

# One Identity Defender 5.9.5

## Release Notes

Wednesday, October 23, 2019

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

- [About One Identity Defender 5.9.5](#)
- [New features](#)
- [Resolved issues](#)
- [Known issues](#)
- [System requirements](#)
- [Product licensing](#)
- [Getting started with Defender 5.9.5](#)
- [Globalization](#)
- [About us](#)

## About One Identity Defender 5.9.5

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 5.9.5 is a minor release providing support for Active Roles 7.4.

See [New features](#).

## New features

New features in Defender 5.9.5:

- **Support for One Identity Active Roles 7.4** Added support for Active Roles 7.4 to One Identity Defender

See also:

[Resolved issues](#)

## Resolved issues

The following is a list of issues addressed in 5.9.5 release.

**Table 1: Defender Desktop Login resolved issues**

Resolved Issue	Issue ID
Defender Desktop Login does not try to search for the available DCs or GCs in the forest.	TFS790429
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
Delayed log on observed on Windows 10 when logging in from outside of the network.	124285

**Table 2: Defender Management Portal resolved issues**

Resolved Issue	Issue ID
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	TFS799703

<b>Resolved Issue</b>	<b>Issue ID</b>
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.	
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

**Table 3: Defender Security Server resolved issues**

<b>Resolved Issue</b>	<b>Issue ID</b>
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
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**

<b>Resolved Issue</b>	<b>Issue ID</b>
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**

<b>Resolved Issue</b>	<b>Issue ID</b>
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
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

## 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**

<b>Known Issue</b>	<b>Issue ID</b>
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 - <i>Invalid token response. Enter a valid token response</i>	TFS783463

**Workaround**

Known Issue	Issue ID
<p>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.</p>	
<p>Defender Desktop Login component does not allow to log in when the NTLM v2 is enabled and Kerberos authentication is disabled.</p>	TFS776920
<p><b>Workaround</b></p>	
<p>Enable the Kerberos authentication.</p>	
<p>The user is not allowed to log in to the system when the group name is renamed in Active Directory.</p>	TFS781927
<p><b>Workaround</b></p>	
<p>The Admin user must log into the client machine, remove and add the group from Defender Desktop Login configuration tool (GinaConfig.exe).</p>	
<p>If <b>Test connection automatically</b> setting in the DSS configuration is enabled, a very large number of DSS logs may be generated.</p>	TFS712795
<p><b>Workaround</b></p>	
<ul style="list-style-type: none"> <li>• Workaround 1: Disable the 'Test connection automatically' setting.</li> <li>• Workaround 2: Make sure you have enough space for DSS log files, and periodically delete old log files.</li> </ul>	
<p>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.</p>	TFS723423
<p><b>Workaround</b></p>	
<p>Make sure that no other tokens are assigned to the user, if they are using the GrIDSure token for authentication.</p>	
<p>"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.</p>	TFS588772
<p><b>Workaround</b></p>	
<p>Make sure that the Active Directory functions correctly, and the machine with Defender Management Portal is able to reach a domain controller.</p>	
<p>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</p>	TFS366713

**Known Issue****Issue ID**

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.

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.

TFS366722

**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.

TFS366743

**Workaround**

Install the VIP credential certificate in the child domain.

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.

TFS366794

**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.

TFS366822

**Workaround**

Restart the Defender Security Server service. You can use the Defender Security Server Configuration utility to do this.

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."

TFS366824

**Workaround**

This error message indicates that you cannot log on as a local user without

Known Issue	Issue ID
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.	TFS366941
<b>Workaround</b>	
Make sure that users who are assigned a token with a PIN do not have a GrIDSure token assigned to them.	
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.	TFS417432
<b>Workaround</b>	
Use only a single instance of Defender Administration Console and close the 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.	TFS417457
<b>Workaround</b>	
This behavior is due to the replication latency in Active Directory. View the list of tokens after the changes have been replicated.	
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.	TFS417714
<b>Workaround</b>	
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.	TFS420395
<b>Workaround</b>	
When you unlock an account locked by Defender, the violation count is automatically reset as well.	
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.	TFS421707
<b>Workaround</b>	
Navigate to the Management Portal Administration user interface and configure the service account.	

