One Identity Defender 6.6.0

Release Notes

12 November 2024, 06:57

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

About One Identity Defender 6.6.0

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.

See New features.

New features

New feature in Defender 6.6.0:

- **Integration of One Identity License Validator (OID LV)**: Defender now uses the One Identity branded version of License Validator (OID LV) for generating and validating licenses exclusively for One Identity products.

  NOTE: This new version is not backward compatible with the previous Quest license version and requires new OID LV license keys for upgrades to Defender v6.6.0 or later.

- **Update to Curl Library Version 8.8.0** - Defender has been updated to integrate Curl library version 8.8.0, addressing two key vulnerabilities:
  - CVE-2023-38545: A high-severity heap-based buffer overflow that could lead to data corruption or arbitrary code execution.
  - CVE-2023-38546: A low-severity cookie injection vulnerability, mitigated to enhance security robustness.

Resolved issues

The following is a list of issues addressed in 6.6.0 release.

Table 1: General issues

Resolved Issue	Issue ID
High severity security vulnerabilities fixed (Polaris Scan Tool) and remediation of high-severity security issues identified by the Polaris scan tool with Defender pipelines, including out-of-bounds vulnerabilities and resource leaks, enhancing memory handling and resource management.	413217
Security vulnerabilities identified by the Mend-White source scan tool have been fixed. Upgraded the zlib library to version 1.1.4 following deprecation identified by the Mend tool.	469253

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 2: General known issues

Known Issue	Issue ID
Push notification authentication flows do not work properly on ADFS client. **Workaround** Push notification can be disabled. Alternatively, user can enter passcode from token manually on passcode field to login.	406536
Push notification timeout flows should not fail for EAP with radius proxy when user has more than 2 tokens **Workaround** Push notification can be disabled for the EAP client. Alternatively, user could be restricted to use only 2 tokens while using push notification with EAP client. If both push notification and more than 3 tokens must be used then user can login by restarting the DSS service and subsequently the authentication process.	408220
MS token displays 'Bad response' error after performing reset operation on the token. **Workaround:** Use OATH Compliant tokens as those are not affected by this issue and are considered counter-based. If user must use Google Authenticator (TOTP) or Microsoft Authenticator (Time based), then they would have to delete the existing token and program a new token.	401643
FIDO2 registration and authentication screens do not load when defender is used as proxy and the next requests are rejected.	394549
On radius proxy environments certain push notification flows do not work as expected. **Workaround:** Push notification can be disabled on radius proxy environments to allow authentication using Defender.	392972
Defender soft token for OneLogin Protect cannot be activated using the activation code. **Workaround:** Defender soft token for OneLogin Protect can be activated using the QR code from Defender management portal self service.	399821
"Push notification rejected" error is observed for timeout flow on EAP client if user has 3 or more tokens. **Workaround:**	404010

Known Issue	Issue ID
Push notification can be disabled for the EAP client. Alternatively, user could be restricted to use only 2 tokens while using push notification with EAP client. If both push notification and more than 3 tokens must be used then user can login by restarting the authentication process on timeout.	
Audit trial report does not displays all the data from DSS logs **Workaround** Logs can be picked from the DSS path or from management portal DSS logs section.	325245
Defender users are unable to login using complex token policy with both FIDO2 and Android/iOS tokens **Workaround** The user can either remove or disable the FIDO2 tokens or use token only policy.	315618
Unable to register the FIDO2 token using Firefox browser	315541
Users see a blank token when the FIDO2 token is programmed and deleted by the admin **Workaround** Restart the DSS service.	316375
Windows 2022 EAP client failed to connect with the error "wlanapi.ddl" not found	300642
Desktop login offline authentication shows the Windows login logo spinning before going back to the login screen. **Workaround** Increase the IdleTimeOut for Windows Logon UI by creating the registry key below: • Path: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI • Add a DWORD key named: IdleTimeOut • Set the decimal value to: 240000 (which equals 240 seconds) This setting can also be deployed via Microsoft group policy, please consult with Microsoft's documentation on updating machine settings via GPOs.	339090
When 2012 R2 Server or Windows 8 machine is used to set up DDL component with Soft token for iOS/Android, Resend button and field to enter passcode/ "push" keyword will not be available if push notification times out.	298022

Known Issue	Issue ID
The user needs to restart the authentication process by providing username and password.	
On Hyper V DDL client with Soft token for iOS/Android, certain policies are displaying incorrect message on UI upon push notification timeout if username format used is - "domain\username". **Workaround** Enter "username" instead of "domain\username" in the user name field.	298121
When 2012 R2 server or Windows 8 machine is used to set up DDL component with Soft token for iOS/Android, then any complex policy combination with token along with Defender/Active Directory password is not supported.	297740
Error message is displayed when service account is configured using UPN format in Defender Management Portal. **Workaround** Use sAMAccountName format instead of UPN format.	122498
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.	TFS78438-0
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.	TFS78346-3
The user is not allowed to log in to the system when the group name is renamed in Active Directory. **Workaround**	TFS78192-7

Known Issue	Issue ID
The Admin user must log into the client machine, remove and add the group from Defender Desktop Login configuration tool (GinaConfig.exe).	
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.	TFS71279-5
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.	TFS72342-3
"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.	TFS58877-2
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.	TFS36671-3
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.	TFS36672-2

Known Issue	Issue ID
Workaround Switch the user to use the default UPN suffix during the logon procedure.	
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.	TFS36674-3
A user, authenticating via 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.	TFS36679-4
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.	TFS36682-2
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.	TFS36682-4
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.	TFS36694-1
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	TFS41743-2

