One Identity Defender 5.9

Release Notes

Monday, October 30, 2017

These release notes provide information about the One Identity Defender release.

About One Identity Defender 5.9

Defender enhances security by using two-factor authentication to authenticate the users who request access to valuable resources within your organization. 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 5.9 is a minor release, with the product rebranded to One Identity Defender.

See New features and Enhancements.

New features

New features in Defender 5.9:

- **Rebrand to One Identity** This product was rebranded as One Identity Defender.
- **Support for Windows Server 2016** Added support for Windows Server 2016 to One Identity Defender
- **Support for Active Roles 7.1** Added support for Active Roles 7.1 to One Identity Defender
- **Support for Active Roles 7.2** Added support for Active Roles 7.2 to One Identity Defender

See also:

Enhancements

Resolved issues

Enhancements

The following is a list of enhancements implemented in Defender 5.9.

Table 1: General enhancements

Enhancement	Issue ID
Defender Self-Service Portal integration with TeleSign now uses the TeleSign REST API.	639825

Resolved issues

The following is a list of issues addressed in 5.9 release.

Table 2: Defender Desktop Login resolved issues

Resolved Issue	Issue ID
The offline cache count in the Defender Desktop Login may not be reset correctly. This may happen if the user has a VPN connection to an external network.	616766
Offline login to the Defender Desktop Login is slow.	598868
In an environment with multiple domain controllers, when a domain controller is unavailable, users may be able to log on to a system using Defender Desktop Login bypassing Defender authentication.	654124
The authentication may be slower than usual, when authenticating using the Defender Desktop Login.	695466
The Defender Desktop Login may have a security vulnerability.	620882
The Defender Desktop Login may have a security vulnerability.	672530
Slow response when logging in using Defender Desktop Login.	695466
The offline token cache used by the Defender Desktop Login may not be updated for a user. This can happen if the user's DN contains a backslash ('\').	366766
Offline login using Defender Desktop Login may take several minutes.	598868
The Defender documentation erroneously states that the shared secret specified in an Access Node can be up to 256 characters. The shared secret is limited to 63 characters and authentication may fail, if a longer shared secret is specified.	595786
When trying to authenticate using Defender with correct passcode, user gets an error "The passcode you entered is invalid. Enter a correct passcode followed by token response."	715156

Table 3: Defender Management Portal resolved issues

Resolved Issue	Issue ID
The service account specified in the Defender Management Portal settings may not be added to the Administrators group. This can happen if the Local Administrators group name is different from "Administrators".	612874
On Defender Management Portal, reports are not getting generated.	645603
When scheduling multiple reports in the Defender Management Portal, not all the reports may be generated.	632151
In User details report, the Logon Count is displayed as 0.	683314
A user with correct permissions may receive an error when trying to log in to the Defender Management Portal. This can happen when Windows Authorization Access Group or Pre-Windows 2000 Compatible Access permissions have been	690209

Resolved Issue	Issue ID
removed for the user.	
Defender Self-Service Portal integration with TeleSign now uses the TeleSign REST API.	639825
When the "Use service account for all actions" is enabled in the Defender Management Portal setting and the service account password is changed, the user may be unable to log in to the Management Portal.	628666
A scheduled report may not be generated in the Defender Management Portal. This can happen if the DSS logs used in the report generation contain ASCII extended characters.	606901
The Defender Management Portal may have a security vulnerability issue.	682626
When generating a Authentication Activity report using the Defender Management Portal, the report may be erroneously empty.	604955
When requesting an Authy token through the Defender Self-Service Portal, the supplied URL to download the token is incorrect.	720795

