Tungsten Token Vault
Installation Guide

Version: 3.8.0

Date: 2024-05-02

TUNGSTEN
AUTOMATION

Table of Contents

Preface

This guide is intended for administrators who are responsible for installing and deploying Tungsten Token Vault. To learn more about configuring Token Vault for use with cloud systems such as Microsoft 365, iManage Work, Google, Box, Dropbox or NetDocuments, refer to the documentation from the respective provider. The provider documentation will explain how to acquire tokens to communicate with the applicable cloud system.

Product documentation

The full documentation set for Tungsten eCopy ShareScan is available online:

https://docshield.tungstenautomation.com/Portal/Products/eCopy/6.7.0-u94fwgiq3l/eCopy.htm

The Tungsten eCopy ShareScan documentation set includes the items listed in the following table.

Guide	Description
Tungsten eCopy ShareScan Pre-installation Checklist (PDF)	Provides information on the issues to be addressed before deploying Tungsten eCopy ShareScan.
Tungsten eCopy ShareScan Installation Guide (PDF)	Provides information on how to install and upgrade Tungsten eCopy ShareScan, along with hardware and software prerequisites.
Tungsten eCopy ShareScan Online Help	The integrated help of the application, covering the use of Tungsten eCopy ShareScan beyond installation, including configuration information. ⓘ The help is accessible by pressing **F1** on the eCopy ShareScan Administration Console.
Tungsten eCopy ShareScan Troubleshooter User Guide (PDF)	Provides information on how to use the eCopy ShareScan Troubleshooter, a built-in diagnostic tool.
Tungsten eCopy ShareScan Release Notes (PDF)	Provides an overview of late-breaking details for the current product release.

Guide	Description
Tungsten eCopy ShareScan High Availability Deployment Guide (PDF)	Provides guidance on how to deploy eCopy ShareScan to function in high availability mode.
Tungsten eCopy ShareScan Glossary Editor Recommendations (PDF)	Contains information on proper use of the Glossary Editor Tool.

Training

Tungsten Automation offers both classroom and computer-based training to help you make the most of your eCopy ShareScan solution. Visit the Tungsten Automation website at www.tungstenautomation.com for details about the available training options and schedules.

Getting help with Tungsten Automation products

The **Tungsten Automation Knowledge Base** repository contains articles that are updated on a regular basis to keep you informed about Tungsten Automation products. We encourage you to use the Knowledge Base to obtain answers to your product questions.

To access the **Tungsten Automation Knowledge Base**, go to the Tungsten Automation website and select **Support** on the home page.

ⓘ The **Tungsten Automation Knowledge Base** is optimized for use with Google Chrome, Mozilla Firefox or Microsoft Edge.

The **Tungsten Automation Knowledge Base** provides:
- Powerful search capabilities to help you quickly locate the information you need.

    Type your search terms or phrase into the **Search** box, and then click the search icon.
- Product information, configuration details and documentation, including release news.

    Scroll through the **Tungsten Automation Knowledge Base** home page to locate a product family. Then click a product family name to view a list of related articles. Please note that some product families require a valid Tungsten Automation Portal login to view related articles.
- Access to the **Tungsten Automation Customer Portal** (for eligible customers).

    Click the **Customer Support** link at the top of the page, and then click **Log in to the Customer Portal**.
- Access to the Tungsten Automation Partner Portal (for eligible partners).

    Click the **Partner Support** link at the top of the page, and then click **Log in to the Partner Portal**.
- Access to Tungsten Automation support commitments, lifecycle policies, electronic fulfillment details, and self-service tools.

    Scroll to the **General Support** section, click **Support Details**, and then select the appropriate tab.

Install Token Vault

Token Vault is a web application hosted by a Windows service. It is used to manage and store authentication tokens, and provide them to other applications that interact with cloud systems. Token Vault also manages authorization provider registrations and user authorizations, along with one-time passcode generation and verification.

One Token Vault instance can serve several Token Vault clients, such as eCopy ShareScan connectors on different eCopy ShareScan servers.

Prerequisites

Before you install Token Vault, ensure that:
- You have Microsoft SQL Server 2016 or later installed and accessible.
- Your system has the setup prerequisites installed:
  - Microsoft ASP.NET Core 8.0.3 - Shared Framework (x64)
  - Microsoft .NET Core Runtime - 8.0.3 (x64)
  - Microsoft .NET Framework 4.8 Setup
- You deploy Token Vault on a computer that is a member of a domain.

If any of these prerequisites is missing, the installer files are available from your Token Vault deployment package.

Perform a new installation on a clean system

1. Verify that you are performing installation with administrator privileges.
2. Run TokenVault3.8.exe.
   The **Choose setup language** screen appears.
3. Select a preferred language (English by default) from the list, and click **Next**.
   The **Welcome** screen appears.
4. Click **Next**.
   The End-User License Agreement (EULA) is displayed on the **License Agreement** screen.
5. Accept the EULA and click **Next**.
   The **Destination Folder** screen appears.
6. Accept the default destination folder, or click **Change** to specify another folder. Then click **Next**.

7. Specify service credentials for the Token Vault Service on the **Service Credentials** screen. Alternatively, you can select to use **LocalSystem** credentials.

    Specifying service credentials is the recommended option so that you can use Windows or Microsoft Entra Integrated Authentication for the database connection.

    Click **Next**. The **Installation Summary** screen appears.

8. Review the information and if you are satisfied with the configuration, click **Install**. Otherwise, click **Back**.

9. When the **Install Shield Wizard Completed** screen appears, click on the link above the **Finish** button to open Token Vault configuration, and then click **Finish** to close the installation wizard.

    The Token Vault **Database Settings** page appears in the browser to perform database configuration as the required initial configuration. If you have not clicked on the link described in step 9, you should open Token Vault manually by entering the http://localhost:8380 URL in your browser's address bar.

10. On the **Database Settings** page, click **Create New** to create a new Token Vault database.

    The **Create new database** page appears.

11. Specify the hostname or IP (and optionally, the instance name) of the SQL Server (**Server name**) that you are connecting to, along with the database **Catalog name**. Specify settings related to encryption of network traffic between your SQL Server and Token Vault computer (**Use encryption for data** and **Trust server certificate**) according to your SQL Server and environment configuration.

