

# SafeNet Agent for Microsoft Remote Desktop Web 2.0.0

---

INSTALLATION AND CONFIGURATION GUIDE



## Document Information

<b>Product Version</b>	2.0.0
<b>Document Part Number</b>	007-013552-004, Rev. A
<b>Release Date</b>	July 2023

## Trademarks, Copyrights, and Third-Party Software

Copyright © 2020 Thales Group. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales and/or its subsidiaries and affiliates and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the properties of their respective owners.

### Disclaimer

All information herein is either public information or is the property of and owned solely by Thales DIS France S.A. and/or its subsidiaries or affiliates who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Thales DIS France S.A. and any of its subsidiaries and affiliates (collectively referred to herein after as “Thales”) information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

> The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.

> This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Thales makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Thales reserves the right to make **any change or** improvement in the specifications data, information, and the like described herein, at any time.

Thales hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Thales be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Thales does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

# CONTENTS

<b>PREFACE</b> .....	<b>5</b>
Audience .....	5
Related Documents.....	5
Document Conventions.....	5
Command Syntax and Typeface Conventions .....	5
Notifications and Alerts .....	6
Support Contacts .....	7
Customer Support Portal .....	7
Telephone Support .....	7
Email Support .....	7
<b>CHAPTER 1: Introduction</b> .....	<b>8</b>
System Requirements.....	8
Functionality not supported .....	9
Authentication Modes.....	9
<b>CHAPTER 2: Installation</b> .....	<b>10</b>
Prerequisites .....	10
Remote Desktop Web Access Server .....	10
SafeNet Authentication Service (SAS)/SafeNet Trusted Access (STA).....	10
Installing SafeNet Agent for Microsoft RDWeb.....	10
<b>CHAPTER 3: Upgrade</b> .....	<b>14</b>
Upgrading SafeNet Agent for Microsoft RDWeb .....	14
<b>CHAPTER 4: Uninstallation</b> .....	<b>15</b>
<b>CHAPTER 5: Configuration</b> .....	<b>16</b>
Configuring SafeNet Agent for Microsoft RDWeb.....	16
Configuring Policy Settings.....	17
Configuring Authentication Methods.....	18
Configuring Authentication Exceptions .....	19
Configuring Connection Options .....	22
Configuring Logging Settings.....	25
<b>CHAPTER 6: Configuring Proxy Server</b> .....	<b>27</b>
<b>CHAPTER 7: Testing the Solution</b> .....	<b>28</b>
Standard Authentication.....	28
Split Authentication .....	29

# PREFACE

This document describes how to install and configure the **SafeNet Agent for Microsoft Remote Desktop Web**.

## Audience

This document is intended for personnel responsible for maintaining your organization's security infrastructure.

All products manufactured and distributed by Thales are designed to be installed, operated, and maintained by personnel who have the knowledge, training, and qualifications required to safely perform the tasks assigned to them. The information, processes, and procedures contained in this document are intended for use by trained and qualified personnel only.

## Related Documents

The following document contains related information:

- *SafeNet Agent for Microsoft Remote Desktop Web: Customer Release Notes*

## Document Conventions

This section describes the conventions used in this document.

### Command Syntax and Typeface Conventions

This document uses the following conventions for command syntax descriptions, and to highlight elements of the user interface.

Convention	Description
<b>bold</b>	<p>The bold attribute is used to indicate the following:</p> <ul style="list-style-type: none"> <li>&gt; Command-line commands and options (Type <b>dir /p</b>.)</li> <li>&gt; Button names (Click <b>Save As</b>.)</li> <li>&gt; Check box and radio button names (Select the <b>Print Duplex</b> check box.)</li> <li>&gt; Window titles (On the <b>Protect Document</b> window, click <b>Yes</b>.)</li> <li>&gt; Field names (<b>User Name</b>: Enter the name of the user.)</li> <li>&gt; Menu names (On the <b>File</b> menu, click <b>Save</b>.) (Click <b>Menu</b> &gt; <b>Go To</b> &gt; <b>Folders</b>.)</li> <li>&gt; User input (In the <b>Date</b> box, type <b>April 1</b>.)</li> </ul>

<i>italic</i>	The italic attribute is used for emphasis or to indicate a related document. (See the <i>Installation Guide</i> for more information.)
Double quote marks	Double quote marks enclose references to other sections within the document. For example: Refer to “ <b>Error! Reference source not found.</b> ” on page <b>Error! Bookmark not defined.</b>
<variable>	In command descriptions, angle brackets represent variables. You must substitute a value for command line arguments that are enclosed in angle brackets.
[ optional ] [ <optional> ]	Square brackets enclose optional keywords or <variables> in a command line description. Optionally enter the keyword or <variable> that is enclosed in square brackets, if it is necessary or desirable to complete the task.
[ a   b   c ] [ <a>   <b>   <c> ]	Square brackets enclose optional alternate keywords or variables in a command line description. Choose one command line argument enclosed within the braces, if desired. Choices are separated by vertical (OR) bars.
{ a   b   c } { <a>   <b>   <c> }	Braces enclose required alternate keywords or <variables> in a command line description. You must choose one command line argument enclosed within the braces. Choices are separated by vertical (OR) bars.

## Notifications and Alerts

Notifications and alerts are used to highlight important information or alert you to the potential for data loss or personal injury.

### Tips

Tips are used to highlight information that helps to complete a task more efficiently.

**TIP:** This is some information that will allow you to complete your task more efficiently.

### Notes

Notes are used to highlight important or helpful information.

**NOTE:** Take note. Contains important or helpful information.

### Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss.

**CAUTION!** Exercise caution. Contains important information that may help prevent unexpected results or data loss.

### Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury.

**\*\*WARNING\*\*** Be extremely careful and obey all safety and security measures. In this situation you might do something that could result in catastrophic data loss or personal injury.

## Support Contacts

---

If you encounter a problem while installing, registering, or operating this product, please refer to the documentation before contacting support. If you cannot resolve the issue, contact your supplier or [Thales Customer Support](#).

Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

### Customer Support Portal

The Customer Support Portal, at <https://supportportal.thalesgroup.com>, is where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

**NOTE:** You require an account to access the Customer Support Portal. To create a new account, go to the portal and click the **REGISTER** link.

### Telephone Support

The support portal also lists telephone numbers for voice contact ([Contact Us](#)).

### Email Support

You can also contact technical support by email at [technical.support.DIS@thalesgroup.com](mailto:technical.support.DIS@thalesgroup.com).

# CHAPTER 1: Introduction

SafeNet Agent for Microsoft Remote Desktop Web (RDWeb) ensures that the RDWeb is available only to authorized users by prompting for additional credentials during logon.

By default, logon to RDWeb requires that the user provides a correct user name and a password. The SafeNet Agent for Microsoft RDWeb augments this logon mechanism with strong authentication by adding a requirement to provide a One-Time Password (OTP) generated by the token.