Table 4: Other resolved isues

Resolved Issue	Issue ID
When requesting a Windows Phone token through the Defender Self-Service Portal, the supplied URL to download the token is incorrect.	704804
Token activation codes may be logged to log files on the machine with the Defender Administration Console.	681341
A website protected by the Defender ISAPI Agent may experience a CPU spike.	668162
Defender Soft Token for Windows is missing after a system crash.	593528
When programming a token using the Defender Web Services API, a blank activation code may be returned.	596053
The ISAPI Agent may have a security vulnerability issue.	713737
When activating a token using Soft Token for Windows, token activation may fail. This can happen if the name of the token contains a backslash ('\').	412394
The token may be assigned incorrectly, when assigning a token to a user using the Defender Web Service API.	596074
When assigning a token to a user using the Defender Web Service API, the token may not be returned by a subsequent call to getTokensForUser of the Web Service API.	598480

Known issues

The following is a list of issues, including those attributed to third-party products, known to exist at the time of release.

Table 5: General known issues

Known Issue	Issue ID
"The request is not supported" error occurs when trying to authenticate on a Windows Server 2016 machine using Defender EAP Agent. **Workaround:** Use the Microsoft CMAK (Connection Manager Administration Kit) to create a VPN connection. Deploy and use this CMAK created connection with Windows Server 2016 machines. Do the following to create a CMAK profile on Windows Server 2016 • Ensure the Defender EAP agent is installed. • Control panel | Programs and Features | Turn Windows Features on or off. • Enable RAS Connection Manager Administration Kit (CMAK). • Run the CMAK Wizard from administration tools and create the VPN profile. • Execute the .EXE CMAK connection on the Windows Server 2016 machines.	713585
If 'Test connection automatically' setting in the DSS configuration is enabled, a very large number of DSS logs may be generated. **Workaround** • Workaround 1: Disable the 'Test connection automatically' setting. • Workaround 2: Make sure you have enough space for DSS log files, and periodically delete old log files.	712795
When a user using their GrIDsure token authenticates to a website protected by the Defender ISAPI Agent, they are unable to reset the PIP. This can happen if the user has other tokens assigned to them besides the GrIDsure token. **Workaround** Make sure that no other tokens are assigned to the user, if they are using the GrIDsure token for authentication.	723423
"The user name or password is incorrect." error may occur even when user log-in to the Defender Management Portal with correct credentials. This error message may appear if the domain controller is not available to the Management Portal. **Workaround**	588772

Known Issue	Issue ID
Make sure that the Active Directory functions correctly, and the machine with Defender Management Portal is able to reach a domain controller.	
When authenticating via Defender, users may encounter the message "You must change your password before logging on for the first time" that prevents them from logging in. This may occur if the user's password has expired and the Defender security policy is set to use the proper name or Defender ID for authentication. **Workaround** Do either of the following: 1. Allow users to change their expired passwords using some other means. 2. Change the Defender security policy to use a SAM account name or UPN for authentication.	366713
When a user attempts to log on to a computer protected by Defender Desktop Login with a GrIDsure token for the first time the following error may appear: "Access Denied." This may occur if the user uses an alternate UPN suffix. **Workaround** Switch the user to use the default UPN suffix during the logon procedure.	366722
An attempt to authenticate users using a VIP credential may fail in a child domain, when the VIP credential certificate is installed only in the root domain. **Workaround** Install the VIP credential certificate in the child domain.	366743
A user, authenticating via a Defender Password for the first time, is not prompted to change the password, even though the corresponding option was selected when the password was assigned to the user. This may occur if Defender Password expiration is not enabled in the corresponding security policy. **Workaround** Edit the corresponding security policy object in the Administration Console and enable expiration of the Defender Password.	366794
After you changer the User ID setting on an access node, the change is applied, but appears to not come into effect. **Workaround** Restart the Defender Security Server service. You can use the Defender Security Server Configuration utility to do this.	366822
When attempting to log on to a computer protected by Defender Desktop Login as a local user, you may see the following confusing error message: "The	366824

