CHAPTER 3
DEFENDER EAP AGENT ............................................. 33
  INTRODUCTION ................................................. 34
  DEFENDER EAP AGENT .................................... 35
INSTALLING THE DEFENDER EAP AGENT .................. 36
  INSTALLING ON RRAS SERVER OR NETWORK POLICY SERVER . 36
  INSTALLING ON THE WINDOWS CLIENT ................. 38
CONFIGURING THE RRAS SERVER OR NETWORK POLICY .... 43
CONFIGURING THE VPN CLIENT ............................ 48
AUTHENTICATING ............................................. 50
About this Guide

- Quest One Identity Solution
- Why Defender?
- RADIUS Authentication
- Communications Protocol
- Defender Tokens
- Benefits of Defender
- Audience and Scope
- Conventions
- About Quest Software
- Contacting Quest Software
Defender is a component of the Quest One Identity Solution, a set of enabling technologies, products, and integration that empowers organizations to simplify identity and access management by:

- Reducing the number of identities
- Automating identity administration
- Ensuring the security of identities
- Leveraging existing investments, including Microsoft Active Directory

Quest One improves efficiency, enhances security and helps organizations achieve and maintain compliance by addressing identity and access management challenges as they relate to:

- Single sign-on
- Directory consolidation
- Provisioning
- Password management
- Strong authentication
- Privileged account management
- Audit and compliance.
Why Defender?

Defender is an easy-to-install, simple-to-use product that utilizes the power and flexibility of Microsoft Active Directory (AD) to provide strong two-factor authentication for your organization.

The two-factor authentication requires something unique the user has (a security token) and something unique that the user knows (a PIN).

Figure 1: Defender Environment

RADIUS Authentication

Defender allows authentication by means of the RADIUS protocol for environments that include RADIUS users and/or RADIUS protected access devices.
Benefits of Defender

Some of the benefits that Defender brings to your organization are:

- seamless integration with Microsoft AD, using AD administration tools and techniques
- centralized administration for all Defender users
- simple migration from earlier versions of Defender with no change to end-user experience
- automated replication and backup for Defender data
- multiple points of authentication for load balancing and redundancy
- the ability for users to register their own hardware and software tokens using the Token Deployment System
- Defender Desktop Login for Windows
- extensive reporting facilities
- integration with other Quest products including Webthority, Quest Password Manager, ActiveRoles Server, Change Auditor and Quest Authentication Services.

Audience and Scope

This guide is intended for administrators who want to install and configure Defender for use with remote access products.

This book does not provide tutorial information on the use of the Windows operating system or on network communication concepts. Users must have experience in using the specified operating system and an understanding of networking concepts.
# Conventions

In order to help you get the most out of this guide, we have used specific formatting conventions. These conventions apply to procedures, icons, keystrokes, and cross-references.

<table>
<thead>
<tr>
<th>ELEMENT</th>
<th>CONVENTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select</td>
<td>This word refers to actions such as choosing or highlighting various interface elements, such as files and radio buttons.</td>
</tr>
<tr>
<td><strong>Bolded text</strong></td>
<td>Used to highlight installation questions and responses.</td>
</tr>
<tr>
<td><strong>courier text</strong></td>
<td>File, daemon, utility, option, attribute names.</td>
</tr>
<tr>
<td><strong>Italic text</strong></td>
<td>Used for comments.</td>
</tr>
<tr>
<td><strong>Bold Italic text</strong></td>
<td>Used for emphasis.</td>
</tr>
<tr>
<td><strong>Blue text</strong></td>
<td>Indicates a cross-reference. When viewed in Adobe Acrobat, this format can be used as a hyperlink.</td>
</tr>
<tr>
<td><strong>Best Practice</strong></td>
<td>Used to highlight additional information pertinent to the process being described.</td>
</tr>
<tr>
<td><strong>Warning</strong></td>
<td>Used to provide Best Practice information. A best practice details the recommended course of action for the best result.</td>
</tr>
<tr>
<td><strong>Caution</strong></td>
<td>Used to highlight processes that should be performed with care.</td>
</tr>
<tr>
<td>+</td>
<td>A plus sign between two keystrokes means that you must press them at the same time.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>\</td>
<td>The back slash, immediately followed by a new line, indicates a Unix command line continuation.</td>
</tr>
<tr>
<td>&lt;version&gt;.&lt;build number&gt;</td>
<td>References to the product version you are installing are displayed with &lt;version&gt;.&lt;build number&gt; in angle brackets.</td>
</tr>
</tbody>
</table>
About Quest Software