## System Requirements

<b>Operating Systems</b>	<ul style="list-style-type: none"> <li>Windows Server 2012 R2</li> <li>Windows Server 2016 (64-bit)</li> <li>Windows Server 2019 (64-bit)</li> </ul>
<b>Remote Desktop Web</b>	<ul style="list-style-type: none"> <li>Windows Server 2012 R2 Remote Desktop Web</li> <li>Windows Server 2016 (64-bit) Remote Desktop Web</li> <li>Windows Server 2019 (64-bit) Remote Desktop Web</li> </ul>
<b>Authentication Server</b>	<ul style="list-style-type: none"> <li>SafeNet Authentication Service PCE/SPE 3.9.1 (and above)</li> <li>SafeNet Trusted Access (earlier, SafeNet Authentication Service Cloud)</li> </ul>
<b>Software Components</b>	<ul style="list-style-type: none"> <li>Microsoft .NET Framework 4.8</li> <li>IIS 6 Management Compatibility</li> </ul>
<b>Network</b>	TCP Port 80 or 443
<b>Supported Web Servers</b>	<ul style="list-style-type: none"> <li>IIS 8.5 [for Windows Server 2012 R2]</li> <li>IIS 10 [for Windows Server 2016 (64-bit) and Windows Server 2019 (64-bit)]</li> </ul>
<b>Supported IIS Authentication Type</b>	Microsoft Forms Authentication
<b>Supported Web Browsers</b>	<ul style="list-style-type: none"> <li>Chrome</li> <li>Internet Explorer 11</li> <li>Microsoft Edge</li> <li>Mozilla Firefox</li> </ul>
<b>Additional Web Browser Requirements</b>	<ul style="list-style-type: none"> <li>Cookies must be enabled</li> <li>JavaScript must be enabled</li> </ul>



<b>Supported Authentication Methods</b>	All tokens and authentication methods supported by SafeNet server <b>Note:</b> Push OTP is not supported.
---	--

## Functionality not supported

The following functionality is not supported by SafeNet Agent for Microsoft RDWeb:

- The multi-browser support feature introduced in SafeNet Agent for Microsoft RDWeb 1.2.0 does not work with RDGateway agent.
- SafeNet static password change is not supported.

## Authentication Modes

There are two login authentication modes available in the SafeNet Agent for Microsoft RDWeb.

Mode	Description
<b>Standard Authentication Mode</b>	Standard Authentication Mode enables a single-stage login process. Microsoft and SafeNet credentials must be entered in the login page.
<b>Split Authentication Mode</b>	Split Authentication Mode enables a two-stage login process: <ol style="list-style-type: none"> <li>1. Users provide their Microsoft credentials.</li> <li>2. Users provide their SafeNet credentials.</li> </ol>

By default, **Split Authentication Mode** is enabled. The authentication mode can be modified after installation using the **SafeNet RDWeb Agent Manager**.

# CHAPTER 2: Installation

## Prerequisites

**NOTE:** Always work in **Run as administrator** mode when installing, configuring, upgrading or uninstalling the SafeNet Agent for Microsoft RDWeb.

- The following must be installed before installation: **Microsoft .NET Framework 4.8**.

### Remote Desktop Web Access Server

- **RDWeb Access Site** - verify that Forms Authentication is enabled, and that all other authentication types are disabled (default setting).
- **RDWeb Access Pages** - verify that Forms Authentication and Anonymous Authentication are enabled, and that all other authentication types are disabled (default setting).

### SafeNet Authentication Service (SAS)/SafeNet Trusted Access (STA)

Add an Auth Node in the SafeNet server, by following the below steps:

1. In the **SafeNet Server Management Console**, select **VIRTUAL SERVERS > COMMS > Auth Nodes**.
2. Enter the name or IP address of the computer where the SafeNet Agent for Microsoft RDWeb is installed.  
For details, refer **SafeNet Authentication Service (SAS) Service Provider Administrator Guide**.

In addition, communication must be established between the SafeNet Agent for Microsoft RDWeb and the SafeNet server.

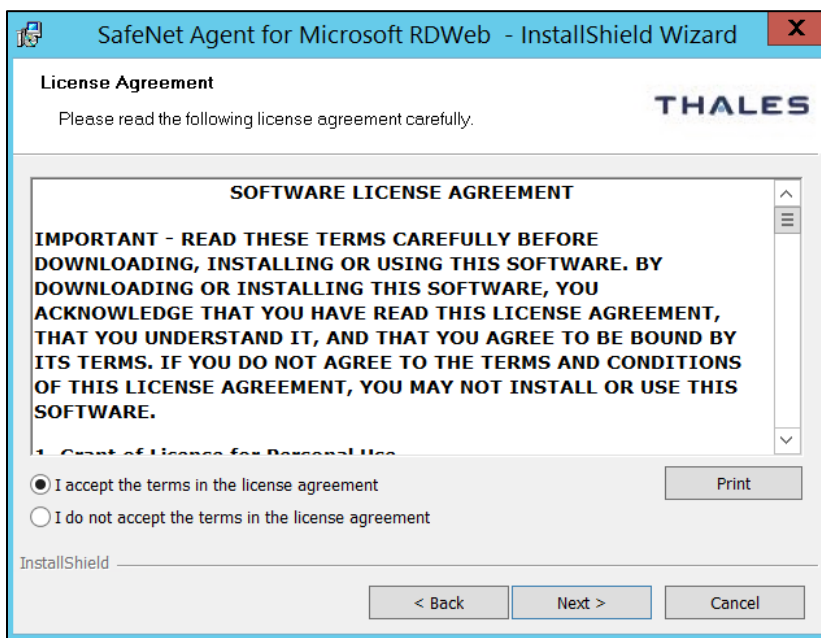
## Installing SafeNet Agent for Microsoft RDWeb

1. Log on to RDWeb server as a user with administrative privileges.
2. Locate and run the following installation package:
  - *SafeNet Agent for Microsoft RDWeb.exe*

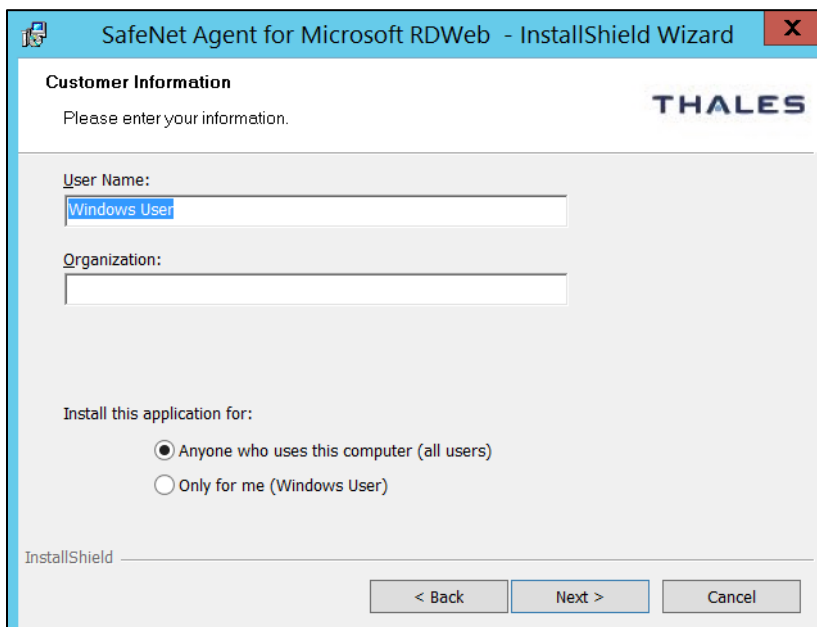
3. On the **Welcome...** screen, click **Next**.



