Pulse Secure

Pulse Connect Secure

Network Connect to Pulse Desktop Migration Guide

Published Date **June 2016**

SUMMARY

This article highlights the measures needed for a phased migration from the Network Connect client to the Pulse Secure desktop client.

Follow the steps below in order 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, 8.2 and 8.1, which are the latest versions of the PCS gateway as of this writing). Network Connect shares the same versioning scheme as the Pulse Connect Secure gateway (e.g., 8.2 PCS contains 8.2 NC, and 8.1 PCS contains 8.1 NC).

The versioning scheme for the Pulse Secure desktop client differs from that of PCS and NC. By default, PCS 8.2 contains the 5.2 desktop client, and PCS 8.1 contains the 5.1 desktop client.

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. Although the Pulse Secure desktop client is more feature-rich than Network Connect, there are a few features in Network Connect that were not migrated to the Pulse Secure desktop client. For a full accounting, refer to Table 13 (on page 172) in the Pulse Secure Desktop Client Admin Guide.

Also note that Pulse Secure, LLC offers a lightweight app-store app for Windows 10 devices. This app is called the "Universal" app because it runs on all Windows 10 devices – including desktops and mobile devices (phones). Although the Universal App provides only a subset of the capability of the full Pulse Secure desktop client, the Universal App is as easy to deploy as any Windows Store app-store app. The Pulse Secure Universal App is highly recommended for organizations whose needs can be met by it. You can learn more about the Universal App in its Release Notes and Quick Start 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 there is no test or staging PCS gateway, then you can upgrade your production PCS gateway, upgrade Network Connect as needed, and then create a role for a pilot group of Pulse client users which gives these users option of using and testing Pulse Secure client. If tests go well, you can migrate all the users to the Pulse Secure desktop client.

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 8.2r3, although PCS 8.1r9 is an alternative choice. 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 to consider when determining what version of the PCS to upgrade to:

Full Rebranding

PCS 8.2r3 is preferred (over 8.1r9) because 8.2 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 8.2 (rather than 8.1) 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 PCS 8.2r2 or later. For more information on Pulse Secure desktop client support for Custom Sign-In pages, see the section entitled "Support for Custom Sign-In Pages" in the 5.2r2 Pulse Secure Desktop Client Release Notes.

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 5.2 Pulse Secure desktop client (which is shipped with the 8.2 PCS gateway) has runtime existence only with the 8.2 and 8.1 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 8.1 if installing the 5.2 Pulse Secure desktop client (and you would need to update Network Connect to at least 8.0 if installing the 5.1 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. (The 5.2 guide is here, and the 5.1 guide is here.)

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" in Table 2 of the release notes for the version of the PCS gateway you intend to upgrade to. (For example, the 8.2r2 release notes are here, and the 8.1r1 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 that neither the 8.1/8.2 Network Connect clients nor the 5.1/5.2 Pulse Secure desktop clients support Mac OS X 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.

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, 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 Admin Guide.

Web Deployment

Whether you can choose the web-deploy deployment methodology depends on two factors:

- Whether your end users have administrative privileges on their endpoint devices
- What version of the PCS gateway they will be connecting to

If your end users have administrative credentials on their endpoint devices, then web-deploy is a possible deployment mechanism. But if your end users are **restricted**, then there are two caveats:

- If you wish to **web deploy** the Pulse Secure desktop client from an **8.1** PCS gateway, you'll want to upgrade to PCS 8.1r9 or later, due to a bug in 8.1R8 that caused restricted users to be prompted for admin credentials during the upgrade. Note: Web deployment of the desktop client from an 8.1 PCS gateway to restricted users is possibly only if the endpoints already have the Pulse Secure Installer Service installed.
- You cannot web-deploy a fresh installation of the Pulse Secure desktop client from an **8.2** PCS gateway if your users are **restricted users**. In this case, you must use a software-distribution mechanism to deploy the Pulse client.

Note that you can have multiple versions of the Pulse Secure desktop client package hosted on a particular PCS gateway, and you can configure which one is activated for your users. This allows you to upgrade a PCS gateway and ensure that a new Pulse Secure desktop client is not deployed until you are ready to do so.

For More Information

Please note that more information on the deployment of the Pulse Secure desktop client can be found in Chapter 6 ("Deploying Pulse Secure Client") on page 133 of the Pulse Secure Desktop Client Administrator's 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 latter 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 titled "Pulse Connection Set Options for Pulse Connect Secure" in the Pulse Secure Desktop Client Admin 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 particular 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.