12. Under the **Admin credentials** group on the same page, select **Authentication type**, and specify the credentials (**User name** and **Password**) for database creation.

    The following authentication types can be selected:
    *   SQL Server Authentication
    *   Windows Authentication
    *   Microsoft Entra Password
    *   Microsoft Entra Integrated

    In case of "Windows Authentication" and "Microsoft Entra Integrated" authentication types, the **User name** must be specified in DOMAIN\USERNAME format.

    The credentials specified are only used during database creation to run the Token Vault SQL scripts on the selected database.

13. Under the **Runtime credentials** group on the same page, you can specify a runtime account for the configuration database.

    You need to select an **Authentication type** to determine how the Token Vault service connects to the SQL Server database:
    *   Via **SQL Server Authentication**, you can specify an SQL user by entering its **User name** and **Password**.

        > ⓘ The specified user will be created on the SQL server if it does not exist.

    *   Via **Windows Authentication**, using the identity of the account running the Token Vault Windows service.
    *   Via **Microsoft Entra Password**, you can specify an existing Microsoft Entra user by entering its **User name** and **Password**.

        Select this option only when you specify an Azure SQL server.

- Via **Microsoft Entra Integrated**, using the identity of the account running the Token Vault Windows service.

  Select this option only when you specify an Azure SQL server, and your local Active Directory is synchronized with Microsoft Entra ID.

  The Token Vault service uses these credentials only for runtime connection to the SQL Server.

14. Click **Create & Save** to create the database with the specified parameters, and save the database configuration.

  > ⛔ If you specified an Azure SQL server, the Token Vault database must be created manually, and only the user and other database objects (such as SQL tables and indices, etc.) will be created when you click **Create & Save**.

15. Click **Restart service** to restart Token Vault Windows service and use the new database.

Upgrade Token Vault

If you have Token Vault version 3.0, 3.5 or 3.6 installed already, perform the following steps to upgrade to the current version.

> ℹ️ A direct upgrade from Token Vault 2.0, 2.5 or 2.7 is not supported.
>
> If you are upgrading from a Token Vault version earlier than 3.0 (2.0, 2.5 or 2.7), you first need to upgrade to version 3.7. Once you have a verified working installation of Token Vault 3.7, you are ready to proceed with the upgrade to version 3.8.

1. Run TokenVault3.8.exe.

   The installer automatically detects the earlier version.

   The **Choose setup language** screen appears.
2. Select a preferred language (English by default) from the list, and then click **Next**.

   The **Welcome** screen appears.
3. Click **Next**.

   The End-User License Agreement (EULA) is displayed on the **License Agreement** screen.
4. Accept the EULA, and then click **Next**.

   The **Destination Folder** screen appears.
5. Accept the default destination folder, or click **Change** to specify another folder. Then click **Next**.
6. Specify the service credentials for the Token Vault service on the **Service Credentials** screen. Alternatively, you can select to use **LocalSystem** credentials.

   Specifying service credentials is the recommended option so that you can use Windows or Microsoft Entra Integrated Authentication for the database connection.
7. Click **Next**.

   The **Installation Summary** screen appears.

8. Review the information, and if you are satisfied with the configuration, click **Install**. Otherwise, click **Back**.

9. When the **Install Shield Wizard Completed** screen appears, click on the link above the **Finish** button to open Token Vault configuration, and then click **Finish** to close the installation wizard.

   The Token Vault **Database Settings** page appears in the browser to perform database configuration as the required initial configuration. If you have not clicked on the link described in step 9, you should open Token Vault manually by entering the http://localhost:8380 URL in your browser's address bar.

   The **Database Settings** page displays the current Token Vault database connection parameters and shows that the current Token Vault database is outdated.

10. Click **Upgrade** on this page to upgrade the database.

    The **Upgrade database** page appears displaying the **Database parameters** and the **Runtime credentials**.

11. Under the **Admin credentials** group, select **Authentication type**, and then specify the credentials (**User name** and **Password**) for database upgrade.

    The following authentication types can be selected:

    - SQL Server Authentication
    - Windows Authentication
    - Microsoft Entra Password
    - Microsoft Entra Integrated

    In case of "Windows Authentication" and "Microsoft Entra Integrated" authentication types, the **User name** must be specified in DOMAIN\USERNAME format.

    The credentials specified are only used during database upgrade to run the Token Vault SQL scripts on the selected database.

12. Click **Upgrade** to upgrade the database.

13. Click **Restart service** to restart Token Vault Windows service and use the upgraded database.

🛑 Upgrade from Token Vault 1.x is not supported.

Chapter 2

Configuration settings

Token Vault configuration settings are stored in the Token Vault database and in the appsettings.json file. This json file is located in the <Common Application Data folder> for Token Vault, such as `C:\ProgramData\Tungsten\TokenVault`.

To modify Token Vault configuration settings, log in with your Token Vault administrator credentials and click **Settings** on the left, and then select the setting category to be configured from the options that appear.

These setting categories include:
* Server settings
* Database settings
* Authentication settings
* One-time passcode settings
* Logging settings

By default, when the administrator clicks **Settings** on the left, the **Database settings** page appears.

To be able to save the configuration settings into the appsettings.json file and restart the Token Vault windows service by a Token Vault administrator user from the Token Vault UI, the user who runs the Token Vault windows service must have the following privileges:
* Read and Write permission on the <Common Application Data>\Tungsten\TokenVault folder (typically `C:\ProgramData\Tungsten\TokenVault`)
* 'Start service', 'Stop service' and 'Pause/Continue service' permissions on the Token Vault Windows service

The installer sets these permissions automatically, but when changing the user who runs Token Vault Windows service, these permissions must be set manually.

When the Token Vault is not usable for configuration issues, Token Vault opens in maintenance mode and only configuration settings pages are available. A red triangle-shaped icon with exclamation mark indicates the setting page(s) where the Token Vault administrator must take actions to make Token Vault usable.

In maintenance mode, Token Vault web application is accessible only from the Token Vault server machine using either the http://localhost:8380 URL or the https://localhost:8381 URL (the ports vary according to your configuration). If other users open Token Vault in a browser from their machine, an error page appears with the "Site is temporarily unavailable" error message.