Quest Software, Inc., a two-time winner of Microsoft’s Global Independent Software Vendor Partner of the Year award, delivers innovative products that help organizations get more performance and productivity from their applications, databases, Windows infrastructure and virtual environments. Through a deep expertise in IT operations and a continued focus on what works best, Quest helps more than 100,000 customers worldwide meet higher expectations for enterprise IT. Quest’s Windows management solutions simplify, automate secure and extend Active Directory, Exchange Server, SharePoint, SQL Server, .NET and Windows Server as well as integrating Unix, Linux and Java into the managed environment. Quest Software can be found in offices around the globe and at www.quest.com.

Contacting Quest Software

Phone  949.754.8000 (United States and Canada)
Email  info@quest.com
Mail  Quest Software World Headquarters
      5 Polaris Way
      Aliso Viejo, CA 92656
Web site  www.quest.com

Please refer to our Web site for regional and international office information.

Contacting Customer Support

Quest Software's world-class support team is dedicated to ensuring successful product installation and use for all Quest Software solutions.

SupportLink  www.quest.com/support
Email at  support@quest.com

You can use SupportLink to do the following:

- Create, update, or view support requests
- Search the knowledge base
- Access FAQs
- Download patches
Remote Access

- Introduction
- VPN
- Network Access Server (NAS)
- Defender EAP Agent
Introduction

Defender authentication can be used by 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 permitted access.

This guide describes how to utilize the strong two factor authentication of Defender whilst providing users with remote access facilities.
Remote Access

Remote access is the ability to get access to a computer or a network from a remote distance. Employees in branch offices, telecommuters, and people who are travelling 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.

Remote Access Server

A remote access server is the computer and associated software that is set up to handle users seeking access to your company’s network remotely. 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).
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.

Refer to Defender EAP Agent for installation and configuration information.
Remote Access Configuration

This section describes how to configure Defender for remote access. The configuration described is an example only of a basic configuration using a Cisco ASA Server.

Existing Defender Configuration

It is assumed that you have already performed the following tasks in Defender:

- installed and configured the Defender Security Server that you will later define as the AAAServer
- if you are using hardware tokens, you have imported the token definitions into Defender
- if you are using Defender Desktop tokens, you have installed the Defender Desktop token license.

For installation information, please refer to the Defender Installation Guide.

For configuration information, please refer to the Defender Configuration Guide and Defender Token Administration Guide.
Additional Defender Configuration

This section describes the additional Defender configuration required to enable remote access.

In a step-by-step walk through guide, you will:

- create and configure the Access Node that will handle access requests from remote users
- assign the Access Node to the Defender Security Server where the remote users logon credentials will be authenticated
- configure the Defender Security Policy that will determine the:
  - method of access
  - level of access
  - time period within which access is permitted
  - lockout conditions for invalid logon attempts made by the user.
- assign the Defender Security Policy to the Access Node
- assign users or groups of users to the Access Node
- assign tokens to users
- perform the configuration required on the remote access device you are using.

The **Configuration Example** describes a basic configuration of the Cisco Adaptive Security Device (ASDM) version 6.1, for use with Defender. The configuration procedure will vary depending on the remote access device you are using.
Configuration Example

• Introduction
• Configuration Example
• Configuring your Remote Access Device
• Configuring an IPsec Connection Profile
• Additonal Defender Configuration
• Adding Users or User Groups
Introduction

This section describes the configuration procedure required to enable authentication of remote users who require access to your company’s network.

