RSA Authentication Agent 7.1 for Web for IIS 7.0, 7.5, and 8.0 Installation and Configuration Guide

Revision 1

Contact Information

RSA Link at **https://community.rsa.com** contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. 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**.

License Agreement

This software and the associated documentation are proprietary and confidential to EMC, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by EMC.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

April 2012
Revised: November 2016

Contents

Revision History

Revision Number	Date	Revision
1	November 2016	• Added a procedure to allow different RSA SecurID and Microsoft Windows User Names if you do not plan to enable the Web Agent for single sign-on (SSO). • Described how to configure Microsoft Exchange Server 2013 to support the Modal Popup feature. Earlier versions of Microsoft Exchange Server do not require these additional steps. • Added information about how to configure the Web Agent for single sign-on (SSO) to OWA using Microsoft Exchange Server 2013 and Microsoft Exchange Server 2010. • Added information about how to integrate the Web Agent with Microsoft Office SharePoint Server 2013 and SharePoint Server 2010. • Described how to configure persistent cookies on SharePoint Server 2013, and added information about configuring SharePoint Server 2010 to use claims-based authentication. • Updated with information about configuring multiple domain authentication, selective SecurID authentication, using the Web Agent with Active Directory Federation Services, and how to clear the node secret. • Described how to install or upgrade the Web Agent without the RSA Response Interceptor module, and how to remove the module if the Web Agent is already installed. This module generates network traffic that might not be wanted in a deployment that uses Microsoft SharePoint Server, but does not use Microsoft Exchange Server with Outlook Web App (OWA).

Preface

About This Guide

This guide describes how to install and configure RSA Authentication Agent for Web for Internet Information Services 7.0, 7.5, and 8.0. It is intended for administrators and other trusted personnel. Do not make this guide available to the general user population.

RSA Authentication Agent for Web for Internet Information Services 7.0, 7.5, and 8.0 Documentation

For more information about RSA Authentication Agent for Web for Internet Information Services 7.0, 7.5, and 8.0, see the following documentation:

Release Notes. Provides information about what is new and changed in this release, as well as workarounds for known issues. The latest version of the *Release Notes* is available from RSA Link at **https://community.rsa.com**.

Installation and Configuration Guide. Describes detailed procedures on how to install and configure the Web Agent.

Developer's Guide. Provides information about developing custom programs using the Web Agent application programming interfaces (APIs).

Integrating RSA Authentication Agent for Web with RSA Authentication Manager Express Guide. Describes detailed procedures on how to install and configure the web agent to work with Authentication Manager Express(AMX).

RSA Authentication Agent Control Panel Help. Describes how to perform test authentications and configure advanced registry settings in the RSA Authentication Agent control panel. To view Help, click the **Help** button in the RSA Authentication Agent control panel.

RSA Web Agent Configuration Help. Describes how to administer the web access authentication properties of the IIS web server. To view Help, click the **Help** link on the RSA SecurID page of any virtual web site in the Internet Information Services (IIS) Manager.

Related Documentation

For more information about products related to RSA Authentication Agent for Web for Internet Information Services 7.0, 7.5, and 8.0, see the following:

RSA Authentication Manager documentation set. The full documentation set for RSA Authentication Manager 6.1.2 is included in the ***InstallPath*\RSA Security\RSA Authentication Manager\doc** directory. The updated documentation set for RSA Authentication Manager 7.1 SP4, is included in the ***InstallPath*\doc** directory.

Getting 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 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.

Before You Call Customer Support

Make sure you have direct access to the computer running the RSA Authentication Agent for Web for Internet Information Services 7.0, 7.5, and 8.0 software.

Please have the following information available when you call:

- ❑ Your RSA Customer/License ID.
- ❑ RSA Authentication Agent for Web for Internet Information Services 7.0, 7.5, and 8.0 software version number. To find this information, click **Start** > **Settings** > **Control Panel**, and then double-click **RSA Authentication Agent**. The version number appears in the **Installed RSA Agents** section in the RSA Authentication Agent control panel.
- ❑ The make and model of the machine on which the problem occurs.
- ❑ The name and version of the operating system under which the problem occurs.

1 Overview of RSA Authentication Agent for Web for IIS 7.0, 7.5, and 8.0

RSA Authentication Agent for Web for Internet Information Services 7.0, 7.5, and 8.0 (Web Agent) allows you to protect selected web pages with RSA SecurID.

The Web Agent software, residing on a web server, intercepts all user requests for protected web pages. When a user attempts to access a URL that RSA SecurID protects, the Web Agent requests the user name and passcode and passes them to RSA Authentication Manager for authentication. If the authentication is successful, the Web Agent stores the information in a cookie in the user's browser. As long as the cookie remains valid, the user is granted access to protected web pages.

Note: Web access authentication protects http and https URLs. Web access authentication does not support gopher, news, ftp, wais, or telnet protocols.

Security Features

When combined with RSA Authentication Manager, the Web Agent enhances web server security with the strong, two-factor authentication of time-based RSA SecurID tokens. The following table describes the security features provided by the Web Agent.

Security Feature	Description
Two-factor authentication	To gain access to a protected web page, users enter their user name and a valid RSA SecurID passcode, which consists of • A personal identification number (PIN). • The tokencode currently displayed on their RSA SecurID token.
Support for SSL	This feature establishes a private communication channel between the user and the web server, which prevents third parties from eavesdropping.

Security Feature	Description
Tamper-evident cookies	Cookies that the Web Agent distributes to a user's browser that contain: • Information indicating that the user has successfully authenticated. • An encrypted data string that is used to detect whether someone has altered the cookie contents. Any tampering is logged in the system Web Agent audit files. The Web Agent administrator can set the expiration times for the cookies during installation to help protect the URL if users walk away from their computers.
Name locking	Name locking protects against the risk that an unauthorized person might observe a user entering the passcode and submit the same passcode on a different agent host in the realm more quickly than the original user. Name locking is not needed for most customers. Name locking has no effect when the Web Agent is configured to authenticate in conjunction with RSA Authentication Manager. To use the feature, name locking must be enabled for the agent host on RSA Authentication Manager. **Note:** The name locking feature offers security trade-offs that may or may not be appropriate for your environment. By enabling name locking, a 30-second lock is created on RSA Authentication Manager. As with any lockout mechanism, this can be used to prevent a valid user from authenticating by continually relocking the valid user name.
Auditing	The Web Agent records: • Access attempts • Status of connections • Any instances of cookie tampering in audit logs on the agent host
Support for Risk Based Authentication	The Web Agent can be configured to support the Risk Based Authentication feature of Authentication Manager Express(AMX). For more information see the *Integrating RSA Authentication Agent for Web with RSA Authentication Manager Express* Guide

Note: The security provided by the Web Agent depends on the security of the protected system. Even if the Web Agent is implemented with no vulnerabilities, the strong authentication it provides can be subverted if the underlying system is compromised. The Web Agent is intended to bolster the security of the web server and not replace it. If the underlying application is insecure, the Web Agent cannot prevent those vulnerabilities from being exploited. The user is still responsible for securing the servers protected by the Web Agent.

It is important to note that securing the servers involves securing the binaries and other files stored on the server. RSA recommends that you allow only Administrators to access production machines hosting web servers. You also need to ensure that sample code is not installed on production machines.

Types of User Access

Users authenticate to the Web Agent to access protected URLs. You can configure the Web Agent to:

- Protect URLs on the local server on which the Web Agent is installed
- Allow users access to URLs on other servers that the Web Agent protects in the same domain or in multiple domains

For each access type, the Web Agent distributes a cookie to the user's browser so that the user does not have to reauthenticate to each protected resource during a browser session.

The following table describes the different types of user access.

Access Type	Cookies Distributed to User's Browser Upon Successful Authentication	URLs the User Can Access	Configuration Instructions
Local	Local cookie	Protected URLs on the local web server	"Configure the Web Access Authentication Cookies" on page 32.
Domain	Domain cookie	Protected URLs on all web servers in the domain	"Set Up Multiple Server and Multiple Domain Authentication" on page 46.
Multiple domains	Domain cookies from each domain	Protected URLs on web servers in multiple domains	"Set Up Multiple Server and Multiple Domain Authentication" on page 46.

Using the Web Agent with Active Directory Federation Services

Use the following resources to help you integrate the Web Agent with Active Directory Federation Services (ADFS).

Review the following topic from Microsoft:

http://technet.microsoft.com/en-us/library/hh344805%28WS.10%29.aspx

Review the RSA SecurID Ready Implementation Guide for AD FS.

1. Click www.rsaready.com.
2. Click the SOLUTIONS GALLERY (RSA READY COMMUNITY) link.
3. In the SEARCH RSA READY field, enter **AD FS**, and click **Search**.
4. From the search results, click **Microsoft Active Directory Federation Service**.
5. Scroll down to the Integration Link and Guide section.
6. Click **Microsoft_ADFS2.0_RSA_AuthMgr8.0.pdf** to access the *RSA SecurID Ready Implementation Guide* for Microsoft Active Directory Federation Services (AD FS) 2.0.

2 Preparing for Installation

Hardware and Operating System Requirements

The Web Agent is supported on Windows Server 2008 (32-bit and 64-bit) for IIS 7.0, Windows 2008 R2 (32-bit and 64-bit) for IIS 7.5, and Windows 2012 (64-bit) for IIS 8.0.

The Web Agent supports Microsoft Exchange Server 2007, 2010, and 2013, and Microsoft Office SharePoint Server 2007, 2010, and 2013. For more information, see Chapter 6, "Configuring the Web Agent for Single Sign-On to Outlook Web Access," and Chapter 7, "Configuring the Web Agent to Microsoft Office SharePoint Server.".

Note: RSA recommends that you do not install the Web Agent on an RSA Authentication Manager primary instance or replica instance. Running both IIS and RSA Authentication Manager on the same machine may result in decreased performance.

The following table describes the operating system requirements to install WebAgent 7.1

Operating System	IIS 7.0	IIS 7.5	IIS 8.0
Windows Server 2008 SP2 Data Center, Standard, Enterprise, Windows Web Server 2008 SP2	✔		
Windows Server 2008 SP2 Data Center, Standard, Enterprise, Windows Web Server 2008 SP2 running on ESX 4	✔		
Windows Server 2008 R2 Data Center, Standard, Enterprise, Windows Web Server 2008 R2		✔	
Windows Server 2008 R2 Data Center, Standard, Enterprise, Windows Web Server 2008 R2 running on ESX 4		✔	
Windows Server 2012 (64-bit)			✔

The following table describes the hardware requirements to install WebAgent 7.1.

Hardware Requirements	IIS 7.0, 7.5, and 8.0
Hardware	Intel XEON AMD Opteron
Memory Requirements	At least 512 MB of RAM
Disk Space	35 MB
Disk Partition	NTFS **Note:** The FAT file system is not supported.

The host machine must also have:

- TCP/IP networking.
- A Secure Sockets Layer (SSL) certificate

  For more information on obtaining an SSL certificate from a Certificate Authority, go the appropriate web site. For example, go to **https://www.thawte.com** to obtain an SSL certificate from Thawte Consulting. For more information on configuring Internet Information Services for SSL, see the Microsoft IIS website at **http://www.iis.net/**.
- A proxy server that supports the passing of cookies, if users access protected web pages through a proxy.

  For instructions on configuring a proxy server or a reverse proxy server, see your proxy server documentation. For example, see the Microsoft IIS website at **http://www.iis.net/**.

Supported Browsers

Users accessing protected web pages must install one of the following web browsers on their computers:

- Microsoft Internet Explorer 10.0
- Microsoft Internet Explorer 9.0
- Microsoft Internet Explorer 8.0
- Microsoft Internet Explorer 7.0
- Mozilla Firefox 47
- Google Chrome 54

Note: For security purposes, instruct end users to disable caching in their browsers. If you do not prevent the caching of protected pages, and the logoff URL does not have a referring page or referrer, the default URL "/" is cached. Unauthorized users are sent to the default web page without being challenged for RSA SecurID credentials. Ensure that you do not place any sensitive information in the root "/".

Supported Mobile Devices

The following mobile devices are supported by the Web Agent:

- BlackBerry
- Windows Mobile

Wireless Support

RSA SecurID web authentication through wireless access protocol requires the following WAP 1.1 and WAP 1.2.1 specifications:

- Caching of cookies
- WML Document Type Definition (DTD) version 1.1

RSA SecurID users must enable the cookie acceptance feature in their browsers. They must also use web browsers that support FORMs and Persistent Client State HTTP Cookies.

Interoperability with RSA Authentication Manager and Authentication Manager Express

The RSA Authentication Agent 7.1 for Web for IIS 7.0, 7.5, and 8.0 is supported on RSA Authentication Manager 6.1.2, RSA Authentication Manager 7.1 SP4 and Authentication Manager Express 1.0. The Authentication Agent administrator must be familiar with Authentication Manager and its features.

In addition, make sure that the Authentication Manager administrator has registered users in the Authentication Manager database and has distributed tokens to the users.

Note: If you intend to use WebAgent 7.1 to protect the files of multihomed servers, you must account for the extra IP addresses in the Authentication Manager database. The Authentication Manager administrator has to define a secondary node for each additional IP address used on the agent host. In addition, you must specify an IP address override from the Advanced tab of the RSA Authentication Agent control panel. The override address must match the network address specified for the agent host in the server database. For instructions on how to define secondary nodes, see the RSA Authentication Manager documentation.

Pre-Installation Tasks

Install Role Services

The Common HTTP Features role service is installed when you install IIS 7.0 or 7.5. You must install the following role services, including all the role services under them:

- Common HTTP features
- Application development
- IIS 6.0 management compatibility

Note: If these role services are not installed, you cannot uninstall or reinstall the Web Agent.

Verify that .NET 3.5 is Installed on Windows Server 2012

To install the Web Agent on Windows Server 2012, you must have .NET Framework 3.5 installed on the Windows Server 2012 machine.

Windows Server 2012 comes prepackaged with .NET 4.5. However, .NET 3.5 is required.

Specify the Character Set

You can specify the character set used by the application either at the Web Agent level or at the web site level. The character set specified at the Web Agent level is used as the default value for all protected web sites. If you specify the character set at both the Web Agent and the web site levels, the Web Agent uses the web site settings. If you do not specify any character set, the Web Agent returns an error when you try to access protected pages.

For servers hosting multiple character set encoding, you must specify character sets for each web site. If you do not specify the character sets correctly, the web site does not function properly and data may get corrupted.

UTF-8 is the default character set that is used when the Web Agent is installed.

During installation, you can specify the character set at the Web Agent level. You can use the Internet Information Services (IIS) Manager to specify character sets at the web site level. For more information, see the Help topic "Configuring Web Agent Character Settings."

When you specify the character set, you must also specify the corresponding code page. You can find the code page at **http://msdn.microsoft.com/en-us/library/aa288104.aspx**.

By default, the Web Agent assumes the character set to be UTF-8. The character set configured during installation is inherited by all the web sites under IIS, unless overridden by the site level settings. If you prefer to specify the character set for each web site individually, you can leave the settings blank during installation.

Allow Different RSA SecurID and Microsoft Windows User Names

If you do not plan to enable the Web Agent for single sign-on (SSO), then you can create a Windows registry entry that allows the RSA SecurID and Microsoft Windows user names to be different.

As installed, the Web Agent requires the RSA SecurID user name to be the same as the Microsoft Windows user name. This allows you to deploy the Web Agent for single sign-on (SSO) to the Microsoft SharePoint Server or the Outlook Web App. With SSO, users can authenticate through RSA SecurID to access a web application that would otherwise be protected by a Microsoft Windows password.

Note: Do not perform this procedure if you plan to enable SSO.

To allow different user names for RSA SecurID and Microsoft Windows:

1. In the Windows registry, access **HKLM\SOFTWARE\SDTI\RSAWebAgent**.
2. Create a new DWORD Value named **MatchOnSecurIDUsername**.
3. Set the Value to **0**. This value allows different user names.
   To require the user names to match, set the value to **1**.
4. Restart IIS. Do the following:
   a. On the IIS server, click **Start > Run**.
   b. Type **IISReset**, and click **OK**.

The Command Prompt window displays the IISReset command status.

c. Verify that IIS stops and restarts.

Before You Install the Web Agent

Before installing the Web Agent, complete these tasks:

1. Install RSA Authentication Manager 6.1.2, or 7.1 SP4. For instructions, see the corresponding *RSA Authentication Manager Installation Guide.*
2. Copy the Authentication Manager **sdconf.rec** file to the agent host.
3. Register the Web Agent Machine as an agent of Authentication Manager. Select the Agent type to be **Net OS Client** for RSA Authentication Manager 6.1.2, latest service pack and **Web Agent** for RSA Authentication Manager 7.1 SP4.
4. For more information about adding the Web Agent to RSA Authentication Manager 7.1 SP4, see the RSA Security Console Help topic *Add Authentication Agents*.
5. Register RSA SecurID users in the Authentication Manager database and distribute RSA SecurID tokens to those users.

   Note: For more information about distributing tokens to users in RSA Authentication Manager 7.1 SP4, see the RSA Security Console Help topic "Tokens."

6. Ask your Authentication Manager administrator if the user names in the Authentication Manager database records have the users' Windows domain name attached (for example, DOMAIN\user name). If so, select the **Send domain and user name to RSA Authentication Manager** option when you enable Authentication Agent authentication.

   Note: For more information about this option, see "Configure Advanced Settings" on page 36.

3 Installing RSA Authentication Agent for Web for IIS 7.0, 7.5, and 8.0

Install the Web Agent

The Web Agent can be installed to work with compatible versions of the Authentication Manager as well as Authentication Manager Express.

Perform the following steps to install the Web Agent to work with either Authentication Manager or Authentication Manager Express (AMX).

To install the Web Agent:

1. "Install the Web Agent."
2. "Configure the Agent to Work with AMX."

   Note: This step is not required for the Web Agent to work with Authentication Manager.

3. "Configure the Internet Information Services Manager SSL Certificate."
4. "Perform a Test Authentication."

Install the Web Agent

Note: To reduce the amount of network traffic in a deployment that includes Microsoft SharePoint Server but does not include Microsoft Exchange Server with Outlook Web App (OWA), you can disable the RSA Response Interceptor Module. For instructions, see "Install or Upgrade the Web Agent without Enabling the RSA Response Interceptor Module" on page 27.

To install the Web Agent:

1. Log on to the machine as an administrator.
2. Browse to the location, where you downloaded the software, and double-click **setup.exe**.

Note: There are separate web agent installers for 32 bit and 64 bit OS versions. Select the installer that is appropriate for your operating system.

3. Follow the prompts until the sdconf.rec Location dialog box opens. Specify the location of the configuration file.
4. Specify the default character settings for the web agent.

Note: If you leave the fields blank on the Character Set page, you must configure the character settings for each web site. If you don't configure the character settings at both the Web Agent and web site levels, the Web Agent returns an error when you access protected pages from these web sites.

5. Follow the prompts to complete the installation.
6. Specify a primary agent host overriding IP address in the **IP Address Override** field in Other Settings in the RSA Authentication Agent Advanced tab.

   This ensures that the Web Agent always uses the specified IP to communicate with Authentication Manager.

Note: Perform this step only when the Web Agent runs on a host that has multiple network interface cards, and therefore multiple IP addresses. Typically the Web Agent host attempts to discover their own IP addresses and may choose an IP address that is unknown to the RSA Authentication Manager. This makes communication between the Web Agent and Authentication Manager impossible.

7. Restart the IIS web server.

Note: Use the Repair option in the installation wizard to reinstall the Web Agent. You will be able to reinstall the Web Agent successfully using the Repair option only if you have installed the Internet Information Services 7.0, 7.5, and 8.0 features, as mentioned in "Pre-Installation Tasks" on page 18.

After you finish installing the Web Agent, you must configure the Microsoft Internet Information Services (IIS) Manager. For instructions, see "Configure the Internet Information Services Manager SSL Certificate."

Configure the Agent to Work with AMX

The Web Agent has to be configured for it to work with the Risk Based Authentication feature of Authentication Manager Express.

For more information on the configuration steps for the Agent to work with AMX, refer to the *Integrating RSA Authentication Agent for Web with RSA Authentication Manager Express Guide*.

Note: The following features are unavailable in a Web Agent configured for AMX:
Enable Selective SecurID Authentication
Use Separate User Name and PASSCODE Pages
Use JavaScript Pop-Up Window to Authenticate in Frames

Configure the Internet Information Services Manager SSL Certificate

Install a Secure Sockets Layer (SSL) certificate on the web server. For more information on obtaining an SSL certificate from a Certificate Authority, go the appropriate web site. For example, go to https://www.thawte.com to obtain an SSL certificate from Thawte Consulting. For more information on configuring Internet Information Services for SSL, see the Microsoft IIS website at http://www.iis.net/.

Note: If you do not have an SSL certificate installed, the web access authentication user name and passcode will not be encrypted before transmission

Perform a Test Authentication

You test authentication to:

- Verify the authentication environment
- Create a node secret for the Web Agent

The node secret is a symmetric encryption key that Authentication Manager and the Web Agent use to encrypt and decrypt packets of data as they travel across the network. The first time a user successfully authenticates or tests authentication from a Web Agent host, Authentication Manager creates a node secret for that Web Agent host and stores it in the Authentication Manager database. A copy of the node secret is encrypted and sent to the Web Agent. The node secret is stored in a file on the Web Agent host.

If the node secret on the Web Agent host is corrupted or does not match the node secret in the Authentication Manager database, encrypted communications between the Web Agent and Authentication Manager cannot work. If this happens, Authentication Manager logs a node verification failure message in the Authentication Manager Activity Monitor. For troubleshooting information, see "Node Secrets" on page 133.

Before you deploy tokens to users, use the RSA Authentication Agent control panel to test that Web Agent authentication has been correctly implemented. The test verifies that:

- The **sdconf.rec** file you installed on the Web Agent host points to the appropriate Authentication Manager database.
- The host has a valid node secret file.
- Your system is configured properly for authentication.

To test authentication:

1. Click **Start** > **Settings** > **Control Panel**, and then double-click **RSA Authentication Agent**.
2. In the RSA Authentication Agent control panel, from the **Main** tab, click **Test Authentication with RSA Authentication Manager**.
3. In the RSA SecurID Authentication Information dialog box, click **RSA ACE/Server Status**, verify the information, and then click **OK**.

   For more information about the server status, see the Help topic "Verifying the Status of Your Environment."
4. Click **RSA ACE/Server Test Directly**.
5. In the **Token type** list, select **Key fob or metal card**.
6. In the **User name** field, enter the user name of the registered RSA SecurID user assigned to the token.
7. In the **Passcode** field, enter the passcode, which is the PIN followed by the tokencode generated by your RSA SecurID token.
8. Click **OK**.

   If the system is correctly implemented and configured, it displays a message that the user authenticated successfully. If you cannot authenticate, see Chapter 8, "Troubleshooting."

Co-existence of the Web Agent and the Windows Agent

If the WebAgent is installed on a machine, that already has the Windows Agent installed on it and if both the agents are configured to use the same Authentication Manager, the administrator has to perform some configuration steps for the agents to work together.

Follow the guidelines below to complete configuration steps for the agents to work together:

1. As the agent host for Windows Agent has already been registered in the Authentication Manager, the administrator must use the same agent host entry for the WebAgent. For more information on this, see Chapter 2, "Preparing for Installation."
2. If the Windows agent is working successfully with the Authentication manager, the node secret will already be present in the agent host. The administrator should use the same node secret with the WebAgent. As the node secret format is different for the Windows Agent and the WebAgent, the administrator should first convert the node secret to the WebAgent format using the agent_nsload utility.

   The agent_nsload utility is available with the Authentication SDK. To download the Authentication SDK, please go to **https://community.rsa.com**. Refer the documentation available with the SDK kit to find how to use the utility.

   The name of the node secret file should be **securid**. After the node secret is converted, copy it to the Web Agent installation location.

   Note: The default location of the node secret is **C:\Program Files\RSA Security\RSAWebAgent**.
3. Restart the IIS Web Server.

Upgrade to Web Agent 7.1

You can upgrade to Web Agent 7.1 only from Web Agent 7.0.

Important: Ensure that you have installed the Microsoft Visual C++ 2005 Redistributable Package (x64) or (x86), before upgrading from Web Agent 7.0 to Web Agent 7.1.

Note: Create a back up of the **securid** file before you proceed with the upgrade.

To upgrade from Web Agent 7.0 to Web Agent 7.1:

1. Log on to the machine as a local administrator.
2. Browse to the directory you created when you downloaded the software. Unzip the **iis_upgrade.zip** file. Navigate to the **iis_upgrade** folder. Follow the steps provided in the **README_BEFORE_UPGRADE.txt** file (present inside the iis_upgrade_64 or iis_upgrade_32 zip files) to upgrade to Web Agent 7.1.

Note: To reduce the amount of network traffic in a deployment that includes Microsoft SharePoint Server but does not include Microsoft Exchange Server with Outlook Web App (OWA), you can disable the RSA Response Interceptor Module.

When the **README_BEFORE_UPGRADE.txt** file instructs you to run **setup.exe**, see "Install or Upgrade the Web Agent without Enabling the RSA Response Interceptor Module" on page 27.

3. Check the Web Agent version number in the control panel to verify if the upgrade has been successful.

Note: Use the Repair option in the installation wizard to reinstall the Web Agent. You will be able to reinstall the Web Agent successfully using the Repair option only if you have installed the Internet Information Services 7.0, 7.5, and 8.0 features, as mentioned in "Pre-Installation Tasks" on page 18.

4. Follow the steps below to convert the node secret from the old format to the new format, after upgrading to Web Agent 7.1.
   a. Download the Authentication SDK from **https://community.rsa.com**. The agent_nsload utility that is used to convert the node secret from the old format to the new format, is available with the Authentication SDK.
   b. Refer to the documentation available with the SDK to find how to use the utility.
   c. Use the utility to convert the node secret to the new format.
   d. Copy the node secret to the location where you installed the WebAgent.

Note: The default location of the node secret is **C:\Program Files\RSASecurity\RSAWebAgent**.

