Pulse Secure®

Pulse Connect Secure

WSAM to Pulse SAM Migration Guide

Release Number	9.0R1
Published Date	July, 2018
Document Version	1.0

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.

Contents

Introduction

This document highlights the measures needed for the migration from WSAM to the Pulse SAM client.

Follow the document to migrate from WSAM to the Pulse SAM client.

Note: In this document, we will be using terms "Pulse SAM Client" and "Pulse Desktop Client", it is the same as the Pulse SAM client is Pulse Desktop client with WSAM tunneling enabled.

Understanding Product Versioning

This document makes references to various Pulse Connect Secure versions (for example, 9.0R1 which is the latest version of the PCS gateway as of this writing). WSAM shares the same versioning scheme as the Pulse Connect Secure gateway (for example 9.0 PCS contains 9.0 WSAM, 8.3 PCS contains 8.3 WSAM, 8.2 PCS contains 8.2 WSAM and 8.1 PCS contains 8.1 WSAM).

The versioning scheme for the PCS and Pulse SAM client will be same with PCS 9.0R1 onwards which contains 9.0R1 client whereas PCS 8.3 contains the 5.3 Client, and PCS 8.2 contains the 5.2 Client.

Understanding Client Differences

Before moving from WSAM to the Pulse Secure desktop client, it is worthwhile to familiarize yourself with feature sets of each. The Pulse SAM client has all the features of WSAM.

Since it is built in within the Pulse Desktop client, the advantage of migrating to Pulse SAM Client is that we can add multiple connections to multiple PCS gateways. Also, all future enhancements are planned for the Pulse SAM Client.

Figure: WSAM Interface

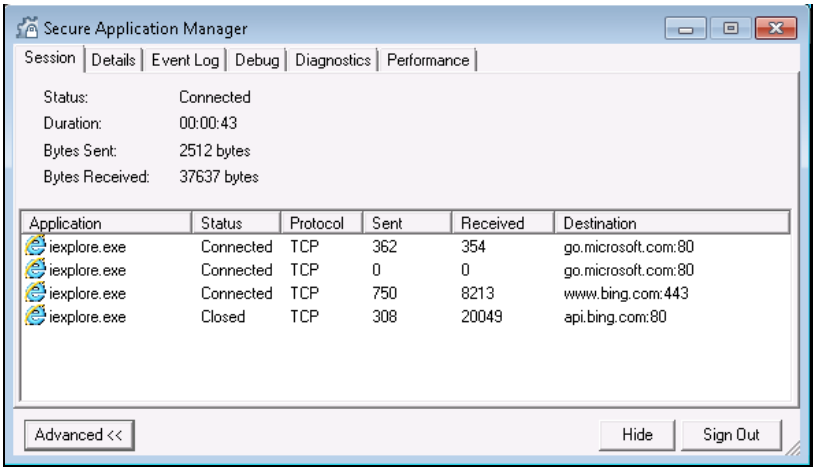
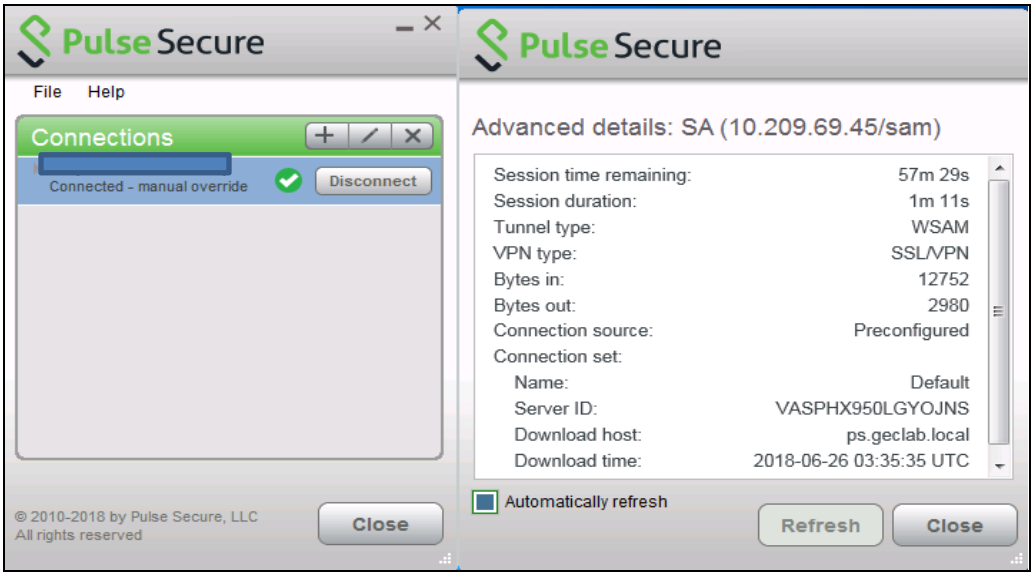


Figure: Pulse SAM Interface



Creating a Pilot Program with a Test PCS Gateway

For a seamless migration from WSAM to the Pulse SAM 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 SAM client. It is ideal that you 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 WSAM as needed, and then create a role for a pilot group of Pulse SAM client users which gives these users option of using and testing Pulse SAM client. If tests go well, you can migrate all the users to the Pulse SAM client.