The configuration example will guide you through:

- how to configure your remote access device
- the additional Defender configuration required.

Configuration Example

Depending on the remote access device you are deploying, the configuration procedure for your own system may vary from the example used in this guide. Refer to the documentation for your remote access device.

The 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 accept the default settings for all other fields.
Configuring your Remote Access Device

During the configuration procedure, you will:

- create an AAA Server Group
- assign the Defender Security Server to the AAA Server Group
- configure an IPsec connection profile.

Perform the following steps:

1. From the Cisco ASDM Console, select Configuration, Remote Access VPN, AAA/Local Users, AAA Server Groups.

![Cisco ASDM Console](image)

Figure 1: Cisco ASDM Console
2. Click **Add**. The **Add AAA Server** dialog is displayed:

![Add AAA Server Group dialog]

**Figure 2: Cisco - Add AAA Server Group**

You will now create an AAA Server group called Defender. The Defender Security Server will be added to this group later in the procedure.

3. In the **Server Group** field, enter the name of the group, **Defender**.
4. In the **Protocol** field, select **RADIUS**.
5. Click **OK**. The Defender group is displayed in the **AAA Server Groups** window of the Cisco ASDM console:

![Cisco ASDM Console]

**Figure 3: Cisco ASDM Console**
6. In the **Servers in the Selected Group** window, click **Add**. The **Add AAA Server to Group** dialog is displayed:

![Add AAA Server](image)

**Figure 4: Cisco - Add AAA Server**

7. In the **Server Name or IP Address** field, enter the name or IP address of the Defender Security Server where the users will be authenticated.

8. In the **Server Authentication Port** field, enter the port used by the Defender Security Server to receive authentication requests, **1645**.

9. In the **Server Secret Key** field, enter the shared secret used by the Defender Access Node and Defender Security Server. This is found in the
Shared Secret field on the Defender Access Node Connection Details dialog.

![Add AAA Server](image)

**Figure 5: Cisco - Add AAA Server**

10. Click **OK** to return to the Cisco ASDM console.
The AAA Server Group, **Defender**, and the IP Address of the Defender Security Server belonging to the AAA Server Group, are listed.

**Figure 6: Cisco ASDM Console**
Configuring an IPsec Connection Profile

1. From the Cisco ASDM console, select Configuration, Remote Access VPN, Network (Client) Access, IPsec Connection Profiles:

![Cisco ASDM Console](image)

**Figure 7: Cisco ASDM Console**

This example assumes you are using an existing profile. For information on creating a connection profile, refer to the documentation for your remote access device.

2. In the **Connection Profiles** window, select the required profile. For this example we have selected **VPNtest**.
3. Click **Edit**. The **Edit IPsec Remote Access Connection Profile** dialog is displayed:

![Cisco - Edit IPsec Remote Access Communication Profile](image)

**Figure 8: Cisco - Edit IPsec Remote Access Communication Profile**

4. In the **User Authentication, Server Group** field, select **Defender**.
5. Click **OK**.
Additonal Defender Configuration

This section describes the Defender configuration. In the following steps, we will:

- configure the Defender access node
- assign the access node to the Defender Security Server
- create and assign a security profile to the access node
- add users and user groups to the access node
- assign a Defender token to a user.

From the Defender Administration Console, click the **Defender** OU and then right-click **Access Nodes**.

1. From the menu, select **New, Defender Access Node**.
2. The **New Object - Defender Access Node** dialog is displayed:

![New Object - Defender Access Node dialog](image)

**Figure 9: New Object – Defender Access Node** (name and description) dialog

3. In the **Name** field, enter a name for this access node, **Cisco**.
4. In the **Description** field, type a description for this access node.
5. Click **Next** to continue. The **New Object - Defender Access Node** (node type) dialog is displayed:

![New Object - Defender Access Node dialog](image)

**Figure 10: New Object – Defender Access Node dialog**

6. In the **Node Type** field, click the arrow and select **Radius Agent**. This node type will allow Cisco ACS devices to connect to Defender using the RADIUS protocol. RADIUS is transmitted over UDP and uses port 1645 or 1812.

