One Identity Defender 6.4.1

Product Overview

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (http://www.OneIdentity.com) for regional and international office information.

Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at http://www.OneIdentity.com/legal/patents.aspx.

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal. All other trademarks are the property of their respective owners.

Legend

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

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

Defender Product Overview
Updated - 13 April 2023, 02:54
Version - 6.4.1

Contents

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=.
- **Push Notifications to your mobile devices**: Defender can be configured to send push notifications on mobile devices with the help of the MMC tokens. These push notifications display the customized information related to Defender's functional and operational aspects. For more information about this feature, see "Push Notifications" section in the *Defender Administration Guide*.
- **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 Guide*.
- **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*.
- **Managed Service Accounts**: In Windows Server 2008 R2, Microsoft introduced the managed service account, which improves security by eliminating the need for an administrator to manually manage the credentials for each service account. Instead, an sMSA establishes a complex password and changes that password on a regular basis (by default, every 30 days). Defender also supports Managed service accounts and they can be used to delegate control, securely run services, applications and scheduled tasks. The sMSA functionality with Defender is similar to that in Active Directory.

What you can do with Defender

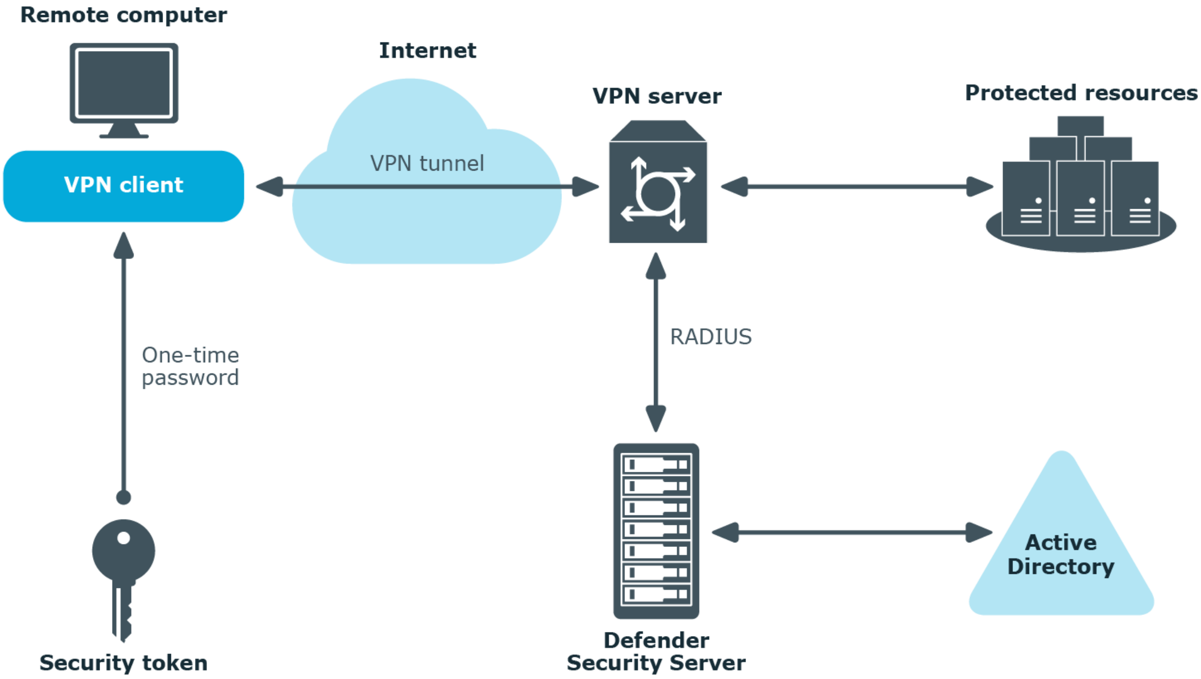
This section provides an overview of the most common Defender usage scenarios and the Defender components required for each scenario. For instructions on how to configure Defender for a particular scenario, see the *Defender Administration Guide*.

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):