The most frequent conditions when Token Vault starts in maintenance mode can be listed as below:
* Immediately after a clean installation, since the database connection parameters are missing.
* Immediately after an upgrade installation, since the database is required to upgrade.

- If the database is inaccessible due to any reasons.
- If HTTPS certificate configured for Token Vault has been expired or has been removed from the Certificate Store (Certificates (Local Computer)\Personal), or the user who runs the Token Vault Windows service has no privileges to use the private key of that certificate.

Server settings

On this setting page, server settings can be configured (such as port for HTTP and HTTPS protocols, HTTPS certificate thumbprint, cluster settings and proxy settings, and setting that Token Vault accept requests only from registered client).

General settings

Under this setting group, you can change the **Port** for HTTP protocol to a valid, available port. The default HTTP port for Token Vault is 8380. If you want to use Token Vault with HTTP protocol the **HTTPS certificate thumbprint** must be blank under **HTTPS settings** group.

> ⛔ Tungsten Automation highly recommends using HTTPS ptotocol.

Here you can also specify for Token Vault to accept requests only from registered client.

If the **Accept requests only from registered clients** setting is configured as **Yes**, Token Vault accepts only requests from those applications which are registered as Token Vault clients on the Token Vault Manage Clients page. Otherwise, Token Vault accepts token or one-time passcode verification requests from any application/computer.

The registration of an application as Token Vault client is based on the certificate of the computer where the application is running on. This certificate is used by Token Vault to verify that a request is coming from a registered client.

> ℹ️ For higher security we recommend that you configure this setting as Yes, and register applications allowed to communicate with Token Vault as Token Vault client.

To register an applications as Token Vault client:

1. On the computer where the application is running on, export the certificate (without the private key) of the computer into a file.

2. Click **Manage Clients** on the left sidebar of the Token Vault.
   The Manage Clients page with the list of already registered Token Vault clients is displayed.

3. Click **Register new**.
   The Register client page is displayed.

4. Click **Browse** and select the file containing the certificate exported in Step 1.

5. Click **Save** to import the certificate into Token Vault from the selected file.

The Manage Clients page with the list containing the registered client with its name and the thumbprint of the imported certificate is displayed. To unregister a client on this page, mark the checkbox of a list item and click **Remove**.

HTTPS settings

Under this setting group, you can enable HTTPS protocol and configure related settings:

1. Set **HTTPS port** to a valid, available port. The default port is 8381.

2. Set **HTTPS certificate thumbprint** to the thumbprint of the certificate that you want to use for your Token Vault instance or generate a self-signed certificate by Token Vault.

   Requirements for the certificate:

   - **Issued to** or **Subject** property must be the fully qualified name of the computer where Token Vault is installed.
   - Must be stored in the Local Computer store: Certificates (Local Computer)\Personal.
   - The user account of the Windows service running Token Vault must have privileges to use the private key of the certificate.

To generate a self-signed certificate by Token Vault:

1. Delete the **HTTPS certificate thumprint** if specified.

2. Click **General new...** button next to the HTTPS certificate thumbprint textbox.
   The **New self-signed certificate** page is displayed.

3. Enter the fully qualified name of the computer where Token Vault is installed as **Host name**.

4. Select the **Key size** and **Expiration** for the certificate.

5. Specify a password (**Password** and **Confirm password**) for the certificate.

6. Click on **Create** to create the self-signed certificate.
   The **Server settings** page with the thumbprint of the newly created self-signed certificate as **HTTPS certificate thumprint** and the certificate expiration date is displayed.

7. Click **Download the root certificate** button next to the HTTPS certificate thumbprint textbox to download the root certificate (TokenVault Root CA.pfx file) belonging to the newly created self-signed certificate. This root certificate needs to be deployed to users' computer to make the newly created self-signed certificate trusted.

8. Click **Save** to save the general settings.

9. Click **Restart service** to restart the Token Vault Windows service and use Token Vault with HTTPS protocol and the newly generated self-signed certificate.

If the Token Vault does not appear in the browser automatically, enter the Token Vault URL into the address bar of your browser according to your Token Vault configuration in the following format:

```
https://<FQDN>:<port>/
```

where:

- FQDN is the fully qualified domain name of the Token Vault machine and

- port is the value of the HTTPS Port setting configured on the Server Settings page

For example:

```
https://tokenvaultmachine.testdomain.com:8381.
```

Cluster settings

This setting group contains the **Node network interface** setting for configuring Token Vault in a high availability environment. Select the address of an appropriate physical network interface for the Token Vault node to use in the communication between Token Vault server nodes.

Proxy settings

Under this setting group, you can override the system proxy settings and specify a proxy server for Token Vault.

1. Change **Override system proxy settings** value to **Yes**.

2. Enter your **Proxy server address** and your **Proxy server port**, and specify a user credentials for your proxy server (**Username**, **Password**, **Domain**).

When you configured the server settings, click **Save** to save your changes. These changes will not have any effect until Token Vault service restarts.

To restart the Token Vault service and apply your configuration changes, click **Restart service** at the bottom of this page. After the service restarts, you might be required to manually refresh the Token Vault page in the browser.

Database settings

On this setting page, you can verify the Token Vault database status and configure the database connection parameters.

To modify the database connection parameters, do the following:

1. Click **Configure**.
   The **Configure database connection** page appears.

2. Specify the hostname or IP (and optionally, the instance name) of the SQL Server (**Server name**) that you are connecting to, along with the database **Catalog name** and settings related to encryption of network traffic between your SQL Server and Token Vault computer (**Use encryption for data** and **Trust server certificate**) according to your SQL Server and environment configuration.

3. Under the **Runtime credentials** group on the same page, you can specify a runtime account for the Token Vault database.
   You need to select the **Authentication type** to determine how the Token Vault service connects to the SQL Server database:

   • Via **SQL Server Authentication**, you can specify an SQL user by entering its **User name** and **Password**.

   • Via **Windows Authentication**, using the identity of the account running the Token Vault Windows service.

