IBM Security Verify Privilege Vault

Quick Start Guide

This guide describes a quick way to get started with the product.

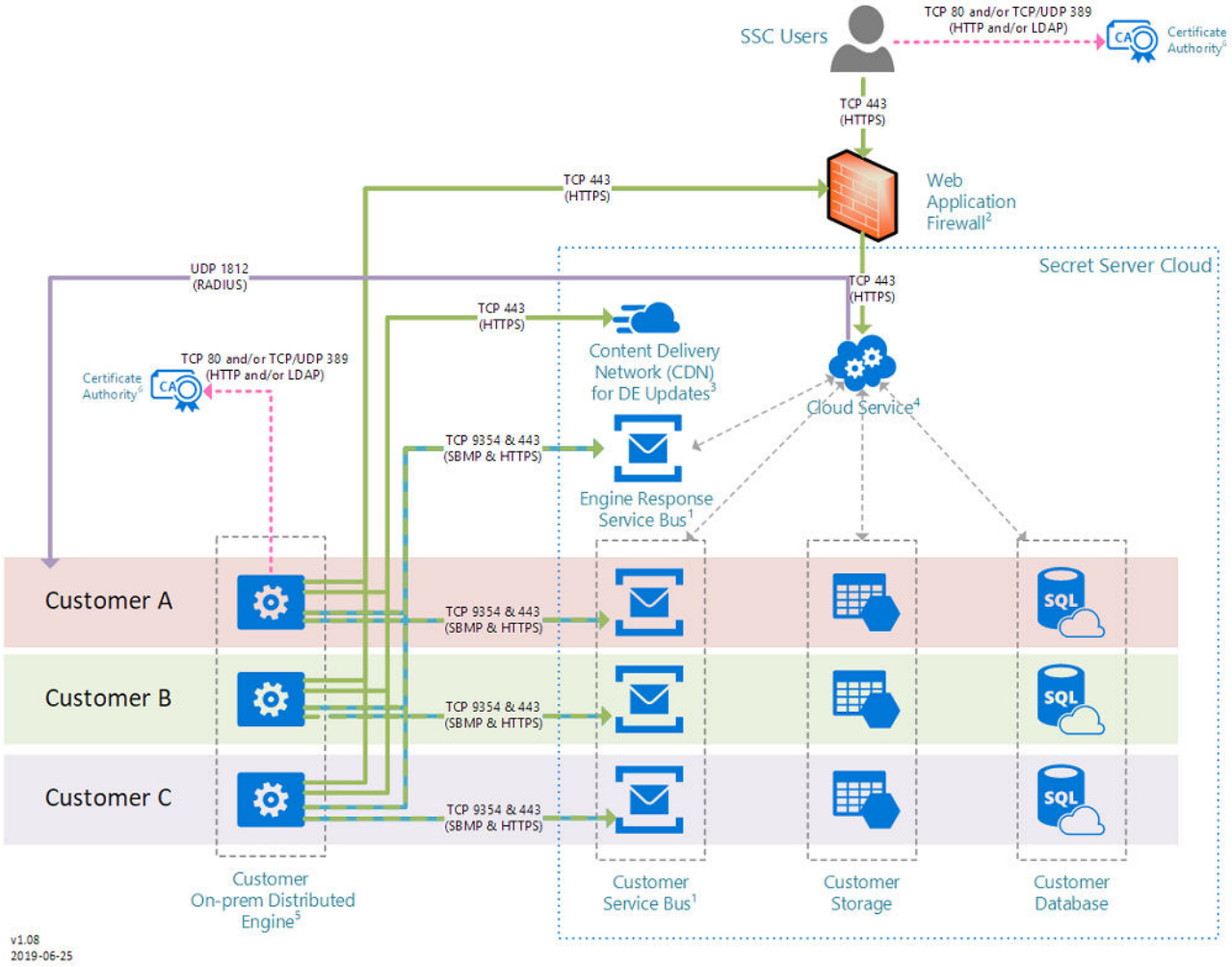
Product overview

IBM Security Verify Privilege Vault helps organizations manage, automate, and track the use of shared privileged identities from a scalable, multi-tenant cloud platform.

1 Step 1: Evaluate the hardware and system configuration

Evaluate the detailed system requirements.

Note: Alternatively, start the Software Product Compatibility Reports tool. Search for the product name, for example, by entering `Verify Privilege`, and follow the instructions.



2 Step 2: Initial setup

On the Setup page, choose your Cloud Environment location. Click **Continue**.

You are directed to the Thycotic One portal to create the password for your first user account with Administrator credentials. The account is assigned to the email address that you entered to request the trial. After you confirm the password, click **Set Password and Login**.

Note: This account is the backup admin account that you might need in a 'break the glass' or unlimited admin scenario. It is suggested that you store the password in a secure physical location such as a safe or locked cabinet. You can reset the password by using an email reset, but if this password is forgotten or you no longer have access to the email account, IBM cannot reset the password.

On the login page, click the button that corresponds to your new Cloud Thycotic One location.

