One Identity Defender 5.11

Quick Start Guide

Legend

WARNING: A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.

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

Defender Quick Start Guide
Updated - August 2020
Version - 5.11

Contents

Deploying Defender

This section describes how to install Defender for the first time. Before you start, make sure that:

- **The target computer is in a safe location** The computer on which you plan to install the required Defender features is in a secure location to which you have physical access, has TCP/IP installed and static IP address, and meets the applicable system requirements described in the D*efender Release Notes*.
- **The account under which you plan to install Defender has sufficient permissions** The account under which you will be running the Defender Setup must be a member of the local administrators group. To install the Defender Management Portal, this account must also have the permissions to create and delete child Active Directory objects under the computer account object corresponding to the computer where the Management Portal is installed.
- **You have prepared a service account** This is the account under which Defender will be accessing Active Directory®. The Defender Setup extends standard Active Directory schema classes and attributes and defines new Defender-specific classes in the Active Directory schema. For more information about these classes and attributes, see "Appendix C: Defender classes and attributes in Active Directory" in the *Defender Administration Guide*.

  The service account must have the following permissions:

  - Create and modify Active Directory classes and attributes in the forest schema. By default, members of the Schema Admins group have these permissions.
  - Create and modify control access right objects in the forest configuration container. By default, members of the Enterprise Admins group have these permissions.
  - Create organizational units in the specified Active Directory domain. By default, members of the Domain Admins group have these permissions.

You can install Defender on physical computers or virtual machines. To install Defender for the first time, complete the following steps:

- Install required Defender components
- Configure Defender Security Server
- Create and configure objects in Active Directory
- Program and assign security tokens to users

By completing these steps, you get a base Defender configuration which you can then extend to suit your needs. For example, you can extend the base configuration to do the following:

- Authenticate users who access you company's resources via VPN. For more information, see "Securing VPN access" in the Defender Administration Guide.

- Authenticate users when they access Web sites hosted on Microsoft Web Server (IIS). For more information, see "Securing Web sites" in the Defender Administration Guide.
- Authenticate users when they sign in to their Windows®-based computers. For more information, see "Securing Windows-based computers" in the Defender Administration Guide.
- Authenticate users when they access a PAM-enabled service in UNIX or Linux®. For more information, see "Securing PAM-enabled services" in the Defender Administration Guide.

Install required Defender components

To install the required Defender components

1. In the Defender distribution package, open the Setup folder, and run the **Defender.exe** file.
2. Complete the Defender Setup Wizard to install the required Defender components.

   For more information on how to start and use the Defender Security Server Configuration tool, see Defender Setup Wizard reference.

Configure Defender Security Server

Use the Defender Security Server Configuration tool to configure the Defender Security Server you have installed in Install required Defender components. By default, this tool starts automatically when you complete the Defender Setup Wizard.

For more information on how to start and use the Defender Security Server Configuration tool, see Defender Security Server Configuration tool reference.

Create and configure objects in Active Directory

In this step, you create and configure a number of required Defender-related objects in Active Directory. The required objects are:

- Defender Security Policy
- Defender Security Server
- Access Node

For detailed instructions on how to create and configure Defender objects in Active Directory, see "Managing Defender objects in Active Directory" in the *Defender Administration Guide*.

Defender Security Policy

A *Defender Security Policy* object defines a number of authentication settings for Defender users, such as primary and secondary authentication methods, number of allowed failed authentication attempts, lockout and unlock conditions for the user accounts, and allowed logon hours. You can also use a Defender Security Policy object to enable and configure built-in security tokens, such as SMS token, e-mail token, and GrIDsure token.

After creating a Defender Security Policy object, you need to assign it to the appropriate user objects in Active Directory. You can assign a Defender Security Policy in one of the following ways:

- **Explicitly** Assign a policy directly to a user object in Active Directory.
- **Implicitly** Apply a policy to a user by assigning it to the Defender Security Server or Access Node to which the user belongs.

If you assign a Defender Security Policy to a Defender Security Server, that policy is applied to the users who authenticate through that Defender Security Server.

If you assign a Defender Security Policy to an Access Node object, that policy is applied to the users who are listed as members of that Access Node.

When a user is a member of an Access Node and no Defender Security Policy is defined for the user explicitly or implicitly, then a default Defender Security Policy applies to the user. For more information, see "Default Defender Security Policy" in the *Defender Administration Guide*.

