Kofax Token Vault

Installation Guide

Version: 3.0

Date: 2020-07-08

Contents

Introduction

This guide is intended for Token Vault administrators. It provides instructions for deploying Token Vault. To learn more about configuring Token Vault for managing cloud storages such as Exchange Online or NetDocuments registrations, refer to the documentation of the actual product that integrates with Token Vault in order to acquire tokens and communicate with cloud storages.

Token Vault is a web application hosted by a windows service. Use Token Vault to manage and store authentication tokens by user for supported cloud storages, and to provide these tokens to other applications that interact with these cloud storages. (These interacting applications are referred to as "Token Vault clients" – e.g. eCopy ShareScan connectors). Token Vault also manages cloud storage and Token Vault client registrations and user authorizations.

One Token Vault instance can serve several Token Vault clients (e.g. eCopy ShareScan connectors on different eCopy ShareScan servers.)

Support Information

This section contains information on the various languages and browsers supported by Token Vault.

SUPPORTED LANGUAGES

- Brazilian Portuguese
- Catalan
- Chinese (Simplified)
- Dutch
- English
- French
- German
- Italian
- Japanese
- Spanish

SUPPORTED BROWSERS

- Chrome
- Edge
- Firefox
- Internet Explorer 11

Deploying 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 2.1.17 - Shared Framework
  - Microsoft .NET Core Runtime - 2.1.17 (x64), and
  - Microsoft .NET Framework 4.7.1 Setup

  Installer files for these prerequisites are included in the Token Vault deployment package.
- You deploy Token Vault on a machine which is a member of a domain.

Deploying on a clean system

Verify that you are performing installation with administrator privileges.

1. Run TokenVault3.0.exe. Choose setup language screen is displayed. Select a preferred language (English by default) from the dropdown list and click Next.
2. The Welcome screen is displayed. Click Next.
3. The End-User License Agreement (EULA) is displayed on the License Agreement screen. Accept the EULA and click Next.
4. The Destination Folder screen is displayed. Click the Change button to modify the default destination folder then click Next.
5. Specify service credentials for the Token Vault Service on the Service Credentials screen. Alternatively, you can choose to use LocalSystem credentials. Specifying service credentials is the recommended option so that you can use Windows Integrated Authentication for database connection.
6. The Database Server – Administrative Credentials is displayed. Specify the database server that you are connecting to as well as the database catalog name.
7. In the same screen select the authentication method for database actions:
   a. Either use the Windows authentication credentials of the current user, or
   b. Specify SQL Server authentication credentials. The credentials specified in this dialog are only used during deployment to run the Token Vault SQL scripts on the selected database.
8. Next specify Runtime Credentials for the Database Server. The Token Vault service will use these credentials only for runtime connection to the SQL server.
9. The Installation Summary screen is displayed. Review the information and if you are satisfied with the configuration click Install, otherwise click Back.
10. Click Finish when the InstallShield Wizard Completed screen appears.

Upgrading Token Vault

If you have Token Vault version 2.x installed already:

1. Run TokenVault3.0.exe. The installer automatically detects the earlier version.
2. Follow the instructions to complete the upgrade process.

IMPORTANT: Upgrade from Token Vault 1.x is not supported.

Configuration settings

Token Vault and cloud storage configuration settings are stored in json files under the common application data folder of Token Vault (e.g. 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 of Token Vault (e.g. 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: It is recommended that you always keep a backup copy of this file. An incorrect ***appsettings.json*** file can make the Token Vault service inoperable.

Database connection

The database connection parameters are collected and set by the *setup.ps1* script.

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.

It is highly recommended that you use Windows Integrated Authentication for Token Vault database connection.

Port (for HTTP protocol)

The default HTTP port for Token Vault is 8380.

To change the port number, modify the ***Port*** property of the ***appsettings.json*** file.

```
…
     "Port": 8380,
…
```

It is highly recommended that you use HTTPS protocol.

HTTPS protocol and configuration settings

To enable the HTTPS protocol perform the following steps:

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. The certificate
   - "Issued to" or "Subject" property must be the fully qualified name of the machine where the Token Vault is installed and
   - it must be stored in the Local Computer store:
     Certificates (Local Computer)\Personal
   - The user account of the windows service running Token Vault must have privilege to use the private key of the certificate.
     For example:

```
…
    "HttpsCertificateThumbprint": "f5997a4edf5e9a1f67665d17167ef5a6da4a571b",
…
```

3. Save your changes to the ***appsettings.json*** file.
4. Restart the **"*Kofax Token Vault Service*"** windows service.

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*', '*Off '*.

To turn off tracing change this property to *'Off '* and restart the "*Kofax Token Vault Service*" windows service.

The Token Vault trace file is created in the <*Common Application Data folder*>*Kofax**TokenVault**Logs* folder (typically *C:\ProgramData**Kofax**TokenVault**Logs*).

NetDocuments connector configuration settings

NetDocuments connector configuration settings are stored in the *TokenVault.Connectors.NetDocuments.config.json* file.

This file is located in the common application data folder of the NetDocuments connector (e.g. C:\ProgramData\Kofax\TokenVault\plugins\NetDocuments).

Modify this *TokenVault.Connectors.NetDocuments.config.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: It is recommended that you keep a backup copy of this file at all times. An incorrect *TokenVault.Connectors.NetDocuments.config.json* file can make the Token Vault NetDocuments connector inoperable.

NETDOCUMENTS SERVICE HOST

NetDocuments service hosts vary by region:

- US: vault.netvoyage.com
- EU: eu.netdocuments.com
- AU: au.netdocuments.com

The Token Vault NetDocuments connector communicates with and requests authentication tokens from a NetDocuments service host. The NetDocuments service host is specified in the **WebService** setting value.

The default value is '*vault.netvoyage.com*'; that is the host that belongs to the US region:

```
...
    "WebService": "vault.netvoyage.com",    // US
  //"WebService": "eu.netdocuments.com",    // EU
  //"WebService": "au.netdocuments.com",    // AU
…
```

To modify the default value comment out the corresponding by inserting '//' before the *"WebService"* string and uncomment the line containing your chosen service host by deleting '//' from the beginning of the line.

Other configuration settings (**LoginUrl**, **ApiUrl** and **LogoutUrl**) in this json file are static and based on the value of the **WebService** setting.

Token Vault URLs

Token Vault has an admin website and an end-user website.

The **admin website** is intended for Token Vault administrators to

- register cloud storages such as Exchange Online, SharePoint Online or NetDocuments
- manage Token Vault administrators, Token Vault clients, and
- review and delete cloud storage registrations by users and cloud storages.

The first user who logs into the admin website automatically becomes Token Vault administrator.

The **end-user web site** is intended for users to authorize Token Vault for cloud storages (such as Exchange Online, SharePoint Online or NetDocuments) to use applications (for example eCopy ShareScan Exchange connectors configured with modern authentication). These applications are referred to as Token Vault clients. They interact with Token Vault and get access tokens for communication with the cloud storages.

The actual URLs to access these two Token Vault websites depend on the configured value of **HttpsPort** or **Port** configuration settings in the ***appsettings.json*** configuration file:

Using HTTPS:

Admin website	End-user website
https://FQDN:port/admin	https://FQDN:port or https://FQDN:port/user

FQDN is the Fully Qualified Domain Name of the machine where Token Vault is deployed **port** is the port configured as the value of **HttpsPort** configuration setting

Examples for admin and end-user websites:

https://machinename.mydomain.com:8381/admin
https://machinename.mydomain.com:8381/user

Using HTTP:

Admin website	End-user website
http://FQDN:port/admin	http://FQDN:port or http://FQDN:port/user

FQDN is the Fully Qualified Domain Name of the machine where Token Vault is deployed **port** is the port configured as the value of **Port** configuration setting

Examples for administrator and end-user websites:

http://machinename.mydomain.com:8380/admin
http://machinename.mydomain.com:8380/user

IMPORTANT: It is highly recommended that you use https. When HTTPS is used, all requests arriving to the HTTP port will be redirected to HTTPS.

Next Steps

After you successfully installed Token Vault, you are ready to configure it for managing cloud storages such as Exchange Online or NetDocuments.