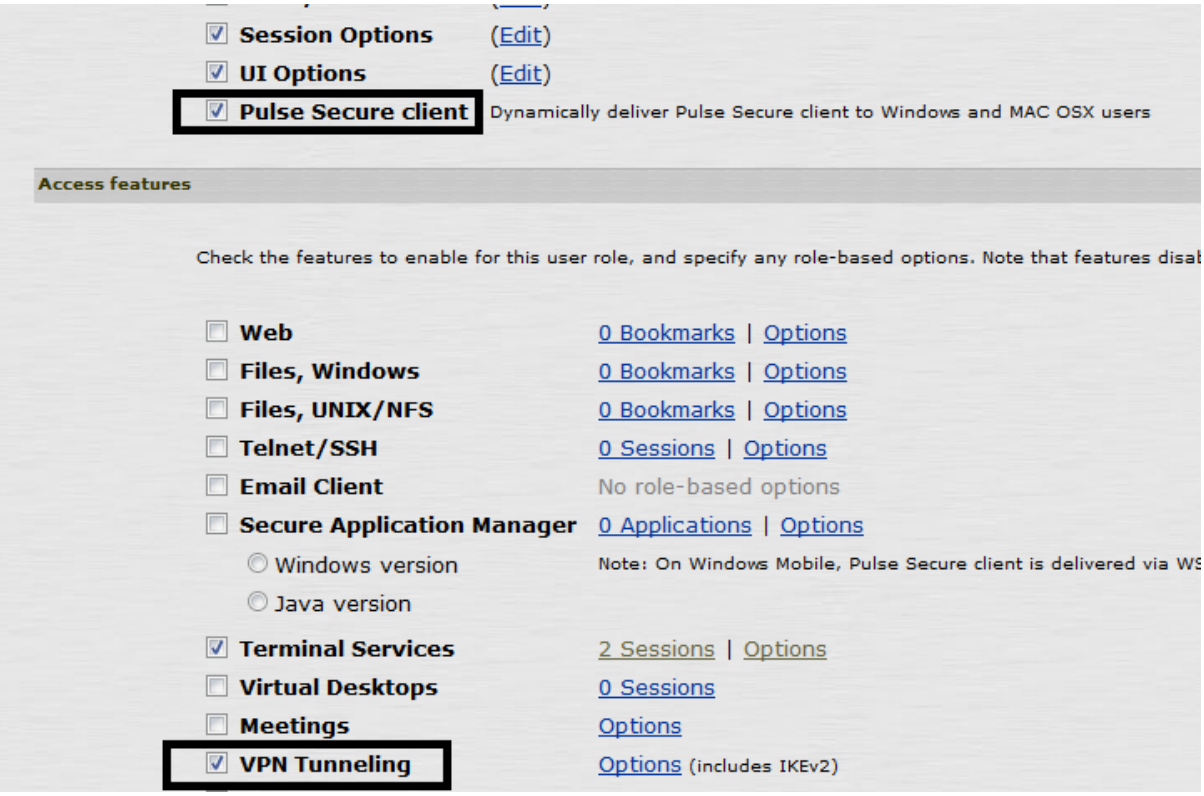
Note that PCS 8.2r3 (and the embedded Pulse Secure desktop client 5.2r3) contain several improvements and visual indicators to simplify the management of Server IDs in multi-gateway environments. For more information on this, consult the section titled "Improved Large-scale Configuration Deployment and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

PCS Gateway Configuration: Creating a Pilot Role

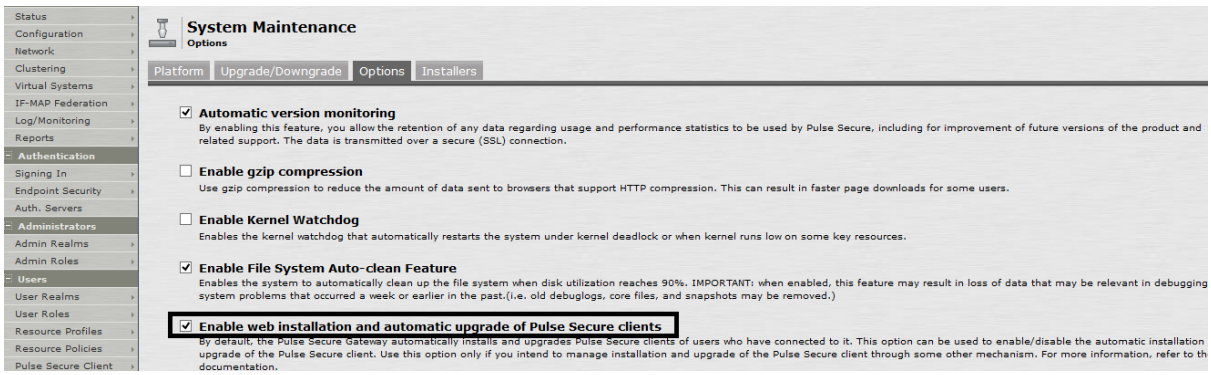
On either a test PCS gateway dedicated to the Pulse Desktop pilot, or, on a production PCS gateway, create a role that will enable the Pulse Secure desktop client. Details for this can be found in the Pulse Secure desktop client administrator's guide – especially in Chapter 3 ("Configuring Pulse Connect Secure") and Chapter 6 ("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 the figure below:



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 (see pages 119-120 in the Pulse Secure Desktop Client Administrator's Guide for details). 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.



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.

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:

7.1

C:\Program Files (x86)\Juniper Networks\Network Connect 7.1.16>"uninstall.exe" /S _?=C:\Program Files (x86)\Juniper Networks\Network Connect 7.1.16

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

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

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

https://kb.pulsesecure.net/articles/Pulse_Secure_Article/how-to-manually-remove-network-connect-in-mac-os-x-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.

In order 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 (e.g., if you are running the 5.2 Pulse Secure desktop client, do not have a version of the Pulse Connect Secure gateway earlier than 8.1).