One Identity Defender AD FS Adapter 5.10

Administration Guide

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Defender AD FS Adapter Administration Guide
Updated - February 2019
Version - 5.10

Contents

1

Overview

One Identity Defender AD FS Adapter integrates with Microsoft Active Directory Federation Services (AD FS) to add Two-Factor authentication to services using browser-based federated logins. Defender AD FS Adapter supports relying parties that use Microsoft WS-Federation protocol, such as Office 365, and SAML 2.0 federated logons for cloud apps such as Google Apps, and salesforce.com. Defender AD FS Adapter supports Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019.

2

Prerequisites

Before installing Defender AD FS Adapter in the system, verify the following:

- Microsoft .NET Framework 4.5.2 or later is installed
- Defender Client SDK 5.9.1 or later is installed
- AD FS role is installed and the AD FS service is running
- PowerShell 4.0 or later is installed
- The federated logins to the relying parties are configured and working

Connectivity Requirements

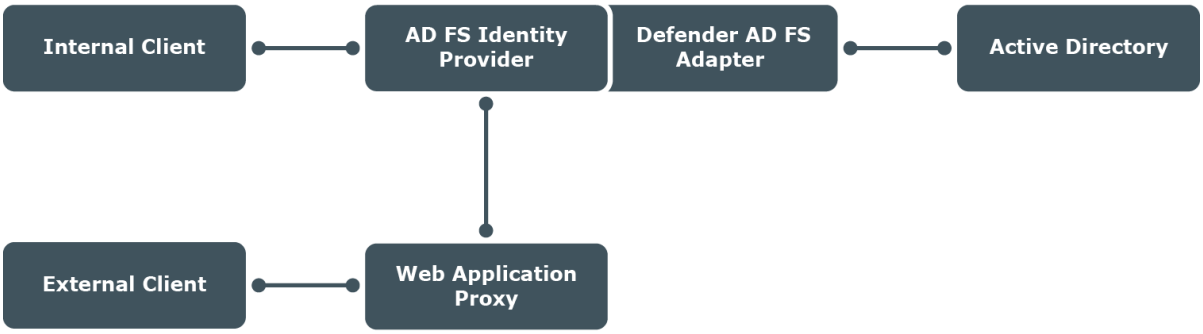
After verifying and setting up the prerequisites, connecting to Defender through Defender AD FS Adapter requires the following parameters:

- IP address or DNS name of Defender Security Server (DSS)
- Port number (Default value is 1812)
- Timeout (Default value is 15 seconds)
- Shared Secret (The shared secret must be same as the shared secret configured in Defender Access Node.)
- User ID Attribute (The User ID Attribute must be same as the User ID Attribute configured in Defender Access Node. The default value is the SAM Account Name.)

Deployment Overview

Defender AD FS Adapter adds Multi-Factor Authentication (MFA) that provides a Two-Factor authentication prompt to web-based logins through AD FS server or Web Application Proxy. After completing the primary AD FS server authentication (using standard means such as Windows Integrated or Forms-Based), you must complete Defender authentication

challenge before getting redirected to the relying party. If the deployment is in an AD FS farm, install Defender AD FS Adapter on all AD FS servers in the farm.



After the installation of Defender AD FS Adapter on the AD FS servers in the farm, while configuring the Multi-Factor Authentication policies, select the MFA location (**Internal access** or **External access** or both as per the requirement). If you require Two-Factor authentication for External access locations, a Web Application Proxy is required and you do not have to install Defender AD FS Adapter on the Web Application Proxy server.

Installing Defender AD FS Adapter

This section describes the procedure that is required to run the installer and complete the installation of Defender AD FS Adapter.

To run the Installer

1. Launch Defender AD FS Adapter installer EXE from an elevated command prompt (right-click **Command Prompt** and select **Run as Administrator**).
2. Accept the license agreement and continue with the installation.
3. Complete the remaining steps for installing Defender AD FS Adapter.

   NOTE: AD FS service will restart during installation.
4. By default the **Start Defender AD FS Configuration Tool** check box is selected. Clear the check box if you do not want to configure Defender AD FS. Click **Finish** to complete the setup and start Defender AD FS Adapter configuration tool.

