



# Pulse Connect Secure

WSAM to Pulse SAM Migration Guide

Pulse Secure, LLC  
2700 Zanker Road, Suite 200 San  
Jose, CA 95134

<http://www.pulsesecure.net>

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

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

Copyright © 2020, Pulse Secure, LLC. All rights reserved.

Printed in USA.

# Revision History

The following table lists the revision history for this document.

Date	Document Version	Description
October 2020	2.4	Removed Note from Determining the Pulse Secure Desktop Client Deployment Methodology.
October 2019	2.3	Updated "Upgrading Your PCS Gateway", "WSAM / Pulse SAM Client Coexistence" and "Determining Plan for Removing WSAM" sections.
October 2019	2.2	Updated "WSAM / Pulse SAM Client Coexistence" and "Determining Plan for Removing WSAM" sections.
August 2019	2.1	9.1R2 Updates
June 2019	2.0	9.1R1 Updates

# Contents

Revision History.....	3
Introduction.....	5
Understanding Product Versioning.....	5
Understanding Client Differences.....	5
Creating a Pilot Program with a Test PCS Gateway.....	6
PCS Gateway Configuration: Creating a Pilot Role.....	6
Deploying Pulse Desktop Clients to Pilot Users.....	8
Upgrading Your PCS Gateway.....	8
Full Rebranding.....	8
WSAM / Pulse SAM Client Coexistence.....	8
Intermediate PCS Gateway Upgrades.....	8
Upgrading WSAM.....	8
Determining the Pulse Secure Desktop Client Deployment Methodology.....	9
For More Information.....	9
Determining Plan for Removing WSAM.....	9
Going Live with Your Production PCS Gateways.....	10
Ongoing Maintenance of Your Pulse Secure Ecosystem.....	10

## 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, 9.1R2 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 Pulse SAM client, we suggest, PCS and Pulse SAM client versions should be within two versions of each other. For example, if we are running Pulse SAM client 9.1R2 or 9.0Rx latest version, PCS version should be minimum 8.3Rx.

## 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

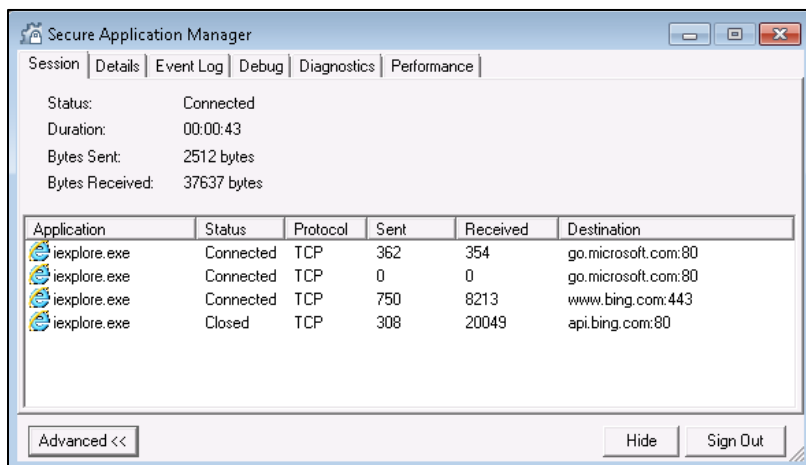
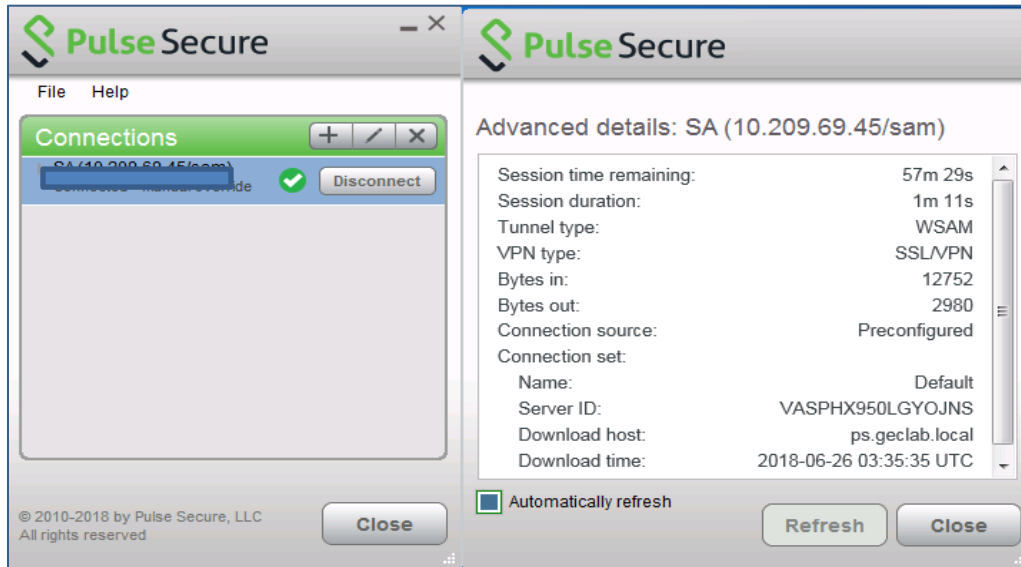


Figure: Pulse SAM Interface



## 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 the 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 these settings are not specified by any roles assigned to the user, the settings specified in [Default Options](#) will be used.