After you finish installing the Web Agent, you must configure the Microsoft Internet Information Services (IIS) Manager. For instructions, see "Configure the Internet Information Services Manager SSL Certificate" on page 23.

Install or Upgrade the Web Agent without Enabling the RSA Response Interceptor Module

The RSA Response Interceptor module monitors web site activity and triggers a modal popup privacy screen when cookies expire. If your Web Agent deployment uses Microsoft SharePoint Server, but does not use Microsoft Exchange Server with Outlook Web App (OWA), you do not require this additional monitoring of your web sites. Disabling the RSA Response Interceptor module results in less network traffic, prevents the Web Agent installer from updating your **web.config** files with information about this module, and prevents the modal popup privacy screen from displaying.

You can run a command line script to install or upgrade the Web Agent without enabling the RSA Response Interceptor module. If you upgrade the Web Agent while disabling the RSA Response Interceptor Module, any RSA Response Interceptor Module data is removed from the **web.config** files.

To install or upgrade the Web Agent without enabling the RSA Response Interceptor Module:

1. Log on to the machine as an administrator.
2. Open the Windows Command Prompt, for example, click **Start > Search**, type **cmd**, and press ENTER.
3. Change directories to the location where you downloaded and extracted the software, for example, **C:\Program Files\RSA Security\RSAWebAgent**. Type:

   ```
   cd C:\Program Files\RSA Security\RSAWebAgent
   ```

   and press ENTER.
4. Run the installation or upgrade script. Type:

   ```
   setup.exe /v"NO_RESPONSE_INTERCEPTOR=1"
   ```

   and press ENTER.

Note: Do not enter a space between the "/v" option and the `"NO_RESPONSE_INTERCEPTOR=1"` argument.

Next Steps

- (New installations only) After you finish installing the Web Agent for the first time, you must configure the Microsoft Internet Information Services (IIS) Manager. For instructions, see "Configure the Internet Information Services Manager SSL Certificate" on page 23.
- (Upgrades only) After you run **setup.exe**, see step 3 in "Upgrade to Web Agent 7.1" on page 25.

Uninstall the Web Agent

Important: To uninstall a Web Agent that is configured for single sign-on (SSO) access to Outlook Web Access, see "Before You Uninstall the Web Agent" on page 93. To uninstall a Web Agent that is configured for SSO to Microsoft Office SharePoint Server 2007 SP2 or 2010, see "Before You Uninstall the Web Agent" on page 119.

To uninstall the Web Agent:

1. Click **Start > Settings > Control Panel > Programs and Features**.
2. Scroll down the list of programs installed, and then click **RSA Authentication Agent for Web for IIS**.
3. Click **Uninstall**.
4. In the modules list, verify if an entry exists for the SecurIDModule.Click **Remove** from the Actions pane of the IIS Manager to remove the module.

Next Step

Do the following:

- If the Web Agent was deployed with Microsoft Exchange Server 2013 SP1 with or without SSO, see "Reconfigure Microsoft Exchange Server 2013 After Uninstalling Web Agent" on page 28.
- If the Web Agent was deployed with Microsoft Exchange Server 2010 or 2007 without SSO, see "Reconfigure Microsoft Exchange Server 2010 or 2007 After Uninstalling Web Agent" on page 29.
- If the Web Agent was deployed with Microsoft Exchange Server 2010 or 2007 with SSO, no additional procedures are required.

Reconfigure Microsoft Exchange Server 2013 After Uninstalling Web Agent

After you uninstall Web Agent, Microsoft Exchange Server 2013 SP1 requires an additional procedure to remove the RSAResponseInterceptorModule from the Exchange Back End modules list.

To remove the RSAResponseInterceptorModule:

1. On the Microsoft Exchange Server, click **Start > Settings > Control Panel > RSA Web Agent**.
2. In the Connections pane, double-click *server_name*, and click **Sites > Exchange Back End > owa**, where *server_name* is the name of the IIS Server Machine.

3. Remove the RSAResponseInterceptorModule from the Modules list:
   a. Using a text editor, open web.config of *server_name*, and click **Sites > Exchange Back End > owa**, where *server_name* is the name of the IIS Server Machine.
   b. Remove the following entry from the <modules> tag, which is before the </system.webServer> tag:

```
<add name="RSAResponseInterceptorModule"
type="SecurityModules.ResponseInterceptor,
RSAResponseInterceptorModule, Version=version_number,
Culture=neutral, PublicKeyToken=3b8ca08bdac1d008" />
</modules>
```

   c. Save and close the **web.config** file.
4. Restart IIS. Do the following:
   a. On the IIS server, click **Start > Run**.
   b. Type **IISReset**, and click **OK**.
      The Command Prompt window displays the IISReset command status.
   c. Verify that IIS stops and restarts.

Reconfigure Microsoft Exchange Server 2010 or 2007 After Uninstalling Web Agent

This procedure is required if the Web Agent was deployed with Microsoft Exchange Server 2010 or 2007 without single sign-on (SSO). If the Web Agent was deployed with Microsoft Exchange Server 2010 or 2007 with SSO, no additional procedures are required.

To reconfigure Microsoft Exchange Server 2010 or 2007:

1. On the Microsoft Exchange Client Access Server, click **Start > Programs > Microsoft Exchange Server 2007/2010 > Exchange Management Console**.
2. In the left pane of the Exchange Management Console, double-click **Server Configuration > Client Access**.
3. In the bottom portion of the Client Access pane, right-click **owa** and select **Properties**.
4. In the owa (Default Web Site) Properties dialog box, click the **Authentication** tab, and then select **Use forms-based authentication** and **Domain/user name**.
5. Click **OK**.
6. Restart the IIS web server.

4 Configuring Web Access Authentication Properties

Administer the Web Access Authentication Properties

You administer the web access authentication properties of your IIS web server through the IIS Manager that has been extended with the RSA SecurID web access authentication properties sheet.

From the IIS Manager, you can:

- Configure web access authentication cookies.
- Protect entire sites, individual directories, and individual files.
- Configure advanced settings.
- Specify the location of customized templates.
- Set up multiple server and multiple domain authentication.

Note: When you make changes to the web access authentication properties of a virtual server, you must restart the IIS server.

To open the RSA SecurID web access authentication properties sheet:

1. Click **Start > Settings > Control Panel**, and then double-click **RSA Web Agent**.
2. In the Connections pane, double-click ***server_name*** **> Sites**, and then click the name of the web site whose properties you want to view.
3. In the *web_site* Home pane, double-click **RSA SecurID**.

Configure the Web Access Authentication Cookies

Each time an RSA SecurID user enters a valid passcode at the web access authentication prompt, the web server stores a web access authentication cookie in the user's web browser. The cookie passes the user's authentication information to the server when the user browses to a protected file or directory on that server. As long as the cookie is still valid, the user does not have to authenticate again during the current session. A cookie is valid only during the browsing session for which it was created. If the user closes the web browser, he or she must reauthenticate to get a new cookie. After cookie expires the end-user will get a popup for re-authentication.

Note: This works only if the protected site's application pool is in the integrated mode. Outlook Web Access/ SharePoint 2007 only works in the Classic mode. After cookie expiry in OWA/SharePoint 2007, the end-user will not get a modal popup and must re-login to proceed.

For instructions on setting cookie expiration times, see the Help topics "Controlling Cookie Expiration Times" and "Setting Cookie Expiration Times." For information about cookies that are valid on multiple servers in a domain or on multiple domains, see "Set Up Multiple Server and Multiple Domain Authentication" on page 46.

Note: You can use the Web Agent Cookie API to add information, which you extract at a later time, to the cookie. For more information, see the *Developer's Guide*.

Protect Resources

The following table describes the different options for protecting resources and provides the related Help topic for each option.

Protected Resource	Option	Related Help Topic	Description
Entire web site	Protect This Resource	Protecting an Entire Site	By protecting the virtual server, you are protecting the root directory and everything it contains. Do not attempt to protect only the **default.htm** file. Instead, protect the entire virtual web server, but remove the protection settings on specific directories or files that you want to make available for general access. **Note:** The Web Agent supports multiple virtual servers on the same physical machine.
Individual directories	Protect This Resource with RSA SecurID	Protecting Individual Directories	RSA recommends that you protect entire directories. Any files or subdirectories that you add to the directory after you change its web access authentication settings will automatically inherit those settings, unless you change the settings on a specific file or directory.

Protected Resource	Option	Related Help Topic	Description
Individual files	Protect This Resource with RSA SecurID	Protecting Individual Files	When you protect a directory, any files or subdirectories you add to the directory later are protected automatically. Protecting files instead of specific directories creates additional administrative overhead. With individual file protection, you must enable URL protection on each file, which may result in some files being overlooked and left unprotected. **Note:** Assume that you have protected a file, but not the virtual directory containing the file. In this case, when you type **www.exampledomain.com/file.htm**, you are prompted for SecurID credentials. But, when you try to access **www.exampledomain.com**, you are not prompted for credentials. To ensure that you are prompted for credentials in both the cases, protect the directory by selecting **Protect This Resource with RSA SecurID**, but do not select **Apply Change Recursively**, and manually protect the individual file.

Protected Resource	Option	Related Help Topic	Description
			Once the SecurID protection is enabled, make sure the SecurIDModule is given high priority by performing the following steps. This is done to ensure no other modules bypasses the SecurID authentication 1. Click **Start > Settings > Control Panel**, and then double-click **RSA Web Agent**. 2. In the Connections pane, double-click ***server_name*** **> Sites**, and then click the name of the virtual server whose properties you want to view. 3. In the protected site Home pane, double-click **Modules**. 4. In the Actions pane, click **View Ordered List**. 5. In the Modules pane, move the SecurIDModule to the top of the list. To do this, select the module, and click **Move Up** in the Actions pane.

Configure Advanced Settings

The following table describes the configuration options available through the RSA SecurID web access authentication properties sheet and provides the related Help topic for each option.

Option	Related Help Topic	Description
Web Agent Character Settings	Configuring Web Agent Character Settings	This setting enables you to enhance the security of your web site. You must determine the character settings used by the web site to configure this setting. By default, this setting is inherited from the Web Agent level default setting that is set during installation. If you want to override the Web Agent level settings, you can configure the character sets for individual web sites. If your web site is designed to support the UTF-8 character set, you must set the site-level character setting to UTF-8. You can find the code page corresponding to the character setting at **http://msdn.microsoft.com/en-us/library/aa288104.aspx** If you do not specify the character sets correctly, the web site might not function as expected and data might get corrupted.
Require Secure Connections to Access Protected Pages	Requiring Secure Connections to Access Protected Pages	A Secure Sockets Layer certificate prevents unauthorized users from monitoring the connection, intercepting a user's passcode, and gaining access to protected pages. RSA recommends that you enable SSL.
Redirect HTTP Connections to Secure Server	Controlling Redirection of HTTP Connections	If you enable SSL, clients that connect using a non-SSL (HTTP) connection are redirected to a page with a link to the HTTPS server. Rather than display a page with a link, you can automatically redirect users to the secure server. For example, if a user attempts to access a protected resource at **http://www.exampledomain.com/sales_figures/**, the user's request would be redirected automatically to **https://www.exampledomain.com/sales_figures/** (note use of the **HTTPS** protocol).

Option	Related Help Topic	Description
Disable IIS Server if Agent Fails to Load	Disabling the Internet Information Services (IIS) Server if the Agent Fails to Initialize	If the web access authentication feature set fails to load properly during web service startup, the IIS server is disabled. All users who try to access URLs on the server see an error page. The server is disabled to ensure that unauthorized users do not gain access to protected resources. RSA recommends that you enable this feature for optimum protection of web resources. If you do not disable the virtual web server, in the event of a failure, all protected resources are fully available to any person who gains access to the server.
Enable Group Security	Enabling Group Security	The Group Security feature allows you to control group access to protected web resources. For more information, see "Control Group Access to Protected Web Resources" on page 47.
Send Domain and User Name to RSA Authentication Manager	Sending the Domain Name with the User Name	If your Authentication Manager database records have users' domain names appended to their user names, for example, DOMAIN\jsmith instead of simply jsmith, you can configure web access authentication to send the full domain\user name string during authentication to the Authentication Manager. To use this feature, you must have Windows authentication enabled on your web server. For more information, see the Microsoft Internet Information Server (IIS) documentation. When RSA SecurID users attempt to access a page that is protected by web access authentication, they must first enter their Windows user name and password. You must instruct users to always enter their domain names with their user names (for example, DOMAIN\jsmith). When the RSA SecurID passcode authentication prompt displays, the full domain\user name string is inserted automatically in the **User name** field.

Option	Related Help Topic	Description
Prevent Caching of Protected Pages on Clients	Preventing Caching of Protected Pages	If an RSA SecurID user's browser is left unattended, an unauthorized user can view pages that are stored in the cache long after the user has quit his or her browsing session. When you prevent the caching of protected pages, you minimize the security risk. If you do not prevent the caching of protected pages, and the logoff URL does not have a referrer, the default URL "/" is cached, and the unauthorized user is sent to the default web page without being challenged for RSA SecurID credentials. Ensure that you do not place any sensitive information in the root "/".
Ignore Browser IP Address for Cookie Validation	Ignoring the Browser IP Address for Cookie Validation	By default, this feature is disabled so that the Web Agent uses the browser IP address to sign the cookie. However, if there is a proxy or a firewall between the browser and the Web Agent, the IP address used may be the same. If you have web sites that are accessed through load balanced proxy servers, which means that the browser IP addresses may change, you may want to enable this feature. Otherwise, the user may have to authenticate quite frequently.

Option	Related Help Topic	Description
Use RSA Authentication Manager Name Locking Feature	Enabling Name Locking	Name locking protects against the risk that an unauthorized person might observe a user entering the passcode and submit the same passcode on a different agent host in the realm more quickly than the original user. With name lock, the agent host sends the user's logon name and passcode to the Authentication Manager separately. If someone attempts to use the same user name and passcode, the Authentication Manager refuses the authentication request. Name locking is not needed for most customers. Name locking has no effect when the Web Agent is configured to authenticate in conjunction with RSA Authentication Manager 7.1. Name locking must be enabled for the agent host on RSA Authentication Manager 6.1.2 to gain any benefit from the feature. **Note:** The name locking feature offers security tradeoffs that may or may not be appropriate for your environment. By enabling name locking, a 30-second lock is created on RSA Authentication Manager 6.1.2. As with any lockout mechanism, this can be used to prevent a valid user from authenticating by continually relocking the valid user name.
Use Separate User Name and PASSCODE Pages	Using Separate User Name and Passcode Pages	If you enabled name locking, you can also configure the Web Agent to display separate user name and passcode pages to the user. **Note:** Displaying the user name and passcode prompts as separate pages, necessary to fully receive the security offered by name locking, comes with security tradeoffs that may or may not be appropriate for your environment. When the prompts are separated onto different pages, the Web Agent creates new sessions while submitting the user names. As with most session management systems, this creates the possibility that all sessions will be reserved, and new authentication attempts will be rejected until old sessions complete.

Option	Related Help Topic	Description
Use JavaScript Pop-Up Window to Authenticate in Frames	Using a JavaScript Pop-Up Window to Authenticate in Frames	If the protected web site uses HTML frames, sometimes the passcode prompt is too small to read clearly. To avoid this problem, display the passcode prompt in a JavaScript pop-up window. **Note:** This feature will not work if cross frame scripting is prevented by WebAgent, which is a security feature enabled by default. If the user wants to use the 'JavaScript popup' feature cross frame busting has to be disabled by setting the environment variable RSA_NO_FRAME_BUSTING=1 in the WebAgent machine. In general, it is recommended to protect the main page, instead of protecting individual frames in the page.
Auto-Submit (Avoid Having to Click Continue After Successful Authentication)	Enabling Auto Submit	By default, after a user authenticates successfully, the Web Agent displays a success page on which the user must click **Continue** in order to access the desired URL. When you enable Auto Submit, after a user authenticates successfully, the desired URL opens without the user having to click **Continue**.
Use Text Link Authentication Mechanisms for Multiple Domain WML Access	Using the Text Link Authentication Mechanism for Multiple Domain WML Access	During multiple domain authentication, the Web Agent attempts to get an image from each of the domains to verify that it has made a connection. Some cell phones display the image even though the Web Agent has not connected successfully. Once users authenticate in a multiple domain environment and attempt to access a URL in another domain, they are prompted to authenticate again. This option forces the users to manually click a text link for each domain instead of attempting to automatically making the connection using images.
Disable Cookie API Processing	Disabling Cookie API Processing	This option allows you to disable any cookie API processing that you have implemented. **Note:** If you enable single sign-on, cookie API processing is automatically enabled.

Option	Related Help Topic	Description
Use Standard Page Cache Prevention Mechanism for WML Access	Using the Standard Page Cache Prevention Mechanism for WML Access	Because many cell phones do not respond to the standard method of preventing page caching, the Web Agent uses an alternative method for WML access. However, the standard method is more efficient. This option configures the Web Agent to attempt to use the standard method of preventing page caching. To use this feature, you must first enable **Prevent Caching of Protected Pages on Clients**, and the user's cell phone must be capable of using the standard no cache method.
Use RSA Token for Cross-Site Request Forgery Protection	Using the RSA Token for Cross-Site Request Forgery Protection	Enabling this option protects RSA SecurID Authentication web pages from cross-site request forgery attacks. This feature works by adding a random number, referred to as an RSA token, as a hidden parameter in the forms and pages, which are based on the templates provided by RSA. The RSA Web Authentication API provides functions to get the RSA token from the web access authentication cookie. A request is allowed only if the RSA token is found to be valid, as verified by the Web Agent. For the logoff URL, the web page containing the link to the RSA logoff URL uses this API to retrieve the RSA token and set it in a hidden field. This token is sent along with the logoff request. If this option is enabled, the Web Agent verifies the RSA token and accepts the request only if the token in the request is valid. To learn more about how to use the RSA Web Authentication API to add the RSA token in the logoff URL, refer to the sample programs provided with the Web Agent installer. The Web Agent also sets a pre-logon cookie containing an RSA token in all the RSA web pages, such as the Logon page and New PIN page, which is verified when you submit these pages.

Option	Related Help Topic	Description
Templates	Specifying the Location of Customized Templates	During installation, the default HTML and WML templates are stored in the **/templates** directory. If you customize these templates, you need to store them in a different directory and specify the location in the web access authentication properties sheet.
Target This Resource for Single-sign On	Using Single-sign On	With single sign-on (SSO), users authenticate using only RSA SecurID tokens to access a web application or web portal that would otherwise also be protected by a Microsoft Windows logon. SSO access is applicable for Outlook Web Access and Microsoft Office SharePoint Server 2007 SP2 and 2010 on Windows Server 2008 SP2 and Windows 2008 R2 only.
Manage SharePoint Settings	Manage SharePoint Settings	You can configure the persistent cookie settings for single sign-on between Internet Explorer and Microsoft Office 2003/2007/2010 when client integration is enabled on Microsoft Office SharePoint Server 2007 SP2, 2010, and 2013 SP1.
Cookies expire if not used within the specified time	Setting Cookie Expiration Time	You can set the cookies to expire if they remain idle (server side) for the specified expiration time during the current browsing session. The minimum time is one minute. The maximum time is 1440 minutes (one day). This value applies to both session cookies and persistent cookies. If you have legacy applications that require you to prevent persistent cookies from expiring, see "Remove the Idle Timeout Value for Persistent Cookies" on page 43. When cookies expire, the Modal Popup feature displays a black privacy screen. For instructions on implementing this feature, see "Configure Microsoft Exchange Server 2013 to Support the Modal Popup Feature" on page 44. **Note:** For increased security on WAP browsers, RSA recommends setting the idle cookie expiration time to less than the default of five minutes.

Option	Related Help Topic	Description
Cookies Always Expire After the Specified Time	Setting Cookie Expiration Time	You can set cookies to expire after the specified expiration time is reached during a browser session, whether or not the cookie is idle. The minimum time is one minute. The maximum time is 1440 minutes (one day). This value applies to session cookies. It does not apply to persistent cookies. **Note:** For increased security on WAP browsers, RSA recommends setting the cookie expiration time to less than the default of 15 minutes.

Remove the Idle Timeout Value for Persistent Cookies

Persistent cookies allow users to open SharePoint documents in Microsoft Office without authenticating multiple times. Both session cookies and persistent cookies use the idle timeout value that is specified by the "Cookies expire if not used within the specified time" advanced setting in the RSA SecurID web access authentication properties sheet. Persistent cookies are deemed vulnerable to attacks because they continue to exist even when a browser with a user session is closed, but the idle timeout value allows persistent cookies to expire.

You can create a Windows registry entry that causes persistent cookies to expire only when the cookie lifetime expires. This behavior may be necessary if you have legacy applications, such as the ActiveSync application, that require you to prevent persistent cookies from expiring when they remain idle on the server.

For information on how to set up persistent cookies, see Chapter 7, "Configuring the Web Agent to Microsoft Office SharePoint Server."

To remove the cookie idle timeout property from persistent cookies:

1. In the Windows registry, access **HKLM\SOFTWARE\SDTI\RSAWebAgent**.
2. Create a new DWORD Value named **PersistentCookieIdleTime**.
3. Set the Value to **0**. This value remove the cookie idle timeout option **Cookies expire if not used within the specified time** from persistent cookies only.
   To apply the idle timeout option to persistent cookies, set the value to **1**.
4. Restart IIS. Do the following:
   a. On the IIS server, click **Start > Run**.
   b. Type **IISReset**, and click **OK**.
      The Command Prompt window displays the IISReset command status.
   c. Verify that IIS stops and restarts.

Configure Microsoft Exchange Server 2013 to Support the Modal Popup Feature

Microsoft Exchange Server 2013 requires additional configuration to support the Modal Popup feature. The Modal Popup feature displays a black privacy screen when cookies expired. The web session is still active, however, so this option is not a security feature.

Note: This additional procedure does not apply to Microsoft Exchange Server 2007 or 2010.

To enable the Modal Popup Feature for Microsoft Exchange Server 2013:

1. Make sure that the application pool of the site to be protected is in Integrated mode. If the application pool is in Classic mode, you must change it.
2. Verify that the RSAResponseInterceptorModule is in the Exchange Back End Modules list. Do the following:
   a. On the Microsoft Exchange Server, click **Start > Settings > Control Panel > RSA Web Agent**.
   b. In the Connections pane, double-click ***server_name***, and click **Sites > Exchange Back End > owa**, where *server_name* is the name of the IIS Server Machine.
   c. Verify that the RSAResponseInterceptorModule is in the Modules list. If the module is not listed, you must add it.
   d. Using a text editor, open **web.config** of ***server_name***, and click **Sites > Exchange Back End > owa**, where *server_name* is the name of the IIS Server Machine.

      By default, the **web.config** file is located in the following directory:

      C:\Program Files\Microsoft\Exchange Server\v15\ClientAcess\OWA
   e. Add the following entry in the <modules> tag, which is before the </system.webServer> tag:

      ```
      <add name="RSAResponseInterceptorModule"
      type="SecurityModules.ResponseInterceptor,

      RSAResponseInterceptorModule, Version=7.1.4.194,
      Culture=neutral, PublicKeyToken=3b8ca08bdac1d008" />

      </modules>
      ```
   f. Save and close the **web.config** file.
   g. In the Connections pane, double-click ***server_name***, and click **Sites > Exchange Back End > ecp**, where *server_name* is the name of the IIS Server Machine.

      By default, the **web.config** file is located in the following directory:

      C:\Program Files\Microsoft\Exchange Server\v15\ClientAcess\ECP
   h. Repeat step c through step f for the ecp site.

3. Make sure that OWA and the ECP of the Exchange Back End is SecurID protected. Do the following:
   a. On the Microsoft Exchange Server, click **Start > Settings > Control Panel > RSA Web Agent**.
   b. In the Connections pane, double-click ***server_name***, and click **Sites > Exchange Back End > owa**, where *server_name* is the name of the IIS Server Machine.
   c. In the owa Home pane, double-click **RSA SecurID**.
   d. In the RSA SecurID pane, select **Protect This Resource with RSA SecurID**.
   e. In the Actions pane, click **Apply**.
   f. In the Connections pane, double-click ***server_name***, and click **Sites > Exchange Back End > ecp**, where *server_name* is the name of the IIS Server Machine.
   g. In the ecp Home pane, double-click **RSA SecurID**.
   h. In the RSA SecurID pane, select **Protect This Resource with RSA SecurID**.
   i. In the Actions pane, click **Apply**.
4. Restart IIS from the command prompt. Do not use the IIS Manager GUI to restart IIS. Do the following:
   a. On the IIS server, click **Start > Run**.
   b. Type **IISReset**, and click **OK**.
      The Command Prompt window displays the IISReset command status.
   c. Verify that IIS stops and restarts.

Prevent Caching of Static HTML Pages in Client Browsers

The IIS Manager caches the frequently accessed static HTML pages. Any request to access the cached page, is not routed through the Web Agent. As a result, the user might be able to view the cached page without being prompted for SecurID authentication. To disable this caching, the administrator has to set the following response headers.

To prevent caching of static HTML pages in client browsers:

1. From the IIS Manager on the WebAgent machine, in the Connections pane, double-click ***server_name***, and click **Sites > Default Web Site**.
2. In the Web Site home page, double-click **Output Caching**.
3. In the Actions pane, click **Add** to add a rule in the Add Cache Rule dialog box:
   a. Enter the file name extension as **.htm/.html** to add Cache Rule for HTML pages.
   b. Check **User-mode caching** check-box and select **Prevent all caching**.
   c. Check **Kernel-mode caching** check-box and select **Prevent all caching**.
   d. Click **OK**.

Specify the Location of Customized Templates

During Web Agent installation, the default templates are copied into the ***install_path*/RSA Security/RSAWebAgent/templates** directory. If you decide to use customized templates, you must store them in a different directory, and point the Web Agent to that directory. For instructions, see the Help topic "Specifying the Location of Customized Templates."

Note: The Web Agent comes with sample Microsoft Exchange Server ActiveSync templates, located in **/samples/ActiveSync/Template_Examples.zip**. For instructions on customizing these samples or creating your own ActiveSync-specific templates, see Chapter 5, "Customizing Templates and Message Strings."