Known Issue	Issue ID
Defender Security Server could not log you on as your system administrator has denied you the right to log on locally." **Workaround** This error message actually means that you cannot log on as a local user without Defender authentication.	
A user may encounter an error when trying to change the PIN on a token. This issue may occur if a GrIDsure token is also assigned to that same user. **Workaround** Make sure that users who are assigned a token with a PIN do not have a GrIDsure token assigned to them.	366941
The Token Program wizard in the Defender Administration Console may skip pages and produce errors. This may occur when two or more instances of the Administration Console are running at the same time on the same computer. **Workaround** Close all extra instances of the Defender Administration Console and use only one instance.	417432
When you assign a token to a user in the Administration Console, the token may fail to immediately appear in the user's list of tokens. **Workaround** This behavior is due to the replication latency in Active Directory. View the list of tokens after the changes have been replicated.	417457
After you change the user's token list in the Management Portal (e.g. assign a token to the user, or unassigning a token), the list of tokens may remain unchanged. **Workaround** This behavior is due to the replication latency in Active Directory. View the list of tokens after the changes have been replicated.	417714
When using the Management Portal to unlock an account locked by Defender (not Windows), you may see a confusing confirmation message about resetting the violation count. **Workaround** When you unlock an account locked by Defender, the violation count is automatically reset as well.	420395
When accessing the Management Portal for the first time, it is possible to access the Defender reports site, but the reports are non-functional. This may happen because the Management Portal service account has not yet been	421707

Known Issue	Issue ID
configured. **Workaround** Navigate to the Management Portal Administration user interface and configure the service account.	
When you point the mouse cursor on the "Authentication requests by DSS" diagram in the Management Portal Dashboard, the tooltip may list an incorrect value, while the diagram lists the correct value for the number of authentication requests. **Workaround** Do either of the following: 1. Use the value on the diagram. 2. Reload the web page (CTRL+F5) to update the value in the tooltip.	421715
When you use the Defender Integration Pack for ActiveRoles, the Defender license allocation value seen in the ActiveRoles Administration Console may be different from the values in the Defender Administration Console. This may occur in a multi-domain environment when ActiveRoles Server accesses a domain using a domain controller that is not a global catalog. **Workaround** Use the values in the Defender Administration Console, these are the correct values.	429274
When you program mobile software tokens using the Defender Integration Pack for ActiveRoles, the option to program the tokens in challenge-response mode is available. Selecting this option may produce an error. **Workaround** Defender software tokens for mobile devices currently do not support challenge-response mode. Disregard this option.	431278
When trying to access a site protected by the Defender ISAPI Agent, you may see the following error: "Calling LoadLibraryEx on ISAPI filter failed." This may occur if the web site protected by the ISAPI Agent is a 32-bit site running on a 64-bit IIS. **Workaround** If you need to run a 32-bit web site, consider running it on a 32-bit computer with a 32-bit IIS and install the 32-bit version of the Defender ISAPI Agent.	435240
When you enter a verification code when requesting a software token through the Self-Service Portal, you may see the following confusing error message: "The link has expired."	436701

Known Issue	Issue ID
Workaround This error message means that the verification code has expired. Start over with requesting a software token.	
In an environment where the Defender EAP Agent is used in conjunction with the Soft Token for Windows, the passcode from the token may not be accepted when establishing a VPN connection. This issue occurs when Soft Token for Windows is programed in challenge-response mode. **Workaround** Program the Soft Token for Windows in synchronous mode.	439473
The Defender EAP Agent may not integrate with the Soft Token for Windows to retrieve the token response automatically. This issue occurs on a 64-bit operating system. **Workaround** Launch the Soft Token for Windows, and enter the passcode into the VPN client manually.	441655
Users who are directly assigned to an access node cannot be moved to a different OU. **Workaround** Un-assign the user from the access node, move the user, and then assign the user back to the access node. To prevent this issue, assign groups rather than individual users to access nodes.	452765
When Defender EAP Agent is used with a VPN connection, the dialog box to enter the token response does not appear. This issue may occur if EAP Agent is installed on a computer running Windows 10 operating system. **Workaround** Use the EAP Agent installed on a computer running an operating system other than Windows 10.	462928
When you try to uninstall the Defender Soft Token for Java, the uninstallation wizard may finish successfully, but no application files are removed. This may occur on computers running Windows 8 or later with User Account Control enabled. **Workaround** Open the command prompt as administrator and run the following command: java -jar <path to uninstaller file>	487077
When configuring the option "Use service account for all actions" in the Management Portal settings, the 'Save' button is not enabled to save the	504067

