One Identity Defender 5.10

Release Notes

Wednesday, May 27, 2020

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

About One Identity Defender 5.10

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 5.10 is a minor release.

See New features.

New features

New features in Defender 5.10

- Supports more than 256 concurrent authentication requests in Defender Security Server.
- Defender Group Policy ADM templates are migrated to ADMX format.
- Supports One Identity Active Roles Server 7.4 and above.
- Supports Java 13 and Java 14 in Defender Soft Token for Java.
- Supports Russian language localization in Defender Self Service portal.

Deprecated features

Deprecated features in Defender 5.10

- Removed obsolete hardware tokens page from Administration console.

Resolved issues

The following is a list of issues addressed in 5.10 release.

Table 1: Defender Desktop Login resolved issues

Resolved Issue	Issue ID
Offline cache data is not updated after logging in to corporate VPN.	142181 TFS799974
Delayed log on observed on Windows 10 when logging in from outside of the network.	124285
Defender Desktop Login does not try to search for the available DCs or GCs	TFS790429

Resolved Issue	Issue ID
in the forest.	
User authentication to Defender Desktop Login using Google Authenticator tokens that are prefixed with PIN fails, when Defender Service is unavailable.	TFS795260
When a user authenticates to a Windows 10 system via Defender Desktop Login, the logon process is delayed.	TFS799227

Table 2: Defender Management Portal resolved issues

Resolved Issue	Issue ID
In the Self Service Portal, minimum and maximum length information of the PIN is missing while registering Hardware Tokens.	234648
When Defender Administrator searches for a user in the Management portal, username does not appear in the header.	219523
When User search is performed using Defender Management Portal, a delay is seen while retrieving User Properties.	122497
Self-service User is unable to request for Software Tokens from the Defender Management Portal.	140565
Unable to schedule the Defender reports.	TFS791194
When Defender Management Portal is installed with a non-Domain Admin Group as the default administrator group of the Management Portal, and a user who is member of the non-Domain Admin Group logs in to the Management Portal, then the Administrator privileges are not provided to the user.	TFS799703

Table 3: Defender Security Server resolved issues

Resolved Issue	Issue ID
Defender Security Server is unable to switch to the next available GC in the AD forest.	139493
The DSS Service restarts when a username consists of special characters and exceeds the defined character limit.	TFS792148
Authentication is abandoned when a user authenticates through VPN.	TFS795681 TFS796768
Defender Security Server service crashes if the SMTP server is not available.	TFS796950

Resolved Issue	Issue ID
When Defender Security Server is configured to use SSL port 636 and server is rebooted, the DSS service fails to start.	TFS802183
When a User is assigned with an email or an SMS token along with an Authy token, the email or SMS is not sent to the User.	TFS800967
DSS Audit logs display incorrect Active Users count.	TFS796783
DSS Audit logs capture GC connections repeatedly.	TFS789612
YubiCloud tokens are not working with Defender.	TFS794403

Table 4: Defender Soft Token for Java resolved issues

Resolved Issue	Issue ID
When you attempt to run the Soft Token for Java with Java 9 or later installed on the system, you encounter the following error: ClassCastException: class jdk.internal.loader.ClassLoaders$AppClassLoader cannot be cast to class java.net.URLClassLoader (jdk.internal.loader.ClassLoaders$AppClassLoader and java.net.URLClassLoader are in module java.base of loader 'bootstrap').	TFS798816

Table 5: Other resolved issues

Resolved Issue	Issue ID
Defender License fails to install when the Defender Organizational Unit is in the custom location.	235292
When trying to access Management Portal site protected by the Defender ISAPI Agent, HTTP Internal Server error 500 is displayed.	166936
Soft token license mismatch seen in Administration Console and Defender Management Reports.	128649
Authentication using Temporary Tokens for Defender Soft Token for Android fails.	142255
Authentication using Temporary Tokens for Defender Soft Token for iOS fails.	142256
Authentication using Temporary Tokens for Defender Soft Token for Windows fails.	142288
In the Defender Administration Console, Administrator is not able to set PIN for tokens.	221449

Resolved Issue	Issue ID
After you install Microsoft July 2018 Security and Quality Rollup updates for .NET Framework updates, an error is displayed when you view Defender Properties in the Active Roles Web Interface.	122503
The Done and Swipe buttons in Defender Soft Token for iOS have UI issues on the iPhone XS Max device.	141465
Unable to delete GrIDsure Token/Defender Password from a User when the name contains forward slash.	134405
User is able to login to the clients only with Active Directory password even after completing the token registration.	126626
YubiCloud fails to validate the token response.	216093
The Active Roles Web interface does not allow assigning Soft Tokens for iOS for users.	TFS798859
Time-based non-OATH iOS tokens generate invalid responses when an expiry date is set for the token activation code.	TFS799224
In Active Roles Web interface, when a user assigned with Defender-Administrator Access template tries to program Defender tokens, a permission related error message is displayed.	TFS801613
Diagnostic logging for Integration Pack for Active Roles display token activation Code when programming token via Active Roles Console.	TFS795246
When Defender Soft Token for iOS is programmed with an expiration date, Token Properties are not updated correctly in Administration Console.	TFS629609