7. In the **User ID** field, select the required user ID type from the list.

   This is the user ID that will be used to locate the user in the Active Directory. The options are:
   
   - SAM Account Name
   - Defender ID
   - User Principal Name
   - Proper Name
   - Email Address.
8. Click Next to continue. The New Object - Defender Access Node (connection details) dialog is displayed:

![New Object - Defender Access Node Connection Details dialog](image)

**Figure 11: New Object – Defender Access Node Connection Details dialog**

9. In the **IP Address or DNS Name** field, type the IP address or DNS name of the Cisco AAA Server.

10. In the **Port** field, type the port number that this Access Node will use to establish a connection with the Defender Security Server. The default port number is 1812.

   This is the same as the entry in the **Server Authentication Port** field on the Cisco **Add AAA Server** dialog.

11. In the **Shared Secret** field, type the secret that will be used when this Access Node attempts to establish a connection with the Defender Security Server.

   The shared secret can be up to 256 alphanumeric characters.

   This is the same as the entry in the **Server Secret Key** field defined on the Cisco **Add AAA Server** dialog.
12. Click **Next** to continue. The **New Object - Defender Access Node** (summary) dialog is displayed:

![New Object - Defender Access Node Summary dialog](image)

**Figure 12: New Object – Defender Access Node Summary dialog**

**Adding Users or User Groups**

To specify the users and/or groups of users who will be authenticated by the Defender Security Server via this Access Node, perform the following steps:

1. Click the **Defender** OU, then click **Access Nodes**.
2. Right-click the required Access Node.
3. From the menu, select **Properties**. The **Access Node** dialog is displayed.
4. Select the **Members** tab. The **Cisco Properties - Members** dialog is displayed:

![Cisco Properties - Members dialog]

**Figure 13: nodename Properties - Members dialog**

5. Click **Add** to select a user or group of users. The **Select Users or Groups** dialog is displayed.

![Select Users or Groups dialog]

**Figure 14: Select Users or Groups dialog**

6. To specify the object type(s) to be included in the search, click **Object Types**. The **Object Types** dialog is displayed. Check the box adjacent to the required object types, then click **OK**. The **Select Users** dialog box is displayed.
7. To specify the directory location that will be searched, click **Locations**. The **Locations** dialog box is displayed. Select the required directory location, then click **OK**. The **Select Users** dialog box is displayed.

8. In the **Enter the object names to select** field, type the object name(s) that will be used to match with users and/or groups.

   For more specific search options, click **Advanced**.

9. Click **OK** to save your settings and return to the **Members** dialog box. Selected users/groups are displayed in the **Members** table.

10. Click **OK** to return to the AD **Users and Computers** tree.

    The additional Defender configuration is now complete.
Defender EAP Agent

- Introduction
- Installing the Defender EAP Agent
Introduction

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 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.
Defender EAP Agent

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 is installed on the VPN Server and VPN Client machine.

System Requirements
Microsoft Windows Operating System:

- Microsoft Windows 2003/2008/2008 R2
- Microsoft Windows XP
- Microsoft Windows Vista
- Windows 7.
Installing the Defender EAP Agent

This section describes how to install the Defender EAP Agent on your VPN server and VPN Client.

Installing on the RRAS Server or Network Policy Server (VPN Server)

1. To install the Defender EAP Agent on the Windows Server, select Defender EAP Agent from the Components tab of the Defender Autroun or run Defender5_EAP_Install.exe. You must restart your machine to complete the installation.
2. Select Next. The **License Agreement** dialog is displayed.

3. Accept the License Agreement before continuing. Select **Next** to display the **Install Location** dialog.
4. Either accept the default location or use the **Browse** button to select a different location. Select **Next** to continue.

5. The installation will continue and the **Installation Complete** dialog is displayed on completion. Ensure that **Create a VPN connection with Defender** is not selected. Select **Finish**.

