One Identity Defender 6.3.0

Administration Guide

Defender Administration Guide
Updated - 04 October 2022, 06:01
Version - 6.3.0

Contents

Getting started

Features and benefits

Defender is a cost-effective solution that enhances security in your organization by authenticating users who access valuable network resources. Only those users who successfully authenticate via Defender are granted access to the secured resource.

Defender uses your current identity store within Microsoft Active Directory to enable two-factor authentication, taking advantage of its inherent scalability and security, and eliminating the costs and time involved to set up and maintain proprietary databases. Defender's Web-based administration and user self-service ease the implementation of two-factor authentication for both administrators and users. Defender also provides a comprehensive audit trail that enables compliance and forensics.

Key features of Defender are as follows:

- **Centralized administration and tight integration with Active Directory** Defender is designed to base all administration and identity management on an organization's existing investment in Active Directory. This saves your time and resources, because to deploy and use Defender you can take advantage of the corporate directory already in place. Defender provides an administration and configuration interface called the Defender Administration Console. This console is implemented as an extension to Microsoft's Active Directory Users and Computers tool known to any Active Directory administrator.
- **Authentication by means of the RADIUS protocol** Defender allows authentication by means of the RADIUS protocol for environments that include

RADIUS users or RADIUS-protected access devices. Defender includes the facility for Vendor Specific Attributes (VSAs) to be specified in the RADIUS payload. For more information on VSAs, refer to the RADIUS RFCs posted on www.ietf.org. At the time of writing, the RFCs were available at datatracker.ietf.org/doc/search/?name=radius&rfcs=on&sort=.

- **Secure access to VPN** You can use Defender to authenticate users who connect to your organization's resources by using a virtual private network (VPN). Only those users who successfully authenticate via Defender are allowed to connect through VPN. For more information about this feature, see "Securing VPN access" in the *Defender Administration Guid*e.
- **Secure access to Web sites** With Defender, you can authenticate users who access Web sites hosted on Microsoft Internet Information Services (IIS) in your organization. For more information, see "Securing Web sites" in the *Defender Administration Guide*.
- **Secure Windows-based computers** You can use Defender to authenticate the users of computers running the Windows operating system. To sign in to a secured computer, the user needs to authenticate via Defender by supplying the correct passcode on the Windows sign-in screen. For more information, see "Securing Windows-based computers" in the *Defender Administration Guide*.
- **Secure access to PAM-enabled services in UNIX** You can use Defender to authenticate the users of popular UNIX services that support Pluggable Authentication Modules (PAMs), such as login, telnet, ftp, and ssh. For more information, see "Securing PAM-enabled services" in the *Defender Administration Guide*.
- **Data encryption** Defender supports AES, DES, and Triple DES encryption standards.
- **A wide range of supported security tokens** One of the authentication methods supported by Defender is security token. Defender provides native software and hardware security tokens and supports a variety of tokens produced by third-party vendors, such as Google Authenticator, Authy, GrIDsure, DIGIPASS, VIP credentials, and YubiKey. You can also deploy and use with Defender any hardware tokens that comply with the Initiative for Open Authentication (OATH) standard. For more information, see "Configuring security tokens" in the *Defender Administration Guide*.
- **Role-based management portal** This feature allows you to administer Defender from a Web browser. On the Defender Management Portal, you can manage software and hardware tokens and Defender users in your organization, view authentication reports and Defender logs, troubleshoot Defender authentication issues, and assign specific Defender roles to Active Directory groups of your choice. A portal role defines the Defender Management Portal functionality that is available to the user and the tasks the user can perform through the Defender Management Portal. For more information, see "Defender Management Portal (Web interface)" in the *Defender Administration Guide*.
- **User self-service** You can simplify the administration of your Defender environment by deploying and configuring a self-service Web site called the Defender Self-Service Portal. On this portal, users can request and receive new

software tokens, download and activate token software, and register existing hardware tokens without the need to contact a system administrator. The actions and tokens available to the users through the self-service portal are controlled by a number of settings you can configure to suit your needs. For more information, see "Defender Management Portal (Web interface)" in the *Defender Administration Guide*.

- **Delegation** Defender provides a scalable approach to the administration of access rights, enabling you to delegate specific Defender roles, tasks, or functions to the users or groups you want. The Defender administration interface provides a wizard you can use to search for and select one or multiple user accounts, and then choose which Defender roles or tasks you want to delegate to those accounts.

  Besides delegating roles or tasks, you can also delegate specific Defender functions. For example, you can appoint selected user accounts as service accounts for the Defender Security Servers or Defender Self-Service Portal or grant full control over particular Defender objects, such as Access Nodes, Defender Security Servers, licenses, RADIUS payloads, or security tokens. For more information, see "Delegating Defender roles, tasks, and functions" in the *Defender Administration Guide*.
- **Automation of administrative tasks** Defender Management Shell, built on Microsoft Windows PowerShell technology, provides a command-line interface that enables the automation of Defender administrative tasks. With the Defender Management Shell, you can perform token-related tasks, for example, assign tokens to users, assign PINs, or check for expired tokens. For more information, see "Automating administrative tasks" in the *Defender Administration Guide*.
- **Integration with Active Roles** Defender Integration Pack for Active Roles supplied in the Defender distribution package allows you to extend the functionality of the Active Roles Web Interface and Active Roles console. For example, with this Integration Pack installed, you can use the Active Roles user interface to perform Defender-related tasks: assign, remove, test, recover, and program security tokens and set Defender IDs and Defender passwords. Also you can enable the automatic deletion of tokens for deprovisioned users and use the Active Roles console to administer Defender objects and delegate Defender roles or tasks to the users you want. For more information, see "Integration with Active Roles" in the *Defender Administration Guide*.

What you can do with Defender

This section provides an overview of the most common Defender usage scenarios and the Defender components required for each scenario. For instructions on how to configure Defender for a particular scenario, see the *Defender Administration Guide*.

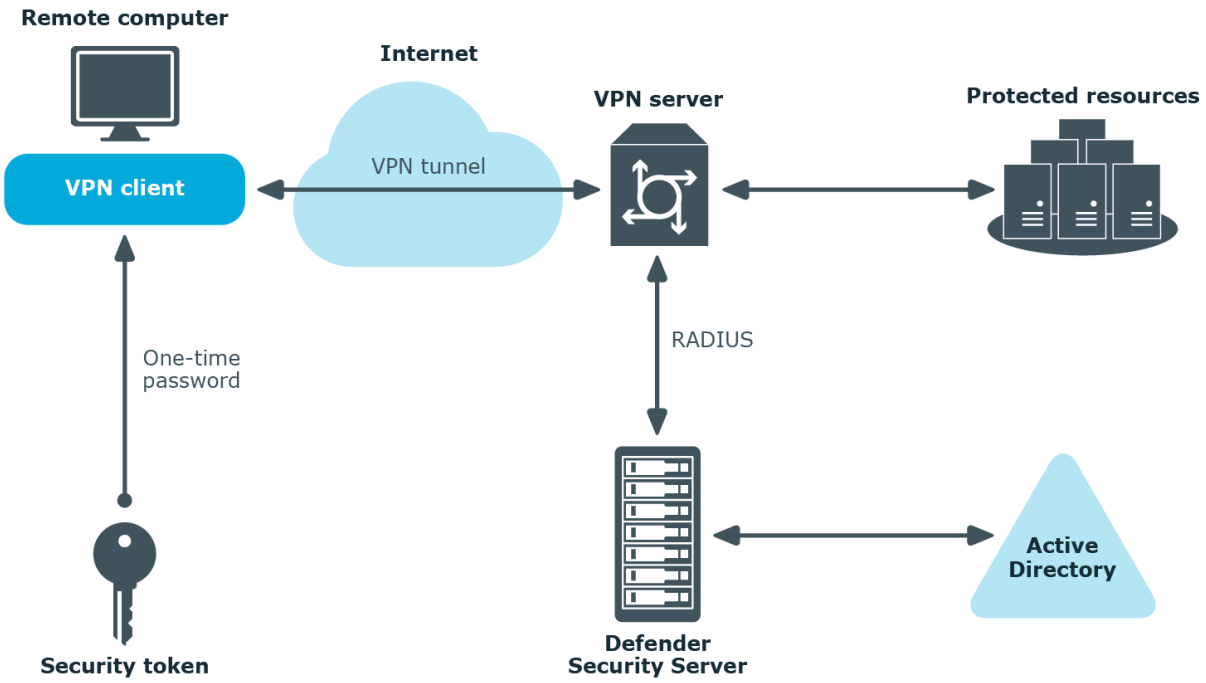
In this section:

- Authenticating VPN users
- Authenticating Web site users

- Authenticating users of Windows-based computers

Authenticating VPN users

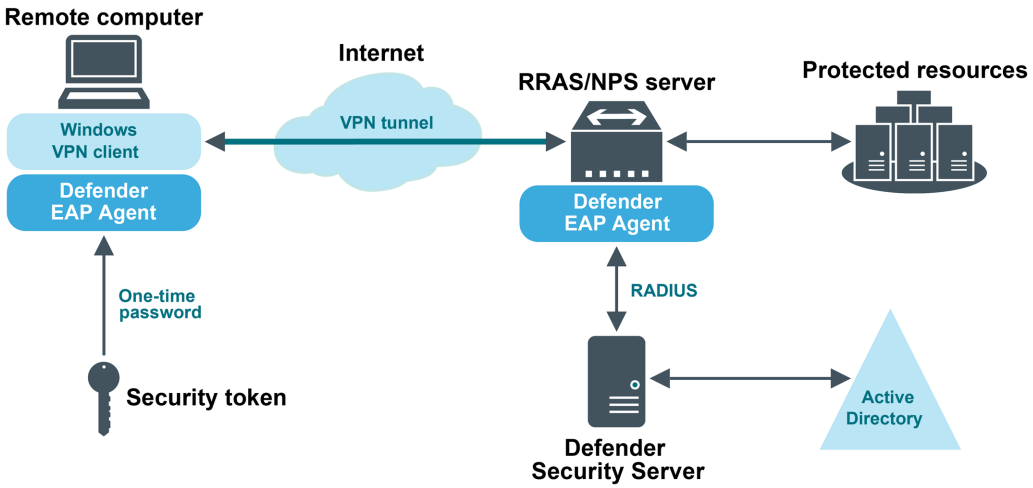
The following diagram illustrates a scenario where Defender authenticates the users who access an organization's network via a virtual private network (VPN):



In this scenario, the VPN server is configured to redirect the user to the Defender Security Server, which prompts the user to submit a passcode. The user needs to generate a passcode by using a security token provided by Defender administrator. The Defender Security Server validates the passcode entered by the user, and if the passcode is correct allows the user to establish a VPN connection.

The next diagram illustrates a scenario where Defender is configured to authenticate the users who establish a VPN connection via the Routing and Remote Access service (RRAS).

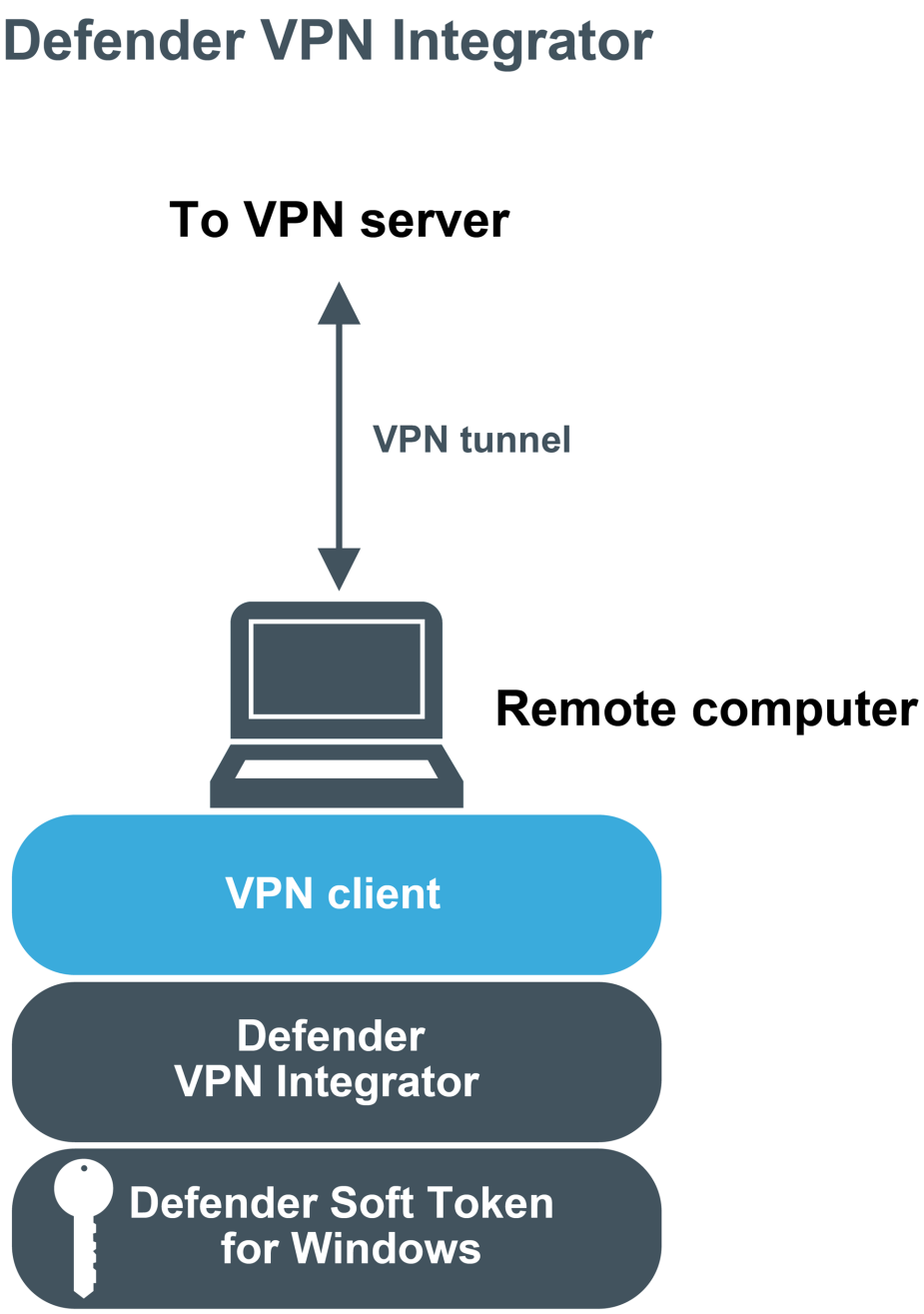
Defender and VPN access via RRAS/NPS server



In this scenario, a component called the Defender EAP Agent must be installed both on the VPN client computer and VPN server. Extensible Authentication Protocol (EAP) is a general protocol for authentication that also supports multiple authentication methods, such as Kerberos, token cards, one-time passwords, certificates, public key authentication, and smart cards.

Defender uses the EAP protocol to integrate its two-factor authentication into the existing user authentication process. The Defender EAP Agent supports Microsoft Remote Access clients and servers for both dial-up and VPN (PPTP and L2TP/IPSec).

If VPN users in your environment authenticate using the Defender Soft Token for Windows, you can simplify the authentication experience for these users by deploying the Defender VPN Integrator component on their workstations.

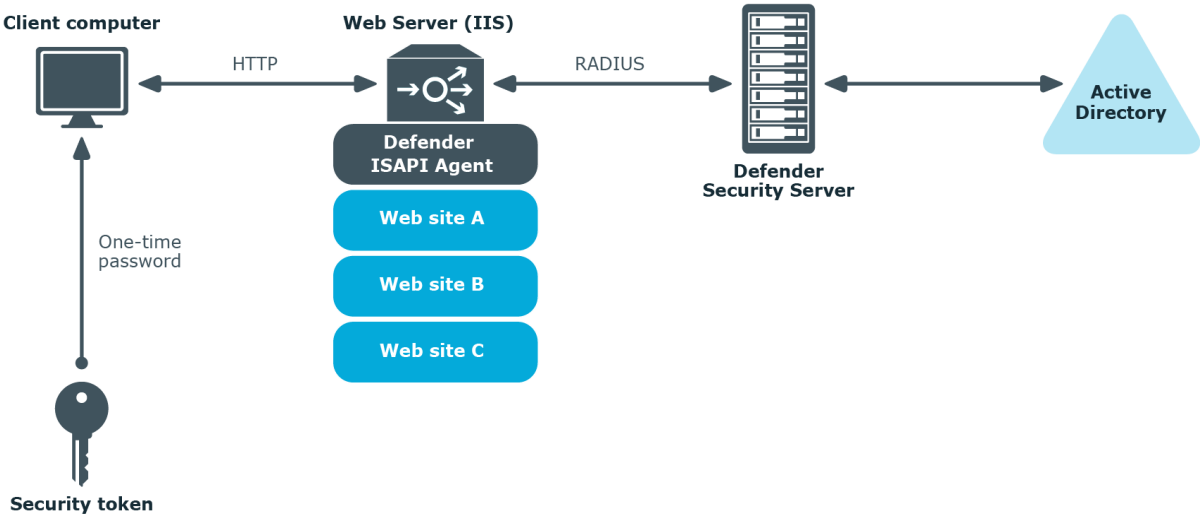


To do so, you need to install the Defender VPN Integrator on the computer where the Soft Token for Windows is installed. When the user initiates a VPN connection, VPN Integrator

communicates between the Soft Token for Windows and the third-party VPN client to ensure that the secure, one-time password authentication process is handled automatically. The entire operation is seamless and very fast—only the passphrase for the Defender Soft Token for Windows is required from the user.

Authenticating Web site users

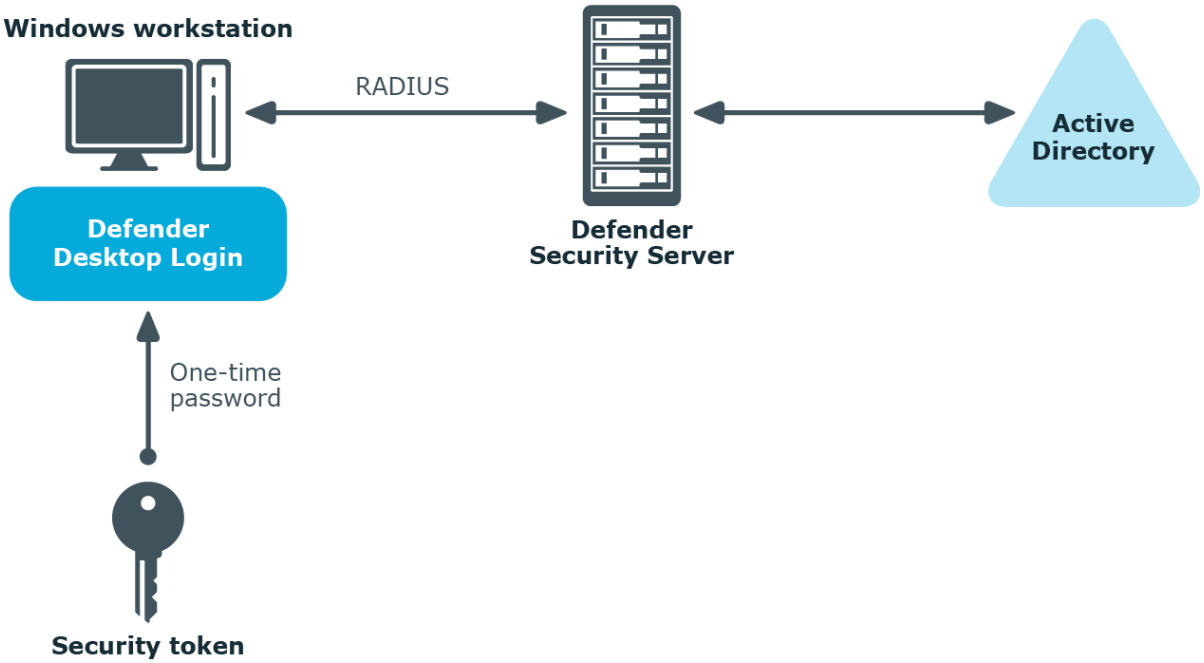
The next diagram illustrates a scenario where Defender is configured to authenticate the users who access Web sites hosted on Microsoft Internet Information Services (IIS).



In this scenario, the Defender ISAPI Agent must be deployed on the Web Server that hosts the Web sites to be secured with Defender. The ISAPI Agent acts as an ISAPI filter and requires users to authenticate via Defender in order to get access to the Web sites hosted on the Web Server.

Authenticating users of Windows-based computers

Defender can also be configured to authenticate users when they sign in to their workstations running the Windows operating system.



To implement this scenario, you need to install and configure a component called the Defender Desktop Login on each Windows workstation whose users you want to authenticate via Defender.

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 *Defender 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, see Appendix D: Defender classes and attributes in Active Directory on page 216.

  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:

- Step 1: Install required Defender components
- Step 2: Configure Defender Security Server
- Step 3: Create and configure objects in Active Directory
- Step 4: 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.

Step 1: 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.
3. For more information about the wizard steps and options, see Defender Setup Wizard reference.

Step 2: Configure Defender Security Server

Use the Defender Security Server Configuration tool to configure the Defender Security Server you have installed in Step 1: 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.

Step 3: 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 Nodes" in the *Defender Administration Guide*.

Step 4: 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 Server becomes unavailable. After installing the Defender Security Server, you need to configure it. For details, see Step 2: 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

Wizard step	Options
	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 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.

Wizard step	Options
	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 Step 2: 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.

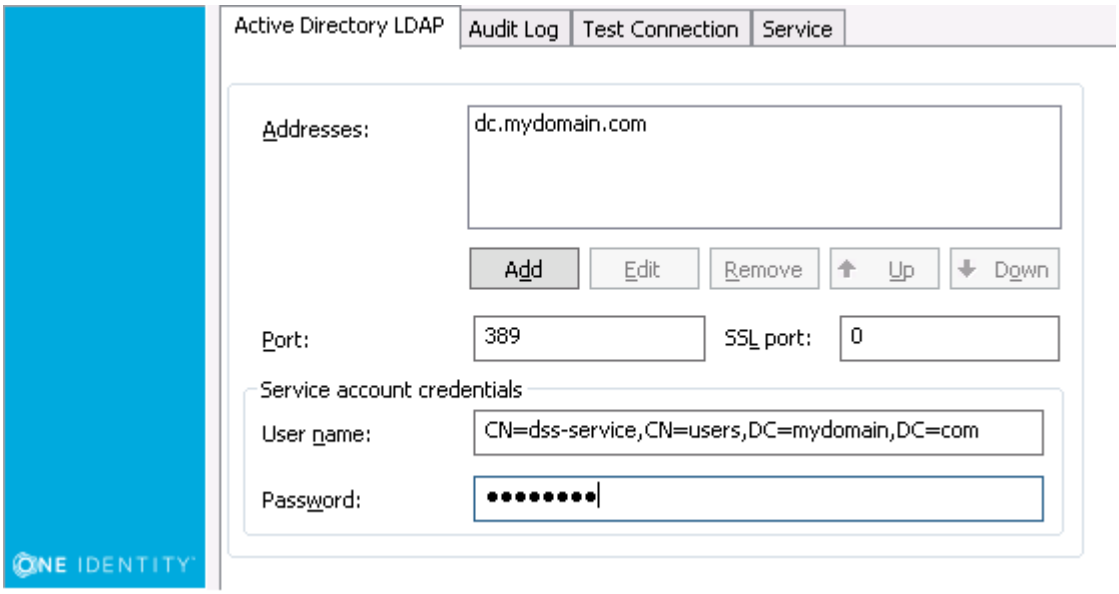
To open the Defender Security Server Configuration tool, complete the steps related to your version of Windows in the following table:

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**
1. Click the **Windows Start** button, and then scroll through the alphabetical list on the left. 2. Click **One Identity** to expand the list of components of Defender products installed on the system. 3. 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. 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

Tab	Description
	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**. 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

Tab	Description
	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.
5228/5229/5230	TCP/UDP	If the organization has a firewall to restrict traffic to or from the Internet on the mobile devices, you need to configure the port on the firewall to receive push notifications
443	SSL	For DSS to send the authentication request to the third party cloud messaging service to send the push notifications, the SSL port 443 needs to be enabled on the server.

Upgrading Defender

This section provides information on how to upgrade the Defender components. Defender is upgradeable from version 5.10.0 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 5.10.0, it is recommended to upgrade to version 5.10.0 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.

After you have installed the Defender Management Shell 6.3.0, you can uninstall a previous version of the Management Shell.

To uninstall a previous version of Defender Management Shell

1. Open the list of installed programs (appwiz.cpl).
2. In the list, select the **PowerShell Management for Defender** entry and click **Uninstall**.

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 One Identity 6.3.0 from a previous version, the existing Defender licenses are transferred to the new installation of One Identity. During Defender upgrade, the built-in trial license is not installed.

See also:

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

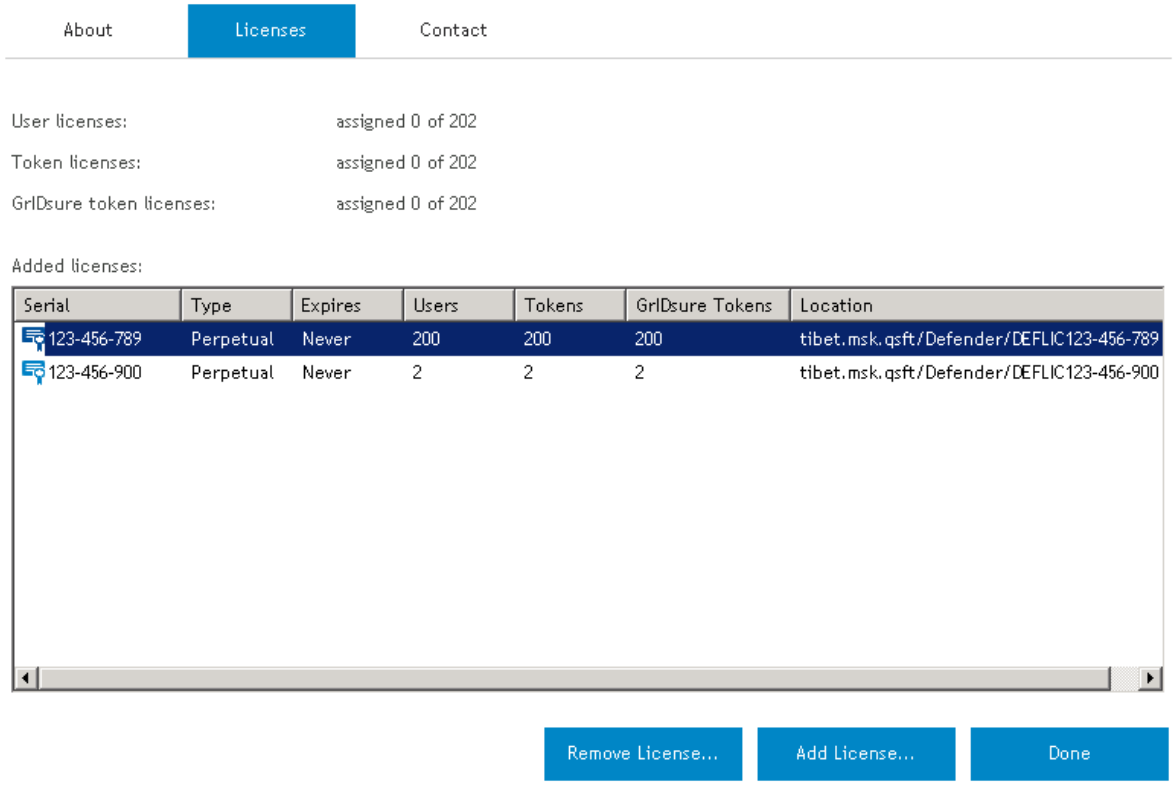
User interface for managing licenses

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.

Element	Description
	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.

2

Managing Defender objects in Active Directory

Managing user objects

You can use the properties of a user object in Active Directory to perform Defender-related tasks. For example, you can manage and view information about tokens assigned to the user and Security Policies and RADIUS payloads that apply to the user.

Managing tokens for a user

To manage tokens for a user

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 to select the container that holds the user for whom you want manage tokens (typically, this is the **Users** container).
3. In the right pane, double-click the user.
4. In the dialog box that opens, click the **Defender** tab.
5. Use the following areas to make changes or view information as necessary:
    - **Tokens** This list allows you to manage tokens for the user. This list shows the tokens that are currently assigned to the user. For each token in the list, you can view the token type, serial number, and whether PIN is enabled. For more information, see Tokens list buttons.
    - **Authentication Details** Allows you to specify a Defender ID for the user. Also you can view violation count, reset count, and last logon date and time for the user. Optionally, you can reset the violation count. For more information, see Authentication Details area elements on page 40.
6. When you are finished, click **OK** to close the dialog box.

Tokens list buttons

Table 6:
Tokens list buttons

Button	Description
Program	Click to program a token for the user.
Recover	Click to recover the token selected in the list or reset the token's passphrase. You may need to reset a token when it has reached its preset use limit or been invalidated because the user exceeded the preset number of bad PIN attempts.
Test	Allows you to verify that the token is programmed correctly and valid for the user. After you click this button, use the **Response** text box to type the one-time password displayed on the token. If a PIN is enabled for the token, you can also test the PIN by entering it in the **PIN (Optional)** text box. Click **Verify** to run the test on the token. If you use the **Test** button to test a token response, that token response cannot then be used for user authentication.
Helpdesk	Allows you to resynchronize the token selected in the list with the Defender Security Server or assign a temporary password to the token user. After you click the **Helpdesk** button, a dialog box opens. This dialog box

Button	Description
	provides the following options: • **Reset** Click this button to resynchronize the token with the Defender Security Server. The token generates a one-time password that is based on an internal time clock and DES keys. For successful authentication, the Defender Security Server must agree with the token's time clock and DES keys. The token's time clock can become out-of-sync with the Defender Security Server. If this value is out-of-sync, the user cannot use the token for authentication. If access is denied to the user, the token clock must be synchronized with the Defender Security Server clock. After resetting the token, instruct the user to use the token to generate a one-time password and use it for Defender authentication. • **Expires** Allows you to select a validity period for the temporary password. • **Allow response to be used multiple times** Select this check box to allow the temporary password to be used more than once for authentication. If you leave this check box cleared, the temporary password can only be used once. • **Assign** Assigns the generated temporary password to the user. • **Clear** Removes the temporary password from the user. • **Response** Shows the generated temporary password.
Unassign	Removes the token selected in the list from the user. You can also use this option to delete the corresponding token object from Active Directory. To remove the token from the user and keep the token object in Active Directory, in the confirmation message that appears after you click this button, click **No**. In this case, the token object does not get deleted from Active Directory and can be reassigned. To remove the token from the user and delete the token object from Active Directory, in the confirmation message, click **Yes**.
Add	Allows you to search for and assign a token to the user. After you click this button, a new dialog box opens. In that dialog box, you can use the following elements: • **Token Serial Number** Type the serial number of the token you want to assign to the user. If you do not know the serial number, leave this text box blank. • **Show unassigned tokens only** Select this check box to search for the tokens that are not assigned to users. If you leave this check

Button	Description
	box cleared, the search results will include both assigned and not assigned tokens. • **Token Type** Select the token type you want to search for. Click **OK** to start your search. When the search completes, in the **Select Defender Tokens** dialog box, double-click the token you want to assign, and then click **OK** to assign the token to the user. The assigned token appears on the **Defender** tab in the **Tokens** list.
Set PIN	Allows you to set a new PIN for the token selected in the list. After you click the **Set PIN** button, a dialog box opens. This dialog box provides the following options: • **Enable PINs** Enables PIN for the selected token. • **New PIN** Type the new PIN you want to assign to the selected token. • **Confirm PIN** Confirm the new PIN you want to assign. • **Expire** Select this check box if you want the PIN to expire. When you require users to enter a PIN set for a selected token, users should enter the PIN followed by the token response to access a resource protected by Defender. For example, if the PIN is 1234 and the response is 5678, users should enter 12345678 when prompted for authentication. When users need to reset the PIN, they should enter the old and new PINs in the following format: <old PIN><new PIN><new PIN>. For example, if the old PIN is 1234 and the new PIN is 5678, users should enter the following: 123456785678.
Password	Allows you to specify the Defender password that the user must enter during the authentication process. The password is only required if Defender password is selected as the primary or secondary authentication method in the Defender Security Policy that applies to the user. After you click the **Password** button, a new dialog box opens. In the dialog box, use the **Password** and **Confirm** text boxes to type the new Defender password you want to assign. If you want the password to expire, select the **Expire** check box.

Authentication Details area elements

Table 7:
Authentication Details area elements

Element	Description
Defender ID	Use this text box to type the Defender ID you want the Defender Security Server to use to identify the user. You only need to specify a Defender ID for a user if the Access Node of which the user is a member has been configured to identify users by Defender ID.
Violation Count	Displays the number of violations accumulated by this user. The violation count is incremented each time the user exceeds the specified number of failed logon attempts.
Reset Count	Displays the number of times the user account has been reset following an account lockout.
Last Logon	Displays the time and date of the last successful logon.
Reset	Resets the violation count to zero and increments the reset count.

Resetting passphrase for a user

You can reset the passphrase for a user. For example, you can do so if the user has forgotten the passphrase and the passprhase has been locked. In order you could reset the passphrase, the user must provide to you the challenge code generated by the token.

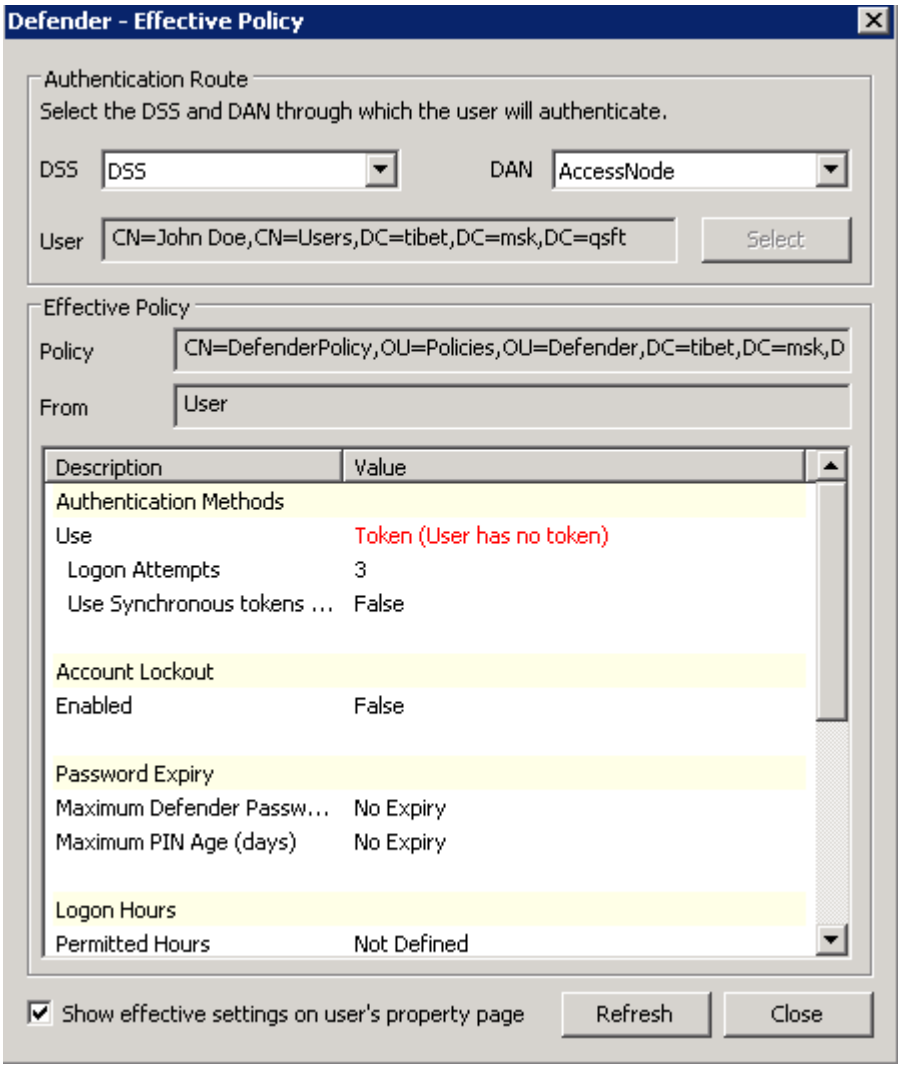
To reset the passphrase for a user

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 to select the container that contains the user.
3. In the right pane, double-click the user object.
4. In the dialog box that opens, click the **Defender** tab.
5. In the **Tokens** area, select the token, and then click the **Recover** button.
6. In the dialog box that opens, use the **Challenge** text box to type the challenge code provided to you by the user, and then click the **Get Response** button.
7. Copy the passphrase unlock code displayed in the **Response** box and provide the code to the user.

Managing Defender Security Policy for a user

To manage Defender Security Policy for a user

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 to select the container that contains the user for whom you want to manage Defender Security Policy (typically, this is the **Users** container).
3. In the right pane, double-click the user object.
4. In the dialog box that opens, click the **Policy** tab. This tab allows you to view the current or assign a new Defender Security Policy to the user. The tab has the following elements:
    - **Assigned Policy** Shows the Defender Security Policy that is currently assigned to the user. When there is no Defender Security Policy assigned to the user, this option displays <undefined>.
    - **Select** Allows you to select an existing Defender Security Policy to assign to the user.
    - **Clear** Unassigns the current Defender Security Policy from the user.
    - **Effective** Click this button to view the Defender Security Policy settings that will apply to the user for a particular Defender Security Server/Access Node combination. The window that opens looks similar to the following:



The **DSS** list shows the Defender Security Server that is currently selected for the user. If necessary, select any other Defender Security Server.

The **DAN** list shows the Access Node of which the user is a member. If necessary, select any other Access Node.

The **User** option displays the current user.

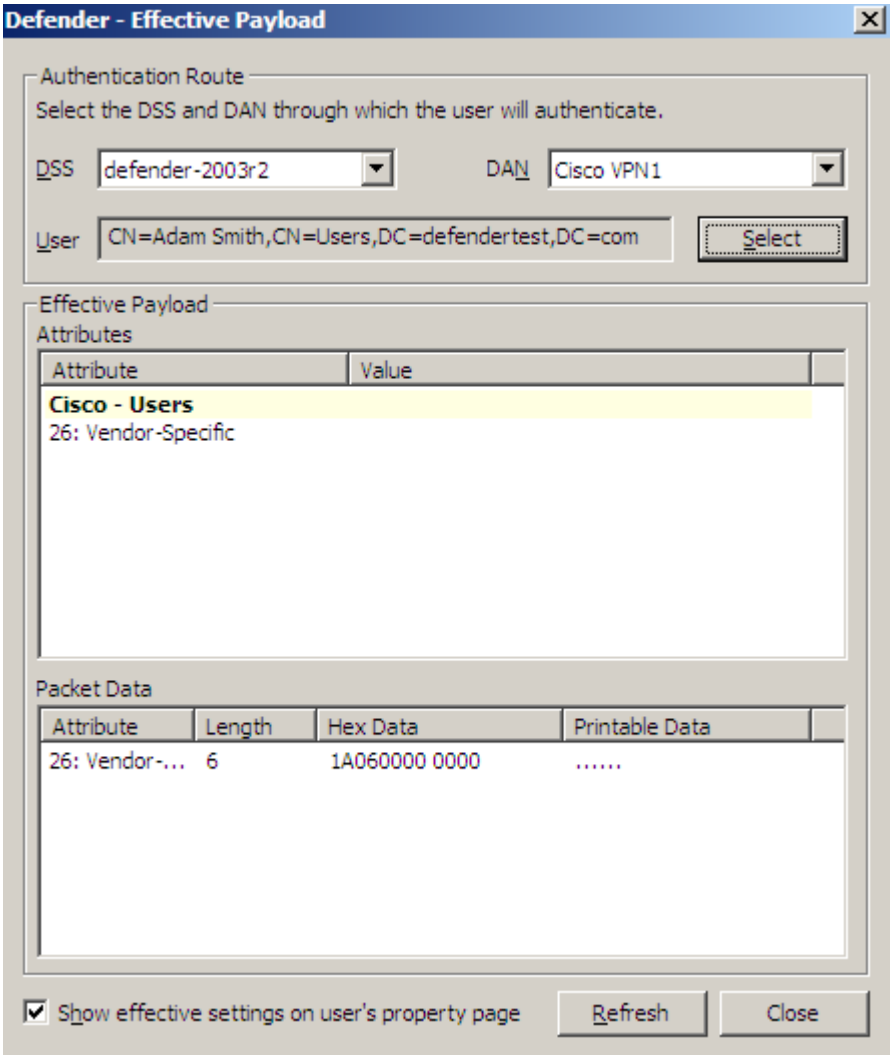
The **Effective Policy** area displays the Defender Security Policy details and authentication settings that will be effective when the user authenticates via Defender.

Managing RADIUS payload for a user

To manage RADIUS payload for a user

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 to select the container that contains the user for whom you want to manage RADIUS payload (typically, this is the **Users** container).
3. In the right pane, double-click the user.
4. In the dialog box that opens, click the **RADIUS Payload** tab. This tab allows you to view the current or assign a new RADIUS payload to the user. The tab has the following elements:
    - **Assigned Payload** Shows the RADIUS payload that is currently assigned to the user. When there is no RADIUS payload assigned to the user, this option displays <undefined>.
    - **Select** Allows you to select a RADIUS payload to assign to the user.
    - **Clear** Unassigns the current RADIUS payload from the user.
    - **Inherit payload entries from parent. Include these with entries explicitly defined here.** When selected, causes the user to inherit the RADIUS payload from the Access Node of which the user is a member.
    - **Effective** Click this button to view the RADIUS payload that will apply to the user for a particular Defender Security Server/Access Node combination. The windows that opens looks similar to the following:
    - **Effective** Click this button to view the RADIUS payload that will apply to the user for a particular Defender Security Server/Access Node combination. The

windows that opens looks similar to the following:



The **DSS** list shows the Defender Security Server that is currently selected for the user. If necessary, select any other Defender Security Server.

The **DAN** list shows the Access Node that is currently selected for the user. If necessary, select any other Access Node.

The **User** option displays the current user.

The **Effective Payload** area displays the details of the RADIUS payload that will be effective when the selected user authenticates via Defender.

Managing security token objects

Importing hardware token objects

In order to assign hardware tokens to users in your environment, you first need to import the corresponding hardware token objects into Active Directory.

To import hardware token objects, you need to have the file that contains the definitions of the token objects you want to import. Normally, this file is provided together with hardware tokens.

Note that the instructions in this section do not apply to hardware VIP credentials.

To import hardware token objects into Active Directory

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 | Import Tokens**.
4. Complete the wizard to import the token objects.

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

Assigning a hardware token object to a user

Before providing a hardware token to a user, you need to assign the corresponding hardware token object to the user in Active Directory. In order you could assign a hardware token object, you need to import it first into Active Directory. For instructions, see Importing hardware token objects.

To assign a hardware token object 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 (console tree), expand the appropriate domain node to select the container that holds the user to which you want to assign the hardware token object.

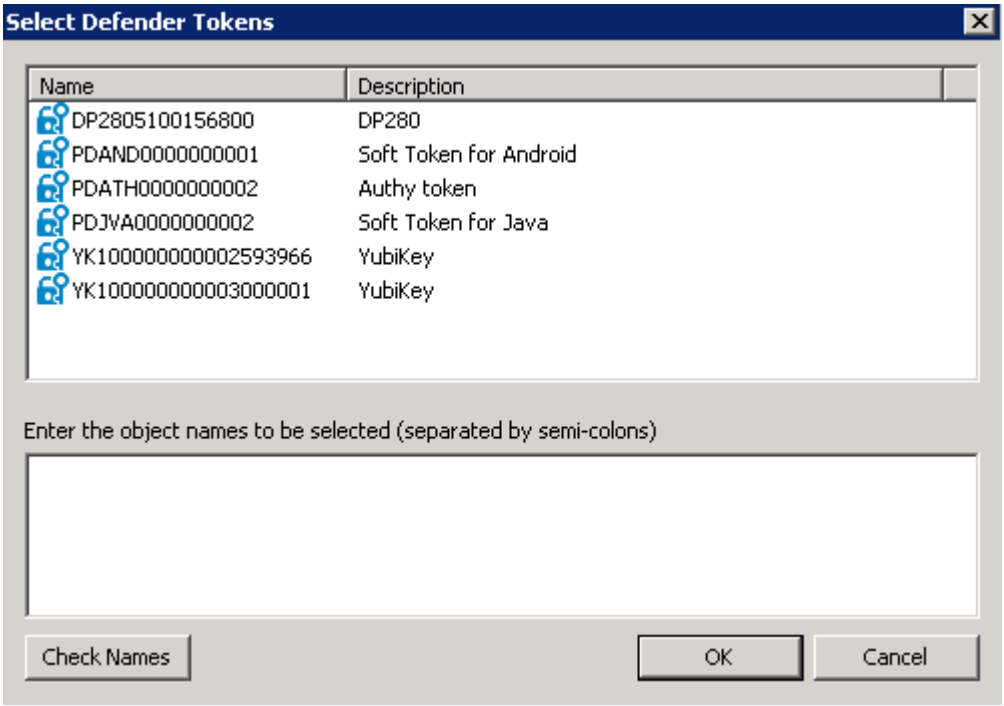
3. In the right pane, double-click the user object.
4. In the dialog box that opens, on the **Defender** tab, under the **Tokens** list, click the **Add** button.
5. Use the dialog box that opens to specify search criteria to search for the token object you want to assign.

The dialog box has the following elements:

- **Token Serial Number** Type the token serial number to search for the corresponding token object. If you do not know the token serial number, leave this text box blank.
- **Show unassigned tokens only** Select this check box if you want to search for token objects not assigned to any user. When this check box is cleared, the search results will include both assigned and unassigned token objects.
- **Token Type** Use this list to select the token type you want to search for.