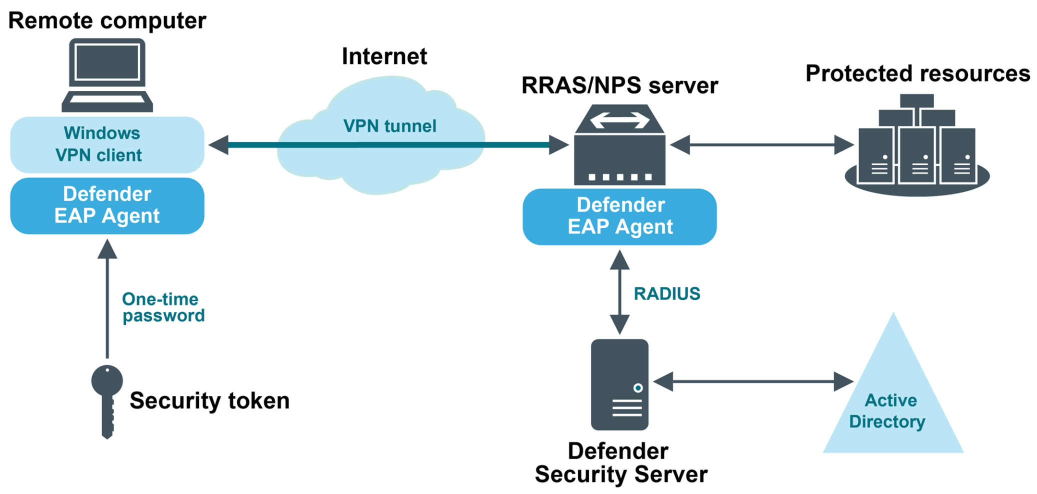


In this scenario, the VPN server is configured to redirect the user to the Defender Security Server, which prompts the user to submit a passcode. The user needs to generate a passcode by using a security token provided by Defender administrator. The Defender

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).

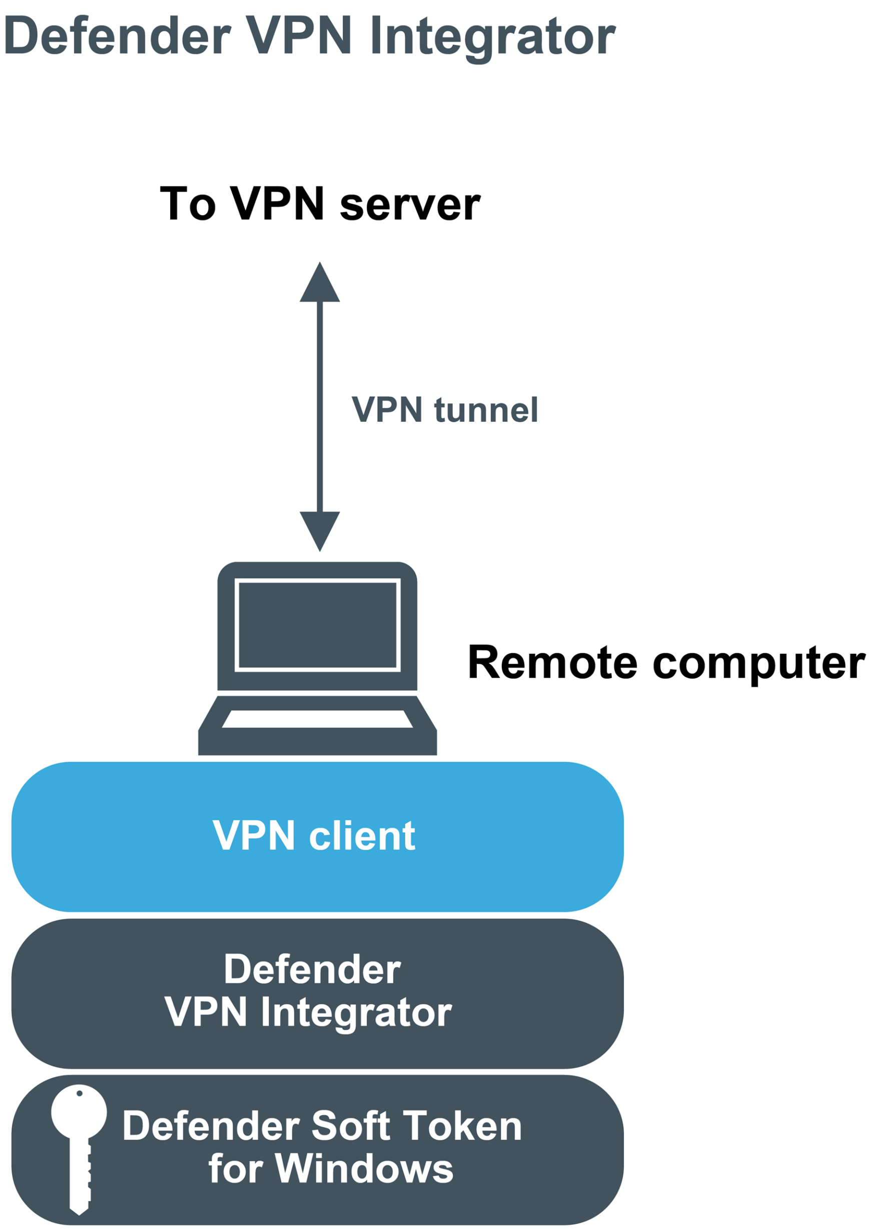
Defender and VPN access via RRAS/NPS server



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).

