Pulse Secure Windows Hello for Business

Deployment Guide

Document Revision	1.0
Published Date	January 2020

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

https://www.pulsesecure.net

Pulse Secure Windows Hello for Business - Deployment Guide

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

END USER LICENSE AGREEMENT

Revision History

Revision and Date	Added/Updated/Removed	Remarks
1.0, January 2020	NA	Initial publication for 9.1R4 release

Table of Contents

Overview

On a Windows Hello for Business (WHFB) registered Windows client under the certificate trust model, a Pulse end user can make use of the same WHFB certificate to log in to Pulse Connect Secure (PCS) without the need to enter the user name and password.
The WHFB users who meet the following requirements will be allowed to authenticate with PCS without a username/password by using the WHFB credentials.

- PCS supports WHFB with certificate trust model.
- PCS uses the WHFB certificate to allow authentication to PCS.
- This model works only for Windows client.
- This model works with Pulse Desktop client (PDC).
- This model works only on those Windows versions that are Azure Active Directory Joined (AADJ).
- Browsers supported – Microsoft IE, Microsoft Edge and Chrome with Microsoft WHFB extension.

Hardware and Software Requirements

PCS needs a way to sign-in with WHFB credentials for all the registered Windows users with Certificate trust model. This model requires the following:

- Microsoft Network Device Enrollment Service (NDES) server. This can be deployed On-premises or in Cloud.
- Active Directory (AD) and Certificate Authority (CA) server. This can be in On-premises or in Cloud.

Prerequisites

You need to set up Certificate Trust model based on the deployment scenario.

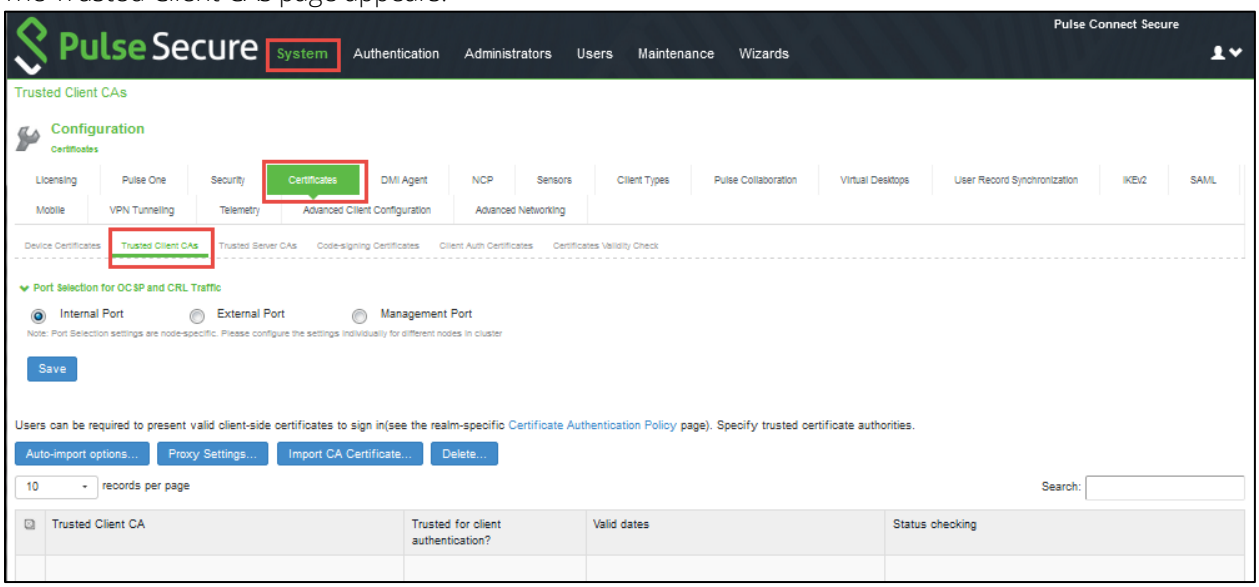
1. For hybrid AADJ certificate trust deployment, refer to the Microsoft document at https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-hybrid-cert-trust.
2. For AADJ single sign-on deployment, refer to the Microsoft document at: https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-hybrid-aadj-sso.
3. To configure AADJ devices for on-premises single sign-on using WHFB, refer to the Microsoft document at: https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-hybrid-aadj-sso-base
4. To use certificates for AADJ on-premises single sign-on, refer to the Microsoft document at: https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-hybrid-aadj-sso-cert.
5. To set up Azure portal to achieve automatic enrolment to Intune, refer to the Microsoft document at: https://docs.microsoft.com/en-us/intune/enrollment/windows-enroll.

