TECH BRIEF

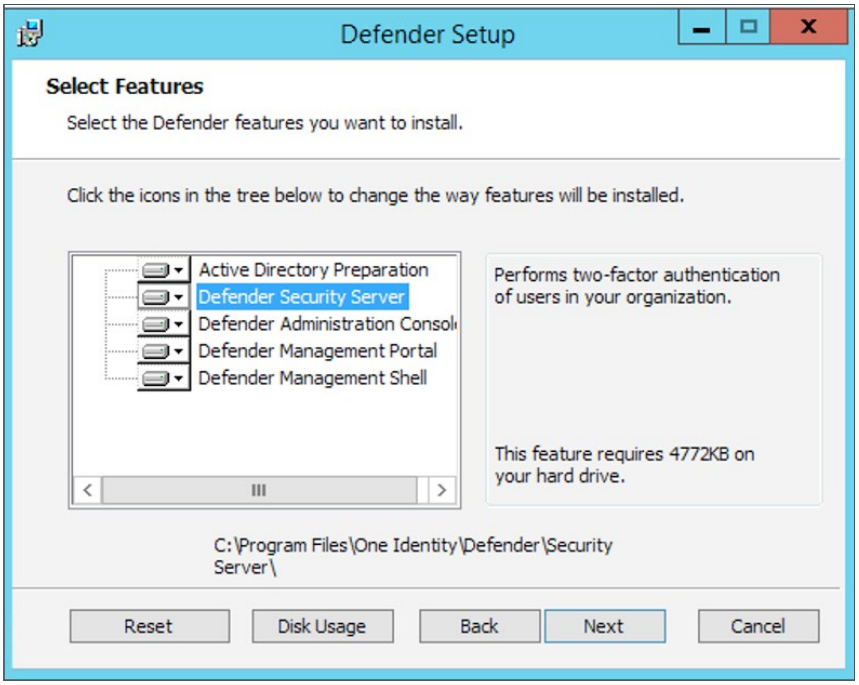
ONE IDENTITY™

Installing and Configuring Defender: The Quick Version

Empowering your remote workforce

1. Install Defender

a. For this step, all components can be installed on one Member Server or they can be individually installed on purpose-specific servers. Select the components to be installed and click Next.



Select Features

Select the Defender features you want to install.

Click the icons in the tree below to change the way features will be installed.

- Active Directory Preparation
- Defender Security Server
- Defender Administration Consol
- Defender Management Portal
- Defender Management Shell

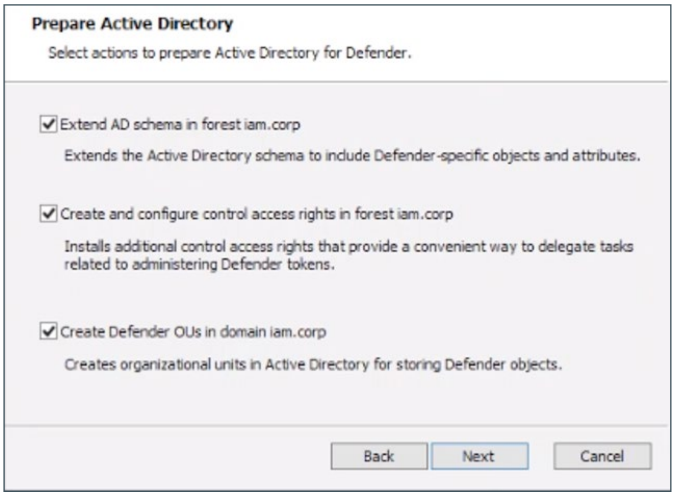
Performs two-factor authentication of users in your organization.

This feature requires 4772KB on your hard drive.

C:\Program Files\One Identity\Defender\Security Server\

b. Enter your domain controller or domain name and supply a service account with the appropriate level of administrative rights to extend the Active Directory schema and install the product. Click Next.

c. Leave all checkboxes checked, click Next.



Prepare Active Directory

Select actions to prepare Active Directory for Defender.

☑ Extend AD schema in forest iam.corp

Extends the Active Directory schema to include Defender-specific objects and attributes.

