

# RSA<sup>®</sup> MFA Agent for Microsoft Windows

## Release Notes

July 2020

This document describes the RSA<sup>®</sup> MFA Agent 2.0.1 for Microsoft Windows release. It also includes workarounds for known issues. Read this document before installing the software. This document contains the following sections:

- [Product Overview below](#)
- [What's New in This Release below](#)
- [Installing This Product on page 4](#)
- [Package Contents on page 5](#)
- [Documentation and Application Help on page 6](#)
- [Fixed Issues on page 6](#)
- [Known Issues on page 6](#)
- [Support and Service on page 8](#)

These *Release Notes* may be updated. The most current version can be found on RSA Link at <https://community.rsa.com/community/products/securid/mfa-agent-windows/>.

### Product Overview

---

RSA MFA Agent 2.0.1 for Microsoft Windows works with RSA SecurID Access to require users to perform additional authentication when accessing Windows computers and User Account Control. A user enters the username and password and then can be prompted for additional authentication (for example, by approving a request in the RSA SecurID Authenticate app). If the user credentials are correct, the user gains access to the computer.

The MFA Agent is installed on Windows computers. When users try to sign into or unlock computers, the MFA Agent communicates with either Cloud Authentication Service or RSA Authentication Manager 8.5 to manage authentication.

The MFA Agent can connect directly to the Cloud Authentication Service or RSA Authentication Manager 8.5. Authentication Manager can act as a secure proxy server that sends authentication requests to the Cloud Authentication Service.

Note that RSA MFA Agent for Microsoft Windows is different from the RSA Authentication Agent for Microsoft Windows. For more information on the differences, see the *Installation and Administration Guide*.

### What's New in This Release

---

This section lists the new features and enhancements that are introduced in RSA MFA Agent for Microsoft

Windows.

### **Version 2.0.1, July 2020**

RSA MFA Agent 2.0.1 for Microsoft Windows includes the following key features:

- Authentication to both Cloud Authentication Service and RSA Authentication Manager 8.5. You can choose from the supported multifactor authentication options based upon your business needs.
- Offline authentication available for both RSA Authentication Manager and Cloud Authentication Service users.
- Ability to specify whether the MFA Agent prompts users for a Windows password after successful multifactor authentication, instead of prompting before multifactor authentication. Users are required to successfully authenticate with both their Windows password and an additional authentication method. This setting can be used with the Cloud Authentication Service and RSA Authentication Manager.
- Challenge group support allows the MFA Agent to challenge all users or a specific group of users for RSA SecurID Access credentials.
- The MFA Agent can send the domain and user name to RSA Authentication Manager during authentication. You enable this policy if you or the Authentication Manager administrator set up the user account with a domain name and user name (NetBIOS\user\_name) in Authentication Manager.
- If the MFA Agent connects to RSA SecurID Access, users can check their supply of offline days by using the RSA SecurID Access icon in the notification area. To display the notification, an MFA Agent administrator must first enable the GPO policy 'Specify when message displays to users about expiring offline days,' if the MFA Agent is connected to the Cloud Authentication Service, or an Authentication Manager administrator must configure an offline authentication policy, if the MFA Agent is connected to Authentication Manager.

If the informational icon (ℹ) appears, the user can right-click the icon to refresh the supply of offline days. The Agent prompts the user for the last online authentication method used. After the user successfully authenticates online, offline days are downloaded to the computer.

- The MFA Agent automatically balances authentication request loads that are sent to RSA Authentication Manager. An administrator can configure load balancing and failover settings.
- You can specify a custom background image shown when collecting RSA SecurID Access credentials.
- The RSA Authentication Agent 7.4.3 for Microsoft Windows and RSA MFA Agent 2.0.1 for Microsoft Windows can be installed on the same computer.
- RSA MFA Agent 2.0.1 for Microsoft Windows co-exist with other REST protocol RSA SecurID Agents on the same computer, for example, RSA® Authentication Agent 2.0 for Citrix StoreFront or RSA® Authentication Agent 2.0 for Microsoft AD FS.
- You can upgrade from MFA Agent 1.1, 1.2, or 1.2.1 to 2.0.1. Customers looking to use the MFA Agent for Microsoft Windows should install version 2.0.1.

### **Version 1.2.1, March 2020**

RSA MFA Agent 1.2.1 is a maintenance patch that resolves customer-reported issues. For more information, see [Fixed Issues on page 6](#).

The GPO Templates were not updated for this release.

**Version 1.2, March 2020**

RSA has verified that RSA MFA Agent 1.2 can coexist with Windows Hello for Business on Windows 10, versions 1803 and 1809. Both the agent and Windows Hello for Business can be used for authentication on the same device.

**Version 1.2, October 2019**

The following updates were introduced in RSA MFA Agent 1.2, released in October 2019:

**Functionality:**

- The MFA Agent supports the Device Biometrics, SecurID Token, SMS Tokencode, Voice Tokencode, and Emergency Tokencode authentication methods, in addition to the Approve and Authenticate Tokencode methods supported in version 1.1.
- The MFA Agent provides additional authentication during the User Account Control (UAC) process.
- You can upgrade from MFA Agent 1.1 to 1.2. Customers using version 1.1 should upgrade to version 1.2. Customers looking to use the MFA Agent for Microsoft Windows should install version 1.2.
- The RSA Authentication Agent 7.4.2 or later for Microsoft Windows and RSA MFA Agent 1.2 for Microsoft Windows can be installed on the same computer.
- If you are using offline authentication, the management of offline days has improved:
  - Administrators can specify the number of offline days downloaded to users' computers and when a message displays to users about expiring offline days. Use the GPO settings "Specify number of offline days" and "Specify when message displays to users about expiring offline days."
  - When the RSA SecurID Access icon () appears in the notification area, users can click the notification to download more offline days.

- The MFA Agent supports the reserve password.

If users cannot use any other authentication method, administrators can enter the reserve password on the user's computer after the user has entered the Windows password. Use the GPO setting "Enable reserve password." You can generate a hash value of the reserve password using a command line interface in interactive or non-interactive mode.

- The MFA Agent now helps protect remote applications. You can streamline authentication to remote applications using the GPO setting "Sign-on with credentials from remote applications." If you do not want the Agent to protect certain remote desktop applications, use the GPO setting "Specify remote desktop applications that do not require RSA SecurID Access authentication."
- You can customize the look and feel of the user interface with the following GPO settings:
  - Specify custom tile image for RSA SecurID Access Credential Provider
  - Specify custom text show when collecting RSA SecurID Access credentials
  - Specify custom logo shown when collecting RSA SecurID Access credentials
- You can allow the user to sign into the computer with only a Windows password during the time-out period. Use the GPO setting "Unlock with Windows Password."

- If you do not want to use the MFA Agent on a computer, use the GPO setting "Exclude RSA SecurID Access Credential Provider in Credential Provider Filter Settings" and confirm that at least one credential provider is available.
- The MFA Agent supports the following languages for users:
  - Chinese (zh-cn)
  - Chinese (zh-tw)
  - English (en-us)
  - French (fr)
  - German (de)
  - Japanese (ja)
  - Korean (ko)
  - Russian (ru)
  - Spanish (mx)

**Version 1.1, May 2019**

The following updates were introduced in RSA MFA Agent 1.1, released in May 2019:

**Functionality:**

- Test Authentication tool allows an administrator to test authentication on a computer with the Authentication Agent.
- Added the following new settings to the GPO template:
  - Specify Cloud Authentication Service Timeout
  - Disable Cloud Authentication Service Authentication for Local User
  - Enable Offline Authentication
  - Configure the RSA SecurID Access Credential Provider Filter Settings

## Installing This Product

---

You can install RSA MFA Agent 2.0.1 on a new machine or upgrade directly to RSA MFA Agent 2.0.1 from any of the following versions:

- RSA MFA Agent 1.1
- RSA MFA Agent 1.2
- RSA MFA Agent 1.2.1

You can also install the RSA Authentication Agent 7.4.3 for Microsoft Windows and RSA MFA Agent 2.0.1 for Microsoft Windows on the same computer.

You can migrate GPO policy settings from RSA Authentication Agent 7.4.0 to 7.4.3 for Microsoft Windows to MFA Agent 2.0.1.

For installation and upgrade instructions, see Chapter 3, "Installing RSA MFA Agent" in the *Installation and Administration Guide*.

## Package Contents

RSA MFA Agent is available at <https://community.rsa.com/community/products/securoid/mfa-agent-windows/downloads>.

The RSA MFA Agent 2.0.1 package contains the following:

- **RSA\_MFA\_Agent\_2.0\_PolicyTemplates.zip**
- **RSA\_MFA\_Agent\_2.0\_PolicyTemplates.zip.sha256.rtf**
- **RSA\_MFA\_Agent\_2.0.1.zip**
- **RSA\_MFA\_Agent\_2.0.1.zip.sha256.rtf**
- **RSA\_MFA\_Agent\_Reserve\_Password\_Hash\_Generator\_1.2.zip**
- **RSA\_MFA\_Agent\_Reserve\_Password\_Hash\_Generator\_1.2.zip.sha256.rtf**

The following table describes each file.

File	Description
<b>RSA_MFA_Agent_2.0_PolicyTemplates.zip</b>	<p>Contains the Group Policy Object (GPO) administrative templates for managing authentication settings.</p> <p>The template files are automatically installed as part of local installation. Only use the zip file if you delete the files and need to re-install them on a computer.</p> <p>Contains the Migration Tool utility to automate the process of migrating your GPO settings from RSA Authentication Agent 7.4.0 to 7.4.3 for Microsoft Windows to MFA Agent 2.0.1.</p>
<b>RSA_MFA_Agent_2.0.1.zip</b>	<p>Contains the following folders:</p> <ul style="list-style-type: none"> <li>• x86 and x64: The Windows Installer Packages for local installation of RSA MFA Agent on 32-bit and 64-bit computers.</li> <li>• Licenses: Contains the RSA License Agreement.</li> </ul>
<b>RSA_MFA_Agent_Reserve_Password_Hash_Generator_1.2.zip</b>	x86 and x64: The Windows Installer Packages for local installation of the RSA MFA Agent Reserve Password Hash Generator utility on 32-bit and 64-bit computers.
<b>RSA_MFA_Agent_2.0_PolicyTemplates.zip.sha256.rtf</b>	Used to verify the authenticity of the product zip files.
<b>RSA_MFA_Agent_2.0.1.zip.sha256.rtf</b>	
<b>RSA_MFA_Agent_Reserve_Password_Hash_Generator_1.2.zip.sha256.rtf</b>	

## Documentation and Application Help

---

The following product documentation is available on RSA Link:

<https://community.rsa.com/community/products/securid/mfa-agent-windows/>

Title	Filename
<i>RSA MFA Agent 2.0.1 for Microsoft Windows Installation and Administration Guide</i>	<b>rsa_mfa_agent_windows_2.0.1_installation_administration_guide.pdf</b>
<i>RSA MFA Agent 2.0 for Microsoft Windows Group Policy Object Template Guide</i>	<b>rsa_mfa_agent_windows_2.0_gpo_template_guide.pdf</b>
RSA SecurID Access User Help	Available from within the RSA SecurID Authenticate app

## Fixed Issues

---

### RSA MFA Agent 2.0.1 July 2020

This release includes a fix for the following issue:

**AAWIN-3943** - Some users were required to enter their domain and username when logging in with the "Other User" credential when the domain was not accessible. Users can now log on with just their usernames.

### RSA MFA Agent 1.2.1 March 2020

This release includes fixes for the following issues:

**AAWIN-3896** - Users with expired passwords were unable to log on to their computer. Users are now prompted to change their expired passwords at the next logon.

**AAWIN-3889** - The "RSA Windows Agent Service" has been renamed as the "RSA MFA Agent Service." This resolves conflicts that prevented the MFA Agent from being installed on a computer that uses the SolarWinds N-able tool.

**AAWIN-3805** - System-generated emergency access codes that contain an asterisk, \*, are now accepted for authentication.

**AAWIN-3674** - The MFA Agent uses the TLS 1.2 protocol to download offline authentication data, if TLS 1.2 is available from Windows, instead of the system default value.

### RSA MFA Agent 1.2 October 2019

This release includes a fix for the following issue:

**AAWIN-3444** - A user signing in with the "Other user" credential in a domain with a multi-level DNS domain name can now enter only a user name (without specifying a domain) in the **User name** field.

## Known Issues

---

This section describes known issues and workarounds.

**MFA Agent slow to process authentication requests on Windows 8.1 when Windows location service is disabled but Agent is collecting system attributes**

**Tracking Number:** NGX-31029

**Problem:** If you disable Windows location service on a Windows 8.1 computer and you have enabled or not configured the GPO setting **Collect system attributes for Cloud Authentication Service access policy**, the MFA Agent is slow to process authentication requests during sign-in.

**Workaround:** If you disable Windows location service on a Windows 8.1 computer, disable the GPO setting **Collect system attributes for Cloud Authentication Service access policy**.

## Support and Service

---

You can access community and support information on RSA Link at <https://community.rsa.com>. RSA Link contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

The RSA Ready Partner Program website at [www.rsaready.com](http://www.rsaready.com) provides information about third-party hardware and software products that have been certified to work with RSA products. The website includes Implementation Guides with step-by-step instructions and other information on how RSA products work with third-party products.

Copyright © 2006-2020 Dell Inc or its subsidiaries. All Rights Reserved.

### **Trademarks**

RSA, the RSA Logo, SecurID, and EMC are either registered trademarks or trademarks of Dell Inc throughout the world. All other trademarks used herein are the property of their respective owners. For a list of RSA trademarks, go to [www.emc.com/legal/emc-corporation-trademarks.htm#rsa](http://www.emc.com/legal/emc-corporation-trademarks.htm#rsa).

### **Intellectual Property Notice**

This software contains the intellectual property of Dell Inc or is licensed to Dell Inc from third parties. Use of this software and the intellectual property contained therein is expressly limited to the terms and conditions of the License Agreement under which it is provided by or on behalf of Dell Inc.

### **Open Source License**

This product may be distributed with open source code, licensed to you in accordance with the applicable open source license. If you would like a copy of any such source code, EMC will provide a copy of the source code that is required to be made available in accordance with the applicable open source license. EMC may charge reasonable shipping and handling charges for such distribution. Please direct requests in writing to EMC Legal, 176 South St., Hopkinton, MA 01748, ATTN: Open Source Program Office.