Set Up Multiple Server and Multiple Domain Authentication

The Web Agent enables RSA SecurID users to authenticate on virtual web servers across multiple web domains. A user enters his or her passcode only once to authenticate to each of the participating web servers. After authenticating successfully, the user has access to protected resources in the participating web servers' domains.

Important: Domain cookies bypass a workstation's agent host activations in the RSA Authentication Manager database. RSA SecurID users, whose browsers use a domain cookie from one server, might gain access to information on other servers that they are usually not allowed to view. Restrict access to confidential directories by assigning **Read** permission only to the appropriate RSA SecurID users. For information on setting security permissions, see the Windows 2008 documentation.

Ensure that you test the multiple server and multiple domain authentication features from the client machine and not the machine on which the Web Agent is installed. For multiple domain authentication to work, you need to allow access to third-party cookies in the web browser.

For instructions on setting up multiple server or multiple domain authentication, see the Help topics "Setting Up Multiple Server Authentication" and "Setting Up Multiple Domain Authentication."

Configuring Multiple Domain Authentication

When configuring multiple domain support, observe the following guidelines:

- Add only one server per domain in the Manage Domain Configuration dialog box.
- A Web Agent for IIS in one domain can share multiple domain support with a Web Agent for Apache in another domain. However, the type of web server added must be the same as the configuring server. That is, if the configuring server is Web Agent for IIS, then only an IIS web server protected by Web Agent for IIS in the another domain should be added. If the other domain has only, say, Web Agent for Apache, then a Web Agent for IIS should be setup in that domain and be added to the configuring server for the multiple domain support to work.

- Do not mix secure and non-secure web servers. Multiple domain support will not work if in one domain, the server is accessed through non-secure HTTP and through secure HTTP in the other domain. For example, if on one Apache server "Require secure connection to access protected pages" is enabled, authenticating to this server first does not allow access to other servers without another authentication. By disabling this setting, the problem is resolved.

Note: The browser should consider all Web Agent-protected domains in the local intranet. For example, a problem accessing ***.net** after first authenticating at ***.com:88** can be resolved by adding ***.net** as a local intranet. To do this in Internet Explorer, perform the following steps:

1.Select **Tools > Internet options > Security > Local intranet > Sites > Advanced**.
2.Add the ***.net** domain to the web sites.

Control Group Access to Protected Web Resources

The Group Security feature allows you to control group access to protected web resources.

When you enable Group Security, during user authentication, the Web Agent stores the list of group memberships from the user's Authentication Manager record in the user's web access authentication cookie. Once the user is authenticated, the system compares the Windows group permissions of the requested resource to the groups listed in the user's cookie. If a valid match is found, the user gains access to the resource. If no valid match is found, the user is denied access to the resource.

For example, you want only managers to gain access to the **Inet451** directory on the web server. By enabling the Group Security feature, you can ensure that:

- The **Inet451** directory is protected by web access authentication.
- Only users who have Manager in the Shell field of their Authentication Manager database record can gain access to the directory.

Note: If the IIS machine is a primary domain controller or backup domain controller, you cannot use the Group Security feature.

To enable the Group Security feature, you must perform the following tasks:

1. "Create a Local Group."
2. "Activate a User on the Agent Host."

Note: In RSA Authentication Manager 6.1.x, perform this procedure through the RSA Authentication Manager Database Administration application. In RSA Authentication Manager 7.1.x, perform this procedure using the RSA Security Console.

3. "Associate the Local Group with a File Protected by RSA SecurID."
4. "Enable Group Security."

Note: On IIS 7.0, even after you enable the group security feature, users who are not part of the group and who do not have the required permission might still be able to view the content of the web page along with an error message. You must download the hot fix available at **http://support.microsoft.com/kb/960267**.

Create a Local Group

To control group access to a protected web resource, you must first create a local group on the Web Server.

To create a local group:

1. On the web server, click **Start > Programs > Administrative Tools > Computer Management**.
2. Double-click **Local Users and Groups**.
3. Right-click **Groups**, and select **New Group**.
4. Fill in the appropriate name and description, and click **Create**.

   Note: You do not need to fill in the **Members** field.

5. Repeat step 4 for each group you want to create.

Activate a User on the Agent Host

Note: Authentication Manager also allows you to activate users on agent hosts through Authentication Manager groups. If a user is activated directly on the agent host and through an Authentication Manager group with the same user name but different **Shell** fields, the direct **Shell** field overrides the group **Shell** field.

To activate a user on the agent host in Authentication Manager 6.1.x:

1. From the RSA Authentication Manager 6.1 Administration application, open the appropriate user record.
2. Click **Agent Host Activations**.
3. In the **Available Agent Hosts** panel, select the web server, and click **Activate On Agent Hosts**.

4. In the Activate User dialog box, do the following:
   - In the **Login** field, type the appropriate user name.
   - In the **Shell** field, type the name of the local group you created on the web server.

     Note: If you are entering multiple group names in the **Shell** field, you must separate the names by a comma. Do not insert any spaces in the field. For example, Sales,Marketing,HQ.

   - Click **Exit > OK**.

To activate a user on the agent host in Authentication Manager 7.1:

1. Access the appropriate user record in Authentication Manager 7.1.
2. Select **User Authentication Settings** for the user.
   The User Authentication Settings page is displayed for the user.
3. In the **Default Shell** field, enter the name of the local group created on the web server.
4. Click **Save**.

Associate the Local Group with a File Protected by RSA SecurID

The local group created on the Web Server must be associated with the file, protected by RSA SecurID.

To associate the local group with a file protected by RSA SecurID:

Note: You must perform this procedure through Windows Explorer, not the IIS Manager.

1. On the web server, open Windows Explorer, and browse to the file you want to associate with the local group.
2. Right-click the file, and select **Properties**.
3. Click the **Security** tab, and click **Edit**
4. In the Permissions for *file_name* dialog box, click **Add**.
5. In the Select Users, Computers, or Groups dialog box, add the local group you created on the web server.
6. Assign the appropriate permissions.
7. Click **OK**.

Enable Group Security

You can control group access to protected web resources by enabling group security on the Web Server.

To enable group security:

1. In the *web_site* Home pane, double-click **RSA SecurID**.
2. Under **Advanced Settings**, select **Enable Group Security**.
3. In the Actions pane, click **Apply**.
4. Restart the IIS server.

Enable Selective SecurID Authentication

You can configure the agent to selectively always prompt or never prompt users for authentication. Users who are not prompted for RSA SecurID authentication are prompted for Windows passwords, provided the user is available in Active Directory

Note: In the Password Only mode, the user must enter the password in the **Passcode** field.

Note: In a group hierarchy, restricting RSA SecurID authentication to a particular group only works for one level in the group hierarchy. It does not work for users that belong to a group, within the protected group.

To enable selective RSA SecurID authentication:

1. Click **Start > Control Panel**, and click RSA Authentication Agent.
2. Select the Advanced tab.
3. From the **Challenge Configuration** dropdown, select the required option.

Option	Description
All Users	All users will be prompted for SecurID authentication.
None	No users will be prompted for SecurID authentication.
All Users In	All users in the active directory groups listed will be prompted for SecurID authentication.
All Users Except	All users except those listed will be prompted for SecurID authentication.

4. If either the All Users In or All Users Except options are selected, enter the user names or Active Directory group names, separated by a semicolon (;), with no spaces before or after each semicolon.

   Configure Web Agent selective authentication exactly as follows:

   Group specification

   Valid groups (in combination with any other setting) are:

   a. Local groups

      To specify a local group, the syntax is ***groupName***. No prefix, such as ".\", is acceptable.

   b. Domain groups, defined as domain local

      To specify a domain group, the syntax is ***domainName\groupName*** where *domainName* must be the "flat" domain name, as specified by the NETBIOS name.

   For either a Local or Domain group, the members must be domain users. No other type of group content is acceptable.

   User specification

   A username can represent a local user or a domain user.

   To specify a user name, the syntax is ***username***. No prefix specifying a domain is acceptable.

   Multiple group and user specification

   You can specify multiple groups, multiple users, or multiple groups and users. Make sure that the groups and users are separated by a semicolon (;), with no spaces before or after each semicolon.

5. Click **Apply**.

6. Click **Close**.

Note: The groups listed under All Users In and All Users Except can be local groups or domain groups. If the group is a domain group, the group scope should be Domain Local.

Use the Logoff URL to Invalidate Web Access Authentication Cookies

The logoff URL enables you to set up a link on a web page that automatically invalidates a user's web access authentication cookies and prompts the user to authenticate.

To set up the logoff URL, use a relative path to add the following URL to a link on your web pages:

```
http://www.server.domain.com/WebID/IISWebAgentIF.dll?logoff?
referrer=/sample.html
```

where

- *server* is the name of your server.
- *domain* is the name of your domain.
- ***sample*.html** is the web page.

This logoff URL works only if you have not selected the **Use RSA Token for Cross-Site Request Forgery Protection** option in the web access authentication properties sheet. If you select this option, the web page containing the link to the logoff URL sets the RSA token as a query parameter in the logoff URL. The logoff URL is generated dynamically, as shown in this example:

```
http://www.server.domain.com/WebID/IISWebAgentIF.dll?logoff?
RSArand=<RSA token>&referrer=/sample.html
```

You can retrieve the RSA token from the web access authentication cookie using the RSA Web Authentication API. For more information on how to use the RSA Web Authentication API to add the RSA token in the logoff URL, see the sample programs provided with the Web Agent installer.

Note: If you do not provide an argument to **referrer=** in the logoff URL, users are sent to the root directory on the virtual web server.

Important: If you do not use a relative path to set up the logoff URL, the URL logs off the user and fails to connect to the referrer web site. The user is not prompted to reauthenticate. If you use an absolute path to set up the logoff URL, you must add an auto-redirect script to enforce RSA SecurID authentication. For information about auto-redirect scripts, see the following section, "Enforce RSA SecurID Authentication using Auto-Redirect Scripts."

To ensure that the copied cookies are not reused after the user performs a WebAgent LogOff(), the logged off cookies are stored in a cookie cache until the cookies expire.This feature is enabled by default.

Note: To disable this feature, under HKLM\SOFTWARE\SDTI\RSAWebAgent create a DWORD Value 'CopiedCookieProtectionSupported' and set its value to 0.

Enforce RSA SecurID Authentication using Auto-Redirect Scripts

The Web Agent includes auto-redirect scripts you can use to require users to authenticate before accessing a URL that is not protected by RSA SecurID. The URL does not have to be hosted on the same server or be within the same domain as the server on which the Web Agent is installed.

You use the customized redirect URL from the script as the hyperlink to the unprotected site. When a user clicks the HTML link to the URL that you want to protect, the script is invoked, and the user is forced to authenticate before gaining access to the site.

The ASP and Perl scripts included with the Web Agent are sample scripts only. To use them, you must first customize them with your own code.

To customize an auto-redirect script:

1. Copy either the ASP sample script (**AspScriptRedirect.asp**) or the Perl sample script (**PerlScriptRedirect.pl**) from the **/CGI_Scripts** directory of your Web Agent installation, and store it in the web server scripts directory (usually **/inetpub/scripts**).
2. Customize the script with your own code.

   Important: RSA recommends that your script contain a list of URLs that users are allowed to access using the redirect URL. Compare the script's input argument to the list of allowed URLs before any redirect takes place. Any user who attempts to access the redirect hyperlink can see the link definition and can potentially use the redirect script to access the authentication cookie. By implementing a URL comparison list, you minimize the security risk.

3. Use the customized redirect URL from the script as the hyperlink to the unprotected site.

   An example redirect URL looks like this:

   ```
   http://
   protectedHostname/WebID/IISWebAgentIF.dll?referrer=/Scripts/
   AspScriptRedirect.asp?target=http://
   unprotectedHostname/new_application.jsp
   ```

   In this example:

   - **/WebID/IISWebAgentIF.dll/** is the virtual Web Agent reference. It ensures that a user attempting to access the unprotected URL is prompted to authenticate.
   - **/Scripts/AspScriptRedirect.asp** is the script that performs the redirect to the input argument.
   - **http:// *unprotectedHostname*/new_application.jsp** is the input argument, or unprotected URL.

   For more information about customizing auto-redirect scripts, see the instructions included in each script.

Protect the Site, Application, Files, or Folders

To protect the entire Site:

Note: These steps are applicable to protect any web site (including SharePoint sites) with RSA SecurID.

1. On the IIS Server Machine, click **Start > Settings > Control Panel > RSA Web Agent**.
2. In the Connections pane, double-click <*server_name*>, and click **Sites > WebSite**, where *server_name* is the name of the IIS Server Machine and WebSite is the name of the web site to be protected.
3. In the Site Home pane, double-click **RSA SecurID**.
4. In the RSA SecurID pane, select E**nable RSA SecurID Web Access Authentication** and **Protect This Resource with RSA SecurID**.
5. In the Actions pane, click **Apply**.
6. Refresh IIS Manager Connections pane, click <*server_name*>, and click **Sites > WebSite > WebID**.
7. In the WebID Home pane, double-click **Authentication**.
8. In the Authentication pane, select **Anonymous Authentication**, and click **Enable** in the Actions pane.
9. Restart the IIS Web Server.

Note: To protect Outlook Web Access see "Protect Outlook Web Access Application" on page 55. To protect the ActiveSync application, see "Protect the ActiveSync Application" on page 56.

To protect only certain files, folders, or application under the site:

1. On the IIS Server Machine, click **Start > Settings > Control Panel > RSA Web Agent**.
2. In the Connections pane, double-click <*server_name*>, and click **Sites > WebSite**, where *server_name* is the name of the IIS Server Machine and WebSite is the name of the site to be protected.
3. In Site Home pane, double-click **RSA SecurID**.
4. In the RSA SecurID pane, select **Enable RSA SecurID Web Access Authentication**.
5. In the Actions pane, click **Apply**.
6. In the Connections pane, double-click <*server_name*>, and click **Sites > WebSite**, and then select the resource (file, folder or application) to be protected.
7. In the Resource home pane, double-click **RSA SecurID**.
8. In the RSA SecurID pane, select **Protect This Resource with RSA SecurID**.

9. In the Actions pane, click **Apply**.
10. Refresh the IIS Manager Connection pane, click <*server_name*>, and click **Sites > WebSite > WebID**.
11. In the WebID Home pane, double-click **Authentication**.
12. In the Authentication pane, select **Anonymous Authentication**, and click **Enable** in the Actions pane.
13. Restart the IIS Web Server.

The user will now be prompted for SecurID Authentication, while accessing the protected resource.

Note: If the administrator wants to change the Applications Pool Identity settings for the Protected Site or for the WebID application see "Web Agent Protection and Application Pool Identity Settings" on page 60.

Protect Outlook Web Access Application

Perform the following steps to protect Outlook Web Access (OWA) with WebAgent:

1. "Protect Outlook Web Access."
2. "Verify Authentication and Application pool settings for WebID Application."

Note: For information on configuring the Web Agent for single sign-on (SSO) to Outlook Web Access, see Chapter 6, "Configuring the Web Agent for Single Sign-On to Outlook Web Access."

Protect Outlook Web Access

To protect Outlook Web Access:

1. On the Microsoft Exchange Server, click **Start > Settings > Control Panel > RSA Web Agent**.
2. In the Connections pane, double-click ***<server_name>***, and click **Sites > Default Web Site**, where *server_name* is the name of the IIS Server Machine and WebSite is the name of the site to be protected.
3. In the Site Home pane, double-click **RSA SecurID**.
4. In the RSA SecurID pane, select **Enable RSA SecurID Web Access Authentication**.
5. In the Actions pane, click **Apply**.
6. In the Connections pane, double-click ***<server_name>***, and click **Sites > Default Web Site > owa**
7. In the owa Home pane, double-click **RSA SecurID**.

8. In the RSA SecurID pane, select **Protect This Resource with RSA SecurID**.
9. In the Actions pane, click **Apply**.

Note: The Exchange Management Console will not be able to authenticate to Powershell, if SecurID protection is enabled on the Powershell virtual directory under the Default Web Site.

Verify Authentication and Application pool settings for WebID Application

To verify the authentication and application pool settings for the WebID Application

1. Refresh the IIS Manager, click **<*server_name*>**, and click **Sites > Default Web Site > WebID**.
2. In the WebID Home pane, double-click **Authentication**.
3. In the Authentication pane, select **Anonymous Authentication**, and click **Enable** in the Actions pane.
4. In the Connections pane, double-click **<*server_name*>**, and then click **Sites > Default Web Site > WebID**.
5. Right click **WebID** and select **Manage Application > Advanced Settings**.
6. Select the Application pool as **RSA SecurID Pool**.

Note: Enabling SecurID protection in the OWA virtual directory does not protect the Calendar operations. To protect OWA Calendar or Appointments, the administrator has to enable SecurID protection in the /ecp virtual directory under the Default Web Site.

Protect the ActiveSync Application

Perform the following steps to protect the ActiveSync application:

1. "Protect the ActiveSync Application."
2. "Verify Authentication and Application pool settings for WebID Application."
3. "Customize the HTTP Response Header for Devices (ActiveSync Only)."

Protect the ActiveSync Application

To protect the ActiveSync application:

1. On the Microsoft Exchange Server machine, click **Start** > **Settings** > **Control Panel** > **RSA Web Agent**.
2. In the Connections pane, double-click ***server_name***, and click **Sites** > **Default Web Site**

   where *server_name* is the name of the Microsoft Exchange Server and WebSite is the name of the site to be protected.

3. In the Site Home pane, double-click **RSA SecurID**.
4. In the RSA SecurID pane, select **Enable RSA SecurID Web Access Authentication**.
5. In the Action pane, click **Apply**.
6. In the Connections pane, double-click ***server_name***, and click **Sites > Default Web Site >Microsoft-Server-ActiveSync**
7. In the Microsoft-Server- ActiveSync Home pane, double-click **RSA SecurID**.
8. In the RSA SecurID pane, select **Protect This Resource with RSA SecurID**.
9. In the Actions pane, click **Apply**.

Note: Before synchronising the ActiveSync device and the server, ensure that the time on the device and the server are in sync.

Verify Authentication and Application pool settings for WebID Application

To verify the authentication and application pool settings for the WebID Application

1. Refresh the IIS Manager, click **<*server_name*>**, and click **Sites > Default Web Site > WebID**.
2. In the WebID Home pane, double-click **Authentication**.
3. In the Authentication pane, select **Anonymous Authentication**, and click **Enable** in the Actions pane.
4. In the Connections pane, double-click **<*server_name*>**, and then click **Sites > Default Web Site > WebID**.
5. Right click **WebID** and select **Manage Application > Advanced Settings**.
6. Select the Application pool as **RSA SecurID Pool**.

Customize the HTTP Response Header for Devices (ActiveSync Only)

By customizing the HTTP Response Header, you give the ActiveSync client on the Microsoft Windows Mobile device the capability to distinguish between RSA SecurID authentication and Exchange ActiveSync responses.

To customize the HTTP response header:

1. From the IIS Manager on the server on which you installed the Web Agent, enable RSA web access protection on the default web site. For instructions, see the Help topic “Enabling Web Access Authentication.”
2. In the IIS Manager Connections pane, double-click ***server_name***, and click **Sites** > **Default Web Site** > **WebID**.
3. In the WebID Home pane, double-click **HTTP Response Headers**.

4. In the Actions pane, click **Add** to add the following headers in the Add Custom HTTP Response Headers dialog box:
   - **Name**: MSAS-TwoFactorAuth
     Value: True
   - **Name**: MS-ASProtocolVersions
     Value: 1.0,2.0,2.1,2.5, 12.0, 12.1, 14.0
   - **Name**: MS-ASProtocolCommands
     Value:Sync,SendMail,SmartForward,SmartReply,GetAttachment, GetHierarchy,CreateCollection,DeleteCollection,MoveCollection, FolderSync,FolderCreate,FolderDelete,FolderUpdate,MoveItems, GetItemEstimate,MeetingResponse,ResolveRecipients,ValidateCert, Provision,Search,Notify,Ping
5. Click **OK**.

Enable Single Sign-On a Protected Site

You can enable Single Sign-On to any site protected by SecurID, provided the site supports Windows Authentication. When the Single Sign-on is enabled on the protected site, the user will be prompted for only SecurID credentials and not Windows credentials to logon, to the site.

Prerequisites

- Windows 2008 Server running at the Windows 2008 or Windows 2008R2 functional level on the environment domain controller.
- The site should be disabled for Anonymous authentication.
- The site should be enabled for Windows authentication, where the credentials the user enters should be validated by the Domain Controller.
- The site should be protected by SecurID, and when the user attempts to access the site should be challenged by both RSA SecurID and Windows credentials.
- Unique user names across all domains.
  In addition, user names in the Active Directory Server must match the user names in the RSA Authentication Manager database.
- Using Active Directory, assign the right to delegate services:
  - On the domain controller, click **Start > Programs > Administrative Tools > Active Directory Users and Computers**.
  - In the left pane, double-click ***domain name***.
  - Double-click **Computers**, and in the right pane, double-click < ***server name***>.
  - In the Delegation tab, select **Trust this computer for delegation to any service (Kerberos only)**, and click **OK**.

Enable Single Sign-On

Perform the below steps to enable Single Sign-On:

1. Protect the site. For more information see "Protect the Site, Application, Files, or Folders" on page 54.
2. Select **System32 > inetsrv > config > applicationHost.config**.
3. Search for the SecurIDModule in the file and add an entry for SecurIDSSOModule under that in the format:
<add name="SecurIDSSOModule" image="PATH_TO_ RSASinglesignon.dll"/>,

   Note: RSASinglesignon.dll can be found inside the WebAgent installation directory.

4. In the Connections pane of the IIS Manager, double-click <***server_name***>, and click **Sites > < *Site_name*>**
where *Site_name* is the site to be enabled for Single Sign-On,
5. In the *Site_name* Home pane, double-click **Modules**.
6. In the Actions pane, click **Configure Native Modules** and add the SecurIDSSOModule.
7. In the Connections pane of IIS Manager, double-click ***server_name***, and click **Sites > Site>WebID**.
8. In the WebID Home pane, double-click **Modules**.
9. In the Actions pane, select the SecurIDSSOModule, and click **Remove**.

Verify Application Pool identity Settings for the Site

To verify Application pool identity settings for the site:

1. Access the InetMgr in the WebAgent machine. In the Connection Pane, click **Server Name > Application Pool**.
2. Click the website's application pool and in the Actions pane, click **Advanced Settings**.
3. Under the Process Model, click the **Identity field** to open the Application Pool Identity dialog box.
4. Click **Built-In account** and select **LocalSystem**.
5. Click **OK** to apply the changes.

Phantom Entries

Phantom Entries are the directory or file paths that have been marked as protected or unprotected in the configuration, but they no longer exist in the system.

It is advisable to remove any phantom entries in applicatioHost.config before protecting a site.The phantom entries can be identified by running the ConfigUpdateHelper.exe command line utility available in the Installation directory.

To run the ConfigUpdateHelper utility

1. From the Windows desktop click **Start > Run**.
2. Enter **cmd** to run the command line utility.
3. At the command prompt, enter **cd** <*WebAgent Installation Directory*>.
4. In the WebAgent installation directory, enter **ConfigUpdateHelper.exe pe**.
   A dialog box displays the phantom entries in applicationHost.config.
5. Click **Ok** to close the message box.

Note: The Task scheduler can be configured to run this utility periodically

Web Agent Protection and Application Pool Identity Settings

It is important to configure the protected web site application pool identity correctly to ensure that the WebAgent functions properly. When WebAgent protection is enabled on a web site, an application with the name **WebID** is created under the web site, which serves the WebAgent's login page.

The WebID's default application pool will be the **RSA SecurID** pool which runs under the **LocalSystem** identity. The administrator can change it to any other domain user account, if required.

The web site Application Pool identity settings required for the WebAgent to function correctly are described in the table below:

Site	Protected site's Application Pool Identity
OWA with SSO	LocalSystem
OWA without SSO	LocalSystem
SharePoint with SSO	LocalSystem
SharePoint Server 2013 with SSO	Network Service

Site	Protected site's Application Pool Identity
SharePoint without SSO	Domain Administrator or LocalSystem,
Other web sites	LocalSystem or Domain Administrator or Domain User or Network Service

To change the Application Pool Identity:

1. Access the InetMgr in the WebAgent machine. In the Connection Pane, click **Server Name > Application Pool**.
2. Click the website's application pool and in the Actions pane, click **Advanced Settings**.
3. Under Process Model, click the **Identity** field to change the identity to the required account.

To run the web Application Pool as a Network Service:

1. Grant Read permission to the following registry entries for the Network Service:
   - **HKLM\System\CurrentControlSet\Services\WinSock2\Parameters**
   - **HKLM\SOFTWARE\SDTI\RSAWebAgent**
   - **HKLM\SOFTWARE\SDTI\ACECLIENT**
2. Grant Read and Execute, List folder contents, and Read permissions to the directory:
   \Program Files\RSA Security\RSAWebAgent
3. Grant Read and Execute, and Read permissions to the file:
   \Program Files\RSA Security\RSAWebAgent\securid
4. Grant Read and Execute, and Read permissions to the file:
   \Program Files\RSA Security\RSAWebAgent\sdstatus.12

Note: WebAgent accesses some registry entries. The permissions for the WebAgent registry entries and WebAgent configuration files are restricted to SYSTEM and Domain Administrator. So if the application pool is configured to any identity other than SYSTEM and Domain Administrator, that particular account should be explicitly given permission to read the registry settings and configuration files.

To change registry access permissions:

1. Access **HKLM\SOFTWARE\SDTI**. Right-click **RSAWebAgent**, and select **Permissions**, and add the required account in the **Group** or **User names** text area and assign read permissions.
2. Access **HKLM\SOFTWARE\SDTI.** Right-click **ACECLIENT**, and select **Permissions**, and add the required account in the Group or User names text area and assign read permissions.
3. Access **C:\Program Files\RSA Security**. Right-click **RSAWebAgent** and select **Properties > Security Tab > Edit**, and add the required account in the Group or User names text area and assign read permissions.
4. Follow the steps below to assign permissions to read the node secret file:
   a. Access **C:\Program Files\RSA Security\ RSAWebAgent**.
   b. Right-click the securid file and select **Properties**. In the Security Tab, click **Edit** and add the required account in the Group or User names text area and assign read permissions.