- Via **Microsoft Entra Password**, you can specify an existing Microsoft Entra user by entering its **User name** and **Password**.

  Select this option only when you specify an Azure SQL server.

- Via **Microsoft Entra Integrated**, using the identity of the account running the Token Vault Windows service.

  Select this option only when you specify an Azure SQL server, and your local Active Directory is synchronized with Microsoft Entra ID.

The Token Vault service uses these credentials only for runtime connection to the SQL Server.

> ⊘ Tungsten Automation highly recommends using Windows or Microsoft Entra Integrated Authentication for Token Vault database connection.

4. Click **Verify & Save** to save the database configuration settings.

    The **Database settings** page appears displaying the Token Vault database status and the new database connection parameters.

    If you configure an earlier version of a Token Vault database, the **Database settings** page shows that the database is outdated, and it cannot be used with this Token Vault version.

    To upgrade this database so that it is usable with this Token Vault version, continue with the following steps.

5. Click **Upgrade** on this page.
    The **Upgrade database** page appears displaying the **Database parameters** and **Runtime credentials**.

6. Under the **Admin credentials** group, select the **Authentication type** and specify the credentials (**User name** and **Password**) for the database upgrade.
    The following authentication types can be selected:
    - SQL Server Authentication
    - Windows Authentication
    - Microsoft Entra Password
    - Microsoft Entra Integrated

    In case of "Windows Authentication" and "Microsoft Entra Integrated" authentication types, the **User name** must be specified in DOMAIN\USERNAME format.

    The credentials specified are only used during database upgrade to run the Token Vault SQL scripts on the selected database.

7. Click **Upgrade** to upgrade the selected database.

8. Click **Restart service** to restart the Token Vault Windows service and use the newly configured database.

> ⊘ Before you configure another database, which was used by another Token Vault configured with HTTPS protocol earlier, the sensitive data in the database must be re-encrypted manually in order for the database to be usable on this Token Vault machine. To perform the re-encryption, see the **Encrypt sensitive data manually** section below.

Encrypt sensitive data manually:

<u>If the other Token Vault machine is still usable:</u>

1. On the other Token Vault machine, open a Command prompt window as the user who runs the Tungsten Token Vault Windows service.

   If this user is LocalSystem, then open a Command prompt window as such a user who has privileges to use the private key of the certificate whose thumbprint is configured as the HTTPS certificate thumbprint on the Token Vault General Settings page.

2. Navigate to the Token Vault installation folder.

3. Run the following command:

   `tokenvault.exe cert update old:<old certificate thumbprint>`

   where `<old certificate thumbprint>` is the configured certificate thumbprint.

4. Restart the Tungsten Token Vault Service.

   Now, the encryption of sensitive data in the database is not certificate-based.

   The following steps are required only if this Token Vault is configured with HTTPS protocol, after the database is configured successfully, and it is alive and up-to-date.

5. On this Token Vault machine, open a Command prompt window as the user who runs the Tungsten Token Vault Windows service.

   If this user is LocalSystem, then open a Command prompt window as such a user who has privileges to use the private key of the certificate whose thumbprint is configured as the HTTPS certificate thumbprint on the Token Vault General Settings page.

6. Navigate to the Token Vault installation folder.

7. Run the following command:

   `tokenvault.exe cert update new:<new certificate thumbprint>`

   where `<new certificate thumbprint>` is the HTTPS certificate thumbprint that is configured on the General Settings page.

8. Restart the Tungsten Token Vault Service.

<u>If the other Token Vault machine is no longer usable:</u>

1. On this Token Vault machine, import the certificate earlier used by the other Token Vault machine into the Local Computer store (Certificates (Local Computer)\Personal).

2. Add permission to the user account of the Windows service running Token Vault to use the private key of the imported certificate.

3. Open a Command prompt window as the user who runs the Tungsten Token Vault Windows service.

   If this user is LocalSystem, then open a Command prompt window as such a user who has privileges to use the private key of both the imported certificate and the certificate whose thumbprint is configured as the HTTPS certificate thumbprint on the Token Vault General Settings page.

4. Navigate to the Token Vault installation folder.

5. Run the following command:

   `tokenvault.exe cert update old:<old certificate thumbprint> new:<new certificate thumbprint>`

where:

- `<old certificate thumbprint>` is the thumbprint of the imported certificate, and
- `<new certificate thumbprint>` is the HTTPS certificate thumbprint that is configured on the General Settings page.

6. Restart the Tungsten Token Vault Windows service.

Authentication settings

On this setting page, you can configure the authentication methods and on-premises Active Directory and Microsoft Entra ID-related settings.

The **Authentication Type** setting value determines what kind of users can log in to Token Vault.

The possible values of this configuration setting include:

- **On-premises**: Only users of an on-premises Active Directory can log in to Token Vault.

  This is the default value and can be configured only when the Token Vault server machine is a member of any domain.
- **Microsoft Entra ID & on-premises**: Both on-premises Active Directory and Microsoft Entra users can log in to Token Vault.
- **Microsoft Entra ID**: Only Microsoft Entra users can log in to Token Vault.

> ⛔ **Microsoft Entra ID** and **Microsoft Entra ID & on-premises** values can be configured only when Token Vault is configured with HTTPS.

Manage user domains

When certain on-premises Active Directory users cannot log in to Token Vault as they do not have permissions to access Active Directory to retrieve own user and group membership data from the Active Directory, the access to Active Directory domains would be required to configure.

This setting is available only when **On-premises** or **Microsoft Entra ID & on-premises** is selected for **Authentication Type**.

To configure access to Active Directory domains:

1. Select **On-premises** or **Microsoft Entra ID & on-premises** for **Authentication Type**.

2. Click **Manage user domains** under **Active Directory settings** group.
   The **Manage user domains** page with the list of configured domain names is displayed.

3. Click **Register new** to configure Active Directory access to a new domain.
   The **Add new domain** page is displayed.

4. Enter the **Domain name**.

5. As **Domain controller host** specify the domain controller server host name as **Domain controller host** or leave it blank to use the **Domain Name** as domain controller server host name.

> ℹ️ Users whose Active Directory objects are managed by the specified **Domain controller host** must specify the **Domain name** as domain when specifying their username in DOMAIN \USERNAME format at logging in to Token Vault.