Known Issue	Issue ID
<p>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.</p> <p><b>Workaround</b></p> <p>Do either of the following:</p> <ol style="list-style-type: none"> <li>1. Use the value on the diagram.</li> <li>2. Reload the web page (CTRL+F5) to update the value in the tooltip.</li> </ol>	TFS421715
<p>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.</p> <p><b>Workaround</b></p> <p>Use the values in the Defender Administration Console, these are the correct values.</p>	TFS429274
<p>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.</p> <p><b>Workaround</b></p> <p>Defender software tokens for mobile devices currently do not support challenge-response mode. Ignore this option.</p>	TFS431278
<p>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.</p> <p><b>Workaround</b></p> <p>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.</p>	TFS435240
<p>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."</p> <p><b>Workaround</b></p> <p>This error message means that the verification code has expired. Start over by requesting a software token.</p>	TFS436701
<p>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</p>	TFS439473



Known Issue	Issue ID
<p>accepted when establishing a VPN connection. This issue occurs when Soft Token for Windows is programmed in challenge-response mode.</p> <p><b>Workaround</b></p> <p>Program the Soft Token for Windows in synchronous mode.</p>	
<p>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.</p> <p><b>Workaround</b></p> <p>Launch the Soft Token for Windows, and enter the passcode in the VPN client manually.</p>	TFS441655
<p>Users who are directly assigned to an access node cannot be moved to a different OU.</p> <p><b>Workaround</b></p> <p>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.</p>	TFS452765
<p>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.</p> <p><b>Workaround</b></p> <p>Use the EAP Agent installed on a computer running an operating system other than Windows 10.</p>	TFS462928
<p>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.</p> <p><b>Workaround</b></p> <p>Open the command prompt as administrator and run the following command: <code>java -jar &lt;path to uninstaller file&gt;</code></p>	TFS487077
<p>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.</p> <p><b>Workaround</b></p> <p>Re-enter and re-confirm the service account password to enable the 'Save' button.</p>	TFS504067
<p>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</p>	TFS504432

Known Issue	Issue ID
one user. This occurs when Internet Explorer is used as the browser.	
<b>Workaround</b>	
Use a different supported browser.	
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.	TFS591408
<b>Workaround</b>	
Make sure that the DSS is available and retry the login attempt.	
When Web Service API is the only Defender component installed on a computer, it does not work.	TFS597986
<b>Workaround</b>	
Install Defender Management Shell or Management Portal component on the 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.	TFS598397
<b>Workaround</b>	
Only the latest version gets installed. You can ignore the old version that is listed.	
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.	TFS598605
<b>Workaround</b>	
On the final page of the Program Token wizard, click <b>Back</b> , click <b>Next</b> , and then click <b>Finish</b> .	
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.	TFS722484
<b>Workaround</b>	
Clear the browser cache.	
When GetToken.exe is manually executed on a machine that is installed with Defender Desktop Login, Offline token cache does not get updated.	TFS799974
Defender Desktop Login component does not allow to log in when the NTLM v2 is enabled and Kerberos authentication is disabled.	122492
<b>Workaround</b>	
When NTLM v2 is enabled, make sure to enable NTLM v1 as well.	

<b>Known Issue</b>	<b>Issue ID</b>
Error message is displayed when service account is configured using UPN format in Defender Management Portal.	122498
<b>Workaround</b>	
Use sAMAccountName format instead of UPN format.	
Soft token license mismatch seen in Administration Console and Defender Management Reports.	128649
While installing Defender Soft Token for Java on Windows OS, shortcuts are not created in the location specified during installation.	141508
<b>Workaround</b>	
Launch Defender Soft Token for Java from the installation folder.	
Authentication to GC/DC is failing until the Defender Security Server Service is restarted.	142261
<b>Workaround</b>	
Restart Defender Security Server service manually.	
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

## 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)	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): <ul style="list-style-type: none"> <li>• Windows Server 2019</li> <li>• Windows Server 2016</li> <li>• Windows Server 2012 R2</li> <li>• Windows Server 2012</li> <li>• Windows Server 2008 R2</li> <li>• Windows Server 2008 (32 and 64 bit editions)</li> </ul>

## Defender Administration Console

**Table 8:**  
**Defender Administration Console system requirements**

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

<b>Requirement</b>	<b>Details</b>
Memory (RAM)	512 MB or more
Hard disk space	2 GB or more
Operating system	<p>Your computer must be running one of the following operating systems (with or without any Service Pack):</p> <ul style="list-style-type: none"> <li>• Windows Server 2019</li> <li>• Windows Server 2016</li> <li>• Windows Server 2012 R2</li> <li>• Windows Server 2012</li> <li>• Windows Server 2008 R2</li> <li>• Windows Server 2008 (32- and 64-bit editions)</li> <li>• Windows 10 (32- and 64-bit editions)</li> <li>• Windows 8.1 (32- and 64-bit editions)</li> <li>• Windows 8 (32- and 64-bit editions)</li> <li>• Windows 7 (32- and 64-bit editions)</li> </ul>
Additional software	<ul style="list-style-type: none"> <li>• Active Directory Users and Computers (ADUC) tool</li> <li>• Microsoft Visual C++ 2013 Redistributable Package (installed automatically together with the Defender Administration Console)</li> <li>• Microsoft .NET Framework 4.7.2 (installed automatically together with the Defender Administration Console)</li> </ul>