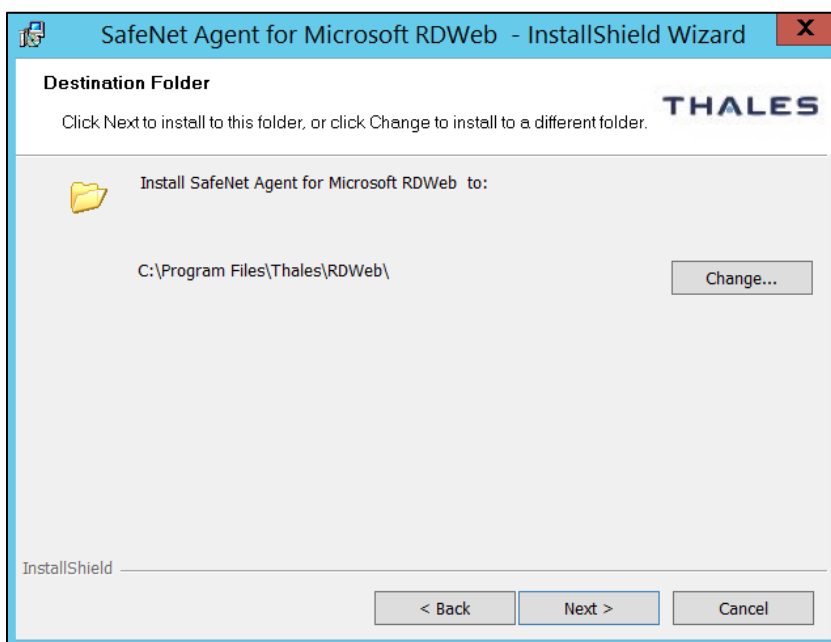
4. On the **License Agreement** screen, accept the license agreement, and click **Next**.



5. On the **Customer Information** screen, enter **User Name** and **Organization** (any names can be used), and click **Next**.

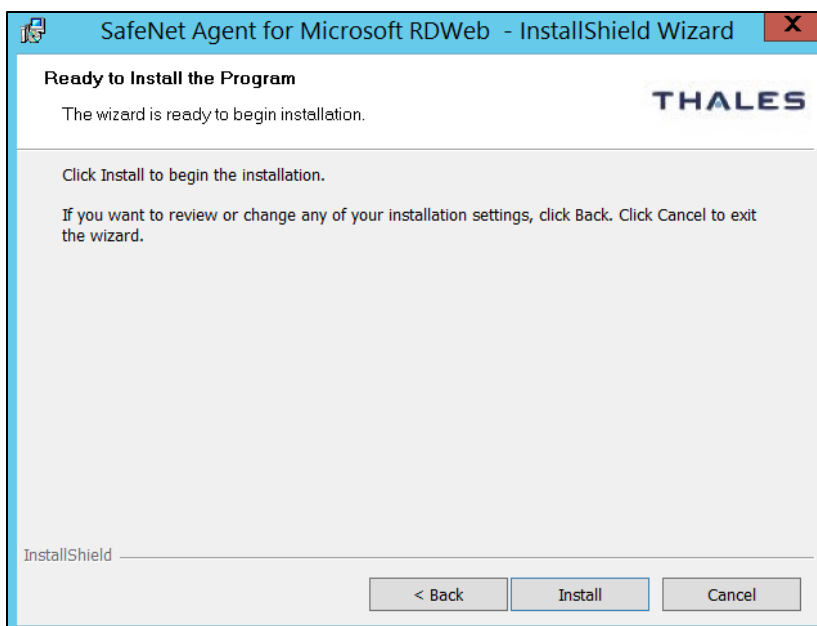


6. On the **Destination Folder** window, perform one of the following:
- To change the installation folder, click **Change** and navigate to the required folder, and then click **Next**.
  - To accept the default installation folder as displayed, click **Next**.

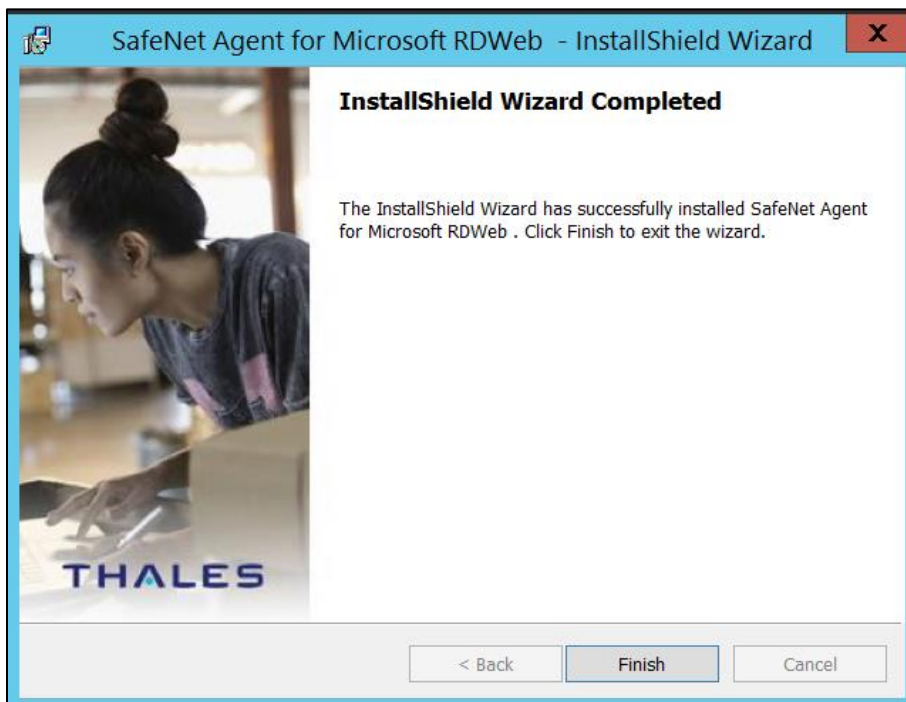


**NOTE:** The default location is **C:\Program Files\Thales\RDWeb**.

7. On the **Ready to Install the Program** window, click **Install**.



8. Once the installation is completed, the **InstallShield Wizard Completed** window is displayed. Click **Finish** to exit the installation wizard.



# CHAPTER 3: Upgrade

## Upgrading SafeNet Agent for Microsoft RDWeb

Direct upgrade to the SafeNet Agent for Microsoft RDWeb 2.0.0 from previous versions (1.0 or 1.0.1 or 1.1.0 or 1.2.0) is supported.

**NOTE:** This is a major upgrade from existing agent versions with name change in the Installer (SafeNet Agent for Microsoft RDWeb), Management Console (SafeNet RDWeb Agent Manager) and the Destination folder (C:\Program Files\Thales\RDWeb\).

To upgrade, run the current (installed) version of the agent. Allow the agent to be upgraded, when prompted.

**NOTE:** For new features to reflect after an upgrade, the following additional steps need to be performed:

1. Clear the **Enable Agent** checkbox and click **Apply**. Select **YES** when IIS Restart is prompted.
2. Select the **Enable Agent** checkbox and click **Apply**. Select **YES** when IIS Restart is prompted.