☑ Create and configure control access rights in forest iam.corp

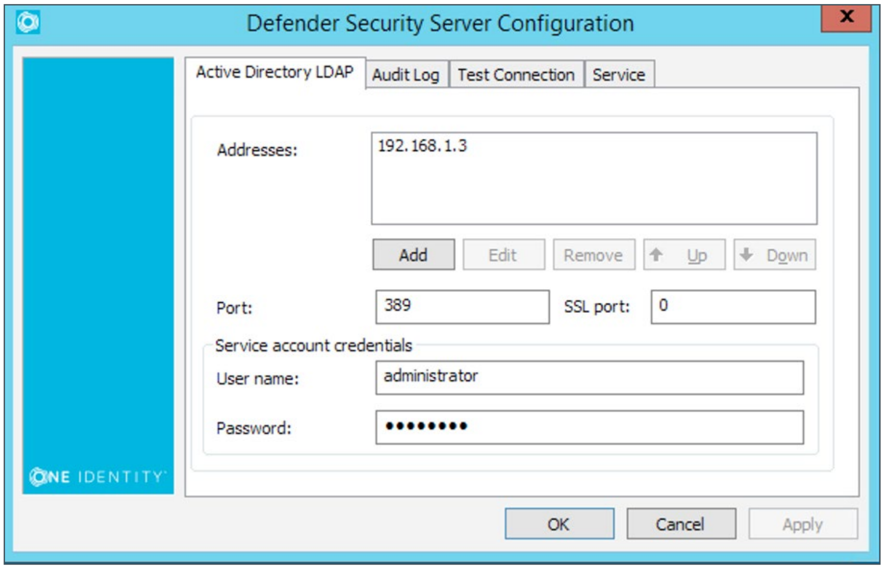
Installs additional control access rights that provide a convenient way to delegate tasks related to administering Defender tokens.

☑ Create Defender OUs in domain iam.corp

Creates organizational units in Active Directory for storing Defender objects.

2. Initial Defender Configuration

a. Setup your Defender Security Server. Simply add the IP addresses or DNS names of your domain controllers and enter a service account to be used during the authentication process.



Addresses: 192.168.1.3

Port: 389

SSL port: 0

Service account credentials

User name: administrator

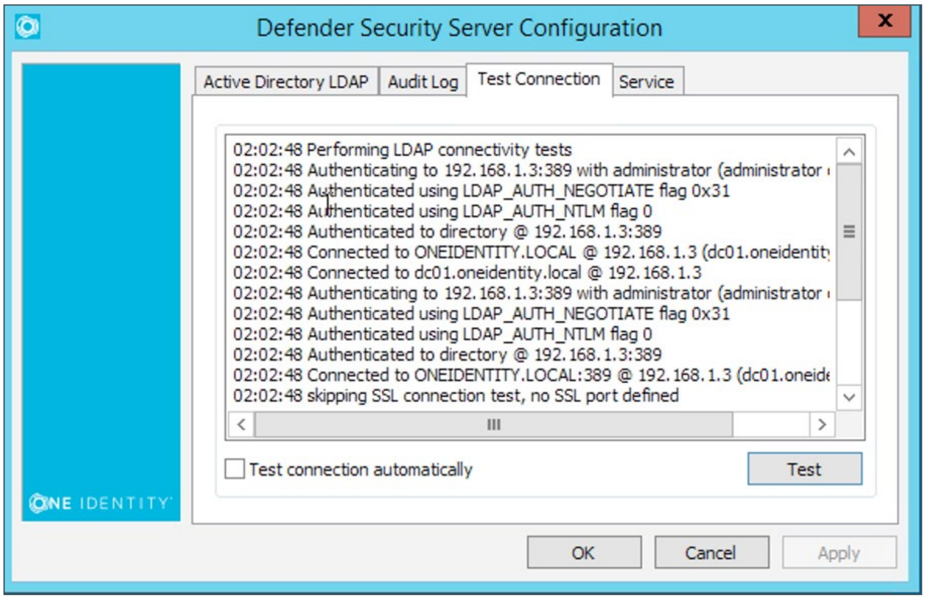
Password: ••••••••

Pro tip: Type the username of the service account under which you want the Defender Security Server to connect to Active Directory. Use either <domain>\<user name> format or distinguished name (DN).

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.