- VLAN/Source IP [\(Edit\)](#)
- Session Options [\(Edit\)](#)
- UI Options [\(Edit\)](#)
- Pulse Secure client [Dynamically deliver Pulse Secure client to Windows and MAC OSX users](#)

▼ Access features

Check the features to enable for this user role, and specify any role-based options. Note that features disabled here may be granted by other roles assigned to the user.

- Web [0 Bookmarks | Options](#)
- Files, Windows [2 Bookmarks | Options](#)
- Files, UNIX/NFS [0 Bookmarks | Options](#)
- Telnet/SSH [0 Sessions | Options](#)
- Secure Application Manager [0 Applications | Options](#)
  - Windows version Note: On Windows Mobile, Pulse Secure client is delivered via WSAM
  - Java version
- Terminal Services [0 Sessions | Options](#)
- Virtual Desktops [0 Sessions](#)
- HTML5 Access [0 Sessions | Options](#)
- Meetings [Options](#)
- VPN Tunneling [Options \(includes IKEv2\)](#)
- Secure Mail [Options](#)

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

Pulse Secure System Authentication Administrators Users Maintenance Wizards

System Maintenance > Options

Options


- Automatic version monitoring  
By enabling this feature, you allow the retention of any data regarding usage and performance statistics to be used by Pulse Secure, including for improvement of future versions of the product and related support. The data is transmitted over a secure connection.
- Enable gzip compression  
Use gzip compression to reduce the amount of data sent to browsers that support HTTP compression. This can result in faster page downloads for some users.
- Enable Kernel Watchdog  
Enables the kernel watchdog that automatically restarts the system under kernel deadlock or when kernel runs low on some key resources.
- Enable File System Auto-clean Feature  
Enables the system to automatically clean up the file system when disk utilization reaches 90%. IMPORTANT: when enabled, this feature may result in loss of data that may be relevant in debugging system problems that occurred a week or earlier in old debuglogs, core files, and snapshots may be removed.)
- Enable web installation and automatic upgrade of Pulse Secure clients  
By default, the Pulse Secure gateway automatically installs and upgrades Pulse Secure clients on users who have connected to it. This option can be used to enable/disable the automatic installation and upgrade of the Pulse Secure client. Use this option to manage installation and upgrade of the Pulse Secure client through some other mechanism. For more information, refer to the documentation.

# 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 9.1R2, 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.

 **Note:** It is suggested to upgrade to latest maintenance releases of 9.1 which is available on the support portal when you start the migration, as 9.0 is end of engineering (EoE) in October.

<https://support.pulsesecure.net/product-service-policies/eol/software/pulse-connect-secure-software-dates-milestones/>.

## Full Rebranding

PCS 9.0Rx latest version and above 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 9.0Rx and later versions (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

Since WSAM uses TDI drivers and Pulse SAM in 9.1R1 and above uses WFP drivers, having both the drivers installed could cause issues with tunneling. Hence, it is suggested to uninstall the older WSAM drivers before migrating to Pulse SAM 9.1R1.

WSAM/Pulse Desktop Client 9.0Rx and below uses TDI (jnprTdi\_824\_597.sys) driver signed by sha1.  
Pulse Desktop Client 9.1R1 and above uses WFP (jnprTdi\_911\_607.sys) driver signed by sha2.

## 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 9.1R2 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, 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.

- [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 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](#).

## Determining Plan for Removing WSAM

You can remove WSAM by running the UninstallSAM.exe via a script file that can be run locally or as a session start script under **User Roles > SAM options**.

### WSAM 8.1 and 8.2

```
echo Secure Application Manager Uninstallation
start "Secure Application Manager" /W "C:\Program Files (x86)\Juniper Networks\Secure Application Manager\UninstallSAM.exe
```

UninstallSAM.exe location

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

### WSAM 8.3 and above

```
echo Secure Application Manager Uninstallation
start "Secure Application Manager" /W "C:\Program Files (x86)\Pulse Secure\Secure Application Manager\UninstallSAM.exe
```

UninstallSAM.exe location

```
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.