On the Setup page, enter the name for your subdomain. Do not use special characters or spaces.

Read the license agreement and to proceed, accept the agreement.

After a few minutes, the IBM Security Verify Privilege Vault setup completes. Click **Go to your Privilege Vault** and **Login with Thycotic One**.

3 Step 3: Install the Distributed Engine

Interaction with Privilege Vault tenant and your on-premises network uses the Distributed Engine service to communicate. The Distributed Engine, performs Active Directory authentication, password change, and heartbeats. The computer where the engine is installed must have outbound communication on port 443 and port 9354.

a. Browse to **ADMIN** > **Distributed Engine**.

b. Click **Download Engine Installer**.

Note: You can install Distributed Engine on either your workstation or laptop for test if needed. However for production installs, the Distributed Engine Server must be installed on a server. Secret Server use the Distributed Engine to communicate with your domain,. So, if your computer is turned off, user might not be able to log in with their domain accounts and heartbeat and password changing will fail.

c. Run `setup.exe` as an administrator to install the engine service.

The engine service is installed in the following location: `Thycotic Software Ltd\Distributed Engine`.

d. Go to **Admin** > **Distributed Engine**, click **Manage Sites** and then **Manage New Engines**.

A new engine is now available.

e. Assign the engine to the **Default** site and approve it.

f. Validate the engine connectivity.

Go to **ADMIN** > **Distributed Engine** > **Manage Sites** and click the **Default** site. Click **Validate Connectivity** to test the communication between the engine and Privilege Vault. It takes several minutes for the Engine to register. It does not immediately validate. You might need to wait for a few minutes before you try again.

4 Step 4: Configure Active Directory integration.

Active Directory integration lets users log in with their domain credentials. The Distributed Engine service that is running in your network, routes connections to your domain.

Watch video: Configure Active Directory integration in Privilege Vault to let users log in with their domain credentials.

a. On the dashboard, from the **Create Secret** widget,create a new Active Directory Secret.

The domain account that is used must be able to read the users and groups from the domain that you want to sync.

b. In the Create Secret page, enter the domain, username, and password and then save the secret.
c. Browse to **ADMIN** > **Active Directory**.
d. Click **Edit**. Select **Enable Active Directory Integration** and **Enable Synchronization of Active Directory**.
e. Click **Save**.
f. Click **Edit Domains** and then click **Create New**.
g. Enter a fully qualified domain name and a friendly domain name that users will see on the login page.
h. For the **Sync Secret** select the secret that you created in step 4.a on page 3.

The Domain Site is set to Default. The Active Directory authentication and synchronization runs through the Distributed Engine service that is installed on your network.

i. Click **Save** and then click **Back**
j. Click **Edit Synchronization** and choose the domain groups that you want to be able to log in on the Privilege Vault SaaS instance.
k. Save the selected groups.
l. Click **Synchronize Now**. This action starts the user and group synchronization immediately. The synchronization process runs automatically. For immediate results you can start the process manually.

5 Step 5: Test heartbeat and password changing

Heartbeats validate the secrets that you have stored are using the correct password and that password changing can change passwords on demand or a schedule.

a. Browse to **Admin** > **Remote Password Changing**.
b. Click **Edit**.
c. Select **Enable Remote Password Changing** and **Enable Heartbeat** and then click **Save**.
d. Under the **Remote Password Changing** and **Heartbeat Log**, click **Run Now**.

The **Heartbeat** and **Remote Password Changing** processes start so that you do not have to wait.

After you create a secret, the **Last Heartbeat** status shows **Pending** or **Processing**.After heartbeat completes, one of the following status is displayed:

i. Unable to Connect: Privilege Vault cannot reach the target computer. Some possible cause for this message is a firewall issue or the computer or IP address is wrong.
ii. Failed: Privilege Vault can connect but cannot authenticate. This might mean that the password for the secret is incorrect.
iii. Success: Privilege Vault is able to successfully connect with the specified user name and password.

e. Test the password change by viewing a secret and clicking **Change Password Remotely**.

Note: You will change the actual password on the target system.

You can view the status of password changes and heartbeats in the log under **Admin** > **Remote Password Changing**.

6 Step 6: Next steps and other actions you can take.

- Add another user to the administrator role in Privilege Vault.
- Add a folder and share it with the group you are synchronized from Active Directory.
- Create a secret in that folder for other users to see. When you create a secret, you can click the folder and save it to another folder.
- Get other users to log in. Any users that are synchronized to Privilege Vault through the domain synchronization will be able to log in with their domain credentials.
- Enable Google two factor authentication. You can turn on two factor for auser by going to **Admin** > **Users**, editing the user, and specifying the **Two Factor** option.

More information

Product documentation: http://www.ibm.com/support/knowledgecenter/SSWHLP_cloud.

Product support: http://www.ibm.com/support

IBM® Security Verify Privilege Vault Licensed Materials - Property of IBM. © Copyright IBM Corporation and others 2020. U.S. Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" (www.ibm.com/legal/copytrade.shtml).