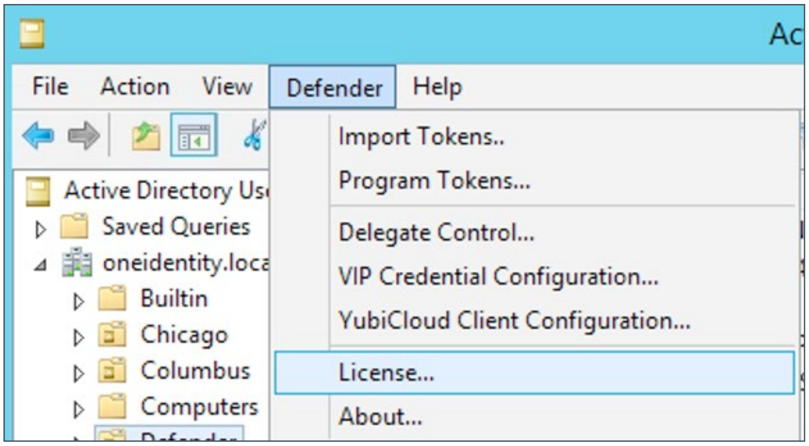
b. Test authentication to the domain.



```
02:02:48 Performing LDAP connectivity tests
02:02:48 Authenticating to 192.168.1.3:389 with administrator (administrator
02:02:48 Authenticated using LDAP_AUTH_NEGOTIATE flag 0x31
02:02:48 Authenticated using LDAP_AUTH_NTLM flag 0
02:02:48 Authenticated to directory @ 192.168.1.3:389
02:02:48 Connected to ONEIDENTITY.LOCAL @ 192.168.1.3 (dc01.oneidentit
02:02:48 Connected to dc01.oneidentity.local @ 192.168.1.3
02:02:48 Authenticating to 192.168.1.3:389 with administrator (administrator
02:02:48 Authenticated using LDAP_AUTH_NEGOTIATE flag 0x31
02:02:48 Authenticated using LDAP_AUTH_NTLM flag 0
02:02:48 Authenticated to directory @ 192.168.1.3:389
02:02:48 Connected to ONEIDENTITY.LOCAL:389 @ 192.168.1.3 (dc01.oneide
02:02:48 skipping SSL connection test, no SSL port defined
```

☐ Test connection automatically

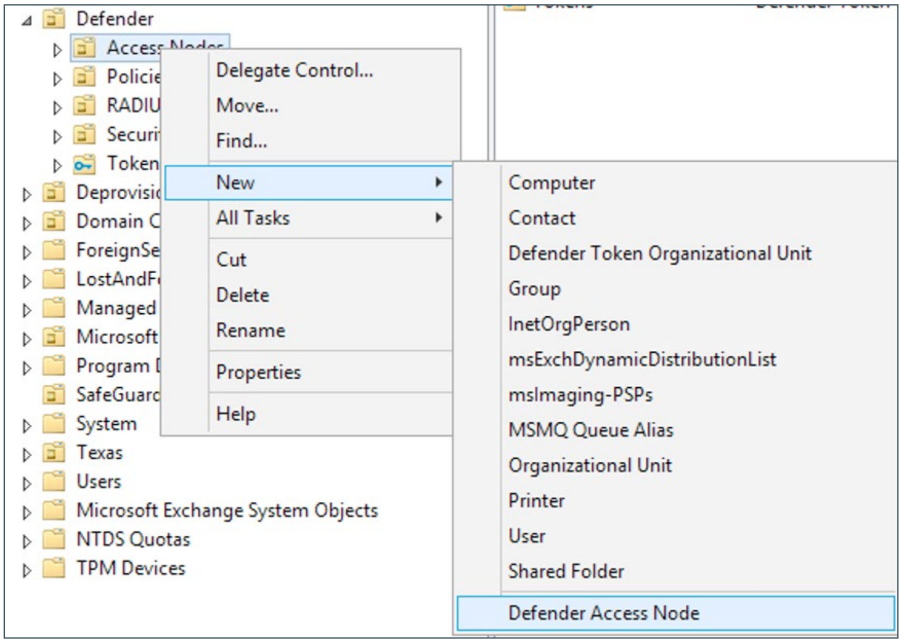
c. Open Active Directory Users and Computers, then click the Defender menu tab and select License.



d. Click “Add Licenses” and enter the “License Key” and “Site Message” contained in the email from our licensing department

   i. To import hardware tokens, simply click “Import Tokens” under the Defender menu option and select the \NOSTATIC\EXPORT.DPX file sent to you, along with the import key.