Configuring PCS

Once you have configured the certificate trust model, a certificate is issued by the CA server used in the configuration. You need to upload this certificate to the Trusted Client store.
To upload the certificate, do the following:

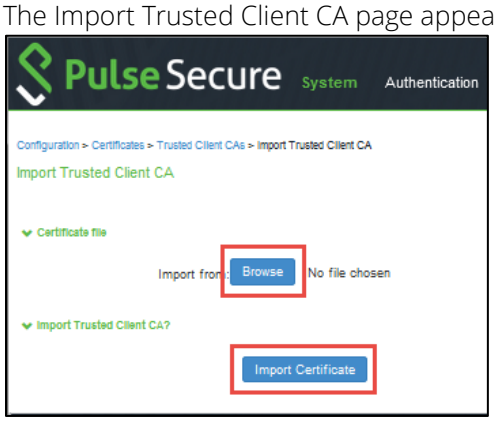
1. In the PCS admin console, select the **System** menu, and then select **Configuration > Certificates > Trusted Client CA**.

   The Trusted Client CAs page appears.



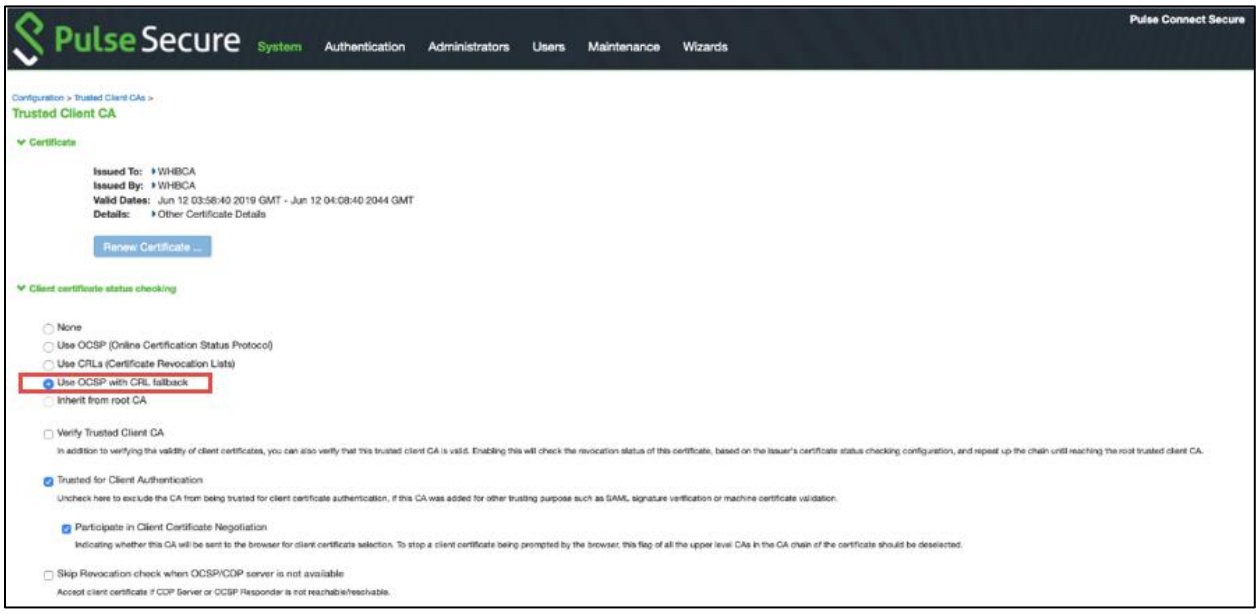
2. Click **Import CA Certificate**.

   The Import Trusted Client CA page appears.