Note: If the SecurID file is not present in **C:\Program Files\RSA Security\ RSAWebAgent**, it means that the node secret has not yet been created. Create a node secret by following the steps in, "Perform a Test Authentication" on page 23 and then perform step 4.

Support for Forms-Based Authentication in Microsoft Office

The Web Agent supports forms-based authentication in Microsoft Office 2007/ 2010. To support forms-based authentication in Microsoft Office 2007, the user should install Microsoft Office 2007 SP1 with the hot fix available at **http://support.microsoft.com/kb/960499**.

When you try to access a Microsoft Office document that is available on the Microsoft Office SharePoint Server, and the web access authentication cookie does not exist, Microsoft Office displays a browser-like window to display the SecurID authentication page to capture the SecurID credentials. You can view the document, after authentication is successful.

If you do not want the user to be prompted each time a document from the SharePoint Server is accessed through a Microsoft Office 2007/2010 application, enable web access authentication persistent cookies. When the persistent cookie expires, you need to log on to the Microsoft SharePoint Server again with your SecurID credentials to view the document. To avoid this problem, you can choose to use long-term persistent cookies that have a time-out value from 30 minutes to 1 hour or more.

In the case of Microsoft Office 2007/2010, you can set a small time-out value for the persistent cookie, such as 20-30 seconds. This option is more secure compared to using long-term persistent cookies to access Microsoft Office 2007/2010 documents from the SharePoint Server. For more information, see "Configure Short-Term Persistent Cookies for Microsoft Office" on page 99.

Web Agent Logging

You can use the logging or tracing option to troubleshoot WebAgent problems. To enable logging, you must select one or more tracing level settings and one or more tracing destinations.

To enable WebAgent logging in Windows:

1. On the agent machine click, **Start > Settings > Control Panel > RSA Authentication Agent**.
2. In the RSA Authentication Agent GUI, click the **Advanced** tab.
3. In the Tracing section, select one or more of the tracing levels as explained below.

Value	Description
Regular Messages	Logs regular messages
Function Entry Points	Logs function entry points
Function Exit Points	Logs function exit points
Flow Control Statements	All logic flow controls use this (ifs)

4. In the Tracing section, select one or more of the tracing destinations as explained below.

Location	Description
Event Logger	Logs are sent to the event log
Console	Logs are sent to the console
Log File	Logs are saved in log files
Debugger	Logs are saved as debugger output

5. By default the log files are created in %WINDIR% directory with the name ACECLIENT.LOG.

Note: To change the default location, create a string value TraceFile under HKLM\SOFTWARE\SDTI\ACECLIENT and provide the log file location. For example, to change it to C:\logs folder, specify **TraceFile = C:\LOGS\ACECLIENT.LOG**.

6. After the changing the location of the log file, follow the steps below to apply the changes:
   a. Restart the **RSA Pipe Service**.
   b. Restart the **RSA Config Service**.
   c. Restart the **w3wp** using iisreset.
   d. Close and re-open the **IIS Manager**.

5 Customizing Templates and Message Strings

Customized Templates

When users authenticate successfully to the Web Agent using a standard browser, the system returns a message informing them about the success of the authentication attempt through an HTML page. For wireless device micro browsers, the system returns messages in WML format.

The Web Agent provides default versions of HTML and WML templates and messages that you can customize to reflect your company's image and administrative needs. You can:

- Add a custom greeting message.
- Add your own custom graphics.
- Change standard buttons to custom graphics.
- Display web access authentication prompts in a language other than English.
- Customize the web access authentication messages.

The WebAgent templates can be classified into HTML templates and WML templates.

- **HTML Templates**
  - **Manual Authentication templates**: These templates are displayed when a user accesses the protected page from a client machine which does not have a RSA SecurID Software Token installed in it. The user has to manually enter the username and passcode.
  - **WebID Plugin templates**: These templates provide compatibility with the RSA SecurID Software Token for Windows WebID components. These components integrate the RSA SecurID software token application with Internet Explorer and Mozilla Firefox on Windows. When users navigate to a site that is protected by the RSA Authentication Agent for Web, the Web ID authentication page is displayed, which allows them to select their software token and authenticate with their user name and pin. They do not have to enter their user name and passcode, as is required in the manual authentication page.

  - **Forms Based Authentication templates**: These templates are displayed when a user tries to access a protected Microsoft Office document from a protected Sharepoint site. The user will be shown a Pop-Up like browser window to collect the credentials if cookie is not shared between the browser and Microsoft office.
  - **Modal Popup templates**: These templates are displayed after cookie expiry. The user will be shown a small popup to collect the passcode alone, which will refresh the cookie after validation.
- **WML templates**: If the user accesses the protected resource using wireless device micro browsers, the system returns the authentication pages in WML format.

Default Templates

The following table describes the default templates.

Note: If you are using RSA SecurID PIN Pads instead of tokens, you need to change the **passcode** and **useridandpasscode** templates to display the correct message to your users. The correct message to display is included in the templates in a comment section.

Template	Description
Errors	
error.htm **error.wml**	The page that RSA SecurID users see when a fatal error occurs during authentication. The **@@sub** macro in the template substitutes the error message passed from the system or from the **strings.txt** file.
forbidden.htm **forbidden.wml**	The page that RSA SecurID users see in response to requesting a forbidden URL.
Authentication Templates	
newpin.htm **newpin.wml**	The New PIN page is displayed when users are in the new pin mode or are authenticating with their token for the first time. From this page, users create their own PINs. This then loads either the WebID NewPin page (newpinplugin.htm) or the manual authentication page (newpinmanual.htm)
newpinplugin.htm	This page is displayed if the user's computer has the Software Token WebID plug-in installed. The user enters the PIN to authenticate.
newpinmanual.htm	This page is displayed if the user's computer does not have the Software Token WebID plug-in installed. The user enters passcode.

Template	Description
newpin_fba.htm	This page is displayed when the user is in NewPin mode and during Forms Based Authentication, which happens when user opens a Microsoft Office Document from a Sharepoint Site.
newpin1.htm **newpin1.wml**	This is the landing page to receive a system-generated PIN, which then loads either the WebID page (newpin1plugin.htm) or the manual authentication page (newpin1manual.htm). This functionality is determined in Authentication Manager.
newpin1plugin.htm	This page is if the user's computer has the Software Token WebID plug-in installed.
newpin1manual.htm	This page is displayed if the user's computer does not have the Software Token WebID plug-in installed.
newpin1_fba.htm	This page is displayed to display system-generated new pin and during Forms Based Authentication, which happens when user opens a Microsoft Office Document from a Sharepoint Site.
newpin2.htm **newpin2.wml**	The New PIN page is displayed when a user is given the choice of whether to create a PIN or receive a system-generated PIN. This page then loads either the WebID page (newpin2plugin.htm) or the manual authentication page (newpin2manual.htm). This functionality is determined in Authentication Manager.
newpin2plugin.htm	This page is displayed if the user's computer has the Software Token WebID plug-in installed.
newpin2manual.htm	This page is displayed if the user's computer does not have the Software Token WebID plug-in installed.
newpin2_fba.htm	This page is displayed during Forms Based Authentication, which happens when user opens a Microsoft Office Document from a Sharepoint Site.
nextprn.htm **nextprn.wml**	The page is displayed when a token is in Next Tokencode mode. This happens when a user enters a series of incorrect passcodes during authentication. After the user finally enters a correct tokencode, the user is prompted for another correct tokencode before being allowed access. This then loads either the WebID page (nextprnplugin.htm) or the manual authentication page (nextprnmanual.htm).
nextprnplugin.htm	This page is loaded if the user's computer has the Software Token WebID plug-in installed.
nextprnmanual.htm	This page is loaded if the user's computer does not have the Software Token WebID plug-in installed.

Template	Description
nextprn_fba.htm	This page is displayed during 'Forms Based Authentication', which happens when user opens a Microsoft Office Document from a Sharepoint Site.
sslredir.htm **sslredir.wml** **sslredir-post.htm**	The page users might see momentarily with some browsers when they must use a secure channel to access protected pages. In some cases, users must click a link on the **sslredir** or **sslredir-post.htm** page to continue.
redirect.htm **/redirect-get.htm** **redirect.wml**	The page is displayed when users complete the authorization process or when they log off. **Note:** If you customize **redirect.htm**, you must customize **redirect-get.htm** to look the same.
redirectmanual.wml	This page is displayed to cell phone users when the cell phone does not support automatic redirection to a protected URL. The user is provided with a list of secure URLs and must manually choose one.
cancel.htm/cancel-get.htm **cancel.wml**	The page is displayed to users when they cancel the authorization process. **Note:** If you customize **cancel.htm**, you must customize **cancel-get.htm** to look the same.
showsys.htm **showsys.wml**	The page is displayed to users for ten seconds while the system generates an RSA SecurID PIN for them.
showsys_fba	This page displays the system generated pin during Forms Based Authentication which happens when Microsoft Office Document is opened from a Sharepoint site.
multidom.htm/ **multidom-get.htm** **multidom.wml**	The page is displayed when users are authenticating across multiple domains. **Note:** If you customize **multidom.htm**, you must customize **multidom-get.htm** to look the same.
userid.htm **userid.wml**	If you chose to present separate web pages to users to input the user name and passcode, this template is used for the user name. If you did not choose to present separate pages, the **useridandpasscode** template is used. This page then loads either the WebID authentication page (useridplugin.htm) or the manual authentication page (useridmanual.htm)

Template	Description
useridplugin.htm	This page is loaded if the user's computer has the Software Token WebID plug-in installed. The user enters the PIN to authenticate.
useridmanual.htm	This page is loaded if the user's computer does not have the Software Token WebID plug-in installed. The user enters passcode.
userid_fba.htm	This page is loaded for authentication and during 'Forms Based Authentication', which happens when user opens a Microsoft Office Document from a Sharepoint Site.
passcode.htm **passcode.wml**	If you chose to present separate web pages to users to input the user name and passcode, this template is used for the passcode. If you did not choose to present separate pages, the **useridandpasscode** template is used. This then loads either the WebID authentication page (passcodeplugin.htm) or the manual authentication page (passcodemanual.htm).
passcodeplugin.htm	This page is loaded if the user's computer has the Software Token WebID plug-in installed. The user enters the PIN to authenticate.
passcodemanual.htm	This page is loaded if the user's computer does not have the Software Token WebID plug-in installed. The user enters passcode.
passcode_fba.htm	This page is loaded to collect passcode during 'Forms Based Authentication', which happens when user opens a Microsoft Office Document from a Sharepoint Site.
useridandpasscode.htm **useridandpasscode.wml**	If you chose to present one web page to users to input both the user name and passcode, this template is used. If you chose to present separate web pages to input the user name and passcode, the userid and passcode templates are used. This then loads either the WebID authentication page (useridandpasscodeplugin.htm) or the manual authentication page (useridandpasscodemanual.htm).
useridandpasscodeplugin.htm	This page is loaded if the user's computer has the Software Token WebID plug-in installed. The user enters the PIN to authenticate.
useridandpasscodemanual.htm	This page is loaded if the user's computer does not have the Software Token WebID plug-in installed. The user enters passcode.
useridandpasscode_fba.htm	This page is loaded for authentication and during 'Forms Based Authentication', which happens when user opens a Microsoft Office Document from a Sharepoint Site.

The HTML and WML templates use the following files, which are also installed in the **/templates** directory.

Template	Description
Bitmaps	
modalContent.html	This page displays a modal popup after cookie expiry if the application pool of the protected site is configured in Integrated mode.
maskBG.png	This is the background mask for modal popup.
denied.jpg **denied.wbmp**	If you have configured the Web Agent to allow multiple domain authentications, the word “Denied” displays if a user’s authentication request to a virtual web server does not succeed.
ok.jpg **ok.wbmp**	If you have configured the Web Agent to allow multiple domain authentications, the word “OK” displays if a user’s authentication request to a virtual web server succeeds.
rsalogo.jpg	This is the background graphic used on the authentication pages.
securid_banner.jpg	This graphic displays the RSA SecurID banner on the authentication pages.
Other Files	
strings.txt	This file contains text strings that display various messages while users interact with the web access authentication prompt pages.
style.css	The cascading style sheet used for the web pages.

Templates Management

The following sections list the general guidelines for customizing templates and describe the procedure to customize the text, images, and buttons used in the default templates.

Guidelines for Using Templates

To ensure that the templates function properly after you have made changes, follow these guidelines:

- Copy the templates into a new directory before making changes to them.
- Use a text editor to make changes.

  HTML editors add unnecessary additional HTML/WML tags to templates and may alter the substitution strings that are necessary in the templates.
- After you have completed your changes, test the templates to make sure they are functioning properly. For information on utilities you can use to troubleshoot problems, see Chapter 8, "Troubleshooting."
- For security purposes, do not change the administrative privileges when customizing templates. Also, the web server may not be able to read the templates if you change the privileges.
- Do not alter any of the substitution strings in the templates or message text files (**webagent.msg** and **strings.txt**).

  Substitution strings are used to include error messages and text from the Authentication Manager and provide placeholders for graphics and message strings. These strings begin with two "at" signs (@@).

Modify Static Text

You can change the static text in the default templates, or you can add your own static text.

To modify the text in a default template:

1. Using a text editor, open one of the templates in the directory. The templates are listed in "Default Templates" on page 66.

   Important: When editing templates, avoid altering the contents of substitution strings.

2. Delete the static text you want to change, and add the new text.

   For example, the tag **<H1>Welcome to ABC, Inc.</H1>**, when placed in the **passcode.htm** or **passcode.wml** file, changes the text of the first heading in that page from "RSA SecurID Passcode Request" to "Welcome to ABC, Inc."
3. Save and close the file.

Add Custom Graphics

You can add one or more custom graphics to the default templates.

Note: WAP or WML devices usually have limited display space for graphics. Be sure the use of graphics is appropriate for your WAP devices before using them.

To add a custom graphic to a default template:

1. Using a text editor, open one of the templates in the directory. The templates are listed in "Default Templates" on page 66.
2. Decide where you want the image to be placed on the page, and insert the appropriate tag in the HTML or WML markup pointing to the image file. Use one of the following methods for naming graphic files:
   - A substitution macro (@@URL?GetPic?image=) works with HTML and WML. With HTML, the images must be JPG. With WML, the images must be WBMP. Substitution macros cannot have absolute paths. The images must be in the same directory as the templates, and you must omit the filename extension from the file specification. For example:

     ```
     <IMG src="@@URL?GetPic?image=logo" ALIGN="left">
     ```

   - You can use HTTP URLs instead of substitutions if the image files reside in an area of the server that is unprotected by RSA SecurID authentication, or on a separate server hosting the URL. HTTP URLs are always absolute. Relative URLs cannot be used in templates. The image types for HTTP URLs can be .jpg, .gif, or .wbmp. For example:

     ```
     <IMG src="http://server.domain.com/img/logo.jpg"
     ALIGN="left">
     ```

     Note: When using HTTP URLs, ensure the image file you point to in the **src** path is in a directory that is not protected by RSA SecurID and that you always specify a fully qualified path to the image file.
3. Save and close the file.
4. Stop and restart the web server for the changes to take effect.

   The web authentication prompt displays the new graphic.

Change the Buttons (HTML Only)

You can replace the standard **Send**, **Reset**, and **Cancel** buttons in the HTML templates with custom graphics.

Note: Make sure the image file you point to in the **src** path is in a directory that is not protected by RSA SecurID and that you always specify a fully qualified path to the image file.

To change the buttons in a default HTML template:

1. Using a text editor, open one of the HTML templates in the directory. The templates are listed in "Default Templates" on page 66.
2. Do one or all of the following:
   - To replace the **Send** button, replace the line that reads

     ```
     <INPUT TYPE=SUBMIT VALUE="Send">.
     ```

     with

     ```
     <A HREF="JavaScript:document.forms[0].submit()"><IMG
     SRC="path to your image" BORDER="0"></A>
     ```

     where ***path to your image*** is a fully qualified path to an image file.
   - To replace the **Reset** button, replace the line

     ```
     <INPUT TYPE=RESET VALUE="Reset">
     ```

     with

     ```
     <A HREF="JavaScript:document.forms[0].reset()"><IMG
     SRC="path to your image" BORDER="0"></A>
     ```

     where ***path to your image*** is a fully qualified path to an image file.
   - To replace the **Cancel** button, replace the line

     ```
     <INPUT TYPE=CANCEL VALUE="Cancel">
     ```

     with

     ```
     <A HREF="JavaScript:document.forms[0].cancel()"><IMG
     SRC="path to your image" BORDER="0"></A>
     ```

     where ***path to your image*** is a fully qualified path to an image file.
3. Save and close the file.
4. Stop and restart the web server for the changes to take effect.

Customize Templates for Another Language

To customize the templates for a language other than English:

1. Set the browser language preference to use the appropriate language code.

   The code must correspond to your language-customized template directory name. The new language preference must appear at the top of the web browser's list of language preferences.

   Note: If the preference settings are incorrect, language-customized templates do not exist, or the Web Agent cannot find the specified templates for a virtual web server, the browser displays the default English version of the templates.

2. Store the templates in a language-specific directory under the Web Agent **/templates** directory.

   The default directory for language-specific templates is */**Web_Agent_installation_directory**/**templates/nls/<*language_code*>* where *language_code* is the language preference code used by web browsers.

Note: To find the correct language code, see the language preferences list of codes in the Internet Explorer or Firefox web browser. For more information about using international character sets in HTML documents, consult an HTML reference book or go to **www.w3.org/pub/WWW/International**.

To translate HTML and WML template text for a non-English language:

1. Create a language-specific subdirectory in the **/templates** directory of the Web Agent.
2. Copy the templates to the directory you created in step 1.
3. Customize the text strings within the templates.

   Note: Do not remove the substitution macros. (These macros begin with @@.) The macros are replaced with actual values when the text is displayed.

4. Save and close the template file.

Note: The character encoding of the language being customized should be the same as the character set configured for the Web Agent. After editing the template files, you must save them using the same configured character encoding. Otherwise, the templates will not work properly in the Web Agent authentication pages. For more information, see "Pre-Installation Tasks" on page 18.

Customize Message Strings in Templates

You can customize certain messages that display while users interact with the web access authentication prompt pages that are produced from the templates. The message strings are contained in a file named **strings.txt** located in the **/*Web_Agent_installation_directory*/templates** directory.

For example, **strings.txt** contains passcode page errors such as:

```
[Messages]
; PASSCODE page errors and messages.
1="100: Access denied. The RSA Authentication Manager
rejected the PASSCODE you supplied. Please try again."
2="101: Access denied. Unexpected RSA Authentication
AgentError %d. Please try again."
3="102: You must enter a valid PASSCODE. Please try again."
```

Important: If you modify the message strings, make certain that you do not remove or alter the position of the variable strings (**@@SUB1**, **@@SUB2**, and so on) contained in the message text. The strings are replaced by actual values when the messages are displayed.

To customize the text displayed by the **multidom.htm** or **multidom.wml** template, search for the following section in the **strings.txt** file:

```
; multiple domain authentication string
; This is HTML only
22="<strong>Requesting authentication from server
@@SUB1</strong> <img alt=failed src="@@SUB2"><br>"
; This is for WML with image tag support
23="<strong>Server @@SUB1 <img alt="failed"
src="@@SUB2"/></strong><br/>"
```

Note: If you translate the text messages in **strings.txt** into a language other than English, you must store the translated file in the same language-specific directory where other translated templates are stored. For more information, see "Customize Templates for Another Language" on page 73.

The character encoding of the language being customized should be the same as the character set configured for the Web Agent. After editing the **strings.txt** file, you must save it using the same configured character encoding. Otherwise, the templates will not work properly in the Web Agent authentication pages. For more information, see "Specify the Character Set" on page 19.

6 Configuring the Web Agent for Single Sign-On to Outlook Web Access

With single sign-on (SSO), users authenticate only through RSA SecurID to access a web application that would otherwise also be protected by a Microsoft Windows logon.

This chapter describes how to configure the Web Agent for SSO to Outlook Web Access (OWA) using one of the following combinations:

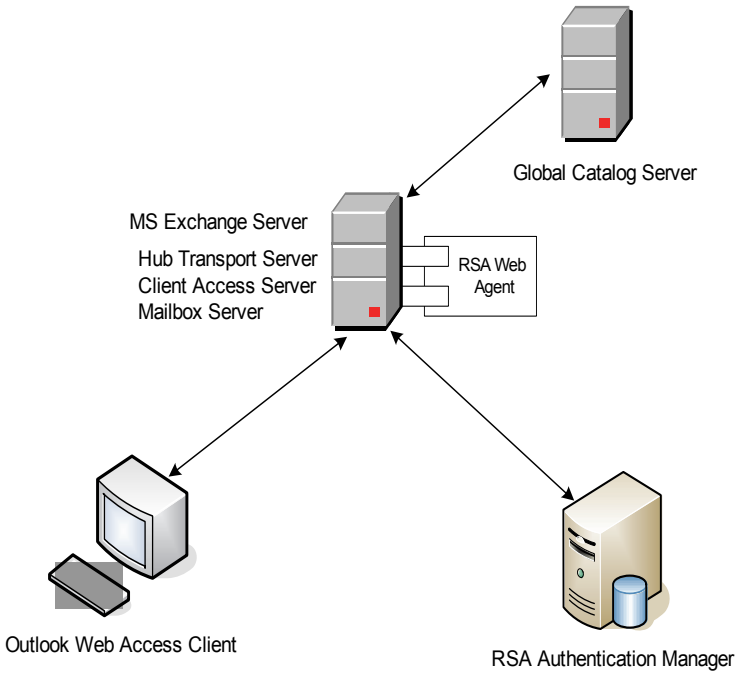
- Microsoft Exchange Server 2013 SP1 (with the latest patch) on the one of the following platforms:
  - Windows Server 2008 R2 SP1 (64-bit) platform with Internet Information Services (IIS) 7.5.
  - Windows Server 2012 (64-bit) platform with Internet Information Services (IIS) 8.0.
- Microsoft Exchange Server 2010 SP3 (with the latest patch applied) on the Windows Server 2008 R2 SP1 (64-bit) platform with Internet Information Services (IIS) 7.5.
- Microsoft Exchange Server 2007 SP2 or 2010 SP1 on the Windows Server 2008 SP2 or Windows 2008 R2 platform with Internet Information Services (IIS) 7.0 or 7.5.

Note: For Microsoft Exchange Server 2010 only, do not apply RSA SecurID protection to the EWS of the Exchange Back End. Protecting the EWS prevents emails from being deleted.

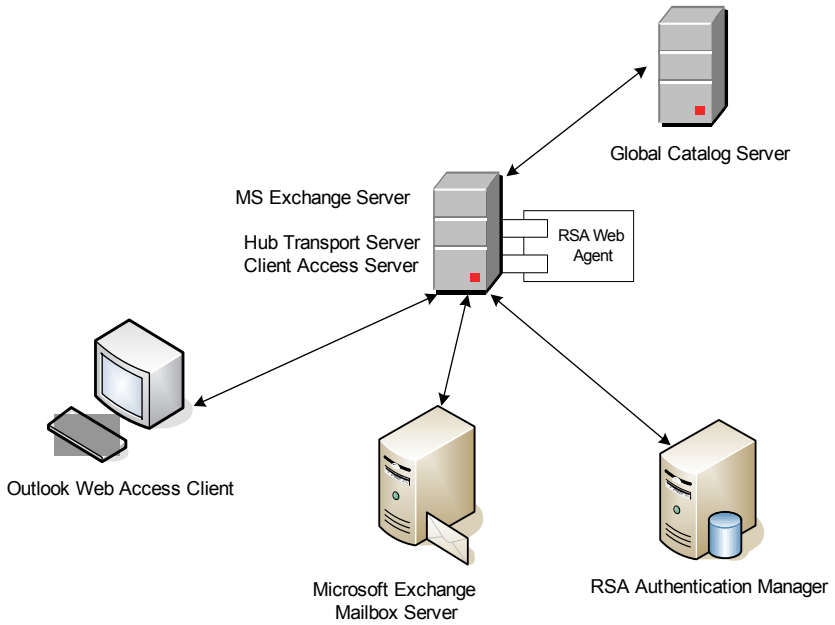
Set Up a Supported Configuration

The Web Agent supports both a simple configuration and a standard configuration.

The following figure shows a simple configuration.



The following figure shows a standard configuration in which the Microsoft Exchange Mailbox Server is deployed on a separate machine.



Prepare to Set Up SSO Access

Make sure you have the following:

- Install Microsoft Exchange Server on one of the following supported platforms:
  - Microsoft Exchange Server 2013 SP1 (with the latest patch) on the Windows Server 2008 R2 SP1 (64-bit) platform with Internet Information Services (IIS) 7.5.
  - Microsoft Exchange Server 2013 SP1 (with the latest patch) on Windows Server 2012 (64-bit) platform with Internet Information Services (IIS) 8.0.
  - Microsoft Exchange Server 2010 SP3 (with the latest patch applied) on the Windows Server 2008 R2 SP1 (64-bit) platform with Internet Information Services (IIS) 7.5.
  - Microsoft Exchange Server 2007 SP2 or 2010 SP1 on the Windows Server 2008 SP2 or Windows 2008 R2 platform with Internet Information Services (IIS) 7.0 or 7.5.
- Microsoft Exchange Server 2013 SP1, 2010 SP3, or 2007 SP2 installed with the following roles:
  - Hub transport server
  - Client access server
  - (Simple Configuration Only) Mailbox server

  For instructions on configuring the Microsoft Exchange Server, see the Microsoft Exchange Server 2013 SP1, 2010, or 2007 documentation.
- (Standard Configuration Only) Microsoft Exchange Server 2013 SP1, 2010 SP3, or 2007 installed on a separate supported Windows Server with the Mailbox Server role.
- Windows Server 2008 R2 (64-bit) or Windows Server 2012 (64-bit) on the environment domain controller.
- Unique user names across all domains.

