Kofax Token Vault

Installation Guide

Version: 3.5

Date: 2021-03-05

KOFAX

Table of Contents

Preface

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

Training

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

Getting help with Kofax products

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

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

Note The Kofax Knowledge Base is optimized for use with Google Chrome, Mozilla Firefox or Microsoft Edge.

The Kofax 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 Kofax 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 Kofax Portal login to view related articles.
- Access to the Kofax 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 Kofax 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 Kofax 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.

Chapter 1

Introduction

Token Vault is a web application hosted by a Windows service. Token Vault manages and stores authentication tokens and provides these tokens to other applications that interact with cloud systems. Token Vault also manages authorization provider registrations and user authorizations.

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

Chapter 2

Install Token Vault

Before you install Token Vault, ensure that:

- You have Microsoft SQL Server 2014 or later installed and accessible
- Your system has the setup prerequisites installed:
  - Microsoft ASP.NET Core 3.1.8 - Shared Framework
  - Microsoft .NET Core Runtime - 3.1.8 (x64)
  - Microsoft .NET Framework 4.8 Setup
- You deploy Token Vault on a computer which is a member of a domain.

If any of these prerequisites are missing, check the Token Vault deployment package for their installer files.

Perform a new installation

1. Verify that you are performing installation with administrator privileges.
2. Run TokenVault3.5.exe.

   The **Choose setup language** screen is displayed.
3. Select a preferred language (English by default) from the list and click **Next**.

   The **Welcome** screen is displayed.
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 is displayed.
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 Integrated Authentication for the database connection.

   The **Database Server – Administrative Credentials** is displayed.
8. Specify the database server that you are connecting to, along with the database catalog name.

9. In the same screen, select one of the following authentication methods for database actions:
   a. Use the Windows authentication credentials of the current user
   b. Specify SQL Server authentication credentials.

   The credentials specified are only used during deployment to run the Token Vault SQL scripts on the selected database.
10. Next specify Runtime Credentials for the Database Server.

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

    The **Installation Summary** screen is displayed.
11. Review the information and if you are satisfied with the configuration click **Install**, otherwise click **Back**.
12. Click **Finish** when the **InstallShield Wizard Completed** screen appears.

Upgrade Token Vault

If you have Token Vault version 2.x or 3.0 installed already, perform the following steps to upgrade to the current version:

1. Run TokenVault3.5.exe.

   The installer automatically detects the earlier version.
2. Follow the installer prompts to complete the upgrade process.

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

Chapter 3

Configuration settings

Token Vault and authorization provider configuration settings are stored in .json files under the <Common Application Data folder> of Token Vault, such as `C:\ProgramData\Kofax\TokenVault`.

Token Vault configuration settings

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

Modify this *appsettings.json* file using any text editor to change the behavior of Token Vault. Restart the Kofax Token Vault Service Windows service to apply the changes.

Note We recommend that you always keep a backup copy of this file. An incorrect *appsettings.json* file may cause the Token Vault service to become inoperable.

Database connection

To change the database connection manually, modify the "DatabaseConnectionString" property of the "appsettings.json" file.

The following example shows a database connection string: the SQL Server is *MySqlServer*, database name is *TokenVault* and Integrated Windows authentication is configured (Integrated Security=*True*).

```
...
  "DatabaseConnectionString": "Data Source=MySqlServer\\MySQLInstance;
Initial Catalog=TokenVault;Integrated Security=True;Connect Timeout=30;",
...
```

Note Backslash ('\') characters in the connection string must be duplicated.

We highly recommend that you use Windows Integrated Authentication for Token Vault database connection.

Set port for HTTP protocol

- The default HTTP port for Token Vault is 8380.
- **We highly recommend that you use HTTPS protocol.**
- To change the port number, modify the *Port* property of the *appsettings.json* file.

```
...
"Port": 8380,
```

```
...
```

Set HTTPS protocol and related configuration settings

To enable the HTTPS protocol:

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

   ```
   ...
   "HttpsPort": 8381,
   ...
   ```

2. Set *HttpsCertificateThumbprint* to the thumbprint of the certificate that you want to use for your Token Vault instance.

   Certificate:

   - *Issued to* or *Subject* property must be the fully qualified name of the computer where the Token Vault is installed and
   - 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.

     Example:

     ```
     ...
     "HttpsCertificateThumbprint": "f5997a4edf5e9a1f67665d17167ef5a6da4a571b",
     ...
     ```

3. Save your changes to the *appsettings.json* file.
4. Encrypt Token Vault sensitive data with the certificate
   a. Open a Command prompt window as the user who runs the Kofax Token Vault Windows service.
   b. Navigate to the Token Vault installation folder.
   c. Run the following command:

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

      where

      - <new certificate thumbprint> is the thumbprint of the new certificate
      - <old certificate thumbprint> is the thumbprint of the old certificate. Leave blank if HTTP protocol was previously specified.
5. Restart the *Kofax Token Vault Service*.

Important When you replace the certificate configured for Token Vault with a new one, Token Vault sensitive data must be re-encrypted with the new certificate by repeating the steps described in step 4 above. In this case, the <old certificate thumbprint> parameter value must be the thumbprint of the old certificate.

Set configuration settings related to tracing

- The *LoggingTraceLevel* setting value determines how detailed the Token Vault trace is. The default value of this configuration setting is *Verbose*.

```
...
   "LoggingTraceLevel": "Verbose",
...
```

  Other possible values are: *Error*, *Warning*, *Info*, and *Off* .
- To turn off tracing, change this property to *Off* and restart the *Kofax Token Vault Service*.
- The Token Vault trace files (one on each day) are created in the <Common Application Data folder>\Kofax\TokenVault\Logs folder (typically C:\ProgramData\Kofax\TokenVault\Logs).
- The *PreserveLogFilesInDays* 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.

Next steps

After you successfully install 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.

Chapter 4

Token Vault URL and functions

The URL required to access the Token Vault website depends on the configured value of *HttpsPort* or *Port* configuration settings in the *appsettings.json* configuration file.

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 *HttpsPort* 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

Important We highly recommend that you use 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

Note The first user who logs into the Token Vault website automatically becomes 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 eCopy, for example eCopy ShareScan Exchange connectors configured with modern authentication. These applications interact with Token Vault and get access tokens for communication with the cloud systems.