



# DigitalPersona® Defender

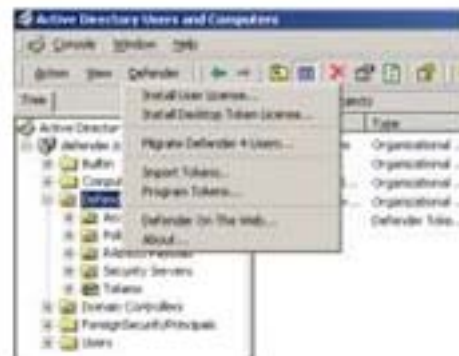
## Quick Start Guide



DATA PROTECTION • REMOTE ACCESS • SECURE COMMUNICATION • STRONG AUTHENTICATION • ACCESS RECOVERY • SINGLE SIGN-ON

## Key questions

- Are the machines where I will install Defender in a secure location?
- Do the machines where I will install the Defender Security Server(s) have static IP addresses?
- Do I have the required administrative privileges on these machines?
- Have I configured the service account that will be used by the Defender Security Server to connect to Active Directory?
- Have I got my Defender User License, and, if appropriate, my Desktop Token License?
- Have I got the token information file(s) delivered with my tokens?



## Pre-installation Considerations

DigitalPersona recommends that all machines running Defender are located where you can strictly control access to them. Consider adding a second Defender Security Server to ensure that user authentication can continue if one becomes unavailable. Defender components communicate with each other using the methods described below. If your environment uses routers and firewalls, these must be configured to allow the Defender components to communicate.

The Defender Security Server uses LDAP to communicate with the domain controllers in Active Directory using port 389 and port 636.

Defender Access Nodes relate to the firewalls, VPN devices, etc within your environment. These use RADIUS to communicate with the Defender Security Server. RADIUS communication uses ports UDP 1812/1813 or 1645/1646.

Defender Agents use TCP port 2626 to communicate with the Defender Security Server.

Before you install Defender, ensure that the following tasks have been completed.

- The account used to install Defender is a member of the Domain Admins group
- The account used to install the Schema updates is a member of the Schema Admins group. Schema updates are installed the first time you install the Defender Console
- You have created the service account that the Defender Security Server will use to access Active Directory, and that this account is a member of the Domain Admins group, or has the correct permissions assigned. For further information, refer to Setting Permissions and Control Access Rights in the Defender Installation Guide.

## Installing Defender

The essential Defender components are:

- MMC Snap-in - extends the Active Directory Users and Computers tool to include the Defender Management Console
- Schema updates - updates to your Active Directory Schema required to support Defender. Schema updates are installed the first time you install the Defender Console
- Defender OU - default container for Defender objects
- Defender Security Server - authenticates RADIUS and Defender Agent requests.

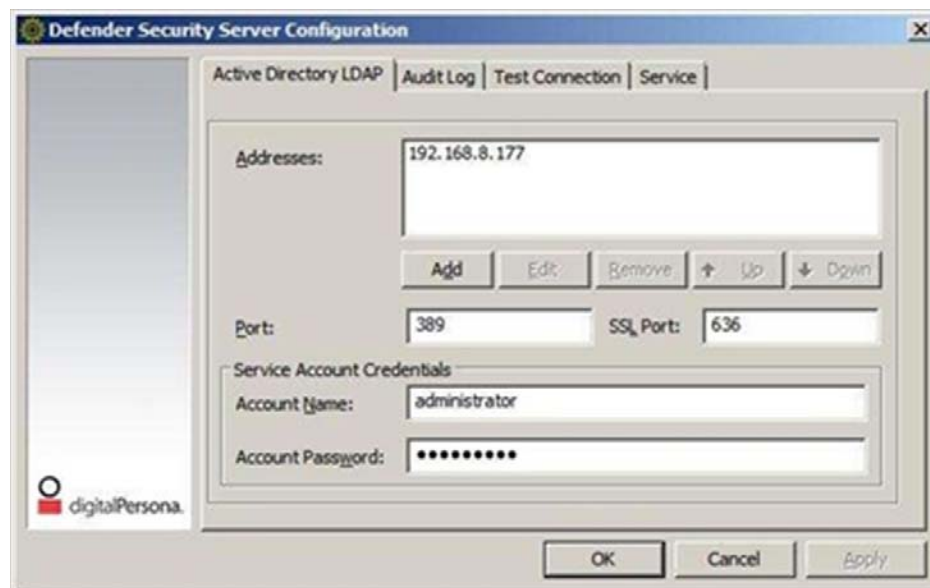
If you can answer YES to all of the KEY QUESTIONS, you are ready to install Defender:

- run DefenderADE MMC Installer.exe to install the Schema updates, MMC Snap-ins and create the Defender container
- run Defender Security Server Installer.exe to install the Defender Security Server and configure LDAP options for communication with Active Directory.