  In addition, user names in the Active Directory Server must match the user names in the RSA Authentication Manager database.
- (Simple Configuration Only) RSA Authentication Agent for Web installed on the Microsoft Exchange Server and configured for web site protection with default options.
- (Standard Configuration Only) RSA Authentication Agent for Web installed on Microsoft Exchange Server with a Client Access Server role and configured for web site protection with default options.
- At least one domain user with a mailbox on the Microsoft Exchange Server.

Before setting up SSO access:

- Attempt to access your OWA mailbox to verify that your Web Agent setup is correct. When you attempt to access your OWA mailbox, you should be challenged by both RSA SecurID and OWA.

- In Active Directory on the domain controller, create a domain-level user account. You will use this account later for setting up anonymous access.

Next Steps:

Follow the procedure for your version of Microsoft Exchange Server:

- "Configure the Web Agent for SSO for Microsoft Exchange Server 2013 SP1" on page 80
- "Configure the Web Agent for SSO for Microsoft Exchange Server 2010 SP3" on page 84
- "Configure the Web Agent for SSO for Microsoft Exchange Server 2007 SP2" on page 88

Configure the Web Agent for SSO for Microsoft Exchange Server 2013 SP1

After you have met the prerequisites described in "Prepare to Set Up SSO Access" on page 79, follow these steps in order:

1. Configure Outlook Web App (OWA) and WebID for Anonymous Access in Microsoft Exchange Server 2013
2. Enable Single Sign-On in Microsoft Exchange Server 2013
3. Verify Application Pool Settings in Microsoft Exchange Server 2013
4. Test the Configuration for Single Sign-on with Microsoft Exchange Server 2013

Configure Outlook Web App (OWA) and WebID for Anonymous Access in Microsoft Exchange Server 2013

To configure the OWA for anonymous access:

1. On the Microsoft Exchange Server, click **Start > Settings > Control Panel > RSA Web Agent**.
2. In the Connections pane of the IIS Manager, double-click ***server_name***, and then click **Sites > Default Web Site**, where *server_name* is the name of the Microsoft Exchange Server.
3. In the Default web site home page, double-click **RSA SecurID**. In the RSA SecurID pane, select **Enable RSA SecurID Web Access Authentication** and click **Apply** on the Actions pane.
4. In the Connections pane of the IIS Manager, double-click ***server_name***, and then click **Sites > Default Web Site > OWA** where *server_name* is the name of the Microsoft Exchange Server.
5. In the OWA home pane, double-click **Authentication**, and perform the following tasks:

a. In the Authentication pane, select A**nonymous Authentication**, and click **Enable** in the Actions pane. Similarly, select **Windows Authentication**, and click **Enable** in the Actions pane.

b. In the Authentication pane, select **Anonymous Authentication**, and then click **Edit** in the Actions pane.

c. In the Edit Anonymous Authentication Credentials dialog box, click **Set** to set the user identity to the specific domain-level user account you created in "Prepare to Set Up SSO Access" on page 79.

d. Click **OK**.

To configure the WebID application for anonymous access:

1. In the Connections pane of the IIS Manager, double-click ***server_name***, and then click **Sites > Default Web Site > WebID**, where *server_name* is the name of the Microsoft Exchange Server.
2. In the WebID home pane, double-click **Authentication**, and select **Anonymous Authentication**, in the Authentication pane.
3. Click **Enable** in the Actions pane.
4. Restart the IIS Web Server.

Next Step

"Enable Single Sign-On in Microsoft Exchange Server 2013."

Enable Single Sign-On in Microsoft Exchange Server 2013

Perform the following steps to enable single sign-on in Microsoft Exchange Server 2013.

To enable single sign-on in Exchange Server 2013:

1. On the Microsoft Exchange Server, open the Microsoft Exchange Administration Center (EAC).
2. On the left pane, click **Servers**.
3. Click **Virtual Directories**.
4. Click OWA, and edit server properties.
5. Click **Authentication**.
6. Select **Use one or more standard authentication methods**.
7. Select **Integrated Windows authentication**.
8. Click **Save**.
9. A warning message states that you must run the IISReset command for the changes to take effect. Click **OK**.
10. On the Microsoft Exchange Server, open the Internet Information Services (IIS) Manager. Click **Start > Settings > Control Panel > RSA Web Agent**.

11. Select **Target This Resource for Single Sign-On** for the ecp website. Do the following:
    a. In the Connections pane of the IIS Manager, double-click ***server_name***, and click **Sites > Default Web Site > ecp**
       where *server_name* is the name of the Microsoft Exchange Server.
    b. In the ecp Home pane, double-click **RSA SecurID**.
    c. In the RSA SecurID pane, select **Target This Resource for Single Sign-On**.
    d. In the Actions pane, click **Apply**.
12. Select **Target This Resource for Single Sign-On** for the owa website. Do the following:
    a. In the Connections pane of the IIS Manager, double-click ***server_name***, and click **Sites > Default Web Site > owa**
       where *server_name* is the name of the Microsoft Exchange Server.
    b. In the owa Home pane, double-click **RSA SecurID**.
    c. In the RSA SecurID pane, select **Target This Resource for Single Sign-On**.
    d. In the Actions pane, click **Apply**.
       If you have a custom application pool, an RSA Authentication Agent Properties dialog box states that you must change the application pool to "RSA SecurID Pool."
13. Restart IIS. Do the following:
    a. On the IIS server, click **Start > Run**.
    b. Type **IISReset**, and click **OK**.
       The Command Prompt window displays the IISReset command status.
    c. Verify that IIS stops and restarts.

Next Step

"Verify Application Pool Settings in Microsoft Exchange Server 2013."

Verify Application Pool Settings in Microsoft Exchange Server 2013

To verify Application Pool settings:

1. In the Connections pane of the IIS Manager, double-click ***server_name***, and then click **Sites > Default Web Site > OWA**.
2. Right click OWA and select **Manage Application > Advanced Settings**.
3. Select the Application pool as **MSExchangeOWAAppPool**.
4. In the **Connections** pane, double-click ***server_name***, and then click **Sites > Default Web Site > WebID**.
5. Right click **WebID** and select **Manage Application > Advanced Settings**.
6. Select the Application pool as **RSA SecurID Pool**.

Note: By default, the RSA SecurID pool is in the LocalSystem identity. Perform the optional steps 7–9 to change the identity.

7. (Optional) In the **Connections** pane, double-click ***server_name***, and then click **Application Pools**.
8. (Optional) Click **RSA SecurID Pool > Advanced Settings**.
9. (Optional) Click **Identity > Application Pool Identity > Custom Account**. Specify the administrator account privileges here.
10. Verify that the ecp website is protected by RSA SecurID. Do the following:
    a. In the Connections pane of the IIS Manager, double-click ***server_name***, and click **Sites > Default Web Site > ecp**
    b. In the ecp Home pane, double-click **RSA SecurID**.
    c. In the RSA SecurID pane, verify that **Target This Resource for Single Sign-On** is selected.

Next Step

"Test the Configuration for Single Sign-on with Microsoft Exchange Server 2013."

Test the Configuration for Single Sign-on with Microsoft Exchange Server 2013

The following procedure assumes you have satisfied all of the requirements and preparations listed in the section "Prepare to Set Up SSO Access" on page 79.

To test the SSO configuration:

1. Start the browser on your OWA client computer.
2. In the address field of the browser, enter **https://*server_name*/owa**
   where ***server_name*** is the name of the Microsoft Exchange Server.
   You are prompted for your RSA SecurID user name and passcode.
3. Enter your RSA SecurID user name and passcode, and click **Log In**.
   If authentication is successful, you see the RSA SecurID success screen.
4. To go to your user mailbox, click **Continue**.

Note: If the Web Agent is configured for Auto Submit, you do not have to click **Continue**. Your mailbox opens automatically. For more information, see "Configure Advanced Settings" on page 36.

You have now successfully configured SSO for Microsoft Exchange Server 2013.

Next Step

If your deployment includes Microsoft SharePoint Server, see Chapter 7, "Configuring the Web Agent to Microsoft Office SharePoint Server."

Configure the Web Agent for SSO for Microsoft Exchange Server 2010 SP3

After you have met the prerequisites described in "Prepare to Set Up SSO Access" on page 79, follow these steps in order:

1. Configure Outlook Web Access (OWA) and WebID for Anonymous Access in Microsoft Exchange Server 2010
2. Enable Single Sign-On in Microsoft Exchange Server 2010
3. Verify Application Pool Settings in Microsoft Exchange Server 2010
4. Test the Configuration for Single Sign-On with Microsoft Exchange Server 2010

Configure Outlook Web Access (OWA) and WebID for Anonymous Access in Microsoft Exchange Server 2010

To configure the OWA for anonymous access:

1. On the Microsoft Exchange Server, click **Start > Settings > Control Panel > RSA WebAgent**.
2. In the Connections pane of the IIS Manager, double-click ***server_name***, and then click **Sites > Default Web Site**, where *server_name* is the name of the Microsoft Exchange Server.
3. In the Default Web Site home page, double-click **RSA SecurID**. In the RSA SecurID pane, select **Enable RSA SecurID Web Access Authentication** and click **Apply** on the Actions pane.
4. In the Connections pane of the IIS Manager, double-click ***server_name***, and then click **Sites > Default Web Site > OWA** where *server_name* is the name of the Microsoft Exchange Server.
5. In the OWA home pane, double-click **Authentication**, and perform the following tasks:
   a. In the Authentication pane, select A**nonymous Authentication**, and click **Enable** in the Actions pane. Similarly, select **Windows Authentication**, and click **Enable** in the Actions pane.
   b. In the Authentication pane, select **Anonymous Authentication**, and then click **Edit** in the Actions pane.
   c. In the Edit Anonymous Authentication Credentials dialog box, click **Set** to set the user identity to the specific domain-level user account you created in "Prepare to Set Up SSO Access" on page 79.
   d. Click **OK**.

To configure the WebID application for anonymous access:

1. In the Connections pane of the IIS Manager, double-click ***server_name***, and then click **Sites > Default Web Site > WebID**, where *server_name* is the name of the Microsoft Exchange Server.
2. In the WebID home pane, double-click **Authentication**, and select **Anonymous Authentication**, in the Authentication pane.
3. Click **Enable** in the Actions pane.
4. Restart the IIS Web Server.

Next Step

"Enable Single Sign-On in Microsoft Exchange Server 2010."

Enable Single Sign-On in Microsoft Exchange Server 2010

Perform the following steps to enable single sign-on in Microsoft Exchange Server 2010.

To enable single sign-on in Microsoft Exchange Server 2010:

1. On the Microsoft Exchange Client Access Server, click **Start > Programs > Microsoft Exchange Server 2007/2010 > Exchange Management Console**.
2. In the left pane of the Exchange Management Console, double-click **Server Configuration > Client Access**.
3. In the bottom portion of the Client Access pane, right-click **owa** and select **Properties**.
4. In the owa (Default Web Site) Properties dialog box, click the **Authentication** tab, and then select **Use one or more standard authentication methods** and **Integrated Windows authentication**.

   Important: Make sure no other options are selected.

5. Click **OK**.
6. On the Microsoft Exchange Server, open the Internet Information Services (IIS) Manager. Click **Start > Settings > Control Panel > RSA Web Agent**.
7. Select **Target This Resource for Single Sign-On** for the ecp website. Do the following:
   a. In the Connections pane of the IIS Manager, double-click ***server_name***, and click **Sites > Default Web Site > ecp**

      where *server_name* is the name of the Microsoft Exchange Server.
   b. In the ecp Home pane, double-click **RSA SecurID**.
   c. In the RSA SecurID pane, select **Target This Resource for Single Sign-On**.
   d. In the Actions pane, click **Apply**.

8. In the Connections pane of the IIS Manager, double-click ***server_name***, and click **Sites > Default Web Site > owa**

   where *server_name* is the name of the Microsoft Exchange Server.

9. In the owa Home pane, double-click **RSA SecurID**.
10. In the RSA SecurID pane, select **Target This Resource for Single Sign-On**.
11. In the Actions pane, click **Apply**.

    If you have a custom application pool, an RSA Authentication Agent Properties dialog box states that you must change the application pool to "RSA SecurID Pool."

12. Restart IIS. Do the following:
    a. On the IIS server, click **Start > Run**.
    b. Type **IISReset**, and click **OK**.

       The Command Prompt window displays the IISReset command status.

    c. Verify that IIS stops and restarts.

Next Step

"Verify Application Pool Settings in Microsoft Exchange Server 2010."

Verify Application Pool Settings in Microsoft Exchange Server 2010

To verify Application Pool settings:

1. In the Connections pane of the IIS Manager, double-click ***server_name***, and then click **Sites > Default Web Site > OWA**.
2. Right click OWA and select **Manage Application > Advanced Settings**.
3. Select the Application pool as **MSExchangeOWAAppPool**.
4. In the **Connections** pane, double-click ***server_name***, and then click **Sites > Default Web Site > WebID**.
5. Right click **WebID** and select **Manage Application > Advanced Settings**.
6. Select the Application pool as **RSA SecurID Pool**.

   Note: By default, the RSA SecurID pool is in the LocalSystem identity. Perform the optional steps 7–9 to change the identity.

7. (Optional) In the **Connections** pane, double-click ***server_name***, and then click **Application Pools**.
8. (Optional) Click **RSA SecurID Pool > Advanced Settings**.
9. (Optional) Click **Identity > Application Pool Identity > Custom Account**. Specify the administrator account privileges here.

10. Verify that the ecp website is protected by RSA SecurID. Do the following:
    a. In the Connections pane of the IIS Manager, double-click ***server_name***, and click **Sites > Default Web Site > ecp**
    b. In the ecp Home pane, double-click **RSA SecurID**.
    c. In the RSA SecurID pane, verify that **Target This Resource for Single Sign-On** is selected.

Next Step

"Test the Configuration for Single Sign-On with Microsoft Exchange Server 2010."

Test the Configuration for Single Sign-On with Microsoft Exchange Server 2010

The following procedure assumes you have satisfied all of the requirements and preparations listed in the section "Prepare to Set Up SSO Access" on page 79.

To test the SSO configuration:

1. Start the browser on your OWA client computer.
2. In the address field of the browser, enter **https://*server_name*/owa**
   where *server_name* is the name of the Microsoft Exchange Server.
   You are prompted for your RSA SecurID user name and passcode.
3. Enter your RSA SecurID user name and passcode, and click **Log In**.
   If authentication is successful, you see the RSA SecurID success screen.
4. To go to your user mailbox, click **Continue**.

   Note: If the Web Agent is configured for Auto Submit, you do not have to click **Continue**. Your mailbox opens automatically. For more information, see "Configure Advanced Settings" on page 36.

   You have now successfully configured SSO for Microsoft Exchange Server 2010 SP3.

Note: If offloading SSL with Exchange is enabled, and require SSL and redirect to SSL are disabled, users will have to enter their credentials on the http login page.

Next Step

If your deployment includes Microsoft SharePoint Server, see Chapter 7, "Configuring the Web Agent to Microsoft Office SharePoint Server."

Configure the Web Agent for SSO for Microsoft Exchange Server 2007 SP2

After you have met the prerequisites described in "Prepare to Set Up SSO Access" on page 79, follow these steps in order:

1. Configure Outlook Web Access (OWA) and WebID for Anonymous Access
2. Enable Single Sign-On
3. Verify Application Pool settings
4. Test the Configuration

Configure Outlook Web Access (OWA) and WebID for Anonymous Access

To configure the OWA for anonymous access:

1. On the Microsoft Exchange Server, click **Start > Settings > Control Panel > RSA WebAgent**.
2. In the Connections pane of the IIS Manager, double-click ***server_name***, and then click **Sites > Default Web Site**, where *server_name* is the name of the Microsoft Exchange Server.
3. In the Default web site home page, double-click **RSA SecurID**. In the RSA SecurID pane, select **Enable RSA SecurID Web Access Authentication** and click **Apply** on the Actions pane.
4. In the Connections pane of the IIS Manager, double-click ***server_name***, and then click **Sites > Default Web Site > OWA** where *server_name* is the name of the Microsoft Exchange Server.
5. In the OWA home pane, double-click **Authentication**, and perform the following tasks:
   a. In the Authentication pane, select A**nonymous Authentication**, and click **Enable** in the Actions pane. Similarly, select **Windows Authentication**, and click **Enable** in the Actions pane.
   b. In the Authentication pane, select **Anonymous Authentication**, and then click **Edit** in the Actions pane.
   c. In the Edit Anonymous Authentication Credentials dialog box, click **Set** to set the user identity to the specific domain-level user account you created in "Prepare to Set Up SSO Access" on page 79.
   d. Click **OK**.

To configure the WebID for anonymous access:

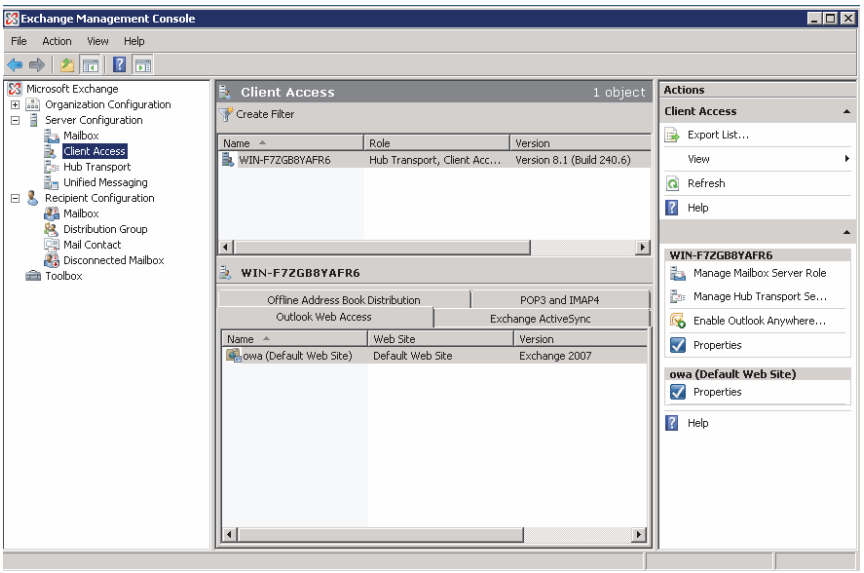
1. In the Connections pane of the IIS Manager, double-click ***server_name***, and then click **Sites > Default Web Site > WebID**, where *server_name* is the name of the Microsoft Exchange Server.
2. In the WebID home pane, double-click **Authentication**, and select **Anonymous Authentication**, in the Authentication pane.

3. Click **Enable** in the Actions pane.
4. Restart the IIS Web Server.

Enable Single Sign-On

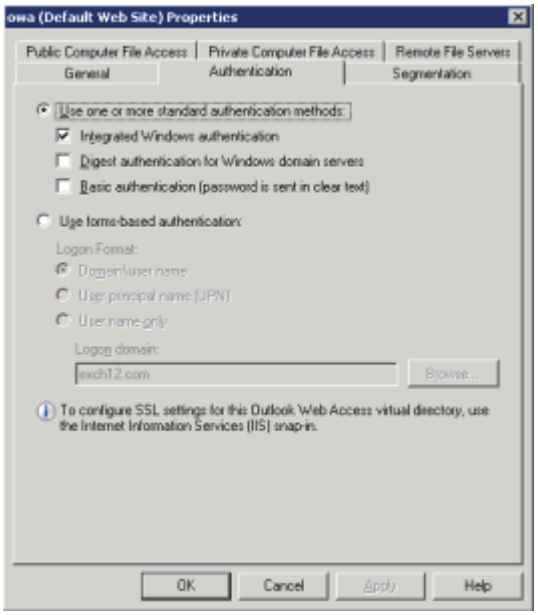
To enable single sign-on:

1. On the Microsoft Exchange Server, click **Start > Programs > Microsoft Exchange Server 2007/2010 > Exchange Management Console**.
2. In the left pane of the Exchange Management Console, double-click **Server Configuration > Client Access**.
3. In the bottom portion of the Client Access pane, right-click **owa** and select **Properties**.



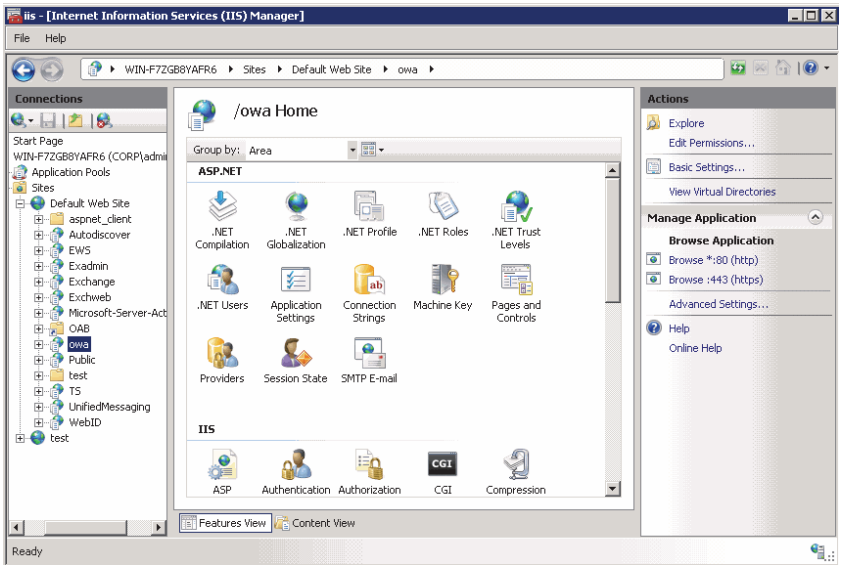
4. In the owa (Default Web Site) Properties dialog box, click the **Authentication** tab, and then select **Use one or more standard authentication methods** and **Integrated Windows authentication**.

Important: Make sure no other options are selected.



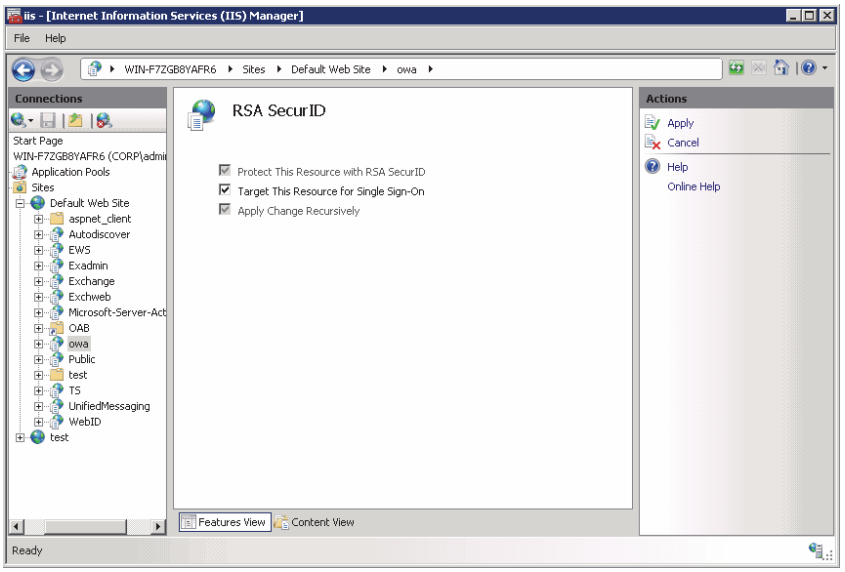
5. Click **OK**.
6. On the Microsoft Exchange Server machine, click **Start > Settings > Control Panel > RSA Web Agent**.
7. In the Connections pane, double-click ***server_name,*** and then click **Sites > Default Web Site > owa**

   where ***server_name*** is the name of the Microsoft Exchange Server.



8. In the owa Home pane, double-click **RSA SecurID**.

9. In the RSA SecurID pane, select **Target This Resource for Single Sign-On**.



10. In the Actions pane, click **Apply**.

To enable SecurID protection and Single Sign-On for calendar operations,

1. In the Connections pane, double-click ***server_name,*** and then click **Sites > Default Web Site > ecp**

   where ***server_name*** is the name of the Microsoft Exchange Server.
2. In the Connections pane of the IIS Manager, select **ecp**, and then double-click **RSA SecurID** in the ecp Home pane.
3. In the RSA SecurID pane, select **Protect this resource with RSA SecurID** and then select **Target This Resource for Single Sign-On**.
4. In the Actions pane, click **Apply**.

Verify Application Pool settings

To verify Application Pool settings:

1. In the **Connections** pane, double-click server_name, and then click **Sites > Default Web Site > OWA**.
2. Right click OWA and select **Manage Application > Advanced Settings**.
3. Select the Application pool as **MSExchangeOWAAppPool**.
4. In the **Connections** pane, double-click server_name, and then click **Sites > Default Web Site > WebID**.
5. Right click **WebID** and select **Manage Application > Advanced Settings**.
6. Select the Application pool as **RSA SecurID Pool**.
7. (Optional) In the **Connections** pane, double-click server_name, and then click **Application Pools**.

8. (Optional) Click **RSA SecurID Pool>Advanced Settings**.
9. (Optional) Click **Identity>Application Pool Identity>Custom Account**. Specify the administrator account privileges here.

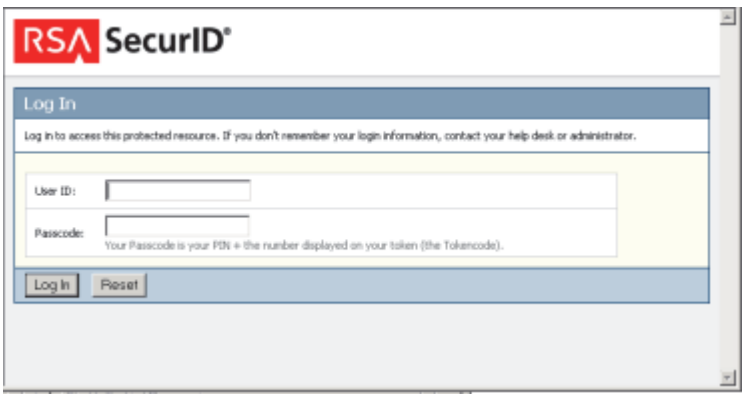
Note: By default RSA SecurID's pool will be in the LocalSystem identity. Perform Steps 7-9 to change the identity.