e. Expand the Defender OU, right click Access Nodes > New > Defender Access Node



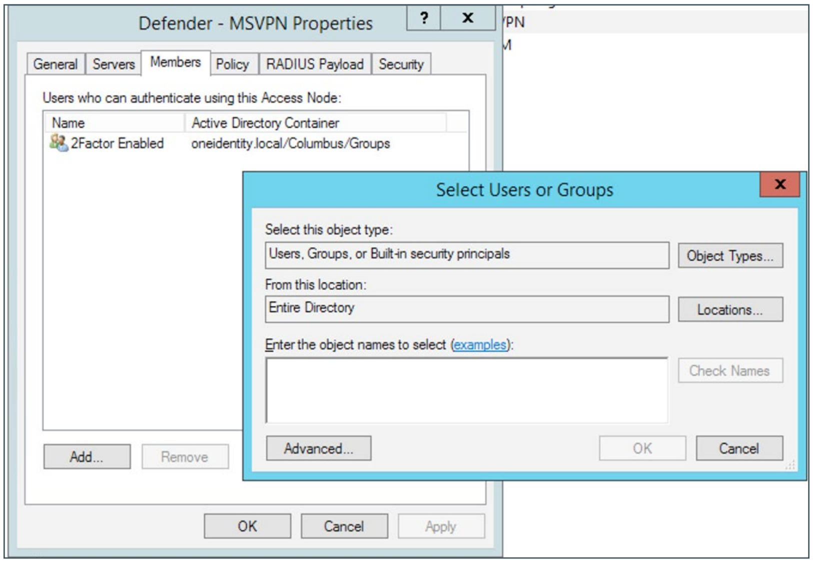
i. Follow the wizard. Enter a name for the access node (usually the name of the access point i.e. Juniper VPN)

ii. Node Type = Radius Agent, User ID = SAM Account Name

iii. IP Address or DNS name = Internal IP of your access point, Port (1812 is standard), Subnet Mask is usually okay to leave at 255.255.255.255 unless network subnet requirements dictate otherwise, Shared Secret should be a complex password that is saved/remembered as it will need to be entered into your RADIUS configuration on your access point. Click Next, then Finish.

iv. Double-click your newly created policy to open the properties. Click the Members Tab, then Add. Select a domain security group that contains the users which you want to use Defender 2FA via this access point and Click OK.

v. Click OK to save and close the properties window.



Users who can authenticate using this Access Node:

Name	Active Directory Container
2Factor Enabled	oneidentity.local/Columbus/Groups

Select this object type: Users, Groups, or Built-in security principals

From this location: Entire Directory

Enter the object names to select (examples):

f. Right-Click Policies > New > Defender Policy

   i. Enter a name for the policy, such as "Token Auth" then click Next

   ii. Leave Token selected for the method, change the login attempts if required, leave "Use Synchronous tokens as Event tokens" unchecked, click Next

   iii. Leave "none" selected, click Next

   iv. Uncheck "Enable account Lockout". This setting can be re-enabled later on once all testing has been concluded and users are using the product normally. Click Next

   v. Leave "Enable Defender Password Expiry" and "Enable PIN Expiry" unchecked, click Next. Click Finish.

g. Right-Click Security Servers > New > Defender Security Server

   i. Type a user friendly name such as DSS1

   ii. Enter the IP or DNS name of the server that the security server is installed on.

   iii. Next > Next > Finish

h. Double-Click your Security Server object that has just been created to bring open the properties window.

   i. Click on the Access Nodes tab, then click Assign. Double-click your newly created Access Node, then click Ok

   ii. Click on the Policy Tab, then Select. Double-click your newly created policy, then click Ok

   iii. Click Ok to save and close the properties window.

Pro-Tip: It is advised to install more than one Defender Security Server in your network for redundancy. To do this, simply repeat steps 2a and 2b on a different server, preferably running on different hardware. Then repeat steps 2g, and 2h in Active Directory. If your company has more than one office, it is advised that you install at least two instances of the Defender Security Server in each geographical location to reduce latency and provide fault tolerance for the enterprise.