PCS Gateway Configuration: Creating a Pilot Role

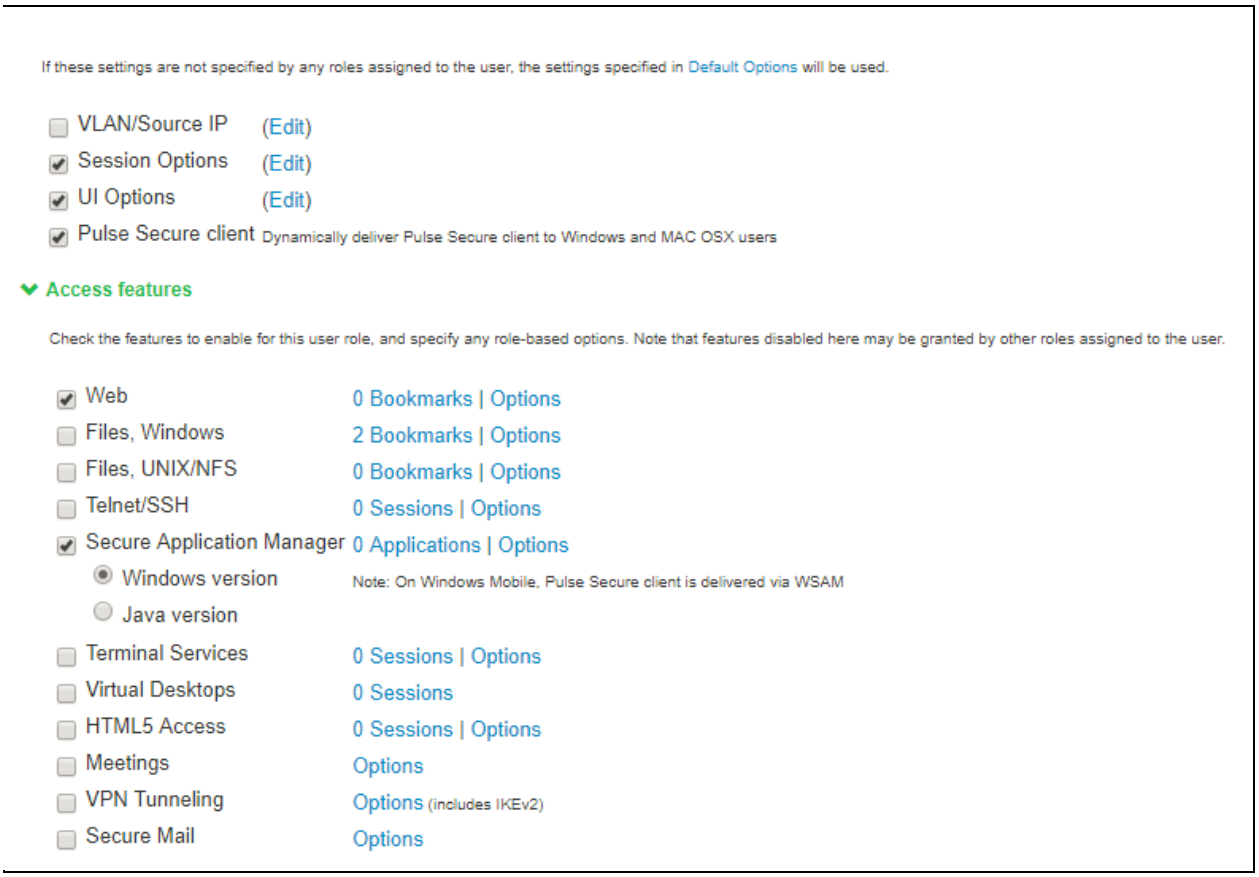
On either a test PCS gateway dedicated to the Pulse SAM pilot, or, on a production PCS gateway, create a role that will enable the Pulse SAM client. For more information refer to **Pulse Secure desktop client administration guide** – especially in section "Configuring Pulse Secure client for Secure Application Manager".

Generally, you would require to add parallel roles for the Pulse SAM client to correspond to all existing roles for WSAM; that way you can migrate your environment and remove the old WSAM roles after the last WSAM client is removed from the endpoints.

To enable Pulse SAM Client for a user role, you must enable the "Pulse Secure client" and "Secure Application Manager" options under the user role (refer **Figure: User Role**)

If "Pulse Secure client" is not checked, the role uses legacy WSAM. If VPN tunneling is also checked, it uses VPN tunneling (L3 VPN) instead of Pulse SAM so make sure VPN tunneling is unchecked.