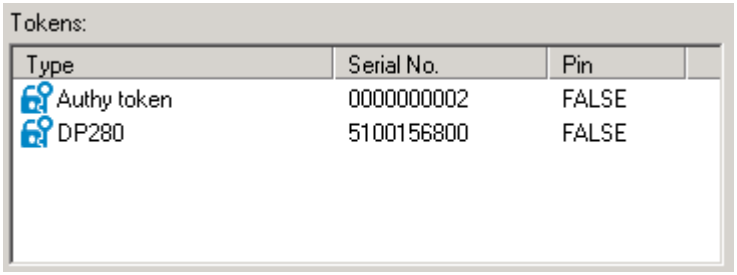
6. After specifying search criteria, click **OK** to start your search.

   When your search completes, a list of search results opens:



7. In the upper pane of this dialog box, double-click the token object you want to assign to the user, and then click **OK** to assign the object.

   The assigned token object appears in the **Tokens** list on the **Defender** tab in the user properties dialog box:



Modifying token object properties

To modify token object properties

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 (console tree), expand the appropriate nodes to select the container that stores the token object whose properties you want to modify.

   By default, token objects are stored in the ***<Domain>*** **| Defender | Tokens** container.
3. In the right pane, double-click the token object whose properties you want to modify.
4. Use the dialog box that opens to modify the token object properties as necessary. You can use the following tabs:
   - **General tab** Provides the token type and token activation code expiry date. You can also use this tab to program, reset, test, and recover the token.
   - **Details tab** Displays information about the token.
   - **Assigned Users** Provides a list of users to whom the token is assigned. You can use this tab to assign or remove the token from users.
5. When you are finished, click **OK** to apply your changes.

General tab

This tab provides information about the token type and token manufacturing date or token activation code expiry date. You can also use this tab to program, reset, test, and recover the token.

On this tab, you can use the following elements:

- **Token Type** Displays the token type.
- **Token Date** For objects representing hardware tokens, this option displays the manufacture date of the token. By using this date, you can calculate the approximate expiry date of the token's battery. For objects representing software tokens, this option displays the activation code expiry date or indicates that the token has already been activated.

- **Program** Click this button to program the token.
- **Reset** Click this button to synchronize the token with the Defender Security Server.

  The token generates a one-time password that is based on an internal time clock and DES keys. For successful authentication, the Defender Security Server must agree with the token's time clock and DES keys. The token's time clock can become out-of-sync with the Defender Security Server. If this value is out-of-sync, the user cannot use the token for authentication. If access is denied, the token clock must be synchronized with the Defender Security Server clock.

  After resetting the token, instruct the user to generate a one-time password on the token and use it for Defender authentication.
- **Test** Click this button to run a test that verifies the token is programmed correctly and valid for the user. After you click this button, use the **Response** text box to type the one-time password displayed on the token, and then click **Verify**.
- **Recover** Click this button to remotely recover the token after it has reached its preset use limit or been invalidated because the user exceeded the preset number of bad PIN attempts. The **Recover** button also allows you to reset a passphrase for the token. These values are defined in the token profile assigned to the user.

  After you click this button, use the **Unlock Challenge** text box to type the challenge value displayed on the token, and then click the **Get Response** button. Enter the displayed response into the token to complete the recover procedure.

Details tab

This tab displays information about the token. The information provided depends on the token type.

For a hardware token, this tab can display the following settings and their values:

- **Token Type** Displays the type of token.
- **Usage Count** Displays the number of times this token has been used for successful authentication.
- **Last Token Time Used** Displays the most recent successful authentication.
- **Last Token Time Shift** Displays the time difference between the token clock and the Defender Security Server clock.
- **Current Error Count** Not applicable.
- **Binary Codeword** Not applicable.
- **Triple DES flag** Indicates whether Triple DES is enabled or disabled for this token
- C**hallenge/Data fields nbr** Not applicable.
- **Response Length** Displays the number of digits included in a token response.
- **Output Type** Displays the type of output (decimal or hexadecimal).
- **Checksum Requested Flag** Not applicable.

- **Time step used if any** Displays the time interval at which new responses are generated by the token.
- For a software token, this tab can display the following:
- **Token Type** Displays the type of token.
- **Encryption Type** Displays the type of encryption used by the token (such as AES, DES or Triple DES)
- **Response Length** Displays the number of digits included in a token response.
- **Response Type** Displays the type of response used by the token (response only or challenge-response).
- **Response Format** Displays the format of response (decimal or hexadecimal).
- **Platform** Displays the platform on which the token can be used.
- **Activation Key** Displays the key required to activate the token. The key is no longer displayed after token activation.
- **Status** Indicates whether this token has been activated.

Assigned Users

This tab provides a list of users to whom the token is assigned. You can use this tab to assign or remove the token from users.

- **Assign** Allows you to assign the token to one or more users.
- **Unassign** Removes the token from the users or groups selected in the **Assigned Users** list.

Import Wizard reference

The table below provides information about the Import Wizard steps and options.

Table 8:
Import Wizard reference

Wizard step	Your action
File and Key	Browse for and select the file that contains the definitions of the token objects you want to import, and then specify the key for the file. You can use the following options: • **Filename** Click **Browse** to locate and select the file that contains the definitions of the token objects you

Wizard step	Your action
	want to import. • **Key** Type or paste the key for the file selected in the **Filename** option.
Available Tokens	In the list, select the token objects you want to import into Active Directory. You can use the following buttons: • **Select All** Selects all token objects in the list. • **Clear All** Clears currently selected tokens. You can hold down CTRL and click in the list to select token objects. If the token objects in the list support both synchronous and asynchronous modes, the following check boxes are available: • **Response Only** When selected, causes the token objects to operate in the synchronous (response only) mode. • **Challenge Response** When selected, causes the token objects to operate in the asynchronous (challenge-response) mode. If the token objects in the list support both OTP1 and OTP2 applications, the following check boxes are available: • **OTP1** When selected, causes the token to generate a first one-time password (OTP1). • **OTP2** When selected, causes the token to generate a second one-time password (OTP2). If you select only one of these check boxes, make sure to instruct the token users which button they should press on their hardware tokens for generating one-time passwords. For example, when you import DIGIPASS 280 token objects and select the **OTP1** check box while leaving the **OTP2** check box cleared, then the token users should generate one-time passwords by pressing the **OTP1** button on their DIGIPASS 280 tokens. In this scenario, pressing the **OTP2** button will generate invalid one-time passwords.
Storage Location	Specify the Active Directory container in which you want to store the token objects being imported. Click the **Select** button to browse for and select the container. The default container is **Defender | Tokens**.

Wizard step	Your action
	If you change the default container, ensure that the Defender Security Server service account and the Defender administrator account have sufficient permissions on the new container you specify.
Import Progress	View the progress of the hardware token import.

Managing Defender Security Policies

You can use the Defender Administration Console to create and configure Defender Security Policies. A Defender Security Policy can be assigned to a user, group of users, Access Node, or Defender Security Server.

If a different Defender Security Policy is applied to each of the above elements, the policy assigned to the user takes the highest priority, followed by the policy assigned to the group, then the policy assigned to the Access Node and finally, the policy assigned to the Defender Security Server. Security Policies cannot be aggregated.

Logon attempts made by the user are rejected if the user belongs to two groups with conflicting security policies and both groups are assigned to the Access Node through which the user connects to the Defender Security Server.

If no Defender Security Policy has been assigned, the default Defender Security Policy is applied. For more information, see Default Defender Security Policy on page 62.

When you have defined the Defender Security Policy, you can use its property pages to:

- Change the Defender Security Policy configuration.
- Change user account lockout information.
- Configure password and PIN expiration policies.
- Specify permitted logon hours.
- Configure settings for SMS tokens.
- Configure settings for e-mail tokens.
- Configure settings for GrIDsure tokens.

Creating a Defender Security Policy object

To create a Defender Security Policy

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 then expand the **Defender** container.
3. Right-click the **Policies** container, point to **New**, and then click **Defender Policy**.
4. Complete the wizard that starts to create a new Defender Security Policy.

   For more information about the wizard steps and options, see New Object - Defender Policy Wizard reference.

New Object - Defender Policy Wizard reference

Table 9:
New Object - Defender Policy Wizard reference

Wizard step	Options
Enter a name and description for this Policy	Provides the following text boxes: • **Name** Type a name for the Defender Security Policy being created. • **Description** Type a description for the Defender Security Policy being created.
Select an authentication method	Provides the following elements: • **Method** Select a primary authentication method for the Defender Security Policy. An authentication method determines the passcode that the user must enter when attempting to authenticate. You can select one of the following authentication methods: • **Token** The user must use a token response to authenticate. • **Defender password** The user must enter a valid Defender password to authenticate. • **Active Directory password** The user must enter a valid Active Directory password to authenticate. • **Token with Defender password** The user must enter a token response followed by a valid Defender password to authenticate. • **Defender password with token** The user must enter a valid Defender password followed by a token response to authenticate. • **Token with Active Directory password** The user must enter a token response followed by a valid Active Directory password to authenticate.

Wizard step	Options
	• **Active Directory password with token** The user must enter a valid Active Directory password followed by a token response to authenticate. • **Active Directory password (rollout mode)** The user can authenticate with the Active Directory password until a security token is assigned or registered to the user's Active Directory account. After a security token has been assigned or registered for the user, the user must submit the token response to authenticate. For more information, see Defender Rollout Mode • **GrIDsure token (auto-enrollment mode)** The user must authenticate by using a GrIDsure Personal Identification Pattern (PIP). During the first authentication, the user is prompted to configure a GrIDsure PIP to be used for subsequent authentications. • **Logon Attempts** Enter the number of times that the user can attempt to log on. If the number of unsuccessful logon attempts exceeds the specified limit, the violation count for the user's account is incremented. • **Use Synchronous tokens as event tokens** Enables the use of the same DIGIPASS GO token response for logon to more that one system without generating a new response, provided that the logon process takes less than 36 seconds which is the validity period for a DIGIPASS GO token response.
Select the second authentication method	Specify parameters for the additional authentication method you want the user to use. If you want to disable the additional authentication method, from the **Method** list, select **None**. Other options in the **Method** list are identical to those available in the Select an authentication method step of the wizard.
Enter account lockout policy details	Provides the following options: • **Enable Account Lockout** When this check box is selected, it causes the user's Defender account to be locked out if the user has exceeded the number of violations (failed logon attempts) specified n the **Lockout after n violations** option. • If you select the **Lockout Windows account after indicated violations** check box, this causes the

Wizard step	Options
	user's Windows account to be locked out after the specified number of failed logon attempts has been exceeded by the user. This option requires the Windows account lockout option to be enabled in Domain Security Policy or Domain Controller Security Policy. • **Locked accounts must be unlocked by an administrator** Specifies that locked accounts can only be unlocked by an administrator. Use the **Lockout duration** option to set the lockout duration in minutes. The lockout duration period is counted from the moment of most recent logon attempt. That is, if the user attempts to logon while the account is still locked, the lockout duration is recalculated from the moment of that last attempt. If you set the **Lockout duration** value to **0**, the locked user accounts can only be unlocked by an administrator. • **Automatically reset account after successful login** Resets the count of unsuccessful logon attempts to 0 after the user successfully logs on.
Enter Defender Password and PIN expiry details	Provides the following options: • **Enable Defender Password Expiry** When this check box is selected, it causes the Defender password to expire after the number of days specified in the **Expire after** option. • **Enable PIN Expiry** When this check box is selected, it causes the token PIN to expire after the number of days specified in the **Expire after** option. This check box is only available if the token selected for authentication has a PIN.

Defender Rollout Mode

This section explains how to configure the rollout option in the following two scenarios:

- Organizations where limited administration is required: In this scenario, users are switched to token authentication as soon as a token is registered with their user account. No administration is required.
- Organizations with less Defender users, or where token self-registration is not in use: In this scenario, when a token is registered to the user account, administrative action is required to move users to the correct Active Directory group.

In both the scenarios the following security policies are required:

- Token
- Active Directory password (rollout mode)

Automatically Switching to Token Authentication

1. Configure an access node for your access device (NAS), as a Radius Agent, allowing access for domain users using the Token policy.
2. Configure a second access node, as a Radius Agent on a different port, using the IP address of the Defender Security Server and allowing access for domain users with the Active Directory password (rollout mode) policy applied.
3. Configure a third access node as a Radius Proxy, using the IP address of the Defender Security Server on the same port and Shared Secret as configured in step 2.
   NOTE: Do not assign any members or a security policy.
4. This configuration ensures that:
   - Users with tokens can authenticate using the first access node
   - Users without tokens is redirected to the second access node and authenticated using their Active Directory password.

   Once a user has been assigned a token or has used Defender Self-Registration to register a token, the user is not redirected and can authenticate using the first access node (Token policy).

Manually switching to token authentication

1. Create two Active Directory security groups. One group with users who are token authenticated, for example, **Defender Auth**, and the other group with users who require Active Directory password, for example, **Defender AD Password**.
2. Assign the **Token** policy to the **Defender Auth** group.
3. Assign the **Active Directory password** policy to the **Defender AD Password** group.
4. Configure an access node for your access device (NAS), adding both AD groups to the members tab without assigning any policy on the access node.

   Users in the **Defender Auth** security group authenticate with tokens and users in the **Defender AD Password** group authenticate with Active Directory Passwords.

   When the users of **Defender AD Password** group are assigned a token, the administrator has to move users to the **Defender Auth** group and ensure they are removed from the **Defender AD Password** group.

Modifying Defender Security Policy object properties

To modify Defender Security Policy object properties

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 then expand the **Defender** container.
3. Click to select the **Policies** container.
4. In the right pane, double-click the Defender Security Policy whose properties you want to modify.
5. Use the dialog box that opens to modify the Defender Security Policy properties as necessary.

   The dialog box has the following tabs:

   - **General tab** Allows you to configure the Defender Security Policy.
   - **Account tab** Allows you to configure the Defender Security Policy settings related to the lockout of user accounts.
   - **Expiry tab** Allows you to configure expiry settings for Defender passwords and token PINs.
   - **Logon Hours tab** Allows you to configure a time slot when authentication via Defender is permitted or denied to the user.
   - **SMS Token tab** Allows you to configure settings for sending SMS messages containing one-time passwords to users' SMS-capable devices.
   - **E-mail Token tab** Allows you to configure settings for sending e-mail messages containing one-time passwords to the users.
   - **GrIDsure Token tab** Allows you to enable the use of GrIDsure Personal Identification Pattern (PIP) for authentication via Defender.
6. When you are finished, click **OK** to apply your changes.

General tab

This tab allows you to configure the Defender Security Policy. On this tab, you can use the following options:

- **Description** View or change the Defender Security Policy description.
- **Use** Select a primary authentication method for the Defender Security Policy. An authentication method determines the credentials that the user must enter when authenticating. For available authentication methods and their descriptions, see New Object - Defender Policy Wizard reference.

Logon Attempts Enter the number of times that the user can attempt to log on. If the number of unsuccessful logon attempts exceeds the specified limit, the violation count for the user's account is incremented.

Use Synchronous tokens as Event tokens Select this check box to enable the use of the same DIGIPASS GO token response for logon to more that one system without generating a new response, provided that the logon process takes less than 36 seconds which is the validity period for a DIGIPASS GO token response.

- **Followed By** Select an additional authentication method for the Defender Security Policy. To disable the use of additional authentication method, select **None**.

  Logon Attempts Enter the number of times that the user can attempt to log on. If the number of unsuccessful logon attempts exceeds the specified limit, the violation count for the user's account is incremented.

  Use Synchronous tokens as Event tokens Select this check box to enable the use of the same DIGIPASS GO token response for logon to more that one system without generating a new response, provided that the logon process takes less than 36 seconds which is the validity period for a DIGIPASS GO token response.

Account tab

This tab allows you to configure the Defender Security Policy settings related to the lockout of user accounts. On this tab, you can use the following options:

- **Enable Account Lockout** Select this check box to enable the user's Defender account lockout after the number of violations (unsuccessful logon attempts) specified in the **Lockout after n violations** option. Clear this check box to disable account lockout.
- **Lockout Windows account after indicated violations** Select this check box to lock out the user's Windows account after the user has exceeded the specified number of unsuccessful logon attempts. This option requires the Windows account lockout option to be enabled in Domain Security Policy or Domain Controller Security Policy. If the Windows account is locked, the user is unable to logon to their Windows account locally or remotely via Defender.
- **Locked accounts must be unlocked by an administrator** Specifies that locked accounts can only be unlocked by an administrator. Use the **Lockout duration** option to set the lockout duration in minutes. The lockout duration period is counted from the moment of most recent logon attempt. That is, if the user attempts to logon while the account is still locked, the lockout duration is recalculated from the moment of that attempt. If you set the **Lockout duration** value to **0**, the locked user accounts can only be unlocked by an administrator.
- **Automatically reset account after successful login** Resets the count of unsuccessful logon attempts to 0 after the user successfully logs on.

Expiry tab

This tab allows you to configure expiry settings for Defender passwords and token PINs. These settings only apply if authentication requires a Defender password and/or a token protected with a PIN. On this tab, you can use the following options:

- **Enable Defender Password Expiry** Causes the Defender password to expire after the number of days specified in the **Expire after** option.
- **Enable PIN Expiry** Causes the token PIN to expire after the number of days specified in the **Expire after** option.
- **Allow authentication with expired Active Directory password** Enables the user to authenticate via Defender even if the user's Active Directory password has expired. This option only has effect if the authentication method selected for the user is **Active Directory password**, **Active Directory Password with Token** or **Token with Active Directory password**.
- **Allow expired Active Directory password to be changed** Enables the user to change an expired Active Directory password. This setting can only be used if the method used by the user to communicate with Defender also supports the password change option.

Logon Hours tab

This tab allows you to configure a time slot when authentication via Defender is permitted or denied to the user. Click and drag in the grid to select the time slot in which you want to permit or deny authentication via Defender.

On this tab, you can use the following options:

Logon permitted Select this option to allow authentication via Defender in the selected time slot. The time slot during which authentication is allowed is marked in blue.

- **Logon denied** Select this option to deny authentication via Defender in the selected time slot. The time slot during which authentication is denied is marked in white.
- **Permit All** Click to permit authentication via Defender at all times.
- **Deny All** Click to deny authentication via Defender at all times.
- **Invert** Click to change the selected time slot from permit to deny or vice versa.

SMS Token tab

This tab allows you to configure settings for sending SMS messages containing one-time passwords to users' SMS-capable devices. On this tab, you can use the following options:

- **Enable SMS token** Enables the SMS token for the users to whom this Defender Security Policy applies.

- **Send SMS to user as required** Enables Defender to send an SMS message containing new one-time passwords to the user when the user is about to expend the one-time passwords provided in the previous SMS message.
- **Only send SMS when user enters keyword** Causes the Defender Security Server to send an SMS message containing one-time passwords only when the user enters the specified trigger keyword during authentication.
- **Responses per SMS** Allows you to specify the number of one-time passwords you want to include in each SMS message to be sent to the user. You can specify a value from 1 to 10.
- **Keyword** Specify the keyword that will trigger the sending of an SMS message containing one-time passwords to the user. The keyword works as a trigger when it is entered by the user during authentication. If the SMS token has a PIN assigned, you can specify that PIN as the trigger keyword as well.

  You can select the **Use AD Password** check box to make the user's Active Directory password act as the keyword that causes the Defender Security Server to send the SMS message.

  If this check box is selected and an account lockout policy is enforced in the domain, then a number of unsuccessful authentication attempts may lock out the user's Active Directory account. Use this check box with caution.
- **Phone attribute** Select the Active Directory attribute that stores user's mobile phone number to which you want to send SMS messages containing one-time passwords.
- **Mobile provider URL** Type the URL of the mobile service provider through which you want to send SMS messages containing one-time passwords.
- **[USERID]** Type the user name of the account under which you want to access the mobile service provider's Web site.
- **[PASSWORD]** Type the password that matches the user name in the **[USERID]** text box.
- **POST Data** Click this button to enter the information you want to send to the mobile service provider at the URL specified on this tab. The default POST data provided in this option is only applicable to the 2sms mobile service provider. Contact your mobile service provider for more information about the syntax you need to use in this option.
- **Test** Click to test the settings specified on this tab.

E-mail Token tab

This tab allows you to configure settings for sending e-mail messages containing one-time passwords to the users. On this tab, you can use the following options:

- **Enable e-mail token** Enables the e-mail token for the users to whom this Defender Security Policy applies.

- **Send e-mail to user as required** Enables Defender to send an e-mail message containing new one-time passwords to the user when the user is about to expend the one-time passwords provided in the previous e-mail message.
- **Only send e-mail when user enters keyword** Causes the Defender Security Server to send an e-mail message containing one-time passwords only when the user enters the specified trigger keyword during authentication.
- **Responses per e-mail** Specify the number of one-time passwords you want to include in each e-mail message. The one-time passwords must be used sequentially. The penultimate or last one-time password triggers the sending of a new e-mail containing one-time passwords.
- **Keyword** Specify the keyword that will trigger the sending of an e-mail message containing one-time passwords to the user. The keyword works as a trigger when it is entered by the user during authentication. If the e-mail token has a PIN assigned, you can specify that PIN as the trigger keyword as well.

  You can select the **Use AD Password** check box to make the user's Active Directory password act as the keyword that causes the Defender Security Server to send the SMS message.

  If this check box is selected and an account lockout policy is enforced in the domain, then a number of unsuccessful authentication attempts may lock out the user's Active Directory account. Use this check box with caution.
- **E-mail attribute** Select the Active Directory attribute that stores user's e-mail address to which you want to send e-mail messages containing one-time passwords.
- **Subject** Type the subject line you want to display in the **Subject** field of the e-mail messages containing one-time passwords.
- **From address** Type the e-mail address you want to appear in the **From** field of the e-mail messages containing one-time passwords.
- **Send copy to** Type the e-mail address to which you want to send copies of the e-mail messages containing one-time passwords.
- **Mail Content** Click this button to view and edit the text that will be included in the body of each e-mail message containing one-time passwords. The [RESPONSES] variable indicates the position in the text at which the one-time passwords appear. If the [RESPONSES] variable is missing, the one-time passwords appear at the foot of the text.
- **Mail Server** Click this button to specify the SMTP server you want to use for sending e-mail messages containing one-time passwords. In the dialog box that opens, use the following options:
  - **Name** Type the name or IP Address of the SMTP server.
  - **Port** Type the port number used by the SMTP server. The default port is 25.
  - **Authentication** Select the authentication method required by the SMTP server, and then type the user name and password of the access account you want to use.
- **Test** Click to test the settings on this tab by sending a test e-mail message to the address you specify.

GrIDsure Token tab

This tab allows you to enable the use of GrIDsure Personal Identification Pattern (PIP) for authentication via Defender. On this tab, you can use the following options:

- **Enable GrIDsure token** Enables the use of GrIDsure PIP for authentication via Defender.
- **Pattern length between** Allows you to set the minimum and maximum length for the GrIDsure PIP.
- **Block consecutive patters (horizontal, vertial, and diagonal)** Prevents the use of simple GrIDsure PIP.
- **Expire pattern after** Causes the GrIDsure PIP to expire after the specified number of days. Use the drop-down list to set the number of days upon which you want the GrIDsure PIP to expire.
- **Use numbers in grid** Enables the use of numbers in the GrIDsure PIP.
- **Use letters in grid** Enables the use of letters in the GrIDsure PIP.
- **Grid Style** Click to configure the size of the PIP grid and the colors used in the grid.

Default Defender Security Policy

If a user is a member of an Access Node and no Defender Security Policy is applied to the user explicitly or implicitly, then a default Defender Security Policy is effective for the user.

The default Defender Security Policy is configured as follows:

- Primary authentication method is *security token*.
- User's violation count is incremented by one after each 3 unsuccessful authentication attempts.
- Violation count upon which the user's account is locked is 4. Lockout duration is 3 minutes.
- Violation count is reset each time the user successfully authenticates.
- The user can log on 24 hours a day, 7 days a week.
- SMS token, e-mail token, and GrIDsure token are disabled for the user.

Managing Access Nodes

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

After creating an Access Node, you need to assign it to a Defender Security Server, specify its members (users or groups you want to authenticate through the node), and select a Defender Security Policy for the node.

- Creating an Access Node
- Modifying Access Node properties

Creating an Access Node

To create an Access Node

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 then expand the **Defender** container.
3. Right-click the **Access Nodes** container, point to **New**, and then click **Defender Access Node**.
4. Complete the wizard that starts to create a new Access Node.

   For more information about the wizard steps and options, see New Object - Defender Access Node Wizard reference.

New Object - Defender Access Node Wizard reference

Table 10:
New Object - Defender Access Node Wizard reference

Wizard step	Options
Enter a name and description for this Access Node	Provides the following text boxes: • **Name** Type a name for the Access Node being created. • **Description** Type a description for the Access Node being created.
Select the node type and user ID type for this Access Node	Provides the following options: • **Node Type** Use this list to select a type for the Access Node being created. The following node types are available: **Radius Agent** Allows a NAS device to connect to

Wizard step	Options
	Defender using the RADIUS protocol. RADIUS is transmitted over UDP and uses port 1812 by default. This is the default setting and is supported by most access devices. **Radius Proxy** Allows RADIUS requests received from a RADIUS Agent access node to be forwarded to another RADIUS Server. **Radius Proxy (to non-negotiating server)** Allows Defender to issue the response request on behalf of the RADIUS Server. This node type is typically used when migrating from RSA to Defender. In some cases, the user ID included in the request sent from the Access Node and proxied by the Defender Security Server to the RADIUS Server cannot be processed by the RADIUS Server, unless accompanied by a password. **Defender Agent** Allows Defender agents to connect and process authentication requests. Typically, this node type is required for use with legacy Cisco ACS devices. Defender agents use a proprietary protocol to transmit data and use TCP (default port number 2626), instead of the UDP of RADIUS. **NetScreen Agent** Select this node type if your Access Node is a NetScreen VPN. **NC-PASS Radius Agent** Select this node type if you are using the NC-Pass two-factor authentication software. **Nortel VPN Agent** Select this node type if you plan to authenticate using an SNK token in synchronous mode. • **User ID** Use this list to select the required user ID type. This is the user ID that will be used to locate the user in Active Directory. The available options are **SAM Account Name**, **Defender ID**, **User Principal Name**, **Proper Name**, and **E-mail Address**. If you select **E-mail Address**, the e-mail address specified on the **General** tab of the user **Properties** dialog box is used.
Enter the connection details for this Access Node	• **IP Address or DNS Name** Type the IP address or Network ID (IP address or DNS name) from which the Defender Security Server will accept authentication requests. If you specify a single IP address, you must use the

Wizard step	Options
	255.255.255.255 subnet mask. If you specify a network ID (for example, 192.168.10.0) and subnet mask 255.255.255.0, this causes the corresponding Defender Security Server to accept authentication requests from all hosts on the specified subnet (192.168.10.0). • **Port** Type the port number of the Defender Security Server. • **Subnet Mask** Type the subnet mask you want to use for the Access Node. • **Shared Secret** Type the shared secret you want to use. The shared secret configured on the access device must match the shared secret specified for the Access Node. The shared secret can be up to 63 alphanumeric characters. (For a Defender Agent Access Node, the shared secret can be 16 hex or 24 octal digits).

Modifying Access Node properties

To modify Access Node properties

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 then expand the **Defender** container.
3. Click to select the **Access Nodes** container.
4. In the right pane, double-click the Access Node whose properties you want to modify.
5. Use the dialog box that opens to modify the Access Node properties as necessary.

The dialog box has the following tabs:

- **General tab** Allows you to view or edit the Access Node configuration.
- **Servers tab** Allows you to view or edit a list of the Defender Security Servers to which the Access Node is assigned.
- **Members tab** Allows you to specify users or groups whose members can authenticate via the Access Node.
- **Policy tab** Allows you to assign a Defender Security Policy to the Access Node.
- **RADIUS Payload tab** Allows you to configure the RADIUS payload for the Access Node.

6. When you are finished, click **OK** to apply your changes.

General tab

This tab allows you to view or edit the Access Node configuration. The tab has the following elements:

- **Description** View or edit the Access Node description.
- **IP Address or DNS Name** View or edit the IP address or DNS name of the NAS device.

  Examples:

  192.168.70.9 Allows connections from this IP address only.

  192.168.70.0 Allows connections from any IP address on the 192.168.70.0 subnet (subnet mask 255.255.255.0 would also be required).
- **Subnet Mask** View or edit subnet mask for the Access Nodes that connect to the Defender Security Server.
- **Authentication Port** View or edit the number of the port on which the Access Node accepts RADIUS requests.

  The default ports are:

  1812 RADIUS agent, RADIUS proxy.

  2626 Defender agent.
- **Accounting Port** View or edit the port number on which the Access Node accepts RADIUS accounting packets. Upon receipt of an accounting packet, its contents are written to an accounting log. The default port number is 1813.
- **Node Type** View or change the current node type. For available node types and their descriptions, see New Object - Defender Access Node Wizard reference.
- **Shared Secret** View or edit the shared secret that this Access Node uses when attempting to establish a connection with the Defender Security Server. To view a hidden shared secret, click the **Reveal** button next to this text box. To conceal a visible shared secret, click the **Hide** button next to this text box.
- **User ID** View or change the type of user ID by which the Defender Security Server searches for users in Active Directory. Possible values are **Defender ID**, **User Principle Name**, **SAM Account Name**, **Proper Name**, and **E-mail Address**.

Servers tab

This tab allows you to view or change a list of the Defender Security Servers to which the Access Node is assigned. To add a new Defender Security Server to the list, click **Assign**. To remove a Defender Security Server from the list, select that server, and then click **Unassign**.

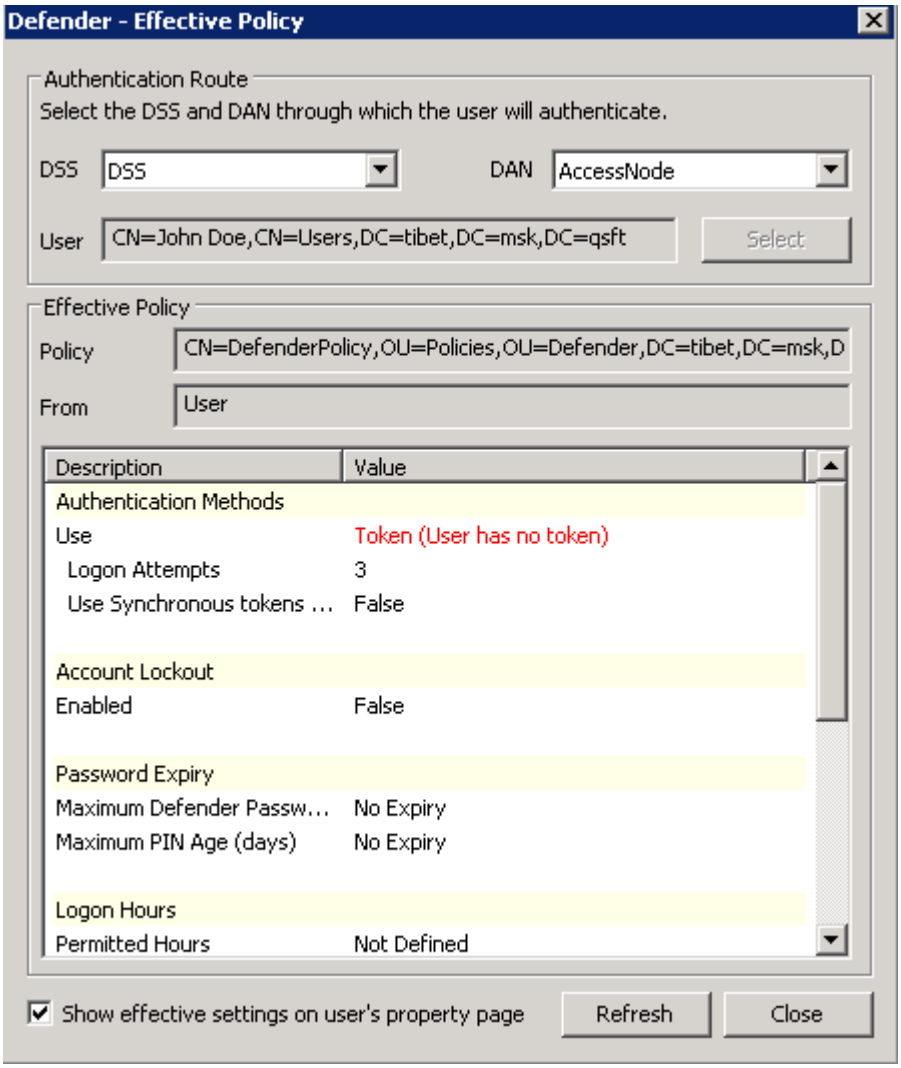
Members tab

This tab allows you to set up a list of users who can authenticate via this Access Node. To add users or groups to the list, click **Add**. To remove an entry from the list, select that entry, and then click **Remove**.

Policy tab

This tab allows you to view the current or assign a new Defender Security Policy to the Access Node. The tab has the following elements:

- **Assigned Policy** Shows the Defender Security Policy that is currently assigned to the Access Node. When there is no Defender Security Policy assigned to the Access Node, this option displays <undefined>.
- **Select** Allows you to select a Defender Security Policy to assign to the Access Node.
- **Clear** Unassigns the current Defender Security Policy from the Access Node.
- **Effective** Click this button to view the Defender Security Policy settings that will apply to a specific user for a particular Defender Security Server/Access Node combination. The window that opens looks similar to the following:

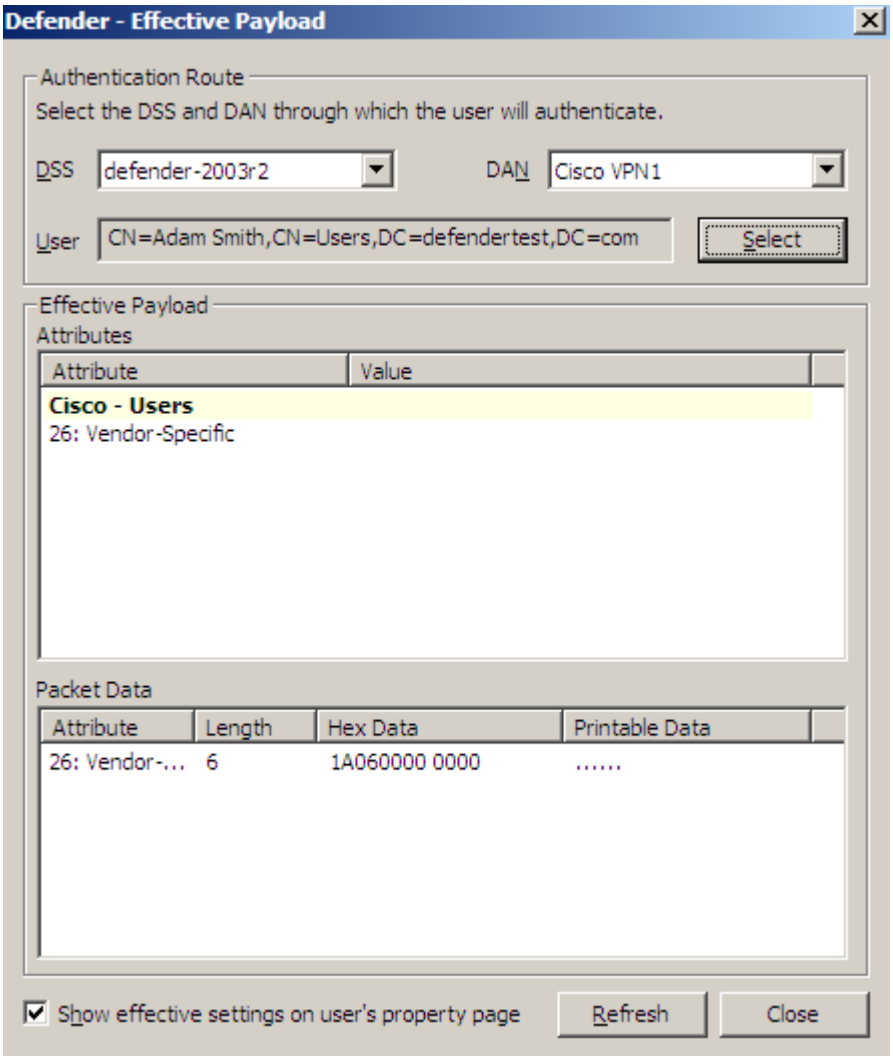


- Click the **Select** button to select the user for whom you want to view the Defender Security Policy that will apply.
- The **DSS** list shows the Defender Security Server that is currently selected for the user. If necessary, select any other Defender Security Server.
- The **DAN** list shows the Access Node that is currently selected for the user. If necessary, select any other Access Node.
- The **Effective Policy** area displays the Defender Security Policy details and authentication settings that will be effective when the user authenticates via Defender.

RADIUS Payload tab

This tab allows you to view the current and assign a new RADIUS payload to the Access Node. The tab has the following elements:

- **Assigned Payload** Shows the RADIUS payload that is currently assigned to the Access Node. When there is no RADIUS payload assigned to the Access Node, this option displays <undefined>.
- **Select** Allows you to select a RADIUS payload to assign to the Access Node.
- **Clear** Unassigns the current RADIUS payload from the Access Node.
- **Inherit payload entries from parent. Include these with entries explicitly defined here.** When selected, causes the Access Node to inherit RADIUS payload from the Defender Security Servers to which the Access Node is assigned.
- **Effective** Click this button to view the RADIUS payload that will apply to a specific user for a particular Defender Security Server/Access Node combination. The windows that opens looks similar to the following:



Click the **Select** button to select the user for whom you want to view the RADIUS payload that will apply.

The **DSS** list shows the Defender Security Server that is currently selected for the user. If necessary, select any other Defender Security Server.

The **DAN** list shows the Access Node that is currently selected for the user. If necessary, select any other Access Node.

The **Effective Payload** area displays the details of the RADIUS payload that will be effective when the selected user authenticates via Defender.

Managing Defender Security Servers

Defender Security Server is the point in your network where user authentication is performed. If authentication is successful, the user is allowed access to the network.

- Creating a Defender Security Server object
- Modify Defender Security Server object properties

Creating a Defender Security Server object

To create a Defender Security Server 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 (console tree), expand the appropriate domain node, and then expand the **Defender** container.
3. Right-click the **Security Servers** container, point to **New**, and then click **Defender Security Server**.

   A wizard starts.
4. In the **Enter a name, IP address and description for the Security Server** step, use the following options:
   - **Name** Type a name for the Defender Security Server object to be created in Active Directory. This name can be different from the name of the computer on which the Defender Security Server component is installed.
   - **IP Address** Type the IP address of the computer on which you have installed the Defender Security Server component.
   - **Description** Type a friendly Defender Security Server description to be displayed in Active Directory.
5. Complete the wizard to create the Defender Security Server object in Active Directory.

After creating a Defender Security Server object, you need to modify its properties to assign a Defender Security Policy, Access Node, and RADIUS payload to that object. For more information, see Modify Defender Security Server object properties on page 72.

Modify Defender Security Server object properties

To modify Defender Security Server object properties

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 then expand the **Defender** container.
3. Click to select the **Security Servers** container.
4. In the right pane, double-click the Defender Security Server whose properties you want to modify.
5. Use the dialog box that opens to modify the Defender Security Server properties as necessary.

   The dialog box has the following tabs:

   - **Security Server tab** Allows you to specify a computer on which the Defender Security Server component is installed by IP address, change description provided for the Defender Security Server object in Active Directory, and assign or unassign Access Nodes for the Defender Security Server object.
   - **Prompts tab** Allows you to view and modify the messages and prompts that may be displayed to the user during the authentication process.
   - **Policy tab** Allows you to assign a Defender Security Policy to the Defender Security Server object.
   - **RADIUS Payload tab** Allows you to assign a RADIUS payload to the Defender Security Server object.
6. When you are finished, click **OK** to apply your changes.

General tab

This tab allows you to specify the IP address of the computer on which the Defender Security Server component is installed and change the description provided for the Defender Security Server object in Active Directory.

On this tab, you can use the following options:

- **Description** View or edit the Defender Security Server description that is displayed in Active Directory.
- **Address** View or edit the IP address of the computer on which you have installed the Defender Security Server component.
- **Version** Displays the version number of the Defender Security Server component.
- **Status** Displays the current status of the Defender Security Server.

Security Server tab

This tab allows you to assign or unassign Access Nodes for the Defender Security Server object.

Use the **Assigned Access Nodes** list to view or edit the list of Access Nodes whose users authenticate through this Defender Security Server. To add a new Access Node to the list, click the **Assign** button. To remove an Access Node from the list, select that Access Node, and then click the **Unassign** button.

Prompts tab

This tab allows you to view and modify the messages displayed to the user during the authentication process. If you have modified a message in the list, you can always return to the default version of the message that existed before your modifications.

To edit a message

1. In the list, click the message you want to edit.
2. Edit the message as necessary in the text box below the list.
3. Click the **Update** button to apply your changes.

To roll back to the default version of a message

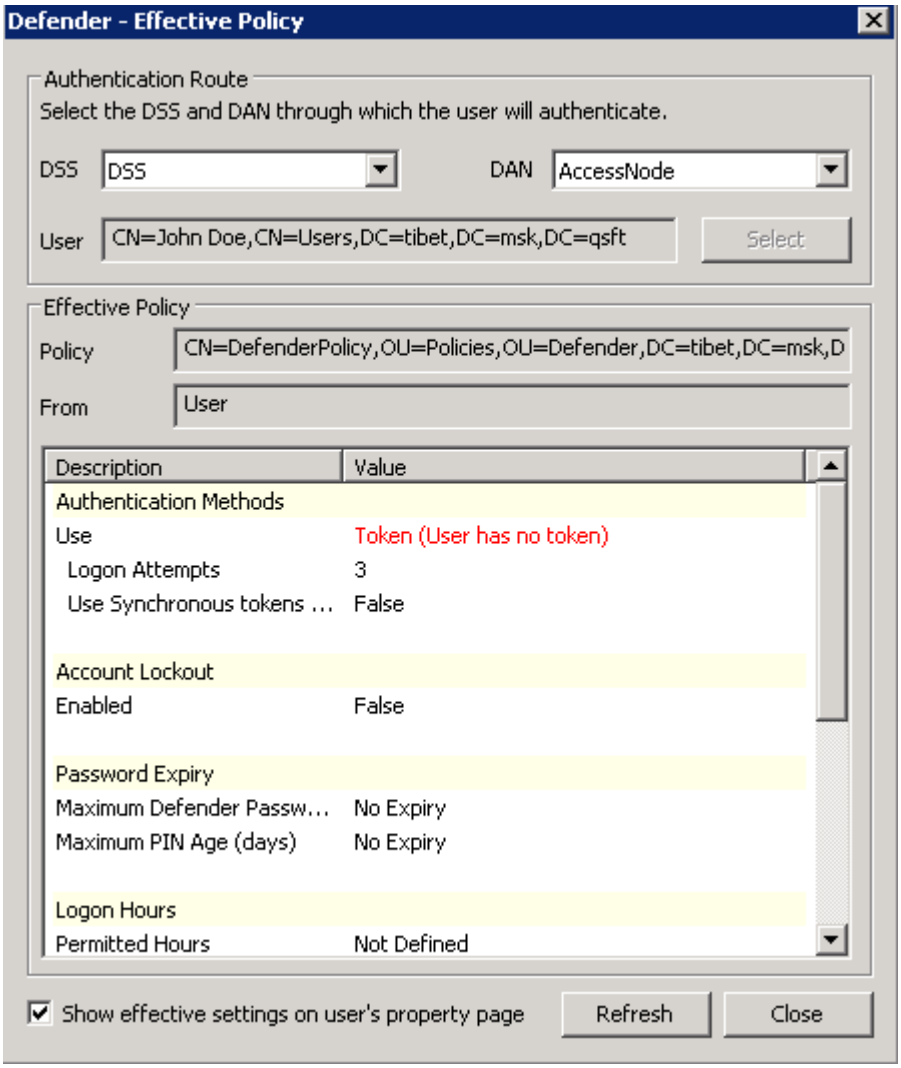
1. In the list, click the message you have modified earlier.
2. Click the **Default** button, and then click the **Update** button.

Policy tab

This tab allows you to view the current and assign a new Defender Security Policy to the Defender Security Server object.

On this tab, you can use the following elements:

- **Policy** Shows the Defender Security Policy that is currently assigned to the Defender Security Server object. When there is no Defender Security Policy assigned to the Defender Security Server object, this option displays <undefined>.
- **Select** Allows you to select a Defender Security Policy to assign to the Defender Security Server object.
- **Clear** Unassigns the current Defender Security Policy from the Defender Security Server object.
- **Effective** Click this button to view the Defender Security Policy settings that will apply to a specific user for a particular Defender Security Server/Access Node combination. The window that opens looks similar to the following:



Click the **Select** button to select the user for whom you want to view the Defender Security Policy that will apply.

The **DSS** list shows the Defender Security Server that is currently selected for the user. If necessary, select any other Defender Security Server.

The **DAN** list shows the Access Node that is currently selected for the user. If necessary, select any other Access Node.