NOTE: After the configuration of Defender AD FS Adapter, in the AD FS Management console, select **One Identity Defender AD FS Adapter** as the Multi-factor Authentication method.

Upgrading Defender AD FS Adapter

This section describes the procedures that must be followed before upgrading One Identity Defender AD FS Adapter on the operating systems listed below.

- Windows Server 2012 R2
- Windows Server 2016 or Windows Server 2019

Windows Server 2012 R2

Before Upgrading One Identity Defender AD FS Adapter, perform the following:

1. Launch the **AD FS Management console** on the primary server in the AD FS farm.
2. Navigate to **AD FS | Authentication Policies**, and click **Edit Global Multi-factor Authentication**. Alternatively, navigate to **Multi-factor Authentication | Global Settings**, and click **Edit**.
3. In the **Edit Global Authentication Policy** dialog box, click **Multi-factor**.
4. Clear the **One Identity Defender AD FS Adapter** authentication method.

Windows Server 2016 or Windows Server 2019

Before Upgrading One Identity Defender AD FS Adapter, perform the following:

1. Launch the **AD FS Management console** on the primary server in the AD FS farm.
2. Navigate to **AD FS | Service | Authentication Methods**.
3. Click **Edit** under **Multi-factor Authentication Methods**. Alternatively, click **Edit Multi-factor Authentication Methods**.
4. Clear the **One Identity Defender AD FS Adapter** authentication method.

To install the One Identity Defender AD FS Adapter, use the **DefenderADFSAdapter.exe** file, and follow the on-screen instructions. For information on the procedure to be followed after installing Defender AD FS Adapter, see Configuring AD FS Multi-factor Authentication (MFA).

Configuring Defender AD FS Adapter

This section provides the procedure that you must follow to configure Defender AD FS Adapter.