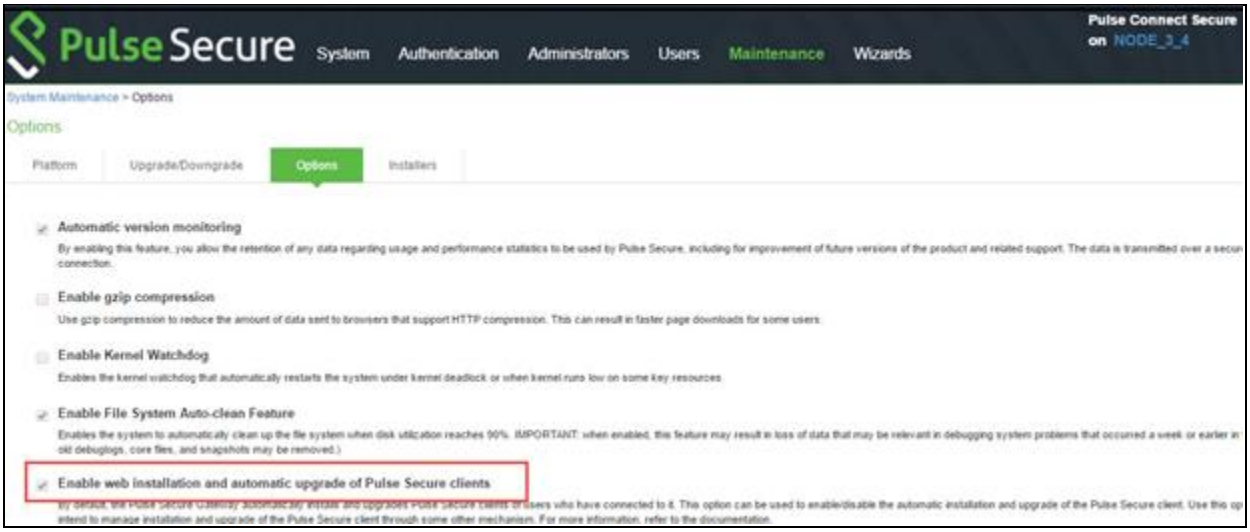
Figure: User Role



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 (refer **Figure: Options**).

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: 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 SAM 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 9.0R1, although PCS 8.3 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.

Note: It is suggested to upgrade to latest maintenance releases of 8.3 and 9.0 available on the support portal when you plan to start the migration.

There are some factors which need to be considered before we upgrade the PCS gateway and Pulse SAM Client.

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 9.0R1 (rather than older versions) ensures that you do not have to undergo two client migrations (one migration from WSAM to the Pulse SAM client, and a subsequent future migration to a Pulse SAM client with new filenames and install paths).

WSAM / Pulse SAM Client Coexistence

All versions of WSAM and the Pulse SAM client have installation co-existence, which means that they can be resident on the same machine at the same time.

Note: Both clients cannot run at the same time.

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 9.0R1 guide is **here**, and the 5.3R4 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 "Upgrade Paths" section of the release notes for the version of the PCS gateway you intend to upgrade to. For example, the 9.0R1 release notes are **here**, and the 8.3R5 release notes are **here**.

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

Upgrading WSAM

Once you have updated the PCS gateway software, your pilot end users can connect to the updated PCS and upgrade WSAM as an intermediate step.

Server, Platform and Browser Compatibility

For more information on supported platforms, refer to the Pulse Secure Desktop Client Supported Platforms Guide.

https://www.pulsesecure.net/download/techpubs/current/1164/pulse-client/pulse-secure-client-desktop/5.3rx/ps-pulse-5.3r4-supportedplatforms.pdf

https://www.pulsesecure.net/download/techpubs/current/1210/pulse-client/pulse-secure-client-desktop/9.0rx/ps-pulse-9.0r1-supportedplatforms.pdf .

Determining the Pulse Secure Desktop Client Deployment Methodology

There are two main ways of installing the Pulse SAM client on an endpoint machine that already has WSAM 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)

For More Information

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

Note: the section "Installing the Pulse Secure Client on Windows Endpoints Using a Preconfiguration File" does not apply for Pulse SAM and only applies to L3 VPN connections.

Determining Plan for Removing WSAM

As stated above, the Pulse SAM Client and WSAM can peacefully co-exist on an endpoint machine. As such, it is not required to remove WSAM 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 WSAM to reduce end-user confusion and clutter. You can uninstall WSAM at any time you wish.

You can remove WSAM by running the UninstallSAM.exe

WSAM 8.1 and 8.2

C:\Program Files (x86)\Juniper Networks\ Secure Application Manager>" UninstallSAM.exe"

WSAM 8.3 and 9.0

C:\Program Files (x86)\Pulse Secure\ Secure Application Manager >" UninstallSAM.exe"

WSAM can also be uninstalled under Add/Remove programs if user has privileges.

Going Live with Your Production PCS Gateways

For any issues found during Migration, open a **support case**.

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 (e.g., if you are running the 5.3 Pulse Secure desktop client, it is not suggested to have a PCS version less than 8.2 and if you are running the 9.0R1 Pulse Secure desktop client, it is not suggested to have a PCS version less than 8.3)