6. Specify the distinguished name of the Active Directory container under which the user objects are located as **Base DN** or leave it blank to use the default "Users" Container (CN=Users,DC=yourDomain,DC=COM) and the "Computers" Container (CN=Computers,DC=yourDomain,DC=COM) as root.

7. Select **Directory access type** to retrieve user and group data from the Active Directory.

   The possible values of this configuration setting include:
   - **Use end-user's credential**: for retrieving user and group data from the Active Directory the logged in user is used.
   - **Use specified credentials**: for retrieving user and group data from the Active Directory the specified service user is used.

8. In case if "Use end-user's credentials" directory access type, specify a user credentials (**User name for testing** and **Password for testing**) for testing the access to and for retrieving user and group data from the specified Active Directory domain controller.

   In case of "Use specified credentials" directory access type, specify the service user credentials (**Username** and **Password**) for accessing to and retrieved user and group data from the specified Active Directory domain controller. The Username must be specified in DOMAIN \USERNAME format.

9. Click **Save**.

   The **Manage user domains** page with the list containing the configured domain names is displayed.

   To edit a domain configuration, click **Edit** button belonging to a list item and modify the same settings as above on the **Edit domain** page.

   To remove a domain configuration, mark the checkbox of a list item and click **Remove**.

Allowing Microsoft Entra users to log in to Token Vault

To allow Microsoft Entra users to log in to Token Vault, the following two tasks must be completed:

1. Register an application at the Microsoft Identity Platform (Microsoft Entra ID) admin center associated with your Microsoft 365 subscription.

2. Configure Microsoft Entra ID settings on Token Vault Authentication settings page accordingly.

Register an application at the Microsoft Identity Platform (Microsoft Entra ID) admin center

To register an application for Token Vault to allow Microsoft Entra users to log in, you need to specify certain properties of this Microsoft Entra application (Application (client ID), Client secret and Redirect URI). To perform this, do the following.

1. Navigate to https://portal.azure.com.

Your organization may use a national cloud because of data residency or compliance requirements. In this case, navigate to the corresponding national cloud Microsoft Entra portal endpoint instead.

- https://portal.azure.us - for Microsoft Entra ID for US Government.
- https://portal.azure.cn - for Microsoft Entra China operated by 21Vianet.

2. Log in with an existing Microsoft 365 account.

3. Select **Microsoft Entra ID** in the left navigation pane.

4. Select **App registrations**.
   The **App registrations** page appears.

5. Click the **New registration** button to register a new application.
   The **Register an application** page opens.

6. Fill out the registration information of the application:
   - Specify a **Name** for the application.
   - Under **Supported account types**, select an account type.

     While configuring Microsoft Entra ID settings in Token Vault, **Directory (tenant) ID** must be configured according to this application property.

   - From the **Redirect URI (optional)** list, select **Web** type, and then enter the URI corresponding to your Token Vault configuration in the following format:

     ```
     https://<FQDN>:<port>/callback
     ```
     where:
     - FQDN is the fully qualified domain name of the Token Vault machine.
     - port is the value of the HTTPS Port setting on the Token Vault Server Settings page in case of https usage.

     For example, `https://tokenvaultmachine.testdomain.com:8381/callback`.

     > ⓘ Token Vault must be configured with HTTPS for Microsoft Entra ID-based authentication. Otherwise, an error occurs when the user tries to sign in with Microsoft.

7. Click **Register**.
   The new application is created with the specified name and a generated **Application (client) ID**, but the application does not have any certificate or secret yet.

8. Copy the **Application (client) ID** and the **Directory (tenant) ID** for later use.
   These are required for the configuration of Microsoft Entra ID settings in Token Vault.

9. Select **Authentication** in the left menu.

10. Click **Add URI** in the **Redirect URIs** on the right to configure the second Redirect URI for the application. Enter the URI corresponding to your Token Vault configuration in the following format:

    ```
    https://<FQDN>:<port>/signin-oidc
    ```
    where:
    - FQDN is the fully qualified domain name of the Token Vault machine.
    - port is the value of the HTTPS Port setting on the Token Vault Server Settings page in case of https usage.

    For example, `https://tokenvaultmachine.testdomain.com:8381/signin-oidc`.

> ⓘ Token Vault must be configured with HTTPS for Microsoft Entra ID-based authentication. Otherwise, an error occurs when the user tries to sign in with Microsoft.

11. Under **Implicit grant and hybrid flows**, select **Access tokens (used for implicit flows)** and **ID tokens (used for implicit and hybrid flows)**.

12. Click **Save**.

13. Select **Certificates & secrets** in the left menu.

14. Click **New client secret** in the right panel to generate a new client secret for the application.

15. Specify a **Description**, and then select the expiry option according to your policy requirements.

16. Click **Add**.

17. Copy the newly generated client secret value for later use.
    This is another required application property for configuring Microsoft Entra ID settings in Token Vault.

> 🛑 You can only copy the client secret at this point in the workflow. After you leave or refresh this page, you are not able to retrieve it. If you leave this page without copying the client secret value, you must repeat the corresponding steps above and create a new one.

18. Select **API permissions** in the left menu, and click **Add a permission** on the **API permissions** page.

19. Under the **Commonly used Microsoft APIs** group on the **Request API permissions** page, locate **Microsoft Graph**, and select it.
    The Microsoft Graph API is displayed on the **Request API permissions** page.

20. Select **Delegated permissions**.

21. Locate the **User** permission group, and select the **User.ReadBasic.All** check box to allow login to Token Vault and search for Microsoft Entra users to add them as Token Vault administrator.

22. Locate the **Group** permission group, and select **GroupMember.Read.All** check box to allow search for Microsoft Entra groups to add them as Token Vault administrator groups.
    For this permission, admin consent is required.

23. Click **Add permissions**.
    There might be a delay between permissions being configured and when they appear on the consent prompt.

24. If permissions are configured and displayed on the consent prompt, click **Grant admin consent for...** to allow this app to search for Microsoft Entra groups so that no consent screen appears at the Microsoft Entra user logins.

The application is now configured and has permissions to access Microsoft Entra users and groups.

