy your clients to your pilot users using the methodology you chose.

Upgrading Your PCS Gateway

Before you migrate to the Pulse Secure Desktop Client, you should ensure that your test/pilot Pulse Connect Secure gateway is running a recent, supported version of the PCS software. As of this writing, the best choice is PCS 9.1R2, although PCS 9.0Rx latest version is an alternative. If you are not using one of these versions (or a version that supplants them) already, then you will need to upgrade your PCS gateway.

There are several factors which need to be considered before we upgrade the PCS gateway and PDC.

New Features in PDC 9.1R2

Please refer to the section Pulse Secure Desktop Client 9.1R2 > Highlighted Features in this Release.

9.1R2 PCS, PPS and PDC What's New Document

Full Rebranding

PCS 9.0Rx is preferred over previous releases because 9.0Rx and later contain clients whose binary objects (filenames, libraries, directory names, code signatures, etc.) have been rebranded to reflect the separation of Pulse Secure, LLC from Juniper Networks, Inc. Upgrading to latest 9.1R2 (rather than older versions) ensures that you don't have to undergo two client migrations (one migration from Network Connect to the Pulse Secure Desktop Client, and a subsequent future migration to a Pulse Secure Desktop Client with new filenames and install paths).

Support for Custom Sign-In Pages

If your organization uses Custom Sign-In pages with Network Connect and if you wish to continue using these pages with the Pulse Secure desktop client, then you will need to upgrade your PCS gateway to 9.1Rx latest version or 9.0Rx. Although support for Custom Sign-In pages was introduced in 8.2R2, we suggest upgrading to 8.3 latest version or 9.1R2 version.

End of engineering and support for 8.2 and 8.3

Please refer https://www.pulsesecure.net/support/eol/software/pulse-connect-secure

Network Connect / Pulse Secure Desktop Client Coexistence

All versions of the Network Connect client and the Pulse Secure Desktop Client have installation co-existence, which means that they can be resident on the same machine at the same time. However, the usage of both installed clients is only supported if the clients are within one release of each other. For example, the 9.1 Pulse Secure Desktop Client (which is shipped with the 9.1 PCS gateway) has runtime existence only with the 9.1 and 9.0 Network Connect clients. As such, if you intend for your end users to be able to run both Network Connect and the Pulse Secure Desktop Client for some period before Network Connect is ultimately uninstalled, then you first must upgrade Network Connect to at least 9.0 if installing the 9.1 Pulse Secure Desktop Client (and you would need to update Network Connect to at least 8.3 if installing the 9.0 Pulse Secure desktop client).

- For more information on client coexistence, see the section titled "Client Interoperability" in the Pulse Secure Desktop Client Supported Platforms Guide associated with the version of the desktop client you wish to install.

- **9.1R2 Pulse Desktop Client Supported Platforms Guide**
- **9.0R4 Pulse Desktop Client Supported Platforms Guide**

Intermediate PCS Gateway Upgrades

When upgrading the PCS gateway, you first must determine whether upgrading directly from your current PCS version to the desired version can be done in one upgrade step, or, whether multiple steps are required. To determine this, see the section called "Upgrade Paths" of the release notes for the version of the PCS gateway you intend to upgrade to. (For example, the 9.1R2 release notes are **here,** and the 9.0R4 release notes are **here**.)

Once the PCS upgrade steps are understood, the PCS gateway (and, if need be, the Network Connect clients) can be upgraded using the guidance given in the appropriate PCS administrator's guide.

Upgrading the Network Connect Client

Once you have updated the PCS gateway software, your pilot end users can connect to the updated PCS to download the latest Network Connect client as an intermediate step.

Note: Neither the 8.1/8.2 Network Connect clients nor the 5.1/5.2 Pulse Secure Desktop Clients support macOS 10.7 and below and Windows XP. As such, if you have these client operating systems in your network, these client operating systems will need to be upgraded before deploying updated Pulse clients. For more information on client supported platforms, refer to the Pulse Secure Desktop Client Supported Platforms Guide.

- **9.1R2 Pulse Desktop Client Supported Platforms Guide**
- **9.0R4 Pulse Desktop Client Supported Platforms Guide**

Determining the Pulse Secure Desktop Client Deployment Methodology

There are two main ways of installing the Pulse Secure Desktop Client on an endpoint machine that already has Network Connect software installed:

- Using a software-distribution mechanism, like SMS/SCCM, to distribute and install the Pulse client
- Using the PCS gateway's "web-deploy" functionality (end users connect to PCS gateway via a web browser and initiate the Pulse Secure Desktop Client installation)

Generally, third-party enterprise-grade software-distribution mechanisms provide tighter control of which endpoints get modified and when, but web-deploy is often the desired mechanism for BYOD ("bring your own device") environments.