Known Issue	Issue ID
multiple instances.	
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.	TFS41745-7
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.	TFS41771-4
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.	TFS42039-5
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.	TFS42170-7
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.	TFS42171-5
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	TFS42927-4

Known Issue	Issue ID
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.	
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. **Workaround** Defender software tokens for mobile devices currently do not support challenge-response mode. Ignore this option.	TFS43127-8
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.	TFS43524-0
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.	TFS43670-1
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.	TFS43947-3
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.	TFS44165-5
Users who are directly assigned to an access node cannot be moved to a different OU.	TFS45276-5

Known Issue	Issue ID
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.	
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.	TFS46292-8
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>	TFS48707-7
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.	TFS50406-7
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.	TFS50443-2
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.	TFS59140-8
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	TFS59798-6

Known Issue	Issue ID
same computer.	
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.	TFS59839-7
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**.	TFS59860-5

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 iOS

- Defender Soft Token for Java
- Defender Soft Token for Windows

Defender Security Server

Table 3:
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 2022 • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012
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 4:
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):

Requirement	Details
	• Windows Server 2022 • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 • Windows 11 (32- and 64-bit editions) • Windows 10 (32- and 64-bit editions) • Windows 8.1 (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 5:
Desktop Login system requirements

Requirement	Details
Processor	1.4 GHz or faster, x86 or x64 architecture
Memory (RAM)	1 GB 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 2022 • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 • Windows 11 (32- and 64-bit editions) • Windows 10 (32- and 64-bit editions)

Requirement	Details
	• Windows 8.1 (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 6:
Desktop Login Group Policy system requirements

Requirement	Details
Processor	1.4 GHz or faster, x86 or x64 architecture
Memory (RAM)	1 GB 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 2022 • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 • Windows 11 (32- and 64-bit editions) • Windows 10 (32- and 64-bit editions) • Windows 8.1 (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 7:
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 2022 • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012

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 8:
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 10 (32- and 64-bit editions) • Windows 8.1 (32- and 64-bit editions) • Windows 8 (32- and 64-bit editions)

NOTE: Defender EAP components work only with Windows Server 2012 and Windows 8 client machines.

Defender Integration Pack for Active Roles

Table 9:
Defender Integration Pack for Active Roles system requirements

Requirement	Details

Required software	• Active Roles v8.1.x, v8.0.x, v7.6.x, v7.5.x
	• 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

Requirement	Details
	operating systems (with or without any Service Pack): • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012
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 10:
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 2022 • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012

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

Requirement	Details
	• 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 11:
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 2022 • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 • Windows 11 (32- and 64-bit editions) • Windows 10 (32- and 64-bit editions) • Windows 8.1 (32- and 64-bit editions)

Requirement	Details
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 12:
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 10 (32- and 64-bit editions) • Windows 8.1 (32- and 64-bit editions) • Windows 8 (32- and 64-bit editions)

Client SDK

Table 13:
Client SDK system requirements

Requirement	Details
Processor	1.4 GHz or faster, x86 or x64 architecture
Memory (RAM)	512 MB or more

Requirement	Details
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 10 (32- and 64-bit editions) • Windows 8.1 (32- and 64-bit editions) • Windows 8 (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 14:
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 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 • Windows 10 (32- and 64-bit editions) • Windows 8.1 (32- and 64-bit editions) • Windows 8 (32- and 64-bit editions)
Additional Software	• Microsoft Visual C++ Redistributable for Visual Studio 2019 (installed automatically together with the Web

Requirement	Details
	Service API) • Microsoft .NET Framework 4.8 (installed automatically together with the Web Service API)

Defender Soft Token for Android™

Requires Android 4.4 (8.0 for push notification) or later.

Defender Soft Token for iOS

Requires one of the following:

- iOS 9.0 or later for iPhone (iOS 10.0 or later to enable the push notification).
- 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 2022
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2012
  - Windows 11 (32- and 64-bit editions)
  - Windows 10 (32- and 64-bit editions)
  - Windows 8.1 (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 15:
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 2022 • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 • Windows 11 (32- and 64-bit editions) • Windows 10 (32- and 64-bit editions) • Windows 8.1 (32- and 64-bit editions)
Additional software	• Microsoft Visual C++ Redistributable for Visual Studio 2019 (installed automatically together with Defender Soft Token for Windows)

Upgrade and compatibility

One Identity Defender is upgradeable from version 6.1.0 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 6.1.0, it is recommended to upgrade to version 6.1.0 or later.
- For Defender versions older than 6.1.0, upgrading to Defender 6.1.0 or above requires the **Schema Admin** role due to the inclusion of schema extension from version 6.1.0 onwards.

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 6.6.0

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 16: 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.Net 12.0.3	Copyright (c) 2007 James Newton-King This component is governed by MIT Json.NET 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
cpprestsdk 2.10.15	Copyright (c) MIT 2020 This component is governed by MIT N/A 1.0
zlib 1.3.1	Copyright (c) 1995-2024 Jean-loup Gailly and Mark Adler This component is governed by zlib
libcurl 8.8.0	Copyright (c) 1996 - 2024, Daniel Stenberg. All rights reserved. This component is governed by curl
liblic	Copyright (c) 2010, 3rd Party License Information Copyright Notice - sxmlc 4.5 , Matthieu Labas All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the

Component	License or Acknowledgement
	above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the FreeBSD Project

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.