Test the Configuration

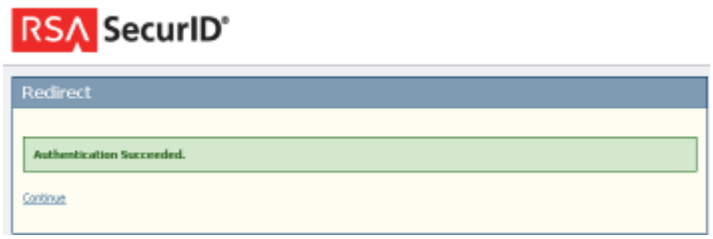
The following procedure assumes you have satisfied all of the requirements and preparations listed in the section "Prepare to Set Up SSO Access" on page 79.

To test the SSO configuration:

1. Start the browser on your OWA client computer.
2. In the address field of the browser, enter **https://*server_name*/owa** where ***server_name*** is the name of the Microsoft Exchange Server. You are prompted for your RSA SecurID user name and passcode.



3. Enter your RSA SecurID user name and passcode, and click **Log In**. If authentication is successful, you see the RSA SecurID success screen.



4. To go to your user mailbox, click **Continue**.

Note: If the Web Agent is configured for Auto Submit, you do not have to click **Continue**. Your mailbox opens automatically. For more information, see "Configure Advanced Settings" on page 36.

Before You Uninstall the Web Agent

Before you can uninstall the Web Agent, you must disable anonymous access for the web application and disable SSO in Outlook Web Access.

To disable anonymous access for the web application:

1. On the Microsoft Exchange Server, open the Information Services (IIS) Manager. Click **Start > Settings > Control Panel > RSA Web Agent**.
2. In the Connections pane of the IIS Manager, double-click ***server_name***, and click **Sites > Default Web Site > owa**

   where *server_name* is the name of the Microsoft Exchange Server.
3. In the owa Home pane, double-click **Authentication**.
4. In the Authentication pane, disable anonymous access. Select **Anonymous Authentication**, and click **Disable** in the Actions pane.

To disable SSO in Outlook Web Access:

1. In the Connections pane of the IIS Manager, select **OWA**, and double-click **RSA SecurID** in the OWA Home pane.
2. In the RSA SecurID pane, deselect **Target This Resource for Single Sign-O**n.
3. Restart the IIS web server.

Next Steps

Additional configuration steps are required. For instructions, see "Reconfigure Microsoft Exchange Server."

Reconfigure Microsoft Exchange Server

You need to reconfigure Microsoft Exchange Server if you have either disabled SSO, disabled the Web Agent, or uninstalled the Web Agent.

Important: If you do not reconfigure Microsoft Exchange Server after disabling SSO, disabling the Web Agent, or uninstalling the Web Agent, Microsoft Exchange Server will not work.

Follow the procedure for your Microsoft Exchange Server version:

- Reconfigure Microsoft Exchange Server 2013
- Reconfigure Microsoft Exchange Server 2010 or 2007

Reconfigure Microsoft Exchange Server 2013

To reconfigure Microsoft Exchange Server 2013:

1. Open the Microsoft Exchange Administration Center (EAC).
1. On the Microsoft Exchange Server, open the Internet Information Services (IIS) Manager. Click **Start > Settings > Control Panel > RSA Web Agent**.
2. Select **Target This Resource for Single Sign-On** for the ecp website. Do the following:
   a. In the Connections pane of the IIS Manager, double-click ***server_name***, and click **Sites > Default Web Site > ecp**
      where *server_name* is the name of the Microsoft Exchange Server.
   b. In the ecp Home pane, double-click **RSA SecurID**.
   c. In the RSA SecurID pane, select **Target This Resource for Single Sign-On**.
   d. In the Actions pane, click **Apply**.
3. Change the authentication method for the ecp website. Do the following:
   a. Log on to the ecp website as an SecurID administrator.
   b. Change from **Integrated Windows authentication** to **Domain\User name**.
4. Restart the IIS Web Server.
5. Deselect **Target This Resource for Single Sign-On** for the ecp website. Do the following:
   a. In the Connections pane of the IIS Manager, double-click ***server_name***, and click **Sites > Default Web Site > ecp**
      where *server_name* is the name of the Microsoft Exchange Server.
   b. In the ecp Home pane, double-click **RSA SecurID**.
   c. In the RSA SecurID pane, select **Target This Resource for Single Sign-On**.
   d. In the Actions pane, click **Apply**.

6. Deselect **Target This Resource for Single Sign-On** for the owa website. Do the following:
   a. In the Connections pane of the IIS Manager, double-click ***server_name***, and click **Sites > Default Web Site > owa**
      where *server_name* is the name of the Microsoft Exchange Server.
   b. In the owa Home pane, double-click **RSA SecurID**.
   c. In the RSA SecurID pane, select **Target This Resource for Single Sign-On**.
   d. In the Actions pane, click **Apply**.

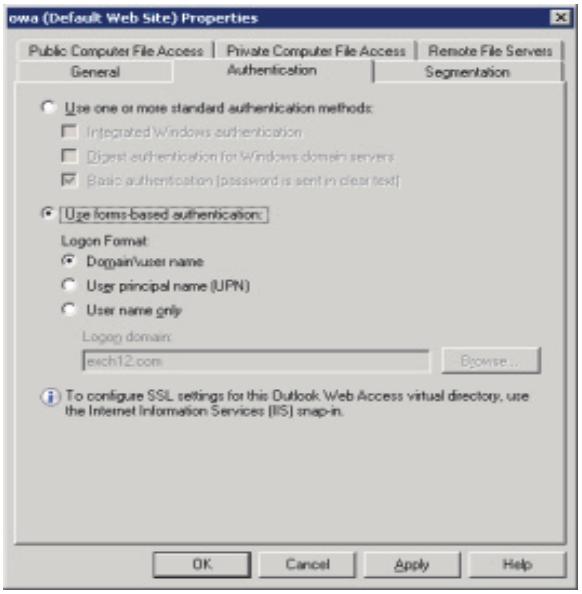
Next Steps

If you are uninstalling the Web Agent, see "Uninstall the Web Agent" on page 28. Otherwise, the procedure is complete.

Reconfigure Microsoft Exchange Server 2010 or 2007

To reconfigure Microsoft Exchange Server:

1. On the Microsoft Exchange Client Access Server, click **Start > Programs > Microsoft Exchange Server 2007/2010 > Exchange Management Console**.
2. In the left pane of the Exchange Management Console, double-click **Server Configuration > Client Access**.
3. In the bottom portion of the Client Access pane, right-click **owa** and select **Properties**.
4. In the owa (Default Web Site) Properties dialog box, click the **Authentication** tab, and then select **Use forms-based authentication** and **Domain/user name**



5. Click **OK**.
6. Restart the IIS web server.

If you enabled SSO from Web Agent, you must disable SSO from OWA. Follow the steps below to disable SSO from OWA.

To disable SSO from OWA:

1. In the Connections pane of the IIS Manager, select **OWA.**
2. In the OWA home pane double click **RSASecurID**.
3. In the RSA SecurID pane, deselect **Target this Resource for Single Sign-On**.
4. In the Actions pane, click **Apply**.
5. Restart the IIS Web Server.

Next Steps

If you are uninstalling the Web Agent, see "Uninstall the Web Agent" on page 28. Otherwise, the procedure is complete.

Add Domain Suffixes if the Exchange Server and User Accounts are on Different Domains

When the Exchange Server front-end and the Web Agent are installed on one domain and the user accounts are enabled in other trusted domains, the administrator can specify a list of possible domain suffixes for a user.

To specify a list of domain suffixes:

1. Under **HKLM\SOFTWARE\SDTI\RSAWebAgent** create a registry key **'Suffix'**
2. Under **'Suffix'** create a String Value **'SSODomainSuffix'**.
3. Update the **SSODomainSuffix** key with a list of domain suffixes, separated by colon(:), for example dom1.com:dom2.com

The WebAgent appends the username with dom1.com and performs single sign-on (SSO). If the user exists in the domain dom1.com, a valid SSO authentication occurs.If the user is not present in the domain dom1.com, the WebAgent appends the username with dom2.com and performs SSO. This continues until a successful SSO authentication is achieved.

7 Configuring the Web Agent to Microsoft Office SharePoint Server

This chapter describes how to integrate the Web Agent with Microsoft Office SharePoint Server. The Web Agent supports the following versions:

- SharePoint Server 2013 SP1 on Windows Server 2012 with Internet Information Services 8.0
- SharePoint Server 2010 SP2 (with the latest patches) on Windows Server 2008 R2 SP1 (64-bit) with Internet Information Services 7.5
- SharePoint Server 2007 SP2, 2010 and 2013 on the Windows 2008 platform with Internet Information Services 7.0 and 7.5

You can protect the SharePoint site with single sign-on (SSO). With SSO, users authenticate through RSA SecurID to access a web application that would otherwise be protected by a Microsoft Windows logon. To protect the SharePoint site without SSO refer to "Protect the Site, Application, Files, or Folders" on page 54.

Important: In SharePoint 2013 and SharePoint 2010, add the statement **<remove name="OutputCache" />** in the web.config modules list, of the SharePoint site to be protected.

Note: If you are using a SharePoint farm configuration, see the following Microsoft topics about using a domain administrator for the application pool identity.

For SharePoint Server 2013, see:
https://technet.microsoft.com/en-us/library/hh344224.aspx

For SharePoint Server 2010, see:
https://technet.microsoft.com/en-us/library/ff805066(v=office.14).aspx

Prerequisites for Using Web Agent with SharePoint Server 2013

You must perform the following tasks to use Web Agent with SharePoint Server 2013. SharePoint Server 2010 and 2007 do not require these procedures.

To run the web Application Pool as a Network Service:

1. Grant Read permission to the following registry entries for the Network Service:
   - **HKLM\System\CurrentControlSet\Services\WinSock2\Parameters**
   - **HKLM\SOFTWARE\SDTI\RSAWebAgent**
   - **HKLM\SOFTWARE\SDTI\ACECLIENT**
2. Grant Read and Execute, List folder contents, and Read permissions to the directory:
   \Program Files\RSA Security\RSAWebAgent
3. Grant Read and Execute, and Read permissions to the file:
   \Program Files\RSA Security\RSAWebAgent\securid
4. Grant Read and Execute, and Read permissions to the file:
   \Program Files\RSA Security\RSAWebAgent\sdstatus.12

To change the Application Pool settings for the site:

1. In the Connection pane of the IIS Manager, click ***server_name*** **> Application Pools**.
2. Click the application pool for the SharePoint website.
3. In the Actions pane, click **Advanced Settings**.
4. Under Process Model, click the **Identity** field and change the identity to **NetworkService**.

To verify the RSA SecurID Pool Application Pool setting for the Windows Server:

1. Go to Application Pools in IIS Manager.
2. Verify the .Net Framework Version setting for RSA SecurID Pool.

Windows Server	.NET Framework
Windows Server 2008	.NET Framework 2.x
Windows Server 2008 R2	.NET Framework 2.x
Windows Server 2012	.NET Framework 4.x

Next Step

"Configuring Web Access Authentication Persistent Cookies."

Configuring Web Access Authentication Persistent Cookies

Web access authentication persistent cookies must be configured in order to open SharePoint documents in their native applications, such as Microsoft Word documents in Microsoft Office or PDF files in Adobe Acrobat Reader. This step is not required to use Office Online (Office Web Apps).

If you have enabled client integration on the Microsoft SharePoint Server, clicking a browser link to a document residing on the SharePoint Server opens the document in its native application, such as Microsoft Office. Because this is a new session, the web access authentication cookie created in the browser session is not available for the Microsoft Office session. This causes Microsoft Office to prompt for RSA SecurID credentials each time a Microsoft Office document is opened.

To avoid the need for users to re-authenticate multiple times, enable the creation of persistent cookies. You can configure persistent cookies by selecting one of the following options:

- "Configure Short-Term Persistent Cookies for Microsoft Office"
- "Configure Long-Term Persistent Cookies for Microsoft Office"

For security vulnerabilities related to persistent cookies, "Security Vulnerabilities Related to Persistent Cookies" on page 105.

Configure Short-Term Persistent Cookies for Microsoft Office

If your environment uses Microsoft Office 2007 or later, you can configure short-term persistent cookies that rely upon modifying a copy of the Microsoft SharePoint Server **core.js** file. This option utilizes a short-term persistent cookie that typically exists for a few seconds on the client machine, where the browser is running. These cookies are created when you try to open the Microsoft Office document. When a session cookie is created, the short-term persistent cookie is deleted.

The expiry time for this cookie is the sum of the maximum time it takes for Internet Explorer to launch Microsoft Office and the maximum time it takes for Microsoft Office to send a request to the SharePoint Server. If necessary, you can increase the lifetime of short-term persistent cookies.

To configure persistent cookie settings:

1. Click **Start > Settings > Control Panel**, and double-click **RSA Web Agent**.
2. In the Connections pane of the IIS Manager, double-click ***server_name*** **> Sites,** and then click the name of the SharePoint web site.
3. In the *SharePoint web_site* Home pane, double-click **RSA SecurID**.

4. Perform the following tasks in the RSA SecurID Home pane:
   a. Select **Enable RSA SecurID Web Access Authentication Feature on This Server** and **Protect This Resource**.
   b. In the SharePoint Settings section, click **Configure**.
   c. In the Manage SharePoint Settings dialog box, select **Access Microsoft Office 2007/ 2010 Documents from the SharePoint Server**.
   d. Set the short-term persistent cookie expiration time.
   e. Click **OK** to return to the RSA SecurID pane.
5. In the Actions pane, click **Apply**.
6. Add an http request for creating short-term persistent cookies. Instead of modifying the original **core.js** file, create a file named **customcore.js**.
   Do the following:
   a. Create a blank file on the SharePoint Server with the name **customcore.js**.
   b. Add the sendRSAShortTermCookieRequest() function at the beginning of the **customcore.js** file on the SharePoint Server:

```
function sendRSAShortTermCookieRequest() {
   var cookieRequest = false;
   try {
      cookieRequest = new XMLHttpRequest();
   }
   catch (trymicrosoft) {
      try {
            cookieRequest = new
ActiveXObject("Msxml2.XMLHTTP");
      }catch (othermicrosoft)
      {
            try {
            cookieRequest = new
ActiveXObject("Microsoft.XMLHTTP");
            } catch (failed) {
            cookieRequest = false;
            }
      }
   }
   if (!cookieRequest)
      alert("Error initializing XMLHttpRequest!");
    var url = "/writeshorttermpersisted.asmx";
    cookieRequest.open("GET", url, false);
    cookieRequest.send(null);
   if(!cookieRequest.getResponseHeader("Date"))
   {
```

```
        var cached = cookieRequest;
        cookieRequest = false;
        try {
              cookieRequest = new XMLHttpRequest();
        } catch (trymicrosoft) {
              try {
              cookieRequest = new
ActiveXObject("Msxml2.XMLHTTP");
              } catch (othermicrosoft) {
              try {
              cookieRequest = new
ActiveXObject("Microsoft.XMLHTTP");
              } catch (failed) {
              cookieRequest = false;
              }
        }
     }
     var ifModifiedSince =
cached.getResponseHeader("Last-Modified");
     ifModifiedSince = (ifModifiedSince)?ifModifiedSince
: new Date(0);
     cookieRequest.open("GET", url, false);
     cookieRequest.setRequestHeader("If-Modified-Since",
ifModifiedSince);
     cookieRequest.send("");
     }
     if (cookieRequest.status!= 200)
     {
        alert("ERROR: Single-Signon Cookie Request"+
"Failed!,Application may not load Document");
     }
}
```

c. Copy the following functions from **core.js** to **customcore.js**:

- For SharePoint Server 2013 and 2010:

  ```
  function _DispEx
  function _DispDocItemEx
  function editDocumentWithProgID2
  function createNewDocumentWithProgIDCore
  ```

- For SharePoint Server 2007:

  ```
  function DispEx
  function DispDocItemEx
  function editDocumentWithProgID2
  function createNewDocumentWithProgIDCore
  ```

d. Add the call sendRSAShortTermCookieRequest() function at the beginning of the functions copied from **core.js**.

Note: These functions are called when a new Microsoft Office session is launched. If these functions do not cover any custom behavior, you can add the call to the sendRSAShortTermCookieRequest**()** function in the required modules.

e. Copy the **customcore.js** file to the same directory as core.js. Use one of the following locations:

- In a default SharePoint Server 2013 installation, the **core.js** file is at **C:\Program Files\Common Files\microsoft shared\Web Server Extensions\15\TEMPLATE\LAYOUTS**.
- In a default SharePoint Server 2010 installation, the **core.js** file is at **C:\Program Files\Common Files\Microsoft Shared\web server extensions\14\TEMPLATE\LAYOUTS\1033**.
- In a default SharePoint Server 2007 SP2 installation, the **core.js** file is at **C:\Program Files\Common Files\Microsoft Shared\web server extensions\12\TEMPLATE\LAYOUTS\1033**.

If you use a non-standard layout template, this path may be different.

7. Create a custom master page for the site that hosts Microsoft Office documents. Do the following:

a. Determine the location of the original master page. For example, run the following command in the SharePoint Management Shell:

```
$site = Get-SPSite http://SharePointSITEURL
$web = $site.RootWeb
$web.MasterUrl
```

b. In SharePoint Designer, open the SharePoint site, and click **Master pages**.

If the SharePoint is already protected by RSA SecurID, you must remove that protection until the custom master page procedure is complete. Do the following:

a. On the IIS server, click **Start > Settings > Control Panel > RSA Web Agent**.

b. In the Connections pane, double-click *server_name*, and click **Sites > *WebSite***, where *server_name* is the name of the IIS Server Machine and ***WebSite*** is the name of the protected web site.

c. In the Site Home pane, double-click **RSA SecurID**.

d. In the RSA SecurID pane, clear the **Protect This Resource** checkbox.

e. In the Actions pane, click **Apply**.

f. Restart the IIS Web Server. Do the following:

On the IIS server, click **Start > Run**.

Type **IISReset**, and click **OK**. The Command Prompt window displays the IISReset command status.

Verify that IIS stops and restarts.

c. Copy the master page and rename it **custom.master**.

d. Open **custom.master** for editing and replace the following line,

```
<SharePoint:ScriptLink language="javascript"
name="core.js" OnDemand="true" runat="server" />
```

With

```
<SharePoint:ScriptLink language="javascript"
name="core.js" Defer="true" runat="server"/>
<SharePoint:ScriptLink language="javascript"
name="customcore.js" Defer="true" runat="server"/>
```

e. Right click **custom.master** and set it as the **Custom** and **Default Master** page.

f. If you removed RSA SecurID protection before creating a custom master page, apply it again. Do the following:

a. On the IIS server, click **Start > Settings > Control Panel > RSA Web Agent**.

b. In the Connections pane, double-click *server_name*, and click **Sites > *WebSite***, where *server_name* is the name of the IIS Server Machine and ***WebSite*** is the name of the web site to be protected.

c. In the Site Home pane, double-click **RSA SecurID**.

d. In the RSA SecurID pane, select the **Protect This Resource** checkbox.

e. In the Actions pane, click **Apply**.

f. Restart the IIS Web Server. Do the following:

On the IIS server, click **Start > Run**.

Type **IISReset**, and click **OK**. The Command Prompt window displays the IISReset command status.

Verify that IIS stops and restarts.

Configure Long-Term Persistent Cookies for Microsoft Office

The long-term persistent cookie option does not require modifications to a copy of the Microsoft SharePoint Server **core.js** file. Instead, you configure web authentication persistent cookies with the Web Agent software.

This more convenient option might avoid the need to re-authenticate as often. You might choose this option if editing a copy of the **core.js** file is not working in your environment. For example, if you apply an update from Microsoft that changes **core.js**.

This option enables the creation of long-term persistent cookies for an environment with both Microsoft Office 2003 and 2007/2010. Microsoft Office 2003 and earlier versions do not support forms-based authentication. Because of this, you might not be able to view the RSA SecurID page in earlier versions of Microsoft Office, and you cannot open the Microsoft Office document.

You need to set the expiry time of the persistent cookie to the maximum allowed time for a session in the SharePoint Server. You can set the time-out value for the persistent cookie for 30 minutes or more. The persistent cookie is created for the URLs entered in the URL list.

Important: Microsoft Office uses the privacy settings you select in Internet Explorer. It does not download cookies if you have selected not to allow cookies to be downloaded. However, those features that use cookies may not work correctly. If you previously saved cookies to your hard disk, Microsoft Office may still read these cookies unless you remove previously saved cookies in Internet Explorer.

To set persistent cookies:

1. Click **Start > Settings > Control Panel**, and double-click **RSA Web Agent**.
2. In the Connections pane of the IIS Manager, double-click ***server_name*** > **Sites,** and then click the name of the SharePoint web site.
3. In the *SharePoint web_site* Home pane, double-click **RSA SecurID**.
4. Perform the following tasks in the RSA SecurID Home pane:
   a. Select **Enable RSA SecurID Web Access Authentication Feature on This Server** and **Protect This Resource**.
   b. Click **Manage SharePoint Settings**.
   c. In the Manage SharePoint Settings dialog box, select **Access Microsoft Office 2003 or 2007/ 2010 documents from the SharePoint Server**.
   d. Set the long-term persistent cookie expiration time.
   e. In the URL list box, click **Add**, and enter the URL for which you want to enable long-term persistent cookies.

      Use an asterisk character *, known as a wildcard, to allow access to all documents in a folder on a site. You can use a wildcard in any location in a URL.

You can use wildcards to exclude SharePoint logon pages that require user authentication and to specify the directories that are commonly used for SharePoint documents. For example, you can enter the following URLs:

- **/*/_layouts/***
- **/_vti_bin/***
- **/*/_vti_bin/***
- **/Shared Documents/***
- **/*/Shared Documents/***

f. Click **OK**.

g. Click **OK** to return to the RSA SecurID Home pane.

5. In the Actions pane, click **Apply**.
6. Restart the IIS web server.
7. Configure the application pools for SharePoint. For instructions, see "Prevent Caching of Static HTML Pages in Client Browsers" on page 45.

Note: Microsoft Office applications communicating with Web Servers do not send persistent cookies that are saved by Internet Explorer back to the Web Server. This may result in a user being asked for authentication each time a Office document is opened, even if persistent cookies are configured in WebAgent. To avoid this, users should perform the resolution mentioned in **http://support.microsoft.com/kb/932118**

Security Vulnerabilities Related to Persistent Cookies

Persistent cookies are deemed vulnerable to attacks because they continue to exist even when a browser with a user session is closed, until the persistent cookies expire. Persistent cookies expire based upon the idle timeout value that is specified by the "Cookies expire if not used within the specified time" advanced setting in the RSA SecurID web access authentication properties sheet. For information, see "Configure Advanced Settings" on page 36.

You can remove persistent cookies by explicitly logging off the application.

Important: Always use the SharePoint Server **Sign Out** command to end SharePoint Server sessions. When you click ***user_name*** **> Sign Out**, the Web Agent deletes all session cookies and persistent cookies.

If you have only Microsoft Office 2007 clients, and do not want to enable persistent cookie creation, you are prompted for authentication each time a document is accessed from the SharePoint Server. For more information, see "Support for Forms-Based Authentication in Microsoft Office" on page 62.

Allow Back-End SharePoint Web App Servers

The Web Agent supports SharePoint Server configurations that use back-end Office Web Apps servers for accessing and manipulating shared documents. You must specify a policy in the system registry to grant special permission to access the Office Web Apps servers. If the policy is not specified, the functionality provided by the Web Apps servers is denied.

Before You Begin

In the IIS Configuration Manager, right-click your website, select **Manage Website > Advanced Settings**, and record the **Sharepoint ID**.

To allow back-end Office Web Apps servers:

1. In the Windows registry, access **HKLM\SOFTWARE\SDTI\RSAWebAgent**.
2. Create a new REG_DWORD Value named **SharePointFarmSupport**.
3. Set the Value to **1**. This value allows access to the Office Web App servers.
   To deny access, set the value to **0**.
4. Create a new REG_SZ Value named **SharePointID**.
5. Set the value to the SharePoint website ID. Enclose the value in parentheses.
   To determine the website ID, in the IIS Configuration Manager, select **Manage Web Site > Advanced Settings > ID**.
   For example, **SharePointID = (1)**
6. Restart IIS. Do the following:
   a. On the IIS server, click **Start > Run**.
   b. Type **IISReset**, and click **OK**.
      The Command Prompt window displays the IISReset command status.
   c. Verify that IIS stops and restarts.

Configure the Web Agent for Single Sign-On to the SharePoint Server 2013

To configure the Web Agent for single sign-on to the Microsoft Office SharePoint Server:

- You must have Windows Server 2012 (64-bit) on the environment domain controller. For more information, see your Microsoft Active Directory documentation.
- You must have unique user names across all domains. In addition, user names in the Active Directory Server must match the user names in the RSA Authentication Manager database.
- You must install Microsoft SharePoint Server 2013 SP1 and configure it to work with IIS.

- You must install the Web Agent, as described in Chapter 3, "Installing RSA Authentication Agent for Web for IIS 7.0, 7.5, and 8.0," follow the prerequisities in this chapter, including "Prerequisites for Using Web Agent with SharePoint Server 2013" on page 98, and enable RSA web access protection on the portal web site. For instructions, see the Web Agent Help topic, "Enabling Web Access Authentication."
- You must perform the configuration steps in "Prepare to Set Up Single Sign-On to the SharePoint Server 2013" on page 107.

Before setting up SSO access, verify that your setup is correct. When users attempt to access the portal, they must be challenged by both RSA SecurID and SharePoint.

Prepare to Set Up Single Sign-On to the SharePoint Server 2013

Before setting up single sign-on (SSO) access to the Microsoft SharePoint Server:

Note: The following steps are applicable for the Windows Server 2012 (64-bit) domain controller.