Each mechanism is described, below.

Third-Party Deployment Mechanisms

For large enterprise-grade deployments, using a third-party distribution mechanism is often the best choice. In general, the procedure here is to build an installer MSI and pre-configuration file on an appliance with an appropriate Pulse Secure Desktop Client activated package. You can then install the MSI files using command-line options. The Pulse Secure Desktop Client has a rich set of command-line options that can be used to tailor the installation to your needs. For information about these options, see the sections entitled "Installing the Pulse Client Using Advanced Command-Line Options" and "jamCommand Reference" in the **Pulse Secure**

Desktop Client Administration Guide.

For more information on the deployment of the Pulse Secure Desktop Client, refer to the section "Deploying Pulse Secure Client" of the **Pulse Secure Desktop Client Administration Guide**.

PCS Gateway Configuration: Creating a Pulse Secure Desktop Client Connection Set

One important difference between Network Connect and the Pulse Secure Desktop Client is that the later can be pre-configured with a Connection Set, which makes it easier for end users to know which PCS gateways exist and prevents end users from having to know the proper URL(s) associated with a PCS gateway. Configuring a Connection Set is a key element of a Pulse Secure Desktop Client deployment.

For more information on creating Connection Sets, see the section "Pulse Connection Set Options for Pulse Connect Secure" in the **Pulse Secure Desktop Client Administration Guide**.

Considering Best Practices in a Multi-Gateway Environment

If your enterprise has (or will have) multiple Pulse Secure gateways (either Pulse Connect Secure or Pulse Policy Secure), it is best to first understand best practices regarding the management of Connection Sets across multiple Pulse Secure gateways.

When a Pulse Secure Desktop Client is deployed, that client receives an initial Connection Set that is associated ("bound") to a Server ID. This means that the client will get Connection Set updates upon connection to a gateway only if the Server ID of the gateway's Connection Set matches the Server ID of Connection Set that the client was initially bound to.

In other words, if a client is deployed with a Connection Set associated with gateway "X" (i.e., having the Server ID of X), and then if the client later connects to a gateway "Y" that contains a Connection Set associated with gateway "Y" (i.e., having the Server ID of Y), then the client will not receive the Connection Set from Y – even if Y's Connection Set differs from X's. This outcome may be desirable or undesirable, depending on your objectives.

If your objective is to ensure that Connection Sets are consistent across all your gateways, then it is recommended that you modify your Connection Sets in the following way:

1. Designate one gateway as the primary gateway, and make all Connection Set changes on that primary gateway.
2. Move that Connection Set to the other gateways – either through the gateways' XML export and import functionality, or, through the gateways' "Push Config" mechanism.

This approach will ensure that Connection Sets on all gateways are identical and share the same Server ID, regardless of which gateway a client connects to.

Note: PCS 8.2r3 (and the embedded Pulse Secure Desktop Client 5.2r3) contain several improvements and visual indicators to simplify the management of Server IDs in multi-gateway environments. For more information on this, consult the section titled "Improved Large-scale Configuration Deployment and Diagnosis" in the 5.2r3 Pulse Secure Desktop Client release notes, which can be found **here**.

Important Changes

Embedded Browser for SAML

After migration from Network Connect to the Pulse Secure Desktop Client, if your Pulse environment uses Security Assertion Markup Language (SAML) for a Single Sign-on (SSO) authentication environment,

- Pulse user sees an embedded browser if Enable embedded browser for authentication is enabled in Pulse Secure Connection Set Options.

  Pulse client will close the embedded browser, once the SAML authentication is done.
- Otherwise, Pulse user sees an external web browser.

Web Browser for Custom Sign-In Pages

After migration from Network Connect to the Pulse Secure Desktop Client, if your Pulse environment uses Custom Sign-In pages for authentication, the Pulse user sees an external web browser or embedded web browser.

Pulse user sees an embedded browser if **Enable embedded browser for authentication** check box is enabled in Pulse Secure Connection Set Options.

Pulse user sees an external browser if **Enable embedded browser for authentication** check box is disabled in Pulse Secure Connection Set Options.