## CHAPTER 4: Uninstallation

To uninstall the SafeNet Agent for Microsoft RDWeb, use the **Windows Control Panel**. All installed files will be removed except the log files. The default location for the log files:

C:\Program Files\Thales\RDWeb\Log

**NOTE:**

- Always work in **Run as administrator** mode when installing, configuring, upgrading or uninstalling the SafeNet Agent for Microsoft RDWeb.
- If RDGateway agent is also installed, uninstall it before uninstalling the RDWeb agent.

# CHAPTER 5: Configuration

**NOTE:** Always work in **Run as administrator** mode when installing, configuring, upgrading or uninstalling the SafeNet Agent for Microsoft RDWeb.

## Configuring SafeNet Agent for Microsoft RDWeb

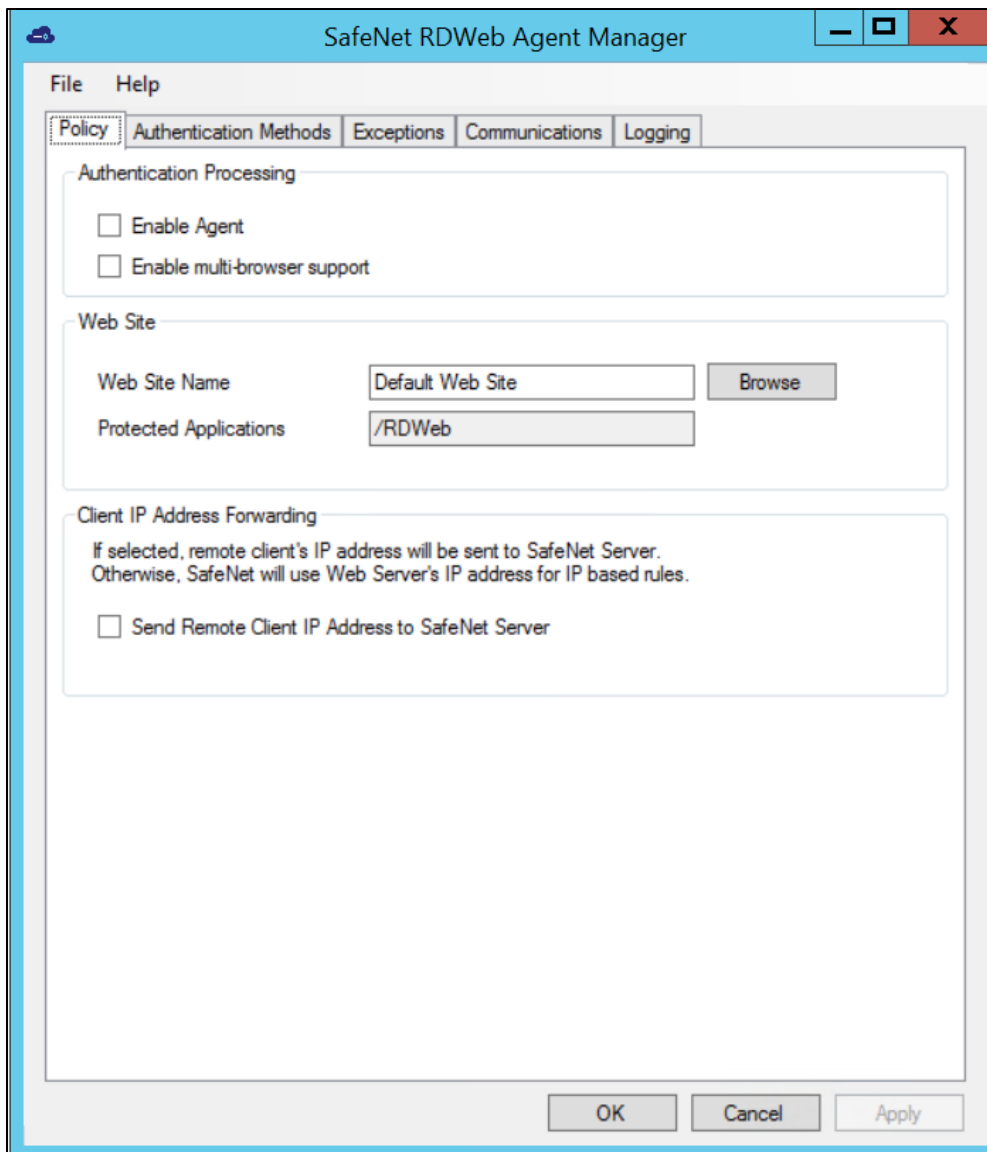
The SafeNet RDWeb Agent Manager enables the modification of various features available within the SafeNet Agent for Microsoft RDWeb. To open the **SafeNet RDWeb Agent Manager**, navigate to installed apps and search for **RDWeb Agent Manager**. After completing configuration of the required setting(s), click **Apply**.



## Configuring Policy Settings

To configure policy settings:

1. Select **Policy** tab.



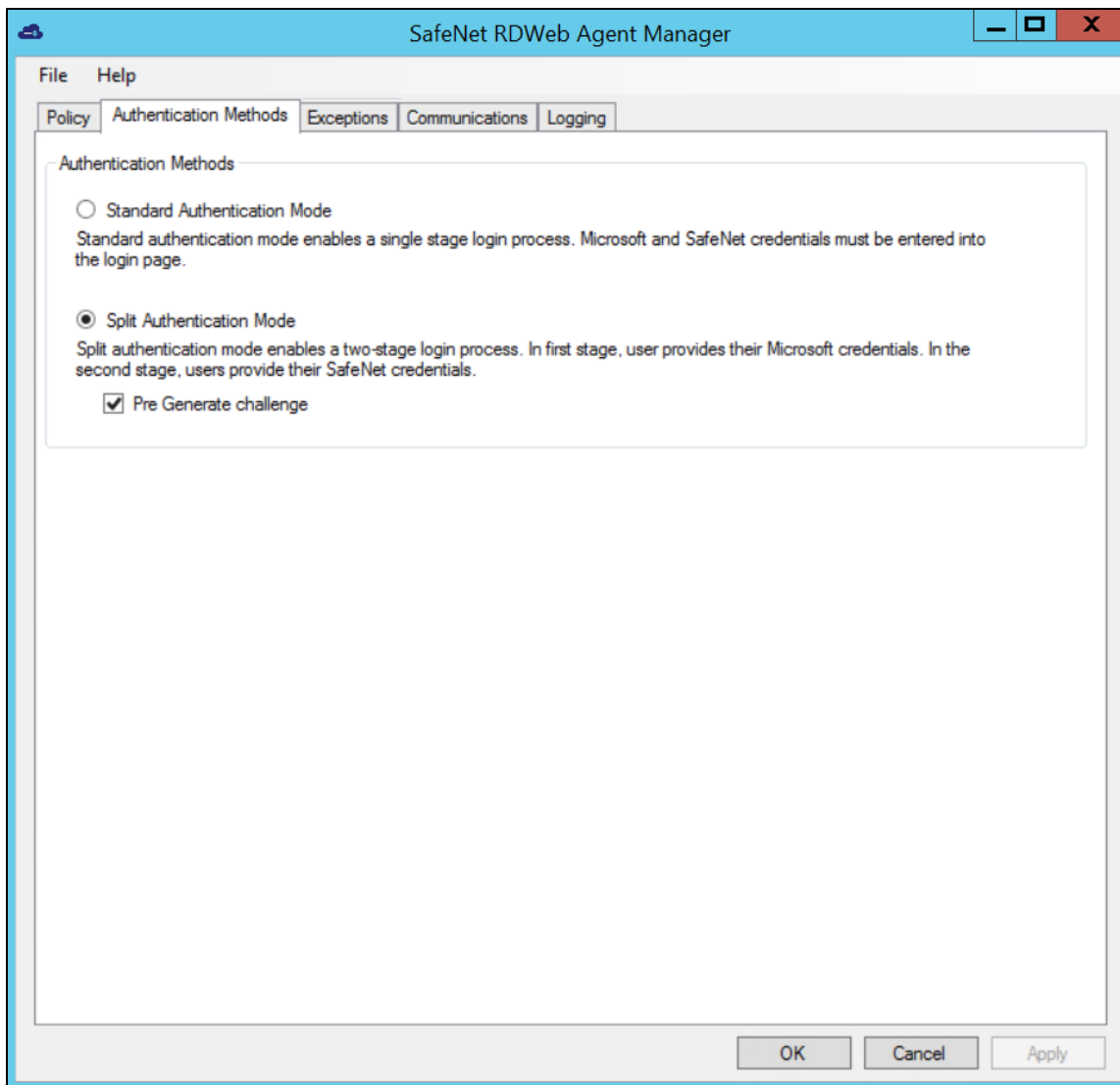
2. To activate SafeNet Agent for Microsoft RDWeb, select **Enable Agent**.
3. To make it compatible with all the browsers, select **Enable multi-browser support**.
 