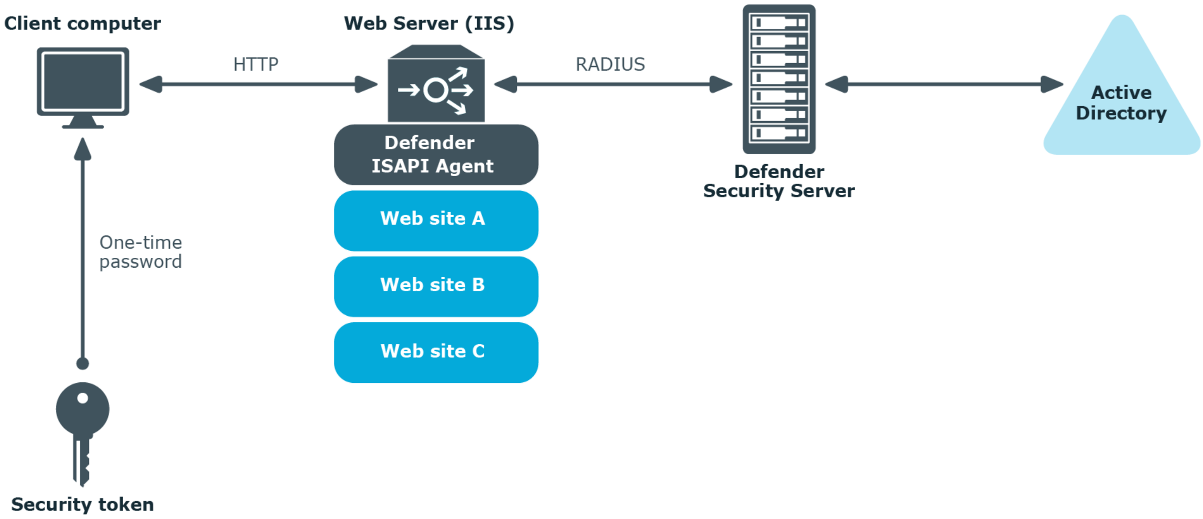
If VPN users in your environment authenticate using the Defender Soft Token for Windows, you can simplify the authentication experience for these users by deploying the Defender VPN Integrator component on their workstations.



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

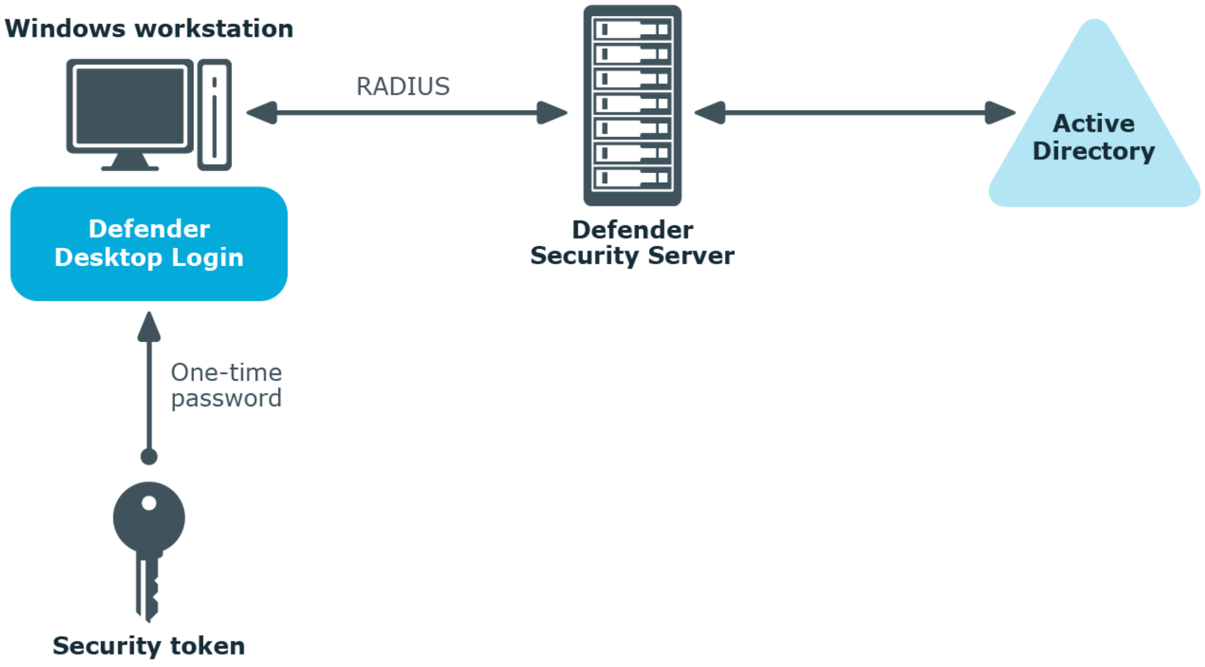
The next diagram illustrates a scenario where Defender is configured to authenticate the users who access Web sites hosted on Microsoft Internet Information Services (IIS).



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.

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