Known Issue	Issue ID
changes. **Workaround** Re-enter and re-confirm the service account password to enable the 'Save' button.	
When searching for tokens on the Management Portal, a token is displayed as assigned to a single user, even though the token is assigned to more than one user. This occurs when Internet Explorer is used as the browser. **Workaround** Use a different supported browser.	504432
When trying to authenticate through the ISAPI Agent the following error is displayed: "Invalid Token Response.", even though you have entered the correct token response. This occurs when DSS is unavailable. **Workaround** Make sure that the DSS is available and retry the login attempt.	591408
When Web Service API is the only Defender component installed on a computer, it does not work. **Workaround** Install Defender Management Shell or Management Portal component on the same computer.	597986
After upgrading to the latest version of the Web Service API, both the old and the new versions of the component are present in Windows "Installed Programs" list. **Workaround** Only the latest version gets installed. You can ignore the old version that is listed.	598397
When requesting an SMS token through the Self-Service Portal, the Program Token wizard finishes successfully, but the token is not assigned. This occurs when out-of-band verification is used and the verification link is opened on a device different from the original one. **Workaround** On the final page of the Program Token wizard, click 'Back', click 'Next', and then click 'Finish'.	598605
While trying to log in to the Defender Management Portal after an upgrade to version 5.9, user may see the login screen of the previous version. **Workaround** Clear the browser cache.	722484

Deprecated features

The following features have been deprecated in this release:

- Support for Active Roles Server 6.7 and 6.8
- Support for Windows Vista
- Defender Soft Token for BlackBerry devices running OS 5,6 and 7
- Defender Soft Token for BlackBerry QNX, a legacy Android port for devices running BlackBerry OS 10

  NOTE: If you have already installed soft token on BlackBerry with OS 5, 6 or 7 or soft token for Blackberry QNX, you can continue to use it. But, it is recommended to use soft token on BlackBerry with OS 10 or SMS tokens.

System requirements

You can install Defender on physical computers or virtual machines.

System requirements for Defender components:

- Defender Security Server
- Defender Administration Console
- Desktop Login
- Desktop Login Group Policy
- Defender Management Portal
- Extensible Authentication Protocol (EAP) Agent
- Defender Integration Pack for Active Roles
- ISAPI Agent
- Defender Management Shell
- VPN Integrator
- Client SDK
- Web Service API

System requirements for native Defender software tokens:

- Defender Soft Token for Android™
- Defender Soft Token for BlackBerry
- Defender Soft Token for iOS
- Defender Soft Token for Java

- Defender Soft Token for Windows
- Defender Soft Token for Windows Phone

Defender Security Server

Table 6:
Defender Security Server system requirements

Requirement	Details
Processor	2 GHz or faster, x86 or x64 architecture
Memory (RAM)	2 GB or more
Hard disk space	40 GB or more
Operating system	Your computer must be running one of the following operating systems (with or without any Service Pack): • Windows Server 2016 • Windows Server 2012 R2 (64-bit editions only) • Windows Server 2012 R2 (64-bit editions only) • Windows Server 2012 (64-bit editions only) • Windows Server 2008 R2 (64-bit editions only) • Windows Server 2008 (32- and 64-bit editions)

Defender Administration Console

Table 7:
Defender Administration Console system requirements

Requirement	Details
Processor	1.4 GHz or faster, x86 or x64 architecture
Memory (RAM)	512 MB or more
Hard disk space	2 GB or more
Operating system	Your computer must be running one of the following operating systems (with or without any Service Pack): • Windows Server 2016 • Windows Server 2012 R2 (64-bit editions only) • Windows Server 2012 (64-bit editions only)