## Desktop Login

**Table 9:**  
**Desktop Login system requirements**

<b>Requirement</b>	<b>Details</b>
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	<p>Your computer must be running one of the following operating systems (with or without any Service Pack):</p> <ul style="list-style-type: none"> <li>• Windows Server 2019</li> </ul>

Requirement	Details
	<ul style="list-style-type: none"> <li>Windows Server 2016</li> <li>Windows Server 2012 R2</li> <li>Windows Server 2012</li> <li>Windows Server 2008 R2</li> <li>Windows Server 2008 (32- and 64-bit editions)</li> <li>Windows 10 (32- and 64-bit editions)</li> <li>Windows 8.1 (32- and 64-bit editions)</li> <li>Windows 8 (32- and 64-bit editions)</li> <li>Windows 7 (32- and 64-bit editions)</li> </ul>

## 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	<p>Your computer must be running one of the following operating systems (with or without any Service Pack):</p> <ul style="list-style-type: none"> <li>Windows Server 2019</li> <li>Windows Server 2016</li> <li>Windows Server 2012 R2</li> <li>Windows Server 2012</li> <li>Windows Server 2008 R2</li> <li>Windows Server 2008 (32- and 64-bit editions)</li> <li>Windows 10 (32- and 64-bit editions)</li> <li>Windows 8.1 (32- and 64-bit editions)</li> <li>Windows 8 (32- and 64-bit editions)</li> <li>Windows 7 (32- and 64-bit editions)</li> </ul>

# 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): <ul style="list-style-type: none"><li>• Windows Server 2019</li><li>• Windows Server 2016</li><li>• Windows Server 2012 R2</li><li>• Windows Server 2012</li><li>• Windows Server 2008 R2</li><li>• Windows Server 2008 (32- and 64-bit editions)</li></ul>
Additional software	<ul style="list-style-type: none"><li>• 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)</li><li>• Microsoft .NET Framework 4.7.2 (installed automatically together with the Defender Management Portal)</li><li>• To access the Defender Management Portal, you can use any of the following Web browsers:<ul style="list-style-type: none"><li>• Chrome 15 or later</li><li>• Firefox 8 or later</li><li>• Internet Explorer 9 or later (Internet Explorer run in compatibility mode is not supported)</li><li>• Opera 11.1 or later</li><li>• Safari 5.1 or later</li></ul></li></ul>

# 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): <ul style="list-style-type: none"><li>• Windows Server 2019</li><li>• Windows Server 2016</li><li>• Windows Server 2012 R2</li><li>• Windows Server 2012</li><li>• Windows Server 2008 R2</li><li>• Windows Server 2008 (32- and 64-bit editions)</li><li>• Windows 10 (32- and 64-bit editions)</li><li>• Windows 8.1 (32- and 64-bit editions)</li><li>• Windows 8 (32- and 64-bit editions)</li><li>• Windows 7 (32- and 64-bit editions)</li></ul>

## Defender Integration Pack for Active Roles

**Table 13:**  
**Defender Integration Pack for Active Roles system requirements**

Requirement	Details
Required software	<ul style="list-style-type: none"><li>• Active Roles 7.4</li></ul> Required Active Roles components: <ul style="list-style-type: none"><li>• Administration Service</li><li>• Web Interface</li><li>• Active Roles console</li></ul> <ul style="list-style-type: none"><li>• Defender Administration Console</li></ul>



Requirement	Details
Operating system	Your computer must be running one of the following operating systems (with or without any Service Pack): <ul style="list-style-type: none"> <li>• Windows Server 2019</li> <li>• Windows Server 2016</li> <li>• Windows Server 2012 R2</li> <li>• Windows Server 2012</li> <li>• Windows Server 2008 R2</li> <li>• Windows Server 2008 (32- and 64-bit editions)</li> </ul>
Additional software	Microsoft .NET Framework 4.7.2 (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): <ul style="list-style-type: none"> <li>• Windows Server 2019</li> <li>• Windows Server 2016</li> <li>• Windows Server 2012 R2</li> <li>• Windows Server 2012</li> <li>• Windows Server 2008 R2</li> <li>• Windows Server 2008 (32- and 64-bit editions)</li> </ul>
Microsoft Internet Information Services (IIS)	IIS 10.0, 8.5, 8.0, 7.5, or 7.0 with the following role services enabled: <ul style="list-style-type: none"> <li>• Web Server/Application Development <ul style="list-style-type: none"> <li>• ASP</li> <li>• ISAPI Filters</li> </ul> </li> </ul>