**Note:** This feature does not work with RD Gateway agent. Therefore, to use RD Gateway agent together with RDWeb, this checkbox must be unchecked.
4. In the **Web Site Name** field, enter **Default Web Site, or any other website**.
5. The **Protected Applications** field displays **/RDWeb** (This is for information only and cannot be changed).
6. To send the remote client IP address to the SafeNet server, select **Send Remote Client IP Address to SafeNet Server**. If not selected, the agent's IP address will be used.

## Configuring Authentication Methods

To select the required authentication method:

1. Select **Authentication Methods** tab.



2. Select one of the following authentication methods:

Authentication Method	Description
<b>Standard Authentication Mode</b>	Enables a single step login process. <b>Default value:</b> Disabled. Microsoft and SafeNet credentials must be entered in a single login page.

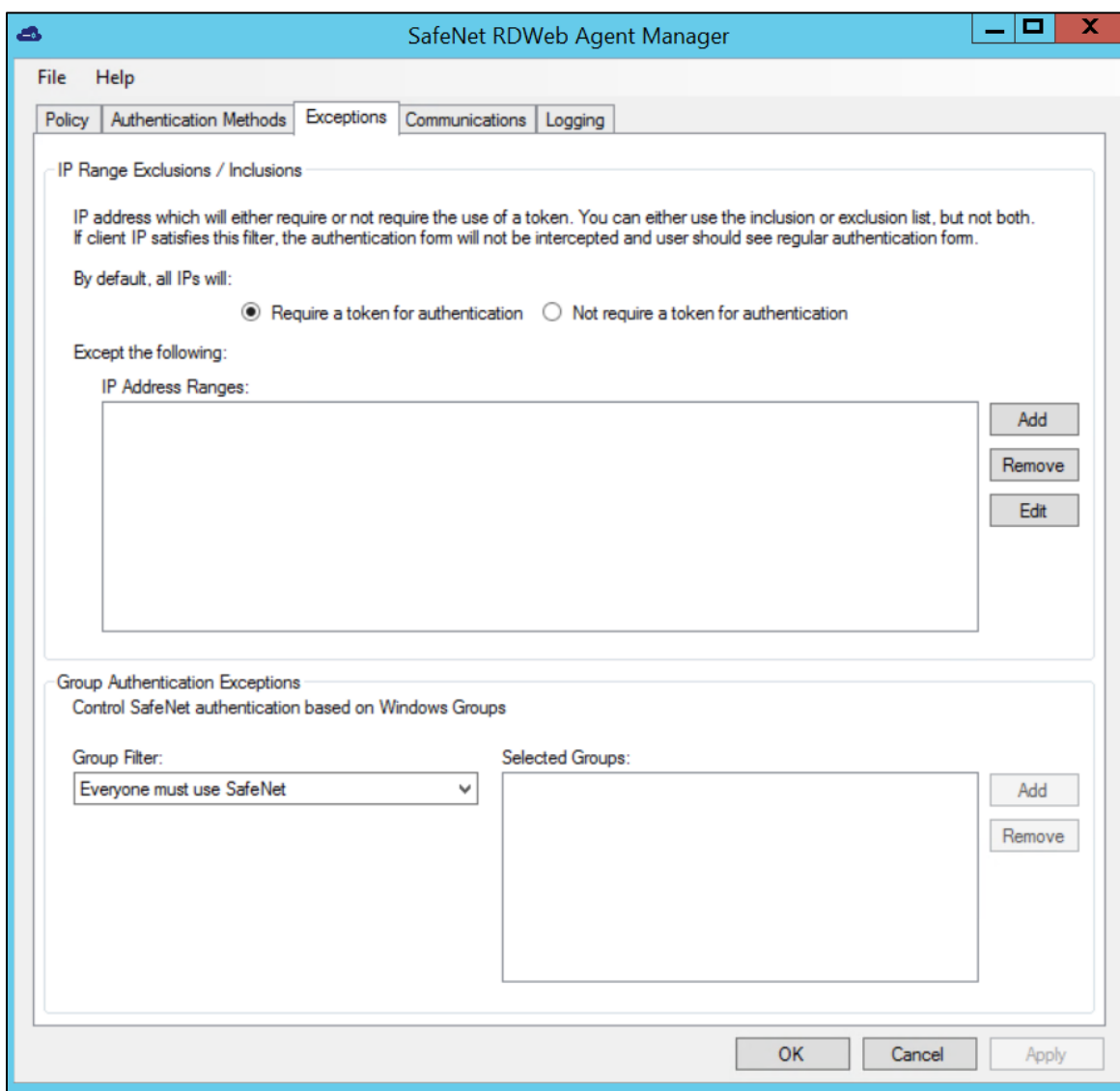
Authentication Method	Description
<b>Split Authentication Mode</b>	<p>Enables a two-stage login process.</p> <p><b>Default value:</b> Enabled.</p> <p>In the first stage, users provide their Microsoft credentials. In the second stage, users provide their SafeNet credentials.</p>

- Pre Generate challenge** (available with Split Authentication Mode): Select to activate [pre generate challenge](#). If selected, the challenge-response token will receive a challenge in the second login screen.

## Configuring Authentication Exceptions

To configure Microsoft groups or network traffic to bypass SafeNet Authentication:

- Select **Exceptions** tab.



2. Under **By default, all IPs will** field, select one of the following
  - **Require a token for authentication** (default)
  - **Not require a token for authentication**
3. In the **IP Address Ranges** box, click **Add** to add the IP addresses to be exempt from using SafeNet Authentication.