To create a Defender Security Policy object

1. On the computer where the Defender Administration Console is installed, open the Active Directory Users and Computers tool (dsa.msc).
2. In the left pane, expand the node representing the domain where you installed Defender.
3. Expand the **Defender** container, right-click the **Policies** container, and then from the shortcut menu select **New | Defender Policy**.

For detailed instructions on how to create and configure a Defender Security Policy object, see "Managing Defender Security Policy objects" in the *Defender Administration Guide*.

Defender Security Server

A *Defender Security Server* object represents a computer on which the Defender Security Server component is installed. Therefore, when creating or configuring a Defender Security

Policy object, make sure you specify the correct IP address of the corresponding computer in the object properties.

To create a Defender Security Server object

1. On the computer where the Defender Administration Console is installed, start the Active Directory Users and Computers tool (dsa.msc).
2. In the left pane, expand the node representing the domain where you installed Defender.
3. Expand the **Defender** container, right-click the **Security Servers** container, and then select **New | Defender Security Server**.

For detailed instructions on how to create and configure a Defender Security Server object, see "Managing Security Server objects" in the *Defender Administration Guide*.

Access Node

An Access Node object defines an IP address or a range of IP addresses from which the Defender Security Server accepts authentication requests. If Access Node is misconfigured, authentication requests may not reach the Defender Security Server and the user cannot get access to the required resources.

To create an Access Node object

1. On the computer where the Defender Administration Console is installed, open the Active Directory Users and Computers tool (dsa.msc).
2. In the left pane, expand the node representing the domain where you installed Defender.
3. Expand the **Defender** container, right-click the **Access Nodes** container, and then from the shortcut menu select **New | Defender Access Node**.

After creating an Access Node object, use its properties to assign the Access Node to a Defender Security Server, specify Access Node members (users or groups that will be authenticating through the Access Node), and assign a Defender Security Policy object to the Access Node.

For detailed instructions on how to create and configure an Access Node object, see "Managing Access Node objects" in the *Defender Administration Guide*.

Program and assign security tokens to users

To assign a security token to a user

1. On the computer on which the Defender Administration Console is installed, open the Active Directory Users and Computers tool (dsa.msc).
2. In the left pane, expand the node representing the domain where you installed Defender, and then click to select the **Users** container.
3. In the right pane, double-click the user for whom you want to program and assign a security token.
4. In the dialog box that opens, on the **Defender** tab, do one of the following:
   - To assign a software token, click the **Program** button, and then complete the wizard. If necessary, install the token software on the user's computer and activate the token by entering the activation code.
   - To assign a hardware token, click the **Add** button, and then follow the on-screen instructions.

     Before assigning a hardware token to a user, you may need to import the corresponding hardware token object into Active Directory. For more information about importing and assigning hardware token objects, see "Managing security token objects" in the Defender Administration Guide.

Defender Setup Wizard reference

Table 1: Defender Setup Wizard reference

Wizard step	Options
Software Transaction Agreement	Select the **I accept these terms** check box to accept the terms in the Software Transaction Agreement.
Select Features	Select the features you want to install. Make sure you install the following required features: • **Active Directory Preparation** Installs Active Directory schema extensions, creates and configures control access rights, and creates organizational units required by Defender. • **Defender Security Server** Installs a server that performs two-factor authentication of users in your organization. Consider adding a second Defender Security Server to ensure that user authentication continues to work in case the primary Defender Security

Wizard step	Options
	Server becomes unavailable. After installing the Defender Security Server, you need to configure it. For details, see Configure Defender Security Server • **Defender Administration Console** Adds Defender menus and commands into Microsoft's Active Directory Users and Computers tool. You can also install the following optional features: • **Defender Management Portal** Installs a Web-based portal that allows administrators to manage and deploy tokens, view Defender logs in real time, troubleshoot authentication issues, and view a number of reports providing information about Defender configuration, users, authentication statistics, audit trail, and security tokens. The portal also includes a self-service Web site for users called the Defender Self-Service Portal. Where possible, to guard against external password-based attacks, we recommend you to place the Defender Self-Service Portal on the internal network with no access from the Internet. • **Defender Management Shell** Installs a command-line interface that enables the automation of Defender administrative tasks. With the Defender Management Shell, administrators can use Windows PowerShell® scripts to perform token-related tasks such as assign tokens to users, assign PINs, or check for expired tokens.
Upgrade Installed Features	If this step appears, it indicates that there are previous versions of Defender features installed on the computer on which you are using the Defender Setup Wizard. By default, only the features that are currently installed are selected for upgrade in this step. If necessary, you can select to install other features. For the descriptions of the Defender features you can select in this step, see the Select Features step description earlier in this table.
Connect to Active Directory	Use the following options to specify parameters for connecting to Active Directory: • **AD domain or domain controller name** Type the fully qualified domain name of the domain or domain controller in the domain where you want to install Defender. Defender Setup will use the specified domain to extend Active Directory schema with Defender classes and attributes and create