Requirement	Details
	<ul style="list-style-type: none"> <li>Management Tools/IIS 6 Management Compatibility <ul style="list-style-type: none"> <li>IIS 6 Metabase Compatibility</li> </ul> </li> </ul> <p>The above mentioned roles services are activated automatically by the setup. The Web Server (IIS) role is not installed by the setup.</p>
Web browsers	<p>You can use any of the following web browsers to access web sites protected by ISAPI Agent:</p> <ul style="list-style-type: none"> <li>Chrome 15 or later</li> <li>Firefox 8 or later</li> <li>Internet Explorer 9 or later (Internet Explorer run in compatibility mode is not supported)</li> <li>Opera 11.1 or later</li> <li>Safari 5.1 or later</li> </ul>

## 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	<p>Your computer must be running one of the following operating systems (with or without any Service Pack):</p> <ul style="list-style-type: none"> <li>Windows Server 2019</li> <li>Windows Server 2016</li> <li>Windows Server 2012 R2</li> <li>Windows Server 2012</li> <li>Windows Server 2008 R2</li> <li>Windows Server 2008 (32- and 64-bit editions)</li> <li>Windows 10 (32- and 64-bit editions)</li> <li>Windows 8.1 (32- and 64-bit editions)</li> <li>Windows 8 (32- and 64-bit editions)</li> </ul>

Requirement	Details
	<ul style="list-style-type: none"> <li>Windows 7 (32- and 64-bit editions)</li> </ul>
Additional software	Windows PowerShell 3.0

## 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	<p>Your computer must be running one of the following operating systems (with or without any Service Pack):</p> <ul style="list-style-type: none"> <li>Windows Server 2019</li> <li>Windows Server 2016</li> <li>Windows Server 2012 R2</li> <li>Windows Server 2012</li> <li>Windows Server 2008 R2</li> <li>Windows Server 2008 (32- and 64-bit editions)</li> <li>Windows 10 (32- and 64-bit editions)</li> <li>Windows 8.1 (32- and 64-bit editions)</li> <li>Windows 8 (32- and 64-bit editions)</li> <li>Windows 7 (32- and 64-bit editions)</li> </ul>

## 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

## 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): <ul style="list-style-type: none"><li>• Windows Server 2019</li><li>• Windows Server 2016</li><li>• Windows Server 2012 R2</li><li>• Windows Server 2012</li><li>• Windows Server 2008 R2</li><li>• Windows Server 2008 (32- and 64-bit editions)</li><li>• Windows 10 (32- and 64-bit editions)</li><li>• Windows 8.1 (32- and 64-bit editions)</li><li>• Windows 8 (32- and 64-bit editions)</li><li>• Windows 7 (32- and 64-bit editions)</li></ul>

## 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): <ul style="list-style-type: none"><li>• Windows Server 2019</li><li>• Windows Server 2016</li><li>• Windows Server 2012 R2</li><li>• Windows Server 2012</li><li>• Windows Server 2008 R2</li><li>• Windows Server 2008 (32- and 64-bit editions)</li><li>• Windows 10 (32- and 64-bit editions)</li><li>• Windows 8.1 (32- and 64-bit editions)</li></ul>

## Requirement

## Details

- Windows 8 (32- and 64-bit editions)
- Windows 7 (32- and 64-bit editions)

## 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 8.0 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):

- 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 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 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 5.9.5

For installation instructions, see the *Defender Administration 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

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 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 at [www.YouTube.com/OneIdentity](http://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 19: List of Third-Party Contributions**

<b>Component</b>	<b>License or Acknowledgement</b>
IZPack Installer 4.3.5	Copyright © 2001 – 2018 Julien Ponge, René Krell and the IzPack contributors <b>License:</b> <a href="#">Apache License</a>
Log4Net 2.0.8	Copyright 2004-2017 The Apache Software Foundation <b>License:</b> <a href="#">Apache License</a>
Newtonsoft.Json 12.0.2	Copyright (c) 2007 James Newton-King <b>License:</b> MIT N/A
QrCode.Net 0.4	Copyright (c) 2011 George Mamaladze <b>License:</b> MIT N/A
QT 4.7.1*	Copyright © 2010 Nokia Corporation and/or its subsidiary(-ies). Contact: Nokia Corporation (qt-info@nokia.com) <b>License:</b> LGPL (GNU Lesser General Public License) 2.1

#### Apache License

Version 2.0, January 2004

<http://www.apache.org/licenses/>

#### TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

##### 1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document. "Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License. "Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity. "You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License. "Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files. "Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types. "Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below). "Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative

Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for

informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

**Copyright 2019 One Identity LLC.**

**ALL RIGHTS RESERVED.**

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC .

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

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

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

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




**Patents**

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

**Trademarks**

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

**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.**