Configure Microsoft Entra ID settings on Token Vault Authentication settings page

1. Select **Microsoft Entra ID & on-premises** or **Microsoft Entra ID** for **Authentication Type**.

2. Enter your **Application (client) ID** and **Client Secret (value)** (provided by Microsoft Identity Platform (Microsoft Entra ID) during the application registration task).

3. Specify the **Directory (tenant) ID** according to the **Supported account types** property of the application registered at the Microsoft Identity Platform (Microsoft Entra ID) admin center:
   - Enter the **Directory (tenant) ID** of the application registered at the Microsoft Identity Platform (Microsoft Entra ID) when selected 'Accounts in this organizational directory only (<your tenant's name> only - Single tenant)' as **Supported account types** during application registration.
   - Enter **organizations** when selected 'Accounts in any organizational directory (Any Microsoft Entra tenant - Multitenant)' as **Supported account types** during the application registration at the Microsoft Identity Platform (Microsoft Entra ID) admin center.
   - Enter **common** when selected 'Accounts in any organizational directory (Any Microsoft Entra tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)' as **Supported account types** during the application registration at the Microsoft Identity Platform (Microsoft Entra ID) admin center.

4. Select the proper national cloud from the **National Cloud** list if your organization uses a national cloud due to data residency or compliance requirements. Otherwise, keep the default Microsoft Entra ID (global service) value.

5. Click **Save** to save the authentication settings.
   To validate the configuration settings, your browser will redirect you to the login page for the Microsoft Identity Platform (Microsoft Entra ID) where you must login as a Global Administrator, an Application Administrator, or a Cloud Application Administrator. If the user was already logged in to the Microsoft Identity Platform (Microsoft Entra ID), it is possible that no user interaction is needed for login.

6. Click **Restart service** at the bottom of this page to restart the Token Vault service and apply your configuration changes.

When the user is logged in with an on-premises Active Directory user in Token Vault and change the **Authentication Type** to **Microsoft Entra ID** but the browser already has a signed-in Microsoft Entra user, then this Microsoft Entra user became the logged-on user in Token Vault automatically.

Authentication types and login to Token Vault

When **On-premises** is configured as the **Authentication Type**, to log in to Token Vault, on the **Login** page, you must enter your Windows **User name** in DOMAIN\USERNAME format and **Password**, and then click **Log in**.

When **Microsoft Entra ID & On-premises** is configured as the **Authentication Type**, a new **Sign-in with Microsoft** button is available on the Token Vault **Login** page. To log in to Token Vault with an Microsoft Entra user, you must click this button. Then the browser will redirect you to the login page for the Microsoft Identity Platform (Microsoft Entra ID) where you can complete the login process. After a successful login, the browser will direct you back to Token Vault displaying either the **Manage authorization providers** page (if the user is a Token Vault administrator) or the **Available authorization providers** page (otherwise). If you were already logged in to Microsoft Identity Platform (Microsoft Entra ID) in a different browser tab, and you click the **Sign-in with Microsoft** button, it is possible that no user interaction is needed for login.

To log in to Token Vault with an on-premises Active Directory user, you must enter your Windows **User name** in DOMAIN\USERNAME format and their **Password**, and then click **Log in**.

When **Microsoft Entra ID** is configured as the **Authentication Type**, Token Vault **Login** page does not appear when you open the Token Vault URL in a browser. The same will happen as if you would

have clicked the **Sign-in with Microsoft** button on the Token Vault **Login** page at the Microsoft Entra ID & On-premises setting but automatically.

One-time passcode settings

Token Vault enables for users to configure one-time passcode generation method to generate one-time passcodes in Token Vault, and Token Vault provides a one-time passcode verification service for applications. Applications such as eCopy ShareScanAutoStore can use one-time passcode authentication method without implementing one-time passcode generation and/or verification on their own. They request one-time passcode verification from Token Vault to authenticate users.

On this settings page, you can configure settings related to one-time passcode generation and verification.

General settings

Under this setting group, the **Passcode generator** setting value determines how the logged in user can generate one-time passcodes.

The possible values of this configuration setting include:
- **None**: Users cannot configure a passcode generator for their user account.
- **Token Vault**: Users can enable Token Vault for generating one-time passcodes for their user account.
- **Authenticator app**: Users can set up an Authenticator app for generating one-time passcodes for their user account.
- **Authenticator app or Token Vault**: Users can decide either to set up an Authenticator app or to enable Token Vault for generating one-time passcodes.

When **Token Vault** or **Authenticator app or Token Vault** is configured as the **Passcode generator**, you can specify as the value of the **Expiry of Token Vault generated passcodes (in seconds)** setting the expiration time of Token Vault generated passcodes. Its value can be configured between 30 and 900 seconds. The default value is 300 seconds (5 minutes).

Blocking settings

Under this setting group, the **Passcode blocking threshold** value determines the number of passcode verification failures before passcodes get blocked temporarily for the given user. Its value can be configured between 1 and 15. The default value is 3.

The **Passcode blocking duration** value determines for how long the passcodes of a user remain blocked after the passcode blocking threshold is reached. You can select one of the following values: 5 minutes, 10 minutes, 15 minutes, 30 minutes, 60 minutes. Its default value is 15 minutes.

If you select **Yes** as the value of the **Allow unblock for end-users** setting, users, whose passcodes got blocked, does not have to wait for the passcode blocking duration time to use passcode again. They can unblock on their own. Otherwise, only a Token Vault administrator user can unblock passcodes of users.

After you modify any of the One-time passcode settings, click **Save** to save your changes and then click **Restart sevice** for your changes to take effect.

How to generate one-time passcodes

Users can enable one-time passcode generation on the **Available authorization providers** page when the **Passcode generator** setting is not configured as **None**.

When **Token Vault** is configured as the **Passcode generator** setting, click **Enable** to enable generating one-time passcodes by Token Vault. Your current passcode is displayed as masked. To show your current passcode and that till what time it is valid, keep the **Show** button pressed. Token Vault automatically generates a new passcode in every 30 seconds even if the previous passcode is still valid.