**NOTE:** If the **IP Address Ranges** box is left empty, all networks are required to perform SafeNet authentication.

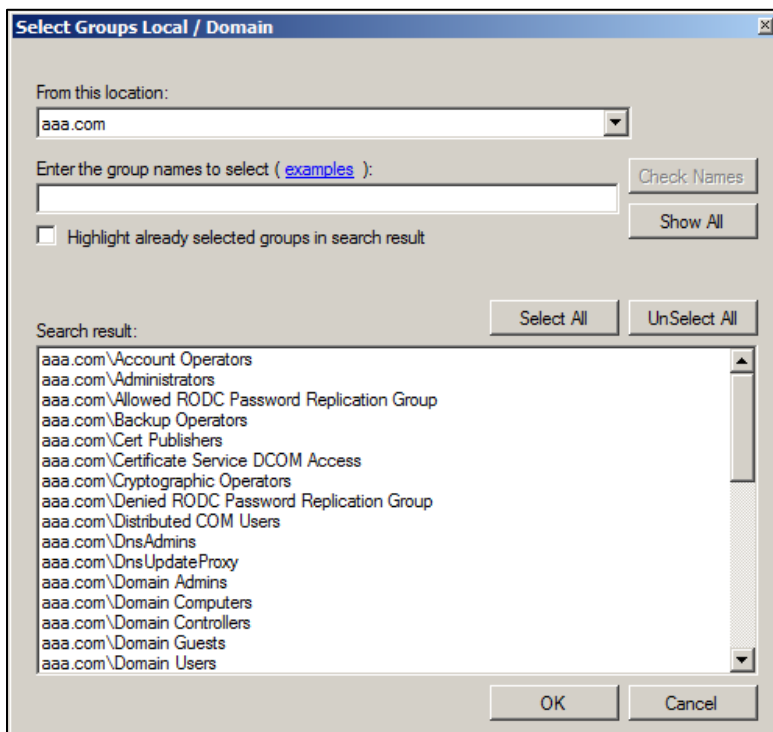
4. To set group authentication exceptions, under **Group Authentication Exceptions**, in the **Group Filter** list, select one of the following:

<b>Everyone must use SafeNet</b>	All users must perform SafeNet Authentication (default).
<b>Only selected groups will bypass SafeNet</b>	All users are required to perform SafeNet Authentication except the defined Microsoft Group(s).
<b>Only selected groups must use SafeNet</b>	Not all users are required to perform SafeNet Authentication; only the defined Microsoft group(s).

**NOTE:**

- Nested Groups are not supported.
- Group authentication exceptions omit single and/ or multiple domain groups from performing SafeNet Authentication. Only one group filter option is valid at any given time, and it cannot overlap with another group authentication exception.

5. To select groups to include as authentication exceptions, next to the **Selected Groups** box, click **Add**. The **Select Groups Local / Domain** window is displayed:



6. Complete fields, as follows:

<p><b>From this location</b></p>	<p>Select the location from which the results will be searched.</p>
<p><b>Enter the group name to select</b></p>	<p>Used in conjunction with <b>Check Names</b> or <b>Show all</b>. Allows searches for Microsoft groups.</p>
<p><b>Highlight already selected groups in search results</b></p>	<p>If a Microsoft group has already been configured in the exception, it will appear as a highlighted result.</p>

## Configuring Connection Options

### Authentication Server Settings

To configure connection options for SafeNet:

1. Select **Communications** tab.

The screenshot shows the 'SafeNet RDWeb Agent Manager' window with the 'Communications' tab selected. The window has a menu bar with 'File' and 'Help'. The 'Communications' tab is active, showing the following settings:

- Authentication Server Settings:**
  - Primary Server (IP:Port): [Empty text box]
  - Failover Server (optional): [Empty text box]
  - Ignore server SSL certificate check:
  - Use SSL (requires a valid certificate):  (next to Primary Server)
  - Use SSL (requires a valid certificate):  (next to Failover Server)
  - Strip domain (username@domain.com, domain\username will be sent as username):
  - Attempt to return to primary Authentication Server every: 6 [up/down arrows] minute(s).
  - Agent Encryption Key File: C:\Program Files\Thales\RDWeb\bsidkey\agent.bsidkey [Browse...]
- Authentication Test:**
  - Test authentication from the agent to the Authentication Server Result:
  - User Name: [Empty text box]
  - Passcode: [Empty text box]
  - Test: [Test button]
- Server Status Check:**
  - Test that the Authentication Server is online [Test button]

At the bottom of the window are buttons for 'OK', 'Cancel', and 'Apply'.

2. Under **Authentication Server Settings**, enter values for the following fields:

Field	Description
<b>Primary Server (IP:Port):</b>	<p>Enter the IP address/ hostname of the primary SafeNet server.</p> <p>Default: Port 80.</p> <p>Select <b>Use SSL...</b> if required. The default TCP port for SSL requests is 443.</p>
<b>Ignore server SSL certificate check</b>	<p>Select the checkbox to disable the SSL server certificate error check on the agent.</p> <p>It is unchecked by default.</p> <p>If customers are using the on-premise deployment of SafeNet server within a well-controlled network (where self-signed certificates are used and cannot be properly validated by the RDWeb Agent), this checkbox needs to be selected.</p> <p><b>NOTE:</b> We strongly recommend the use of SSL certificates.</p>
<b>Failover Server (optional)</b>	<p>Enter the IP address/ hostname of the failover SafeNet server.</p> <p>Default: Port 80</p> <p>Select <b>Use SSL...</b> if required. The default TCP port for SSL requests is 443.</p>
<b>Strip Domain... (username@domain.com, domain\username)</b>	<p>Select if the SafeNet username is required without the suffix <b>@domain</b> or prefix <b>domain</b>.</p> <p><b>NOTE:</b> The realm-stripping feature applies to SafeNet usernames only. Active Directory usernames are not affected.</p> <p>Once stripping is activated or deactivated for an RD Remote Access site, the agent stores these values and uses them as default for each new site protected by the agent.</p>
<b>Attempt to return to primary Authentication Server every</b>	<p>Enter the Primary Authentication server retry interval in minutes. This sets the interval between attempts to return to the primary server.</p>
<b>Agent Encryption Key File</b>	<p>Enter the location of the SafeNet server key file.</p>

## Authentication Test

To test authentication between the SafeNet Agent for Microsoft RDWeb and the SafeNet server:

1. Under **Authentication Test**, enter **Username** and **Passcode**.
2. Click **Test**.

The result is displayed in the **Result** box.

**NOTE:** The behavior of the test will be in accordance with the realm-stripping configuration. For example, if realm stripping has been activated and the user name is entered in the format `username@domain`, then `@domain` will be removed.

To verify the connection between the SafeNet Agent for Microsoft RDWeb and the SafeNet server, click **Server Status Check**. A message is displayed, confirming the connection.