Requirement	Details
	• Windows Server 2008 R2 (64-bit editions only) • Windows Server 2008 (32- and 64-bit editions) • Windows 10 (32- and 64-bit editions) • Windows 8.1 (32- and 64-bit editions) • Windows 8 (32- and 64-bit editions) • Windows 7 (32- and 64-bit editions)
Additional software	• Active Directory Users and Computers (ADUC) tool • Microsoft Visual C++ 2013 Redistributable Package (installed automatically together with the Defender Administration Console) • Microsoft .NET Framework 4.5.2 (installed automatically together with the Defender Administration Console)

Desktop Login

Table 8:
Desktop Login system requirements

Requirement	Details
Processor	1.4 GHz or faster, x86 or x64 architecture
Memory (RAM)	512 MB or more
Hard disk space	20 MB or more
Operating system	Your computer must be running one of the following operating systems (with or without any Service Pack): • Windows Server 2016 • Windows Server 2012 R2 (64-bit editions only) • Windows Server 2012 (64-bit editions only) • Windows Server 2008 R2 (64-bit editions only) • Windows Server 2008 (32- and 64-bit editions) • Windows 10 (32- and 64-bit editions) • Windows 8.1 (32- and 64-bit editions) • Windows 8 (32- and 64-bit editions) • Windows 7 (32- and 64-bit editions)

Desktop Login Group Policy

Table 9:
Desktop Login Group Policy system requirements

Requirement	Details
Processor	1.4 GHz or faster, x86 or x64 architecture
Memory (RAM)	512 MB or more
Hard disk space	20 MB or more
Operating system	Your computer must be running one of the following operating systems (with or without any Service Pack): • Windows Server 2016 • Windows Server 2012 R2 (64-bit editions only) • Windows Server 2012 (64-bit editions only) • Windows Server 2008 R2 (64-bit editions only) • Windows Server 2008 (32- and 64-bit editions) • Windows 10 (32- and 64-bit editions) • Windows 8.1 (32- and 64-bit editions) • Windows 8 (32- and 64-bit editions) • Windows 7 (32- and 64-bit editions)

Defender Management Portal

Table 10:
Defender Management Portal system requirements

Requirement	Details
Processor	2 GHz or faster, x86 or x64 architecture
Memory (RAM)	2 GB or more
Hard disk space	40 GB or more
Operating system	Your computer must be running one of the following operating systems (with or without any Service Pack): • Windows Server 2016 • Windows Server 2012 R2 (64-bit editions only)

Requirement	Details
	• Windows Server 2012 (64-bit editions only) • Windows Server 2008 R2 (64-bit editions only) • Windows Server 2008 (32- and 64-bit editions)

Additional software	• Microsoft Internet Information Services (IIS) 10.0, 8.5, 8.0, 7.5, or 7.0, with Forms Authentication and ASP .NET role services enabled (configured automatically by the setup)
	• Microsoft .NET Framework 4.5.2 (installed automatically together with the Defender Management Portal)
	• To access the Defender Management Portal, you can use any of the following Web browsers:
	  • Chrome 15 or later
	  • Firefox 8 or later
	  • Internet Explorer 9 or later (Internet Explorer run in compatibility mode is not supported)
	  • Opera 11.1 or later
	  • Safari 5.1 or later

Extensible Authentication Protocol (EAP) Agent

Table 11:
EAP Agent system requirements

Requirement	Details
Processor	1.4 GHz or faster, x86 or x64 architecture
Memory (RAM)	512 MB or more
Hard disk space	10 MB or more
Operating system	Your computer must be running one of the following operating systems (with or without any Service Pack): • Windows Server 2012 R2 (64-bit editions only) • Windows Server 2012 (64-bit editions only) • Windows Server 2008 R2 (64-bit editions only) • Windows Server 2008 (32- and 64-bit editions) • Windows 10 (32- and 64-bit editions)

Requirement	Details
	• Windows 8.1 (32- and 64-bit editions) • Windows 8 (32- and 64-bit editions) • Windows 7 (32- and 64-bit editions)