When **Authenticator app** is configured as the **Passcode generator** setting, click **Set up** to set up an authenticator app to generate one-time passcodes and follow the instructions on the appearing **Set up an Authenticator app** page:

1. Download a two-factor authenticator app like Microsoft Authenticator or Google Authenticator for your mobile device.

2. Scan the displayed QR code or enter the displayed key generated by Token Vault into your authenticator app to register your user account.

3. Once you have scanned the displayed QR code or input the displayed key, your authenticator app will provide you with a unique code. Enter this code in the **Code** textbox on the Token Vault **Set up an Authenticator app** page.

4. Click **Verify** to finish setting up an Authenticator app.

   Token Vault displays that you have set up an authenticator app to generate one-time passcodes.

   If you no longer want to use the Authenticator app with the key displayed earlier on the **Set up an Authenticator app** page or you want to set up the Authenticator app with a new key, click **Reset**.

When **Authenticator app or Token Vault** is configured as the **Passcode generator** setting, users can select between the Authenticator app or Token Vault to generate one-time passcodes:

- click on the **Set up an Authenticator app** link to set up an authenticator app to generate one-time passcodes and follow the instructions on the appearing **Set up an Authenticator app** page as described above, or

- click on the **Enable Token Vault** link when you want to use Token Vault for generating one-time passcodes.

When your passcodes got blocked, Token Vault displays this information on the **Available authorization providers** page, you can unblock your passcodes by clicking **Unblock** if the **Allow unblock for end-users** setting is configured as **Yes**.

Manage passcodes

On the **Manage Passcode** page, the Token Vault administrator users can see the list of users, who set up one-time passcode generation, containing the username, the selected passcode generator and that whether the passcodes are got blocked.

To remove the passcode generator selection of a user, select the user in the list and click **Reset**.

To unblock passcodes of a user, select the user in the list and click **Unblock**.

Logging settings

On this setting page, logging-related settings can be configured.

The **Trace Level** setting value determines how detailed the Token Vault trace is.

The default value of this configuration setting is *Verbose*.

Other possible values are: *Error*, *Warning*, *Info*, and *Off*.

The **Log file preservation (in days)** setting value determines how many days a log file is preserved. A log file older than the number of days specified in this setting is deleted automatically.

After you modify any of these settings, click **Save** and then click **Restart service** for your changes to take effect.

Next steps

After you successfully install and configure Token Vault, you are ready to configure it for managing authorization providers for cloud systems such as Microsoft 365, iManage Work, Google, Box or Dropbox.

Token Vault URL and functions

The URL required to access the Token Vault website depends on the configured value of HTTPS port or Port configuration settings.

Using HTTPS

`https://FQDN:port`

For example, `https://computername.mydomain.com:8381`.

FQDN is the Fully Qualified Domain Name of the computer where Token Vault is deployed.

Port is the port configured as the value of HTTPS port configuration setting.

Using HTTP

`http://FQDN:port`

For example, `http://computername.mydomain.com:8381`.

FQDN is the Fully Qualified Domain Name of the computer where Token Vault is deployed.

Port is the port configured as the value of Port configuration setting

> 🛑 Tungsten Automation highly recommends using HTTPS. When HTTPS is used, all requests arriving to the HTTP port will be redirected to HTTPS.

Certain Token Vault functions can be accessed only by administrators:
- Register and manage Token Vault authorization providers for cloud systems, such as Microsoft 365, iManage Work, Google, Box, Dropbox or NetDocuments
- Manage Token Vault administrators
- Manage tokens by users and Token Vault authorization providers
- Manage users' one-time passcodes configurations
- Register and manage Token Vault clients
- Manage Token Vault configuration settings (Server, Database, Authentication, One-time passcode and Logging)

> ℹ️ The first user who logs in to the Token Vault website automatically becomes the Token Vault administrator.

End-users who are not Token Vault administrator can access only the **Available authorization providers** page in Token Vault. They can authorize configured Token Vault authorization providers in a cloud system, such as Microsoft 365, iManage Work, Google, Box, Dropbox or NetDocuments to use related applications in AutoStore, such as SharePoint component configured with

modern authentication. These applications interact with Token Vault and get access tokens for communication with the cloud systems.

End-users who are not Token Vault administrator can access only the **Available authorization providers** page in Token Vault. They can authorize configured Token Vault authorization providers in a cloud system, such as Microsoft 365, iManage Work, Google, Box, Dropbox or NetDocuments to use certain eCopy ShareScan components, such as eCopy ShareScan Exchange connectors configured with modern authentication. These components interact with Token Vault and get access tokens for communication with the cloud systems. Also on this page, users can set up an Authenticator app or enable Token Vault for generating one-time passcodes to use certain eCopy components with one-time passcode authentication method, such as Session logon service configured with Microsoft Entra ID or eCopy SharePoint connector configured with modern authentication. These components interact with Token Vault to verify one-time passcode given by users.

Token Vault in a high availability environment

Multiple Token Vault servers with a common SQL Server database can be configured as part of a network load balancing (NLB) cluster to provide high availability and load balancing features. In this case, Token Vault server nodes form a network load balancing cluster. This means that the cluster is seen by the Token Vault clients (such as eCopy ShareScan) behind the same cluster name/IP address and all Token Vault servers use the same configuration database.

System requirements

To use Token Vault in a high availability environment, make sure the following system requirements are met.

- At least two server machines with supported server operating systems (same version on all nodes)
- Two Network Interface Cards (one for cluster and one for non-cluster operation). Single NIC is not supported
- Only IPv4 is supported (IPv6 is recommended to be disabled on all network adapters used for the cluster)
- Make sure you add the cluster name/IP to the DNS after the cluster configuration, as it may cause issues in the process
- Having a proper DNS entry for the fixed IPs of the nodes used on the NIC which is used for the cluster

Token Vault requirements

To use Token Vault in a high availability environment, make sure the following Token Vault requirements are met.

- The same Token Vault version must be installed on all nodes.
- Centralized common SQL database residing on a server which is not functioning as a Token Vault server node in the cluster. For information on supported SQL server versions, see *Tungsten eCopy ShareScan Technical Specifications*.
- It is recommended to have an SQL cluster instead of a single SQL server, as a single SQL server would be a single point of failure. For full system high availability, a SQL cluster is required (However, it is not enforced by Token Vault. For testing purposes, a single SQL server is appropriate). Token Vault is able to support Microsoft SQL clusters with no limitation.