6. Restart the server to complete the installation.

**Installing on the Windows Client**

1. To install the Defender EAP Agent on your Windows client, select Defender EAP Agent from the Components tab of the Defender Autroun
or run Defender5_EAP_Install.exe. You must restart your machine to complete the installation.

2. Select **Next**. The **License Agreement** dialog is displayed.
3. Accept the License Agreement before continuing. Select **Next** to display the **Install Location** dialog.

![Installation Location Dialog]

4. Either accept the default location or use the **Browse** button to select a different location. Select **Next** to continue.

![Browse Button]

5. The Installation will continue and the **Installation Complete** dialog displayed on completion. To create a VPN connection that will be automatically configured to use Defender EAP ensure that **Create a VPN connection with Defender now** is selected.

![Installation Complete Dialog]
6. Select Finish to run the **VPN Connection wizard** or **Cancel** if you wish to create the connection at a later date.

7. Select **Next** to continue.
8. Enter a display name for this connection and select **Next** to continue.

![VPN Server Selection](image1.png)

9. Enter the IP Address or Name of the server that you will be connecting to, then select **Next**.

![Defender New VPN Connection Wizard](image2.png)

10. The **VPN Connection wizard** is now complete, select **Finish**.

11. Restart the workstation to complete the installation.
Configuring the RRAS Server or Network Policy

The following examples describe the configuration settings required for Defender EAP. A network policy must be configured allowing VPN access to your network.

**Windows Server running RRAS only**

To configure the RRAS Server, follow the instructions below. Please note that configuration instructions for RRAS Server 2008 may differ slightly from the instructions provided below.

Server Configuration - Stage 1

1. From **Administrative Tools**, select the **Routing and Remote Access Administration** option. The **Routing and Remote Access** page is displayed:

2. Right click the required server name, then select **Properties**.
3. Select the **Security** tab.
4. Select **Authentication Methods**.
5. Select **EAP Methods**.
6. Select **Defender 5.x**.
7. Select **OK** to return to the **Routing and Remote Access** page.

Server Configuration - Stage 2
1. From the **Routing and Remote Access** page:

2. Select **Remote Access Policies**.
3. From the right hand window pane, right click the required policy and select **Properties**.

4. Select **Edit Profile**, then select the **Authentication** tab.

5. Select **EAP Methods**, then select **Add**.

6. Select **Defender 5** from the list and select **OK**.

7. Click **Edit**.

8. In the **IP Address** field, type the IP Address of the server hosting your Defender Security Server.

9. In the **Port** field, type the port number that is defined on your Access Node.

10. In the **Shared Secret** field, specify the shared secret defined on your Access Node.

11. Select **OK**.

12. Restart the RRAS service.

    The RRAS server configuration is now complete.
Windows Server running Network Policy Server

To configure a server such as Windows 2008 where Network Policy server is running please follow the instructions below.

1. Select the network policy that will be used by your users and view the **Properties** dialog.
2. Select the **Constraints** tab and then **Authentication Methods**.
3. Select **Add**.
4. From the **Add EAP** dialog select **Defender 5**.

5. Select **OK**.
6. Highlight **Defender 5** within the **EAP Types** table and select **Edit**.

7. Enter the address of the DSS that will be used to authenticate your users, together with the Port and Shared Secret that correspond to the access node that will be used.
Configuring the VPN Client

This section describes how to configure the Microsoft VPN Client. This procedure must be performed on the connection object, not a short-cut to the connection.

1. Access the **Properties** pages for your VPN Connection, then select the **Security** tab.

2. Select **Advanced (custom settings)**.
3. Select **Settings**. The **Advanced Security Settings** dialog is displayed:

![Advanced Security Settings dialog]

4. In the **Logon Security** section, click **Use Extensible Authentication Protocol (EAP)**.
5. Select **Defender 5** from the list of providers.
6. Select **OK** to close any open dialog boxes.

Your VPN Client configuration is now complete.
Authenticating

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 access to the network.