Defender Integration Pack for Active Roles

Table 12:
Defender Integration Pack for Active Roles system requirements

Requirement	Details

Required software	• Active Roles 7.2, 7.1, 7.0 or 6.9
	Required Active Roles components:
	  • Administration Service
	  • Web Interface
	  • Active Roles console
	• Defender Administration Console

Operating system	Your computer must be running one of the following operating systems (with or without any Service Pack): • Windows Server 2016 • Windows Server 2012 R2 (64-bit editions only) • Windows Server 2012 (64-bit editions only) • Windows Server 2008 R2 (64-bit editions only) • Windows Server 2008 (32- and 64-bit editions)
Additional software	Microsoft .NET Framework 4.5.2 (installed automatically together with the Defender Integration Pack for Active Roles)

ISAPI Agent

Table 13:
ISAPI Agent system requirements

Requirement	Details
Processor	1.4 GHz or faster, x86 or x64 architecture

Requirement	Details
Memory (RAM)	512 MB or more
Hard disk space	20 MB or more
Operating system	Your computer must be running one of the following operating systems (with or without any Service Pack): • Windows Server 2016 • Windows Server 2012 R2 (64-bit editions only) • Windows Server 2012 (64-bit editions only) • Windows Server 2008 R2 (64-bit editions only) • Windows Server 2008 (32- and 64-bit editions)

Microsoft Internet Information Services (IIS)	IIS 10.0, 8.5, 8.0, 7.5, or 7.0 with the following role services enabled:
	• Web Server/Application Development
	  • ASP
	  • ISAPI Filters
	• Management Tools/IIS 6 Management Compatibility
	  • IIS 6 Metabase Compatibility
	The above mentioned roles services are activated automatically by the setup. The Web Server (IIS) role is not installed by the setup.

Web browsers	You can use any of the following web browsers to access web sites protected by ISAPI Agent: • Chrome 15 or later • Firefox 8 or later • Internet Explorer 9 or later (Internet Explorer run in compatibility mode is not supported) • Opera 11.1 or later • Safari 5.1 or later

Defender Management Shell

Table 14:
Defender Management Shell system requirements

Requirement	Details
Processor	1.4 GHz or faster, x86 or x64 architecture
Memory (RAM)	512 MB or more
Hard disk space	10 MB or more
Operating system	Your computer must be running one of the following operating systems (with or without any Service Pack): • Windows Server 2016 • Windows Server 2012 R2 (64-bit editions only) • Windows Server 2012 (64-bit editions only) • Windows Server 2008 R2 (64-bit editions only) • Windows Server 2008 (32- and 64-bit editions) • Windows 10 (32- and 64-bit editions) • Windows 8.1 (32- and 64-bit editions) • Windows 8 (32- and 64-bit editions) • Windows 7 (32- and 64-bit editions)
Additional software	Windows PowerShell 3.0

VPN Integrator

Table 15:
VPN Integrator system requirements

Requirement	Details
Processor	1.4 GHz or faster, x86 or x64 architecture
Memory (RAM)	512 MB or more
Hard disk space	10 MB or more
Operating system	Your computer must be running one of the following operating systems (with or without any Service Pack): • Windows Server 2016 • Windows Server 2012 R2 (64-bit editions only)

Requirement	Details
	• Windows Server 2012 (64-bit editions only) • Windows Server 2008 R2 (64-bit editions only) • Windows Server 2008 (32- and 64-bit editions) • Windows 10 (32- and 64-bit editions) • Windows 8.1 (32- and 64-bit editions) • Windows 8 (32- and 64-bit editions) • Windows 7 (32- and 64-bit editions)