General recommendations to support high availability

For a high availability implementation, a fully set up and configured Microsoft SQL cluster environment is recommended.

In Windows Service Control Manager, you can enable different actions for the Token Vault service.

To do this, right-click the Token Vault service and select **Properties**. On the **Recovery** of the **Properties** dialog box, select how you want to handle the first, second and subsequent failures. You can also determine the timeframe to reset the fail count or restart the service. It is recommended to enable the automatic service restart in case of a failure with a 1-minute delay.

Depending on your system policy, you may also decide to **Run a program** in the case of a failure. For example, to send a notification email or to perform other action. To do this, select **Run a program** from the **Recovery** tab.

Set up Token Vault in a high availability environment

Before performing the setup, make sure that the following requirements are met.
- Have the Token Vault installer ready
- Have at least two different computers ready for a Token Vault installation in a NLB Cluster environment with unique, fixed IP addresses
- Have a failover-capable Microsoft SQL cluster (recommended) ready to provide the database for your Token Vault installation. A single SQL server instance with proper backup should be sufficient for disaster recovery solutions. However, in a hot failover solution, you may need a SQL cluster with at least two nodes.

To set up all additional Token Vault for high availability, do the following.
1. Install Token Vault on each server node.
2. On the first Token Vault server node, open the Token Vault website and log in with your Token Vault administrator credentials.
3. Configure the database connection parameters for the common Token Vault database.

   For details, see Database settings.
4. On the **Server settings** page, select the address of an appropriate physical network interface as **Node network interface** for Token Vault server node to use in communication between Token Vault server nodes.
5. On the **Server settings** page, configure the **HTTPS port** and the **HTTPS certificate thumbprint**.
   For details, see HTTPS settings.

Requirements for the certificate:
- **Issued to** or **Subject** property must be the fully qualified name of the Token Vault cluster.
- The certificate must be stored in the Local Computer store: Certificates (Local Computer)\Personal.

- The user account of the Windows service running Token Vault must have privileges to use the private key of the certificate.

To use a self-signed certificate for the cluster, generate a new self-signed certificate on the **Server settings** page by following the steps described in HTTPS settings, but in step 3, specify the fully qualified name of the Token Vault cluster as Host name.

Set up additional Token Vault server nodes

To set up all additional Token Vault server nodes, do the following.

1. Install the Token Vault cluster certificate on the new Token Vault server node.

   - If a self-signed certificate was configured in step 5 above:

     a. Copy the following files from the first Token Vault server node to the same location on the new Token Vault server node:
        - `%ProgramData%\Tungsten\TokenVault\TokenVault Root CA.pfx`
        - `%ProgramData%\Tungsten\TokenVault\TokenVault.pfx`
        - `%ProgramData%\Tungsten\TokenVault\TokenVault.pfx.thumbprint.txt`

     b. Install the `%ProgramData%\Tungsten\TokenVault\TokenVault.pfx` certificate file on the new Token Vault server node.

        > ℹ️
        > - The certificate must be stored in the Local Computer store: Certificates (Local Computer)\Personal.
        > - The user account of the Windows service running Token Vault must have privileges to use the private key of the certificate.

   - If your own cluster certificate was configured in step 5 above, copy your own cluster certificate to the new Token Vault server node and install it.

     > ℹ️
     > - The certificate must be stored in the Local Computer store: Certificates (Local Computer)\Personal.
     > - The user account of the Windows service running Token Vault must have privileges to use the private key of the certificate.

2. Open the Token Vault website on the new Token Vault server node and log in with your Token Vault administrator credentials.

3. Configure the database connection parameters for the same common Token Vault database configured for the first Token Vault server node in step 3 above.

   For details, see Database settings.

4. On the **Server settings** page, select the address of the appropriate physical network interface as **Node network interface** for the new Token Vault server node to use in communication between Token Vault server nodes.

> ℹ️ If you modify any Config.json file in any folder under the `%ProgramData%\Tungsten \TokenVault\Plugins` folder, the modified Config.json file must be copied to the same folder on the new Token Vault server node and then the Token Vault Windows service must be restarted.

Upgrade Token Vault in a high availability environment

If you want to upgrade Token Vault in a high availability environment without any down time, do the following.

- Choose a time period when the Token Vault system is not heavily loaded.
- Use the node drain stop (or equivalent) option in the NLB manager tool to take the selected Token Vault server node offline.
- Make sure that all the existing activities have been completed on the selected Token Vault server node.
- Stop the Token Vault Windows service on the selected Token Vault server node.
- Perform the upgrade to a newer Token Vault version on the selected Token Vault server node.
- Test Token Vault functionality by opening the Token Vault website on the selected Token Vault server node and log in with your Token Vault administrator. Token Vault will open in maintenance mode and only configuration settings pages are available.
- Do not select **Upgrade database** on the **Database Settings** page.
- Do not bring the selected Token Vault server node in the NLB Manager tool online/active.

1. Repeat the above steps on the Token Vault server nodes until half of the nodes are upgraded to the new Token Vault version.

   If the first half of the nodes are upgraded, the old nodes (still on earlier Token Vault version) should be taken offline via node drain stop (or equivalent) option in the Microsoft NLB manager tool.

2. When all earlier Token Vault version nodes are in stopped state, stop the Token Vault Windows service on them.

3. On one of the Token Vault server nodes which are already upgraded to the new Token Vault version, upgrade database on the **Database Settings** page (for details, see [Database settings](#)) and restart the Token Vault service.

   This node notifies other Token Vault server nodes with newer Token Vault version about this change and request restart.

4. When all Token Vault server nodes with newer Token Vault version are restarted, bring the upgraded Token Vault server nodes in the NLB manager tool online/active.

5. Perform the upgrade to the newer Token Vault version on all remaining old Token Vault server nodes.

6. Open the Token Vault website on each node and log in with your Token Vault administrator to make sure that each of them works without any issues.

7. Bring the recently upgraded Token Vault server nodes in the NLB manager tool online/active.