3. Configuring the self-service portal

a. On each server hosting a Defender Security Server, navigate to the Logs folder and share the folder with the service account you used during installation. By default, the Logs folder is located in the following directory:

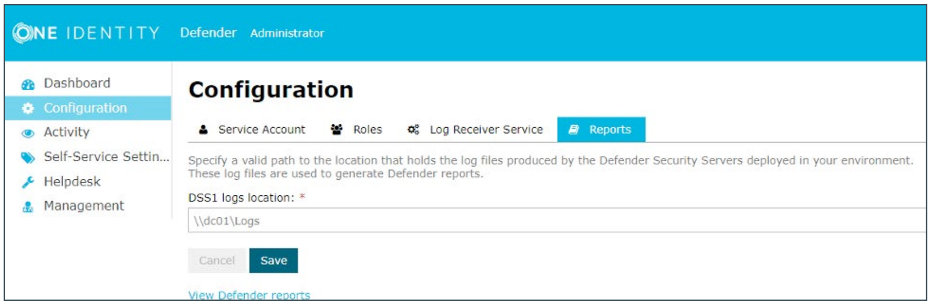
   i. C:\Program Files\One Identity\Defender\Security Server\Logs

b. Open the Defender Management Web portal which can now be found in your installed programs.

   i. Login using a domain admin account, or the account used during installation.

c. Click Administer Defender

d. Click Configuration, and then Reports. For each Security Server instance, type the share path to the Logs folder.



Configuration

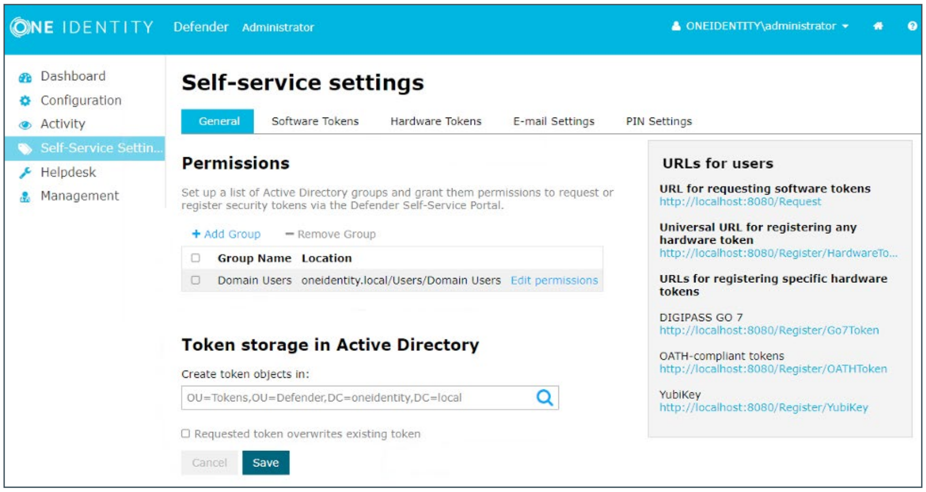
Specify a valid path to the location that holds the log files produced by the Defender Security Servers deployed in your environment. These log files are used to generate Defender reports.

DSS1 logs location: *

\\dc01\Logs

e. Click Self-Service Settings, then + Add Group. Select the security group you want to allow the permission to self-register a software token. This is usually the same group that is defined in the Access Node configuration in step 2e.

   i. Click “Edit Permissions” to modify which platforms can be requested. Once this is done, click Save.



Self-service settings

Permissions

Set up a list of Active Directory groups and grant them permissions to request or register security tokens via the Defender Self-Service Portal.

□	Group Name	Location
□	Domain Users	oneidentity.local/Users/Domain Users

Token storage in Active Directory

Create token objects in:

OU=Tokens,OU=Defender,DC=oneidentity,DC=local

□ Requested token overwrites existing token

URLs for users

URL for requesting software tokens
http://localhost:8080/Request

Universal URL for registering any hardware token
http://localhost:8080/Register/HardwareTo...

URLs for registering specific hardware tokens

DIGIPASS GO 7
http://localhost:8080/Register/Go7Token

OATH-compliant tokens
http://localhost:8080/Register/OATHToken

YubiKey
http://localhost:8080/Register/YubiKey

Pro Tip: It is advised to enable verification during the user self-service experience for security purposes. If this is not a requirement for your company, simply skip step 3f and continue to 3g.

f. Click Software Tokens, select the drop-down menu and pick the method of user verification that works best for your company. Email is an included feature, TeleSign requires an active subscription to the service (not included with Defender). Click Save.

g. Click Email Settings, and enter your company's SMTP details for the product to send emails. Test the settings, and click Save.

Defender is now installed and configured. The last step is to invite your users to access the web portal and self-register their tokens. Additionally, in order for your point of authentication to start using Defender 2FA, you will need to configure it to use RADIUS authentication. This step is not covered in this guide, but you will need to enter the IP addresses for your Defender Security Server in this step, as well as the authentication port (1812 was used in this guide) and shared secret.