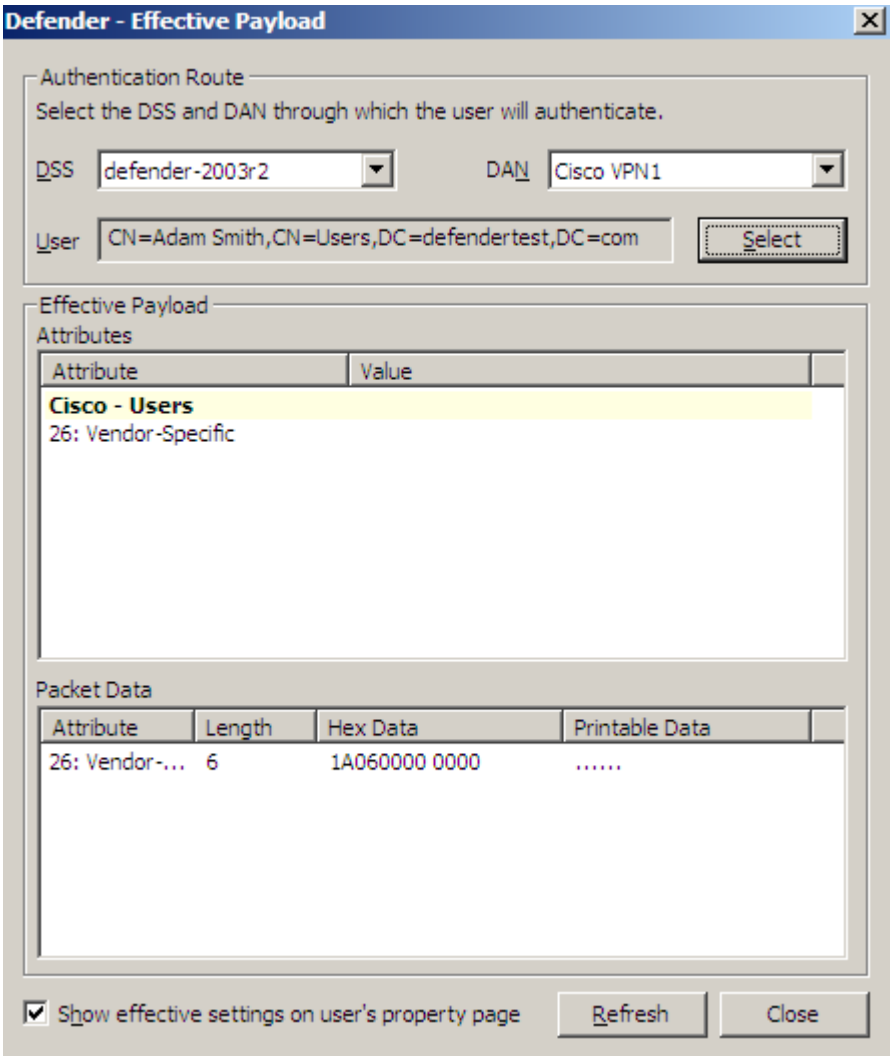
The **Effective Policy** area displays the Defender Security Policy details and authentication settings that will be effective when the user authenticates via Defender.

RADIUS Payload tab

This tab allows you to view the current and assign a new RADIUS payload to the Defender Security Server object.

On this tab, you can use the following elements:

- **Payload** Shows the RADIUS payload that is currently assigned to the Defender Security Server object. When there is no RADIUS payload assigned to the Defender Security Server object, this option displays <undefined>.
- **Select** Allows you to select a RADIUS payload to assign to the Defender Security Server object.
- **Clear** Unassigns the current RADIUS payload from the Defender Security Server object.
- **Effective** Click this button to view the RADIUS payload that will apply to a specific user for a particular Defender Security Server/Access Node combination. The windows that opens looks similar to the following:



Click the **Select** button to select the user for whom you want to view the RADIUS payload that will apply.

The **DSS** list shows the Defender Security Server that is currently selected for the user. If necessary, select any other Defender Security Server.

The **DAN** list shows the Access Node that is currently selected for the user. If necessary, select any other Access Node.

The **Effective Payload** area displays the details of the RADIUS payload that will be effective when the selected user authenticates via Defender.

Creating a RADIUS payload object

Remote Access Dial in User Service (RADIUS) is an access-control protocol that verifies and authenticates users based on challenge-response method. This protocol allows a computer to verify your identity, find out what you are allowed to access, and then tell you all of this.

The RADIUS protocol is built around the AAA concept, which stands for authentication (the process of verifying identity), authorization (the process of defining what you are allowed to do), and accounting (the process of monitoring logging statistics and usage information).

The purpose of RADIUS payload is to have the Defender Security Server send information back to the NAS device for reasons such as extra security or for accounting or other reasons specific to the NAS.

To create a RADIUS payload 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 (console tree), expand the appropriate domain node, and then expand the **Defender** container.
3. Right-click the **RADIUS Payload** container, point to **New**, and then click **Defender RADIUS Payload**.

A wizard starts.

4. In the **Enter a name and description for this RADIUS Payload** step, type a name and description for the payload being created. Click **Next**.
5. On the **Select the attributes to return when access is approved** step, use the **Add** button to add the attributes you want the RADIUS payload to return, and assign values to those attributes. For more information, see RADIUS payload attributes on page 77.

RADIUS payload attributes

The next table lists the attributes you can assign to a RADIUS payload. The RADIUS payload will return these attributes after user's access to the resource has been approved. For instructions on how to create a RADIUS payload, see Creating a RADIUS payload object.

Table 11:
Attributes you can assign to a RADIUS payload

Attribute	Description
06: Service-Type	Specifies the type of service the user has requested or the type of service to be provided. This attribute can take one of the following values: • 1 - Login • 2 - Framed • 3 - Callback Login • 4 - Callback Framed • 5 - Outbound • 6 - Administrative • 7 - NAS Prompt • 8 - Authenticate only • 9 - Callback NAS Prompt • 10 - Call Check • 11 - Callback Administrative • 12 - Voice • 13 - Fax • 14 - Modem Replay • 15 - IAPP-Register • 16 - IAPP-AP-Check • 17 - Authorize Only
07: Framed-Protocol	Specifies the framing to be used for framed access. This attribute can take one of the following values: • 1 - PPP • 2 - SLIP • 3 - Apple Talk Remote Access Protocol (ARAP) • 4 - Gandalf proprietary SingleLink/MultiLink protocol • 5 - Xylogics proprietary IPX/SLIP • 6 - X.75 Synchronous • 7 - GPRS PDP Context
08: Framed-IP-Address	Specifies the address to be configured for the user. This attribute can take one of the following values:

Attribute	Description
	• 0xFFFFFFFF - NAS should allow the user to select an address • 0xFFFFFFFE - NAS should select an address for the user • Specific IP address value
09: Framed-IP-Netmask	Specifies the IP netmask to be configured for the user when the user is a router to a network.
10: Framed-Routing	Specifies the routing method for the user when the user is a router to a network. This attribute can take one of the following values: • 0 - None • 1 - Send routing packets • 2 - Listen for routing packets • 3 - Send and Listen
11: Filter-Id	Specifies the name of the filter list for particular user. The value of this attribute can include individual groups or all groups of which the user is a member. The default value is all groups. When the user has been successfully authenticated by the Defender Security Server, groups that include the authenticated user's ID are returned to the NAS.
12: Framed-MTU	Specifies the maximum transmission unit (MTU) to be configured for the user when it is not negotiated by some other means such as PPP.
13: Framed-Compression	Specifies a compression protocol to be used for the link. This attribute can take one of the following values: • 0 - None • 1 - VJ TCP/IP header compression • 2 - IPX header compression • 3 - Stac-LZS compression
14: Login-IP-Host	Specifies the system with which to connect the user, when the Login-Service attribute is included. This attribute can take one of the following values: • 0xFFFFFFFF - NAS should allow the user to select an address • 0 - NAS should select a host to connect the user to

Attribute	Description
	• Specific address value
25: Class	Available to be sent by the server to the client in an Access-Accept and should be sent unmodified by the client to the accounting server as part of the Accounting-Request packet if accounting is supported. The value of this attribute can include individual groups or all groups of which the user is a member. When the user has been successfully authenticated by the Defender Security Server, groups that include the authenticated user's ID are returned to the NAS that initiated the authentication request.
26: Vendor Specific	Specifies a method for communicating vendor-specific information between Network Access Servers and RADIUS servers. This attribute encapsulates vendor-specific attributes, allowing vendors to support their own extended attributes otherwise not suitable for general use.
Custom	Allows you to specify a custom attribute by attribute ID.

3

Configuring security tokens

For users to authenticate and access resources protected with Defender, you need to configure and assign security tokens supported by Defender to them. Defender can work with a number of security tokens, which include native Defender tokens and third-party tokens.

The native Defender tokens include the following:

- **Defender Soft Token** Can be installed and used in various environments and operating systems, such as Android, Java Runtime Environment, iOS, and Windows.
- **E-mail token** Allows users to authenticate by using one-time passwords sent to their e-mail address.
- **GrIDsure token** Allows users to authenticate by using a GrIDsure Personal Identification Pattern (PIP).
- **SMS token** Allows users to authenticate by using one-time passwords sent to their SMS-capable device.

Third-party security tokens supported by Defender include Authy, DIGIPASS GO, Google Authenticator, Symantec VIP credentials, and YubiKey.

Configuring Defender Soft Token

This section provides instructions on how to configure and assign to users the following security tokens:

- Defender Soft Token for Android
- Defender Soft Token for iOS
- Defender Soft Token for Java
- Defender Soft Token for Windows

To configure and assign Defender Soft Token to a user

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 nodes to select the container where the user object is located.
3. In the right pane, double-click the user object, and then click the **Defender** tab in the dialog box that opens.
4. Below the **Tokens** list, click the **Program** button.
5. In the Select Token Type step, click to select the **Software token** option. Click **Next**.
6. In the Select Software Token step, click to select the Defender Soft Token you want to configure and assign.
7. Complete the wizard to configure and assign the Defender Soft Token.

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

Configuring GrIDsure token

Before configuring and assigning the GrIDsure token, you need to enable the use of GrIDsure for authentication in the Defender Security Policy properties. Then, you need to assign that policy to the users you want to authenticate with the GrIDsure token. For more information, see Managing Defender Security Policies.

To configure the GrIDsure token for a user

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 nodes to select the container where the user object is located.
3. In the right pane, double-click the user object, and then click the **Defender** tab in the dialog box that opens.
4. Below the **Tokens** list, click the **Program** button.
5. In the Select Token Type step, click to select the **Software token** option. Click **Next**.
6. In the Select Software Token step, click to select the **GrIDsure token** option.

7. Complete the wizard to configure and assign the GrIDsure token.

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

Enabling the use of Authy

You can allow users to authenticate via Defender by using one-time passwords generated with the Authy app. For more information about Authy, please visit http://www.authy.com.

To enable Authy for a user

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 nodes to select the container where the user object is located.
3. In the right pane, double-click the user object, and then click the **Defender** tab in the dialog box that opens.
4. Below the **Tokens** list, click the **Program** button.
5. In the Select Token Type step, click to select the **Software token** option. Click **Next**.
6. In the Select Software Token step, click to select the **Authy token** option.
7. Complete the wizard to enable Authy for the user.

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

Enabling the use of Google Authenticator

You can allow users to authenticate via Defender by using one-time passwords generated with Google Authenticator.

To enable Google Authenticator for a user

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 nodes to select the container where the user object is located.
3. In the right pane, double-click the user object, and then click the **Defender** tab in the dialog box that opens.

4. Below the **Tokens** list, click the **Program** button.
5. In the Select Token Type step, click to select the **Software token** option. Click **Next**.
6. In the Select Software Token step, click to select the **Google Authenticator** option.
7. Complete the wizard to enable Google Authenticator for the user.

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

Configuring SMS token

SMS token allows users in your organization to receive SMS messages containing one-time passwords on their SMS-capable devices. Before configuring and assigning the SMS token, you need to enable the use of the SMS token in the Defender Security Policy properties. After enabling the SMS token, make sure you assign the Defender Security Policy to the users you want. For more information, see Managing Defender Security Policies on page 52.

Ensure you provide the following information to each SMS token user:

- User ID
- Initial PIN (if the SMS token is configured to use a PIN)

To configure the SMS token for a user

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 nodes to select the container where the user object is located.
3. In the right pane, double-click the user object, and then click the **Defender** tab in the dialog box that opens.
4. Below the **Tokens** list, click the **Program** button.
5. In the Select Token Type step, click to select the **Software token** option. Click **Next**.
6. In the Select Software Token step, click to select the **SMS token** option.
7. Complete the wizard to configure the SMS token for the user.

   For more information about the wizard steps and options, see Defender Token Programming Wizard reference

Configuring e-mail token

Enabling the e-mail token allows users in your organization to receive e-mail messages containing one-time passwords. To enable the e-mail token, use the properties of a Defender Security Policy. After enabling the e-mail token, make sure you assign the Defender Security Policy to the users you want. For more information, see Managing Defender Security Policies on page 52.

To enable and configure the e-mail token

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 nodes to select the container where the user object is located.
3. In the right pane, double-click the user object, and then click the **Defender** tab in the dialog box that opens.
4. Below the **Tokens** list, click the **Program** button.
5. In the Select Token Type step, click to select the **Software token** option. Click **Next**.
6. In the Select Software Token step, click to select the **E-mail token** option.
7. Complete the wizard to configure the e-mail token for the user.

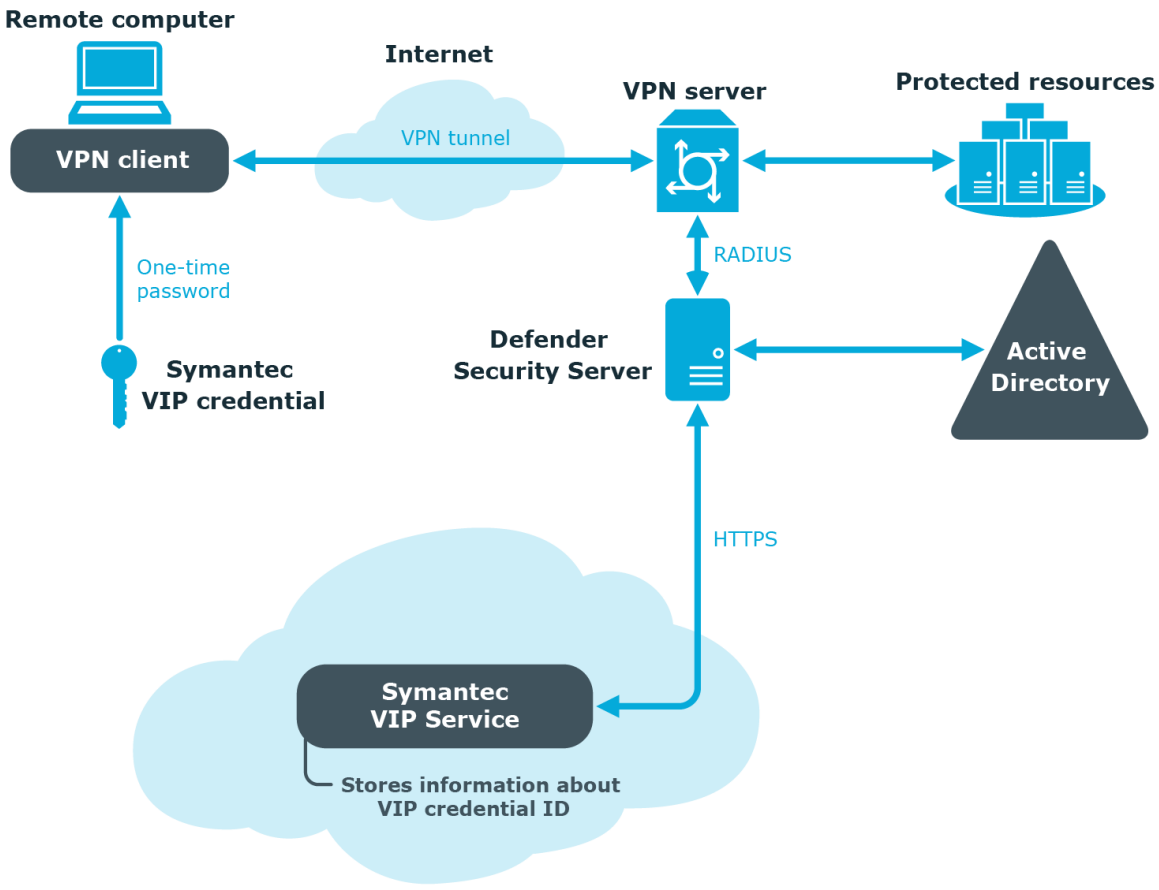
   For more information about the wizard steps and options, see Defender Token Programming Wizard reference

Configuring VIP credentials

You can configure Defender to use Symantec Validation & ID Protection (VIP) credentials for two-factor authentication of users within your organization. VIP credentials are security tokens allowing you to generate one-time passwords. VIP credentials can be implemented as security cards, hardware tokens, and software tokens for mobile phones and Windows-based computers.

When working with VIP credentials, Defender acts as a proxy server, redirecting authentication requests to the Symantec VIP Service, a cloud-based authentication solution.

Two-factor authentication with a VIP credential



Upon receiving an authentication request from a user who has a VIP credential assigned, Defender redirects the request to the Symantec VIP Service via HTTPS. The Symantec VIP Service validates the authentication request—for that, the user's VIP credential must be properly registered with the Symantec VIP Service—and provides a response to Defender. If the user has been successfully authenticated by the Symantec VIP Service, Defender allows that user to access the protected resource.

To configure Defender for working with VIP credentials, you need to install a VIP certificate issued by Symantec, configure the correct URL to the Symantec VIP Service, and program VIP credentials for users in your organization.

- Enabling the use of VIP credentials
- Programming a VIP credential for a user

Enabling the use of VIP credentials

To enable the use of VIP credentials

1. Install a VIP certificate:
    a. On the computer where the Defender Administration Console is installed, start the Active Directory Users and Computers (ADUC) tool (dsa.msc).
    b. In the left pane (console tree), expand the appropriate domain node, and click to select the **Defender** container.
    c. On the menu bar, select **Defender | VIP Credential Configuration**.
    d. In the dialog box that opens, click the **Install** button.
    e. Click **Browse** to select the VIP certificate you want to use, and then type the certificate's password.
    f. When finished, click **OK**.
2. Configure the correct URL for communications with the Symantec VIP Service.

At the time of writing, the Symantec VIP Service URL was **https://services-auth.vip.symantec.com**. For the correct URL, refer to the Symantec VIP Service documentation.

3. Click the **Test** button to ensure you have correctly specified the VIP certificate, certificate password, and URL to the Symantec VIP Service.
4. When you are finished, click **OK** to close the dialog box.

Programming a VIP credential for a user

Before programming a VIP credential, make sure you enable the use of VIP credentials in Defender. For more information, see Enabling the use of VIP credentials on page 87.

In this step, you program and assign a VIP credential to the user you want. You can reassign an existing VIP credential from one user to another or assign a new VIP credential as required.

To program a VIP credential for 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. Locate and double-click the required user object.
3. In the dialog box that opens, click the **Defender** tab.
4. Under the **Tokens** list, click the **Program** button, and then complete the wizard that starts.

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

After you complete the wizard, a new VIP credential entry appears in the **Tokens** list on the **Defender** tab.

Configuring YubiKey

You can allow users to authenticate via Defender by using one-time passwords generated with the YubiKey hardware token. Defender supports the YubiKey token programmed to work either in the Yubico OTP or OATH-HOTP mode.

See the following sections for instructions on enabling the use of the YubiKey token programmed in one of these modes:

- Yubico OTP mode
- OATH-HOTP mode

Yubico OTP mode

When the YubiKey tokens you have purchased are in the Yubico OTP mode, to enable their use with Defender, you need to specify the client ID and API key provided with the tokens in the Defender Administration Console, and then configure self-service settings on the Defender Management Portal to enable users to self-register their YubiKey tokens on the Defender Self-Service Portal.

When a user registers the YubiKey on the Defender Self-Service Portal, the corresponding token object is automatically created in Active Directory.

To enable the use of YubiKey working in Yubico OTP mode

1. In the Defender Administration Console, specify the client ID and API key provided to you with the YubiKey tokens:
    a. On the computer where the Defender Administration Console is installed, open the Active Directory Users and Computers tool (dsa.msc).
    b. In the left pane of the ADUC tool, expand the appropriate domain node, and click to select the **Defender** container.
    c. On the menu bar, select **Defender | YubiCloud Client Configuration**.
    d. In the dialog box that opens, type the client ID and API key provided to you with the YubiKey tokens.
    e. Click the **Test** button, and follow the on-screen instructions to ensure the supplied client ID and API key are valid. If the test completes successfully, click **OK** to save the client ID and API key.
2. Configure the Defender Self-Service Portal to enable the registration of YubiKey tokens for the users:

a. Open the Defender Management Portal. For more information, see Opening the portal.

b. In the left pane, click the **Self-Service Settings** tab.

c. In the right pane, on the **General** tab, use the **Permissions** area to add Active Directory groups and enable their members to register their YubiKey tokens via the Defender Self-Service Portal.

   For the descriptions of elements you can use on the **Self-Service Settings** tab, see Configuring self-service for users.

OATH-HOTP mode

When the YubiKey tokens you have purchased are in the OATH-HOTP mode, to enable their use with Defender you need to import the YubiKey token objects into Active Directory by using the .txt import file (also known as the key file) containing token object definitions. Then, you can assign the imported token objects to users as necessary.

Normally, the .txt import file is provided together with the YubiKey tokens. Before importing token objects, you need to modify the .txt import file so that Defender can read its contents.

To enable the use of YubiKey working in OATH-HOTP mode

1. Change the file name extension of the .txt import file to .csv.
2. Open the .csv file in Microsoft Excel. The .csv file looks similar to the following:

	A	B	C	D
1	2220247	b562e2988c983b9a49d48192bfdf4c3665e0db00	951840	a87280724092
2	507000	36fdb623ba8e06e7b666a0c2f6314c44a468a7d7	21264	98e2c1a178d4
3	507001	1c9408c03022eefba96fcef79cee6c8648e08e61	890752	3ba8e16ac14b

   The columns in the file contain the following:

   - **A** YubiKey serial number.
   - B 160-bit secret set
   - **C** Moving factor seed value.
   - **D** Configuration password. Contains zeros if configuration password is not set.

3. Delete column D.
4. Save the .csv file. Now the file is ready for import.

NOTE: Keep the initial .txt file containing the passwords associated with each of the Yubikeys, to program the second slot though the Yubico interface later.

5. Import token objects from the .csv file into Active Directory. For instructions, see Importing hardware token objects.
6. Assign the imported YubiKey token objects to users as necessary. For instructions, see Assigning a hardware token object to a user.

Defender Token Programming Wizard reference

Table 12:
Defender Token Programming Wizard reference

Wizard step	Your action
Select Token Type	You can select one of the following options: • **Software token** Allows you to program and assign a software token, such as Defender Soft Token, e-mail token, GrIDsure token, or SMS token. • **Hardware token** Allows you to program and assign a hardware token, such as DIGIPASS or YubiKey. This option does not support hardware VIP credentials. • **Symantec VIP credential** Allows you to program and assign a software or hardware VIP credential. This option becomes available after you enable the use of VIP credentials. For details, see Enabling the use of VIP credentials.
Select Software Token	Click to select the software token you want to program and assign to the user.
Activation Settings	Select the **Expire token activation code after** check box if you want to set a validity time period (in days) for the code with which the user must activate the software token. Then, specify the number of days during which you want the token activation code to remain valid. The token activation code is generated when you complete this wizard. Leave the **Expire token activation code after** text box cleared if you do not want to limit the validity time period of the token activation code.
Activation and Passphrase Settings	In this step, you can select the following check boxes:

Wizard step	Your action
	• **Expire token activation code after** Select this check box if you want to set a validity time period (in days) for the code with which the user must activate the software token. Then, specify the number of days during which you want the token activation code to remain valid. The token activation code is generated when you complete this wizard. • **Alert user about failed passphrase attempts** Select this check box to notify the user when the user has entered an incorrect passphrase when unlocking the token. Optionally, you can select the **Lock token passphrase after** check box to lock the passphrase after the user has expended the specified number of attempts to unlock the token. • **Token requires a passphrase** Select this check box to enforce the user to configure a passphrase for using with the token. When this check box is cleared, no passphrase is required. If you select this check box, you can optionally select the **Passphrase must be strong** check box, which requires the user to configure a passphrase that is at least six characters long, includes uppercase and lowercase characters, and numbers or special characters.
Mode, Encryption, and Response	Use the options in this step to specify an operation mode (synchronous or challenge-response), encryption method, and response length for the software token.
Select Password Algorithm	Select the one-time password algorithm you want Google Authenticator to use. You can select one of the following algorithms: • **Time based (TOTP)** One-time password remains valid for a particular amount of time. Then, Google Authenticator automatically generates a new one-time password. • **Counter based (HOTP)** One-time password remains valid until the user manually generates a new one-time password in Google Authenticator. Note that the algorithm you select in this wizard is only used if the user activates Google Authenticator with a QR code. If the user activates Google Authenticator by manually typing the activation code, the one-time password algorithm specified by the user in Google Authenticator during

Wizard step	Your action
	activation takes precedence over the option you select in this wizard.
Select Token Location	Specify the Active Directory container in which you want to store the token object. If you change the default location, ensure that the Defender Security Server service account and the Defender administrator account have sufficient permissions for the new location you specify.
Activation Code Distribution	Specify options for saving the token activation code. In this step, you can use the following options: • **One file for all users** Saves token activation codes for all users to a single file. • **Individual file for each user** Saves token activation code for each user to an individual file. • **File Location** Specify path to the folder in which you want to create files containing token activation codes. • **File Name** Specify name for the file in which you want to store token activation codes. If a file with such name does not exist, it will be created. • **Append activation codes to existing file** If you select this option and the file with the specified name already exists in the specified location, the wizard appends the activation codes to the file without overwriting its contents. If you leave this check box cleared, the existing file's contents will be overwritten with the new token activation codes.
Action for Existing GrIDsure Tokens	This step shows up if the selected users already have a GrIDsure token assigned. Each user can only have one GrIDsure token assigned. Select one of the following options: • **Overwrite existing tokens** Creates new GrIDsure token objects which overwrite the existing GrIDsure token objects assigned to the users. As a result, the users will have to configure their GrIDsure Personal Identification Pattern (PIP) the next time they access a protected resource. • **Keep using existing tokens** Does not create new GrIDsure token objects for the users who already have GrIDsure tokens assigned.

Wizard step	Your action
VIP Credential Activation	Enter the credential ID shown on the VIP credential you want to assign to the user. Make sure you register that credential ID with Symantec.

FIDO2 compatible Hardware Yubikey

Defender6.3.0 version supports FIDO2 compatible hardware Yubikey.

- A FIDO2 token
  - Can be used for authentication only in ISAPI clients.
  - Can be programmed through Management Portal only.
  - Cannot be created as a placeholder Token; it is required to program a FIDO2 token to a specific User.
- It cannot be assigned or unassigned from a user like other tokens because of FIDO2 protocol security.
- If user's hardware key is stolen/broken, it can be deleted from Management Portal.
- FIDO2 tokens will have priority during authentication if multiple other types of Tokens are assigned to user.
  - If user has FIDO2 tokens along with combination of push notification compatible and non-compatible tokens and they choose to Sign with Other option while authenticating with FIDO2, priority will be given to push Notifications.
- FIDO2 tokens will have priority while authentication if multiple other types of Tokens are assigned to user.
  - If FIDO2 with Android/iOS and other Window Token both are assigned to a user and If User chooses to Sign with Other option while authenticating with FIDO2, second priority will be given to Android/iOS tokens push Notifications.
- A maximum of 12 FIDO2 tokens can be programmed for a single user.
- FIDO2 cannot be programmed using management shell and ADUC.
  - YubiKey hardware token can be simultaneously used in FIDO2, Yubico OTP and OATH-HOTP modes.

To Program a FIDO2 Token

a. Open Management Portal, Go to Management Tab and under Users Tab, Search for User to whom you want to assign FIDO2 token.

b. Click on Program option; A window pop up will appear with different options of Software and Hardware Tokens.
c. Choose Hardware Tab and select FIDO2 option and click Program Token.
d. Another window pop-up will appear for user to enter FIDO2 token name:
    - Should be at least four characters.
    - Special character and space are not allowed.
    - Underscore(_) is allowed.
    - Maximum length should be 40 characters.
e. Click on Request and window will display success message.
f. FIDO2 token will appear in assigned token list of user with unique ID.

Operations on FIDO2 Token in Management Portal

a. Each FIDO2 token can be managed from assign token list of user using Manage button next to the token.
b. On clicking Manage, a window will appear with two tabs named EDIT and DELETE.
c. If user chooses EDIT, he can change the name of FIDO2 token.
d. If user chooses DELETE, he can delete the assigned FIDO2 token.

Configuration settings to provide access to request FIDO2 token from Self-Service

1. Sign in to the Defender Management Portal as a portal administrator.
2. Click the **Administer Defender** option.
3. In the left pane, click the **Self-Service Settings** tab.
4. In the right pane, under General tab choose Edit Permissions for AD Group.
5. Window will appear with list of tokens to make available to this group on the Defender Self-Service Portal.
6. Either Select All or select FIDO2 and click on Ok button.
7. Save the Self-Service settings.

Enabling/Disabling FIDO2 token

FIDO2 tokens are enabled by default if assigned to user for authentication. If User Does not want to use FIDO2 token, it can be disable/enable with the addition of registry entry

mentioned below:

On a computer where Defender Security Server is installed, use Registry Editor to create the following value:

```
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\PassGo Technologies\Defender\DSS Active Directory Edition

Value type: REG_DWORD

Value name: FIDO2ENABLED

Value data: 0 to disable and 1 to enable
```

See the following sections for instructions on enabling the use of the YubiKey token programmed in one of these modes:

- Yubico OTP mode
- OATH-HOTP mode

Enabling the use of Microsoft Authenticator

You can allow users to authenticate via Defender by using one-time passwords generated with Microsoft Authenticator.

To enable Microsoft Authenticator for a user

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 nodes to select the container where the user object is located.
3. In the right pane, double-click the user object, and then click the **Defender** tab in the dialog box that opens.
4. Below the **Tokens** list, click the **Program** button.
5. In the Select Token Type step, click to select the **Software token** option. Click **Next**.
6. In the Select Software Token step, click to select the **Microsoft Authenticator** option.
7. Complete the wizard to enable Microsoft Authenticator for the user.
8. For more information about the wizard steps and options, see Defender Token Programming Wizard reference.

Enabling use of OneLogin Authenticator

You can get an activation code either from your system administrator or through a dedicated self-service Web site if it exists in your organization. The self-service Web site is called the Defender Self-Service Portal and it allows you to download and install software tokens, obtain activation code for software tokens, and register hardware tokens.

To enable OneLogin Authenticator for a user

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 nodes to select the container where the user object is located.
3. In the right pane, double-click the user object, and then click the **Defender** tab in the dialog box that opens.
4. Below the **Tokens** list, click the Program button.
5. In the Select Token Type step, click to select the **Software token** option.
6. Click **Next**.
7. In the Select Software Token step, click to select the **OneLogin Authenticator** option.
8. Complete the wizard to enable OneLogin Authenticator for the user.
9. For more information about the wizard steps and options, see Defender Token Programming Wizard reference.

4

Securing VPN access

Remote access is the ability to get access to a computer or a network from a distant location. Employees in branch offices, telecommuters, and people who are traveling may need access to your company's network. Remote access is achieved using a dedicated line between a computer or a remote local area network and the central or main corporate local area network.

You can use Defender to authenticate your employees, business partners, and customers, whether they are local, remote, or mobile. Whether they require access through VPN to remote access applications, wireless access points, network operating systems, intranets, extranets, Web servers, or applications, Defender’s strong two-factor authentication ensures that only authorized users are granted access.

The Defender remote access environment includes the following components:

- **Remote Access Server** A remote access server is the computer and associated software that is set up to handle users seeking remote access to your company’s network. The remote access server usually includes or is associated with a firewall server to ensure security and a router that can forward the remote access request to another part of the corporate network. A remote access server may also be used as part of a virtual private network (VPN).
- **Virtual Private Network (VPN)** A VPN is an extension of a private network that encompasses links across shared or public networks like the Internet. VPN connections leverage the IP connectivity of the Internet using a combination of tunneling and encryption to securely connect two remote points, such as a remote worker and their office base.
- **Network Access Server (NAS)** The Network Access Server (NAS) acts as a gateway to guard access to a protected resource. This can be anything from a telephone network, to printers, to the Internet. The user connects to the NAS. The NAS then connects to another resource asking whether the user's supplied credentials are valid. Based on that answer the NAS then allows or disallows access to the protected resource. The NAS contains no information about which users can connect or which credentials are valid. The NAS simply sends the credentials supplied by the user to a resource which does know how to process the credentials.
- **Defender EAP Agent** Extensible Authentication Protocol (EAP) is a general protocol for authentication that also supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, public key authentication and

smart cards. Defender utilizes the EAP protocol to integrate its two-factor authentication into the existing user authentication process.

In this chapter:

Configuring Defender for remote access

The configuration described in this section is an example only of a basic configuration using a Cisco ASA Server.

We assume that you have installed and configured the Defender Security Server that you will later define as the AAA Server.

To configure remote access, you need to perform the following additional tasks:

- Create and configure the Access Node that will handle access requests from remote users.
- Assign the Access Node to the Defender Security Server that will authenticate the remote users.
- Configure the Defender Security Policy that will determine the method and level of access, time period within which access is permitted, and lockout conditions for failed logon attempts.
- Assign the Defender Security Policy to the Access Node.
- Assign users or groups of users to the Access Node.
- Configure and assign security tokens to users.
- Configure the remote access device in your environment.

The Configuration example illustrates how to configure the Cisco Adaptive Security Device (ASDM) version 6.1 for use with Defender. The configuration procedure may vary depending on the remote access device you are using.

Configuration example

This configuration example shows how to configure the Cisco Adaptive Security Device (ASDM) version 6.1 for use with Defender and assumes that you are using an existing VPN profile. Only the configuration settings required to enable the remote access device to work with Defender are described in this procedure. Please leave the default settings for all other options.

Depending on the remote access device you are deploying, the configuration procedure for your own system may vary from this example.

Configuring your remote access device

To configure your remote access device, you need to complete these steps:

- Step 1: Create an AAA server group, add Defender Security Server
- Step 2: Configure an IPsec connection profile

Step 1: Create an AAA server group, add Defender Security Server

To create an AAA server group

1. Open the Cisco ADSM console, and then do the following:
    a. On the toolbar, click **Configuration**.
    b. In the left pane, click **Remote Access VPN**.
    c. In the left pane, expand the **AAA/Local Users** node to select the **AAA Server Groups** node.
    d. In the right pane, in the **AAA Server Groups** area, click the **Add** button.
2. In the dialog box that opens, do the following:
    a. In the **Server Group** text box, type a descriptive name for your group.
    b. From the **Protocol** drop-down list, select **RADIUS**.
    c. Click **OK** to create the group and close the dialog box.
3. In the right pane, in the **Servers in the Selected Group** area, click the **Add** button.
4. In the dialog box that opens, do the following:
    a. In the **Server Name or IP Address** text box, enter the name or IP address of the Defender Security Server you want to use to authenticate the users.
    b. In the **Server Authentication Port** text box, enter the port used by the Defender Security Server to receive authentication requests (port 1645 by default).
    c. In the **Server Secret Key** text box, enter the shared secret you want to use to establish a connection between the Defender Access Node and Defender Security Server.
    d. Click **OK** to add the Defender Security Server to the list and close the dialog box.

Step 2: Configure an IPsec connection profile

To configure an IPsec profile

1. In the Cisco ADSM console, do the following:
    a. On the toolbar, click **Configuration**.
    b. In the left pane, click **Remote Access VPN**.
    c. In the left pane, expand the **Network (Client) Access** node to select the **IPsec Connection Profiles** node.
2. In the right pane, under **Connection Profiles**, select an existing profile or add a new profile.
3. Modify the selected or created profile (click the **Edit** button): In the **User Authentication** area, from the **Server Group** drop-down list, select the AAA server group you created in Step 1: Create an AAA server group, add Defender Security Server.

Configuring Defender

To configure Defender, you need to complete these steps:

- Step 1: Configure an Access Node
- Step 2: Specify users or groups for the Access Node

Step 1: Configure an Access Node

To configure an Access Node

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 appropriate domain node, and then expand the **Defender** node
3. In the left pane, right-click **Access Nodes**, from the shortcut menu, select **New | Defender Access Node**.
    a. Complete the wizard to configure the Defender Access Node.
        - On the **Enter a name and description for this Access Node** page, type a descriptive name and description for the Access Node.
        - On the **Select the node type and user ID type for this Access Node** page, use the following options:

          Node Type From this list, select **Radius Agent**. This enables the RADIUS protocol for communications between Cisco ACS devices and

Defender. Note that the RADIUS protocol is transmitted over UDP and uses port 1645 or 1812.

User ID From this list, select the user ID type you want to use.

- On the **Enter the connection details for this Access Node** page, use the following options:

  IP Address or DNS Name Specify the Cisco AAA Server by entering its IP address or DNS name.

  Port Type the port number through which you want this Access Node to connect to the Defender Security Server. You must specify the same port as the one you entered in the **Server Authentication Port** text box in Step 1: Create an AAA server group, add Defender Security Server.

  Subnet Mask Keep the default subnet mask.

  Shared Secret Type the same shared secret you entered in the **Server Secret Key** text box in Step 1: Create an AAA server group, add Defender Security Server.

Step 2: Specify users or groups for the Access Node

In this step, you specify the users or groups who will use the configured Access Node to authenticate via Defender.

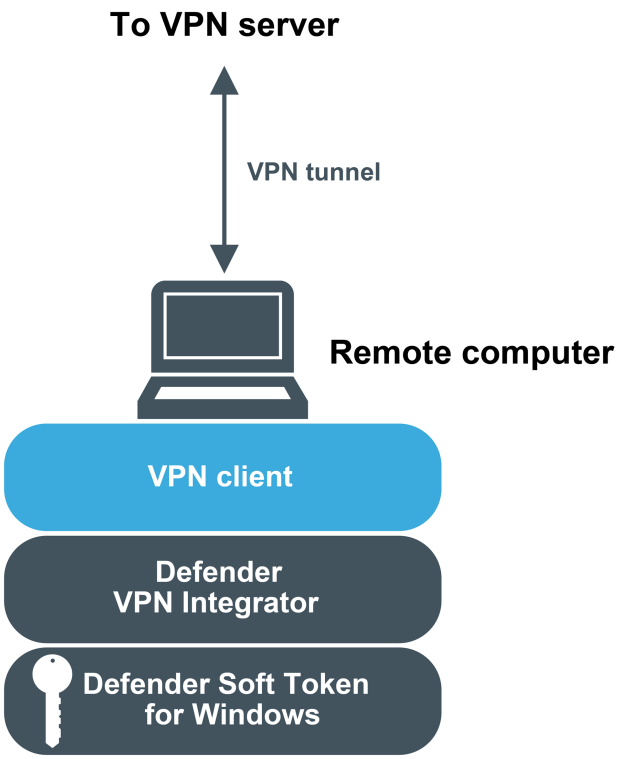
To specify users or groups for the Access Node

1. On the computer where the Defender Administration Console is installed, open the Active Directory Users and Computers tool (dsa.msc).
2. Open the properties of the Access Node you have configured:
   a. In the left pane, expand the domain node, expand the **Defender** node, and then click to select **Access Nodes**.
   b. In the right pane, double-click the Access Node.
3. In the dialog box that opens, use the **Members** tab to add the users or groups to the **Members** list.
4. When you are finished, click **OK**.

Using Defender VPN Integrator

Defender VPN Integrator is a tool that makes it very easy for remote users to utilize all the benefits of both VPN technology and the secure, two-factor authentication provided by Defender. Defender VPN Integrator simplifies the authentication process by integrating with the installed Defender Soft Token for Windows.

Defender VPN Integrator



The Defender VPN Integrator is installed and configured on the end-user's desktop, along with the Soft Token for Windows. When the user initiates a Defender protected VPN connection, VPN Integrator communicates between the Defender Soft Token for Windows and the third-party VPN client, to ensure that the secure, one-time password authentication process is handled automatically. The entire operation is seamless and very fast—only the passphrase for the Defender Soft Token for Windows is required from the user.

The guide describes how to install and configure Defender VPN Integrator within your environment.

Installing Defender VPN Integrator

To install Defender VPN Integrator

1. Run the **DefenderVPNIntegrator.exe** file supplied in the Defender distribution package.
2. Complete the wizard that starts to install the Defender VPN Integrator.

You may be prompted to restart your computer. When you complete the installation, Defender VPN Integrator runs as a service.

If an earlier version of Defender VPN Integrator is installed on your computer, you first need to uninstall the earlier version. Depending upon your version of the Windows operating system, use **Programs and Features** or **Add or Remove Programs** in Control Panel to uninstall the earlier version of Defender VPN Integrator. After uninstall, you may be prompted to restart your computer. When finished, run **DefenderVPNIntegrator.exe** to install the new version of Defender VPN Integrator.

Configuring Defender VPN Integrator

The Defender VPN Integrator does not include a configuration interface. For this reason, you have to make all configuration changes in the pgwc.ini configuration file which you can find in the following location:

%ProgramFiles%\One Identity\Defender\VPN Integrator

A number of sample .ini files are supplied with new installation. You will need to rename the .ini file suitable for your VPN Client to pgwc.ini. If you make any changes to the pgwc.ini file, log off from the computer and then log back on again for the changes to take effect.

You may need to modify the pgwc.ini file to work with your particular VPN client, for example, the Window title= line should include the title displayed on your VPN client window.

Defender EAP Agent

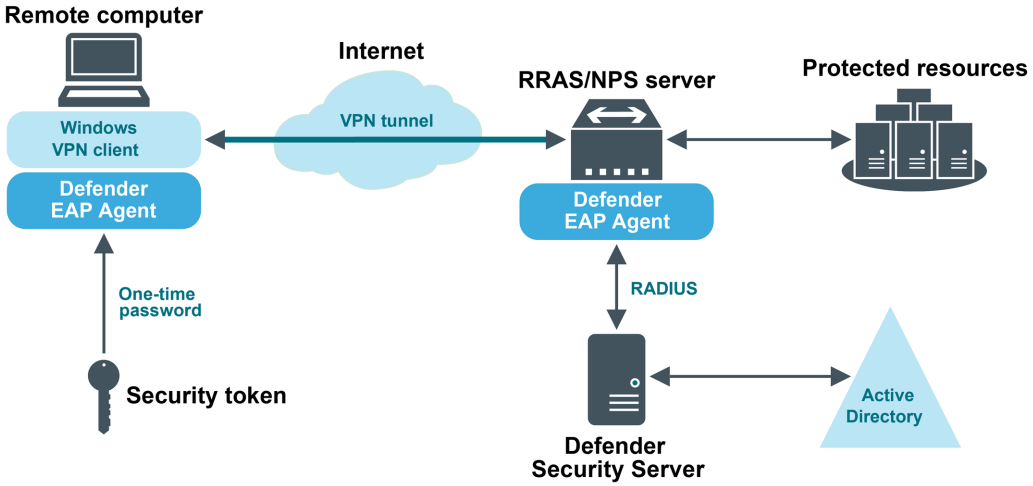
A VPN is an extension of a private network that encompasses links across shared or public networks like the Internet. VPN connections leverage the IP connectivity of the Internet using a combination of tunneling and encryption to securely connect two remote points, such as a remote worker and their office base.

Extensible Authentication Protocol (EAP) is a general protocol for authentication that also supports multiple authentication methods, such as Kerberos, token cards, one-time passwords, certificates, public key authentication, and smart cards.

Defender utilizes the EAP protocol to integrate its two-factor authentication into the existing user authentication process. The Defender EAP Agent supports Microsoft Remote Access clients and servers for both dial-up and VPN (PPTP and L2TP/IPSec) (implemented as an extension to PPP).

The Defender EAP Agent must be installed on the VPN server and VPN client computer.

Defender and VPN access via RRAS/NPS server



Deploying Defender EAP Agent

To benefit from using two-factor authentication over the EAP protocol, you need to install the Defender EAP Agent on the Network Policy Server and on the VPN client computer. Then, you need to configure the Network Policy Server and the VPN client computer for working with the Defender EAP Agent.

To deploy the Defender EAP Agent, complete the following steps:

- Step 1: Install Defender EAP Agent
- Step 2: Configure Network Policy Server
- Step 3: Configure VPN connection on the client computer

Step 1: Install Defender EAP Agent

You must install the Defender EAP Agent on the Network Policy Server, and on the VPN client computer.

To install Defender EAP Agent

1. Run the **DefenderEAPAgent.exe** file supplied with the Defender distribution package.
2. Complete the wizard that starts.

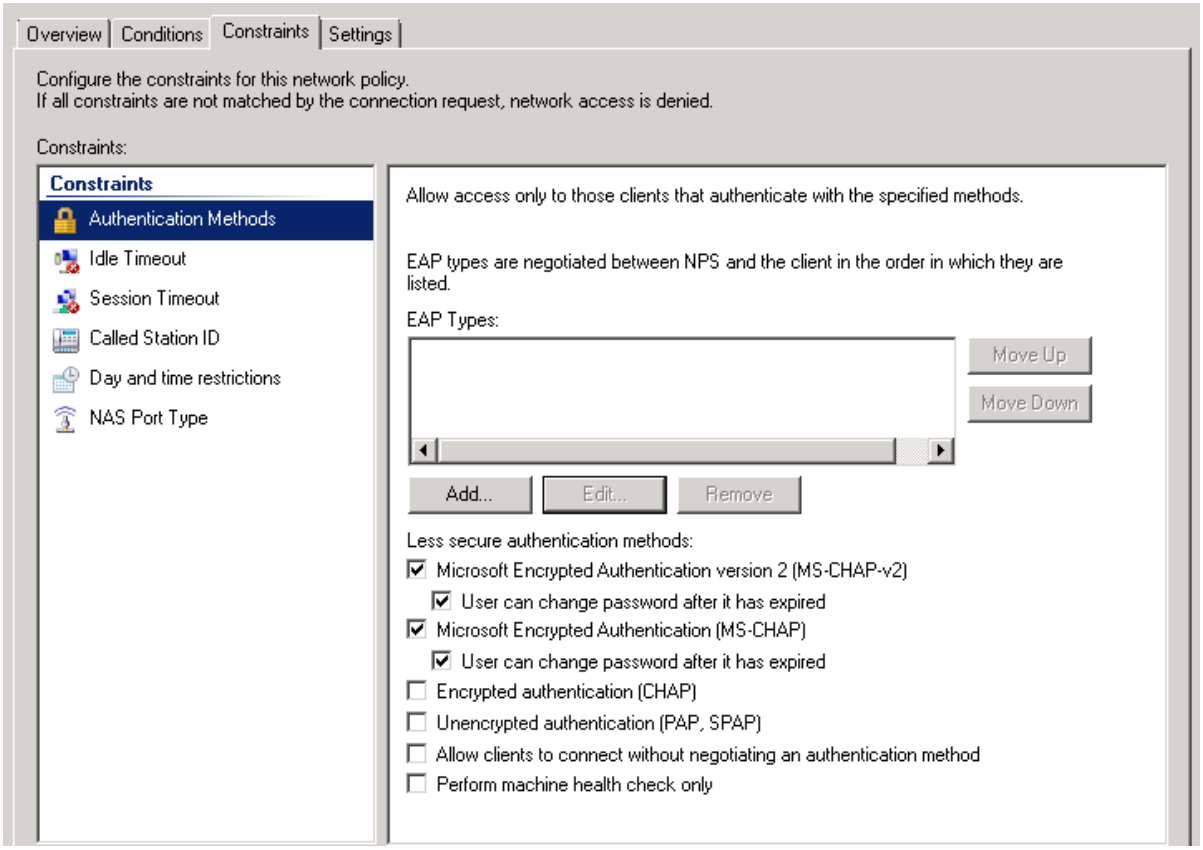
   IMPORTANT:

   - When installing Defender EAP Agent on the Network Policy Server, on the Installation Complete step of the wizard, clear the **Create a VPN connection with Defender now** check box, and then click **Finish**.
   - When installing Defender EAP Agent on the VPN client computer, on the Installation Complete step of the wizard, select the **Create a VPN connection with Defender now** check box, click **Finish**, and follow the wizard that starts to create a new VPN connection.
3. After completing the wizard, restart the computer on which you have just installed Defender EAP Agent.