For more information, refer to "Pulse Secure Connection Set Options" and "Custom Sign-in Page in Embedded browser" sections in **Pulse Desktop Client Administration Guide.**

Disable client-side proxy settings

Pulse Desktop Client will not support the do not allow client proxy. However, Pulse Desktop Client Has Disable client-side proxy settings alternative for this feature.

- do not allow client proxy

  This feature allows the user to prevent a VPN Tunneling tunnel from being created when a client proxy is present. Error 30572, "*VPN Tunneling unable to connect because a client proxy is not allowed*", appears if the user tries to start a VPN Tunneling tunnel. This option is applicable only when you use a VPN Tunneling client. If you are using a Pulse Secure client, this option is ignored.

  For more information refer to the section 'Defining VPN Tunneling Role Settings' section in **Pulse Connect Secure Administration Guide**.
- Disable client-side proxy settings

  This feature is alternative to the do not allow client proxy feature

Machine Authentication in Pulse Client

Pulse Desktop Client will not support the Logoff on Connect. However, Pulse Desktop Client has Machine Authentication in Pulse Client alternative for this feature.

- Logoff on Connect

  This feature allows the user to authenticate against a Windows Domain server in real time, as opposed to authenticating with the locally cached credentials. When this feature is enabled, they are automatically logged off Windows after the VPN tunneling session starts. The standard Windows login screen re-appears and they log in using their Windows credentials. Their Windows environment is now established through the VPN tunnel.

For more information refer to the section '*Logging In To Windows Through a Secure Tunnel*' section of **Pulse Connect Secure Administration Guide**.

- Machine Authentication in Pulse Client

  This feature is alternative to the Logoff On Connect feature.

  Machine authentication uses machine credentials (machine name and password or machine certificate) to authenticate the endpoint.

  For more information, refer to '*Machine Authentication for Pulse Connect Secure Overview*' in **Pulse Desktop Client Administration Guide.**

Determining Plan for Removing Network Connect

As stated above, the Pulse Secure desktop client and the Network Connect client can peacefully co-exist on an endpoint machine. As such, it is not required to remove Network Connect before (or, immediately after) the Pulse Secure Desktop Client is installed. But, at some point after the Pulse Secure Desktop Client has been installed and has been shown to operate correctly, you will want to uninstall the Network Connect client to reduce end-user confusion and clutter. You can uninstall Network Connect at any time you wish.

The preferred mechanism for Windows users is to manually push out a batch file that runs the uninstallation program. The following are command-line examples of how to invoke the uninstall programs:

NC 8.1

C:\Program Files (x86)\Juniper Networks\Network Connect 8.1>"uninstall.exe" /S _?=C:\Program Files (x86)\Juniper Networks\Network Connect 8.1

NC 8.2

C:\Program Files (x86)\Pulse Secure\Network Connect 8.2>"uninstall.exe" /S _?=C:\Program Files (x86)\Pulse Secure\Network Connect 8.2

NC 8.3

C:\Program Files (x86)\Pulse Secure\Network Connect 8.3>"uninstall.exe" /S _?=C:\Program Files (x86)\Pulse Secure\Network Connect 8.3

NC 9.0

C:\Program Files (x86)\Pulse Secure\Network Connect 9.0>"uninstall.exe" /S _?=C:\Program Files (x86)\Pulse Secure\Network Connect 9.0

For macOS users, the best procedure for removing the Network Connect client is given in the following KB:

https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB16265

Going Live with Your Production PCS Gateways

Once any issues are resolved in the Pilot program, production PCS gateways can be configured in an analogous way to deploy the Pulse Secure Desktop Client to your entire enterprise.

Ongoing Maintenance of Your Pulse Secure

Ecosystem

The network and endpoint ecosystem in your enterprise is likely constantly changing:

- New endpoint operating system versions are introduced and patched.
- New network configuration best practices and improved security algorithms are introduced to reflect a changing malware and threat landscape.

To maximize the efficiency and effectiveness of your Pulse Secure secure-connectivity solution within this dynamic ecosystem, it is highly recommended that you:

- Upgrade both your clients and your servers with the latest Pulse Secure maintenance releases in a timely manner.
- Ensure that clients and servers within one revision of each other (for example, if you are running the 9.1R2 Pulse Secure Desktop Client, it is not suggested to have a PCS version less than 8.3).