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 6: General known issues

Known Issue	Issue ID
Defender Desktop Login component does not allow to log in when the NTLM v2 is enabled and Kerberos authentication is disabled. **Workaround** When NTLM v2 is enabled, make sure to enable NTLM v1 as well	122492
Error message is displayed when service account is configured using UPN format in Defender Management Portal.	122498

Known Issue	Issue ID
Workaround Use sAMAccountName format instead of UPN format.	
While installing Defender Soft Token for Java on Windows OS, shortcuts were not created in the location specified during installation. **Workaround** Launch Defender Soft Token for Java from the installation folder.	141508
Authentication to GC/DC is failing until the Defender Security Server Service is restarted. **Workaround** Restart Defender Security Server service manually.	142261
When a user logs in for the first time using Defender Desktop Login provider, the system takes more time to respond after the token details are entered.	TFS784380
When trying to authenticate with the Defender ISAPI Agent, the following error occurs even if a valid token response is entered: Error Message - *Invalid token response. Enter a valid token response* **Workaround** The error message is displayed when the Defender ISAPI Agent is not configured correctly, for example, when the connection to the Defender Security Server is specified incorrectly. Make sure that the settings of the Defender ISAPI Agent are configured correctly.	TFS783463
Defender Desktop Login component does not allow to log in when the NTLM v2 is enabled and Kerberos authentication is disabled. **Workaround** Enable the Kerberos authentication.	TFS776920
The user is not allowed to log in to the system when the group name is renamed in Active Directory. **Workaround** The Admin user must log into the client machine, remove and add the group from Defender Desktop Login configuration tool (GinaConfig.exe).	TFS781927
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.	TFS712795

Known Issue	Issue ID
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 may 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.	TFS723423
"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** Make sure that the Active Directory functions correctly, and the machine with Defender Management Portal is able to reach a domain controller.	TFS588772
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 one 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.	TFS366713
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.	TFS366722
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.	TFS366743
A user, authenticating via Defender Password for the first time, is not	TFS366794

Known Issue	Issue ID
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.	
To change the user ID setting on an access node, the DSS Service must be restarted. **Workaround** Restart the Defender Security Server service. You can use the Defender Security Server Configuration utility to do this.	TFS366822
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 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 indicates that you cannot log on as a local user without Defender authentication.	TFS366824
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.	TFS366941
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** Use only a single instance of Defender Administration Console and close the multiple instances.	TFS417432
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.	TFS417457
After you change the user's token list in the Management Portal (e.g. assign	TFS417714

Known Issue	Issue ID
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.	
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.	TFS420395
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 configured. **Workaround** Navigate to the Management Portal Administration user interface and configure the service account.	TFS421707
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 displays 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.	TFS421715
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.	TFS429274
When you program mobile software tokens using the Defender Integration Pack for Active Roles, the option to program the tokens in challenge-response mode is available. Selecting this option may produce an error.	TFS431278

Known Issue	Issue ID
Workaround Defender software tokens for mobile devices currently do not support challenge-response mode. Ignore this option.	
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.	TFS435240
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." **Workaround** This error message means that the verification code has expired. Start over by requesting a software token.	TFS436701
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.	TFS439473
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 in the VPN client manually.	TFS441655
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.	TFS452765
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.	TFS462928

Known Issue	Issue ID
Workaround Use the EAP Agent installed on a computer running an operating system other than Windows 10.	
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>	TFS487077
When configuring the option "Use service account for all actions" in the Management Portal settings, the 'Save' button is not enabled to save the changes. **Workaround** Re-enter and re-confirm the service account password to enable the 'Save' button.	TFS504067
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.	TFS504432
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.	TFS591408
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.	TFS597986
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.	TFS598397

Known Issue	Issue ID
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**.	TFS598605
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.	TFS722484

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 7:
Defender Security Server system requirements

Requirement	Details
Processor	2 GHz or faster, x86 or x64 architecture
Memory (RAM)	4 GB
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 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2 • Windows Server 2008
Additional Software	• Microsoft Visual C++ 2019 Redistributable Package (installed automatically together with the Defender Security Server) • Microsoft .NET Framework 4.8 (installed automatically together with the Defender Security Server)

Defender Administration Console

Table 8:
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

Requirement	Details
	operating systems (with or without any Service Pack): • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2 • 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++ 2019 Redistributable Package (installed automatically together with the Defender Administration Console) • Microsoft .NET Framework 4.8 (installed automatically together with the Defender Administration Console)

Desktop Login

Table 9:
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 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012