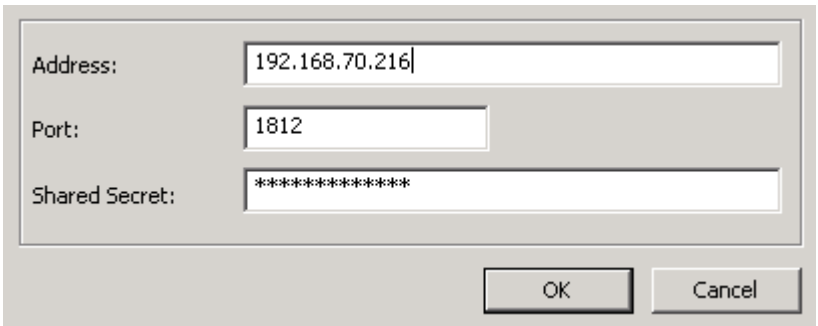
Step 2: Configure Network Policy Server

To configure the Network Policy Server

1. On the Network Policy Server, start the Network Policy Server tool (nps.msc).
2. In the left pane, expand the **Policies** node to select **Network Policies**.
3. In the right pane, right-click the network policy you want to use for Defender, and then on the shortcut menu click **Properties**.
4. In the dialog box that opens, click the **Constraints** tab.



5. Below the **EAP types** list, click the **Add** button.
6. In the dialog box that opens, select **Defender 5** from the list, and then click **OK**.
7. In the **EAP types** list, select the **Defender 5** entry you have just added, and then click the **Edit** button below the list. The following dialog box opens:



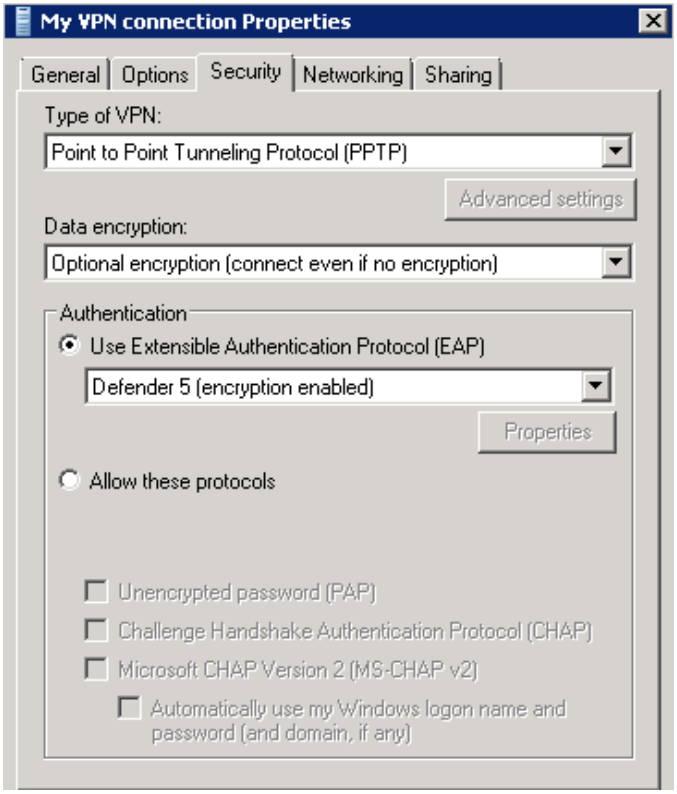
8. Use the following elements:
    - **Address** Type the IP address of the Defender Security Server you want to use for user authentication
    - **Port** Type the port used by the Access Node to which the specified Defender Security Server belongs.
    - **Shared Secret** Type the shared secret that corresponds to the Access Node.
9. Click **OK**.

Step 3: Configure VPN connection on the client computer

In this step, you need to configure the authentication settings of the VPN connection you created on the VPN client computer.

To configure VPN connection

1. Open the properties of the VPN connection you created on the VPN client computer in Step 1: Install Defender EAP Agent.
2. In the **Properties** dialog box, click the **Security** tab.
3. Make sure that in the **Authentication** area you select the **Use Extensible Authentication Protocol (EAP)** option, and then select **Defender 5 (encryption enabled)** from the list below the option:

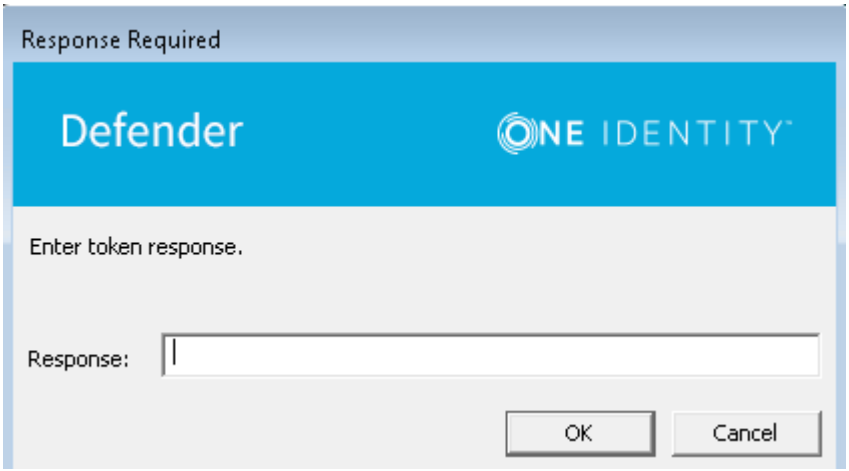


4. Click **OK** to close the dialog box.

   Now when you connect through the configured VPN connection on the client computer, a Defender dialog box opens prompting you to type the response provided by your token.

Authenticating via EAP Agent

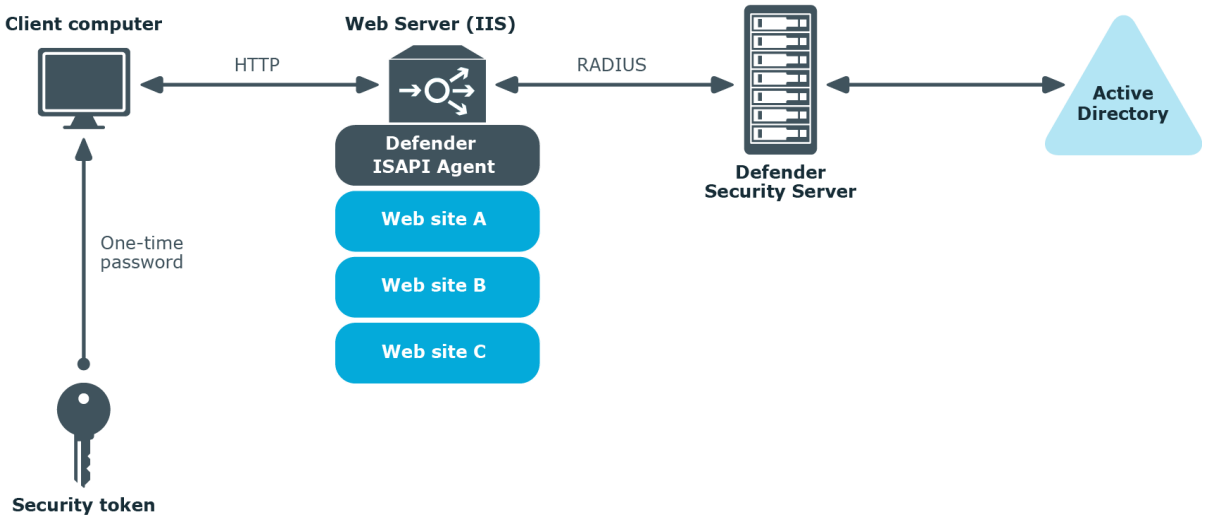
When you attempt to access information via your VPN, the Defender authentication dialog box is displayed:



In the **Response** field, type the response displayed on your token. Select **OK**. If authentication is successful, you are allowed to access the network.

Securing Web sites

You can use Defender to secure access to websites hosted on Microsoft Web Server (IIS). For that you need to use the Defender component called the *ISAPI Agent*.



The ISAPI Agent acts as an ISAPI filter and requires users to authenticate via Defender in order to get access to the websites hosted on IIS.

- Installing ISAPI Agent
- Configuring ISAPI Agent
- Accessing Protected Website

Installing ISAPI Agent

To install ISAPI Agent

1. Under a local administrator account, run the **DefenderISAPIAgent.exe** file supplied with the Defender distribution package.
2. Follow the steps in the wizard to complete the ISAPI Agent installation.
3. On the completion page of the wizard, select the **Start Defender ISAPI Agent Configuration tool** check box to configure the agent.

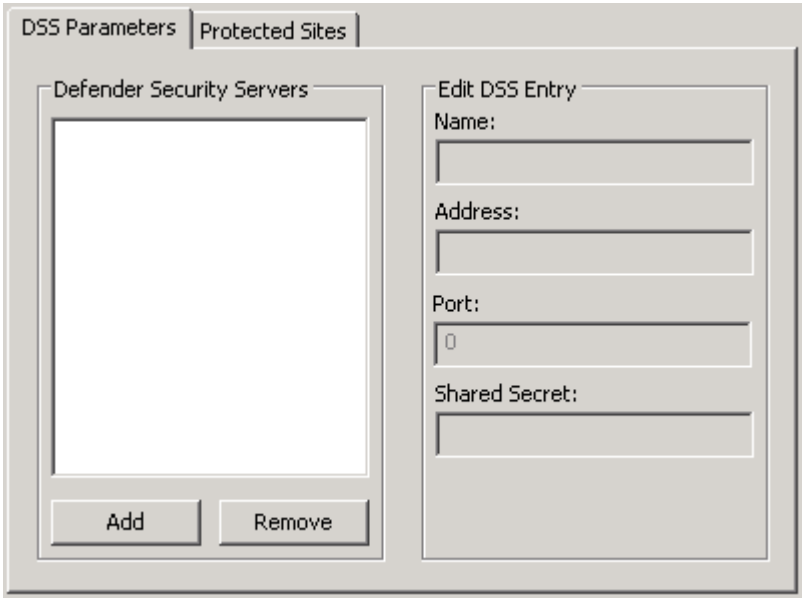
   For more information about available configuration settings, see Configuring ISAPI Agent.

Configuring ISAPI Agent

To configure ISAPI Agent

1. On the computer where the ISAPI Agent is installed, run the Defender ISAPI Agent Configuration tool.
2. In the dialog box that opens, specify the ISAPI Agent settings, and then click **OK**.

The dialog box looks similar to the following:



DSS Parameters tab

On this tab, specify the Defender Security Servers to which you want the ISAPI Agent to connect. You can use the following elements:

- **Defender Security Servers** Use this area to set up a list of the Defender Security Servers to which you want the ISAPI Agent to connect.
  - **Add** Adds a new entry to the list. After adding a new entry, edit its properties 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 ISAPI Agent 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 ISAPI Agent to use.
  - **Shared Secret** Type the shared secret configured on the access node you want the ISAPI Agent to use.

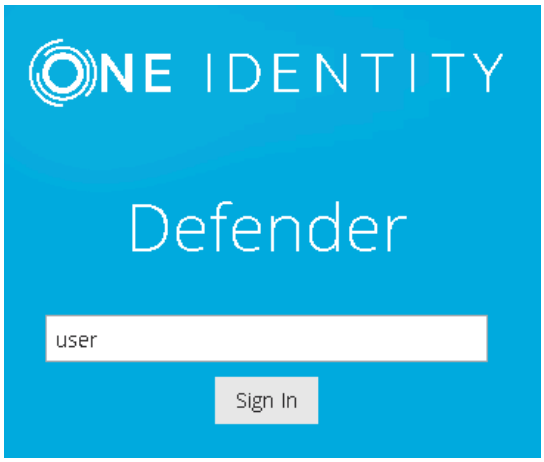
Protected Sites tab

On this tab, select the check boxes next to the websites you want to protect with Defender. By default, Defender protects the whole website. If you want to protect only some parts of the website, use the **default.acl** file located in the ISAPI Agent installation folder. This file contains two sections where you can list parts that should and should not be protected. When specifying the website's parts, use relative URLs.

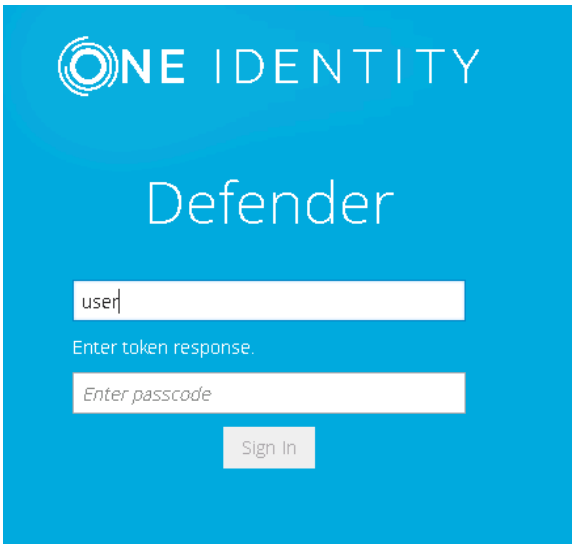
Accessing Protected Website

To access protected website

1. Using any supported browser, access the protected website. On the Login page, enter your user name and click **Sign in**.



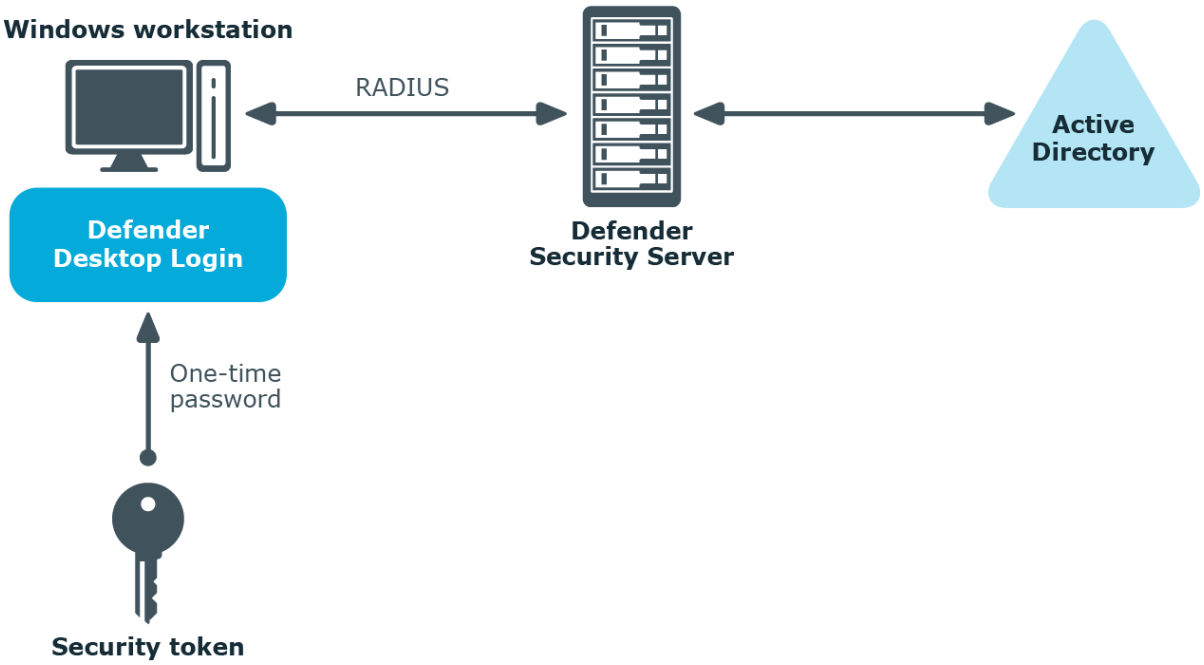
2. In the example below, users are required to authenticate themselves by entering their passcode. The authentication type depends on how the Defender policy has been configured. For example, if Defender is configured to use a token policy, the **Enter Synchronous Response** prompt will be displayed.



3. If users have entered a valid response, they will be authenticated and permitted to access the website.

Securing Windows-based computers

You can configure Defender to authenticate users when they sign in to their Windows-based computers in your organization.



To secure Windows-based computers, in addition to the required Defender components you need to install and configure the component called the *Defender Desktop Login* on each computer you want to secure with Defender. For more information about installing and configuring the required Defender components, see Deploying Defender.

- Installing Defender Desktop Login by using a wizard
- Performing an unattended installation of Defender Desktop Login
- Configuring Defender Desktop Login by using a configuration tool
- Configuring Defender Desktop Login by using Group Policy
- Defender Desktop Login Configuration tool reference

Installing Defender Desktop Login by using a wizard

You can use a wizard to install Defender Desktop Login on a local computer.

To install Defender Desktop Login

1. Run the **DefenderDesktopLogin.exe** file supplied in the Defender distribution package.
2. Complete the wizard to install Defender Desktop Login.

   IMPORTANT: You must configure Defender Desktop Login before restarting the computer. Otherwise, you may not be able to log on after the computer has been restarted.
   For instructions, see Configuring Defender Desktop Login by using a configuration tool and Configuring Defender Desktop Login by using Group Policy.

Performing an unattended installation of Defender Desktop Login

You can perform an unattended installation of Defender Desktop Login by using the following .msi files supplied in the Defender distribution package:

- **DefenderDesktopLogin_x86.msi** Installs Defender Desktop Login on 32-bit systems.
- **DefenderDesktopLogin_x64.msi** Installs Defender Desktop Login on 64-bit systems.

For example, you can use these files to silently install Defender Desktop Login from a command line or by using Group Policy. For instructions on how to install software by using Group Policy, refer to Microsoft's knowledge base article 816102.

When using .msi file to install Defender Desktop Login, you can use the following command-line parameters:

Table 13:
Defender MSI parameters

Parameter	Description	Example
DSS	Specifies a list of Defender Security Servers (by IP address or DNS name) and	• `DSS=10.0.0.1:1812` • `DSS=MyServer1:1812; MyServer2:1812`

Parameter	Description	Example
	ports for the Defender Desktop Login software to authenticate against. Each IP address or DNS name must have a port which is specified using a colon. For multiple entries, use a semicolon as shown in the example (without a space).	
SHARED_SECRET	Specifies the shared secret which is used to securely communicate and authenticate against the Defender Security Server.	`SHARED_ SECRET=MySharedSecretString`
EXCLUSION_MODE	Determines how Defender Desktop Login authenticates users. This parameter can take one of the following values: • **0** Specifies that all users must authenticate via Defender. • **1** Specifies that members of groups in the EXCLUSION_ GROUPS parameter are not required to authenticate via Defender. • **2** Specifies that only members of groups in the EXCLUSION_ GROUPS parameter must authenticate via Defender.	`EXCLUSION_MODE=0`
EXCLUSION_GROUPS	Specifies the groups whose members must or are not required to authenticate via Defender. Behavior of this parameter	`EXCLUSION_GROUPS= Administrators; DEFENDER\Domain Admins`

Parameter	Description	Example
	depends on the value set in the EXCLUSION_MODE parameter. To specify multiple groups in this parameter, use a semicolon as a separator.	
ALWAYS_ALLOW_LOCAL_LOGON	Specifies whether to allow local users to log on to a computer that has Defender Desktop Login installed without authenticating via Defender. This parameter can take one of the following values: • **0** Do not allow local users to bypass Defender authentication (default value) • **1** Always allow local users to bypass Defender authentication	`ALWAYS_ALLOW_LOCAL_LOGON=1`
ALLOW_OFFLINE_LOGON	Specifies whether users are allowed to log on if all Defender Security Servers are unavailable. This parameter can take one of the following values: • **0** Specifies that users cannot log on if all Defender Security Servers are unavailable. • **1** Specifies that users can only log on for a specified period of time from the moment when all Defender Security Servers become	`ALLOW_OFFLINE_LOGON=2`

Parameter	Description	Example
	unavailable. If you specify this value, use the OFFLINE_LOGON_DAYS to set the number of days you want. • **2** Specifies that users can only log on a specified number of times from the moment when all the Defender Security Servers become unavailable. If you specify this value, use the OFFLINE_LOGON_COUNT to set the number of times you want.	
OFFLINE_LOGON_DAYS	Specifies the period of time (in days) during which users can log on. This period is counted from the moment when all Defender Security Servers become unavailable. You can only use this parameter if you set the ALLOW_OFFLINE_LOGON parameter value to **1**.	`OFFLINE_LOGON_DAYS=12`
OFFLINE_LOGON_COUNT	Specifies the number of times user can log on from the moment when all Defender Security Servers become unavailable. You can only use this parameter if you set the ALLOW_OFFLINE_LOGON parameter value to **2**.	`OFFLINE_LOGON_COUNT=45`
DISPLAY_NOTIFICATIONS	Specifies whether to provide the user with information about the	`DISPLAY_NOTIFICATIONS=1`

Parameter	Description	Example
	remaining number of offline logons or the remaining number of days when the offline logon will be available. This parameter can take one of the following values: • **0** Specifies not to display any offline logon notifications. • **1** Specifies to display offline logon notifications.	
STORE_PASSWORDS	Specifies whether to store user's password, so that the user is not prompted to reenter the password during each two-factor login. This parameter can take one of the following values: • **0** Specifies not to store the user's password. • **1** Specifies to store the user's password.	`STORE_PASSWORDS=1`
MANAGE_PASSWORDS	Specifies whether Defender Desktop Login can change a user's password when the password has expired. This parameter can take one of the following values: **0** Specifies that Defender Desktop Login can change user's password. • **1** Specifies that Defender Desktop Login cannot change user's password.	`MANAGE_PASSWORDS=1`
WAIT_FOR_NETWORK	Specifies the time period (in	`WAIT_FOR_NETWORK=60`

Parameter	Description	Example
	seconds) during which Defender Desktop Login waits for the network to become available at startup. The default value is 60 seconds.	
BLOCK_CREDENTIAL_PROVIDERS	Specifies credential providers Defender Desktop Login should block. This parameter can take one of the following values: • **0** Specifies to allow all credential providers. • **1** Specifies to block all credential providers except Defender Credential Provider. • **2** Specifies to block Microsoft's credential providers.	`BLOCK_CREDENTIAL_PROVIDERS=0`

Configuring Defender Desktop Login by using a configuration tool

You can use the Defender Desktop Login configuration tool (GinaConfig.exe) to configure or check the configuration settings of Defender Desktop Login installed on a particular computer. You can find the GinaConfig.exe file in the Defender Desktop Login installation folder (by default, this is %ProgramFiles%\One Identity\Defender\Desktop Login).

To view and configure the Defender Desktop Login settings

1. On the computer where Defender Desktop Login installed, run the GinaConfig.exe file.
2. Use the dialog box that opens to view and configure the Defender Desktop Login settings.

   For more information about these settings, see Defender Desktop Login Configuration tool reference.
3. When finished, **OK** to apply your changes and close the dialog box.

To add a passcode field in Desktop

Improved value parameters for desktop login and inclusion of new GINA settings. Check/Uncheck the "Enable passcode field on logon" option to hide/show the passcode field.

Configuring Defender Desktop Login by using Group Policy

You can use Group Policy to configure and provide the required settings to the computers that are governed by Group Policy and have the Desktop Login Software installed.

To configure Group Policy settings

1. Run the **DefenderDesktopLoginGroupPolicy.exe** file supplied in the Defender distribution package.
2. Complete the wizard that starts to install the Defender Desktop Login Group Policy.
3. Open the Group Policy Management tool (gpmc.msc).
4. In the left pane of the tool, expand the appropriate domain node to locate the Default Domain Policy.
5. Right-click the Default Domain Policy, and then on the shortcut menu click **Edit**.
6. In the left pane of the window that opens, expand **Computer Configuration | Policies**, and then select Defender Desktop Login.
7. In the right-pane, double-click **Desktop Login Settings** and use the dialog box that opens to configure the Defender Desktop Login settings.

   For more information about these settings, see Defender Desktop Login Configuration tool reference.
8. When finished, **OK** to apply your changes and close the dialog box.

   You may want to run the gpupdate command to refresh Group Policy settings in the Active Directory domain. It is also advisable to check that your Group Policy settings have been applied as described in the next steps.

To check if your Group Policy settings have been applied

1. Open the Active Directory Users and Computers tool.
2. In the left pane, right-click the domain for which you have configured Group Policy settings, point to **All Tasks**, and then click **Resultant Set Of Policy (Planning)**.
3. In the wizard that starts, select the **Skip to the final page of this wizard without collecting additional data** check box, and then click **Next**.
4. In the Summary of Selections step, click **Next**.
5. In the completion step, click **Finish**.

6. In the left pane of the window that opens, expand **Computer Configuration** to select the **Defender Desktop Login** node.
7. In the right pane, double-click the **Desktop Login Settings** object to view the current Group Policy settings.

   Alternatively, you can also run these steps against a specific computer object or organizational unit to ensure they use the correct settings.

Defender Desktop Login Configuration tool reference

You can configure a number of settings for Defender Desktop Login. For more information on how to access these settings, see Configuring Defender Desktop Login by using a configuration tool and Configuring Defender Desktop Login by using Group Policy.

Table 14:
Configuration settings for Defender Desktop Login

Tab	Description
DSS	Set up a list of the Defender Security Servers you want Defender Desktop Login to use; specify the shared secret that has been configured on the Access Node to be used for authentication requests. You can use the following elements: • **Add** Adds a new Defender Security Server entry to the list. In the dialog box that opens, type the server IP address or DNS name and communication port. • **Edit** Allows you to edit the selected list entry. • **Remove** Removes the selected list entry. • **Up** Moves the selected list entry up. • **Down** Moves the selected list entry down. • If Defender Desktop Login is configured by using Group Policy, this tab also provides the **Group Policy Settings (read only)** list that shows the Defender Security Servers used by Defender Desktop Login.
Logon Settings	Configure which users or groups are required to authenticate via Defender. You can use the following elements:

Tab	Description
	• **Require domain users to log on using Defender.** Specifies that all domain users who log on to a computer that has Defender Desktop Login installed must authenticate via Defender. • **Allow specified users to bypass Defender authentication.** Specifies that users in groups added to the **Groups** list do not have to authenticate via Defender when logging on to computers that have Defender Desktop Login installed. • **Require specified users to log on using Defender.** Specifies that users in groups added to the **Groups** list must authenticate via Defender when logging on to computers that have Defender Desktop Login installed. If you want local users always to be able to log on to a computer that has Defender Desktop Login installed without authenticating via Defender, select the **Always allow local users to bypass Defender authentication** check box. If Defender Desktop Login is configured by using Group Policy, you can click the **Group Policy (read-only)** tab to view a list of groups whose users must or do not have to authenticate via Defender Desktop Login.
Offline	Configure how to handle users' logon attempts when all the Defender Security Servers installed in your environment are unavailable. • **Logins without the Defender Security Server are disabled** Users cannot log on if all the Defender Security Servers are unavailable. • **Users may login for a set number of days after the previous login against the Defender Security Server** Users can only log on for a specified number of days from the moment when all Defender Security Servers become unavailable. • **Users have a set number of logins after the previous login against the Defender Security Server** Users can only log on a specified number of times from the moment when all the Defender Security Servers become unavailable • **Notify user when offline data is downloaded** When this check box is selected, each time an offline

Tab	Description
	logon occurs, the user is provided with information about the remaining number of offline logons or the remaining number of days when the offline logon will be available.
Options	Configure additional settings for Defender Desktop Login. You can use the following options: • **Remember user's passwords** With this option selected users Active Directory (AD) passwords will be remembered and the user will not need to enter this during the logon process. Only Defender authentication is required. (The user will be prompted for the AD password on first use). • **Automatically change user's password as required** Causes Defender to automatically change user's password when it expires. • **Time to wait for workstation service to be ready (seconds)** • **Credential Provider Filter** Provides a filter that allows you to display only specific credentials providers.
Test Authentication	Allows you to test the Defender Desktop Login settings you have configured. Type the user name and passcode in the appropriate text boxes, use the **Log on to** list to select the domain to which you want to log on, and then click **Test**.

7

Defender Management Portal (Web interface)

Defender provides a Web interface that is called the Defender Management Portal. The portal implements role-based security, so that portal administrators can control who can do what on the portal.

Depending on the assigned portal role, portal users can configure Defender authentication settings, view authentication information and statistics, troubleshoot authentication issues, and view Defender reports. The Defender Management Portal also provides a configurable self-service where users can download and activate software tokens and register their hardware tokens without the need to contact a Defender administrator.

Installing the portal

To install the Defender Management Portal

1. In the Defender distribution package, open the Setup folder, and then run the **Defender.exe** file.
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.

   After installing the Defender Management Portal, you need to prepare it for first use by specifying a service account. For more information, see Specifying a service account for the portal on page 128.

To install the Defender Management Portal from the command line, use the following installation switches

Table 15: Defender Management Console Installation Switches

Switch	Description
/ADDLOCAL=Web	Installs Defender Web Interface component only
/SCHEMAINSTALL =0	Do not install the Defender Schema extensions.
/SCHEMAINSTALL =1	Install the Defender Schema extensions.
/CARINSTALL =0	Do not install Defender Control Access Rights.
/CARINSTALL =1	Install Defender Control Access Rights.
/OUINSTALL =0	Do not create the Defender organizational unit.
/OUINSTALL =1	Create the Defender organizational unit.
/PORTNUM=XXXX (Default 8080)	Set Port Number for Management Portal Web Interface
/ADMINGROUP=xxxx	Set Administrative Group

NOTE: This list doesn't include standard windows installer options (you can get them by running "**msiexec.exe /?**")

Opening the portal

We strongly recommend using HTTPS to access the Defender Management Portal. The secure hypertext transfer protocol (HTTPS) is a communications protocol designed to

transfer encrypted information between computers over the World Wide Web. For instructions on how to configure SSL in order to support HTTPS connections from client applications, see the article "Configuring Secure Sockets Layer in IIS 7" at http://technet.microsoft.com/en-us/library/cc771438%28WS.10%29.aspx.

To open the Defender Management Portal

1. In your Web browser, go to the following address:

   http(s)://<*portal computer*>:<*port*>

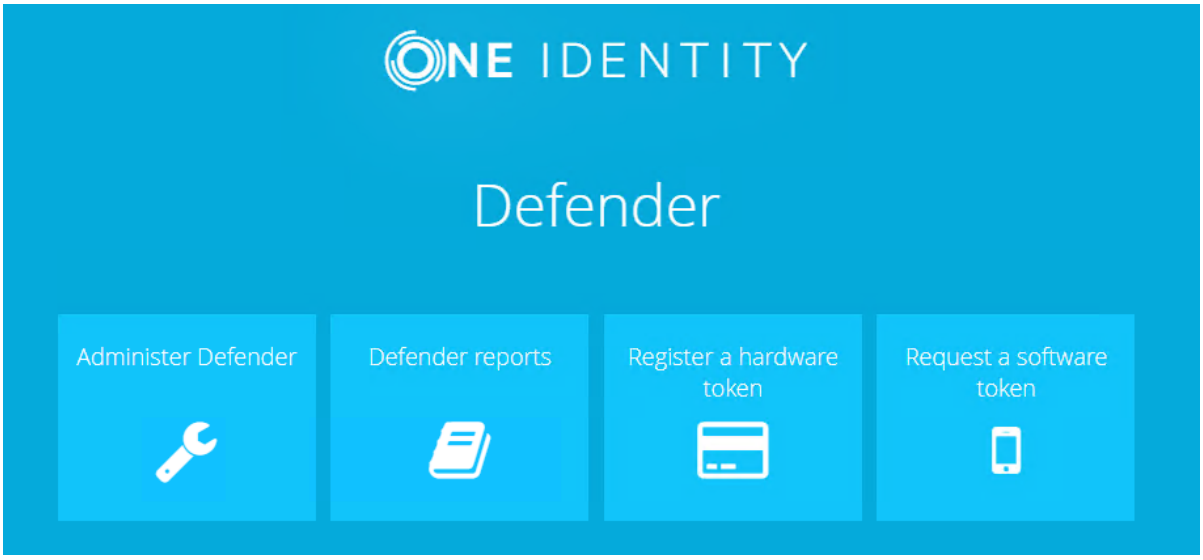
   where

   - <*portal computer*> is the fully qualified domain name of the computer on which the Defender Management Portal is installed.
   - <*port*> is the port number at which the Defender Management Portal can be accessed. You specify this port when installing the Defender Management Portal. The default port is 8080.
2. On the Defender Management Portal sign-in page, enter your user name, password, and domain, and then click **Sign in**.

   The Defender Management Portal home page opens.

The options available to you on the Defender Management Portal home page depend on the portal role assigned to the user account with which you sign in to the portal. For more information, see Portal roles on page 132.

When you sign in to the Defender Management Portal as a portal administrator, the home page provides all available options and looks as follows:



- **Administer Defender** Allows you to manage the Defender Management Portal configuration, configure self-service for users, manage users and security tokens,

diagnose and resolve authentication issues, view authentication statistics, and view information about the Defender Security Servers deployed in your environment.

- **Defender reports** Allows you to schedule, generate, and view Defender reports.
- **Register a hardware token** Starts a wizard that guides you through registering the hardware token given to you by your system administrator.
- **Request a software token** Starts a wizard that helps you to request, download, and activate a software token.

To return to the Defender Management Portal home page from any other page of the portal, in the upper right corner of your current portal page, click the **Home** button.

Specifying a service account for the portal

After installing the Defender Management Portal, you need to specify a service account for the portal. This account must be a member of the Local Administrators group on the computer where the Management Portal is installed and a member of the Domain Users group in the corresponding domain. By default, the Defender Management Portal uses the service account to do the following:

- Program and assign software tokens requested through the Defender Self-Service Portal.
- Retrieve data for Defender reports from Active Directory.

All other operations are performed under the account used to access the Defender Management Portal.

To specify a service account

1. Sign in to the Defender Management Portal as a portal administrator.

   For instructions, see Opening the portal.
2. On the Defender Management Portal home page, click **Administer Defender**:

3. In the left pane, click the **Configuration** tab.
4. In the right pane, click the **Service Account** tab.
5. Type the credentials of the user account you want to set as a service account for the portal.
6. When you are finished, click the **Save** button to save your changes.

   If the specified account does not have the "Log on locally" right, that right is granted to the account automatically after you click the **Save** button.

TIP: You can create a new dedicated user account and appoint that account as the Defender Management Portal service account. For more information, see Delegating Defender roles, tasks, and functions on page 172.

Configuring the portal

When configuring the Defender Management Portal, you can do the following:

- Specify the service account under which the Defender Management Portal will perform operations.
- Assign portal roles to the Active Directory groups of your choice.
- Manage the configuration of the Log Receiver Service.

  This service retrieves log files from the Defender Security Servers to the Defender Management Portal computer. The Defender Management Portal uses the retrieved log files to display authentication statistics and Defender Security Server warning messages and logs.
- Specify the location that holds the Defender Security Server log files.

  The Defender Management Portal uses the log files in the specified location to generate Defender reports.

To configure the Defender Management Portal

1. Sign in to the Defender Management Portal as a portal administrator.
2. For instructions, see Opening the portal.
3. Click the **Administer Defender** option.
4. In the left pane, click the **Configuration** tab.
5. In the right pane use the following tabs to configure the Defender Management Portal:

- **Service Account tab** Use this tab to specify the Defender Management Portal service account.
- **Roles tab** Use this tab to assign the Defender Management Portal roles to the Active Directory groups you want.

- **Log Receiver Service tab** Use this tab to manage the Defender Log Receiver service. This service retrieves log files from the Defender Security Servers to the Defender Management Portal computer.
- **Reports tab** Use this tab to specify folder for storing log files of the Defender Security Servers deployed in your environment.

Service Account tab

Use the **Service Account** tab to specify the Defender Management Portal service account. By default, the Defender Management Portal uses the service account to do the following:

- Program and assign the software tokens requested through the Defender Self-Service Portal.
- Retrieve Active Directory data for Defender reports.

The portal performs all other actions under the account with which the user signs in to the portal.

On the **Service Account** tab, you can use the following elements:

- **User name** Type the user name of the account you want to appoint as the Defender Management Portal service account. The account you specify must be a member of the local Administrators group on the computer where the Defender Management Portal is installed.
- **Password** Type the password that matches the user name you have typed in the **User name** text box.
- **Domain** Type the name of the Active Directory domain to which the user account belongs.
- **Use service account for all actions** Select this check box if you want the Defender Management Portal to perform all actions under the specified service account. If you select this check box, the Defender Management Portal stops providing any information about the actions that users perform through the portal.

If the account you specify does not have the "Log on locally" right, that right is granted to the account automatically after you click the **Save** button on this tab.

You can create a new dedicated user account and appoint it as the Defender Management Portal service account. For more information, see Delegating Defender roles, tasks, and functions on page 172.

Roles tab

Use the **Roles** tab to assign the Defender Management Portal roles to the Active Directory groups you want. A portal role defines the actions available to the role holder in the Defender Management Portal.

You can assign the following portal roles:

- Administrator
- Helpdesk
- Read-Only Helpdesk
- Reports

For more information, see Portal roles.

To assign a portal role, click the magnifying glass button next to the role, and then select the Active Directory group from the list.

In the domain where the Defender Management Portal is installed, the Domain Admins group always has the Administrator portal role assigned, regardless of what group you specify in the **Administrator** option on the **Roles** tab.

Log Receiver Service tab

Use the **Log Receiver Service** tab to manage the Defender Log Receiver service. This service retrieves log files from the Defender Security Servers to the Defender Management Portal computer. The Defender Management Portal uses the retrieved log files to display authentication statistics and Defender Security Server warning messages and logs.

On this tab, you can use the following elements:

- **Service status** Shows the current status of the Defender Log Receiver service.
- **Restart** Restarts the Defender Log Receiver service. This button is only available when the service is running.
- **Stop** Stops the Defender Log Receiver service. This button is only available when the service is running.
- **Start** Starts the Defender Log Receiver service. This button is only available when the service is stopped.
- **Communication port** Specifies the port on which the Defender Log Receiver Service connects to the Defender Security Servers. The default port is TCP 13131. The Defender Management Portal automatically creates a rule in Windows Firewall to allow traffic on port specified in this text box. The rule is automatically updated when you change the port number.
- **DSS log cache size limit (MB)** Specifies the maximum size of the Defender Security Server log cache (.dat) file that is located on each Defender Security Server. The default maximum file size is 1000 MB. When the specified maximum file size is reached, older contents in the .dat file are overwritten. For more information, see Defender Security Server log cache on page 163.
- **Log Receiver Service database size limit (MB)** Specifies the maximum size of each Log Receiver Service database (.sdf) file that stores log data from the corresponding Defender Security Server. A separate .sdf file is created on the Defender Management Portal computer for each Defender Security Server. The default maximum size set for each .sdf file is 1000 MB. For more information, see Log Receiver Service database.

Reports tab

Use the **Reports** tab to specify folder for storing log files of the Defender Security Servers deployed in your environment. These log files are used to generate Defender reports. Use the **DSS logs location** text box to type the local or UNC path to the log files.

Portal roles

A portal role defines the actions available to the role holder in the Defender Management Portal. You can assign the following portal roles to users:

- Administrator
- Helpdesk
- Read-Only Helpdesk
- Reports

The next table provides information about the actions that a particular role allows its holder to perform in the Defender Management Portal. For instructions on how to assign portal roles to users, see Configuring the portal.

Table 16:
Defender Management Portal roles

Action	Administrator	Helpdesk	Read-Only Helpdesk	Reports
View authentication statistics on the Dashboard	Yes	Yes	Yes	No
Configure Defender Management Portal	Yes	No	No	No
View Defender Security Server logs and warnings	Yes	Yes	Yes	No
View token requests from users	Yes	No	No	No
Configure self-service for users	Yes	No	No	No
Use Helpdesk to diagnose authentication	Yes	Yes	Yes	No

Action	Administrator	Helpdesk	Read-Only Helpdesk	Reports
issues				
Use Helpdesk to resolve authentication issues	Yes	Yes	No	No
Manage users	Yes	No	No	No
Manage security tokens	Yes	No	No	No
View Defender reports	Yes	No	No	Yes

Enabling automatic sign-in

By default, the Defender Management Portal is configured to use form-based authentication. As a result, the users need to supply their credentials to sign in to the portal. However, you can enable automatic sign-in for the portal users who are already logged on to the Active Directory domain where the Defender Management Portal is installed.

To enable the automatic sign-in, use IIS Manager to disable anonymous authentication in the Defender Management Portal Web site settings.

To enable automatic sign-in to the portal

1. On the Defender Management Portal computer, open IIS Manager.
2. In the left pane, expand the appropriate nodes to select the **Defender Web Interface** site.
3. In the right pane, under IIS, double-click **Authentication**.
4. Right-click the **Anonymous Authentication** option to select **Disabled**.

With anonymous authentication disabled, when users access the Defender Management Portal, they are automatically signed in with their Windows credentials. When an administrator accesses the Defender Management Portal, the user name and domain name are entered on the sign-in page automatically — only the password is required.

Configuring self-service for users

The Defender Management Portal provides a self-service Web site to users. This site is called the Defender Self-Service Portal. On the Defender Self-Service Portal, users can register their hardware tokens and request, download, and activate software tokens without the need to contact system administrator.

When you sign in to the Defender Management Portal as a portal administrator, you can configure all of the Defender Self-Service Portal settings. For example, you can set up a list of users who are allowed to request software tokens and register hardware tokens via the Defender Self-Service Portal, choose the tokens that users can request or register, select a method for verifying users who request or register tokens, select a method for delivering token activation information to the users, and more.

To configure self-service

1. Sign in to the Defender Management Portal as a portal administrator.

   For more information, see Opening the portal on page 126.
2. Click the **Administer Defender** option.
3. In the left pane, click the **Self-Service Settings** tab.
4. In the right pane, use the following tabs to configure the self-service settings:
   - **General tab** Allows you to set up a list of Active Directory groups whose members are allowed to request software tokens and register hardware tokens via the Defender Self-Service Portal. You can also use this tab to configure settings for storing token objects in Active Directory and view the URLs at which users can self-register their hardware tokens.
   - **Software Tokens tab** Allows you to configure settings for verifying the identity of users who request software tokens via the Defender Self-Service Portal. Only users who successfully confirm their identity can receive the requested token. Also you can configure settings for e-mailing software token activation information to the users.
   - **Hardware Tokens tab** Allows you to configure settings related to hardware tokens users register on the Defender Self-Service Portal.
   - **E-mail Settings tab** Allows you to configure settings for sending e-mail messages to the Defender Self-Service Portal users.
   - **PIN Settings tab** Allows you to configure PIN settings for the tokens requested or registered via the Defender Self-Service Portal.

General tab

Use the **Permissions** area to set up a list of Active Directory groups whose members are allowed to request software tokens and register hardware tokens on the Defender Self-Service Portal. For each group added to the list, you can select the security tokens the members of that group can request or register.

In the **Permissions** area, you can use the following elements:

- **Add Group** Allows you to add an Active Directory group to the list.
- **Remove Group** Removes the Active Directory groups selected in the list. After a group is removed from the list, its members can no longer request or register any security tokens on the Defender Self-Service Portal.

- **Edit permissions** Allows you to select the security tokens that the members of the corresponding Active Directory group can request or register via the Defender Self-Service Portal. This link is only available for the groups added to the list.

Use the **Token storage in Active Directory** area to configure settings for storing token objects in Active Directory.

In the **Token storage in Active Directory** area, you can use the following elements:

- **Create token objects in** Specify the Active Directory container in which you want the Defender Self-Service Portal to create token objects for the security tokens requested or registered by users.
- The default Active Directory container for storing token objects is Tokens. If you specify a different container, make sure the Defender Management Portal service account has sufficient rights on that container.
- **Requested token overwrites existing token** Causes the security token requested or registered via self-service to overwrite the security token of the same type already assigned to the user.

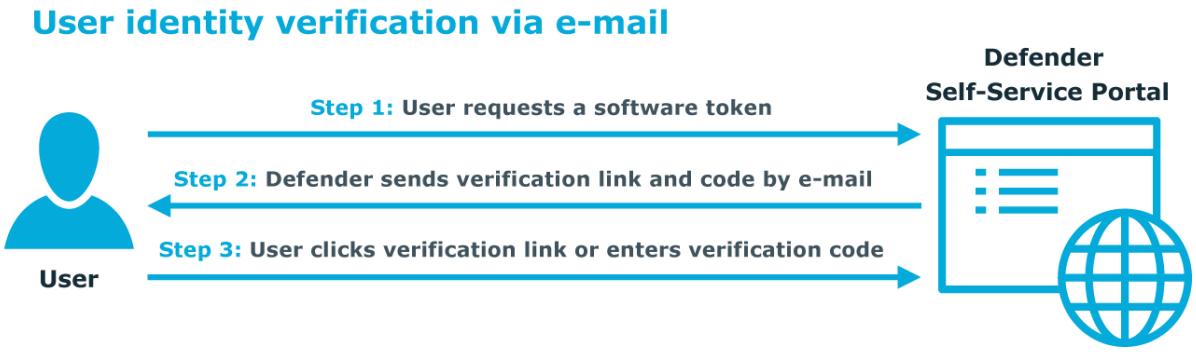
Use the **URLs for users** area to view the self-service URLs at which users can request software tokens and register hardware tokens. You can provide the URLs listed on this page to the users as necessary.