Wizard step	Options
	organizational units (OUs) required by Defender. • **Connect using** Specify the user account under which you want the Defender Setup to make changes in Active Directory.
Prepare Active Directory	Make sure that all check boxes provided in this step are selected.
Specify Port	This step only shows up if you have selected to install the Defender Management Portal (Web interface). Specify a communication port to be used by the Defender Management Portal. The default port is 8080.
Assign Administrator Role	This step only shows up if you have selected to install the Defender Management Portal (Web interface). In this step, you can assign the Defender Management Portal Administrator role to an Active Directory group. As a result, members of that group will have full administrative access to the Defender Management Portal. Note that members of the Domain Admins group always have the Administrator role assigned by default. To select the group to which you want to assign the Administrator role, click the **Change** button. If you specify an Active Directory group other than Domain Admins, ensure you delegate sufficient permissions to that group. You can delegate permissions by using the Defender Delegated Administration Wizard. For more information, see "Delegating Defender roles, tasks, or functions" in the *Defender Administration Guide*.
Completed the Setup Wizard	You can select the **Start Defender Security Server Configuration tool** check box to start the configuration tool after you complete the Defender Setup Wizard. For instructions on how to configure the Defender Security Server, see Configure Defender Security Server.

Defender Security Server Configuration tool reference

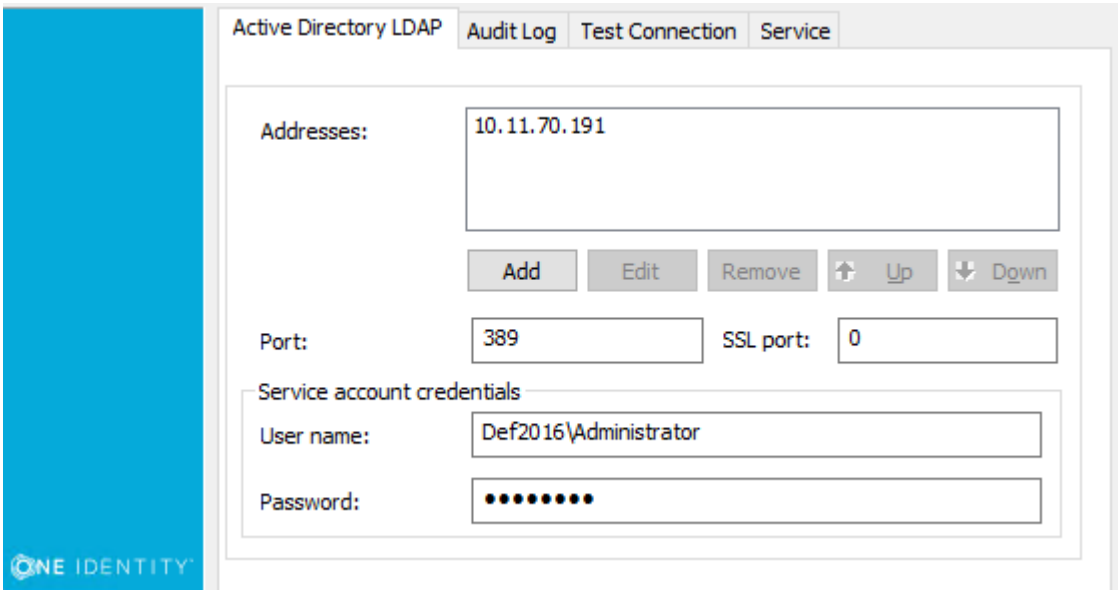
For the Defender Security Server to work properly, you need to connect it to Active Directory. To do that, you need to use the Defender Security Server Configuration tool.