1. On the domain controller, use Microsoft Active Directory to create a domain level user.
2. Using Active Directory, assign the right to delegate services:
   - On the domain controller, click **Start > Programs > Administrative Tools > Active Directory Users and Computers**.
   - In the left pane, double-click ***domain name***.
   - Double-click **Computers**, and in the right pane, double-click ***SharePoint server name***.
   - In the Delegation dialog box, select **Trust this computer for delegation to any service (Kerberos only)**, and click **OK**.
3. Using a text editor, open **web.config**, which is located in the document root directory of your web portal. Make sure the following entry is in the <appsettings> tag, before the </configuration> tag:

```
<appSettings>
<add key="SPS-EnforceIISAnonymousSetting" value="false"/>
</appSettings>
```

Next Step

"Configure Single Sign-On to the SharePoint Server 2013."

Configure Single Sign-On to the SharePoint Server 2013

Perform the following steps to configure Single Sign-On to the Microsoft SharePoint Server:

1. Protect the SharePoint Site
2. Verify Authentication and Application pool settings for WebID Application
3. Verify the Application pool settings for the Site
4. Enable Single Sign-on

Protect the SharePoint Site

To protect the SharePoint site:

1. On the IIS Server machine, click **Start > Settings > Control Panel** > **RSA Web Agent**.
2. In the Connections pane of the IIS Manager, double-click ***server_name*** and click **Sites>SharePoint_site**, where *server_name* is the name of the IIS Server Machine and SharePoint_Site is the name of the site to be protected.
3. In the SharePoint_Site Home pane, double-click **RSA SecurID**.
4. In the RSA SecurID pane, select **Enable RSA SecurID Web Access Authentication**.
5. In the Actions pane, click **Apply**.

Next Step

"Verify Authentication and Application Pool Settings for the WebID Application."

Verify Authentication and Application Pool Settings for the WebID Application

To verify Authentication and Application pool settings for the WebID Application

1. Refresh the IIS Manager, click ***server_name***, and click **Sites > SharePoint_Site > WebID**.
2. In the WebID Home pane, double-click **Authentication**.
3. In the Authentication pane, do the following:
   - Select **Anonymous Authentication**, and click **Enable** on the Actions pane.
   - Select **Windows Authentication**, and click **Disable** on the Actions pane.
4. In the Connections pane, double-click ***server_name***, and then click **Sites > SharePoint_Site > WebID**.
5. Right click **WebID** and select **Manage Application > Advanced Settings**.
6. Select the Application pool as **RSA SecurID Pool**.

Next Step

"Verify the Application Pool Settings for the Site."

Verify the Application Pool Settings for the Site

To verify Application pool settings for the Site

1. In the Connection Pane of the IIS Manager, click ***server_name*** **> Application Pools**.
2. Click the SharePoint website's application pool and in the Actions pane, click **Advanced Settings**.
3. Under Process Model, click the **Identity** field and change the identity to **NetworkService**.

Next Step

"Enable Single Sign-On."

Enable Single Sign-On

To enable single-sign on

1. Access **System32 > inetsrv > config > applicationHost.config**.
2. Search for the SecurIDModule in the file and add an entry for SecurIDSSOModule under that in the format <add name="SecurIDSSOModule" image="PATH_TO_ RSASinglesignon.dll" />,

   Note: RSASinglesignon.dll can be found inside the Web Agent installation directory.

3. In the Connections pane of IIS Manager, double-click ***server_name***, and click **Sites > SharePoint_Site**
4. In the SharePoint_Site Home pane, double-click **Modules**.
5. In the Actions pane, click **Configure Native Modules** and add the SecurIDSSOModule.
6. In the Connections pane of IIS Manager, double-click ***server_name***, and click **Sites > SharePoint_Site>WebID**.
7. In the WebID Home pane, double-click **Modules**.
8. In the Actions pane, select the **SecurIDSSOModule**, and click **Remove**.
9. Restart the IIS Web Server.

   You have successfully configured SSO to the SharePoint Server 2013.

Note: When SSO is enabled, a user cannot sign in as another user on the protected site.

Configure the Web Agent for Single Sign-On to the SharePoint Server 2010

To configure the Web Agent for single sign-on to the Microsoft Office SharePoint Server:

- You must have Windows 2008 R2 SP1 (64-bit) Server running on the environment domain controller. For more information, see your Microsoft Active Directory documentation.
- You must have unique user names across all domains. In addition, user names in the Active Directory Server must match the user names in the RSA Authentication Manager database.
- You must install SharePoint Server 2010, and configure it to work with IIS.
- You must install the Web Agent, as described in Chapter 3, "Installing RSA Authentication Agent for Web for IIS 7.0, 7.5, and 8.0," and enable RSA web access protection on the portal web site. For instructions, see the Web Agent Help topic, "Enabling Web Access Authentication."
- You must perform the configuration steps in "Prepare to Set Up Single Sign-On to the SharePoint Server 2010" on page 110.
- To use SharePoint Server 2010 with the single sign-on feature of RSA Authentication Agent for Web, you must configure SharePoint to use claims-based authentication. For more information, see "Configuring a New SharePoint Server 2010 Site to Use Claims-Based Authentication" on page 113.

Before setting up SSO access, verify that your setup is correct. When users attempt to access the portal, they must be challenged by both RSA SecurID and SharePoint.

Prepare to Set Up Single Sign-On to the SharePoint Server 2010

Before setting up single sign-on (SSO) access to the Microsoft SharePoint Server:

Note: The following steps are applicable for the Windows 2008 R2 SP1 (64-bit) domain controller.

1. On the domain controller, use Microsoft Active Directory to create a domain level user.
2. Using Active Directory, assign the right to delegate services:
   - On the domain controller, click **Start > Programs > Administrative Tools > Active Directory Users and Computers**.
   - In the left pane, double-click ***domain name***.
   - Double-click **Computers**, and in the right pane, double-click ***SharePoint server name***.
   - In the Delegation dialog box, select **Trust this computer for delegation to any service (Kerberos only)**, and click **OK**.

3. Using a text editor, open **web.config**, which is located in the document root directory of your web portal. Make sure the following entry is in the <appsettings> tag, before the </configuration> tag:

```
<appSettings>
<add key="SPS-EnforceIISAnonymousSetting" value="false"/>
</appSettings>
```

Next Step

"Configure the Web Agent for Single Sign-On to the Microsoft Office SharePoint Server 2007" on page 116.

Configure Single Sign-On to the SharePoint Server 2010

Perform the following steps to configure Single Sign-On to the Microsoft SharePoint Server:

1. Protect the SharePoint Site
2. Verify Authentication and Application pool settings for WebID Application
3. Verify the Application pool settings for the Site
4. Enable Single Sign-on

Protect the SharePoint Site

To protect the SharePoint site:

1. On the IIS Server machine, click **Start > Settings > Control Panel** > **RSA Web Agent**.
2. In the Connections pane of the IIS Manager, double-click ***server_name*** and click **Sites>SharePoint_site**, where *server_name* is the name of the IIS Server Machine and SharePoint_Site is the name of the site to be protected.
3. In the SharePoint_Site Home pane, double-click **RSA SecurID**.
4. In the RSA SecurID pane, select **Enable RSA SecurID Web Access Authentication**.
5. In the Actions pane, click **Apply**.

Next Step

"Verify Authentication and Application Pool Settings for the WebID Application."

Verify Authentication and Application Pool Settings for the WebID Application

To verify Authentication and Application pool settings for the WebID Application

1. Refresh the IIS Manager, click ***server_name***, and click **Sites > SharePoint_Site > WebID**.
2. In the WebID Home pane, double-click **Authentication**.

3. In the Authentication pane, do the following:
   - Select **Anonymous Authentication**, and click **Enable** on the Actions pane.
   - Select **Windows Authentication**, and click **Disable** on the Actions pane.
4. In the Connections pane, double-click ***server_name***, and then click **Sites > SharePoint_Site > WebID**.
5. Right click **WebID** and select **Manage Application > Advanced Settings**.
6. Select the Application pool as **RSA SecurID Pool**.

Next Step

"Verify the Application Pool Settings for the Site."

Verify the Application Pool Settings for the Site

To verify Application pool settings for the Site

1. In the Connection Pane of the IIS Manager, click ***server_name*** **> Application Pools**.
2. Click the SharePoint website's application pool and in the Actions pane, click **Advanced Settings**.
3. Under Process Model, click the **Identity** field and change the identity to **LocalSystem**.

Next Step

"Enable Single Sign-On."

Enable Single Sign-On

To enable single-sign on

1. Access **System32 > inetsrv > config > applicationHost.config**.
2. Search for the SecurIDModule in the file and add an entry for SecurIDSSOModule under that in the format <add name="SecurIDSSOModule" image="PATH_TO_ RSASinglesignon.dll" />,

   Note: RSASinglesignon.dll can be found inside the Web Agent installation directory.

3. In the Connections pane of IIS Manager, double-click ***server_name***, and click **Sites > SharePoint_Site**
4. In the SharePoint_Site Home pane, double-click **Modules**.
5. In the Actions pane, click **Configure Native Modules** and add the SecurIDSSOModule.
6. In the Connections pane of IIS Manager, double-click ***server_name***, and click **Sites > SharePoint_Site>WebID**.

7. In the WebID Home pane, double-click **Modules**.
8. In the Actions pane, select the **SecurIDSSOModule**, and click **Remove**.
9. Restart the IIS Web Server.

Note: When SSO is enabled, a user cannot sign in as another user on the protected site.

Next Step

"Configuring a New SharePoint Server 2010 Site to Use Claims-Based Authentication."

Configuring a New SharePoint Server 2010 Site to Use Claims-Based Authentication

In order for SharePoint Server 2010 to work with the single sign-on feature of RSA Authentication Agent for Web, SharePoint must be configured to use claims-based authentication. SharePoint Server 2013 uses claims-based authentication by default, but SharePoint Server 2010 does not. Changing an existing SharePoint site to use claims-based authentication, however, is irreversible. Therefore, RSA recommends creating a new, alternate SharePoint site configured to use claims-based authentication, while preserving the original site and configuration as a fallback.

The following procedures provide an example of how to configure a new SharePoint 2010 site to use claims-based authentication:

1. Create a Backup
2. Create an Alternate Site
3. Populate the Alternate Site
4. Restore SharePoint Data to the Alternate Site
5. Bind the Original SharePoint URL to the New Site

Create a Backup

To create a backup of your existing SharePoint site:

1. Click **Start > Internet Information Services (IIS) Manager > Sites**.
2. Right-click **SharePoint Central Administration** and then select **Manage Web Site > Browse**.
3. On the Central Administration home page, click **Backup and Restore**.
4. Under "Granular Backup," click **Perform a site collection backup**.
5. On the right hand side, make sure the **Site collection** is for the application that currently has your data.
6. Populate the file name, for example:

```
c:\temp\sharepoint80.bak
```

7. Click **Start Backup**.
   The following output appears:

```
Current Job
Status No operation in progress.
Previous Job
Status Succeeded
Completed 3/14/2014 9:12 AM
Duration (hh:mm:ss) 0:00:02
Recovery Step To recover the data, use the PowerShell
restore command Restore-SPSite.  For more details, type
Restore-SPSite -? at the PowerShell command prompt.
```

Create an Alternate Site

To create a new SharePoint site that uses claims-based authentication:

1. On the Central Administration home page, below "Application Management," click **Manage web applications**.
2. In the upper left toolbar click **New**.
3. Change the default Authentication from **Classic Mode Authentication** to **Claims Based Authentication**.
4. Select **Create a new IIS web site**. Complete settings as follows:
   - **Name**: For example, use **SharePoint - New**.
   - **Port**: Specify an unused port such as **8080** (this will be changed later to 80/443 after site is tested).
   - **Host Header**: Leave this blank.
   - **Path**: Specify a location that has space similar to the original you are replicating.
   - Make sure the "Application Pool" section has the user you want for running the pool—either **Network Service**, or a domain user that is used on the original SharePoint site.
   - Leave the defaults for all other settings.
5. Scroll to the bottom and click **OK**.

Populate the Alternate Site

To create an empty collection that you will overwrite with your backup:

1. On the Central Administration home page, click **Application Management**.
2. Under the Site Collections, click **Create site collections**.

Important: Make sure the "Web application" on the right is the **site:8080**.

3. Specify any **Title**.
4. Select a primary and secondary collection administrator.
5. Click **OK**.
6. Test the site to make sure you can log in with the primary or secondary collection administrator, prior to restoring the backup.

Restore SharePoint Data to the Alternate Site

To restore the backup to the newly created IIS / SharePoint instance:

1. Click **Start > All Programs > Microsoft SharePoint 2010 Products > SharePoint 2010 Management Shell**.
2. Run the command **Restore-SPSite -Identity http://*spssite* -Path *path to the .bak file* -Force**.

   For example:

   ```
   Restore-SPSite -Identity http://sharepoint.rsa.com:8080
   -Path c:\temp\sharepoint80.bak -Force
   ```

   If you do not know your SPSite, you can query it by running the following command:

   ```
   Get-SPSite
   ```

Bind the Original SharePoint URL to the New Site

After you are confident that the site is working on port 8080, follow the next procedure to change the alternate access mapping for your original site.

To change the alternate access mapping for your original site:

1. On the Central Administration home page, under System Settings, click **Configure alternate access mappings**.
2. Change the Default URLs to an invalid entry. For example, change **http://sharepoint.rsa.com to http://sharepoint.rsa.com.disable**.
3. Change the Alternate Site that was created to **http://sharepoint.rsa.com**.
4. Change the port bindings in IIS Manager as follows:
   a. Highlight the default site (typically **SharePoint - 80**).
   b. Click **Bindings** in the far right pane.
   c. Change the ports **80** and **443** to invalid ports such as **1080** and **1443**.
   d. Highlight the **SharePoint - New** instance on the left.
   e. Click **Bindings** in the far right pane.
   f. Change the port from **8080** to **80**.
   g. If using SSL, also add **443** and select the appropriate certificate.

   If you encounter issues after binding the original URL to the new site, you can revert just the bindings and alternate access mappings to use the original site.

   If there are no issues after binding the original URL to the new site, you have successfully configured SSO to the SharePoint Server 2010.

Configure the Web Agent for Single Sign-On to the Microsoft Office SharePoint Server 2007

To configure the Web Agent for single sign-on to the Microsoft Office SharePoint Server 2007:

- You must have Windows 2008 Server running at the Windows 2008 functional level on the environment domain controller. For more information, see your Microsoft Active Directory documentation.
- You must have unique user names across all domains. In addition, user names in the Active Directory Server must match the user names in the RSA Authentication Manager database.
- You must install Microsoft Office SharePoint Server 2007 SP2, and configure it to work with IIS.
- You must install the Web Agent, as described in Chapter 3, "Installing RSA Authentication Agent for Web for IIS 7.0, 7.5, and 8.0," and enable RSA web access protection on the portal web site. For instructions, see the Web Agent Help topic, "Enabling Web Access Authentication."

Before setting up SSO access, verify that your setup is correct. When users attempt to access the portal, they must be challenged by both RSA SecurID and SharePoint.

Prepare to Set Up Single Sign-On to the Microsoft Office SharePoint Server 2007

Before setting up single sign-on (SSO) access to the Microsoft Office SharePoint Server:

Note: The following steps are applicable for the Windows 2008 domain controller.

1. On the domain controller, use Microsoft Active Directory to create a domain level user.
2. Using Active Directory, assign the right to delegate services:
   - On the domain controller, click **Start > Programs > Administrative Tools > Active Directory Users and Computers**.
   - In the left pane, double-click ***domain name***.
   - Double-click **Computers**, and in the right pane, double-click ***SharePoint server name***.
   - In the Delegation dialog box, select **Trust this computer for delegation to any service (Kerberos only)**, and click **OK**.

3. Using a text editor, open **web.config**, which is located in the document root directory of your web portal. Make sure the following entry is in the <appsettings> tag, before the </configuration> tag:

```
<appSettings>
<add key="SPS-EnforceIISAnonymousSetting" value="false"/>
</appSettings>
```

4. Perform the following steps in Sharepoint 2007:
   a. Access the Sharepoint Central Administrator site.
   b. Click **Application Management > Application Security > Policy for Web Application**.
   c. Click **Add Users**.
   d. Select the site to be protected and enabled for Single Sign-On (SSO).
   e. Add **NT AUTHORITY\Authenticated Users** under Add Users.
   f. Click **OK**.

Note: To enable all the NT users for SSO, enter **NT AUTHORITY\Authenticated Users** under Add Users.

5. Perform the following steps only for 32bit Sharepoint 2007:
   a. Login as Administrator, to the site that has to be enabled for SSO.
   b. Click **Site Actions > Site Settings > Peoples and Groups**.
   c. Select the site's Members Group, and click **New > Add Users**.
   d. In the Add Users section, click **Add all authenticated Users**.
   e. Click **OK**.

Configure Single Sign-On to the Microsoft Office SharePoint Server 2007

Perform the following steps to configure Single Sign-On to the Microsoft Office SharePoint Server:

1. "Protect the SharePoint Site."
2. "Verify Authentication and Application pool settings for WebID Application."
3. "Verify the Application pool settings for the Site."
4. "Enable Single Sign-on."

Protect the SharePoint Site

To protect the SharePoint site:

1. On the IIS Server machine, click **Start > Settings > Control Panel** > **RSA Web Agent**.
2. In the Connections pane of the IIS Manager, double-click <*server_name* > and click **Sites>SharePoint_site**, where *server_name* is the name of the IIS Server Machine and SharePoint_Site is the name of the site to be protected.
3. In the SharePoint_Site Home pane, double-click **RSA SecurID**.
4. In the RSA SecurID pane, select **Enable RSA SecurID Web Access Authentication**.
5. In the Action pane, click **Apply**.

Verify Authentication and Application pool settings for WebID Application

To verify Authentication and Application pool settings for the WebID Application

1. Refresh the IIS Manager, click <*server_name*>, and click **Sites > SharePoint_Site >WebID**.
2. In the WebID Home pane, double-click **Authentication**.
3. In the Authentication pane, select **Anonymous Authentication**, and click **Enable** in the Actions pane.
4. In the Connections pane, double-click <*server_name*>, and then click **Sites > SharePoint_Site > WebID**.
5. Right click **WebID** and select **Manage Application > Advanced Settings**.
6. Select the Application pool as **RSA SecurID Pool**.

Verify the Application pool settings for the Site

To verify Application pool settings for the Site

1. In the Connection Pane of the IIS Manager, click ***<server_name>*** **> Application Pools**.
2. Click the Sharepoint website's application pool and in the Actions pane, click **Advanced Settings**.
3. Under Process Model, click the **Identity** field and change the identity to **LocalSystem**.

Enable Single Sign-on

To enable single-sign on

1. Access **System32 > inetsrv > config > applicationHost.config**.
2. Search for the SecurIDModule in the file and add an entry for SecurIDSSOModule under that in the format <add name="SecurIDSSOModule" image="PATH_TO_ RSASinglesignon.dll" />,

   Note: RSASinglesignon.dll can be found inside the WebAgent installation directory.

3. In the Connections pane of IIS Manager, double-click <*server_name*>, and click **Sites > SharePoint_Site**
4. In the SharePoint_Site Home pane, double-click **Modules**.
5. In the Action pane, click **Configure Native Modules** and add the SecurIDSSOModule.
6. In the Connections pane of IIS Manager, double-click **server_name**, and click **Sites > SharePoint_Site>WebID**.
7. In the WebID Home pane, double-click **Modules**.
8. In the Actions pane, select the **SecurIDSSOModule**, and click **Remove**.
9. Restart the IIS Web Server.

Note: When SSO is enabled, user cannot sign in as another user on the protected site.

Before You Uninstall the Web Agent

Before you uninstall the Web Agent, you must remove the RSA SingleSignOn module from the Microsoft Office SharePoint Server.

To remove the RSA SingleSignOn module from the Microsoft Office SharePoint Server:

1. On the IIS Server Machine, click **Start > Settings > Control Panel > RSA Web Agent**.
2. In the Connections pane, double-click ***server_name*** and click **Sites > *SharePoint_Site*** where *server_name* is the name of the IIS Server Machine and *SharePoint_Site* is the name of the SharePoint site which is enabled for SSO.
3. In the *SharePoint_Site* Home pane, double-click **Modules.**
4. From the list of modules, select **SecurIDSSOModule** and click **Remove** in the Actions pane.
5. Restart IIS.

Next Step

Uninstall the Web Agent. For instructions, see "Uninstall the Web Agent" on page 28.

8 Troubleshooting

RSA Authentication Manager Sdtest Utility

The sdtest utility provides information about RSA Authentication Manager, such as the configuration version, the server name and address, the number of client retries, and the client time-out period. In addition, this utility allows you to test authentication with the Authentication Manager.

For more information about **sdtest**, see the Help topic "Verifying the Status of Your Environment."

Authentication Attempts Logs

Authentication attempts are logged in the Windows Event Viewer.

The following table provides a list of possible error messages and their cause.

Error Message	Possible Cause and Solution
100:Access denied. The RSA ACE/Server rejected the Passcode. Please try again.	The first time an authentication occurs after the Web Agent has been installed on the web server, a node secret is generated by RSA Authentication Manager and sent to the web server. This error is received if the node secret file is missing or the node secret on the Authentication Manager and the web server do not match. The node secret will be generated inside the WebAgent installation directory. The name of the file is **securid**. Contact your RSA Authentication Manager administrator. Frames are not supported if you enable the option **Use RSA Token for Cross-Site Request Forgery Protection**. If you want to use frames, and you have enabled the **Use RSA Token for Cross-Site Request Forgery Protection** option, you must also enable **Use JavaScript Pop-Up Window to Authenticate in Frames**.
Unexpected RSA Authentication Agent error 103. Please try again.	This error is received when there are network problems. Contact your RSA Authentication Manager administrator.
AceInitialize Failed during acetest authentication.	The **sdconf.rec** file is missing. Obtain an **sdconf.rec** file from your Authentication Manager administrator. Place the file inside the WebAgent installation directory. Restart the web server.
The page cannot be found.	The requested page may not be present.
RSA Securid Error. 106: Web server too busy. Please try again later.	This error may occur when communication to RSA Authentication Manager is down or the **sdconf.rec** file is missing. Contact your RSA Authentication Manager administrator.
Unexpected authentication error.	This error may occur when authenticating using the **acetest** utility. Communication to the Authentication Manager is down. Contact your RSA Authentication Manager administrator.

Error Message	Possible Cause and Solution
The Page cannot be displayed.	There are two possible causes for this error message: • Communication to the web server is down. • The web server was started without SSL. Therefore, the Redirect Secure feature in the Web Agent is disabled. The best solution is to restart the web server with SSL. You could also have users access the page with an **https** request.
RSA Web Access Authentication Extension Error. RSA Web Access Authentication: Internal server configuration error.	The path to the templates is invalid. Verify the correct path in the Web Agent configuration.
For Multi-Domain Authentication: Requesting authentication from server http://server Denied.	Make sure that the same domain secret exists on each web server within the multiple domain area.
Access Denied. Test authentication succeeds but access is denied when the user tries to log on to access a protected page.	Make sure that you log on with administrative privileges to the system on which the IIS web server is running.
Outlook Web Access gives 404 login timeout.	Make sure that the WebID virtual application under the Default Web Site has anonymous authentication enabled.
Modal Popup is not displayed after cookie expiry	Make sure that the application pool of the protected site is in Integrated Mode. Use DebugView to get the Modal Popup logs.
SecurID Error. Error generating HTML page.	Make sure that you configure the character sets properly.
500 Internal Server Error When the user browses to the protected page it sends back 500 Internal Server Error.	The reason could be some of the web agent intialization operations would have failed. Enable WebAgent logs to get a detailed error. Also make sure the RSA Config Service is running.
SSO is enabled, but still user is prompted for Windows authentication.	Make sure the WebID virtual application under the SSO enabled site has Anonymous Authentication enabled using IIS Manager. Enable WebAgent logs to get a detailed error. Also make sure the 'RSA Pipe Service' is running.

Error and Event Viewer Log Messages

The Web Agent logs events in the Windows Event Viewer Application Log under the source ACECLIENT on Windows machines. This section lists all error and event messages alphabetically.

ACECheck processing error for userid *user name.*

If the **ACECheck** function returns an error, an Authentication Manager time-out or some other communications error has occurred.

ACEClose processing error *errornumber.*

If the **ACEClose** function returns an error, an Authentication Manager time-out or some other communications error has occurred.

ACENext processing error for userid *user name.*

If the **ACENext** function returns an error, an Authentication Manager time-out or some other communications error has occurred.

ACEPin processing error for userid *user name.*

If the **ACEPin** function returns an error, an Authentication Manager time-out or some other communications error has occurred.

All users challenged. Passcode required.

The specified service is configured to challenge all users of the service with RSA SecurID. The **Challenge** control on the Web Agent control panel is set to **All Users**. The user was challenged to enter a passcode.

An error occurred when accessing the Metabase.

The Web Agent failed while reading from or writing to the Metabase. If this message is displayed, first make sure you have the correct administrative privileges, and then restart the agent host. If the error persists, reinstall the Web Agent to override the existing settings. If that does not resolve the situation, you will have to uninstall, and then reinstall the Web Agent.

Authentication failure.

The subject described in the Event Detail did not authenticate successfully and was therefore refused access.

Authentication Manager: Access Denied.

The user did not enter a valid RSA SecurID passcode.

Authentication Manager: RSA Authentication Agent Library Failure.

The Web Agent could not load the **aceclnt.dll** library file. The file is either corrupted, has been moved to another directory, or has been deleted from the system.

If the **aceclnt.dll** file is no longer on the system, you must reinstall the Web Agent.

Authentication Manager: Cannot resolve address IP address to a host name. The data is the Windows Sockets error.

The Web Agent Network authentication proxy service attempted to get the workstation name, but the service could not resolve the numeric IP address to a host name because the name was not found in DNS. Make sure DNS is working properly on your network.

Authentication Manager: Failed Authentication Attempt. User *user name*.