## Configuring the Defender Security Server

Configure the Defender Security Server to communicate with Active Directory.

- 1 In the Address field, type the DNS name of your Active Directory domain or DNS/IP addresses of the specific domain controllers and global catalog servers that will be used by the Defender Security Server when communicating with Active Directory.



- 2 In the Port field, type the number of the LDAP port that the Defender Security Server will use to establish a connection to Active Directory. The default port number is 389.
- 3 In the SSL Port field, type the number of the port that the Defender Security Server will use to establish a secure connection to Active Directory. The default SSL port number is 636.
- 4 In the Admin User field, type the full distinguished user name for the service account that the Defender Security Server will use to connect to Active Directory, e.g. n=DefSrvAcct,cn=users,dc=acme,dc=com.
- 5 In the Admin Password field, type the password used by the service account defined in the Admin User field above.
- 6 Select the Test Connection tab, then click Test to confirm LDAP connectivity.
- 7 Click OK.

## Installing License(s) and Token Information

- 1 Open Active Directory, Users and Computers.
- 2 Select the Defender container, then select Defender on the menu bar. From the drop-down menu, select the options appropriate to your Defender configuration:
  - Install User License (required)
  - Install Desktop Token License (optional)
- 3 Follow the on-screen installation instructions.

## Importing Hardware Token Serial Numbers

- 1 In Active Directory, Users and Computers, click Defender on the menu
- 2 Select Import Tokens to start the Defender Import Wizard.
- 3 Click Next, then Browse to navigate to the location of the Defender token definitions file, export.dpx.
- 4 Copy the key from the email sent to you by DigitalPersona Licensing.
- 5 Paste the key into the Key field in the File and Key dialog.
- 6 Click Next.
- 7 Specify the mode that you want the tokens to operate in, either challenge/response or response only.

If required, you can check both boxes to import the response only and challenge/response records for each token.

If you are importing a token type that can be used in synchronous mode only, the Response Only and Challenge Response checkboxes are not displayed.

- 8 Click Select All to import all available tokens.
- 9 Click Next.
- 10 Click Next to accept the default location.
- 11 Click Next.
- 12 Click Finish.

## **Defining Defender Components**

### **Defining a Security Policy**

To define a Defender security policy

- 1 Select the Defender container, then right-click Policies, New Defender Policy.
- 2 When prompted, type a name and description for the policy.
- 3 Accept all default responses.

### **Defining a Defender Security Server**

To define a Defender Security Server

- 1 Select the Defender container, then right-click Security Servers, New Defender Security Server.
- 2 When prompted, type a name, the IP address and a description of your Defender Security Server.
- 3 Accept all default responses.

### **Defining an Access Node**

To define a Defender access node

- 1 Select the Defender container, then right-click Access Node, New, Defender Access Node.
- 2 When prompted complete the following tasks.
  - Type a name and description for the access node .
  - Accept the default Access Node type and user ID.
  - Enter the IP address, port number and shared secret of the access device that will communicate through this access node (e.g. VPN Server, RRAS, WebMail).

- 3 In the right-hand pane, double-click your new Access Node.
- 4 The Properties dialog opens. Click **Assign** to assign this Access Node to a Defender Security Server.
- 5 On the Members tab, define the users/groups who will authenticate through this Access Node. On the Policy tab, assign a security policy to this Access Node.

## Assigning a Token to a User

To assign a token to a user

- 1 Select Users, then double-click the required user in the right-hand pane.
- 2 Select the Defender tab and complete one of the following tasks.
  - For a hardware token - click Add to assign a token to this user.
  - For a software token - click Program. The Token Programming Wizard starts. Generate a token Activation Code. Install the Token Software on the user's PC or other device, then enter the Activation Code.

For further information, refer to the Defender Token User Guide.

## Additional Defender Components

Additional Defender components can be included in your Defender environment as required. For further information, refer to the Defender Installation Guide.

- Defender WebMail provides secure web-based access to your e-mail system from any web browser - anytime, anywhere.
- Defender Reports provides detailed reporting on Defender configuration, user configuration, authentication statistics, audit trail and token information.
- Defender Self-Registration allows users to register their own new or replacement Go.x tokens
- Defender Desktop Login adds two-factor authentication to the Windows Desktop Login
- Defender EAP Agent utilizes the EAP protocol to implement two factor authentication on a Microsoft VPN/RRAS Server.