To open the Defender Security Server Configuration tool, complete the steps related to your version of Windows in the following table:

Table 2: Steps to open Defender Security Server Configuration tool

Windows Server 2012 R2 and **Windows Server 2012**
On the **Apps** screen, click the **Defender Security Server Configuration** tile.
Windows Server 2016 and **Windows Server 2019**
Click the **Windows Start** button, and then scroll through the alphabetical list on the left. Click **One Identity** to expand the list of components of Defender products installed, on the system. Click **Defender Security Server Configuration**.

The Defender Security Server Configuration tool looks similar to the following:



The Defender Security Server Configuration tool has the following tabs:

Table 3: Defender Security Server Configuration tool tabs

Tab	Description
Active Directory LDAP	Use this tab to configure Active Directory connection settings. The Defender Security Server uses these settings to read data in Active Directory. • **Addresses** Set up a list of domains or specific domain controllers to which you want the Defender Security Server to connect to read data in Active Directory.

Tab	Description
	To add a domain or domain controller to the list, click the **Add** button, and then enter the DNS name or IP address. To edit a list entry, select that entry, and click the **Edit** button. To remove a list entry, select that entry, and click the **Remove** button. • **Port** Type the number of the LDAP port on which you want the Defender Security Server to connect to Active Directory. The default port is 389. • **SSL port** Type the number of the SSL port on which you want the Defender Security Server to connect to Active Directory. The default SSL port is 0. • **User name** Type the user name of the service account under which you want the Defender Security Server to connect to Active Directory. Use either <*domain*>\<*user name*> format or distinguished name (DN) as shown on the screenshot above. The Defender Security Server communicates with Active Directory during the authentication process to read and write Defender-related data. Therefore, the service account you specify must have sufficient permissions in Active Directory. An account such as the built-in Administrator account or members of the Domain Admins group have the required permissions by default. You may want to create a service account in Active Directory specifically for use with the Defender Security Server. To assign the sufficient permissions to that service account, you can use the Defender Delegated Administration Wizard. For more information, see "Delegating Defender roles, tasks, and functions" in the *Defender Administration Guide*. • **Password** Type the password that matches the user name specified in the User name text box.
Audit Log	Use this tab to configure Defender logging information. To specify a different log path for the Defender Security Server log file, click **Browse** and navigate to the required location. To change the size of the Defender Security Server log file, enter the required size in the **Log size** field. To create a duplicate copy of the current Defender Security Server log, select the **Create additional log with fixed name** check box, and then enter the name of the log file in the **Log name** field. If you want to save Defender Security Server logging information to a syslog server, as well as to the Defender Security Server log, select the **Enable syslog** check box and click **Add**.

Tab	Description
	In the **IP Address or DNS Name** field, enter the name or the IP address of the host computer where the syslog server is running. In the **Port** field, enter the port number used by the computer specified in the **IP Address or DNS Name** field.
Test Connection	Use this tab to test the Active Directory connection settings specified on the **Active Directory LDAP** tab. Click the **Test** button to check if the specified connection settings are correct. You can select the **Test connection automatically** check box to automatically test the specified connection settings.
Service	Use this tab to check the Defender Security Server service status and manage the service. To restart the Defender Security Server service, click **Restart Service**. To stop the Defender Security Server service, click **Stop Service**.

Communication ports

Defender uses the following communication ports:

Table 4: Default communication ports

Port	Protocol	Type of traffic
389	LDAP, TCP/IP	Defender Security Server, Active Directory connections
636	LDAP	Active Directory password changes (only if Defender is configured to handle Active Directory passwords).
1812/1813 or 1645/1646	UDP	RADIUS protocol
2626	TCP	Communications between Defender agents and the Defender Security Server.

Upgrading Defender

This section provides information on how to upgrade the Defender components. Defender is upgradeable from version 5.9.3 and later.

To upgrade a Defender component, install the new version of that component on the computer where an earlier version of the component is installed and follow the instructions mentioned on the screen to complete the upgrade process.

NOTE: If your current Defender version is lower than version 5.9.3, it is recommended to upgrade to version 5.9.3 or later.

Upgrading Defender Security Server and Administration Console

You cannot upgrade Defender Security Server and Administration Console separately. When upgrading the Security Server, select both the Security Server and Administration Console components. Your configuration settings will be automatically applied when the upgrade is complete.