The user entered an invalid passcode, causing the "bad passcode" counter to be incremented by one. If this counter exceeds the configured number of bad passcodes, the user's token will be deactivated until an administrator intervenes.

The number of allowed bad passcodes is stored in the **sdconf.rec** file and can be viewed by running the **sdtest** program.

Authentication Manager: Invalid RSA Authentication Manager configuration. User *user name*.

The **sdconf.rec** file is not valid. The file is either corrupted, has been moved to another directory, or has been deleted from the system.

To correct the problem, get a new copy of **sdconf.rec** from your RSA Authentication Manager administrator.

Authentication Manager: New PIN Accepted. User *user name*.

The user successfully associated a new PIN with his or her token.

Authentication Manager: New PIN Rejected. User *user name*.

The user did not successfully associate a new PIN with his or her token. If the user is attempting to create his or her own PIN, make sure the user understands the PIN length and syntax parameter settings for your Authentication Manager.

Authentication Manager: Next Tokencode Accepted. User *user name*.

After entering a series of bad passcodes, the user was prompted to enter the next tokencode from his or her token. The next tokencode was valid and the user was authenticated successfully.

Authentication Manager: User Canceled New PIN Mode. User *user name*.

The user was prompted to associate a new PIN with his or her token, but the user did not complete the new PIN procedure. Make sure the user understands how to use his or her token in New PIN mode.

Authentication Manager: User Canceled Transaction. User *user name*.

The user was prompted to authenticate, but then canceled out of the **Enter passcode** dialog box. This is a purely informational message.

Authentication Manager: User I/O Timeout. User *user name*.

Because the user waited too long at the **Enter passcode** prompt, the Web Agent canceled the transaction.

Authentication Manager: User Interface Library Failure.

The Web Agent could not load the **sdui.dll** library file. The file is either corrupted, has been moved to another directory, or has been deleted from the system.

If the **sdui.dll** file is no longer on the system, you must reinstall the Web Agent.

Cannot create socket during initialization in RSA SecurID Authentication.

Socket services may not have started. Check the Event Log to find out if there is a problem with the network card or the TCP/IP services.

In addition, open the Authentication Manager machine Network control panel, click the **Services** tab, and make sure **Simple TCP/IP Services** are installed. If they are not, add the **Simple TCP/IP Services**.

Cannot create socket during initialization.

Make sure echo services are running on your Authentication Manager.

Open the Authentication Manager machine Network control panel, click the **Services** tab, and make sure **Simple TCP/IP Services** are installed. If they are not, add the **Simple TCP/IP Services**.

Cannot load RSA Authentication Agent DLL.

Test cannot find **aceclnt.dll** in the **\system32** directory. You must install the Web Agent software in repair mode.

Cannot read server private key from file.

Make sure you have copied both the ***hostname*.crt** and the ***hostname*.key** files to the import location. In addition, make sure you are entering the certificate password correctly.

Connection attempt failed.

This results from a bad server certificate. When a user attempts to mount a network drive or printer or to test authentication in silent mode, this message is logged. During silent mode, the drive will mount successfully.

Cookie rejected. Cached client info does not match.

If a user is using more than one workstation, this message appears each time the user switches from one workstation to another.

Cookie rejected. Cookie failed MD5 test.

An unauthorized user has attempted to access the web server with a bogus web access authentication cookie.

Cookie rejected. Expired cookie. User Name *user name.*

A web access authentication cookie has expired in response to the time-out values defined in the web access authentication properties sheet.

Could not initialize RSA Authentication Agent.

Will be preceded by a number of Web Agent error messages, such as **Cannot find sdconf.rec**. Try reinstalling the **sdconf.rec** file.

Could not initialize Cookie Cache.

A memory error has occurred within an internal function. Your web server may be overloaded; you may need more physical memory.

Could not open HTML template *filename.*

The HTML template file is missing.

Also check the security settings for the file. Make sure the account that the web server is running has Full Access privileges to the HTML file.

Could not open registry key *keyname.*

A serious registry corruption has occurred. You must reinstall the Web Agent.

Could not query value *valuename.*

If you have enabled the Domain Cookies feature without setting a domain secret, you might get a **valuename DomainData** message, followed by a **Domain cookies are disabled** message.

Could not read HTML template *filename.*

The HTML template file is missing.

Could not resolve hostname *hostname.*

The DNS function of the web server is configured incorrectly. Domain cookies cannot be used until the configuration is corrected.

Failed authentication for userid *user name*.

The Authentication Manager did not grant the user access. The most common causes for this are wrong user name or an invalid passcode.

Failed to create event.

These are internal errors. The machine may not have enough free resources to add RSA SecurID authentication. Consider moving the service or services from this machine to another one.

Failed to create service thread, aborting.

There were too many other processes running, so the service did not start.

Failed to find required service WINSOCK.

The Windows socket interface was not found. Check the event log to find out if there is a problem with WINSOCK. Ensure that TCP/IP has been enabled on the machine.

File incorrect size: sdconf.rec.

It is likely that the **sdconf.rec** file was not copied in binary or ftp mode. Ask the Authentication Manager administrator for a new copy of **sdconf.rec**.

File not found: aceclnt.dll.

Software may have been installed incorrectly or **aceclnt.dll** may have been deleted.

File not found: sdconf.rec.

The **sdconf.rec** file was either removed or never copied from Authentication Manager. Ask the Authentication Manager administrator for a new copy of **sdconf.rec**.

Initialization of sdagent.dll library failed.

Users see this error message when there is no root certificate installed on the computer. To correct this problem, obtain a copy of the root certificate and reinstall the Web Agent.

New PIN accepted for userid *user name*.

Authentication Manager verified the RSA SecurID user's new PIN.

New PIN rejected for userid *user name*.

The PIN was rejected by Authentication Manager. The user must reauthenticate to set the PIN. Check the Activity Log on Authentication Manager.

New PIN requested from userid *user name*.

Authentication Manager has prompted the RSA SecurID user to create his or her own PIN or receive a system-generated PIN.

Next code accepted for userid *user name*.

The Next Tokencode was accepted by Authentication Manager and access was granted.

Next code rejected for userid *user name*.

The user must attempt to authenticate again.

Next code requested from userid *user name*.

The user's token was in Next Tokencode mode and Authentication Manager requested the second tokencode.

No cookie or corrupted information.

This message will appear each time a new user logs on to the web server.

Out of memory in *functionname*.

A memory error has occurred within an internal function. Your web server may be overloaded or you may need more physical memory.

Passcode Incorrect (multiple instances of).

If you have RAS authentication and web authentication enabled on a machine, the Web Agent could be sending the encrypted RAS authentication passcode through the wrong IP address. Verify the IP addresses of each service and the client nodes on the Authentication Manager for possible addressing errors.

Remote authentication denied for userid *user name*.

Another web sever within the DNS domain has requested authentication of user *user name* with a domain cookie and was not given access.

Check the security settings for the file. Make sure the account that the web server is running has Full Access privileges to the HTML file.

Remote authentication given for userid *user name*.

Another web server within the DNS domain has requested authentication of user *user name* with a domain cookie and was given access.

Remote authentication received deny for userid *user name*.

A web server requesting authentication of a domain cookie was rejected.

Remote cookie rejected. Cookie failed MD5 test.

An unauthorized user has attempted to access the web server with a bogus web access authentication domain cookie.

Remote: NT/RAS not available.

The machine does not meet one or more of the system or software requirements needed to enable authentication of RAS connections.

RSA Authentication Agent initialization failed.

The Web Agent cannot make the connection to Authentication Manager. Make sure that the Authentication Manager and the network are operational and that all network interface cards and cables are properly installed and in good condition.

RSA Authentication Manager is not responding.

There is a network communications problem between the Authentication Manager and Web Agent, the server cannot be found (because the IP address is wrong, for example), or the Authentication Manager daemon is not running.

RSA Authentication Manager is not responding. Run CLNTCHK to verify port and IP address of RSA Authentication Manager.

There is a network communications problem between the Authentication Manager and the Web Agent, the Authentication Manager cannot be found (because the IP address is wrong, for example), or the Authentication Manager daemon is not running.

Session Manager: Failed to Create Server Thread.

There are too many server threads running (too many users connecting at once). Try widening the intervals at which users attempt to log on.

Session Manager: Failed to Create Socket.

This message results from a memory shortage or WINSOCK error. The cause might be too many users connecting to the server at the same time.

Session Manager: Failed to Resolve Hostname.

Most likely a configuration error. The machine that is connecting has no DNS or NetBIOS name, or has an invalid IP address. Make sure your network is configured properly and that your host file entries are correct.

Session Manager: Not Enough Memory.

The system does not have enough physical RAM, or there were too many other processes running in memory. If you receive this message often, add more physical memory to the computer.

Session Manager: Winsock startup error.

The Microsoft Windows Sockets failed to initialize. To troubleshoot WINSOCK problems, consult your Microsoft networking documentation.

Successful authentication.

The subject described in the Event Detail authenticated successfully and was granted access to the system.

The access control entry for *filename* was not found.

The Windows security entry for this file is corrupted. If you suspect that the ACL has become corrupted, see the Microsoft Windows Help, or contact Microsoft technical support.

The discretionary Access Control List for *filename* was not found.

The Windows security entry for this file is corrupted. If you suspect that the ACL has become corrupted, see the Microsoft Windows Help, or contact Microsoft technical support.

The Help for this program was created in Windows Help format, which depends on a feature that isn't included in this version of Windows. However, you can download a program that will allow you to view Help created in the Windows Help format.

The user has to download and install the Windows Help program (WinHlp32.exe) for Windows Server 2008 R2.

The local group *groupname* does not exist.

Indicates an incorrect implementation of the web access authentication Group Security feature.

The Web Agent could not locate one of the groups listed in the user's Shell field on the local machine. Make sure you created and named the group properly in the Windows User Manager.

The security descriptor could not be found. The file may not exist: *filename*.

A user requested a URL that does not resolve to a file on the machine. Make sure the user is entering the URL correctly.

The user connected to port *portname* has been disconnected...

There is a problem with RSA SecurID authentication. See the Event Detail topic for more specific information.

The user *server/user name* disconnected from port *portnumber*.

The user closed the connection on the specified port.

The user *server/user name* connected on port *portnumber* on date at time and disconnected on date at time. . .

A normal Web Agent disconnection has occurred.

The user *user name* has connected and been authenticated on port *portnumber*.

A normal (authenticated) Web Agent-Server connection occurred.

Unable to open Office document from the SharePoint server using Microsoft Office 2003

The web access authentication persistent cookie has expired. You need to log on to the SharePoint Server with your SecurID credentials.

Unexpected error from RSA Authentication Agent.

The value returned by Authentication Manager is not valid.

User <blank> canceled out of RSA SecurID Authentication routine.

The user canceled without entering a user name.

User I/O Timeout-User took too long to respond.

The system timed out after waiting for a response from the user.

User *user name* canceled out of New PIN routine.

The user canceled the authentication attempt.

User *user name*: ACCESS DENIED. ATTEMPT 1.

The user was denied access. Check the Authentication Manager Activity Log for the specific reason.

User *user name*: Access denied. Attempt to use invalid handle. Closing connection.

An internal error occurred. If the message recurs, call RSA Customer Support.

User *user name*: ACCESS DENIED. Next Tokencode failed.

The user must attempt to authenticate again.

User *user name*: ACCESS DENIED. Server signature invalid.

This message indicates that the identity of Authentication Manager could not be verified by the client. If you see this message, call RSA Customer Support.

User *user name*: ACE Check Error: Invalid group SID. Passcode required.

The user's group SID did not contain a valid group name. The user was challenged for an RSA SecurID passcode.

User *user name*: canceled out of Next Tokencode routine.

The user canceled out of the Next Tokencode process.

User *user name*: canceled out of RSA SecurID Authentication routine.

The user canceled after entering a user name.

User *user name*: Domain not found. User challenged for passcode.

The user may have entered the domain name incorrectly and will be challenged for a passcode.

User *user name*: New PIN accepted.

The user's New PIN was verified.

User *user name*: New PIN rejected.

The PIN was rejected by the Authentication Manager. The user needs to reauthenticate to set the PIN. Check the Authentication Manager Activity Log.

User *user name*: Not found. User challenged for passcode.

The user is unknown to the system, but the system still challenges the user for a passcode.

User *user name*: Successfully logged on with Next Tokencode.

The Next Tokencode was accepted by Authentication Manager and access was granted to the user.

WebAgent Logging

You can use the logging or tracing option to troubleshoot WebAgent problems. For more information on WebAgent logging see "Web Agent Logging" on page 63.

Node Secrets

The node secret is a symmetric encryption key that RSA Authentication Manager and the Web Agent use to encrypt and decrypt packets of data as they travel across the network. For agents that are based upon the UDP protocol, the node secret is stored in both the Authentication Manager database and in a file on the Web Agent host. For agents that are based upon the TCP/IP protocol, a node secret file is optional, and the location is specified in the **rsa_api.properties** file. Instead of a node secret, a dynamically negotiated key is used to encrypt the channel along with a strong encryption algorithm.

For UDP-based agents, if the node secret is missing on either the RSA Authentication Manager server or the Web Agent host, clear the node secret in the other location. If the node secret files on the Authentication Manager and the Web Agent host do not match, clear the node secret in both locations. After you clear the node secret, you must generate a new node secret.

Clear the Node Secret From RSA Authentication Manager

If the node secret does not match on the RSA Authentication Manager and the Web Agent host, or if the node secret is missing from the Web Agent host, you must clear the node secret from RSA Authentication Manager. For example, if you reinstall the Web Agent, the node secret is missing from the Web Agent host.

To clear the node secret on the RSA Authentication Manager server:

1. In the Authentication Manager Security Console, click **Access > Authentication Agents > Manage Existing**.
2. Locate the affected agent host and select **Manage Node Secret** from the drop-down menu.
3. Select the **Clear the node secret** checkbox, and then click **Save**.

Next Steps

- If there is a node secret on the Web Agent host, see "Clear the Node Secret on the Web Agent Host Machine."
- If the Web Agent host does not have a node secret, follow the procedure "Generate a New Node Secret."

Clear the Node Secret on the Web Agent Host Machine

If the node secret does not match on the RSA Authentication Manager instance and the Web Agent host, or if the node secret is missing from the Authentication Manager, you must clear the node secret from Web Agent host. For example, if you install a new Authentication Manager instance and add an existing Web Agent, the node secret is missing from Authentication Manager.

Before You Begin

If there is a node secret on the Authentication Manager, see "Clear the Node Secret From RSA Authentication Manager."

To clear the node secret from the Web Agent host machine:

1. Log on to the Web Agent host machine and locate the node secret file, **nodesecret.rec,** in the **\Program Files\RSA Security\RSAWebAgent** directory.
2. Rename or delete the node secret file.
3. The node secret is also stored in the web server cache. Restart the web server to clear the node secret from the cache.

Next Step

"Generate a New Node Secret."

Generate a New Node Secret

To generate a new node secret:

1. Test authentication from RSA Web Agent to generate the node secret file. For instructions, see "Perform a Test Authentication" on page 23.
2. Check your authentication logs and ensure a new node secret has been sent.
3. Restart your IIS server so that the RSA Web Agent can read the node secret file.

Known Issues Using Third-Party Software

Browser Issues

A user could experience the following browser issues while accessing protected pages:

- Both Internet Explorer and Firefox maintain a single browser session across multiple instances of the browser. If a user has successfully authenticated onto a protected resource in one instance of the browser, as long as that instance remains open, all other instances of the browser share the same authentication cookie. Therefore, the user does not have to authenticate again in any other instances of the browser to access protected resources.

  To exit the browser session, users must close all instances of the browser.

- When a user clicks the logoff URL, it automatically invalidates the user's web access authentication cookies and prompts the user to authenticate.

Microsoft Exchange Server ActiveSync in a Single Machine Environment

If you protect Exchange 2007 SP2 or 2010 SP1 with SecurID, you cannot use ActiveSync, regardless of its protection status. To use ActiveSync on the same machine as Exchange 2007 SP2 or 2010 SP1, you must disable protection for the Exchange 2007 SP2 or 2010 SP1 directory.

Wireless Devices

Web Agent and Authentication Manager administrators must be aware of the following items pertaining to RSA SecurID web authentication. A user could experience these scenarios when using a cellular phone equipped with a microbrowser to access protected URLs.

- If your environment includes a GSM network, your WAP connection needs to be in connection mode. Multiple domain environments require that handset devices and gateways support the receipt of cookies from multiple domains.
- Requiring an SSL connection to protected URLs creates a more secure environment. For ease of use, you can configure the Web Agent to automatically redirect the URL request to a secure connection. However, not all microbrowsers support automatic redirection. In this case you need to disable the redirect option. A web page is then presented with a link to the secure connection that users must manually click.
- When the Web Agent is configured to use a single web page for entering the user name and passcode, the LCD on certain devices may appear to be using separate pages, one for entering the user name and a second page for entering the passcode. However, the microbrowser on the device is sending the data all at once, unless you have specifically enabled the **Use Separate User Name and Passcode Pages** option in the Web Agent.

- When **Name Locking** and **Use Separate User Name and Passcode Pages** are enabled in the Web Agent, and the carrier signal is lost after transmitting the user name, the user name is locked in the Web Agent database until the Name Lock time-out expires. Instruct the user to authenticate again after the Name Lock expiration time.

  Note: The name locking feature offers security tradeoffs that may or may not be appropriate for your environment. By enabling name locking, a 30-second lock is created on RSA Authentication Manager 6.1.2. As with any lockout mechanism, this can be used to prevent a valid user from authenticating by continually relocking the valid user name.

  Displaying the user name and passcode prompts as separate pages, necessary to fully receive the security offered by name locking, comes with security tradeoffs that may or may not be appropriate for your environment. When the prompts are separated onto different pages, the Web Agent creates new sessions while submitting the user names. As with most session management systems, this creates the possibility that all sessions will be reserved, and new authentication attempts will be rejected until old sessions complete.

- It can be difficult for users to enter the PIN and tokencode within the designated time limit (typically 60 seconds) before the tokencode changes again. Most WAP devices by default are set up for alphanumeric entries. That means the user must scroll through the letters assigned to a button before reaching the numbers. Because tokencodes are always numeric, instruct users to switch their phone to numeric entry, if their phone allows this, only after entering the PIN.
- Some gateways have very specific size limitations for WML templates. You may need to reduce the amount of information provided in the templates.
- To enable the **Redirect HTTP Connections to Secure Server** option, the cellular device and its gateway must allow for SSL redirection. RSA recommends that you instruct the user to refer to the documentation provided with his or her cellular device.
- Devices that allow for an image display may, during the course of an authentication, display the status “Failed” for several seconds (depending on the speed of the microbrowser) until an image is shown on the LCD that indicates success. In these instances, the user should wait for several seconds until the success image is shown. If, however, the “Failed” status message is displayed for a substantial amount of time, it is most likely valid, and the user should attempt authentication again.

Multiple Domain Issues

When connecting to multiple domains, a web page that shows the domain URL and the success or failure of the connection opens. In some environments, the “Success” and “Failed” images do not appear in the web page. If this occurs, do not use https when you input domains in your multiple domain list, just use http. As far as RSA has been able to determine, this problem occurs only when there is no valid certificate on the web server and only in some versions of Internet Explorer. Therefore, this problem occurs only in a test environment.

Important: All web servers protected using the multiple domain option should be configured to use only SSL(not plain http).

Note: All servers protected using multiple domain authentication should have the same webID URL. If you have changed the default webID URL value in any of these servers (default value is **/webauthentication**) then you must change it in all the servers, else the feature will not work.

If you have configured some URLs protected by the Web Agent for multiple domain single sign-on access, single sign-on will not work if you use either the Internet Explorer 7.0 or 8.0 browsers even if you have added the URLs to the trusted zone in Internet Explorer. When you access one URL and successfully authenticate, you will still be challenged when accessing the other URL configured for SSO.

To avoid this problem, you must configure the following settings in the Internet Explorer 7.0 or Internet Explorer 8.0 browser in addition to allowing third-party cookies:

1. Click **Tools** > **Internet Options**.
2. In the Internet Options dialog box, click the **Privacy** tab.
3. Click **Sites**.
4. In the Per Site Privacy Actions dialog box, type the URL that you want to configure for multiple domain single sign-on access in **Address of Web site** text box, and click **Allow**.
5. Repeat step 4 for all the URLs participating in single sign-on.
6. Click **OK** in the Per Site Privacy Actions dialog box.
7. Click **Apply** > **OK**.

The following issues might occur when using multiple domain access on wireless devices:

- When Multi-Domain Access is enabled in the Web Agent, a list of URLs for the domains is displayed. WAP devices that allow for an image display may, during the course of an authentication, display the “Failed” status for several seconds (depending on the speed of the microbrowser) until an image is shown on the LCD that indicates success. In these instances, the user should wait for several seconds until the success image is shown. However, if the “Failed” status message remains for a substantial amount of time, it is most likely valid, and the user should attempt to authenticate again.
- When Multi-Domain Access is enabled, the Web Agent attempts to get an image from each of the domains to see if it has connected. With some cell phones, the image is displayed, but the connection was never actually made. When the user has authenticated once in a multiple domain environment and then attempts to access a URL in another domain, the user is asked to authenticate again rather than having single sign-on.
- To work around this issue, enable the **Using Text Link Authentication Mechanism for Multi-Domain WML Access** configuration option. For more information, see “Configure Advanced Settings” on page 36.

Issues during co-existence of Web Agent with Windows Agent

When the Web Agent for IIS and the RSA Windows Agent coexist, an issue is encountered when the Windows Agent is uninstalled. On uninstall of the Windows Agent the Web Agent for IIS is disabled.

The workaround for this is, the Web Agent should be repaired after uninstalling the Windows agent.

Disable the RSA Response Interceptor Module

You can disable the RSA Response Interceptor module to avoid generating network traffic in a deployment that only uses Microsoft SharePoint Server. After disabling this module, you can remove the RSA Response Interceptor module entries that the Web Agent installer created in your **web.config** files. After you disable this feature, the modal popup privacy screen does not display when persistent cookies expire.

The RSA Response Interceptor module provides useful information in a Microsoft Exchange Server environment.

To disable the RSA Response Interceptor module:

1. Log on to the machine as an administrator.
2. Open the Windows Command Prompt, for example, click **Start > Search**, type **cmd**, and press ENTER.
3. Change directories to the location where you downloaded and extracted the software, for example, **C:\Program Files\RSA Security\RSAWebAgent**. Type:

   ```
   cd C:\Program Files\RSA Security\RSAWebAgent
   ```

   and press ENTER.
4. Disable the RSA Response Interceptor module. Type:

   ```
   setup.exe /v"NO_RESPONSE_INTERCEPTOR=1"
   ```

   and press ENTER.

   Note: Do not enter a space between the “/v” option and the "NO_RESPONSE_INTERCEPTOR=1" argument.
5. Remove the RSA Response Interceptor module entries from all of the **web.config** files in your SharePoint Server site. Type:

   ```
   ConfigUpdateHelper.exe c
   ```

   and press ENTER.

Uninstalling the Web Agent

You can uninstall the Web Agent through the Windows Control Panel. Depending upon whether you have installed Microsoft Exchange Server or Microsoft Office SharePoint Server and whether single sign-on (SSO) is enabled, additional procedures might be required.

The following table lists the required procedures for each type of deployment.

Deployed Product Combination	Procedures
Web Agent	In Chapter 3, "Installing Authentication Agent for Web," see "Uninstall the Web Agent" on page 28.
Web Agent with Exchange Server 2013 without SSO	Follow these procedures in Chapter 3, "Installing Authentication Agent for Web:" 1. "Uninstall the Web Agent" on page 28. 2. "Reconfigure Microsoft Exchange Server 2013 After Uninstalling Web Agent" on page 28.
Web Agent with Exchange Server 2010 or 2007 without SSO	Follow these procedures in Chapter 3, "Installing Authentication Agent for Web:" 1. "Uninstall the Web Agent" on page 28. 2. "Reconfigure Microsoft Exchange Server 2010 or 2007 After Uninstalling Web Agent" on page 29.
Web Agent with Exchange Server 2013 with SSO	Follow these procedures: 1. In Chapter 6, "Configuring the Web Agent for Single Sign-On to Outlook Web Access," see the following: a. "Before You Uninstall the Web Agent" on page 93. b. "Reconfigure Microsoft Exchange Server 2013" on page 94. 2. In Chapter 3, "Installing Authentication Agent for Web," see the following: a. "Uninstall the Web Agent" on page 28. b. "Reconfigure Microsoft Exchange Server 2013 After Uninstalling Web Agent" on page 28.

Deployed Product Combination	Procedures
Web Agent with Exchange Server 2010 or 2007 with SSO	Follow these procedures: 1. In Chapter 6, "Configuring the Web Agent for Single Sign-On to Outlook Web Access," see the following: a. "Before You Uninstall the Web Agent" on page 93. b. "Reconfigure Microsoft Exchange Server 2010 or 2007" on page 95. 2. In Chapter 3, "Installing Authentication Agent for Web," see "Uninstall the Web Agent" on page 28.
Web Agent with SharePoint Server 2013 without SSO	In Chapter 3, "Installing Authentication Agent for Web," see "Uninstall the Web Agent" on page 28.
Web Agent with SharePoint Server 2010 without SSO	In Chapter 3, "Installing Authentication Agent for Web," see "Uninstall the Web Agent" on page 28.
Web Agent with SharePoint Server 2013 with SSO	Follow these procedures: 1. In Chapter 7, "Configuring the Web Agent to Microsoft Office SharePoint Server," see "Before You Uninstall the Web Agent" on page 119. 2. In Chapter 3, "Installing Authentication Agent for Web," see "Uninstall the Web Agent" on page 28.
Web Agent with SharePoint Server 2010 with SSO	Follow these procedures: 1. In Chapter 7, "Configuring the Web Agent to Microsoft Office SharePoint Server," see "Before You Uninstall the Web Agent" on page 119. 2. In Chapter 3, "Installing Authentication Agent for Web," see "Uninstall the Web Agent" on page 28.

Index