Client SDK

Table 16:
Client SDK system requirements

Requirement	Details
Processor	1.4 GHz or faster, x86 or x64 architecture
Memory (RAM)	512 MB or more
Hard disk space	10 MB or more
Operating system	Your computer must be running one of the following operating systems (with or without any Service Pack): • Windows Server 2016 • Windows Server 2012 R2 (64-bit editions only) • Windows Server 2012 (64-bit editions only) • Windows Server 2008 R2 (64-bit editions only) • Windows Server 2008 (32- and 64-bit editions) • Windows 10 (32- and 64-bit editions) • Windows 8.1 (32- and 64-bit editions) • Windows 8 (32- and 64-bit editions) • Windows 7 (32- and 64-bit editions)

Web Service API

Table 17:
Web Service API system requirements

Requirement	Details
Processor	1.4 GHz or faster, x86 or x64 architecture
Memory (RAM)	512 MB or more
Hard disk space	10 MB or more
Operating system	Your computer must be running one of the following operating systems (with or without any Service Pack): • Windows Server 2016 • Windows Server 2012 R2 (64-bit editions only) • Windows Server 2012 (64-bit editions only) • Windows Server 2008 R2 (64-bit editions only) • Windows Server 2008 (32- and 64-bit editions) • Windows 10 (32- and 64-bit editions) • Windows 8.1 (32- and 64-bit editions) • Windows 8 (32- and 64-bit editions) • Windows 7 (32- and 64-bit editions)

Defender Soft Token for Android™

Requires Android 2.2 or later.

Defender Soft Token for BlackBerry

Requires the following operating system:

- BlackBerry 10

Defender Soft Token for iOS

Requires iOS 6.1 or later.

Defender Soft Token for Java

Requires Java Runtime Environment 1.6 or later.

Defender Soft Token for Windows

Requires one of the following operating systems (with or without any Service Pack):

- Windows Server 2016
- Windows Server 2012 R2 (64-bit editions only)
- Windows Server 2012 (64-bit editions only)
- Windows Server 2008 R2 (64-bit editions only)
- Windows Server 2008 (32- and 64-bit editions)
- Windows 10 (32- and 64-bit editions)
- Windows 8.1 (32- and 64-bit editions)
- Windows 8 (32- and 64-bit editions)
- Windows 7 (32- and 64-bit editions)

Defender Soft Token for Windows Phone

Requires Windows Phone 7.5 or later.

Upgrade and compatibility

One Identity Defender is upgradeable from version 5.8 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.

Product licensing

To add a Defender 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.

For more information on the product licensing, see the *Defender Administrator Guide*.

Getting started with Defender 5.9

For installation instructions, see the *Defender Administrator Guide*.

Globalization

This section contains information about installing and operating this product in non-English configurations, such as those needed by customers outside of North America. This section does not replace the materials about supported platforms and configurations found elsewhere in the product documentation.

This release is Unicode-enabled and supports any character set. In this release, all product components should be configured to use the same or compatible character encodings and should be installed to use the same locale and regional options. This release is targeted to support operations in the following regions: North America, Western Europe and Latin America, Central and Eastern Europe, Far-East Asia, Japan. It supports bidirectional writing (Arabic and Hebrew). The release supports Complex Script (Central Asia – India, Thailand).

The release is localized to the following languages: German.

This release has the following known capabilities or limitations: Only the Web-based Defender Self-Service Portal has been translated to German.

About us

Contacting us

For sales or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

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
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product

Third-party contributions

This product contains some third-party components (listed below). Copies of their licenses may be found at referencing https://www.oneidentity.com/legal/license-agreements.aspx.

Source code for components marked with an asterisk (*) is available at http://opensource.quest.com.

Table 18: List of Third-Party Contributions

Component	License or Acknowledgement
ASP.NET MVC 4	**License**: Apache 2.0
IZPack Installer 4.3.5	**License**: Apache 2.0
Log4Net 1.2.10	Copyright © 2004 Apache Software Foundation **License**: Apache 2.0
QrCode.Net 0.4	Copyright © 2011 George Mamaladze **License**: MIT
QT 4.7.1*	Copyright © 2010 Nokia Corporation **License**: LGPL (GNU Lesser General Public License) 2.1

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

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

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

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Defender Release Notes
Updated - October 2017
Version - 5.9