Software Tokens tab

In the **User verification settings** area, from the **Deliver verification code to users via** list, you can select a method for verifying the identity of users who request software tokens on the Defender Self-Service Portal.

Enabling user verification provides additional protection against unauthorized token requests and unsanctioned access to sensitive applications. With user verification enabled, in order to receive the requested software token, the users must verify their identity by entering a verification code provided by Defender. You can configure Defender to provide verification code to the users via an automated phone call, in an SMS message, or in an e-mail message.

The following diagram illustrates how user identity verification via e-mail works:



When a user requests a software token on the Defender Self-Service Portal, Defender sends an e-mail message to the user containing a verification code and link. To send the e-mail message, Defender uses the e-mail address specified for the user in the *mail* attribute in Active Directory.

To verify their identity and receive the requested software token, the user must either click the verification link in the e-mail message or enter verification code on the Defender Self-Service Portal.

The verification link and code provided in an e-mail message increase the security because they

- Are hard to guess.
- Expire after a certain configurable period of time.
- Can only be used once.

You can select one of the following verification methods:

- **E-mail** When this method is selected, after requesting a software token, the user receives an e-mail message containing a verification link (URL) and code. To verify their identity and receive the token, the user must either click the link in the message or manually enter the provided verification code on the Defender Self-Service Portal.

  The **E-mail message subject** text box allows you to view and modify the default subject of the e-mail messages containing the verification link and code.

  The **Verification code remains valid for (minutes)** text box allows you to view and change the default period during which the verification link and code remain valid.
- **Automated phone call or SMS (TeleSign)** When this method is selected, after requesting a software token, the user receives a verification code via an automated phone call or SMS message. To verify their identity and receive the token, the user must manually enter the provided verification code on the Defender Self-Service Portal.

  With this method, Defender uses the TeleSign service. If you select this method, make sure you have a valid account in TeleSign and type your TeleSign customer ID and the REST API Key in the corresponding text boxes. For further details about TeleSign, please go to www.telesign.com.

  From the **Use selected verification method** list, select how the user will receive the verification code. You can select to provide the verification code via an automated phone call, SMS message, or let the user choose one of these delivery methods.

  To make an automated phone call or send SMS, Defender can use telephone numbers specified for the user in the following Active Directory attributes: *telephoneNumber*, *homePhone*, *mobile*, *pager*, and *ipPhone*. The user will be prompted to select one of these telephone numbers on the Defender Self-Service Portal.
- **Disable user verification** When this method is selected, users do not have to verify their identity in order to receive the software token requested on the Defender Self-Service Portal.

In the **Token activation information delivery** area, configure e-mail settings to send activation information for software tokens requested via the Defender Self-Service Portal.

- You can use the following elements:
- **Users can specify delivery e-mail address** When this check box is selected, the users who request software tokens via self-service are prompted to specify a preferred e-mail address at which they want to receive the token activation information. When this check box is cleared, the users receive the token activation information at the e-mail address specified for them in Active Directory.
- **E-mail message subject** Allows you to view and edit the subject of e-mail messages containing activation information.

Hardware Tokens tab

In the **Default hardware token** list, select a hardware token that will be automatically selected for the users when they go to the universal token registration URL shown on the **General** tab.

E-mail Settings tab

Use the **E-mail Settings** tab to configure settings for sending e-mail messages to the Defender Self-Service Portal users.

In the **SMTP server settings** area, use the following options:

- **SMTP server** Type the name or IP address of the SMTP server you want to use for sending e-mail messages to the Defender Self-Service Portal users.
- **Port** Type the port number at which you want to connect to the SMTP server.
- **SMTP server requires authentication** Select this check box if the SMTP server requires authentication. Then, type the user name and password of the account with which you want to authenticate on the SMTP server.

In the **Sender details** area, use the following options:

- **From** Type the e-mail address you want to appear in the From field of the e-mail messages sent by the Defender Self-Service Portal.
- **Select how to address the user in e-mail messages** Select by which name you want to address the user in e-mail messages sent by the Defender Self-Service Portal.

PIN Settings tab

Use the **PIN Settings** tab to configure PIN settings for the tokens requested or registered via the Defender Self-Service Portal.

On this tab, you can use the following elements:

- **Require PIN for hardware tokens** Select this check box if you want all hardware tokens to require a PIN. When this check box is cleared, the hardware tokens do not require a PIN.
- **Require PIN for software tokens** Select this check box if you want all software tokens to require a PIN. When this check box is cleared, the software tokens do not require a PIN.
- **Minimum PIN length** Specify the minimum number of digits each PIN must contain.
- **Maximum PIN length** Specify the maximum number of digits each PIN can contain.

When you require users to enter a PIN set for a selected token, users should enter the PIN followed by the token response to access a resource protected by Defender. For example, if the PIN is 1234 and the response is 5678, users should enter 12345678 when prompted for authentication.

When users need to reset the PIN, they should enter the old and new PINs in the following format: <old PIN><new PIN><new PIN>. For example, if the old PIN is 1234 and the new PIN is 5678, users should enter the following: 123456785678.

Troubleshooting authentication issues

You can use the Defender Management Portal to troubleshoot authentication issues experienced by users in your Defender environment. You can search for a particular user, see if the user experiences any authentication issues, and resolve the authentication issues found.

To diagnose and resolve authentication issues, the user account with which you sign in to the Defender Management Portal must have an appropriate portal role assigned. For more information, see Portal roles on page 132.

To troubleshoot authentication issues

1. Sign in to the Defender Management Portal.

   For more information, see Opening the portal on page 126.
2. Click the **Administer Defender** option.
3. In the left pane, click the **Helpdesk** tab.

4. Use the right pane to search for the user for whom you want to troubleshoot authentication issues:
    a. In the **Search by user name** text box, type the complete user name or its part, and then click the **Search** button.
    b. If prompted, select the user from the search results.
5. Use the below-listed tabs to diagnose and resolve authentication issues for the user.

These tabs only appear after you select a user. On these tabs, the values that cause authentication issues are marked in red.

- **User Details tab** Provides a summary for the user account, including user's full name, sAMAccountName, and last successful authentication date and time.
- **Tokens tab** Provides information about the security tokens (if any) assigned to the user, including token type, token serial number, and whether the token requires a PIN. You can use this tab to manage tokens.
- **Authentication Routes tab** Displays the Defender Security Server, Access Node, and Defender Security Policy that apply to the user as configured in the Defender Administration Console.
- **Authentications tab** Lists the authentication attempts made by the user over a period of time. The columns in the table display the date, reason, Defender Security Server, Access Node, Defender Security Policy, and RADIUS payload related to the authentication attempt.

User Details tab

Provides a summary for the user account, including user's full name, sAMAccountName, and last successful authentication date and time.

If an authentication issue is detected, the corresponding value on this tab is displayed in red. This can occur if, for example, the violation count is incremented or the account is locked or disabled. If you can take an action to resolve the issue, this tab provides a link to perform the action.

Tokens tab

Provides information about the security tokens (if any) assigned to the user, including token type, token serial number, and whether the token requires a PIN.

To view details for a token, in the **Token** column, click the token name.

To manage a token, click the **Manage** link provided next to the token. Depending on the token type, the page that opens may provide some or all of the following tabs:

- **Test** Allows you to run a test operation that checks if the token generates a valid response.

- **PIN** Allows you to assign a new PIN to the token. This is required if the authentication issue is related to an incorrect or forgotten PIN. On the page that opens, type the new PIN in the **New PIN** and **Confirm PIN** text boxes.

  If you want the user to change the PIN after the user logs on for the first time, select the **User must change PIN at next authentication** check box.

  When you are finished, click **Set PIN** to save the changes.

  To remove the PIN from the token, click **Remove PIN**.
- **Reset** Causes the token to resynchronize with the Defender Security Server. This is required if the authentication issue is related to a time drift on the token or, for event-based tokens, a number of token responses being used without user authentication taking place.
- **Temporary Response** Allows you to assign a temporary response to the token. You may need to assign a temporary response if the token does not function properly or if the user has lost the token but still needs access to the protected resources.

  Use the **Expire temporary response in** list to select a validity period for the temporary response.

  You can select the **Response can be used multiple times** check box, so that the user could use the temporary response multiple times before the response expires.

  Click **Assign** to assign a temporary response using the specified parameters.

  To remove the temporary response from the token, click **Remove**.

Authentication Routes tab

Displays the Defender Security Server, Access Node, and Defender Security Policy that apply to the user as configured in the Defender Administration Console.

If the **Status** column displays **Invalid**, it indicates that the user cannot authenticate using that route.

The **Comment** column provides a short description of the reason for the route being invalid. You can click the link in the **Comment** column to view suggestions for resolving the issue.

Authentications tab

Lists the authentication attempts made by the user over a period of time. The columns in the table display the date, reason, Defender Security Server, Access Node, Defender Security Policy, and RADIUS payload related to the authentication attempt.

The **Reason** column may include, for example, Access Approved for a successful authentication attempt or a failure reason if the authentication attempt was unsuccessful.

For failed authentication attempts, you can click the link in the **Reason** column to view the failure reason and suggestions to resolve the issue.

Managing users

You can use the Defender Management Portal to manage users in your Defender environment. You can search for and select a particular user, and then do the following:

- View user's authentication details
- Manage security tokens for the user
- Manage Defender password for the user
- Manage PIN for the tokens assigned to the user

To manage users, the account with which you sign in to the Defender Management Portal must have the administrator role assigned. For more information, see Portal roles on page 132.

To manage a user

1. Sign in to the Defender Management Portal.

   For more information, see Opening the portal on page 126.
2. Click the **Administer Defender** option.
3. In the left pane, click the **Management** tab.
4. In the right pane, click the **Users** tab.
5. Search for and select the user you want to manage:
   a. In the **Search by user name** text box, type the complete user name or its part.
   b. Click the **Search** button and wait for your search to complete.
   c. If prompted, select the user from the search results.
6. Use the following areas to manage the user:
   - **Tokens assigned to <*user name*>** Provides a list of security tokens assigned to the user. You can use this area to view information about the assigned tokens, program new software tokens, assign existing token objects to the user, remove tokens from the user, and set a Defender password for the user. For more information about elements you can use in this area, see the table below this procedure.

   a. **Authentication details** Use this area to view information about the user account, such as the time of last authentication, violation count, and violation reset count. If necessary, you can reset the violation count for the user. You can also enable, view, and change user's Defender ID. The user can authenticate to Defender by using the enabled Defender ID.

Table 17:
Tokens assigned to <user name> area

Element	Description
Program Token	Allows you to program a new software token for the user.
Assign Token	Allows you to select and assign an existing token object to the user.
Set Defender Password	Allows you to configure a new Defender password for the user.
Unassign	Removes the tokens selected in the list from the user. Note that this does not delete the corresponding token objects from Active Directory.
Manage	Allows you to manage the corresponding token. Depending on the token type, the page that opens may provide some or all of the following tabs: • **Test** Allows you to run a test operation that checks if the token generates a valid response. • **PIN** Allows you to assign a new PIN to the token. This is required if the authentication issue is related to an incorrect or forgotten PIN. On the page that opens, type the new PIN in the **New PIN** and **Confirm PIN** text boxes. If you want the user to change the PIN after the user logs on for the first time, select the **User must change PIN at next authentication** check box. When you are finished, click **Set PIN** to save the changes. To remove the PIN from the token, click **Remove PIN**. • **Reset** Causes the token to resynchronize with the Defender Security Server. This is required if the authentication issue is related to a time drift on the token or, for event-based tokens, a number of token responses being used without user authentication taking place. • **Temporary Response** Allows you to assign a temporary response to the token. You may need to assign a temporary response if the token does not function properly or if the user has lost the token but still needs access to the protected resources. Use the **Expire temporary response in** list to select a validity period for the temporary response. You can select the **Response can be used multiple times** check box, so that the user could use the temporary response multiple times.

Element	Description
	Click **Assign** to assign a temporary response using the specified parameters. To remove the temporary response from the token, click **Remove**.
<token name>	Click the token name in the **Token** column to view token details. The page that opens provides such information as token type, encryption used by the token, response length and response type, token activation key, and current status of the token.

Managing security tokens

You can use the Defender Management Portal to manage security tokens in your Defender environment. You can search for a particular security token, and then do the following:

- View the token details
- Assign the token to users
- Remove the token from users
- Test or reset the token to ensure it works properly
- Configure a PIN for the token
- Configure a temporary response for the token

To manage security tokens, the account with which you sign in to the Defender Management Portal must have the administrator role assigned. For more information, see Portal roles on page 132.

To manage a security token

1. Sign in to the Defender Management Portal.

   For more information, see Opening the portal on page 126.
2. Click the **Administer Defender** option.
3. In the left pane, click the **Management** tab.
4. In the right pane, click the **Tokens** tab.
5. Search for and select the token you want to manage:
   a. In the **Search by token serial number** text box, type the complete token serial number or its part.
   b. Click the **Search** button and wait for your search to complete.
   c. If prompted, select the token from the search results.

6. Use the following areas to manage the token:
    - **Users who have token <*token number*> assigned** Use this area to assign or remove the token from its users, view the users to whom the token is assigned, test the token, reset the token to resolve authentication issues, configure a token PIN, or create a temporary response for the token user. For more information about the elements in this area, see the table below this procedure.
    - **Token details** Use this area to view information about the token. This area shows the token type, encryption used by the token, token response length, and token activation key.

Table 18:
Users who have token <token number> assigned area

Element	Description
Assign	Allows you to assign the token to a user. When you click this button, a new page opens where you can select the user.
Unassign	Removes the token from the users selected in the list. Note that this does not delete the token object from Active Directory.
Manage	Click this link to manage the token for the corresponding user. Depending on the token type, the page that opens may provide some or all of the following tabs: • **Test** Allows you to run a test operation that checks if the token generates a valid response. • **PIN** Allows you to assign a new PIN to the token. This is required if the authentication issue is related to an incorrect or forgotten PIN. On the page that opens, type a new PIN in the **New PIN** and **Confirm PIN** text boxes. If you want the user to change the PIN after the user logs on for the first time, select the **User must change PIN at next authentication** check box. If you want the user to change the PIN after the user logs on for the first time, select the **User must change PIN at next authentication** check box. When you are finished, click **Set PIN** to save the changes. To remove the PIN from the token, click **Remove PIN**. • **Reset** Causes the token to resynchronize with the Defender Security Server. This is required if the authentication issue is related to a time drift on the token or, for event-based tokens, a number of token responses being used without user authentication taking place.

Element	Description
	• **Temporary Response** Allows you to create a temporary response for the token user. You may need to create a temporary response if the token does not function properly or if the user has lost the token but still needs access to the protected resources. Use the **Expire temporary response in** list to select a validity period for the temporary response. You can select the **Response can be used multiple times** check box, so that the user could use the temporary response multiple times during the specified validity period. Click **Assign** to create and assign a temporary response using the specified parameters. To remove the temporary response, click **Remove**.

Viewing authentication statistics

The Defender Management Portal provides a Dashboard that shows authentication statistics in graphical format. The Dashboard provides information about the number of successful and failed authentication attempts the users have performed, shows warning messages generated by the Defender Security Servers deployed in your environment, and displays the status of the Log Receiver Service.

To view authentication statistics on the Dashboard, the account with which you sign in to the Defender Management Portal must have an appropriate portal role assigned. For more information, see Portal roles.

To view authentication statistics on the Dashboard

1. Sign in to the Defender Management Portal.

   For more information, see Opening the portal.
2. Click the **Administer Defender** option.
3. In the left pane, click the **Dashboard** tab.

   The **Dashboard** tab has the following elements:

   - **Log Receiver Service** Shows the current status of the Defender Log Receiver Service. If the Defender Log Receiver Service is not running, the data on the Dashboard is not updated. If your portal role permits, you can also stop, restart, or configure the service.
   - **Warnings from Defender Security Servers** Displays the most recent warning messages related to the Defender Security Servers in your environment. To view a complete list of warning messages, click **More**.

- **Authentication requests by DSS, last hour** Displays the number of authentication requests received during the last hour for each Defender Security Server running in your Defender environment. Move the cursor over each section of the pie chart to view the total number of authentication requests per Defender Security Server during the last hour and the percentage total.
- **Authentications per hour, last 24 hours** Displays the total number of successful and failed authentication requests received by all Defender Security Servers, per hour, in the last 24 hours.

Viewing Defender Security Server warnings and logs

You can use the Defender Management Portal to view warnings and logs generated by specific Defender Security Server deployed in your environment.

To view Defender Security Server warnings and logs, the account with which you sign in to the Defender Management Portal must have an appropriate portal role assigned. For more information, see Portal roles.

To view Defender Security Server warnings and logs

1. Sign in to the Defender Management Portal.

   For more information, see Opening the portal.
2. Click the **Administer Defender** option.
3. In the left pane, click the **Activity** tab
4. In the right pane, use the following tabs:
   - **DSS Warnings** Displays warning messages generated by the selected Defender Security Server. From the **Select Defender Security Server** list, select the server whose warnings you want to view.
   - **DSS Logs** Displays the Defender Security Server logs in near real-time. From the **Select Defender Security Server** list, select the server whose logs you want to view.

Viewing token requests from users

You can view a list of token requests submitted by users through the Defender Self-Service Portal. This list provides such information as the name of user who requested a token, requested token type, and whether the token has been issued to the user.

To view token requests, the account with which you sign in to the Defender Management Portal must have an appropriate portal role assigned. For more information, see Portal roles.

To view token requests

1. Sign in to the Defender Management Portal.

   For more information, see Opening the portal.
2. Click the **Administer Defender** option.
3. In the left pane, click the **Activity** tab.
4. In the right pane, click the **Token Requests** tab to open a list of token requests.

The list has the following columns:

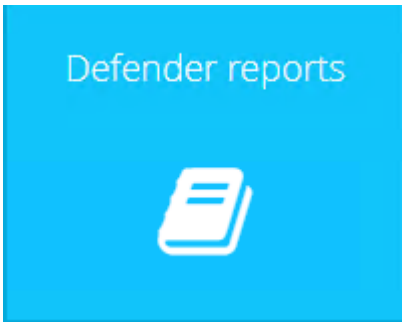
- **User** Shows the name of the user who requested a token through the Defender Self-Service Portal.
- **Token** Shows the type of requested token.
- **Request Type** Shows the method that was used to deliver the token. Possible methods include immediate token delivery with no user verification, verification via an automated phone call or SMS, verification via e-mail.
- **Request Date** Shows the date and time when the request was made or completed.
- **Request Completed** Shows whether the token request was completed.

Using Defender reports

On the Defender Management Portal, you can generate and view a number of reports providing information about the security tokens, authentication requests from users, configuration of Defender Security Servers, installed Defender licenses, RADIUS payloads assigned to users, and more. After generating a report, you can print it out or save it in HTML or XML format.

To use Defender reports, the user account with which you sign in to the Defender Management Portal must have an appropriate portal role assigned. For more information, see Portal roles.

You can start using reports by clicking the **Defender reports** option on the home page of the portal:



The page that opens provides the following tabs you can use to configure, schedule, generate, and view Defender reports:

Report Scheduler Allows you to select a report, configure its settings, and schedule the report for generation.

Scheduled Reports Provides a list of all reports you have scheduled so far. The items in the list are also called *scheduled report definitions*. You can use this node to view the details of scheduled reports, immediately generate scheduled reports without waiting for next generation time, or selectively delete the scheduled report definitions you no longer need. Deleting a scheduled report definition stops the generation of the corresponding report but does not delete already generated reports located on the **Generated Reports** tab.

Generated Reports Provides a list of reports generated from the corresponding report definitions on the **Scheduled Reports** tab. You can use this node to view the generated reports and selectively delete the generated reports you no longer need. Deleting a generated report does not affect the underlying scheduled report definition located on the **Scheduled Reports** tab.

See also:

- Generating a report
- Report scheduling settings
- Viewing a generated report
- Deleting generated reports
- Viewing a list of scheduled reports
- Deleting scheduled reports

Generating a report

To generate a Defender report, you need to configure its settings and schedule its generation. You can schedule a report to generate on a recurring basis or only once.

To use Defender reports, the user account with which you sign in to the Defender Management Portal must have an appropriate portal role assigned. For more information, see Portal roles.

To generate a report

1. Sign in to the Defender Management Portal.

   For more information, see Opening the portal.
2. Click the **Defender reports** option.
3. In the left pane, click the **Report Scheduler** tab.
4. In the right pane, from the **Select a report** list, select the report you want to schedule and generate.
5. In the **Report settings** area, configure settings for your report.

   For more information about available settings, click the report name below.

   - Audit trail
   - Authentication requests
   - Authentication activity
   - Authentication violations
   - Defender Security Server configuration
   - License information
   - Proxied users
   - RADIUS payloads
   - Tokens
   - Active, inactive, and locked users
   - User details
6. After configuring the report settings, click the **Schedule** button, and then type the report description and configure the generation schedule. For more information, see Report scheduling settings.
7. When you are finished with Report scheduling settings, click **Save**.

   After scheduling your report, you can click the **Preview** button to display the report you have just created.

Audit trail

The **Audit trail** report provides information about all user authentication requests processed by a specific Defender Security Server over a specified period of time.

Table 19:
Audit trail report settings

Setting	Description
Select a report type	Select the type of report you want to generate. Basically, this option allows you to specify the type of the Defender Security Server log files from which you want to collect data for your report. You can select one of the following: • **Audit report** This report is generated using the log files whose names have the DSSAudit prefix. • **Accounting Report** This report is generated using the log files whose names have the DSSAcct prefix.
Defender Security Server	Select the Defender Security Server whose data you want to use for generating the report.
Reporting period	Specify the time period for which you want to generate the report.
Select date and time formats	Select this check box to choose the format for displaying times and dates in the report. After selecting this check box, use the following options: • **Time format** Select the format for displaying times in the report. • **Date format** Select the format for displaying dates in the report. • **Time zone** Select the time zone for which you want to generate the report.

Authentication requests

The **Authentication requests** report provides a summary of authentication requests processed by a specific Defender Security Server, for either a single user or all users, over a specified period of time.

Table 20:
Authentication requests report settings

Setting	Description
Defender Security Server	Select the Defender Security Server whose data you want to use for generating the report.
Access Node	Select the Access Node for which you want to generate the report.
Include source address and Access Node	Select this check box to include the source address and Access Node details in the report. Otherwise, leave this check box cleared.
Include users whose name begins with	Type the initial characters of the user names for which you want to generate the report. Leave this text box blank to generate the report for all users.
Include users in Active Directory group	Type the complete name of the Active Directory group for which members you want to generate the report. Alternatively, click the magnifying glass icon to search for and select the Active Directory group. Leave this text box blank to generate the report for users in all groups.
Reporting period	Specify the time period for which you want to generate the report.
Select date and time formats	Select this check box to choose the format for displaying times and dates in the report. After selecting this check box, use the following options: • **Time format** Select the format for displaying times in the report. • **Date format** Select the format for displaying dates in the report. • **Time zone** Select the time zone for which you want to generate the report.

Authentication activity

The **Authentication activity** report provides the success and failure statistics for authentication requests processed by a specific Defender Security Server, over a specific period of time.

Table 21:
Authentication activity report settings

Setting	Description
Defender Security Server	Select the Defender Security Server whose data you want to use for generating the report.
Access Node	Select the Access Node for which you want to generate the report.
Reporting period	Specify the time period for which you want to generate the report.
Select date and time formats	Select this check box to choose the format for displaying times and dates in the report. After selecting this check box, use the following options: • **Time format** Select the format for displaying times in the report. • **Date format** Select the format for displaying dates in the report. • **Time zone** Select the time zone for which you want to generate the report.

Authentication violations

The **Authentication violations** report provides a summary for each authentication violation reported by a specific Defender Security Server over a period of time.

Table 22:
Authentication requests report settings

Setting	Description
Defender Security Server	Select the Defender Security Server whose data you want to use for generating the report.
Access Node	Select the Access Node for which you want to generate the report.
Include users whose name begins with	Type the initial characters of the user names for which you want to generate the report. Leave this text box blank to generate the report for all users.
Include users in Active Directory group	Type the complete name of the Active Directory group for which members you want to generate the report. Alternatively, click the magnifying glass icon to search for and select the Active Directory group. Leave this text box

Setting	Description
	blank to generate the report for users in all groups.
Reporting period	Specify the time period for which you want to generate the report.
Select date and time formats	Select this check box to choose the format for displaying times and dates in the report. After selecting this check box, use the following options: • **Time format** Select the format for displaying times in the report. • **Date format** Select the format for displaying dates in the report. • **Time zone** Select the time zone for which you want to generate the report.

Defender Security Server configuration

The **Defender Security Server configuration** report displays information about the configuration of the Defender Security Servers deployed in your environment.

Use the **Defender Security Server** list to select the Defender Security Server for which you want to generate the report.

License information

The **License information** report displays information about all currently installed Defender licenses. This report does not have any configurable settings.

Proxied users

The **Proxied users** report provides either a list of proxied users and their logon times or a filtered view of the Defender Security Server audit log, showing details of proxied packets.

Table 23:
Proxied users report settings

Setting	Description
Select a report type	Select the type of report you want to generate. You can select one of the following:

Setting	Description
	• **Proxied users** Provides a ist of proxied users and their logon times. • **Proxied packets** Provides a filtered view of the Defender Security Server audit log, showing details of proxied packets.
Defender Security Server	Select the Defender Security Server whose data you want to use for generating the report.
Include users whose name begins with	Type the initial characters of the user names for which you want to generate the report. Leave this text box blank to generate the report for all users.
Reporting period	Specify the time period for which you want to generate the report.
Select date and time formats	Select this check box to choose the format for displaying times and dates in the report. After selecting this check box, use the following options: • **Time format** Select the format for displaying times in the report. • **Date format** Select the format for displaying dates in the report. • **Time zone** Select the time zone for which you want to generate the report.

RADIUS payloads

The **RADIUS payloads** report provides information about the Defender users associated with a specific RADIUS payload.

Table 24:
RADIUS payloads report settings

Setting	Description
RADIUS payload	Select the RADIUS payload for which you want to generate the report.
Only include users who have a RADIUS payload explicitly assigned	Select this check box if you want the report to provide information only about the users who have the selected RADIUS payload directly assigned to their account.
Include users whose name begins with	Type the initial characters of the user names for which you want to generate the report. Leave this text box blank to

Setting	Description
	generate the report for all users.
Include users in Active Directory group	Type the complete name of the Active Directory group for which members you want to generate the report. Alternatively, click the magnifying glass icon to search for and select the Active Directory group. Leave this text box blank to generate the report for users in all groups.

Tokens

The **Tokens** report provides information about security tokens and their users.

Table 25:
Tokens report settings

Setting	Description
Select a report type	Select the type of report you want to generate.
Include specific tokens	Select this check box to select the security tokens for which you want to generate the report. Leave this check box cleared to generate the report for all tokens.

Active, inactive, and locked users

The **Active, inactive, and locked users** report provides information about the active, inactive, and/or locked out users in your Defender environment.

Table 26:
Active, inactive, and locked users report settings

Setting	Description
Select a report type	Select the type of report you want to generate.
Only include users who have a token assigned	Select this check box to display information only about the users who currently have a token assigned. When this check box is cleared, the report provides information about all users.
Include users whose name begins with	Type the initial characters of the user names for which you want to generate the report. Leave this text box blank to generate the report for all users.

Setting	Description
Include users in Active Directory group	Type the complete name of the Active Directory group for which members you want to generate the report. Alternatively, click the magnifying glass icon to search for and select the Active Directory group. Leave this text box blank to generate the report for users in all groups.
Reporting period	Specify the time period for which you want to generate the report.
Select date and time formats	Select this check box to choose the format for displaying times and dates in the report. After selecting this check box, use the following options: • **Time format** Select the format for displaying times in the report. • **Date format** Select the format for displaying dates in the report. • **Time zone** Select the time zone for which you want to generate the report.

User details

The **User details** report provides information about the users who authenticated via Defender.

Table 27:
User details report settings

Setting	Description
Include users whose name begins with	Type the initial characters of the user names for which you want to generate the report. Leave this text box blank to generate the report for all users.
Include users in Active Directory group	Type the complete name of the Active Directory group for which members you want to generate the report. Alternatively, click the magnifying glass icon to search for and select the Active Directory group. Leave this text box blank to generate the report for users in all groups.
Only include users who have a token assigned	Select this check box to display information only about the users who currently have a token assigned. When this check box is cleared, the report provides information about all users.
Select additional information to	Select the check boxes next to the items information about

Setting	Description
include in the report	which you want to include in the report.
Reporting period	Specify the time period for which you want to generate the report.
Defender Security Server	Select the Defender Security Server whose data you want to use for generating the report.
Access Node	Select the Access Node for which you want to generate the report.

Report scheduling settings

You can schedule any Defender report to be generated automatically on a recurring basis at the day and time you want, that is, daily, weekly, or monthly. Also you can schedule a report to be generated only once.

Table 28:
Report scheduling settings

Setting	Description
Report description	Type a description for the report you are scheduling.
Recurrence	Select how frequently you want to generate the report. You can select one for the following: • **Daily** Specify the time (**Start time**) and days when you want to trigger the report generation. You can select to generate the report every day, every weekday (from Monday to Friday), or every specified number of days. • **Weekly** Specify the time (**Start time**) and how often you want to trigger the report generation. You can also select the days of week when you want to generate the report. • **Monthly** Specify the time (**Start time**) and the day of month when you want to trigger the report generation. You can also select the months when you want to generate the report. • **One time only** Allows you to generate the report one time only. Specify if you want to generate the report immediately or at specific time and date.

Viewing a generated report

You can open a list of all generated reports to select and view a specific generated report.

To use Defender reports, the user account with which you sign in to the Defender Management Portal must have an appropriate portal role assigned. For more information, see Portal roles on page 132.

To view a generated report

1. Sign in to the Defender Management Portal.

   For more information, see Opening the portal on page 126.
2. Click the **Defender reports** option.
3. In the left pane of the page that opens, click the **Generated reports** tab.

   The right pane displays a list of all generated reports.
4. Click **View** next to the report you want to view.

Deleting generated reports

You can selectively delete the generated reports you no longer need.

To use Defender reports, the user account with which you sign in to the Defender Management Portal must have an appropriate portal role assigned. For more information, see Portal roles.

To selectively delete generated reports

1. Sign in to the Defender Management Portal.

   For more information, see Opening the portal.
2. Click the **Defender reports** option.
3. In the left pane of the page that opens, click the **Generated reports** tab.

   The right pane displays a list of all generated reports.
4. In the list, select the check boxes next to the generated reports you want to delete.
5. Click **Delete**.

   When you delete generated reports on the **Generated Reports** tab, it does not affect scheduled reports located on the **Scheduled Reports** tab. For more information on how to delete scheduled reports, see Deleting scheduled reports.

Viewing a list of scheduled reports

You can view a list of all reports scheduled for generation. The list provides details for each scheduled report, such as report name, description, recurrence, and time of next run. Optionally, you can immediately generate any scheduled report in the list without waiting for its next generation time.

To use Defender reports, the user account with which you sign in to the Defender Management Portal must have an appropriate portal role assigned. For more information, see Portal roles on page 132.

To view a list of scheduled reports

1. Sign in to the Defender Management Portal.

   For more information, see Opening the portal on page 126.
2. Click the **Defender reports** option.
3. In the left pane of the page that opens, click the **Scheduled reports** tab.

   The right pane displays a list of all scheduled reports.

   To immediately generate a report, click **Run Now** next to that report.

Deleting scheduled reports

You can selectively delete the scheduled reports you no longer need.

To use Defender reports, the user account with which you sign in to the Defender Management Portal must have an appropriate portal role assigned. For more information, see Opening the portal.

To selectively delete generated reports

1. Sign in to the Defender Management Portal.

   For more information, see Opening the portal.
2. Click the **Defender reports** option.
3. In the left pane of the page that opens, click the **Scheduled reports** tab.

   The right pane displays a list of all reports scheduled for generation
4. In the list, select the check boxes next to the reports you want to delete.
5. Click **Delete**.

Managing portal database

The Defender Management Portal database is stored in a file named SelfReg.sdf, held in the folder "%ProgramFiles%\One Identity\Defender\Management Portal\WWW\App_Data" on the computer running the Defender Management Portal. This section covers the following database management tasks:

- Encrypting database
- Changing password for encrypted database
- Decrypting database

Encrypting database

By default, the Defender Management Portal database is not encrypted. However, as this database contains a service account password used by the Defender Management Portal, you may want to encrypt the database.

To encrypt the database

1. In IIS Manager, stop the Defender Web Interface site.
2. On the Defender Management Portal computer, run **DBEncrypt.exe** located in the folder %ProgramFiles%\One Identity\Defender\Management Portal\Tools, and complete the dialog box that appears:
    a. Select the **Encrypt Database** check box.
    b. In the **New Password** and **Confirm New Password** boxes, type the password with which you want to encrypt the database.
    c. Click **Apply**, and then close the dialog box.
3. In the Web.config file, update the database connection string with the new password:
    a. In a text editor, open the Web.config file located in the folder %ProgramFiles%\One Identity\Defender\Management Portal\WWW
    b. In the Web.config file, locate the <connectionStrings> element, and modify the SelfReg.sdf connection string within that element to include the new password. Example:

    ```
    connectionString="data source=|DataDirectory|\SelfReg.sdf;Max Database Size=4091;password=NewDatabasePassword"
    ```

    where `NewDatabasePassword` is the password you have set in Step 2 of this procedure.
    c. Save and close the Web.config file.
4. Use the aspnet_regiis.exe tool to encrypt the database connection string in the Web.config file, so that the password is not displayed as plain text. You can find aspnet_regiis.exe in one of these folders:

- On an x86 system - %WinDir%\Microsoft.NET\Framework\v4.0.30319
- On an x64 system - %WinDir%\Microsoft.NET\Framework64\v4.0.30319

Sample command to encrypt the database connection string on an x86 system:

```
%WinDir%\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe -pef
"connectionStrings" "%ProgramFiles%\One Identity\Defender\Management Portal\WWW"
-prov "DataProtectionConfigurationProvider"
```

5. In IIS Manager, start the Defender Web Interface site.

Changing password for encrypted database

To change the password

1. In IIS Manager, stop the Defender Web Interface site.
2. On the Defender Management Portal computer, run **DBEncrypt.exe** located in the folder %ProgramFiles%\One Identity\Defender\Management Portal\Tools, and complete the dialog box that appears:
   a. In the **Old Password** box, type the password with which the database was encrypted.
   b. In the **New Password** and **Confirm New Password** boxes, type the new password with which you want to encrypt the database.
   c. Click **Apply**, and then close the dialog box.
3. Use the aspnet_regiis.exe tool to decrypt the database connection string in the Web.config file, so that you can specify the new password in that file. You can find aspnet_regiis.exe in one of these folders:
   - On an x86 system - %WinDir%\Microsoft.NET\Framework\v4.0.30319
   - On an x64 system - %WinDir%\Microsoft.NET\Framework64\v4.0.30319

   Sample command to decrypt the database connection string in the Web.config file on an x86 system:

   ```
   %WinDir%\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe -pdf
   "connectionStrings" "%ProgramFiles%\One Identity\Defender\Management Portal\WWW"
   ```

4. In the Web.config file, update the database connection string with the new password:
   a. In a text editor, open the Web.config file located in the folder %ProgramFiles%\One Identity\Defender\Management Portal\WWW
   b. In the Web.config file, locate the <connectionStrings> element, and modify the SelfReg.sdf connection string within that element to include the new password. Example:

   ```
   connectionString="data source=|DataDirectory|\SelfReg.sdf;Max Database
   Size=4091;password=NewDatabasePassword"
   ```

where `NewDatabasePassword` is the password you have set in Step 2 of this procedure.

c. Save and close the Web.config file.

5. Use the aspnet_regiis.exe tool to encrypt the database connection string in the Web.config file, so that the password is not displayed as plain text. You can find aspnet_regiis.exe in one of these folders:
   - On an x86 system - %WinDir%\Microsoft.NET\Framework\v4.0.30319
   - On an x64 system - %WinDir%\Microsoft.NET\Framework64\v4.0.30319

   Sample command to encrypt the database connection string on an x86 system:

   ```
   %WinDir%\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe -pef
   "connectionStrings" "%ProgramFiles%\One Identity\Defender\Management Portal\WWW"
   -prov "DataProtectionConfigurationProvider"
   ```

6. In IIS Manager, start the Defender Web Interface site.

Decrypting database

To decrypt the database

1. On the Defender Management Portal computer, run **DBEncrypt.exe** located in the folder %ProgramFiles%\One Identity\Defender\Management Portal\Tools, and complete the dialog box that appears:
   a. Clear the **Encrypt Database** check box.
   b. In the **Old Password** box, type the password with which the database was encrypted.
   c. Click **Apply**, and then close the dialog box.
2. Use the aspnet_regiis.exe tool to decrypt the database connection string in the Web.config file. You can find aspnet_regiis.exe in one of these folders:
   - On an x86 system - %WinDir%\Microsoft.NET\Framework\v4.0.30319
   - On an x64 system - %WinDir%\Microsoft.NET\Framework64\v4.0.30319

   Sample command to decrypt the database connection string in the Web.config file on an x86 system:

   ```
   %WinDir%\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe -pdf
   "connectionStrings" "%ProgramFiles%\One Identity\Defender\Management Portal\WWW"
   ```

3. In the Web.config file, update the database connection string to remove the password:
   a. In a text editor, open the Web.config file located in the folder %ProgramFiles%\One Identity\Defender\Management Portal\WWW
   b. In the Web.config file, locate the <connectionStrings> element, and modify the SelfReg.sdf connection string within that element to remove the password. Example:

```
connectionString="data source=|DataDirectory|\SelfReg.sdf;Max Database
Size=4091"
```

c. Save and close the Web.config file.

Defender Security Server log cache

Each Defender Security Server generates logs, which are retrieved by the Log Receiver Service running on the Defender Management Portal computer. The retrieved logs are then used to do the following:

- Display authentication statistics on the **Dashboard** tab of the Defender Management Portal.
- Provide troubleshooting information on the **Helpdesk** tab of the Defender Management Portal.
- Display information on the **Actions** tab of the Defender Management Portal.

Defender Security Servers deployed in your environment automatically detect the Log Receiver Service and provide their logs to the service.

In situations where the connection between the Defender Security Server and the Log Receiver Service is interrupted, the logs to be sent to the service are cached in a .dat file on the Defender Security Server. After the connection is restored, the log data cached in the .dat file is sent to the Log Receiver Service.

If the Log Receiver Service is running and the connection between this service and the Defender Security Server is working properly, the .dat file should not grow in size.

On a Defender Security Server, you can find the .dat file in the following folder:

%ProgramFiles%\One Identity\Defender\Security Server\Logs

The name of the .dat file has the following format:

<*ServerName*>.LogQueue.dat

Where <*ServerName*> is the name of the computer on which the Defender Management Portal is installed.

Log Receiver Service database

The Log Receiver Service uses .sdf files to store logs received from Defender Security Servers. For each Defender Security Server, the Log Receiver Service creates a separate .sdf file.

These .sdf files are called the Log Receiver Service database and contain data used by the Defender Management Portal to display authentication log-related data, including the authentication statistics provided on the **Dashboard** tab of the portal.

On the Defender Management Portal computer, you can find these .sdf files in the following folder:

%ProgramFiles%\One Identity\Defender\Management Portal\WWW\App_Data

The name of each .sdf file has the following format: <*DSS name*>.<*domain*>.sdf

where

- <*DSS name*> is the name of the corresponding Defender Security Server.
- <*domain*> is the name of the Active Directory domain where the corresponding Defender Security Server resides.

8

Securing PAM-enabled services

The Defender Pluggable Authentication Module (PAM) is a UNIX/Linux module that authenticates the users of PAM-enabled services (such as ftp, sshd, and su) via Defender. To authenticate users, the Defender PAM module uses the RADIUS protocol and the Defender Security Servers deployed in your environment.

Installing Defender PAM

To install the Defender PAM on your UNIX or Linux system, use the appropriate platform-specific files such as .rpm, .pkg, .deb, .depot, or .bff supplied with Defender. In the Defender distribution package, you can find these files in the Setup\Unix PAM folder.

For example, on a Linux x86_64 system, use the Linux RPM program to install the pamdefender-<version>.x86_64.rpm package. In addition to installing the Defender PAM, the package installs PAM Defender configuration scripts into the /opt/quest/libexec/defender directory.

Because all Defender token information is associated with user objects in Active Directory, an Active Directory user must be given a UNIX identity on the local system before the Defender PAM can validate any security tokens for the user. You can create a UNIX identity for an Active Directory user manually or by using a Name Service Switch (NSS) module that provides UNIX identity information directly from Active Directory.

To manually create a UNIX identity for an Active Directory user, modify the /etc/passwd file so there exists a user who has a local user name that exactly matches the value stored in the user ID attribute of your Active Directory user. The user ID attribute is configurable when you create an Access Node. Usually, it is samAccountName, defender ID, or userPrincipalName.

Alternatively, you can use the Defender PAM in conjunction with the NSS module supplied with the product. With this method, Authentication Services provide UNIX identity information to any UNIX-enabled Active Directory user. To use Authentication Services for getting UNIX identity information for Active Directory users, use the **vastool join** command to join your UNIX/Linux computer to the Active Directory domain. For more information, see the **vastool** man page.

Configuring Defender PAM

After installing the PAM Defender package on your UNIX or Linux system, you need to complete the following steps to enable Defender authentication for the users of PAM-enabled services:

- Step 1: Enable authentication for target service
- Step 2: Specify Defender Security Servers
- Step 3: Configure access control for users and services
- Step 4: Configure Defender objects in Active Directory

You can considerably simplify these steps by using Authentication Services and Group Policy. To find out more about Authentication Services, please visit https://www.oneidentity.com/products/authentication-services/.

Step 1: Enable authentication for target service

You can enable Defender authentication for a PAM-enabled service by adding the Defender PAM to the system PAM configuration for that service. Some UNIX/Linux systems store system PAM configuration in the /etc/pam.conf file, while others keep PAM configuration in a set of files in the /etc/pam.d directory.

To configure the Defender PAM on your system, you can use a PAM configuration utility and script supplied with the Defender PAM. For example, to configure Defender authentication for a single service such as sshd, run the following command:

```
/opt/quest/libexec/defender/configure_pam_defender.sh sshd add
```

This script establishes the correct location for the specified service and adds the configuration for the Defender PAM. If you want to configure Defender authentication for more than one service, run the script again, specifying a new service name in place of sshd.

You can use this same script to remove the Defender PAM configuration. To do this, run the following command:

```
/opt/quest/libexec/defender/configure_pam_defender.sh sshd remove
```

Before enabling the Defender PAM for the sshd service, ensure that the use of PAM modules and challenge-response authentication are enabled on the ssh server. For example, on OpenSSH servers the /etc/ssh/sshd_config file should contain the following configuration lines:

```
UsePAM yes
```

```
ChallengeResponseAuthentication yes
```

You will need to restart sshd after making any changes to the sshd_config file.

Any ssh clients used to login to the server should also be configured to allow challenge-response authentication. For example, on OpenSSH clients, the following line should exist either in the system ssh config file (/etc/ssh/ssh_config) or in the user's ssh config file (~/.ssh/config):

```
ChallengeResponseAuthentication yes
```

When a user accesses a service that has been configured for Defender authentication, they are prompted for a Defender token passcode, as shown in the example below:

```
$ ssh jbloggs@unix002
```

```
Passcode:*******
```

```
Password:*******
```

```
Last login: Wed 14 May 14:03:22 2014 on /dev/pts/2 from unix001
```

```
$
```

After entering a valid passcode, the user may be prompted for further credentials, depending on other authentication methods in the service's System PAM configuration, for example, UNIX password authentication or Authentication Services AD authentication.

Please refer to the PAM_DEFENDER (5) man page on your UNIX system for more information on the Defender PAM (use the command man –M /opt/quest/man pam_ defender to display the man page).

Step 2: Specify Defender Security Servers

The Defender PAM communicates with the Defender Security Server via the RADIUS protocol. The communication details for the Defender Security Server must be specified in the /etc/defender.conf file. This file must be readable by all.

The entries in the file must have the following format:

```
<hostname>:<portnumber> <sharedsecret> <timeout>
```

where

- <hostname> is the name of the RADIUS server, that is, the Defender Security Server.
- <portnumber> is the port number on which the Defender PAM will communicate with the RADIUS server. There must be no spaces between <hostname> and <portnumber>.

- <sharedsecret> is the shared secret specified for the Defender PAM and the RADIUS server.
- <timeout> is the length of time, in seconds, after which the connection between the Defender PAM and the RADIUS server will be lost if no activity is detected.

You can specify more than one RADIUS server in the file. The Defender PAM attempts to connect to the servers in the order they are listed.

The following example enables the Defender PAM to communicate with the RADIUS server on host dss.example.com, port 1645, with shared secret shared_secret, and timeout of 3 seconds:

```
dss.example.com:1645 shared_secret 3
```

Step 3: Configure access control for users and services

The Defender PAM uses a PAM RADIUS Access Control List file (/etc/pam_radius_acl.conf) to determine which service/user combinations will be authenticated by the Defender PAM.

The Access Control file should contain a list of <servicename>:<username> pairs (one line per entry), to indicate which service/user combinations require Defender authentication. The <servicename> and/or <username> may be substituted with an asterisk (*) or left blank to indicate a wildcard (all users or services).

If the pam_radius_acl.conf does not exist, then all users must authenticate via Defender.

Table 29:
pam_radius_acl.conf syntax examples

To configure this...	Do this...

All users must authenticate via Defender for all Defender PAM-enabled services.	Use a single entry with wildcards for both <servicename> and <username>.
	Example 1
	`*:*`
	Example 2
	`:`

All users must authenticate via Defender for a specific service.	Use a wildcard for the <username>.
	Example 1
	`sshd:*`
	Example 2
	`telnet:`

To configure this...	Do this...

Specific users must authenticate via Defender for all services.	List individual users, but specify a wildcard for the <servicename>.
	Example 1
	`:john`
	Example 2
	`*:sally`

Specific users must authenticate via Defender for specific services.	List individual users and services without using wildcards.
	Example
	`sshd:jane`
	`sshd:david`
	`su:adam`

No users require authentication via Defender.	Ensure that the /etc/pam_radius_acl.conf file exists, but remove all entries from the file.

The following is an example pam_radius_acl.conf file:

```
upm:*
telnet:
:john
*:sally
login:david
```

In this example, all users accessing the service `upm` or `telnet` must authenticate via Defender. Users `john` and `sally` must authenticate via Defender for every service. User `david` must authenticate via Defender for the `login` service only. Any servicename:username combination not listed in the file does not require users to authenticate via Defender.

You should ensure that for each service specified in the pam_radius_acl.conf file there is a valid system PAM configuration for that service as described in Step 1: Enable authentication for target service.

Step 4: Configure Defender objects in Active Directory

You may need to add or modify Defender objects in Active Directory so that your UNIX/Linux system can use Defender authentication. You should ensure that an Access Node is defined for your UNIX/Linux system in the Defender configuration and that the

Access Node is assigned to the Defender Security Servers listed in the /etc/defender.conf file.

Also, ensure that your UNIX users are defined in Active Directory, have tokens assigned to them, and are included under the **Members** tab of the Access Node object corresponding to your UNIX system.

Testing Defender PAM configuration

You can test the configuration of the Defender PAM by using a test tool that is installed together with the Defender PAM. You can find this tool in /opt/quest/libexec/defender/check_pam_defender.

The test tool requires two arguments: the user name to test and the name of service for which you want to test Defender authentication. The test tool attempts to access the Defender Security Servers configured in your environment, and if one or more servers are accessible, the tool attempts to authenticate the specified user via Defender by using the Defender PAM. Then, the tool reports the result.

Defender PAM logging

The Defender PAM logs the RADIUS server responses for all failed authentication attempts to the system logger at the Info level. To do that the Defender PAM uses the auth or authpriv facility, depending on platform.

You can enable trace level logging for troubleshooting purposes.

To enable trace level logging

1. Make sure the /tmp/pam_def.ini file exists on your system. The file must specify a location to a log file as well as a trace level.

   Example:

   ```
   filename=/tmp/pam_defender_trace.log
   level=0xffffffff
   ```

2. Append the debug argument to the auth entries for the Defender PAM in the system PAM configuration.

Auth arguments

The following table lists the arguments you can append to the auth entries for the Defender PAM in the system PAM configuration.

Table 30:
Auth arguments

Argument	Description
debug	Enables trace level logging for the Defender PAM entries in the system PAM configuration to which this argument is added. For instructions on how to enable trace level logging, see Defender PAM logging.
skip_password	Causes the Defender PAM to display the "Enter Synchronous Response:" prompt to the user, instead of the "Passcode:" prompt.
use_first_pass	Causes the Defender PAM to use the PAM_AUTHTOK item as the user's passcode. In this case, the user is not prompted to enter a passcode. If the PAM_AUTHTOK item is not set, authentication fails.
try_first_pass	Causes the Defender PAM to use the PAM_AUTHTOK item in the PAM stack as the user's passcode. If the PAM_AUTHTOK item is not set, the Defender PAM prompts the user for a passcode.
conf=<path to Defender configuration file>	Allows you to specify an alternate location for the defender.conf file. The default location is /etc/defender.conf.
client_id=<client ID>	Allows you to specify the client ID for accounting requests which are validated during the pam_session call. When no client ID specified, the PAM service name is used as the client ID.

9

Delegating Defender roles, tasks, and functions

Defender provides a scalable approach to the administration of access rights, enabling you to delegate specific Defender roles, tasks, and functions to the users or groups you want.

The Defender Administration Console provides a wizard you can use to search for and select one or multiple user accounts, and then choose which Defender roles or tasks you want these accounts to perform.

Besides delegating roles or tasks, you can delegate specific Defender functions, for example, appoint selected user accounts as service accounts for the Defender Security Servers or Defender Management Portal, or grant full control over particular Defender objects, such as Access Nodes, Defender Security Servers, licenses, RADIUS payloads, or security tokens.

Steps to delegate roles, tasks, and functions

You can delegate Defender roles, tasks, or functions to specific users or groups by using the Defender Delegated Administration Wizard.

To delegate Defender roles, tasks, or functions

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 | Delegate Control**.

   Step through the wizard.
4. In the Users and Groups step, add the user accounts or groups to which you want to delegate Defender roles, tasks, or functions. Click **Next**.
5. In the Tasks to Delegate step, select the check boxes next to the Defender roles, tasks, or functions you want to delegate. Click **Next**.

For more information, see:

- Roles
- Service accounts
- Advanced control
- Full control

6. Follow the steps in the wizard to complete delegating the roles, tasks, or functions.

   The wizard does not modify any standard Active Directory permissions. Rather, it modifies permissions on the Defender attributes in the Active Directory schema.

Roles

You can delegate the below-listed Defender roles to the users or groups you want. If necessary, you can delegate two or more roles to the same user.

Table 31:
Defender roles

Role	Description
Administrator	Members of this role can modify any Defender object and have complete control over the Defender configuration. This includes modification of all user-based Defender items. Members of this role can: • Assign and unassign tokens. • Set a Defender password. • Set a Defender PIN. • Modify access nodes, Defender Security Servers, Defender policies, tokens, and RADIUS payloads.

Role	Description
	• Manage Defender licenses.
Basic Helpdesk	Members of this role can: • Reset tokens. • Test a token via the Defender Administration Console. • Reset a locked token by resetting the violation count for the user to whom the token is assigned.
Provisioning	Members of this role can: • Assign a Defender token. • Program a Defender token. • Remove a Defender token from a user's account. • Reset a Defender PIN.
Enhanced Helpdesk	Members of this role can: • Assign a Defender token. • Program a Defender token. • Remove a Defender token. • Reset a Defender token. • Recover a Defender token. • Test a Defender token. • Reset a locked Defender token. • Set a Defender PIN. • Set a Defender password. • Assign a temporary token response.
Auditor	Members of this role have read-only access to • All Defender objects of Users and Groups. • All Defender attributes of Users and Groups.

Service accounts

You can delegate permissions to specific user accounts so that they act as service accounts for the Defender components you want.

Table 32:
Options related to service accounts

Role	Description
Defender Security Server	The user account to which you assign this role gets the sufficient permissions to act as the Defender Security Server service account. To specify the user account as the Defender Security Server service account, use the Defender Security Server Configuration tool. For more information, see Defender Security Server Configuration tool reference on page 28.
Defender Management Portal	The user account to which you assign this role gets the sufficient permissions to act as the Defender Management Portal service account. The user account to which you assign this role must be a member of the local Administrators group on the computer where the Defender Management Portal is installed. After assigning this role to a user account, enter the account credentials in the Defender Management Portal. For more information, see Specifying a service account for the portal on page 128.

Advanced control

You can delegate permissions to perform one or several specific Defender tasks to the user accounts you want. You can delegate the following tasks:

- Assign Defender token
- Program Defender token
- Recover Defender token
- Reset Defender token
- Set and clear Defender token's PIN
- Assign Defender token temporary response
- Set Defender password
- Test Defender token
- Unassign Defender token
- Reset Defender token violation Count
- Modify Defender ID

- Select Policy
- Select RADIUS Payload

Full control

You can delegate permissions to manage specific Defender objects, including the permissions to view or modify any of the object properties and the permissions to create, delete, rename or move objects on a user or group.

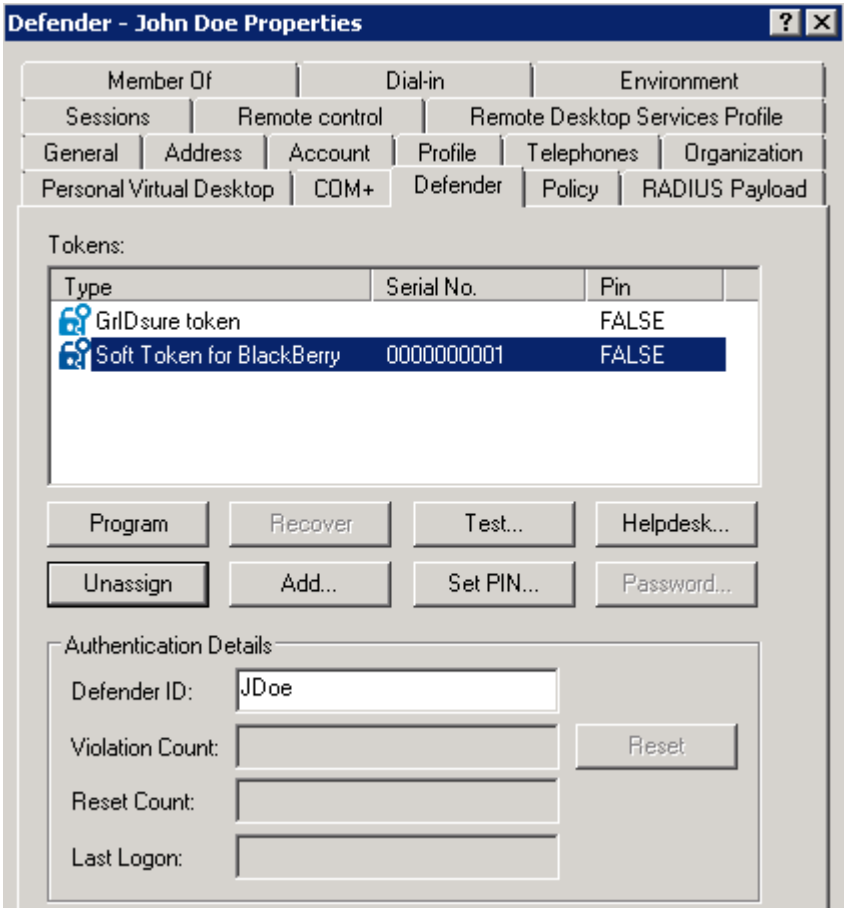
The available options are:

- Defender access node full control
- Defender Security Server full control
- Defender License full control
- Defender Security Policy full control
- Defender RADIUS Payload full control
- Defender Token full Control

Using control access rights

Control access rights are provided as an optional setting during the installation of the Defender Administration Console. Control access rights can be combined with the delegated administration privileges assigned to security groups or users.

The Defender control access rights act as an additional layer of administration security, allowing you to enable or disable the token-related buttons provided below the **Tokens** list on the **Defender** tab in the **Properties** dialog for a Defender user:



With control access rights, you can enable or disable the following buttons:

- **Program** Allows you to program the selected token for the user.
- **Recover** Unlocks the selected token.
- **Test** Starts a non-intrusive test to verify the token's response.
- **Helpdesk** Allows you to reset the token or assign a temporary token response to the user.
- **Unassign** Unassigns the selected token from the user.
- **Add** Assigns a new token to the user.
- **Set PIN** Sets a PIN for the selected token.
- **Password** Allows you set up a new or change the existing Defender password for the user.

To assign control access rights to users

1. Use the Defender Administration Console to enable the **Security** tab for the Defender users. By default, the **Security** tab is disabled.

Do the following:

a. On the computer where the Defender Administration Console is installed, open the Active Directory Users and Computers tool (dsa.msc).

b. In the left pane, expand the appropriate domain node, and then click to select the **Defender** container.

c. On the menu bar, click **View**, and then click **Advanced Features**.

2. In the left pane (console), locate the organizational unit that holds the Defender users to whom you want to assign control access rights.
3. Right-click the OU, and then on the shortcut menu click **Properties**.
4. In the dialog box that opens, click the **Security** tab, and then click **Advanced**.
5. Click **Add** to add the security group or user account.
6. In the **Permission Entry for Users** dialog box, use the following elements:
   - **Apply on** Select the target for the permissions you are going to select (user objects or descendant user objects).
   - **Permissions list** Select the check boxes next to the permissions you want to assign.
7. Click **OK** to apply your changes.

To remove control access rights from a group of users

1. In the **Advanced Security Settings** dialog box, click to select the appropriate entry in the **Permission entries** list.
2. Click the **Remove** button below the list, and then click **OK**.

10

Automating administrative tasks

Defender Management Shell, built on Microsoft Windows PowerShell technology, provides a command-line interface that enables automation of Defender administrative tasks. With the Defender Management Shell, administrators can perform token-related tasks such as assigning tokens to users, assigning PINs, or checking for expired tokens.

The Defender Management Shell command-line tools (cmdlets), like Windows PowerShell cmdlets, are designed to deal with objects—structured information that is more than just a string of characters appearing on the screen. The cmdlets do not use text as the basis for interaction with the system, but use an object model that is based on the Microsoft .NET platform. In contrast to traditional, text-based commands, the cmdlets do not require the use of text-processing tools to extract specific information. Rather, you can access required data directly by using standard Windows PowerShell object manipulation commands.

Before installing the Defender Management Shell feature, make sure your computer meets the system requirements described in the *Defender Release Notes*.

All cmdlets are presented in verb-noun pairs. The verb-noun pair is separated by a hyphen (-) without spaces, and the cmdlet nouns are always singular. The verb refers to the action that the cmdlet performs. The noun identifies the entity on which the action is performed. For example, in the Add-TokenToUser cmdlet name, the verb is Add and the noun is TokenToUser.

Installing Defender Management Shell

To install the Defender Management Shell

1. In the Defender distribution package, open the Setup folder, and run the **Defender.exe** file.
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.

Uninstalling Defender Management Shell

To uninstall the Defender Management Shell

1. Open the list of installed programs (appwiz.cpl).
2. In the list, click to select the **Defender** entry.
3. At the top of the list, click the **Change** button and step through the wizard that starts.
4. In the Change, Repair, or Remove Installation step, click the **Change** button.
5. In the Select Features step, click the **Defender Management Shell** feature, and then click **Entire feature will be unavailable**.
6. Complete the wizard.

Opening Defender Management Shell

You can open the Defender Management Shell by using either of the following procedures. Each procedure loads the Defender Management Shell snap-in into Windows PowerShell. If you do not load the Defender Management Shell snap-in before you run a command (cmdlet) provided by that snap-in, you will receive an error.

To open the Defender Management Shell

1. Start a 32-bit version of Windows PowerShell.
2. At the Windows PowerShell prompt, enter the following command:

   ```
   Add-PSSnapin OneIdentity.Defender.AdminTools
   ```

Alternatively, you can complete the following steps related to your version of Windows:

Table 33:
Alternative steps to open the Management Shell

Windows 8, Windows Server 2012, and Windows Server 2012 R2
On the **Apps** screen (Windows logo key + Q), click the **Defender Management Shell** tile.

Windows 10, Windows Server 2016, and **Windows Server 2019**
1. Click the **Windows Start** button, and then scroll through the alphabetical list on the left. 2. Click **One Identity** to expand the list of components of Defender products installed on the system. 3. Click **Defender Management Shell**.

Upon the shell start, the console may display a message stating that a certain file published by One Identity is not trusted on your system. This security message indicates that the certificate the file is digitally signed with is not trusted on your computer, so the console requires you to enable trust for the certificate issuer before the file can be run. Either press **R** (Run once) or **A** (Always run). To prevent this message from appearing in the future, it is advisable to choose the second option (**A**).

Getting help

This section provides instructions on how to get help information for the cmdlets added by the Defender Management Shell to the Windows PowerShell environment.

Alternatively, you can get detailed information about the Defender Management Shell cmdlets by viewing the **DefenderManagementShell.chm** file located in the Defender Management Shell installation folder (by default, this is **%ProgramFiles%\One Identity\Defender\Management Shell**).

Table 34:
Common help commands

To view this...	Run this command...
A list of all the Defender Management Shell cmdlets available to the shell.	**Get-Command -module OneIdentity.Defender.AdminTools**
Information about the parameters and other components of a Defender Management Shell cmdlet.	**Get-Command** <*CmdletName*> You can use wildcard character expansion. For example, to view information about the cmdlets with the names ending in **Token**,

To view this...	Run this command...
	you can run this command: **Get-Command *Token**
Basic help information for a Defender Management Shell cmdlet.	**Get-Help** <*CmdletName*>
Detailed help information for a Defender Management Shell cmdlet, including descriptions of available parameters and usage examples.	**Get-Help** <*CmdletName*> **-full**
Basic information about how to use the help system in Windows PowerShell, including Help for the Defender Management Shell.	**Get-Help**

Cmdlets provided by Defender Management Shell

For detailed information about the Defender Management Shell cmdlets, please view the **DefenderManagementShell.chm** file located in the Defender Management Shell installation folder (by default, this is **%ProgramFiles%\One Identity\Defender\Management Shell**).

11

Administrative templates

The Defender distribution package includes Group Policy administrative templates, which you can use to configure the additional features and options that are not available in the Defender Administration Console by default.

In the Defender installation package, you can find the below mentioned files in **Setup\Group Policy Templates** folder.

These administrative templates are supplied in the following files:

Table 35:
Defender Group Policy administrative templates

File	Provided functionality
DefenderGroupPolicy.admx	• An option to limit the maximum configurable expiry time for the Temporary Helpdesk Token response feature. • Configuration options for programming software tokens through the Active Roles Web Interface. • An option to include a Send Mail feature allowing the sending of the token activation code by e-mail for a newly programmed software token. • Allows serverless binding for Defender to read and write data in Active Directory.
DefenderGroupPolicy.adml	• Allows Group Policy Object Editor to display a policy setting in the locale.

This chapter consists of the following sections.

Installing administrative templates

To install the administrative templates on Domain Controller

1. Navigate to **%windir%\SYSVOL\sysvol\<DomainName>\Policies** directory.
    a. Create a folder **PolicyDefinitions** and copy the **DefenderGroupPolicy.admx** file into this folder.
    b. In the **PolicyDefinitions** folder, create a language specific folder, such as **en-US**, and then copy the **DefenderGroupPolicy.adml** file into this folder.
2. Open the Group Policy Management window (**gpmc.msc**).
    a. In the left pane (console tree), expand the appropriate forest node, and then expand the **Domains** node.
    b. Right-click the appropriate domain node, and then on the shortcut menu click **Create a GPO in this domain and Link it here**.
    c. In the **New GPO** dialog box, type a name for the GPO being created, and click **OK**.
3. Add the Defender Group Policy administrative templates to the GPO you have just created:
    a. In the left pane (console tree) of Group Policy Management, right-click the GPO you have created, and then on the shortcut menu click **Edit**.

    Group Policy Management Editor opens.
    b. In the left pane (console tree) of Group Policy Management Editor, expand **Computer Configuration\Policies\Administrative Templates**.

You can now see One Identity node and Defender sub-node appearing automatically.

To install the administrative templates on client computer

1. Copy the **DefenderGroupPolicy.admx** file into **%windir%\PolicyDefinitions folder** directory.
2. Copy the **DefenderGroupPolicy.adml** file into **%windir%\PolicyDefinitions\en-us** directory.
3. Open the Local Group Policy Editor (**gpedit.msc**).
    a. In the left pane (console tree) of the Local Group Policy Editor, expand **Computer Configuration\Administrative Templates**.

You can now see One Identity node and Defender sub-node appearing automatically.

Configuring administrative templates

To configure settings for administrative templates

1. Open the Group Policy Management Editor (gpedit.msc).
2. On the left pane, select **Computer Configuration\Administrative Templates\One Identity\Defender**.
3. In the right pane, double-click the setting you want to configure.

The DefenderGroupPolicy.admx file provides the following settings:

- Temporary Responses setting
- Active Roles Web Interface - Token Programming setting
- Mail Configuration setting
- ADSI Configuration setting

Temporary Responses setting

You can use this setting to set a maximum limit on the expiry time for temporary helpdesk token responses. By default, status of these settings are not configured.

To enable this setting

1. Open the **Temporary Responses** setting.
2. Click **Enabled**.
3. From the **Maximum expiry time** drop down, select the maximum length of time that a temporary helpdesk token response can remain valid.

NOTE: Now when you assign a temporary helpdesk token response to a user, the maximum expiry time for the response is set to the value defined by this setting.

4. Click **OK**.

Active Roles Web Interface - Token Programming setting

You can use this setting to select the token types and token programming modes you want to make available for programming through the Active Roles Web Interface.

To enable this setting

1. Open the **ActiveRoles Web Interface - Token Programming** setting.
2. Click **Enabled**.
3. Under **Token Types** and **Token Programming Modes** sections, select one or more token types and token programming modes to make it available for programming through the Active Roles Web Interface.
4. Click **OK**.

Mail Configuration setting

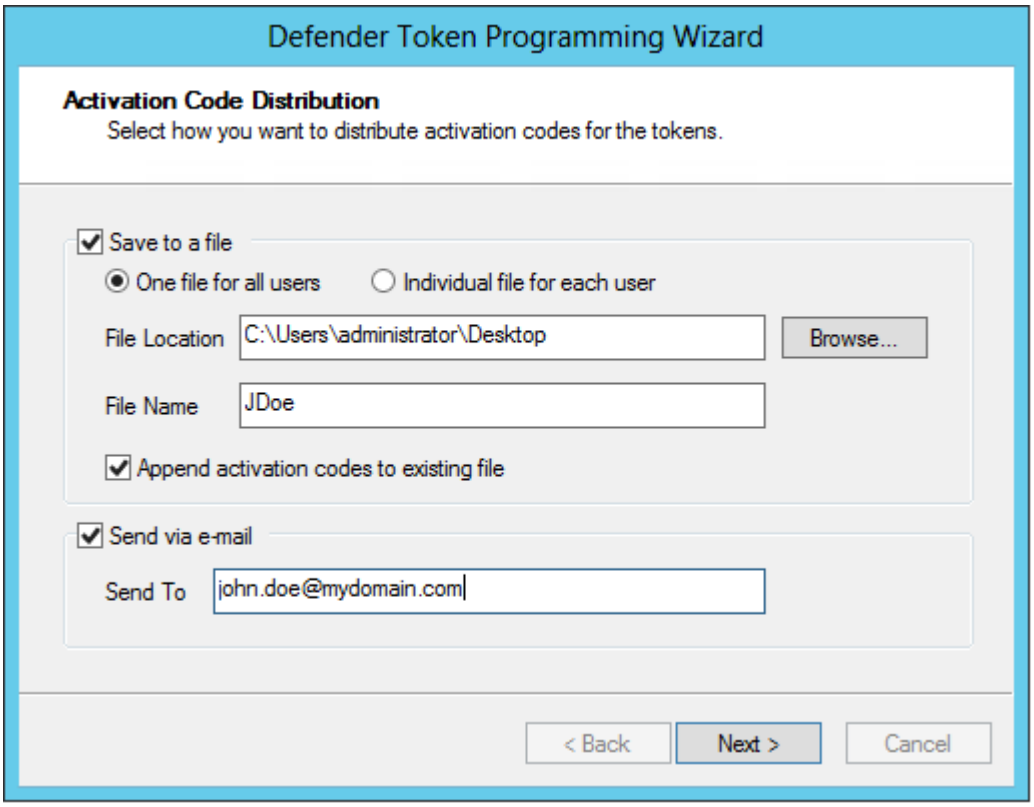
You can use this setting to configure options for sending token activation codes to users via e-mail. With this setting configured, an option to send token activation codes by e-mail becomes available in the Defender Token Programming Wizard.

To enable this setting,

1. Click **Enabled**.
2. Set the following options, and then click **OK**.

- **SMTP Server** Type the IP address or DNS name of the SMTP server you want to use for sending e-mail messages containing token activation codes.
- **SMTP Server Port** Specify the communication port used by the SMTP server.
- **Address from which to send mails** Type the e-mail address you want to appear in the **From** field of the e-mail messages containing token activation codes.
- **CC address to which mails are sent** Type the e-mail address to which you want to send copies of the e-mail messages containing token activation codes.
- **Send message as plain text** Select this check box if you want to send the e-mail messages containing token activation codes in a plain text format. Note, that plain text messages do not contain QR codes or links for token activation. If you want to include QR codes and links for token activation in a message, clear this check box. When this check box is cleared, the e-mail messages are sent in an HTML format.
- **Text to include at the bottom of activation code mails** Type the text you want to include in each e-mail message containing token activation codes.

With the Mail Configuration setting enabled and configured, you can use the Defender Token Programming Wizard to send an e-mail containing token activation codes to the user:



Select the **Send via e-mail** check box, and then use the **Send To** text box to type the recipient's e-mail address.

ADSI Configuration setting

This setting provides a configurable performance enhancement for large installations by ensuring that for read and write operations, Defender always uses the domain controller to which the Active Directory Users and Computer (ADUC) tool is connected.

When this setting is enabled and the **Allow serverless bind** check box is cleared, Defender reads and writes data in Active Directory by using the domain controller to which ADUC is connected.

When this setting is enabled and the **Allow serverless bind** check box is selected, Defender relies on the Active Directory Service Interfaces Editor (ADSI Edit) tool to select a domain controller through which it can read and write data in Active Directory. This is also the default Defender behavior when this setting is not enabled.

Updating administrative templates

You can follow the steps mentioned below to update administrative templates from .adm to .admx on both Domain Controller and Client computer.

Updating templates on Domain Controller

Before updating the templates, you should remove the existing .adm templates and then proceed updating the templates.

To remove the administrative templates on Domain Controller

1. Open the Group Policy Management (**gpmc.msc**).
2. Right click on the GPO you have created, set **Enforced** to disable.
3. Again, right click on the GPO, and on the shortcut menu, click **Edit**.

Group Policy Management Editor opens.

4. In the left pane (console tree) of Group Policy Management Editor, expand **Computer Configuration\Policies**.
5. Right-click the **Administrative Templates** node, and then click **Add/Remove Templates**.
6. In the **Add/Remove Templates** dialog box, select **DefenderGroupPolicy.adm** and **DefenderBindingGroupPolicy.adm** files and click **Remove**.

To update the administrative templates on Domain Controller

1. Navigate to **%windir%\SYSVOL\sysvol\<DomainName>\Policies** directory.
    a. Create a folder **PolicyDefinitions** and copy the **DefenderGroupPolicy.admx** file into this folder.
    b. In the **PolicyDefinitions** folder, create a language specific folder, such as **en-US**, and then copy the **DefenderGroupPolicy.adml** file into this folder.
2. Open the **Group Policy Management Editor** and navigate to the **Computer Configuration\Administrative Templates\One Identity\Defender** directory to see the policy settings.

NOTE: Make sure that the policy configuration settings are retained after updating into .admx templates in the Group Policy Management Editor.

3. Right click the GPO in Group Policy Management, and then click **Enforced** to enable.

Updating templates on client computer

To remove the administrative templates on client computer

1. Open the Group Policy Management Editor (**gpedit.msc**).
2. Expand **Computer Configuration\Policies**.
3. Right-click the **Administrative Templates** node, and then on the shortcut menu, click **Add/Remove Templates**.
4. In the **Add/Remove Templates** dialog box, select **DefenderGroupPolicy.adm** and **DefenderBindingGroupPolicy.adm** files and click **Remove**.

To update the administrative templates on client computer

1. Copy the **DefenderGroupPolicy.admx** file into **%windir%\PolicyDefinitions folder** directory.
2. Copy the **DefenderGroupPolicy.adml** file into **%windir%\PolicyDefinitions\en-us** directory.
3. Open the **Group Policy Management Editor** and navigate to the **Computer Configuration\Administrative Templates\One Identity\Defender** directory to see the policy settings

NOTE: Make sure that the policy configuration settings are retained after updating into .admx templates in the Group Policy Management Editor.

12

Integration with Active Roles

The Defender installation package includes the Defender Integration Pack for Active Roles which extends the Active Roles functionality and allows you to perform Defender-related tasks from within the Active Roles console (MMC Interface) and the Active Roles Web Interface. For example, with this Integration Pack installed, you can assign, remove, test, recover, and program tokens, set Defender IDs and Defender passwords. Also you can enable the automatic deletion of tokens for deprovisioned users and use the Active Roles console to administer Defender objects and delegate specific Defender roles or tasks to the users you want.

Active Roles offers a practical approach to automated user provisioning and administration, for maximum security and efficiency. Active Roles provides total control of user provisioning and administration for Active Directory. For more information about Active Roles, please go to https://www.oneidentity.com/products/active-roles/.

Installing Defender Integration Pack for Active Roles

Before installing the Defender Integration Pack for Active Roles, make sure the target system meets the system requirements listed in the *Defender Release Notes*.

To install the Defender Integration Pack for Active Roles

1. On the target computer, run the **ActiveRolesIntegrationPack.exe** file supplied in the Defender installation package.
2. Step through the Setup Wizard to complete the Integration Pack installation.

   In the Setup Wizard, you can select the following features for installation:

- **Active Roles Web Interface Extension** Install this feature to be able to perform Defender-related tasks from the Active Roles Web Interface. The computer on which you plan to install this feature must have the Active Roles Web Interface installed. For more information about the commands this feature adds to the Active Roles Web Interface, see Commands added to the Active Roles Web Interface.
- **Active Roles Console Extension** Install this feature to be able to perform Defender-related tasks from the Active Roles console (MMC Interface). After installing this feature, you can use the Active Roles console to manage Defender-related objects and perform Defender-related tasks. The steps you should perform in the Active Roles console to manage Defender objects are identical to those you perform in Microsoft's Active Directory Users and Computers tool.For more information, see Managing Defender objects in Active Directory on page 37.

3. After completing the Setup Wizard, restart the Active Roles Administration Service on the computer on which you have installed the Integration Pack.
4. On each remote computer running the Active Roles Administration Service in your environment, install the Defender Integration Pack for Active Roles Administration Service.

   To install the Defender Integration Pack for Active Roles Administration Service, run the **ActiveRolesAdminServiceIntegrationPack.exe** file supplied in the Defender installation package, and then complete the wizard.

Commands added to the Active Roles Web Interface

The Defender Integration Pack for Active Roles adds the **Defender** category to the Active Roles Web Interface:

Click the **Defender** category to access the commands added by the Defender Integration Pack for Active Roles to the Active Roles Web Interface.

These commands are as follows:

- **Defender Properties** Allows you to administer tokens and view and manage the Defender properties for the selected user.
- **Set Defender Password** Allows you to set a Defender password for the selected user.
- **Program Defender Token** Allows you to program a security token for the selected user.

Defender Properties

The **Defender Properties** command allows you to administer tokens, and view and manage the Defender properties for the selected user.

On **Defender Properties** page, you can use the **User tokens** list to view and administer security tokens for the user, view the serial number of each security token assigned to the user, and if the tokens have a PIN configured.

Below the **User tokens** list, you can use the following elements:

- **Add** Click this button to search for existing token objects in Active Directory and assign them to the user if necessary.
- **Defender ID** Allows you to view or change the Defender ID of the user.
- **Violation count** Displays the number of unsuccessful authentication attempts for the user. To reset violation count for the user, click the **Reset Violation Count** button, and then click **Save**.
- **Reset count** Displays how many times the violation count has been reset so far.
- **Last authentication** Displays the time and date of user's last successful authentication.

In the **Type** column of the **User tokens** list, you can click a security token name to administer the token. On the page that opens, you can use the following buttons:

Table 36:
Buttons to administer tokens

Button	Description
Set PIN	Click to set a new PIN for the token. On the page that opens, use the **New PIN** and **Confirm PIN** text boxes to type the new PIN. If you want the user to change the new PIN on first use, select the **Expire PIN** check box. When finished, click the **Set PIN** button.
Clear PIN	Click to remove the current PIN from the token. The PIN is removed right after you click this button.
Temporary Response	Click to generate a temporary response for the token user. A temporary response is required when the user needs to authenticate but does not currently have a token available. On the page that opens use the following options: • **Expires** Sets a validity period for the temporary response. • **Allow response to be used multiple times** Allows you to set if the temporary response can be used more that once during the specified validity period. When this check box is cleared, the temporary response can only be used once.

Button	Description
	• **Assign** Generates the temporary token response, assigns it to the user's token, and displays the assigned response in a separate window. • **Clear** Immediately removes the temporary token response from the user's token.
Test Token	Click to open a page that allows you to test the token response for the selected token: In the **Response** text box, enter a token response, and then click **Verify**.
Reset	Click to re-synchronize the token.
Recover	Click to reset the passphrase for the token.
Unassign	Click to unassign the token from the user.

Set Defender Password

The **Set Defender Password** command allows you to set a Defender password for the selected user.

On **Set Defender Password** page, you can use the following elements:

- **New password** Type the new Defender password for the user.
- **Confirm password** Type the new Defender password to confirm it.
- **Expire password** Select this check box if you want the new Defender password to expire in a preconfigured period of time.
- **Set Password** Click this button to apply the new password.

Program Defender Token

The **Program Defender Token** command allows you to program a security token for the selected user. Clicking this command opens the following page:

On **Program Defender Token** page, select the token you want to program, and, if applicable, a token operational mode (synchronous or challenge-response). When finished, click the **Program** button.

For some token types, a new page with the following additional options may open:

- **Token serial** Displays the serial number of the token you have assigned to the user.
- **Activation code** Displays the code the user must enter to activate the assigned token. You can click the **Copy** button to copy the displayed activation code to the Windows Clipboard.

- **Send activation e-mail to** Allows you to send the token activation code to the user by e-mail. Type the recipient e-mail address in the text box, and then click **Send** to send the e-mail message containing the activation code to the user. This option is only available if you have enabled it via a Group Policy administrative template supplied with Defender. For more information, see Administrative templates on page 183.

Enabling additional features via Group Policy

You can use Group Policy to enable a number of optional features provided by the Defender Integration Pack for Active Roles. These features include the automatic sending of e-mails with token activation codes, propagation of token configuration settings via Group Policy, and the ability to set an expiry period for temporary responses. To enable these features, you need to use the Group Policy administrative template supplied with Defender.

To enable Defender features via Group Policy

1. Install the Defender Group Policy administrative template (DefenderGroupPolicy.adm) on a domain controller.
2. Configure the settings provided by the Defender Group Policy administrative template.

For more information, see Installing administrative templates on page 184.

Enabling automatic deletion of tokens

The Defender Integration Pack for Active Roles installs an additional deprovisioning policy that allows you to enable the automatic deletion of tokens for deprovisioned users.

To enable the automatic deletion of tokens

1. Open the Active Roles console.
2. In the left pane, expand **Configuration | Policies | Administration**.
3. Right-click the **Defender** node, point to **New**, and then click **Deprovisioning Policy**.
4. Step through the wizard.
5. In the Policy to Configure step, in the list, expand the **Defender** node to select **Unassign Tokens**.
6. Complete the wizard. Keep the default settings in the remaining wizard steps.

   The new Unassign Tokens deprovisioning policy is now available for use and you can add it as a deprovisioning policy.

Delegating Defender roles or tasks

The Defender Integration Pack for Active Roles installs a number of additional predefined Access Templates. These Access Templates fall into the following two categories:

- **Role-oriented** Allow you to delegate specific Defender roles, such as Defender administrator or helpdesk operator. In the Active Roles console, you can find these Access Templates in the **Configuration/Access Templates/Defender** container.
- **Task-oriented** Allow you to delegate granular Defender tasks or provide full control over specific Defender components. For example, you can use these Access Templates to delegate such tasks as assign a token, program a token, and test a token. In the Active Roles console, you can find these Access Templates in the **Configuration/Access Templates/Defender/Advanced** container.

To delegate Defender roles or tasks by using Access Templates

1. Open the Active Roles console.
2. In the left pane, expand the **Active Directory** node, right-click the domain you want, and then on the shortcut menu click **Delegate Control**.
3. In the dialog box that opens, click the **Add** button and step though the wizard.
4. In the Access Templates step, select the Access Templates you want to use, and then click **Next**.
    - The Access Templates you can use to delegate Defender roles are located in the **Access Templates/Defender** container.
    - The Access Templates you can use to delegate granular Defender tasks are located in the **Access Templates/Defender/Advanced** container.
5. In the Inheritance Options step, keep the default settings, and then click **Next**.
6. In the Permissions Propagation step, select the **Propagate permissions to Active Directory** check box.
7. Complete the wizard to delegate the roles or tasks.

Upgrading Defender Integration Pack for Active Roles

To upgrade Active Roles Integration Pack

1. On the computer that has a previous version of Active Roles Integration Pack installed, run the **ActiveRolesIntegrationPack.exe** file.

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

2. Complete the Active Roles Integration Pack Setup Wizard.
3. After upgrading restart **Active Roles Administration Service**.

To upgrade Active Roles Admin Service Integration Pack

1. On the computer that has a previous version of Active Roles Admin Service Integration Pack installed, run the **ActiveRolesAdminServiceIntegrationPack.exe** file.

   In the Defender distribution package, you can find the **ActiveRolesAdminServiceIntegrationPack.exe** file in the Setup folder.
2. Complete the Active Roles Admin Service Integration Pack Setup Wizard.

Uninstalling Defender Integration Pack for Active Roles

To uninstall Defender Integration Pack for Active Roles

1. Uninstall Defender Integration Pack for Active Roles.
2. Uninstall Defender Integration Pack for Active Roles Administrative Service.

NOTE: Ensure that you uninstall the Defender Integration Packs for Active Roles in the sequence mentioned above.

To uninstall the Defender Integration Pack for Active Roles

1. Open the list of installed programs (appwiz.cpl).
2. In the list, click to select the **ActiveRolesIntegrationPack.exe** entry.
3. At the top of the list, click the Uninstall button and step through the wizard that starts.
   NOTE: Optionally click **Change** at the top of the list. In the Change, Repair, or Remove Installation step, click the Remove button.
4. Complete the wizard.

To uninstall the Defender Integration Pack for Active Roles Administration Service

1. Open the list of installed programs (appwiz.cpl).
2. In the list, click to select the **ActiveRolesAdminServiceIntegrationPack.exe** entry.
3. At the top of the list, click the Uninstall button and step through the wizard that starts.
   NOTE: Optionally click **Change** at the top of the list. In the Change, Repair, or Remove Installation step, click the Remove button.
4. Complete the wizard.

13

Push Notifications

A notification is a message that displays outside the contextual UI to provide the user with critical reminders or other information from a particular app on the mobile devices. Users can tap the notifications to open the app or take a predefined action directly from the notification. Push notifications for in-house applications allow users in your organization to receive important notification messages on their compatible mobile devices.

How the Defender Push Notification Works

The ***pushnotification*** feature is supported and configurable on both Android (version 8 or later) and iOS (iOS 10 or later) devices. The following sections describe the key Admin and User actions for using push notifications.

NOTE: Push notifications will not be triggered during authentication in offline mode.

Admin

- An admin programs the new Android or iOS tokens which have the Push Notification feature enabled by default. For more information about the wizard steps and options, see Defender Token Programming Wizard reference.
- The admin marks the relevant Defender security token policy to enable the push notification feature for users. For more information, see Managing Defender Security Policies.

User actions

- From Defender 6.2 onwards, the *pushnotification* is implicitly triggered when user initiates the login authentication process to Defender eliminating the need to enter keyword PUSH in token field in first login attempt. The existing functionality with type in keyword PUSH works if the first login attempts fails to authenticate or times out.
- The notification seeks a user response in form of Approve or Deny for access to the resources. Based on the user's response, the respective action takes place and the notification cycle completes.
- In case of a timeout, the user can also use can use "push" keyword/passcode/Gridsure PIP.
- Users activate the newly created token from the 6.1.0 release.

User friendly UX

DDL Client Authentication Process (Applicable from Defender 6.2)

1. When user initiates the Login process, the page asks for credentials only (username and password) and no passcode.
2. The DSS automatically identifies if the user has an Android or iOS Token configured. In such case, the application sends a push notification to Defender Soft Token App.
3. If the user approves the push notification on Defender Soft Token App, they are prompted to next authentication login process to complete the cycle.
4. If the user denies the push notification any time during the authentication process on Defender Soft Token App, the current login process gets canceled, and the user is redirected to the first Page to re-initiate the Login Process.
5. If the user neither approves nor deny the push notification on Defender Soft Token App, then the notification times out for that request and user will be able to select one of the two options (if Authentication method is only Token of any policy) to continue with the authentication process as below:
    a. User can trigger the push notification again by clicking on SUBMIT button.
    b. Or user can enter "push" (without quotes, case insensitive) passcode/keyword in passcode field or use Gridsure PIP for authentication.
6. When DSS identifies that a user does not have Android or iOS token configured, application will prompt the next authentication action (according to the token and Policy selected) on screen for user to complete the login process.
7. If User has selected “Remember password option” under GINA settings, login screen will be prompted with pre-filled password in read only with enabled Submit button to continue the authentication process. Applicable only on the second login attempt, after denial/timeout of first login request.

EAP Client Authentication Process (Applicable from Defender 6.2)

1. When user initiates the Login process, the page asks for credentials only (username and password) under Networks in EAP client.
2. The DSS automatically identifies if the user has an Android or iOS Token configured and sends a PUSH Notification to Defender Soft Token App while displaying a message confirming the notification sent process.
3. If the user approves the push notification on Defender Soft Token App, they are prompted to next authentication login process to complete the cycle.
4. If the user denies the push notification any time during the authentication process on Defender Soft Token App, the current login process gets canceled, and user has to re-initiate the login process.
5. If the user neither approves nor deny the push notification on Defender Soft Token App, then the notification times out for that request. The user can now select one of the two options (if Authentication method is only Token for any policy) to continue with the authentication process as below:
    a. User can trigger the push notification again by clicking the **RESEND** button.
    b. Or user can enter "push" (without quotes, case insensitive) passcode/keyword in passcode field.
6. If DSS identifies that a user does NOT have Android or iOS Token, application will prompt the next authentication action (according to the token and Policy selected) on screen for user to complete the login proces
7. In case no response is received from the user on the Defender Soft Token App then the request times out and user can select between two options to continue the authentication process as below:
    a. User can trigger the push notification again by clicking on **RESEND** button.
    b. Or user can click the **Sign in with another option** button and enter "push" (without quotes, case insensitive) passcode/keyword in passcode field.
8. GridSure Token is not supported with EAP Client.

ISAPI Client Authentication Process (Applicable from Defender 6.2)

1. When user initiates the login process, the page simply asks for 'username'.
2. If DSS identifies that a user has an Android or iOS token configured, the application will send a PUSH Notification to Defender Soft Token App.
3. In the meantime, a waiting page is displayed on the ISAPI client with a message, `"Defender needs to verify your identity. We sent a notification to your Defender Soft Token app. Please respond on your device to continue."`

    NOTE: The waiting page also displays the '**Sign in with another option**' button. The user can choose to sign in with token with out waiting for the push notification to be responded/timed-out.
4. If the user approves the push notification on Defender Soft Token App, they are prompted to the next authentication login process to complete the cycle.

5. If the user denies the push notification any time during the authentication process on Defender Soft Token App, the current login process gets canceled, and user is redirected to a page displaying a message regarding verification denial.

   NOTE: The **Ok** button on the verification denial page can be used to re-initiate the login process.

6. In case no response is received from the user on the Defender Soft Token App then the request times out and user can select between two options to continue the authentication process as below:
   a. User can trigger the push notification again by clicking on **RESEND** button.
   b. Or user can click the **Sign in with another option** button and enter "push" (without quotes, case insensitive) passcode/keyword/Gridsure PIP in passcode field.
7. If DSS identifies that a user does NOT have Android or iOS Token, application will prompt the next authentication action (according to the token and Policy selected) on screen for user to complete the login process.

Push notification timeout configurable

- The Push Notification verification timeout is a configurable value.
- On a computer where Defender Security Server is installed, use Registry Editor to create the following value at:

  `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\PassGo Technologies\Defender\DSS Active Directory Edition`

  `Value type: REG_DWORD`

  `Value name: NOTIFICATIONTIMEOUT`

  `Value data: XX`

  NOTE:
  - The value can range between decimal 1 to 30. Any other value beyond this range is invalid and will set the default timeout to 30 seconds.
  - In case if the registry key for the timeout is not found (not added), then the default timeout of 30 seconds is set.
  - The server will wait till the timeout seconds before sending the response back to client.

Defender push notifications can be disabled

- To turn the notifications off, the user needs to manually create the following registry value at:

  ```
  Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\PassGo
  Technologies\Defender\DSS Active Directory Edition
  ```

  ```
  Value type: REG_DWORD
  ```

  ```
  Value name: PushOff
  ```

  ```
  Value data: XX
  ```

- The value can be either 0 or 1. Any other value beyond this range is invalid and will set the defaul t push notification on. In case if theregistry key for the PushOff is not found (not added), then the default push notification on is set.

14

Appendices

Appendix A: Enabling diagnostic logging

To gather additional information on various Defender components, you can enable diagnostic logging for each component.

To enable the logging for some Defender components, you need to edit the Registry.

CAUTION: The following sections instruct you to modify the Registry. Note that incorrectly modifying the Registry may severely damage the system. Therefore, you should make the changes carefully. It is highly advisable to create a backup of the Registry before making changes to Registry data.

- Administration Console
- Defender Core Token Operations SDK (DTSDK)
- Defender Security Server
- Desktop Login
- EAP Agent
- Integration Pack for Active Roles
- Management Portal

- Management Portal (reports)
- Management Shell
- Service Connection Point
- Soft Token for Windows
- Token Import
- Token Programming
- VPN Integrator
- Web Service API

Administration Console

To enable diagnostic logging for Administration Console

- On a computer where Administration Console is installed, use Registry Editor to create the following value in the **HKLM\SOFTWARE\PassGo Technologies\Defender\Defender AD MMC** registry key:

  Value type: REG_DWORD

  Value name: **Diagnostics**

  Value data: **1**

The path to the log file is %ProgramData%\One Identity\Defender\Diagnostics\defender_ade_mmc.txt.

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

Defender Core Token Operations SDK (DTSDK)

To troubleshoot issues that may occur with token operations, you need to enable diagnostic logging for the DTSDK component which is installed as a part of various Defender components.

To enable diagnostic logging for DTSDK

- On a computer where DTSDK is installed, use Registry Editor to create the following value in the **HKLM\SOFTWARE\PassGo Technologies\Defender** registry key:

  Value type: REG_DWORD

  Value name: **DTSDK Diagnostics**

  Value data: **1**

The path to the log file is %ProgramData%\One Identity\Defender\Diagnostics\dtsdk.txt.

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

Defender Security Server

To enable diagnostic logging for Defender Security Server on a 32-bit (x86) system

On a 32-bit computer where Defender Security Server is installed, use Registry Editor to create the following value in the **HKLM\SOFTWARE\PassGo Technologies\Defender\DSS Active Directory Edition** registry key:

Value type: REG_DWORD

Value name: **Diagnostics**

Value data: **1**

To enable diagnostic logging for Defender Security Server on a 64-bit (x64) system

On a 64-bit computer where Defender Security Server is installed, use Registry Editor to create the following value in the **HKLM\SOFTWARE\WOW6432Node\PassGo Technologies\Defender\DSS Active Directory Edition** registry key:

Value type: REG_DWORD

Value name: **Diagnostics**

Value data: **1**

NOTE: If no registry key is found, manually create the following registry key:

HKLM\SOFTWARE\PassGo Technologies\Defender\DSS Active Directory Edition.

The path to the log file is %ProgramData%\One Identity\Defender\Diagnostics\radproxy.txt.

To disable diagnostic logging for Defender Security Server, delete the **Diagnostics** value from the **DSS Active Directory Edition** registry key, or set the value data to **0**.

Desktop Login

To enable diagnostic logging for Desktop Login

- On a computer where Desktop Login is installed, use Registry Editor to create the following value in the **HKLM\SOFTWARE\PassGo Technologies\Defender\Defender GINA** registry key:

  Value type: REG_DWORD

  Value name: **Diagnostics**

Value data: **1**

The path to the log file is %ProgramData%\One Identity\Defender\Diagnostics\Defender Desktop Login.txt.

To disable diagnostic logging for Desktop Login, delete the **Diagnostics** value from the **Defender GINA** registry key, or set the value data to **0**.

EAP Agent

To enable diagnostic logging for EAP Agent on a 32-bit (x86) system

On a 32-bit computer where EAP Agent is installed, use Registry Editor to create the following value in the **HKLM\SOFTWARE\PassGo Technologies\Defender\Defender 5 EAP** registry key:

Value type: REG_DWORD

Value name: **Diagnostics**

Value data: **1**

To enable diagnostic logging for EAP Agent on a 64-bit (x64) system

On a 64-bit computer where EAP Agent is installed, use Registry Editor to create the following value in the **HKLM\SOFTWARE\Wow6432Node\PassGo Technologies\Defender\Defender 5 EAP** registry key:

Value type: REG_DWORD

Value name: **Diagnostics**

Value data: **1**

The path to the log file is %ProgramData%\One Identity\Defender\Diagnostics\DefenderEAP.txt.

To disable diagnostic logging for EAP Agent, delete the **Diagnostics** value from the **Defender 5 EAP** registry key, or set the value data to **0**.

Integration Pack for Active Roles

To enable diagnostic logging for Integration Pack for Active Roles

- On a computer where Integration Pack for Active Roles is installed, use Registry Editor to create the following value in the **HKLM\SOFTWARE\PassGo Technologies\Defender** registry key:

  Value type: REG_DWORD

  Value name: **DefenderSDK Diagnostics**

  Value data: **1**

The path to the log file is %ProgramData%\One Identity\Defender\Diagnostics\DefenderSDK.txt.

To disable diagnostic logging for Integration Pack for Active Roles, delete the **DefenderSDK Diagnostics** value from the **Defender** registry key, or set the value data to **0**.

Management Portal

To enable diagnostic logging for Management Portal

1. On a computer where Management Portal is installed, go to the **WWW** folder in the Management Portal installation directory.

   Normally, the path to the folder is %ProgramFiles%\One Identity\Defender\Management Portal\WWW.

2. Make the following changes to the **Web.config** text file held in the **WWW** folder:
   - In the <log4net debug="false"> entry, set the value to "true": <log4net debug="true">
   - In the <level value="ERROR" /> entry, set the value to "DEBUG": <level value="DEBUG" />

You can find the log file **DefenderWeb.txt** in the **Logs** folder in the Management Portal installation directory. Normally, the path to the log file is %ProgramFiles%\One Identity\Defender\Management Portal\Logs\DefenderWeb.txt.

To disable diagnostic logging for Management Portal, set the following values in the **Web.config** file:

- <log4net debug="false">
- <level value="ERROR" />

Management Portal (reports)

To enable diagnostic logging for Management Portal (reports)

1. On a computer where Management Portal is installed, go to the **WWW\Areas\Reports\Generators** folder in the Management Portal installation directory.

   Normally, the path to the folder is %ProgramFiles%\One Identity\Defender\Management Portal\WWW\Areas\Reports\Generators.

2. Add the following lines to the **mappath.ini** text file held in the **Generators** folder:

   [Diagnostics]

   Enabled=1

The path to the log file is %ProgramData%\One Identity\Defender\Diagnostics\DefenderReports.txt.

To disable diagnostic logging for Management Portal (reports), remove these lines from the **mappath.ini** file:

```
[Diagnostics]
Enabled=1
```

Management Shell

To enable diagnostic logging for Management Shell

- On a computer where Management Shell is installed, use Registry Editor to create the following value in the **HKLM\SOFTWARE\PassGo Technologies\Defender** registry key:

  Value type: REG_DWORD

  Value name: **PSDiagnostics**

  Value data: **1**

The path to the log file is %ProgramData%\One Identity\Defender\Diagnostics\MgmtShell.txt.

To disable diagnostic logging for Management Shell, delete the **PSDiagnostics** value from the **Defender** registry key, or set the value data to **0**.

Service Connection Point

To troubleshoot issues that may occur with the Log Receiver component of the Management Portal, you need to enable diagnostic logging for the Service Connection Point component.

To enable diagnostic logging for the Service Connection Point component

- The Management Portal is installed or on the corresponding Defender Security Server computers, use Registry Editor to create the following value in the **HKLM\SOFTWARE\PassGo Technologies\Defender** registry key:

  Value type: REG_DWORD

  Value name: **SCP Diagnostics**

  Value data: **1**

The path to the log file is %ProgramData%\One Identity\Defender\Diagnostics\scp.txt.

To disable diagnostic logging for the Service Connection Point component, delete the **SCP Diagnostics** value from the **Defender** registry key, or set the value data to **0**.

Soft Token for Windows

To enable diagnostic logging for Soft Token for Windows on a 32-bit (x86) system

- On a 32-bit computer where Soft Token for Windows is installed, use Registry Editor to create the following value in the **HKLM\SOFTWARE\PassGo Technologies\PassGo Desktop Token** registry key:

  Value type: REG_DWORD

  Value name: **Diagnostics**

  Value data: **1**

To enable diagnostic logging for Soft Token for Windows on a 64-bit (x64) system

- On a 64-bit computer where Soft Token for Windows is installed, use Registry Editor to create the following value in the **HKLM\SOFTWARE\Wow6432Node\PassGo Technologies\PassGo Desktop Token** registry key:

  Value type: REG_DWORD

  Value name: **Diagnostics**

  Value data: **1**

The path to the log file is %ProgramData%\One Identity\Defender\Diagnostics\Defender Desktop Token.txt.

To disable diagnostic logging for Soft Token for Windows, delete the **Diagnostics** value from the **PassGo Desktop Token** registry key, or set the value data to **0**.

Token Import

Diagnostic logging for the token import operations is turned on by default. The path to the log file is %ProgramData%\One Identity\Defender\Diagnostics\Token Import\Token Import.txt on the computer where Defender Administration Console is installed.

Token Programming

Diagnostic logging for the token programming operations is turned on by default. The path to the log file is %ProgramData%\One Identity\Defender\Diagnostics\Token Programming\Token Programming.txt.

VPN Integrator

To enable diagnostic logging for VPN Integrator

1. On a computer where VPN Integrator is installed, go to the VPN Integrator installation directory.

   Normally, the path to the VPN Integrator installation directory is %ProgramFiles%\One Identity\Defender\VPN Integrator.

2. Add the following lines to the **pgwc.ini** text file held in the VPN Integrator installation directory, replacing <*logpath*> with the path to the folder that will hold the VPN Integrator log files:

   trace level = 9

   trace filename = <*logpath*>

   For example, with "trace filename = C:\pgvc_trace", the log files are held in the folder C:\pgvc_trace.

To disable diagnostic logging for VPN Integrator, remove these lines from the **pgwc.ini** file:

trace level = 9

trace filename = <*logpath*>

Web Service API

To enable diagnostic logging for Web Service API

1. On a computer with Web Service API, go to the Web Service API installation directory.

   Normally, the path to the Web Service API installation directory is %ProgramFiles%\One Identity\Defender\Web Service API.

2. Make the following changes to the **DefenderAdminService.exe.config** text file held in the Web Service API installation directory:

   - In the <log4net debug="false"> entry, set the value to "true": <log4net debug="true">
   - In the <level value="ERROR" /> entry, set the value to "DEBUG": <level value="DEBUG" />

You can find the log file **DefenderWebServiceApi.txt** in the **Logs** folder in the Web Service API installation directory. Normally, the path to the log file is %ProgramFiles%\One Identity\Defender\Web Service API\Logs\DefenderWebServiceApi.txt.

To disable diagnostic logging for Web Service API, set these values in the **DefenderAdminService.exe.config** file:

- <log4net debug="false">
- <level value="ERROR" />

Product information tool

The Product Information tool is a diagnostic tool that helps to gather product details. The tool is available at **%ProgramFiles%\Common Files\One Identity\Defender**.

To run the tool:

- Go to the location **%ProgramFiles%\Common Files\One Identity\Defender**.
- Double-click **ProductInfo.exe**.

  The details are generated as text files in the location **%ProgramData% \One Identity\Defender\Diagnostics\ProductInfoLogs**. The generated files are F**ileInfo[*timestamp*].txt** and **SystemInfo [*timestamp*].txt**.

Appendix B: Troubleshooting common authentication issues

If users are experiencing problems authenticating via Defender, there are a number of possible causes, ranging from VPN issues through to individual token failures. To help identify the cause, the information below is useful to collect and send to One Identity Software Support, providing important contextual and diagnostic information.

- Step 1: Gather required information
- Step 2: Analyze Defender Security Server log
- Step 3: Gather further diagnostics

Step 1: Gather required information

Answers to the following questions can help you get the required information about the authentication issues:

- What error message is the user receiving? Ask the user to provide the full error message text (make a screenshot).
- How many users are affected? The total number of Defender users is also useful to put into context.
- Were the affected users working previously? If so, when?
- What token types are the affected users using?

- What Defender Security Server version and platform are being used?
- When did the issue start occurring? It is useful to have a time approximation to help match up with the logs.
- Have any changes been made recently? For example to any Defender components, Active Directory, VPN server, or network.

Obtain the log files from the following location on the Defender Security Server:

%ProgramFiles%\One Identity\Defender\Security Server\Logs

Additionally, obtain user IDs of several affected users. These are required to locate information related to the affected users in the Defender log files. Make sure to obtain the user IDs, not the user names.

Step 2: Analyze Defender Security Server log

The default location for the Defender Security Server log files is %ProgramFiles%\One Identity\Defender\Security Server\Logs.

To analyse the Defender Security Server log files, take the following actions:

1. Locate an affected user in the Defender Security Server log files by searching for the user's ID. Each request received by the Defender Security Server is recorded in the log files. The example log messages in this section show records for a user whose user ID is testuser.
2. If the user ID cannot be found in the log, then verify that any deployed VPN servers are functioning correctly. The log message shown below would be seen for each request received by Defender regardless of whether or not it was successful.

   ```
   <Time> Radius request: Access-Request for <User Id> from <Client IP> through
   NAS:<Access Node Name> Request ID: <N/A> Session ID: <Unique Session ID>
   ```

3. Using the Unique Session ID, cycle through the log messages associated with the user's session. For example a successful session will look like this:

   ```
   Tue 18 Aug 2009 11:57:10 Radius Request from 192.168.10.106:2951 Request ID: 31
   Tue 18 Aug 2009 11:57:10 Radius request: Access-Request for testuser from
   192.100.10.106:2951 through NAS:WebMail Request ID: 31 Session ID: 8A89040F
   Tue 18 Aug 2009 11:57:10 User testuser authenticated with Active Directory
   Password Session ID:8A89040F
   Tue 18 Aug 2009 11:57:10 Radius response: Authentication Acknowledged User-Name:
   testuser, Request ID: 31 Session ID: 8A89040F
   ```

4. Locate the relevant error message reason in the table below and take the recommended actions.

Table 37:
Reasons Defender Security Server log error messages

Message	Meaning	Recommended actions

`Reason: Invalid response`
`Radius response: Authentication rejected`
`User-Name: testuser`
	Incorrect token response.	• Verify the correct response is being entered.
		• Check the response in the administration console.
		• Check if PIN configured for user.

`Reason: Account locked out due to invalid attempts`
`Radius response: Authentication Rejected`
`User-Name: testuser`
	User's account is locked in Defender.	Use the Defender Administration Console to reset violation count for the user.

`Reason: Invalid password`
`Radius response: Authentication Rejected`
`User-Name: testuser`
	Incorrect Active Directory password.	Verify the correct password is being entered.

`authentication abandoned user testuser`	Session timed out while waiting for user response.	Verify connectivity between the client and the Defender Security Server on the configured RADIUS port.

`Reason: User not valid for this route`
`Radius response: Authentication Rejected`
`User-Name: testuser`
	This message can be caused by one of the following:
	• User is not a membe-
		• Verify the members of the Access Node.
		• Verify the user has a Defender

Message	Meaning	Recommended actions
	r of the Access Node. • User does not have a token. • User is not a Defend-er user. • There is no license avail-able for the user. • Client IP not permit-ted by the Access Node.	token assigned. • Verify that suitable licenses exist. • Verify the IP.
`Domain Search from CN=testuser,CN=Users,DC=child,DC=democorp,DC=local took 57 seconds` `LDAP failed (-1)finding user testuser`	Active Directory search has failed. This can happen if, for example, the child domain is unavailable.	Verify that the Defender service account has sufficient permissions or is a member of the Domain Administrators group.
`LDAP failed (50) writing token data for CN=PDWIN1348400003,OU=Tokens,OU=Defender,DC=democorp,DC=local` `Failed to write token data to LDAP`	The Defender service account does not have sufficient permissions in Active	Verify that the Defender service account has sufficient permissions or is a member of the Domain

Message	Meaning	Recommended actions
	Directory to update the user's token information.	Administrators group.

Step 3: Gather further diagnostics

If Step 1: Gather required information and Step 2: Analyze Defender Security Server log have not resolved the issue, further diagnostics may be required, including collecting environmental details and tracing. Contact One Identity Support for advice on how to enable tracing. You will need to provide the version number of the Defender Administration Console and Defender Security Server you are using. Normally, you can find the Defender trace files in the following location: %ProgramData%\One Identity\Diagnostics.

Appendix C: Troubleshooting DIGIPASS token issues

Steps to troubleshoot DIGIPASS hardware token issues are:

- Step 1: Determine type of failure
- Step 2: Verify Defender configuration
- Step 3: Gather further diagnostics

Step 1: Determine type of failure

1. Determine if this is a token hardware failure.

   If the answer is Yes to any of the next questions, refer to the steps described in One Identity Knowledge Article SOL45444 "Defender token failures".

   - Does the token only display **000000**?
   - Is the token display blank when the token button is pressed?
   - Is the token display intermittent?
   - Does the token display the same number every time? Note that the number is set to change every 36 seconds.

- Does the token display **batt x**, where x indicates the number of months the battery has left?

If the answer to the above questions is No, go to the next step.

2. Does the token display **dp G0 7** before a number is displayed?

   If so, this means the token is set to display it's type, that is, DIGIPASS GO 7, before the number. This is not an error. Ask the user to log on with the number displayed. If this is not successful, go to the next step.

   If a six digit number is displayed immediately, go to the next step.

3. If a token number is displayed as expected, but logon fails, further investigation within Defender and Active Directory may be required.

   Gather and record the following information:

   - Has the user ever successfully logged on with this token, if so, when was the last time the user successfully logged on with the token?
   - What are the user ID and the token serial number?
   - What is the error the user sees when they try to log on?

Step 2: Verify Defender configuration

If a hardware issue has been ruled out by the previous troubleshooting steps, and user logon is failing, refer to the steps below. Typically the user will receive the message "invalid synchronous response". This may have a number of causes. Follow the process of elimination below to help diagnose the error.

1. Check the token violation count and reset if necessary by using the **Properties** dialog box provided for the user in the Active Directory Users and Computers tool (use the **Defender** tab). Re-test user authentication. Ask the user to retry their token.

   If the issue persists, go to the next step.

2. Check for the use of a PIN on the token. It may be that the user has forgotten to use the PIN or is using an invalid PIN. Reset PIN if necessary. Ask the user to retry their token.

   If the issue persists, go to the next step.

3. Reset the token by using the **Properties** dialog box provided for the user in the Active Directory Users and Computers tool (use the **Defender** tab). Ask the user to retry their token.

   If the issue persists, go to the next step.

4. If the user receives an "Access denied" message, make sure the user's account is listed on the **Members** tab of the corresponding Access Node, or that the user's account is a member of a group listed for the Access Node. If the user is not defined, the Defender Security Server log includes the error message "User not valid for this route".

If the issue is not resolved by adding the user to the Access Node, go to the next step.

5. Unassign and then re-assign the token to the user. Re-test user authentication.

Step 3: Gather further diagnostics

If Step 1: Determine type of failure and Step 2: Verify Defender configuration have not resolved the issue, further diagnostics may be required.

The following information may be useful to help diagnosis of the issue when raising a case with One Identity Support.

Default location of the Defender Security Server log files

%ProgramFiles%\One Identity\Defender\Security Server\Logs.

User and token information that may be required

- Confirmation of token type and serial number.
- What is the user ID of the user affected?
- Which organizational unit stores the user's account in Active Directory?
- Does the user have more than one token assigned to their account?
- Has the user ever successfully logged on with this token? If so, when was the last time the user successfully logged on with the token?
- What is the error the user sees when they try to log on?
- Do other or all users authenticating via the same route (for example, VPN) experience the same issue?
- Can a helpdesk response be assigned for this user successfully?

Test token

Test the token response in the Active Directory Users and Computers tool: Open the **Properties** dialog box for the user, click the **Defender** tab, select token, click **Test**, and then enter the token response from the token.

Appendix D: Defender classes and attributes in Active Directory

This appendix provides information about the following Microsoft Active Directory schema object classes and attributes:

- Classes defined by Defender
- Classes extended by Defender
- Attributes defined by Defender

Classes defined by Defender

The following is the list of Microsoft Active Directory schema classes that are specifically defined by Defender. Each class has been listed in accordance with the Active Directory schema definitions format as used in the MSDN documentation (for further details, see information on Active Directory Schema published in MSDN at http://msdn.microsoft.com/en-us/library/ms675085(VS.85).aspx). Only attributes that are specific to Defender have been listed; all other attributes are as per the MSDN documentation provided for each respective subclass.

In this section:

defender-tokenClass

- **CN** defender-tokenClass
- **Ldap-Display-Name** defender-tokenClass
- **Governs-Id** 1.2.840.113556.1.8000.1267.1.1
- **Object-Category** 1
- **Subclass of** Leaf
- **Possible Superiors** Organizational-Unit
- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Records of this type are updated each time a Defender token is created, deleted, or modified.
- **Description** A record of this type is created for each token defined to Defender.

This class contains the following attributes:

Table 38: defender-tokenClass attributes

Attribute	Mandatory
defender-id	False

Attribute	Mandatory
defender-tokenData	False
defender-tokenDate	False
defender-tokenType	False
defender-tokenUsersDNs	False

defender-danClass

- **CN** defender-danClass
- **Ldap-Display-Name** defender-danClass
- **Governs-Id** 1.2.840.113556.1.8000.1267.1.2
- **Object-Category** 1
- **Subclass of** Leaf
- **Possible Superiors** Organizational-Unit
- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Records of this type are updated each time an Access Node is created, deleted, or modified.
- **Description** A record of this type is created for each Access Node defined to Defender.

This class contains the following attributes:

Table 39:
defender-danClass attributes

Attribute	Mandatory
defender-danKey	False
defender-danMembers	False
defender-danType	False
defender-dssDNs	False
defender-policy	False
defender-radiusPayloadDn	False
defender-radiusPayloadInherit	False
defender-subnetMask	False
defender-userIdType	False

defender-dssClass

- **CN** defender-dssClass
- **Ldap-Display-Name** defender-dssClass
- **Governs-Id** 1.2.840.113556.1.8000.1267.1.3
- **Object-Category** 1
- **Subclass of** Leaf
- **Possible Superiors** Organizational-Unit
- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Record of this type are updated each time a Defender Security Server (DSS) is created, deleted, or modified.
- **Description** A record of this type is created for each Defender Security Server (DSS) defined to Defender.

This class contains the following attributes:

Table 40:
defender-dssClass attributes

Attribute	Mandatory
defender-dssMembers	False
defender-dssVersion	False
defender-objectActive	False
defender-policy	False
defender-prompts	False
defender-radiusPayloadDn	False

defender-policyClass

- **CN** defender-policyClass
- **Ldap-Display-Name** defender-policyClass
- **Governs-Id** 1.2.840.113556.1.8000.1267.1.4
- **Object-Category** 1
- **Subclass of** Leaf
- **Possible Superiors** Organizational-Unit
- **Update Privilege** Domain or Defender administrator

- **Update Frequency** Records of this type are updated each time a Defender Security Policy is created, deleted, or modified.
- **Description** A record of this type is created for each Defender Security Policy defined in Defender.

This class contains the following attributes:

Table 41:
defender-policyClass attributes

Attribute	Mandatory
defender-accessCategories	False
defender-authMethods	False
defender-lockoutDuration	False
defender-lockoutThreshold	False
defender-policyAutoUnlock	False
defender-policyGINAOptions	False
defender-policyLoginTimes	False
defender-policyMaximumPasswordAge	False
defender-policyMaximumPINAge	False
defender-policyMembers	False
defender-policyMobileUsers	False
defender-policyPasswordChangeFlags	False
defender-policyPasswordFilter	False

defender-licenseClass

- **CN** defender-licenseClass
- **Ldap-Display-Name** defender-licenseClass
- **Governs-Id** 1.2.840.113556.1.8000.1267.1.5
- **Object-Category** 1
- **Subclass of** Leaf
- **Possible Superiors** Organizational-Unit
- **Update Privilege** Domain or Defender administrator

- **Update Frequency** Records of this type are updated each time a Defender license is created, deleted, or modified.
- **Description** A record of this type is created for each license defined in Defender.

This class contains the following attributes:

Table 42:
defender-licenseClass attributes

Attribute	Mandatory
defender-tokenData	False

defender-radiusPayloadClass

- **CN** defender-radiusPayloadClass
- **Ldap-Display-Name** defender-radiusPayloadClass
- **Governs-Id** 1.2.840.113556.1.8000.1267.1.6
- **Object-Category** 1
- **Subclass of** Leaf
- **Possible Superiors** Organizational-Unit
- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Record of this type are updated each time a Defender RADIUS payload is created, deleted, or modified.
- **Description** A record of this type is created for each RADIUS payload defined to Defender.

This class contains the following attributes:

Table 43:
defender-radiusPayloadClass attributes

Attribute	Mandatory
defender-radiusPayloadData	False
defender-radiusPayloadGroups	False
defender-radiusPayloadGroupsDN	False
defender-radiusPayloadMembers	False

defender-tokenLicenseClass

- **CN** defender-tokenLicenseClass
- **Ldap-Display-Name** defender-tokenLicenseClass
- **Governs-Id** 1.2.840.113556.1.8000.1267.1.7
- **Object-Category** 1
- **Subclass of** Leaf
- **Possible Superiors** Organizational-Unit
- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Record of this type are updated each time a Defender token license is created, deleted, or modified.
- **Description** A record of this type is created for each token license defined in Defender.

This class contains the following attributes:

Table 44:
defender-tokenLicenseClass attributes

Attribute	Mandatory
defender-tokenData	False
defender-tokenType	False

Classes extended by Defender

The following is the list of Microsoft Active Directory schema classes that are extended by Defender. Each class has been listed in accordance with the Active Directory schema definitions format as used in the MSDN documentation (for further details, see information on Active Directory Schema published in MSDN at http://msdn.microsoft.com/en-us/library/ms675085(VS.85).aspx). Only attributes that are specific to Defender have been listed; all other attributes are as per the MSDN documentation provided for each extended class specified.

In this section:

- Group
- User

Group

- **CN** Group
- **Ldap-Display-Name** Group
- **Governs-Id** 1.2.840.113556.1.5.8

Defender extends this class to include the following attributes:

Table 45:
Group attributes added by Defender

Attribute	Mandatory
defender-danDNs	False
defender-policy	False
defender-radiusPayloadDn	False
defender-radiusPayloadInherit	False
defender-radiusPayloadGroupsDN	False

User

- **CN** User
- **Ldap-Display-Name** user

Governs-Id 1.2.840.113556.1.5.9

Defender extends this class to include the following attributes:

Table 46:
User attributes added by Defender

Attribute	Mandatory
defender-danDNs	False
defender-id	False
defender-lastLogon	False
defender-lockoutTime	False
defender-policy	False

Attribute	Mandatory
defender-radiusPayloadDn	False
defender-radiusPayloadInherit	False
defender-resetCount	False
defender-tokenUsersDNs	False
defender-userTokenData	False
defender-violationCount	False

Attributes defined by Defender

The following is the list of Microsoft Active Directory schema attributes that are defined by Defender. Each attribute has been listed in accordance with the Active Directory schema definitions format as used in the MSDN documentation (for further details, see information on Active Directory Schema published in MSDN at http://msdn.microsoft.com/en-us/library/ms675085(VS.85).aspx). Only attributes that are specific to Defender have been listed; all other attributes are as per the MSDN documentation.

In this section:

- defender-tokenType
- defender-tokenData
- defender-userTokenData
- defender-tokenUsersDNs
- defender-tokenDate
- defender-dssDNs
- defender-dssMembers
- defender-danKey
- defender-id
- defender-violationCount
- defender-resetCount
- defender-lastLogon
- defender-objectActive
- defender-prompts
- defender-authMethods
- defender-lockoutThreshold
- defender-lockoutDuration
- defender-lockoutTime

- defender-policy
- defender-policyMembers
- defender-danType
- defender-userIdType
- defender-accessCategories
- defender-subnetMask
- defender-danMembers
- defender-danDNs
- defender-dssVersion
- defender-radiusPayloadDn
- defender-radiusPayloadMembers
- defender-radiusPayloadData
- defender-radiusPayloadGroups
- defender-radiusPayloadGroupsDN
- defender-radiusPayloadInherit
- defender-policyAutoUnlock
- defender-policyMobileUsers
- defender-policyMaximumPasswordAge
- defender-policyMaximumPINAge
- defender-policyPasswordChangeFlags
- defender-policyPasswordFilter
- defender-policyGINAOptions
- defender-policyLoginTimes
- defender-notificationId

defender-tokenType

- **CN** defender-tokenType
- **Ldap-Display-Name** defender-tokenType
- **Attribute-Id** 1.2.840.113556.1.8000.1267.2.1
- **Link-Id** -
- **Range-Lower** -
- **Range-Upper** -
- **Size** -
- **Syntax** Integer

- **Is-Single-Valued** True
- **Is-Indexed** True
- **In Global Catalog** False
- **Search-Flags** 0x00000003
- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Whenever a token or token license is created.
- **Description** For a token, contains the major token type. For a token license, contains the license type.
- **Classes used in** defender-tokenClass, defender-tokenLicenseClass

defender-tokenData

- **CN** defender-tokenData
- **Ldap-Display-Name** defender-tokenData
- **Attribute-Id** 1.2.840.113556.1.8000.1267.2.2
- **Link-Id** -
- **Range-Lower** -
- **Range-Upper** -
- **Size** -
- **Syntax** String(Octet)
- **Is-Single-Valued** False
- **Is-Indexed** False
- **In Global Catalog** False
- **Search-Flags** 0x00000000
- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Whenever token data is added or modified.
- **Description** For a token contains the token seed and other information required for authentication. For licenses contains information on the license type and—in the case of a token license—the counts of used and available tokens.
- **Classes used in** defender-tokenClass, defender-tokenLicenseClass, defender-licenseClass

defender-userTokenData

- **CN** defender-userTokenData
- **Ldap-Display-Name** defender-userTokenData

- **Attribute-Id** 1.2.840.113556.1.8000.1267.2.2.1
- **Link-Id** 11962
- **Range-Lower** -
- **Range-Upper** -
- **Size** -
- **Syntax** Object(DN-Binary)
- **Is-Single-Valued** False
- **Is-Indexed** False
- **In Global Catalog** True
- **Search-Flags** 0x00000000
- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Whenever a Token is assigned to or removed from a user.
- **Description** Contains the user specific data associated with a token, together with the tokens' distinguished name.
- **Classes used in** User

defender-tokenUsersDNs

- **CN** defender-tokenUsersDNs
- **Ldap-Display-Name** defender-tokenUsersDNs
- **Attribute-Id** 1.2.840.113556.1.8000.1267.2.2.2
- **Link-Id** 11963
- **Range-Lower** -
- **Range-Upper** -
- **Size** -
- **Syntax** Object(DS-DN)
- **Is-Single-Valued** False
- **Is-Indexed** False
- **In Global Catalog** False
- **Search-Flags** 0x00000010
- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Whenever a token is assigned to or removed from a user.
- **Description** For a token, contains the distinguished names of Users assigned to the token. For a user, this attribute is set when the user is assigned a Defender password or GrIDsure token.
- **Classes used in** defender-tokenLicenseClass, User

defender-tokenDate

- **CN** defender-tokenDate
- **Ldap-Display-Name** defender-tokenDate
- **Attribute-Id** 1.2.840.113556.1.8000.1267.2.4
- **Link-Id** -
- **Range-Lower** -
- **Range-Upper** -
- **Size** 8 Bytes
- **Syntax** String(Generalized-Time)
- **Is-Single-Valued** True
- **Is-Indexed** False
- **In Global Catalog** False
- **Search-Flags** 0x00000000
- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Whenever a date change occurs for a token.
- **Description** Contains date information associated with the token. This may be the manufacturing date of the token or the date of token import.
- **Classes used in** defender-tokenClass

defender-dssDNs

- **CN** defender-dssDNs
- **Ldap-Display-Name** defender-dssDNs
- **Attribute-Id** 1.2.840.113556.1.8000.1267.2.5
- **Link-Id** 11964
- **Range-Lower** -
- **Range-Upper** -
- **Size** -
- **Syntax** Object(DS-DN)
- **Is-Single-Valued** False
- **Is-Indexed** False
- **In Global Catalog** True
- **Search-Flags** 0x00000000
- **Update Privilege** Domain or Defender administrator

- **Update Frequency** Whenever an Access Node is added to or removed from a Defender Security Server.
- **Description** Contains the distinguished names of the Defender Security Server objects to which the Access Node is assigned.
- **Classes used in** defender-danClass

defender-dssMembers

- **CN** defender-dssMembers
- **Ldap-Display-Name** defender-dssMembers
- **Attribute-Id** 1.2.840.113556.1.8000.1267.2.6
- **Link-Id** 11965
- **Range-Lower** -
- **Range-Upper** -
- **Size** -
- **Syntax** Object(DS-DN)
- **Is-Single-Valued** False
- **Is-Indexed** False
- **In Global Catalog** False
- **Search-Flags** 0x00000010
- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Whenever an Access Node is added to or removed from a Defender Security Server.
- **Description** Contains the distinguished names of the Access Node objects assigned to the Defender Security Server.
- **Classes used in** defender-danClass

defender-danKey

- **CN** defender-danKey
- **Ldap-Display-Name** defender-danKey
- **Attribute-Id** 1.2.840.113556.1.8000.1267.2.7
- **Link-Id** -
- **Range-Lower** -
- **Range-Upper** -
- **Size** -

- **Syntax** String(Octet)
- **Is-Single-Valued** True
- **Is-Indexed** False
- **In Global Catalog** False
- **Search-Flags** 0x00000000
- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Whenever an Access Node is added or deleted.
- **Description** Contains the shared secret for the Access Node.
- **Classes used in** defender-danClass

defender-id

- **CN** defender-id
- **Ldap-Display-Name** defender-id
- **Attribute-Id** 1.2.840.113556.1.8000.1267.2.9
- **Link-Id** -
- **Range-Lower** -
- **Range-Upper** -
- **Size** -
- **Syntax** String(Unicode)
- **Is-Single-Valued** True
- **Is-Indexed** True
- **In Global Catalog** True
- **Search-Flags** 0x00000003
- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Whenever a new object is created, or the Id of an existing object is the modified.
- **Description** For a token, contains the type information for Defender soft tokens only. For a user, contains the user's Defender ID.
- **Classes used in** defender-tokenClass, User

defender-violationCount

- **CN** defender-violationCount
- **Ldap-Display-Name** defender-violationCount
- **Attribute-Id** 1.2.840.113556.1.8000.1267.2.10

- **Link-Id** -
- **Range-Lower** -
- **Range-Upper** -
- **Size** -
- **Syntax** Integer
- **Is-Single-Valued** True
- **Is-Indexed** False
- **In Global Catalog** False
- **Search-Flags** 0x00000000
- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Whenever an unsuccessful authentication attempt occurs.
- **Description** Contains the number of unsuccessful authentication attempts since last reset.
- **Classes used in** User

defender-resetCount

- **CN** defender-resetCount
- **Ldap-Display-Name** defender-resetCount
- **Attribute-Id** 1.2.840.113556.1.8000.1267.2.11
- **Link-Id** -
- **Range-Lower** -
- **Range-Upper** -
- **Size** -
- **Syntax** Integer
- **Is-Single-Valued** True
- **Is-Indexed** False
- **In Global Catalog** False
- **Search-Flags** 0x00000000
- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Whenever a user's violation count is reset via Defender.
- **Description** Contains the number of violation count resets.
- **Classes used in** User

defender-lastLogon

- **CN** defender-lastLogon
- **Ldap-Display-Name** defender-lastLogon
- **Attribute-Id** 1.2.840.113556.1.8000.1267.2.12
- **Link-Id** -
- **Range-Lower** -
- **Range-Upper** -
- **Size** 8 Bytes
- **Syntax** Interval
- **Is-Single-Valued** True
- **Is-Indexed** False
- **In Global Catalog** False
- **Search-Flags** 0x00000000
- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Whenever a user successfully authenticates via Defender.
- **Description** Contains the time of the last successful Defender authentication.
- **Classes used in** User

defender-objectActive

- **CN** defender-objectActive
- **Ldap-Display-Name** defender-objectActive
- **Attribute-Id** 1.2.840.113556.1.8000.1267.2.13
- **Link-Id** -
- **Range-Lower** -
- **Range-Upper** -
- **Size** -
- **Syntax** Boolean
- **Is-Single-Valued** True
- **Is-Indexed** False
- **In Global Catalog** False
- **Search-Flags** 0x00000000
- **Update Privilege** Domain or Defender administrator

- **Update Frequency** Whenever a Defender Security Server changes its state (for example, from active to inactive or vice versa).
- **Description** Flag to indicate whether or not the Defender Security Server has up-to-date configuration data.
- **Classes used in** defender-dssClass

defender-prompts

- **CN** defender-prompts
- **Ldap-Display-Name** defender-prompts
- **Attribute-Id** 1.2.840.113556.1.8000.1267.2.14
- **Link-Id** -
- **Range-Lower** -
- **Range-Upper** -
- **Size** -
- **Syntax** String(Unicode)
- **Is-Single-Valued** False
- **Is-Indexed** False
- **In Global Catalog** False
- **Search-Flags** 0x00000000
- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Whenever a Defender Security Server prompt is added, modified, or deleted.
- **Description** Contains the list of authentication prompts used by the Defender Security Server during authentication.
- **Classes used in** defender-policyClass

defender-authMethods

- **CN** defender-authMethods
- **Ldap-Display-Name** defender-authMethods
- **Attribute-Id** 1.2.840.113556.1.8000.1267.2.15
- **Link-Id** -
- **Range-Lower** -
- **Range-Upper** -
- **Size** -

- **Syntax** String(Octet)
- **Is-Single-Valued** True
- **Is-Indexed** False
- **In Global Catalog** False
- **Search-Flags** 0x00000000
- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Whenever the authentication method associated with a Defender Security Policy is modified.
- **Description** Data structure describing the types of authentication methods applicable to users associated with this Defender Security Policy.
- **Classes used in** defender-policyClass

defender-lockoutThreshold

- **CN** defender-lockoutThreshold
- **Ldap-Display-Name** defender-lockoutThreshold
- **Attribute-Id** 1.2.840.113556.1.8000.1267.2.16
- **Link-Id** -
- **Range-Lower** -
- **Range-Upper** -
- **Size** -
- **Syntax** Integer
- **Is-Single-Valued** True
- **Is-Indexed** False
- **In Global Catalog** False
- **Search-Flags** 0x00000000
- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Whenever the lockout duration associated with a Defender Security Policy is modified.
- **Description** Contains the number of unsuccessful authentication attempts before account gets locked.
- **Classes used in** defender-policy

defender-lockoutDuration

- **CN** defender-lockoutDuration
- **Ldap-Display-Name** defender-lockoutDuration
- **Attribute-Id** 1.2.840.113556.1.8000.1267.2.17
- **Link-Id** -
- **Range-Lower** -
- **Range-Upper** -
- **Size** -
- **Syntax** Integer
- **Is-Single-Valued** True
- **Is-Indexed** False
- **In Global Catalog** False
- **Search-Flags** 0x00000000
- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Whenever the lockout duration associated with a Defender Security Policy is modified.
- **Description** Contains the duration for which a user account (which has been locked by Defender) remains locked. After this period has expired the account becomes eligible for unlocking.
- **Classes used in** defender-policy

defender-lockoutTime

- **CN** defender-lockoutTime
- **Ldap-Display-Name** defender-lockoutTime
- **Attribute-Id** -
- **Link-Id** -
- **Range-Lower** -
- **Range-Upper** -
- **Size** 8 Bytes
- **Syntax** Interval
- **Is-Single-Valued** True
- **Is-Indexed** False
- **In Global Catalog** False
- **Search-Flags** 0x00000000

- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Whenever a user account is locked by Defender.
- **Description** Contains the time at which the user was locked by Defender.
- **Classes used in** User

defender-policy

- **CN** defender-policy
- **Ldap-Display-Name** defender-policy
- **Attribute-Id** 1.2.840.113556.1.8000.1267.2.19
- **Link-Id** 11960
- **Range-Lower** -
- **Range-Upper** -
- **Size** -
- **Syntax** Object(DS-DN)
- **Is-Single-Valued** True
- **Is-Indexed** False
- **In Global Catalog** True
- **Search-Flags** 0x00000000
- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Whenever a Defender Security Policy is assigned.
- **Description** Contains the distinguished name of the Defender Security Policy assigned to the object.
- **Classes used in** defender-dssClass, defender-danClass, Group, User

defender-policyMembers

- **CN** defender-policyMembers
- **Ldap-Display-Name** defender-policyMembers
- **Attribute-Id** 1.2.840.113556.1.8000.1267.2.20
- **Link-Id** 11961
- **Range-Lower** -
- **Range-Upper** -
- **Size** -
- **Syntax** Object(DS-DN)

- **Is-Single-Valued** False
- **Is-Indexed** False
- **In Global Catalog** False
- **Search-Flags** 0x00000010
- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Whenever a Defender Security Policy is assigned.
- **Description** Contains the distinguished names of the objects to which this Defender Security Policy is assigned.
- **Classes used in** defender-policyClass

defender-danType

- **CN** defender-danType
- **Ldap-Display-Name** defender-danType
- **Attribute-Id** 1.2.840.113556.1.8000.1267.2.21
- **Link-Id** -
- **Range-Lower** -
- **Range-Upper** -
- **Size** -
- **Syntax** Integer
- **Is-Single-Valued** True
- **Is-Indexed** False
- **In Global Catalog** False
- **Search-Flags** 0x00000000
- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Whenever an Access Node is created.
- **Description** Contains the type of the Access Node.
- **Classes used in** defender-danClass

defender-userIdType

- **CN** defender-userIdType
- **Ldap-Display-Name** defender-userIdType
- **Attribute-Id** 1.2.840.113556.1.8000.1267.2.22
- **Link-Id** -

- **Range-Lower** -
- **Range-Upper** -
- **Size** -
- **Syntax** Integer
- **Is-Single-Valued** True
- **Is-Indexed** False
- **In Global Catalog** False
- **Search-Flags** 0x00000000
- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Whenever the UserId type associated with the Access Node changes.
- **Description** Contains the format of the user ID used for authentication through the Access Node.
- **Classes used in** defender-danClass

defender-subnetMask

- **CN** defender-subnetMask
- **Ldap-Display-Name** defender-subnetMask
- **Attribute-Id** 1.2.840.113556.1.8000.1267.2.24
- **Link-Id** -
- **Range-Lower** -
- **Range-Upper** -
- **Size** -
- **Syntax** Integer
- **Is-Single-Valued** True
- **Is-Indexed** False
- **In Global Catalog** False
- **Search-Flags** 0x00000000
- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Whenever the IP subnet mask of an Access Node changes.
- **Description** Contains the IP subnet mask associated with an Access Node.
- **Classes used in** defender-danClass

defender-accessCategories

- **CN** defender-accessCategories
- **Ldap-Display-Name** defender-accessCategories
- **Attribute-Id** 1.2.840.113556.1.8000.1267.2.23
- **Link-Id** -
- **Range-Lower** -
- **Range-Upper** -
- **Size** -
- **Syntax** Integer
- **Is-Single-Valued** True
- **Is-Indexed** False
- **In Global Catalog** False
- **Search-Flags** 0x00000000
- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Whenever a Defender Security Policy access category changes.
- **Description** Contains the access categories required for Webthority.
- **Classes used in** defender-policyClass

defender-danMembers

- **CN** defender-danMembers
- **Ldap-Display-Name** defender-danMembers
- **Attribute-Id** 1.2.840.113556.1.8000.1267.2.25
- **Link-Id** 11966
- **Range-Lower** -
- **Range-Upper** -
- **Size** -
- **Syntax** Object(DS-DN)
- **Is-Single-Valued** False
- **Is-Indexed** False
- **In Global Catalog** True
- **Search-Flags** 0x00000000
- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Whenever a user is added to or removed from an Access Node.

- **Description** Contains the distinguished names of groups and users allowed to authenticate through the Access Node.
- **Classes used in** defender-danClass

defender-danDNs

- **CN** defender-danDNs
- **Ldap-Display-Name** defender-danDNs
- **Attribute-Id** 1.2.840.113556.1.8000.1267.2.26
- **Link-Id** 11967
- **Range-Lower** -
- **Range-Upper** -
- **Size** -
- **Syntax** Object(DS-DN)
- **Is-Single-Valued** False
- **Is-Indexed** False
- **In Global Catalog** False
- **Search-Flags** 0x00000010
- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Whenever a user is added to or removed from an Access Node.
- **Description** Contains the list of Access Nodes of which the user is a direct member.
- **Classes used in** Group, User

defender-dssVersion

- **CN** defender-dssVersion
- **Ldap-Display-Name** defender-dssVersion
- **Attribute-Id** 1.2.840.113556.1.8000.1267.2.27
- **Link-Id** -
- **Range-Lower** -
- **Range-Upper** -
- **Size** 8 Bytes
- **Syntax** Interval
- **Is-Single-Valued** True
- **Is-Indexed** False

- **In Global Catalog** False
- **Search-Flags** 0x00000000
- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Whenever a Defender Security Server is defined.
- **Description** Contains the version of the Defender Security Server.
- **Classes used in** defender-danClass

defender-radiusPayloadDn

- **CN** defender-radiusPayloadDn
- **Ldap-Display-Name** defender-radiusPayloadDn
- **Attribute-Id** 1.2.840.113556.1.8000.1267.2.28
- **Link-Id** 12780
- **Range-Lower** -
- **Range-Upper** -
- **Size** -
- **Syntax** Object(DS-DN)
- **Is-Single-Valued** True
- **Is-Indexed** False
- **In Global Catalog** True
- **Search-Flags** 0x00000000
- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Whenever a RADIUS payload is assigned.
- **Description** Contains the distinguished name of the assigned RADIUS payload.
- **Classes used in** defender-dssClass, defender-danClass, Group, User

defender-radiusPayloadMembers

- **CN** defender-radiusPayloadMembers
- **Ldap-Display-Name** defender-radiusPayloadMembers
- **Attribute-Id** 1.2.840.113556.1.8000.1267.2.29
- **Link-Id** 12781
- **Range-Lower** -
- **Range-Upper** -
- **Size** -

- **Syntax** Object(DS-DN)
- **Is-Single-Valued** False
- **Is-Indexed** False
- **In Global Catalog** False
- **Search-Flags** 0x00000010
- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Whenever a RADIUS payload is assigned.
- **Description** Contains the distinguished names of objects to which the RADIUS payload is assigned.
- **Classes used in** defender-radiusPayloadClass

defender-radiusPayloadData

- **CN** defender-radiusPayloadData
- **Ldap-Display-Name** defender-radiusPayloadData
- **Attribute-Id** 1.2.840.113556.1.8000.1267.2.30
- **Link-Id** -
- **Range-Lower** -
- **Range-Upper** -
- **Size** -
- **Syntax** String(Octet)
- **Is-Single-Valued** False
- **Is-Indexed** False
- **In Global Catalog** False
- **Search-Flags** 0x00000000
- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Whenever the data associated with a RADIUS payload is modified.
- **Description** Contains RADIUS Payload information.
- **Classes used in** defender-radiusPayloadClass

defender-radiusPayloadGroups

- **CN** defender-radiusPayloadGroups
- **Ldap-Display-Name** defender-radiusPayloadGroups
- **Attribute-Id** 1.2.840.113556.1.8000.1267.2.31

- **Link-Id** 12782
- **Range-Lower** -
- **Range-Upper** -
- **Size** -
- **Syntax** Object(DN-Binary)
- **Is-Single-Valued** False
- **Is-Indexed** False
- **In Global Catalog** True
- **Search-Flags** 0x00000000
- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Whenever the data associated with a group-specific RADIUS payload is modified.
- **Description** Contains the distinguished names of the groups referenced in the RADIUS payload.
- **Classes used in** defender-radiusPayloadClass

defender-radiusPayloadGroupsDN

- **CN** defender-radiusPayloadGroupsDN
- **Ldap-Display-Name** defender-radiusPayloadGroupsDN
- **Attribute-Id** 1.2.840.113556.1.8000.1267.2.32
- **Link-Id** 12783
- **Range-Lower** -
- **Range-Upper** -
- **Size** -
- **Syntax** Object(DS-DN)
- **Is-Single-Valued** False
- **Is-Indexed** False
- **In Global Catalog** False
- **Search-Flags** 0x00000010
- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Whenever the data associated with group-specific RADIUS payload is modified.
- **Description** Contains the distinguished names of the RADIUS payload objects in which this object is referenced.
- **Classes used in** defender-radiusPayloadClass, Group

defender-radiusPayloadInherit

- **CN** defender-radiusPayloadInherit
- **Ldap-Display-Name** defender-radiusPayloadInherit
- **Attribute-Id** 1.2.840.113556.1.8000.1267.2.33
- **Link-Id** -
- **Range-Lower** -
- **Range-Upper** -
- **Size** -
- **Syntax** Boolean
- **Is-Single-Valued** True
- **Is-Indexed** False
- **In Global Catalog** False
- **Search-Flags** 0x00000000
- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Whenever a RADIUS payload is to be inherited.
- **Description** Set if RADIUS payload information assigned to this object is to be inherited by other objects.
- **Classes used in** defender-danClass, Group, User

defender-policyAutoUnlock

- **CN** defender-policyAutoUnlock
- **Ldap-Display-Name** defender-policyAutoUnlock
- **Attribute-Id** 1.2.840.113556.1.8000.1267.2.34
- **Link-Id** -
- **Range-Lower** -
- **Range-Upper** -
- **Size** -
- **Syntax** Boolean
- **Is-Single-Valued** True
- **Is-Indexed** False
- **In Global Catalog** False
- **Search-Flags** 0x00000000
- **Update Privilege** Domain or Defender administrator

- **Update Frequency** Whenever the Auto Unlock setting of a Defender Security Policy is modified.
- **Description** Determines whether Defender accounts are automatically reset after a successful Defender authentication.
- **Classes used in** defender-policyClass

defender-policyMobileUsers

- **CN** defender-policyMobileUsers
- **Ldap-Display-Name** defender-policyMobileUsers
- **Attribute-Id** 1.2.840.113556.1.8000.1267.2.35
- **Link-Id** -
- **Range-Lower** -
- **Range-Upper** -
- **Size** -
- **Syntax** String(Octet)
- **Is-Single-Valued** True
- **Is-Indexed** False
- **In Global Catalog** False
- **Search-Flags** 0x00000000
- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Whenever the Mobile Users setting associated with a Defender Security Policy is modified.
- **Description** Contains the settings for the configuration of the SMS provider policy.
- **Classes used in** defender-policyClass

defender-policyMaximumPasswordAge

- **CN** defender-policyMaximumPasswordAge
- **Ldap-Display-Name** defender-policyMaximumPasswordAge
- **Attribute-Id** 1.2.840.113556.1.8000.1267.2.36
- **Link-Id** -
- **Range-Lower** -
- **Range-Upper** -
- **Size** 8 Bytes
- **Syntax** Interval

- **Is-Single-Valued** True
- **Is-Indexed** False
- **In Global Catalog** False
- **Search-Flags** 0x00000000
- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Whenever the Maximum Password Age value associated with a Defender Security Policy is modified.
- **Description** Contains the number of days after which a Defender password expires.
- **Classes used in** defender-policyClass

defender-policyMaximumPINAge

- **CN** defender-policyMaximumPINAge
- **Ldap-Display-Name** defender-policyMaximumPINAge
- **Attribute-Id** 1.2.840.113556.1.8000.1267.2.37
- **Link-Id** -
- **Range-Lower** -
- **Range-Upper** -
- **Size** 8 Bytes
- **Syntax** Interval
- **Is-Single-Valued** True
- **Is-Indexed** False
- **In Global Catalog** False
- **Search-Flags** 0x00000000
- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Whenever the Maximum PIN Age value associated with a Defender Security Policy is modified.
- **Description** Contains the number of days after which a Defender PIN expires.
- **Classes used in** defender-policyClass

defender-policyPasswordChangeFlags

- **CN** defender-policyPasswordChangeFlags
- **Ldap-Display-Name** defender-policyPasswordChangeFlags
- **Attribute-Id** 1.2.840.113556.1.8000.1267.2.38
- **Link-Id** -

- **Range-Lower** -
- **Range-Upper** -
- **Size** -
- **Syntax** Integer
- **Is-Single-Valued** True
- **Is-Indexed** False
- **In Global Catalog** False
- **Search-Flags** 0x00000000
- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Whenever Password Change flags associated with a Defender Security Policy are modified.
- **Description** Not currently used.
- **Classes used in** defender-policyClass

defender-policyPasswordFilter

- **CN** defender-policyPasswordFilter
- **Ldap-Display-Name** defender-policyPasswordFilter
- **Attribute-Id** 1.2.840.113556.1.8000.1267.2.39
- **Link-Id** -
- **Range-Lower** -
- **Range-Upper** -
- **Size** -
- **Syntax** String(Unicode)
- **Is-Single-Valued** True
- **Is-Indexed** False
- **In Global Catalog** False
- **Search-Flags** 0x00000000
- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Whenever the password filter associated with a Defender Security Policy is modified.
- **Description** Not currently used.
- **Classes used in** defender-policyClass

defender-policyGINAOptions

- **CN** defender-policyGINAOptions
- **Ldap-Display-Name** defender-policyGINAOptions
- **Attribute-Id** 1.2.840.113556.1.8000.1267.2.40
- **Link-Id** -
- **Range-Lower** -
- **Range-Upper** -
- **Size** -
- **Syntax** String(Octet)
- **Is-Single-Valued** True
- **Is-Indexed** False
- **In Global Catalog** False
- **Search-Flags** 0x00000000
- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Whenever the GINA Options value associated with a Defender Security Policy is modified.
- **Description** Not currently used.
- **Classes used in** defender-policyClass

defender-policyLoginTimes

- **CN** defender-policyLoginTimes
- **Ldap-Display-Name** defender-policyLoginTimes
- **Attribute-Id** 1.2.840.113556.1.8000.1267.2.41
- **Link-Id** -
- **Range-Lower** -
- **Range-Upper** -
- **Size** -
- **Syntax** String(Unicode)
- **Is-Single-Valued** True
- **Is-Indexed** False
- **In Global Catalog** False
- **Search-Flags** 0x00000000
- **Update Privilege** Domain or Defender administrator

- **Update Frequency** Whenever the login time associated with a Defender Security Policy is modified.
- **Description** Contains the times when a user is allowed to authenticate using Defender.
- **Classes used in** defender-policyClass

defender-notificationId

- **CN** defender-notificationId
- **Ldap-Display-Name** defender-notificationId
- **Attribute-Id** 1.2.840.113556.1.8000.1267.2.42
- **Link-Id** -
- **Range-Lower** -
- **Range-Upper** -
- **Size** -
- **Syntax** Integer
- **Is-Single-Valued** True
- **Is-Indexed** -
- **In Global Catalog** -
- **Search-Flags** 0x00000003
- **Update Privilege** Domain or Defender administrator
- **Update Frequency** Whenever a token or token license is created.
- **Description** For a token, contains the major token type. For a token license, contains the license type.
- **Classes used in** defender-tokenClass, defender-tokenLicenseClass

Appendix E: Defender Event Log messages

This section lists the messages that Defender components write to the Windows Event Log.

In this section:

- Defender VPN Integrator messages
- Defender Report Scheduler messages
- Defender Administration Console messages

Defender VPN Integrator messages

Defender VPN Integrator can write the following messages to the Windows Event Log, all with Source = pgwcserv, Event = 0:

- Handler not installed
- Service stopped
- Bad service request
- Service started

Defender Report Scheduler messages

Defender Report Scheduler can write the following messages to Windows Event Log, all with Source = Defender Report Scheduler:

- 1000: The Defender Report Scheduler was initialized successfully
- 1001: The Defender Report Scheduler failed to initialize
- 1002: The Defender Report Scheduler has been shutdown
- 1003: The Defender Report DCOM object failed to load. <*Error Message*> (<*Error Code*>)
- 1004: Generated scheduled report - <*Name of report generated*>

Defender Administration Console messages

Defender Administration Console can write the following messages to the Windows Event Log, all with Source = Defender Console:

- 1000: Token <*Distinguished Name of the Token*> assigned to user <*Distinguished Name of the User*>
- 1001: Failed to assign token <*Distinguished Name of the Token*> to user <*Distinguished Name of the User*>, error (<*Error Code*>) <*Error Message*>
- 1002: Defender Password assigned to user <*Distinguished Name of the User*>
- 1003: Failed to assign Defender Password to user <*Distinguished Name of the User*>, error (<*Error Code*>) <*Error Message*>
- 1004: Set PIN on token <*Distinguished Name of the Token*> assigned to user <*Distinguished Name of the User*>
- 1005: Failed to set PIN on token <*Distinguished Name of the Token*> assigned to user <*Distinguished Name of the User*>, error (<*Error Code*>) <*Error Message*>

- 1006: Set temporary response on token <*Distinguished Name of the Token*> assigned to user <*Distinguished Name of the User*>
- 1007: Failed to set temporary response on token <*Distinguished Name of the Token*> assigned to user <*Distinguished Name of the User*>, error (<*Error Code*>) <*Error Message*>
- 1008: Cleared temporary response on token <*Distinguished Name of the Token*> assigned to user <*Distinguished Name of the User*>
- 1009: Failed to clear temporary response on token <*Distinguished Name of the Token*> assigned to user <*Distinguished Name of the User*>, error (<*Error Code*>) <*Error Message*>
- 1010: Modified data of token <*Distinguished Name of the Token*> assigned to user <*Distinguished Name of the User*>
- 1011: Failed to modify data of token <*Distinguished Name of the Token*> assigned to user <*Distinguished Name of the User*>, error (<*Error Code*>) <*Error Message*>
- 1012: Token <*Distinguished Name of the Token*> unassigned from user <*Distinguished Name of the User*>
- 1013: Failed to unassign token <*Distinguished Name of the Token*> from <*Distinguished Name of the User*>, error (<*Error Code*>) <*Error Message*>
- 1014: Defender Password unassigned from user <*Distinguished Name of the User*>
- 1015: Failed to unassign Defender Password from user <*Distinguished Name of the User*>, error (<*Error Code*>) <*Error Message*>
- 1016: Token <*Distinguished Name of the Token*> replicated to all Global Catalog servers
- 1017: Token <*Distinguished Name of the Token*> replicated to <*count*> of <*total count*> Global Catalog servers
- 1018: Token <*Distinguished Name of the Token*> replicated to all AD servers
- 1019: Token <*Distinguished Name of the Token*> replicated to <*count*> of <*total count*> AD servers

Appendix F: Defender Client SDK

The Defender Client SDK provides a public interface to drive the Defender authentication process from a client program. The interface is exposed through the DefenderAuthenticator.Authenticator COM class. The installation program automatically registers this COM class on the client machine.

- Installing Defender Client SDK
- Application Programming Interfaces (APIs)
- Defender Security Server messages

Installing Defender Client SDK

To install the Defender Client SDK

1. Run the **DefenderClientSDK.exe** file supplied in the Defender distribution package.
2. Complete the wizard that starts to install the Defender Client SDK.

Application Programming Interfaces (APIs)

This section contains information about methods and properties provided by the following interfaces:

- IAuthenticator, IAuthenticator2, and IAuthenticator3 interfaces
- IAuthenticator2 and IAuthenticator3 interfaces
- IAuthenticator3 interface

IAuthenticator, IAuthenticator2, and IAuthenticator3 interfaces

Table 47:
Methods

Method	Description
Authenticate method	Sends a RADIUS authentication request to the Defender Security Server and waits for a response.

Table 48:
Properties

Property	Description
challengeMessage property	The prompt or message to be displayed to the user in response to the previous request.
sessionID property	The RADIUS session ID attribute.
timeout property	The number of seconds which the client

Property	Description
	program should wait for a response from the server.

Authenticate method

Submits a RADIUS request to the Defender Security Server and waits for a response. Typically, the Authenticate method would be invoked in a loop, whereby the current value of challengeMessage is displayed to the user, and the response from the user is supplied as the authData parameter on the next call to the Authenticate method. This would continue until the user chooses to cancel, or until the return code is not 1. If any request takes more than timeout seconds to complete, the method returns code -106.

C++ syntax

```
public : HRESULT Authenticate(BSTR userID, BSTR authData, LONG timeout, BSTR
ipAddress, LONG port, BSTR sharedSecret, LONG* returnCode );
```

C# syntax

```
int Authenticate(string userID, string authData, int timeout, string
ipAddress, int port, string sharedSecret);
```

Parameters

- **userID** The username of the user to be authenticated. Maximum length is 255 characters.
- **authData** The information which authenticates this user, such as a password or token response, typically entered by the user. You should set the value of this parameter in response to the current value of challengeMessage. Maximum length is 64 characters.
- **timeout** The number of seconds before the request should be abandoned.
- **ipAddress** The IP address of the Defender Security Server in "dotted decimal" format.
- **port** The port number which the Defender Security Server is listening on for this client (Access Node).
- **sharedSecret** This value is used to encrypt communications between the client program and the Defender Security Server. The value supplied here must match that defined in the Defender Access Node object for this client. See the Defender Installation and Administration Guide for further information on configuring Defender. Maximum length is 64 characters.

Return value

- **0** Authentication successful.
- **1** More information required to complete authentication.
- **2** Access denied.
- **-102** Unable to establish communications environment.
- **-103** API not supported on this platform.

- **-105** Unable to establish session with Defender Security Server.
- **-106** Unable to send request to Defender Security Server.
- **-107** Defender Security Server did not respond.

challengeMessage property

Displays the value of the challenge message to the user after each invocation of the Authenticate method.

C++ syntax

```
public : HRESULT get_challengeMessage(BSTR * bstrDefenderMessage);
```

C# syntax

```
public string challengeMessage { get; }
```

sessionID property

Holds the session attribute for the current session. Defender handles up to 255 concurrent sessions. This value is for information only and should not be set by the calling program.

C++ syntax

```
public : HRESULT get_sessionID(LONG * sessionID);
```

C# syntax

```
public int sessionID { get; }
```

timeout property

Holds the timeout value for the current session. This value is for information only and should not be set by the calling program. the timeout value is set using the timeout parameter on each call to the Authenticate method.

C++ syntax

```
public : HRESULT get_timeout(LONG timeoutValue);
```

C# syntax

```
public int timeout { get; }
```

IAuthenticator2 and IAuthenticator3 interfaces

Table 49:
Properties

Property	Description
challengeMessage property	The ID of the message to be displayed to the user in response to the previous request.
challengeMessageData property	Any variable data contained in the message to be displayed to the user in response to the previous request.

challengeMessageId property

Provides a numeric equivalent of the message to be displayed to the user after each invocation of the Authenticate method. This value could be used to lookup localized messages.

C++ syntax

```
public : HRESULT get_challengeMessageId(LONG * messageId);
```

C# syntax

```
public string challengeMessageId { get; }
```

challengeMessageData property

Provides any variable data contained in the message to be displayed to the user after each invocation of the Authenticate method.

C++ syntax

```
public : HRESULT get_challengeMessageData(BSTR * messageData);
```

C# syntax

```
public string challengeMessageData { get; }
```

IAuthenticator3 interface

.

Table 50:
Methods

Method	Description
AddPayload method	Allows RADIUS payload attributes to be added to the authentication request.
GetGridData method	Gets the raw data used to construct the

Method	Description
	GrIDsure grid.
GetAuthenticationImage method	Returns the GrIDsure grid as a byte array containing a bitmap.
SetGridResetPIPAttribute method	Adds a RADIUS payload attributes to the authentication request indicating that the GrIDsure PIP should be reset.

Table 51:
Properties

Property	Description
payload property	Gets an array of any RADIUS payload attributes returned in response to the previous request.
grIDsureMessage property	The GrIDsure specific message to be displayed to the user in response to the previous request.
grIDsureGridType property	The type of GrIDsure grid to be displayed.

AddPayload method

Allows RADIUS payload attributes to be added to the authentication request. Typically this method is used when the authenticating server or an intermediary requires additional information about the authenticating party.

The structure used to pass data to this function is defined below:

```
struct RADIUSPayloadAttribute
{
   DWORD vendorId;
   unsigned char type;
   unsigned char length;
   unsigned char data[253];
};
```

C++ syntax

```
public : HRESULT AddPayload(struct RADIUSPayloadAttribute *payload)
```

C# syntax

```
void AddPayload(ref RADIUSPayloadAttribute payload);
```

Parameters

payload Application specific payload data as a struct RADIUSPayloadAttribute.

Return value

Always returns S_OK.

GetGridData method

After an authentication request this method can be called to determine whether a user has a grid available and the state of that grid.

C++ syntax

```
public : HRESULT GetGridData(BSTR *grid, VARIANT_BOOL *isRegistrationGrid,
VARIANT_BOOL *isGrIDsureOnly, VARIANT_BOOL *hasGrid);
```

C# syntax

```
bool GetGridData(out string grid, out bool isRegistrationGrid, out bool
isGrIDsureOnly);
```

Parameters

- **grid** A string containing the values for the grid.
- **isRegistrationGrid** Returns TRUE if the user has not yet registered a PIP.
- **isGrIDsureOnly** Returns TRUE if the user only has a GrIDsure token.
- **hasGrid** Returns TRUE if a grid is available.

Return value

Always returns S_OK.

GetAuthenticationImage method

After an authentication request this function can be called to obtain a bitmap of the grid.

C++ syntax

```
public : HRESULT GetAuthenticationImage(VARIANT *imageData);
```

C# syntax

```
object GetAuthenticationImage();
```

Parameters

imageData A byte array containing a bitmap of the grid.

Return value

Returns S_OK if successful.

SetGridResetPIPAttribute method

Call this function before an authentication request to add a RADIUS payload attribute to inform the DSS that the user's GrIDsure PIP should be changed.

C++ syntax

```
public : HRESULT SetGridResetPIPAttribute(void);
```

C# syntax

```
void SetGridResetPIPAttribute();
```

Parameters

None

Return value

Always returns S_OK

payload property

After an authentication request this property will return an array of RADIUS payload attributes returned by the DSS. Each payload attribute will be returned as a struct RADIUSPayloadAttribute.

C++ syntax

```
public : HRESULT get_payload(SAFEARRAY(struct RADIUSPayloadAttribute) *
payload);
```

C# syntax

```
public Array payload { get; }
```

grIDsureMessage property

After an authentication request this property will return the GrIDsure challenge.

C++ syntax

```
public : HRESULT get_grIDsureMessage(BSTR *message);
```

C# syntax

```
public string grIDsureMessage { get; }
```

grIDsureGridType property

After an authentication request this property will return the type of grid.

C++ syntax

```
public : HRESULT get_grIDsureGridType(LONG* gridType);
```

C# syntax

```
public int grIDsureGridType { get; }
```

Return value

- **0x00800000** The user has no grid.
- **0x01000000** The user has a registered grid.
- **0x02000000** The user has a grid but no PIP has been registered.
- **0x04000000** The user has a grid and the PIP has expired.
- **0x80000000** The user has a grid and they have expired the PIP.

IAuthInfo interface

Table 52:
Properties

Property	Description
userIdType property	A value representing the type of user name expected for authentications through a Defender Access Node.
isUserDefenderAuthenticated property	Determines whether a user is to be Defender authenticated through a Defender Security Server and Defender Access Node.

userIdType property

Returns a value representing the type of user name expected for authentications through the passed Defender Access Node. The accessNode parameter should be the common name.

C++ syntax

```
public : HRESULT get_userIdType( BSTR accessNode, LONG* pVal);
```

C# syntax

```
public virtual int get_userIdType(string accessNode)
```

Return value

- **0** Defender ID.
- **1** User Principal Name.
- **2** SAM Account Name.
- **3** Proper Name.
- **-1** Failed to retrieve user ID type.

isUserDefenderAuthenticated property

Returns a non-zero value if the user is Defender authenticated. Otherwise, returns zero.

The user will be Defender authenticated if all of the following is true:

- The Access Node specified is assigned to the Defender Security Server.
- The user is a member of the Access Node, either directly or indirectly.
- The user has a token or Defender Password as required by the effective policy.

C++ syntax

```
public : HRESULT isUserDefenderAuthenticated( BSTR domain, BSTR
samAccountName, BSTR accessNode, BSTR dssIpAddress, VARIANT_BOOL* pVal);;
```

C# syntax

```
public virtual int get_isUserDefenderAuthenticated(string domain, string
samAccountName, string accessNode, string dssIpAddress)
```

Parameters

- **domain** The NetBIOS name of the domain to which the user belongs.
- **samAccountName** The SAM account name of the user.
- **accessNode** The common name (cn) of the Defender Access Node through which the user will authenticate.
- **dssIpAddress** The IP address of the Defender Security Server through which the user will authenticate.

Defender Security Server messages

Messages containing %s will have this replaced with challenge data; this can be obtained via the challengeMessageData property. \r\n denotes a carriage return followed by a line feed.

Table 53:
Defender Security Server messages

Message ID	Default text
00	Enter Synchronous Response:\r\n
01	Invalid Synchronous Response.\r\nEnter Synchronous Response:\r\n
02	Access Denied.\r\n
03	Your PIN has expired and must be changed.\r\nEnter Current PIN and required PIN and confirm PIN:\r\n

Message ID	Default text
04	Enter Defender Password:\r\n
05	Invalid Password.\r\nEnter Defender Password:\r\n
06	PIN change failed, try again.\r\nEnter Current PIN and required PIN and confirm PIN:\r\n
07	Your token is not synchronised to the current system clock.\r\nEnter the next response.\r\n
08	Invalid Response.\r\nYour token is not synchronised to the current system clock.\r\nEnter the next response.\r\n
10	SNK Challenge: %s \r\nEnter Response:\r\n
11	Invalid Response\r\nSNK Challenge: %s \r\nEnter Response:\r\n
12	Confirm Response\r\nSNK Challenge: %s \r\nEnter Response:\r\n
15	Access Approved.\r\n
16	Call has been intercepted by Defender 5. Unauthorized use of this system is PROHIBITED!\r\n\r\nEnter ID:
17	Your account is locked due to excess violations.\r\n
18	Your token appears to be upside down.\r\nRotate it and enter the next response.\r\n
19	Invalid Response.\r\nYour token appears to be upside down.\r\nRotate it and enter the next response.\r\n
20	Enter Windows Password:\r\n
21	Invalid Windows Password.\r\nEnter Windows Password:\r\n
22	Invalid Response.\r\nEnter Synchronous Response with Defender Password:\r\n
23	Enter Synchronous Response with Windows Password:\r\n
24	Invalid Response.\r\nEnter Synchronous Response with Windows Password:\r\n
25	SNK Challenge: %s \r\nEnter Response with Defender Password:\r\n
26	Invalid Response.\r\nSNK Challenge: %s \r\nEnter Response with Defender Password:\r\n
27	SNK Challenge: %s \r\nEnter Response with Windows Password:\r\n
28	Invalid Response.\r\nSNK Challenge: %s \r\nEnter Response with Windows Password:\r\n

Message ID	Default text
39	Your Defender password has expired and must be changed\r\nEnter a new Defender password:\r\n
40	Your Windows password has expired and must be changed\r\nEnter a new Windows password:\r\n
41	Confirm your new Defender password:\r\n
42	Confirm your new Windows password:\r\n
43	Password change failed\r\nEnter a new Defender password:\r\n
44	Password change failed\r\nEnter a new Windows password:\r\n
45	Enter Synchronous Response with Defender Password:\r\n
46	Your token has expired and cannot be activated\r\nPlease contact your administrator.\r\n
47	Access Denied - No valid route found.\r\nPlease contact your administrator.\r\n
48	Access Denied - User account is disabled.\r\nPlease contact your administrator.\r\n
51	Access Denied - No user name.\r\nPlease contact your administrator.\r\n
52	Access Denied - Authentication not permitted at this time\r\n
53	Your token is not synchronised with Defender.\r\nEnter the next response.\r\n
54	Invalid Response.\r\nYour token is not synchronised with Defender.\r\nEnter the next response.\r\n
55	Your Defender password has expired and access has been forbidden.\r\n Please contact your system administrator.\r\n
56	Your Windows password has expired and access has been forbidden.\r\n Please contact your system administrator.\r\n
57	Configure your GrIDsure PIP:\r\n%s
58	Use your GrIDsure PIP:\r\n%s
59	Invalid Response.\r\nUse your GrIDsure PIP:\r\n%s
60	Invalid PIP.\r\nConfigure your GrIDsure PIP:\r\n%s
61	Your PIP has expired and must be changed.\r\nConfigure your GrIDsure PIP:\r\n%s
62	PIP change requested.\r\nConfigure your GrIDsure PIP:\r\n%s

Message ID	Default text
63	PIP does not meet complexity rules.\r\nConfigure your GrIDsure PIP:\r\n%s
64	Access Denied - Ambiguous user name.\r\nPlease contact your administrator.\r\n
65	Your Windows account has expired and access has been forbidden.\r\nPlease contact your system administrator.\r\n

Appendix G: Defender Web Service API

The Defender Web Service API provides a public web interface to the administrative functionality of Defender.

The interface is exposed through the WebServiceAPI Web service. The installation program configures a windows service that will host the WebServiceAPI web service.

- API methods
- API types

API methods

Table 54:
API methods

Method	Description
AddSoftwareTokenToUser method	Assigns a Defender Software token to a user.
AddTokenToUser method	Assigns a Defender token to a user.
GetTokensForUser method	Gets a list of Defender tokens assigned to a user.
RemoveAllTokensFromUser method	Unassigns all Defender tokens from a user.
RemoveDefenderPassword method	Deletes the Defender password for a user or all users in a group.
RemovePinFromUserToken method	Removes a user's PIN from an assigned token.

Method	Description
RemoveTemporaryResponse method	Removes a temporary response from a user's assigned token.
RemoveTokenFromUser method	Unassigns a Defender token from a user.
ResetDefenderToken method	Resets a Defender token to aid authentication when the token is out of synchronization with the server.
ResetDefenderViolationCount method	Reset a user's Defender violation count. Also allows the violation and reset counts to be viewed without resetting them.
SetDefenderPassword method	Sets the Defender password for a user or all users in a group.
SetPinOnUserToken method	Sets a user's PIN for an assigned token.
SetTemporaryResponse method	Sets a temporary response on a user's assigned token.
TestDefenderToken method	Tests a Defender token's response.

AddSoftwareTokenToUser method

If this operation resulted in the token being assigned, then the AssignedToken.TokenCommonName will match the tokenCommonName parameter. If the token was already assigned to this user, then the AssignedToken.TokenCommonName will contain a text message indicating that it was already assigned.

The type of the token added may be one of the following values:

- **Windows**
- **IToken**
- **Mobile**
- **Android**
- **EmailOTP**
- **Java**
- **GrIDsure**
- **Authy**
- **GoogleAuth**
- **MicrosoftAuth**
- **OneLoginAuth**

These types produce tokens for use on the following platforms:

- **Windows** Windows operating system.
- **IToken** iPhone, iPad, or iPod devices running the iOS operating system.
- **Mobile** SMS token, where a text message containing one-time passwords is sent to the user's mobile phone.
- **Android** Devices running the Android operating system.
- **EmailOTP** E-mail token, where an e-mail message containing one-time passwords is sent to the user.
- **Java** Windows, Mac OS, or Linux operating system that supports Java applications.
- **GrIDsure** GrIDsure token allowing users to authenticate themselves with a GrIDsure Personal Identification Pattern.
- **Authy** Authy token allowing users to authenticate themselves with one-time passwords generated by the Authy app.
- **GoogleAuth** Google Authenticator token allowing users to authenticate themselves with one-time passwords generated by Google Authenticator.
- **MicrosoftAuth** Microsoft Authenticator token allowing users to authenticate themselves with one-time passwords generated by Microsoft Authenticator.
- **OneLoginAuth** OneLogin Authenticator token allowing users to authenticate themselves with one-time passwords generated by OneLogin Authenticator.

C# syntax

```
[OperationContract]
[FaultContract(typeof(FaultException))]
AssignedSoftwareToken AddSoftwareTokenToUser(string userCommonName,
ProgrammableSoftwareTokenType tokenType, string tokenPin,
SoftwareTokenConfiguration configuration, string userSearchBase);
```

Parameters

- **userCommonName** Common name of the user to whom the token will be assigned.
- **tokenType** The type of the token added.
- **tokenPin** Optional parameter to specify PIN to assign to the user's token. PINs cannot be used when programming a Windows token.
- **configuration** Optional parameter to configure the following activation and passphrase settings:
  - Activation Code Timeout Days To configure the number of days for which the token activation code is valid. The default value is 7.
  - Enabling Passphrase Locking To configure whether to lock the token passphrase after a specified number of unsuccessful attempts.
  - Passphrase Attempts The configure the number of unsuccessful attempts after which the token passphrase is locked.
  - Require Passphrase To configure whether the token requires a passphrase or not.

- Require Strong Passphrase To configure whether a strong passphrase is required or not.
- Show Passphrase Alerts To configure whether to display alerts about failed passphrase attempts or not.

- **userSearchBase** Optional parameter to specify base container from which to search for users.

Return value

If no error occurs, an AssignedToken is returned. In the case of an error, a Fault is generated. The faultCode can be one of the following:

- **ArgumentOutOfRange** One of the arguments was invalid, further details will be contained in the faultstring.
- **UnknownFault** Any other error, further details may be included in the faultstring.

AddTokenToUser method

If this operation resulted in the token being assigned, then the AssignedToken.TokenCommonName matches the tokenCommonName parameter. If the token was already assigned to this user, then the AssignedToken.TokenCommonName contains a text message indicating that it was already assigned.

C# syntax

```
[OperationContract]
[FaultContract(typeof(FaultException))]
AssignedToken AddTokenToUser(string tokenCommonName, string userCommonName,
string tokenSearchBase, string userSearchBase);
```

Parameters

- **tokenCommonName** Common name of the token to be assigned.
- **userCommonName** Common name of the user to whom the token will be assigned.
- **tokenSearchBase** Optional parameter to specify base container in which to search for tokens.
- **userSearchBase** Optional parameter to specify base container in which to search for users.

Return value

If no error occurs, an AssignedToken is returned. In the case of an error, a Fault is generated. The faultCode can be one of the following:

- **ArgumentOutOfRange** One of the arguments was invalid, further details will be contained in the faultstring.
- **UnknownFault** Any other error, further details may be included in the faultstring.

GetTokensForUser method

Gets a list of Defender tokens assigned to a user.

C# syntax

```
[OperationContract]
[FaultContract(typeof(FaultException))]
TokenList GetTokensForUser(string userCommonName, string userSearchBase);
```

Parameters

- **userCommonName** Common name of the user for whom you want to get a list of assigned tokens.
- **userSearchBase** Optional parameter to specify base container in which to search for users.

Return value

If no error occurs, a list of TokenList is returned. In the case of an error, a Fault is generated. The faultCode can be one of the following:

- **ArgumentOutOfRange** One of the arguments was invalid, further details will be contained in the faultstring.
- **UnknownFault** Any other error, further details may be included in the faultstring.

RemoveAllTokensFromUser method

Unassigns all Defender tokens from a user.

C# syntax

```
[OperationContract]
[FaultContract(typeof(FaultException))]
void RemoveAllTokensFromUser(string userCommonName, bool
deleteSoftwareToken, string userSearchBase);
```

Parameters

- **userCommonName** Common name of the user whose tokens will be unassigned.
- **deleteSoftwareToken** If true then Defender Software tokens are removed from the directory as well as being removed from the user.
- **userSearchBase** Optional parameter to specify base container from which to search for users.

Return value

In the case of an error, a Fault is generated. The faultCode can be one of the following:

- **ArgumentOutOfRange** One of the arguments was invalid, further details will be contained in the faultstring.
- **UnknownFault** Any other error, further details may be included in the faultstring.

RemoveDefenderPassword method

Deletes the Defender password for a user or all users in a group. When a user account name is specified, that user's Defender password is deleted. When a group name is specified, the Defender passwords for all users in that group are deleted.

C# syntax

```
[OperationContract]
[FaultContract(typeof(FaultException))]
void RemoveDefenderPassword(string userGroupCommonName, string
userSearchBase);
```

Parameters

- **userGroupCommonName** Common name of the user or group of users from which the Defender Password will be removed.
- **userSearchBase** Optional parameter to specify base container from which to search for users.

Return value

In the case of an error a Fault is generated. The faultCode can be one of the following:

- **ArgumentOutOfRange** One of the arguments was invalid, further details will be contained in the faultstring.
- **UnknownFault** Any other error, further details may be included in the faultstring.

RemovePinFromUserToken method

Removes a user's PIN from an assigned token.

C# syntax

```
[OperationContract]
[FaultContract(typeof(FaultException))]
void RemovePinFromUserToken(string userCommonName, string tokenCommonName,
string userSearchBase, string tokenSearchBase);
```

Parameters

- **userCommonName** Common name of the user from whom the PIN will be removed.
- **tokenCommonName** Common name of the token from which the PIN wil be removed.
- **userSearchBase** Optional parameter to specify base container from which to search for users.
- **tokenSearchBase** Optional parameter to specify base container from which to search for tokens.

Return value

In the case of an error a Fault is generated. The faultCode can be one of the following:

- **ArgumentOutOfRange** One of the arguments was invalid, further details will be contained in the faultstring.
- **UnknownFault** Any other error, further details may be included in the faultstring.

RemoveTemporaryResponse method

Removes a temporary response from a token assigned to a user.

C# syntax

```
[OperationContract]
[FaultContract(typeof(FaultException))]
void RemoveTemporaryResponse(string userCommonName, string tokenCommonName,
string userSearchBase, string tokenSearchBase);
```

Parameters

- **userCommonName** Common name of the user from which the temporary response will be removed.
- **tokenCommonName** Common name of the user from which the temporary response will be removed.
- **userSearchBase** Optional parameter to specify base container from which to search for users.
- **tokenSearchBase** Optional parameter to specify base container from which to search for tokens.

Return value

In the case of an error a Fault is generated. The faultCode can be one of the following:

- **ArgumentOutOfRange** One of the arguments was invalid, further details will be contained in the faultstring.
- **UnknownFault** Any other error, further details may be included in the faultstring.

RemoveTokenFromUser method

Unassigns a Defender token from a user.

C# syntax

```
[OperationContract]
[FaultContract(typeof(FaultException))]
AssignedToken RemoveTokenFromUser(string userCommonName, string
tokenCommonName, bool deleteSoftwareToken, string userSearchBase, string
tokenSearchBase);
```

Parameters

- **userCommonName** Common name of the user whose tokens are to be unassigned.
- **tokenCommonName** Common name of the token that is to be unassigned.

- **deleteSorfwareToken** If true, then Defender Software tokens are removed from the directory and from the user.
- **userSearchBase** Optional parameter to specify base container in which to search for users.
- **tokenSearchBase** Optional parameter to specify base container in which to search for tokens.

Return value

A successful unassignment results in an AssignedToken being returned. If the token was already unassigned, then the AssignedToken.TokenCommonName indicates this. In the case of an error a Fault is generated.

The faultCode can be one of the following:

- **ArgumentOutOfRange** One of the arguments was invalid, further details are contained in the faultstring.
- **UnknownFault** Any other error, further details may be included in the faultstring.

ResetDefenderToken method

Resets a Defender token to aid authentication when the token is out of synchronization with the server.

C# syntax

```
[OperationContract]
[FaultContract(typeof(FaultException))]
DefenderResult ResetDefenderToken(string tokenCommonName, string
tokenSearchBase);
```

Parameters

- **tokenCommonName** Common name of the token to reset.
- **tokenSearchBase** Optional parameter to specify base container in which to search for tokens.

Return value

A DefenderResult is returned indicating the success or otherwise of the reset. In the case of an error a Fault is generated.

The faultCode can be one of the following:

- **ArgumentOutOfRange** One of the arguments was invalid, further details are contained in the faultstring.
- **UnknownFault** Any other error, further details may be included in the faultstring.

ResetDefenderViolationCount method

Reset a user's Defender violation count. Also allows the violation and reset counts to be viewed without resetting them.

C# syntax

```
[OperationContract]
[FaultContract(typeof(FaultException))]
UserViolationCount ResetDefenderViolationCount(string userCommonName, bool
viewOnly, string userSearchBase);
```

Parameters

- **userCommonName** Common name of the user whose violation count is to be reset.
- **viewOnly** If true, then the violation count and reset count are returned but not adjusted.
- **userSearchBase** Optional parameter to specify base container in which to search for users.

Return value

Successfull calls return a UserViolationCount. In the case of an error, a Fault is generated.

The faultCode can be one of the following:

- **ArgumentOutOfRange** One of the arguments was invalid, further details are contained in the faultstring.
- **UnknownFault** Any other error, further details may be included in the faultstring.

SetDefenderPassword method

Sets the Defender password for a user or all users in a group. When a user account name is specified, that user's Defender password is set. When a group name is specified, the Defender passwords for all users in that group are assigned the specified Defender password.

C# syntax

```
[OperationContract]
[FaultContract(typeof(FaultException))]
void SetDefenderPassword(string userGroupCommonName, string password, bool
expire, bool overwrite, string userSearchBase);
```

Parameters

- **userGroupCommonName** Common name of the user or group of users to which the Defender password is to be set.
- **password** The Defender password to set.
- **expire** Sets the Defender password to the expired state.

- **overwrite** Overwrites an existing Defender Password. By default, an existing Defender password cannot be overwritten.
- **userSearchBase** Optional parameter to specify base container in which to search for users.

Return value

In the case of an error, a Fault is generated. The faultCode can be one of the following:

- **ArgumentOutOfRange** One of the arguments was invalid, further details are contained in the faultstring.
- **UnknownFault** Any other error, further details may be included in the faultstring.

SetPinOnUserToken method

Sets a user's PIN for an assigned token.

C# syntax

```
[OperationContract]
[FaultContract(typeof(FaultException))]
void SetPinOnUserToken(string userCommonName, string tokenCommonName,
string tokenPin, string userSearchBase, string tokenSearchBase);
```

Parameters

- **userCommonName** Common name of the user to whom the PIN is to be assigned.
- **tokenCommonName** Common name of the token to which the PIN is to be assigned.
- **tokenPin** The PIN to assign.
- **userSearchBase** Optional parameter to specify base container in which to search for users.
- **tokenSearchBase** Optional parameter to specify base container in which to search for tokens.

Return value

In the case of an error a Fault is generated. The faultCode can be one of the following:

- **ArgumentOutOfRange** One of the arguments is invalid, further details are contained in the faultstring.
- **UnknownFault** Any other error, further details may be included in the faultstring.

SetTemporaryResponse method

Sets a temporary response on a user's assigned token.

C# syntax

```
[OperationContract]
[FaultContract(typeof(FaultException))]
```

```
TemporaryResponse SetTemporaryResponse(string userCommonName, string
tokenCommonName, int expiryTimeMinutes, bool multipleUse, string
userSearchBase, string tokenSearchBase);
```

Parameters

- **userCommonName** Common name of the user to whom the temporary response is to be assigned.
- **tokenCommonName** Common name of the token to which the temporary response is to be assigned.
- **expiryTimeMinutes** The time interval, in minutes, during which the temporary response remains valid.
- **multipleUse** If true, then the temporary response can be used multiple times.
- **userSearchBase** Optional parameter to specify base container in which to search for users.
- **tokenSearchBase** Optional parameter to specify base container in which to search for tokens.

Return value

A succesful call returns a TemporaryResponse. In the case of an error a Fault is generated.

The faultCode can be one of the following:

- **ArgumentOutOfRange** One of the arguments was invalid, further details will be contained in the faultstring.
- **UnknownFault** Any other error, further details may be included in the faultstring.

TestDefenderToken method

Tests a Defender token's response.

C# syntax

```
[OperationContract]
[FaultContract(typeof(FaultException))]
DefenderResult TestDefenderToken(string tokenCommonName, string response,
string challenge, string tokenSearchBase);
```

Parameters

- **tokenCommonName** Common name of the token to test.
- **response** The token response.
- **challenge** The token challenge, not required for synchronous tokens.
- **tokenSearchBase** Optional parameter to specify the base container in which to search for tokens.

Return value

A valid call results in a DefenderResult. This class provides the following public properties:

- **System.Boolean Success** Returns whether the test was successful.
- **System.String ErrorMessage** Returns the error message associated with the test.

In the case of an error a Fault is generated.

The faultCode can be one of the following:

- **ArgumentOutOfRange** One of the arguments is invalid, further details are contained in the faultstring.
- **UnknownFault** Any other error, further details may be included in the faultstring.

API types

Table 55:
API types

Method	Description
AssignedSoftwareToken type	Details of an assignment of a software token to a user.
AssignedToken type	Details of an assignment of a token to a user.
ProgrammableSoftwareTokenType type	Enumeration of programmable software token types.
TokenList type	A List of UserTokenDetail.
UserTokenDetail type	Details of a token assigned to a user.
DefenderResult type	Result indicating success or otherwise of certain operations.
UserViolationCount type	Details of authentication violations and the number of times the violation count has been reset.
TemporaryResponse type	Details of a temporary response and its expiry time.

AssignedSoftwareToken type

Details of an assignment of a software token to a user. If the token was already assigned to the user then the AssignedToken.TokenCommonName contains a text message indicating that it was already assigned.

C# syntax

```
[DataContract]
```

```
public class AssignedToken
{
    [DataMember]
    public string UserCommonName { get; set; }
    [DataMember]
    public string TokenCommonName { get; set; }
    [DataMember]
    public string ActivationCode { get; set; }
}
```

Properties

- **UserCommonName** Common name of the user to whom the token is assigned.
- **TokenCommonName** Common name of the assigned token.
- **ActivationCode** The activation code used to activate the token on the user's device.

AssignedToken type

Details of an assignment of a token to a user. If the token was already assigned to this user then the AssignedToken.TokenCommonName will contain a text message indicating that it was already assigned.

C# syntax

```
[DataContract]
public class AssignedToken
{
    [DataMember]
    public string UserCommonName { get; set; }
    [DataMember]
    public string TokenCommonName { get; set; }
}
```

Properties

- **UserCommonName** Common name of the user to whom the token is assigned.
- **TokenCommonName** Common name of the assigned token.

ProgrammableSoftwareTokenType type

Enumeration of programmable software token types.

C# syntax

```
[DataContract]
public enum ProgrammableSoftwareTokenType
{
    [EnumMember]
    Windows = 0,
    [EnumMember]
    IToken = 4,
```

```
    [EnumMember]
    Mobile = 5,
    [EnumMember]
    GrIDsure = 6,
    [EnumMember]
    Android = 7,
    [EnumMember]
    EmailOTP = 8,
    [EnumMember]
    Java = 10,
    [EnumMember]
    GoogleAuth = 11,
    [EnumMember]
    Authy = 12
};
```

Values

- **Windows** A token for Windows operating system.
- **IToken** A token for iPhone, iPad, or iPod Touch devices running the iOS operating system
- **Mobile** SMS token, where a text message containing one-time passwords is sent to the user's mobile phone.
- **GrIDsure** A GrIDsure token.
- **Android** A token for devices running the Android operating system.
- **EmailOTP** E-mail token, where an e-mail message containing one-time passwords is sent to the user's mobile phone.
- **Java** A token for Windows, Mac OS, or Linux operating systems that support Java applications.
- **Authy** An Authy token allowing users to authenticate themselves with one-time passwords generated by the Authy app.
- **GoogleAuth** A Google Authenticator token allowing users to authenticate themselves with one-time passwords generated by Google Authenticator.

TokenList type

A list of UserTokenDetail.

C# syntax

```
[CollectionDataContract(Name="TokenList", ItemName="Token")]
public class TokenList : List<UserTokenDetail>
{ }
```

UserTokenDetail type

Details of a token assigned to a user.

C# syntax

```
[DataContract] public class UserTokenDetail
{
    [DataMember]
   public string TokenType { get; set; }
    [DataMember]
   public bool HasPIN { get; set; }
    [DataMember]
   public string CommonName { get; set; }
    [DataMember]
   public string DN { get; set; }
}
```

Properties

- **TokenType** The type of the token.
- **HasPin** Whether the token has a PIN for this user.
- **CommonName** Common name of the token.
- **DN** Distinguished name of the token.

DefenderResult type

Result indicating success or otherwise of certain operations.

C# syntax

```
[DataContract]
public class DefenderResult
{
    [DataMember]
   public bool Success{ get; set; }
    [DataMember]
   public string ErrorMessage { get; set; }
}
```

Properties

- **Success** Indicates whether the operation was successful.
- **ErrorMessage** Contains an error message in the event of operation failure.

UserViolationCount type

Details of authentication violations and the number of times the violation count has been reset.

C# syntax

```
[DataContract]
public class UserViolationCount
{
    [DataMember]
   public string SAMAccountName { get; set; }
    [DataMember]
   public string CommonName { get; set; }
    [DataMember]
   public string DN { get; set; }
    [DataMember]
   public int ViolationCount { get; set; }
    [DataMember]
   public int ResetCount { get; set; }
}
```

Properties

- **SAMAccountName** SAM account name of the user.
- **CommonName** Common name of the user.
- **DN** Distinguished name of the user.
- **ViolationCount** The count of Defender authentication violations.
- **ResetCount** The number of times the violation count has been reset.

TemporaryResponse type

Details of a temporary response and its expiry time.

C# syntax

```
[DataContract]
public class TemporaryResponse
{
    [DataMember]
   public string Response { get; set; }
    [DataMember]
   public DateTime ExpiryTime { get; set; }
}
```

Properties

- **Response** The temporary response assigned to the token.
- **ExpiryTime** When the temporary response expires.

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