To upgrade Defender Security Server and Administration Console

1. On the computer that has a previous version of Defender Security Server and Administration Console installed, run the **Defender.exe** file.

   In the Defender distribution package, you can find the Defender.exe file in the Setup folder.

2. Complete the Defender Setup Wizard.

   When stepping through the wizard, make sure to select the Defender Security Server and Defender Administration Console features for installation.

   For more information about the wizard steps and options, see Defender Setup Wizard reference.

Upgrading Defender Management Portal

When you upgrade the Defender Management Portal, your current portal configuration is automatically applied to the new installation of the portal.

To upgrade Defender Management Portal

1. On the computer that has a previous version of the Defender Management Portal installed, run the **Defender.exe** file.

   In the Defender distribution package, you can find the Defender.exe file in the Setup folder.

2. Complete the Defender Setup Wizard.

   When stepping through the wizard, make sure to select the Defender Management Portal feature for installation.

   For more information about the wizard steps and options, see Defender Setup Wizard reference.

Upgrading Management Shell

When you upgrade the Defender Management Shell, make sure you have installed Windows PowerShell 3.0 or later on the computer running the Defender Management Shell.

To upgrade Defender Management Shell

1. On the computer that has a previous version of the Defender Management Shell installed, run the **Defender.exe** file.

   In the Defender distribution package, you can find the **Defender.exe** file in the Setup folder.

2. Complete the Defender Setup Wizard.

   When stepping through the wizard, make sure to select the **Defender Management Shell** feature for installation.

   For more information about the wizard steps and options, see Defender Setup Wizard reference.

Licensing

To use native Defender software tokens, you need to have a license added in Defender. The native Defender software tokens are the Defender Soft Token, e-mail token, GrIDsure token, and SMS token. Other software or hardware tokens supplied with or supported by Defender do not require any license.

A Defender license can regulate the following:

- Maximum number of users who can have native Defender software tokens assigned.
- Maximum number of native Defender software tokens you can assign to users.

A Defender license can either be perpetual or have a limited validity period (fixed-term). If the validity period of a Defender license expires, the license is not removed from Defender automatically; rather, you have to remove the expired license manually.

Whenever any of the constraints set by the license are violated, Defender does not cease functioning but starts displaying a warning message stating that you are in violation of the software transaction agreement. To get rid of the warning message, you can install an additional license to increase the licensed number of users or tokens. Alternatively, you can unassign security tokens from users in your environment in order to comply with the license constraints.

You can have multiple licenses added in Defender. Adding a new license effectively increases the maximum licensed number of users, native software tokens, or both.

When you perform a clean installation of Defender, the Defender Setup automatically installs a built-in trial license. This trial license sets the following constraints:

- Maximum number of users who can have native Defender tokens assigned: 25
- Maximum number of native Defender tokens (except GrIDsure) you can assign to users: 200
- Maximum number of GrIDsure tokens you can assign to users: 0
- Trial license validity period: 90 days from installation

When you upgrade to Defender 5.11 from a previous version, the existing Defender licenses are transferred to the new installation of Defender. During Defender upgrade, the built-in trial license is not installed.

See also:

- User interface for managing licenses
- Adding a license
- Removing a license

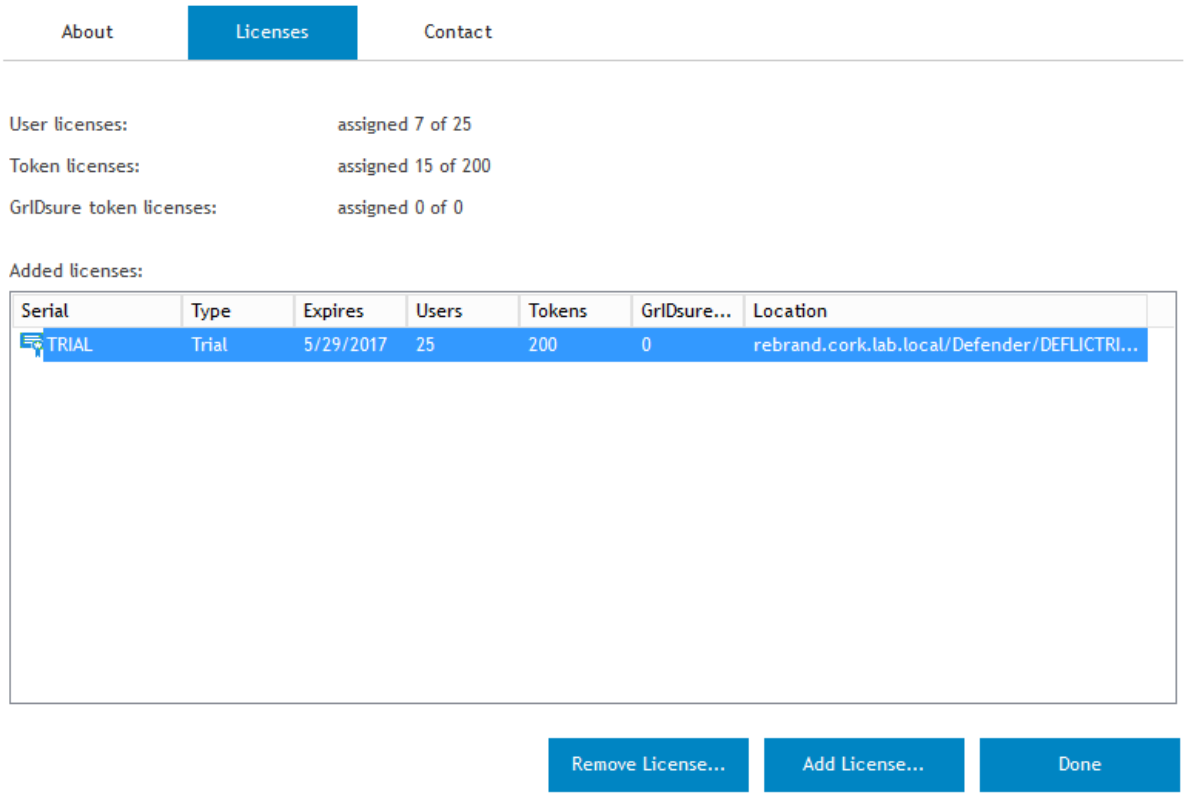
User interface for managing licenses

You can manage Defender licenses in the **About** dialog box on the **Licenses** tab. There you can add new licenses, view the details of added licenses, and remove licenses that have expired.

To open the Licenses tab

1. On the computer where the Defender Administration Console is installed, open the Active Directory Users and Computers tool (dsa.msc).
2. In the left pane (console tree), expand the appropriate domain node, and click to select the Defender container.
3. On the menu bar, select **Defender | License**.

The **Licenses** tab that opens looks similar to the following:



On the Licenses tab, you can use the following elements:

Table 5: Licenses tab elements

Element	Description
User licenses	Shows how many user licenses you have expended so far out of the maximum number available.
Token licenses	Shows how many token licenses you have expended so far out of the maximum number available.
GrIDsure token licenses	Shows how many GrIDsure token licenses you have expended so far out of the maximum number available.
Added licenses	Provides details of the Defender licenses you have added.
Remove License	Allows you to remove the license selected in the **Added licenses** list. For example, you can remove fixed-term licenses whose validity period has expired.
Add License	Allows you to add a new license to the **Added licenses** list. After clicking this button, you are prompted to specify the license key and site message of the license to add.
Done	Closes the **About** dialog box.

Adding a license

To add a license

1. On the computer where the Defender Administration Console is installed, open the Active Directory Users and Computers tool (dsa.msc).
2. In the left pane (console tree), expand the appropriate domain node, and click to select the **Defender** container.
3. On the menu bar, select **Defender | License**.
4. On the **License** tab, click the **Add License** button.
5. In the dialog box that opens, enter the license key and site message provided to you by One Identity.
6. Click **OK**.

Removing a license

You can remove licenses whose validity period has expired.

To remove a license

1. On the computer where the Defender Administration Console is installed, open the Active Directory Users and Computers tool (dsa.msc).
2. In the left pane (console tree), expand the appropriate domain node, and click to select the **Defender** container.
3. On the menu bar, select **Defender | License**.
4. In the **Added licenses** list, click to select the license you want to remove.
5. Below the **Added licenses** list, click the **Remove License** button.

   When prompted, confirm that you want to remove the license.

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 and other inquiries, such as licensing, support, and renewals, visit https://www.oneidentity.com/company/contact-us.aspx.

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