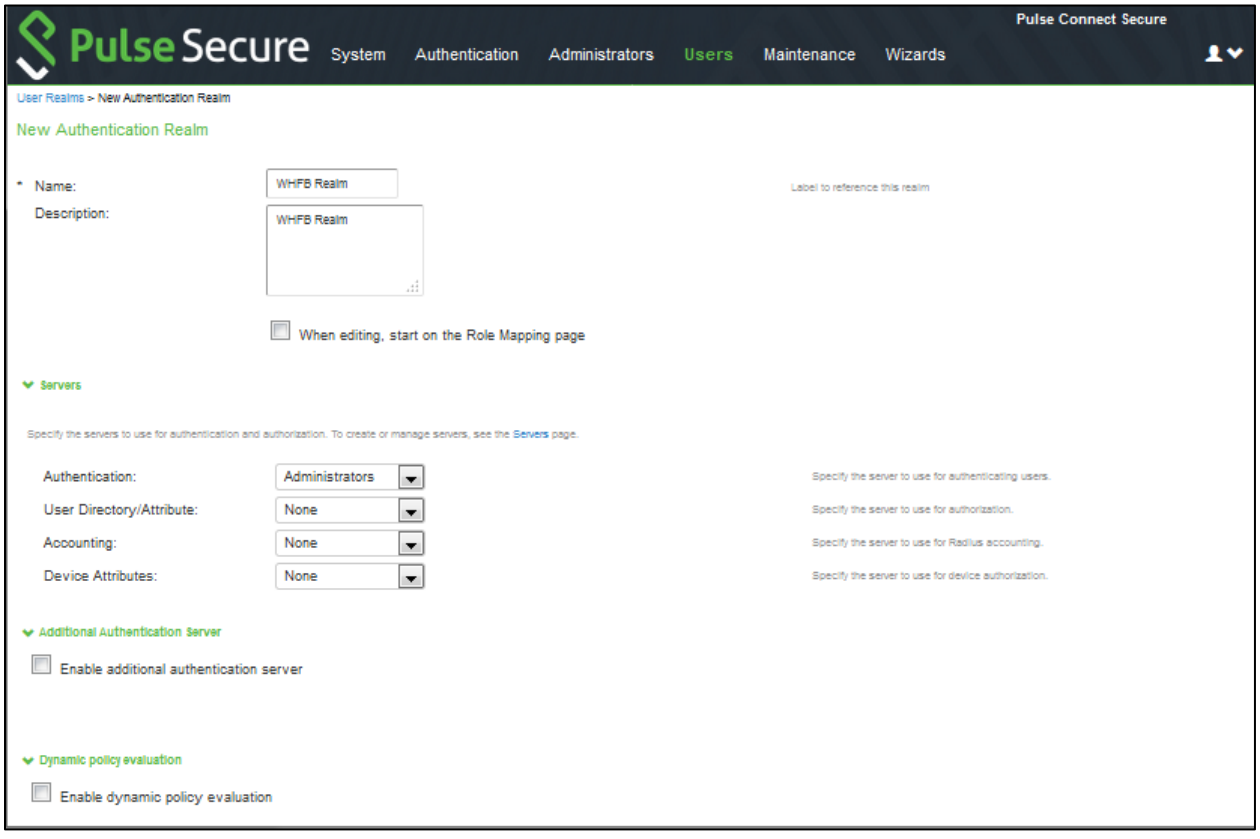
3. Under Certificate file section, click **Browse** and locate your CA client certificate file.
4. Under Import Trusted Client CA? section, click **Import Certificate**.

5. While importing the certificate, ensure that the CRL checks are enabled.



The CA client certificate is added to the list of Trusted Client CAs.

6. Now, create a cert auth realm for WHFB by navigating to Users > User Realms > New User Realm.



User Workflow

A WHFB user needs to join Azure AD domain to connect to PCS.

1. Log in with the WHFB user name.
2. In the WHFB registration page that is displayed, enter the necessary details.
3. Log in using the WHFB credentials that was set during the WHFB registration.
4. If not already installed, install Pulse Client from the web page.
5. Connect to the WHFB realm.
    - This time, authentication happens with the Certificate, which is pushed for WHFB users signed by the CA and uploaded in the PCS.
    - The user will not be prompted for any username or password.

Browser-based Flow

A WHFB user can use IE browser to connect to PCS. During the connection, the user will be prompted with a certificate prompt to log in.

Only IE browser and Chrome browser with WHFB extension are supported for WHFB. But Firefox is not supported for WHFB.

References

WHFB documentation at: https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-identity-verification

Requesting Technical Support

Technical product support is available through the Pulse Secure Global Support Center (PSGSC). If you have a support contract, then file a ticket with PSGSC.

- Product warranties—for product warranty information, visit https://www.pulsesecure.net.