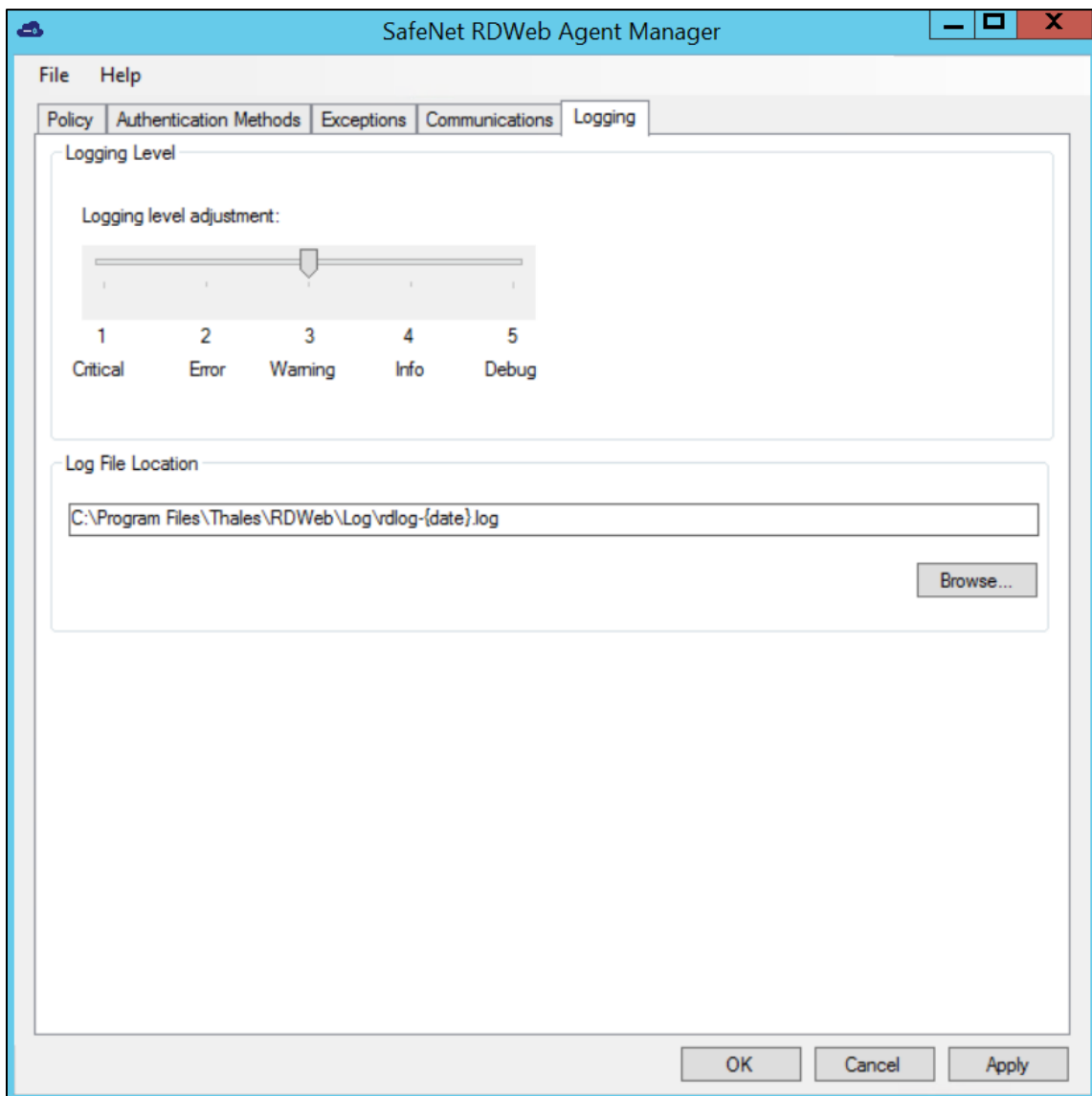


## Configuring Logging Settings

### Adjusting Logging Level

To adjust the Logging Level:

1. Select **Logging** tab.



2. Drag the pointer on the **Logging level adjustment** scale to the required level.

Field	Description
<b>Logging Level</b>	Set the required logging level (default value 3): <b>1 Critical</b> - only critical <b>2 Error</b> - critical and errors <b>3 Warning</b> - critical, errors, and warnings <b>4 Info</b> - critical, errors, warnings, and information messages <b>5 Debug</b> - all available information
<b>Log File Location</b>	Specifies the location of the log files. The log file is rotated on a daily basis. The default log file location is: C:\Program Files\Thales\RDWeb\Log  If you change the default log file location, the folder must be accessible to all users.

3. Click **Apply**.

## CHAPTER 6: Configuring Proxy Server

To set a proxy server, edit the `web.config` file, located at the following path: `C:\Windows\web\RDWeb`  
Insert the following in the section, `<system.web>...</system.web>`

```
<system.net>
  <defaultProxy>
    <proxy proxyaddress="http://myproxyaddress:port"
    />
  </defaultProxy>
</system.net>
```

where,

*http://myproxyaddress:port* is the address and port of the proxy.

# CHAPTER 7: Testing the Solution

## Standard Authentication

1. Browse to the RD Web Access page.

RD Web Access

Work Resources  
RemoteApp and Desktop Connection

THALES

Domain\user name:

Password:

OTP:

Security

Warning: By logging in to this web page, you confirm that this computer complies with your organization's security policy.

Sign in

To protect against unauthorized access, your RD Web Access session will automatically time out after a period of inactivity. If your session ends, refresh your browser and sign in again.

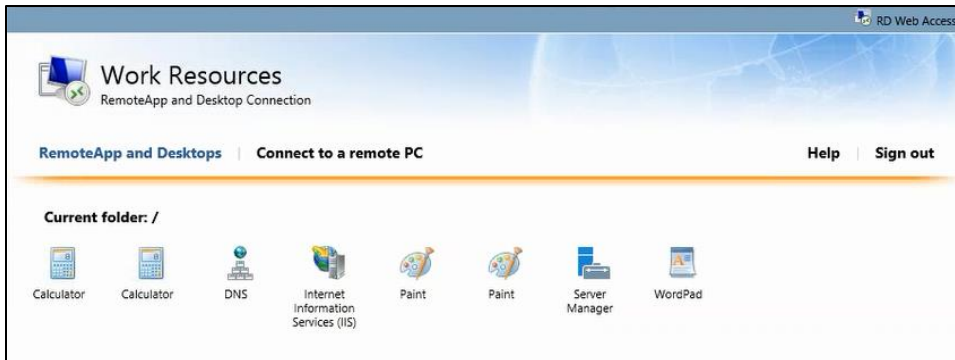
Windows Server 2012 R2

Microsoft

2. Enter the **Domain\user name**, **Password**, and **OTP**.
3. Click **Sign in**.
4. If configured for Grid OTP, leave the **OTP** field empty and click **Sign in** to open the Grid web page.