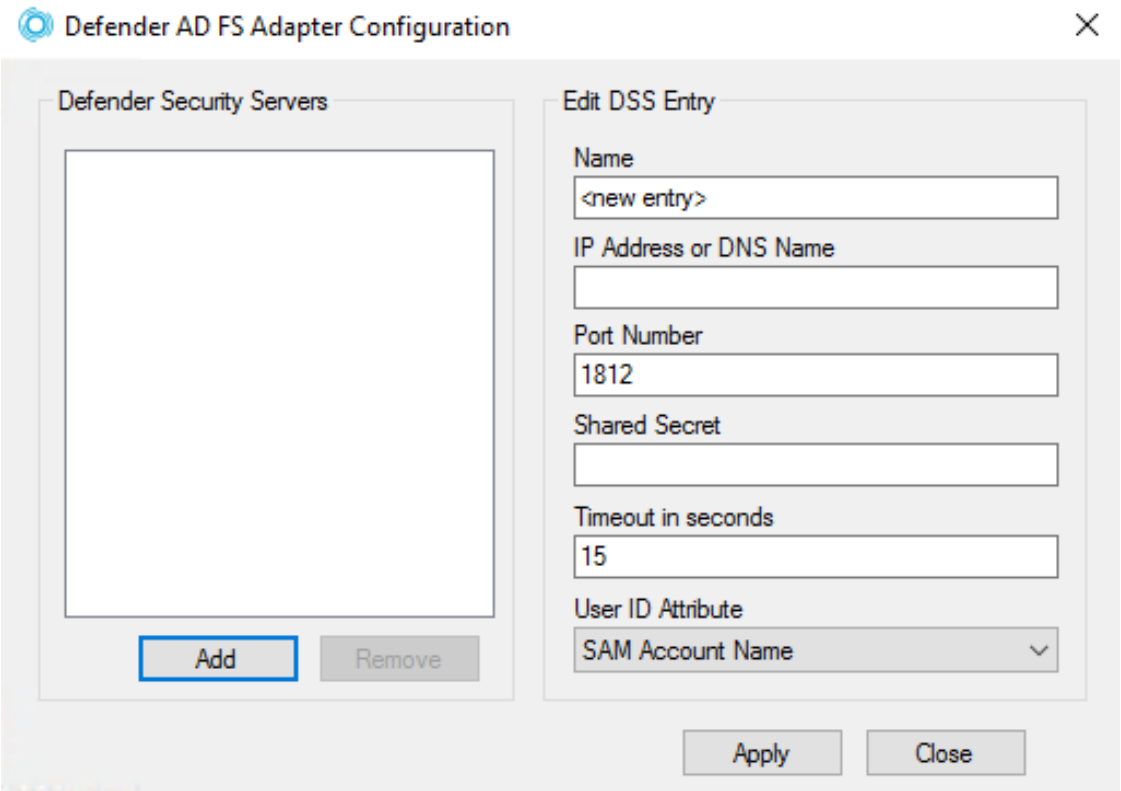
To configure Defender AD FS Adapter

1. On the computer where the Defender AD FS Adapter is installed, run the Defender AD FS Adapter Configuration tool.

   NOTE: Configuration is required for all installations of AD FS servers in the farm.

2. In the dialog box that opens, specify the Defender AD FS Adapter settings, and then click **OK**.

   The dialog box looks similar to the following:



- Use this area to set up a list of the Defender Security Servers to which you want the Defender AD FS Adapter to connect.
  - **Add** Adds a new entry to the Server list. After adding a new entry, edit the properties of the server added in the **Edit DSS Entry** area.
  - **Remove** Removes the selected entry from the list.
- **Edit DSS Entry** Use this area to specify or edit the name, address, port number, and shared secret of the Defender Security Server to which you want the Defender AD FS Adapter to connect.
  - **Name** Type the name of the Defender Security Server you want to use for user authentication.
  - **Address** Type the IP address of the Defender Security Server.
  - **Port** Type the communication port number configured on the access node you want the Defender AD FS Adapter to use. The default value is set to **1812**.
  - **Shared Secret** Type the shared secret configured on the access node you want the Defender AD FS Adapter to use.
  - **Timeout in seconds** Specify the default timeout value in seconds. The default timeout is set to **15** seconds.
  - **User ID Attribute** Select the name of the attribute containing the user ID used to authenticate. User ID value must match with DSS Access Node. The default value is set to **SAM Account Name**.

Enable LDAP over SSL

Enabling LDAP over SSL enables communication with the Active Directory server.

NOTE: Enabling LDAP over SSL is required for all installations of AD FS servers in the farm.

To enable LDAP over SSL for communicating with Active Directory server

On a computer where Defender AD FS Adapter is installed, create the following value in the "**HKEY_LOCAL_MACHINE\SOFTWARE\One Identity\Defender\AD FS Adapter**" registry key using the Registry Editor:

- Value type: **REG_DWORD**
- Value name: **LdapOverSsl**
- Value data: **1**

Configuring AD FS Multi-factor Authentication (MFA)

This section provides information on the configuration of AD FS Multi-factor Authentication on the operating systems listed below.

- Windows Server 2012 R2
- Windows Server 2016 or Windows Server 2019

Windows Server 2012 R2

To configure AD FS Multi-factor Authentication

1. Launch the **AD FS Management console** on the primary AD FS internal server.
2. Navigate to **AD FS | Authentication Policies**, and click **Edit Global Multi-factor Authentication**. Alternatively, under **Multi-factor Authentication | Global Settings** section, click **Edit**.
3. In the **Edit Global Authentication Policy** window, click **Multi-factor**.
4. In **Users/Groups** section, click **Add** and select a domain for MFA (for example, Domain Users).

   NOTE: The Users or the Groups must be a member of Defender Access Node.

5. In the **Location** section, select **Extranet** and/or **Intranet** check boxes depending on the required type of connection.

   For example, if you always require two-factor authentication, select both **Extranet** and **Intranet** when configuring the multi-factor authentication policy. If you want to enforce two-factor authentication for external users, and if you have configured your network such that external users communicate with an AD FS Web Application Proxy while internal users communicate with the Identity Provider, select only **Extranet**.
6. Select **One Identity Defender AD FS Adapter** authentication method to enable multi-factor authentication using Defender.

NOTE: In an advanced multi-factor scenario, you can select **Intranet** and/or **Extranet** for each user or for each relying party. For more information, see the Microsoft's TechNet article *Overview: Manage Risk with Additional Multi-Factor Authentication for Sensitive Applications*.

Windows Server 2016 or Windows Server 2019

To configure AD FS Multi-factor Authentication

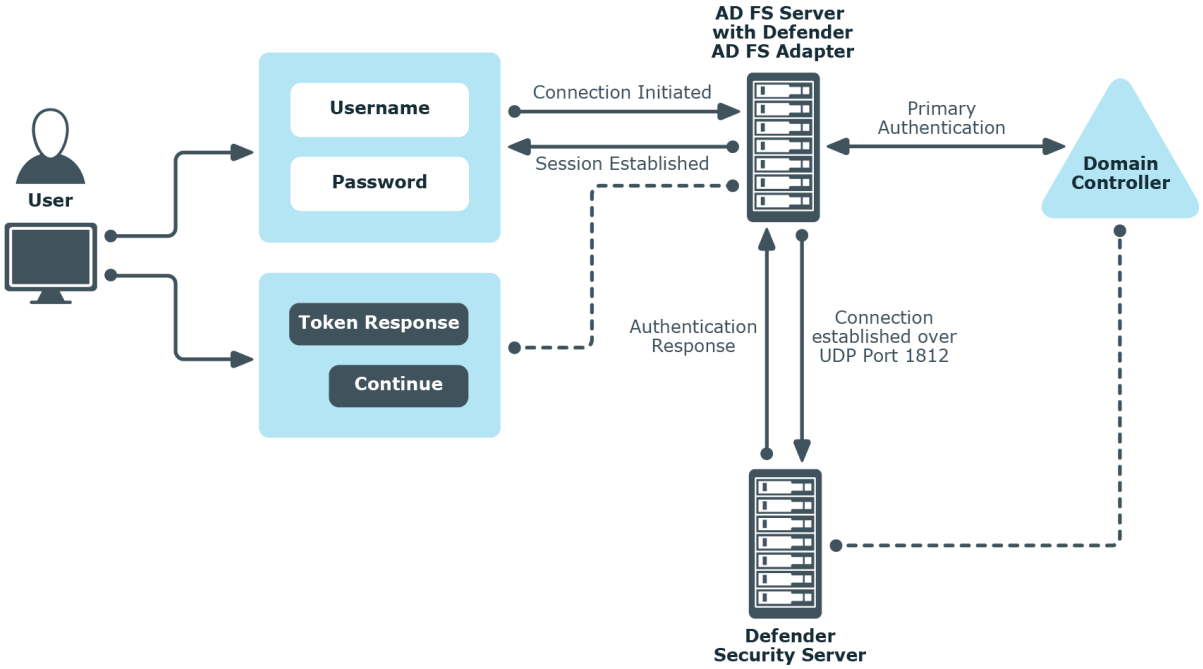
1. Launch the AD FS Management console on your primary AD FS internal server and navigate to **AD FS** | **Service** | **Authentication Methods**.
2. Click the **Edit** link under **Multi-factor Authentication Methods** or click **Edit Multi-factor Authentication Methods**.
3. Select the box next to the **One Identity Defender AD FS Adapter** authentication method to enable MFA authentication. Click **OK**.
4. Go to **AD FS** | **Access Control Policies** and edit one of the existing MFA policies to apply it to users or groups. Alternatively, create a new MFA policy if no pre-defined policy is sufficient for your organization's MFA requirements.
5. Go to **AD FS** | **Relying Party Trusts**, right-click the relying party trust where you want to add Defender AD FS, and then select **Edit Access Control Policy**.
6. Pick a policy for the relying party that includes MFA and then click **OK**. The MFA policy immediately applies to the selected relying party.

Network Diagrams

Diagramatic representations of Defender AD FS Adapter Authentication and Office 365 Integration are made in this section.

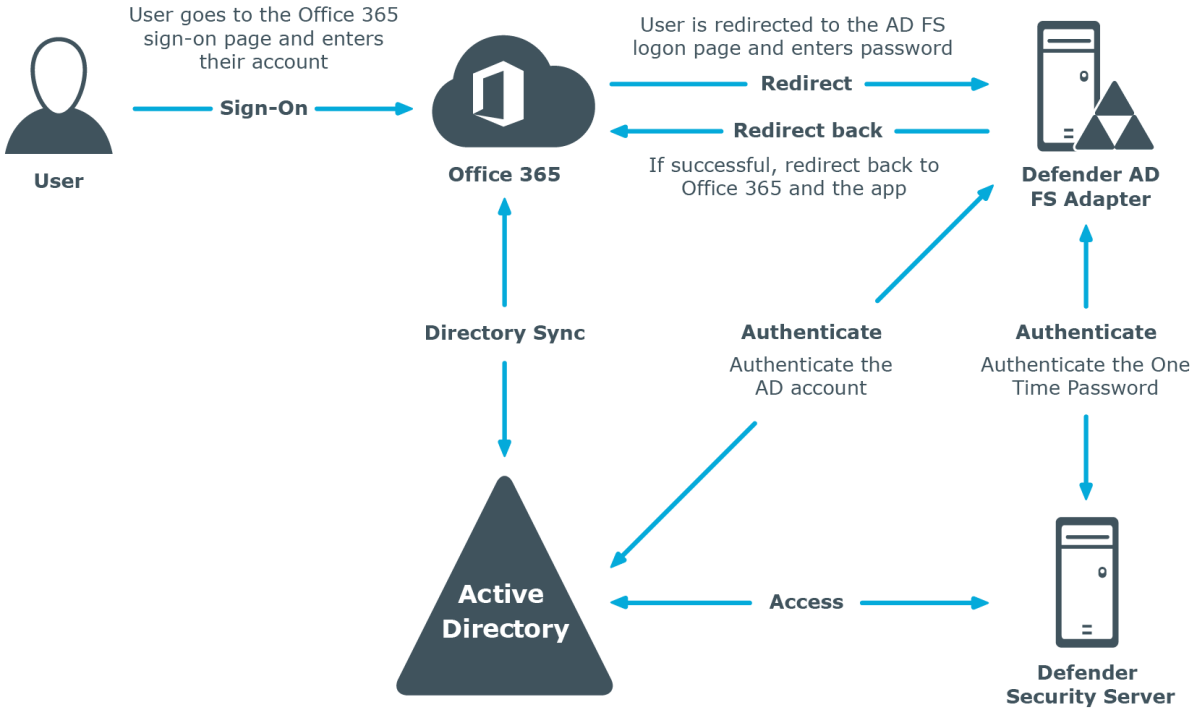
Defender AD FS Adapter Authentication

The Defender AD FS Adapter Authentication workflow is depicted in the diagram below.



Office 365 Integration

The process involved in the integration of Office 365 and Defender AD FS Adapter is depicted in the diagram below.



Test Your Setup

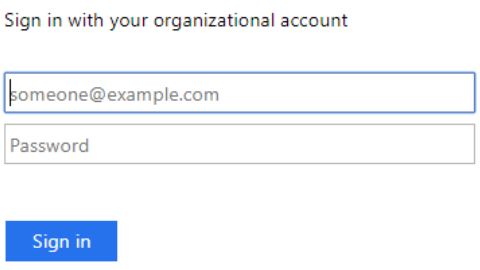
To test your setup, do the following:

1. Using a web browser log in to a relying party for your AD FS deployment. For example, you can log into https://portal.microsoftonline.com to access Office 365.
2. Complete primary authentication of your AD FS server. The two-factor authentication page is displayed.
3. In the **Token Response** field, enter the response displayed on your token. The authentication type depends on the Defender policy that has been configured. For example, if Defender is configured to use a token policy, the **Enter Synchronous Response** prompt is displayed.

Using GrIDsure tokens for Authenticating AD FS relying parties.

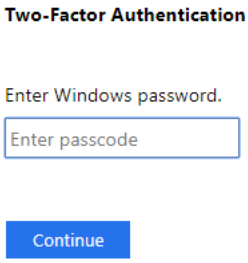
To authenticate on a AD FS relying party by using the GrIDsure token

1. In your Web browser, enter the address of the AD FS relying party you want to access.
   If the AD FS relying party is protected with the GrIDsure personal identification system, the following page opens:

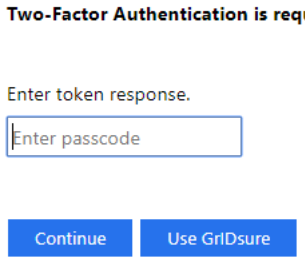


2. Type your user name, password, and then click **Sign In**.

When configuring GrIDsure token for the first time, the login page prompts you to enter your Windows password:



The page that opens may look different if you have two or more types of Defender Tokens assigned:



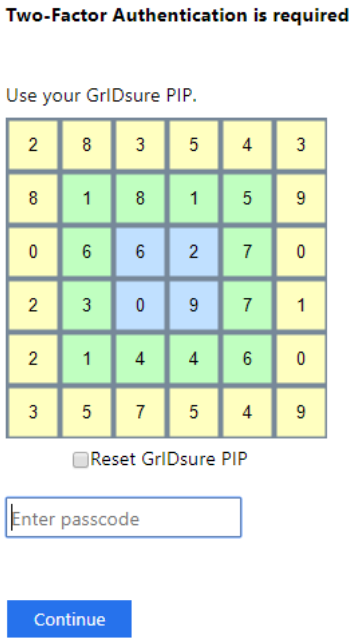
In this case, click **Use GrIDsure**.

3. Type your Windows password, and then click **Continue**.

   If this is the first time you are authenticating using the GrIDsure token, you may be prompted to configure your GrIDsure Personal Identification Pattern (PIP). For more information, see How to configure and use your Personal Identification Pattern (PIP).

4. You are now prompted to authenticate using your GrIDsure PIP. Type the numbers located in the cells you chose when configuring your GrIDsure PIP.
5. In the **Enter passcode** text box, type your PIP, and then click **Sign In** to access the protected Web site. You can select the **Reset PIP** check box to reset your current

PIP after you sign in.



How to configure and use your Personal Identification Pattern (PIP)

To authenticate with the GrIDsure token, you need to use a special code, the GrIDsure Personal Identification Pattern (PIP).

When you access a resource protected with the GrIDsure personal identification system for the first time, you are prompted to configure your PIP. In this case, a matrix of cells similar to the following image is displayed:

In this matrix, choose the cells you want to use for authentication, and then, in the **Configure your GrIDsure PIP** text box, type the codes contained in the cells you have chosen. Do not leave blank spaces between the codes.

For example, if you choose the first four cells in the first row of the matrix above, in the **Configure your GrIDsure PIP** text box, type **CCAPBCAH** (without spaces), and then press **ENTER** or click **Continue**.

From now on, each time you authenticate with your GrIDsure token, you must use the codes displayed in the matrix cells you have chosen when configuring your PIP. These codes will be different each time the matrix of cells displays.

For example, next time the matrix may look as follows:

2	8	3	5	4	3
8	1	8	1	5	9
0	6	6	2	7	0
2	3	0	9	7	1
2	1	4	4	6	0
3	5	7	5	4	9

In this case, use the **Use your GrIDsure PIP** text box to type **2835**, and then press ENTER or click **Continue**.

10

Diagnostic logging

To troubleshoot issues that may occur during authentication with Defender, you must enable diagnostic logging for the Defender AD FS Adapter.

To enable diagnostic logging for Defender AD FS Adapter

- On a computer where Defender AD FS Adapter is installed, create the following value in the

  HKEY_LOCAL_MACHINE\SOFTWARE\One Identity\Defender\AD FS Adapter registry key using the Registry Editor:

  Value type: **REG_DWORD**

  Value name: **Diagnostics**

  Value data: **1**

The path to the log file: **%ProgramData%\One Identity\Defender\Diagnostics\AD FS Adapter**

File name for Adapter: **DefenderAdapter.log**

File name for Configuration tool: **Configuration.log**

To disable diagnostic logging for Defender AD FS Adapter, delete the Diagnostics value from the Defender AD FS Adapter registry key or set the value data to **0**.

About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product