Requirement	Details
	• Windows Server 2008 R2 • 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	Microsoft Visual C++ Redistributable for Visual Studio 2019 (installed automatically together with the Defender Desktop Login)

Desktop Login Group Policy

Table 10:
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 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2 • 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	Microsoft Visual C++ Redistributable for Visual Studio 2019 (installed automatically together with the Desktop Login Group Policy)

Defender Management Portal

Table 11:
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 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2 • 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 Visual C++ Redistributable for Visual Studio 2019 (installed automatically together with the Defender Management Portal)
	• Microsoft .NET Framework 4.8 (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 12:
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 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2 • 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 Integration Pack for Active Roles

Table 13:
Defender Integration Pack for Active Roles system requirements

Requirement	Details
Required software	• Active Roles 7.4 Required Active Roles components: • Administration Service • Web Interface • Active Roles console • Defender Administration Console

Requirement	Details
Operating system	Your computer must be running one of the following operating systems (with or without any Service Pack): • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2 • Windows Server 2008 (32- and 64-bit editions)
Additional software	• Microsoft Visual C++ Redistributable for Visual Studio 2019 (installed automatically together with the Defender Integration Pack for Active Roles) • Microsoft .NET Framework 4.8 (installed automatically together with the Defender Integration Pack for Active Roles)

ISAPI Agent

Table 14:
ISAPI Agent 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 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2 • 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

Requirement	Details
	• 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
Additional Software	Microsoft Visual C++ Redistributable for Visual Studio 2019 (installed automatically together with the ISAPI Agent)

Defender Management Shell

Table 15:
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 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2

Requirement	Details
	• 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 or later • Microsoft Visual C++ Redistributable for Visual Studio 2019 (installed automatically together with the Defender Management Shell) • Microsoft .NET Framework 4.8 (installed automatically together with the Defender Management Shell)

VPN Integrator

Table 16:
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 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2 • 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 17:
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 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2 • 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	• Microsoft Visual C++ Redistributable for Visual Studio 2019 (installed automatically together with Client SDK)

Web Service API

Table 18:
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):

Requirement	Details
	• Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2 • 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	• Microsoft Visual C++ Redistributable for Visual Studio 2019 (installed automatically together with the Web Service API) • Microsoft .NET Framework 4.8 (installed automatically together with the Web Service API)

Defender Soft Token for Android™

Requires Android 4.4 or later.

Defender Soft Token for BlackBerry

Requires the following operating system:

- BlackBerry 10

Defender Soft Token for iOS

Requires one of the following:

- iOS 9.0 or later, for iPhone
- iPadOS 13 or later, for iPad

Defender Soft Token for Java

- Requires JRE version to Java Runtime Environment to 1.8 or later
- Requires one of the following operating systems (with or without any Service Pack):
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2012
  - Windows Server 2008 R2
  - 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)
  - Mac OS X
  - Linux/Unix

Defender Soft Token for Windows

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

Table 19:
Defender Soft Token system requirements

Requirement	Details
Operating system	Your computer must be running one of the following operating systems (with or without any Service Pack): • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2 • 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)

Requirement	Details
	• Windows 7 (32- and 64-bit editions)
Additional software	• Microsoft Visual C++ Redistributable for Visual Studio 2019 (installed automatically together with Defender Soft Token for Windows)

Defender Soft Token for Windows Phone

Requires Windows Phone 7.5 or later.

Upgrade and compatibility

One Identity Defender is upgradeable from version 5.9.3 or 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 and follow the instructions mentioned on the screen to complete the upgrade process.

NOTE: If your current Defender version is lower than version 5.9.3, it is recommended to upgrade to version 5.9.3 or later.

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 select the Defender container.
3. On the menu bar, select **Defender | License**.
4. On the **License** tab, click **Add License**.
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 Administration Guide*.

Getting started with Defender 5.10

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

More Resources

For more information on the latest product information and other helpful resources, see https://www.oneidentity.com/products/defender/.

For the most recent documents and product information, see https://support.oneidentity.com/defender.

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 and Russian.

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

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

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 20: List of Third-Party Contributions

Component	License or Acknowledgement
IZPack Installer 4.3.5	Copyright © 2001 – 2018 Julien Ponge, René Krell and the IzPack contributors This component is governed by Apache License
Log4Net 2.0.8	Copyright 2004-2017 The Apache Software Foundation This component is governed by Apache License
Newtonsoft.Json 12.0.3	Copyright (c) 2007 James Newton-King This component is governed by MIT N/A
QrCode.Net 0.4.1.2	Copyright (c) 2011 George Mamaladze This component is governed by MIT N/A
QT 4.7.1*	Copyright © 2010 Nokia Corporation and/or its subsidiary(-ies). Contact: Nokia Corporation (qt-info@nokia.com) This component is governed by LGPL (GNU Lesser General Public License) 2.1

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.