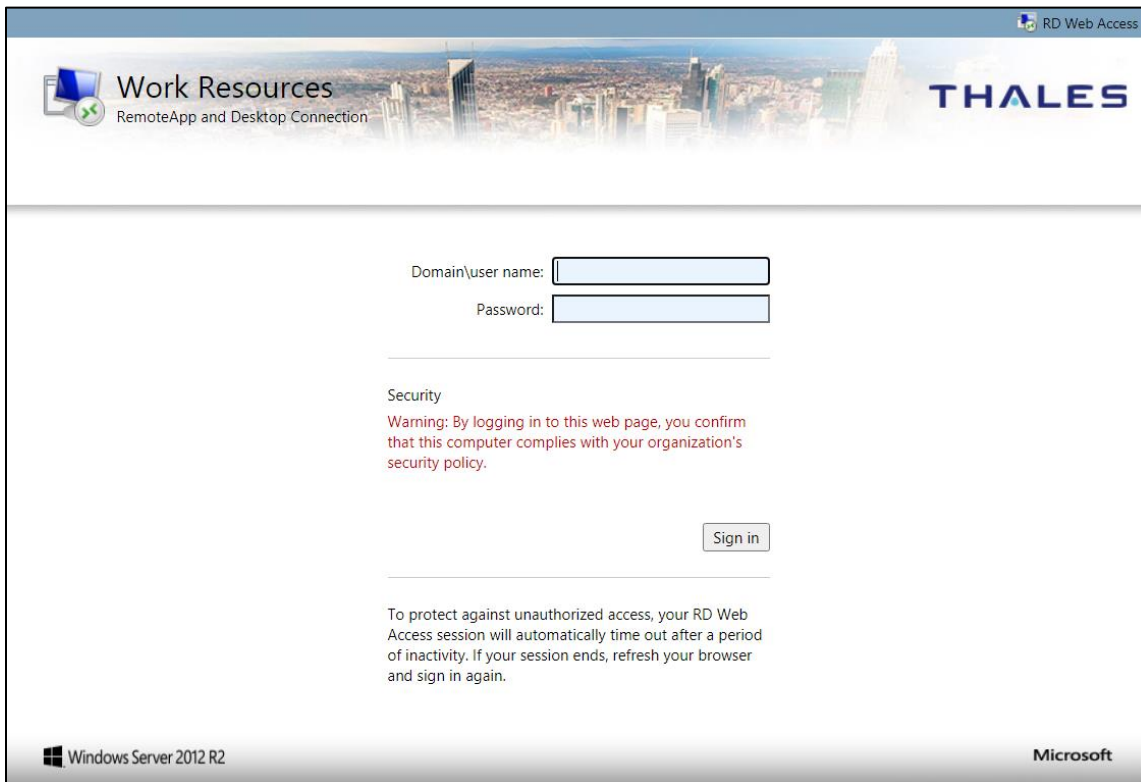
**NOTE:** Self-service AD Password Reset functionality is now added. For details, click [here](#).

5. The remote desktop is displayed:



## Split Authentication

1. Browse to the RD Web Access page.



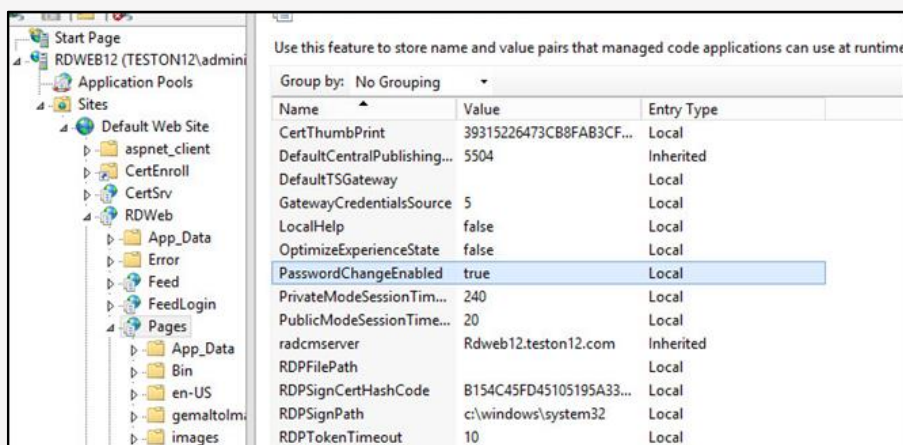
2. Enter the **Domain\user name** and **Password** and click **Sign in**.

If it is configured for split authentication, the **OTP** field is displayed.

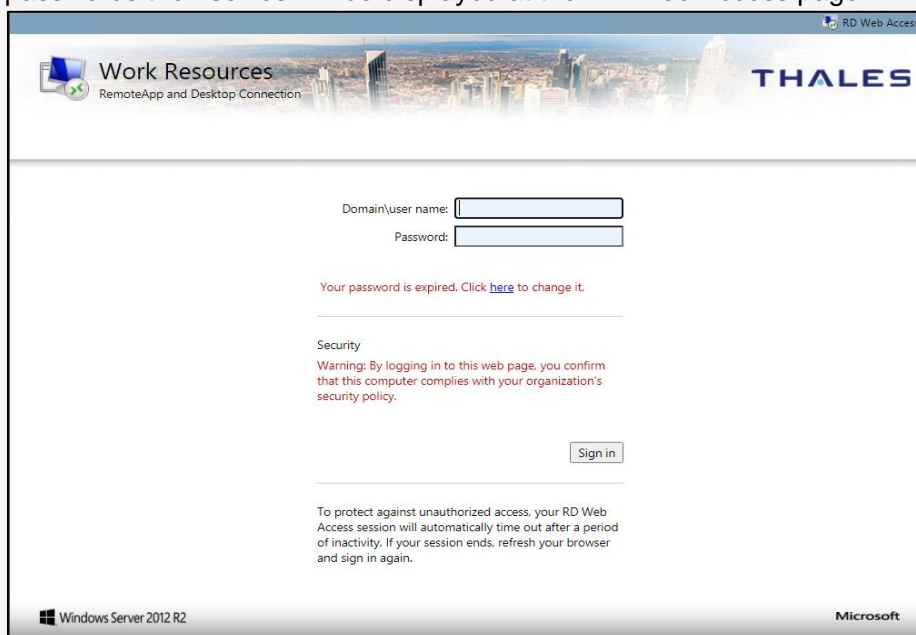
### NOTE:

1. If [Pre Generate challenge](#) was selected during configuration (see [Configuring Authentication Methods](#)), the OTP screen is not displayed. It will jump straight to the Gridsure page.

2. Self-service AD Password Reset functionality is now added. Earlier, if a user's password expired, the user had to contact the administrator to reset it. Now, they can reset the passwords themselves. To enable this functionality, the administrator needs to set the ***PasswordChangeEnabled*** parameter to **True** (if not set already), after [installing](#) the agent, by following the steps:
  - a. Open IIS Manager on the server(s) running RDWeb.
  - b. Navigate to the following path: **Sites** > **Default Web Site** > **RDWeb** > **Pages**  
 Note: **Default Web Site** is the site under which the RDWeb is running. If the RDWeb is running under a different website, navigate to that site and proceed further.
  - c. Select **Application Settings**, and change ***PasswordChangeEnabled*** value to **True**.



Once the parameter is set to **True**, a message (with a link) to enable users to change the passwords themselves will be displayed at the RD Web Access page.



3. In the **OTP** field, enter the passcode and click **Sign in**.

RD Web Access

Work Resources  
RemoteApp and Desktop Connection

THALES

OTP:

Warning: By logging in to this web page, you confirm that this computer complies with your organization's security policy.

Sign in

To protect against unauthorized access, your RD Web Access session will automatically time out after a period of inactivity. If your session ends, refresh your browser and sign in again.

Windows Server 2012 R2 Microsoft

4. If configured for GrIDSure do the following:
  - a. Leave the **OTP** field empty and click **Sign in**.
  - b. The GrIDSure page is displayed. Enter the Grid OTP and click **Sign in**.

RD Web Access

Work Resources  
RemoteApp and Desktop Connection

THALES

9	8	5	1	6
3	4	4	2	0
9	5	0	3	9
8	3	0	7	7
6	2	8	4	1

OTP:

Warning: By logging in to this web page, you confirm that this computer complies with your organization's security policy.

Sign in

To protect against unauthorized access, your RD Web Access session will automatically time out after a period of inactivity. If your session ends, refresh your browser and sign in again.

Windows Server 2012 R2 Microsoft

5. The remote desktop is displayed:

