RSA Authentication Agent 7.2 for Microsoft Windows Group Policy Object Template Guide

Contact Information

Go to the RSA corporate web site for regional Customer Support telephone and fax numbers**:** **www.rsa.com**

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.rsa.com/legal/trademarks_list.pdf**.

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 in the thirdpartylicenses.pdf file.

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.

November 2012

Contents

Preface

About This Guide

This guide describes how to use Group Policy Object (GPO) templates to manage RSA Authentication Agent 7.2 for Microsoft Windows. It is intended for administrators and other trusted personnel. Do not make this guide available to the general user population.

RSA Authentication Agent GPO Template Documentation

For more information about RSA Authentication Agent for Microsoft Windows, 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 on RSA SecurCare Online at **https://knowledge.rsasecurity.com**.

***Installation and Administration Guide*.** Describes detailed procedures about how to install, configure, and manage RSA Authentication Agent 7.2 for Microsoft Windows.

RSA Authentication Agent (RSA SecurID) Help. Describes standard and administrator tasks performed in the RSA Control Center. Standard Help topics include how to copy the tokencode, view logon settings, and manage offline days. Administrator Help topics include how to test authentication, override an IP address, challenge users, enable tracing, clear the node secret, and view the server environment. To view Help, click the **Help** option in the RSA Control Center.

Related Documentation

For more information about products related to RSA Authentication Agent for Microsoft Windows, see the following:

RSA Authentication Manager documentation set. The full documentation set for RSA Authentication Manager 6.1 or 7.1. To access a documentation set, go to **http://knowledge.rsasecurity.com**.

Support and Service

RSA SecurCare Online	https://knowledge.rsasecurity.com
Customer Support Information	www.emc.com/support/rsa/index.htm
RSA Solution Gallery	https://gallery.emc.com/community/marketplace/rsa?view=overview

RSA SecurCare® Online offers a knowledgebase that contains answers to common questions and solutions to known problems. It also offers information on new releases, important technical news, and software downloads.

The RSA Solution Gallery provides information about third-party hardware and software products that have been certified to work with RSA products. The gallery includes Implementation Guides with step-by-step instructions and other information about interoperation of RSA products with these third-party products.

Before You Call Customer Support

Make sure that you have direct access to the computer running RSA Authentication Agent 7.2 for Microsoft Windows.

Please have the following information available when you call:

- ❑ Your RSA Customer/License ID. RSA Authentication Agent for Microsoft Windows is free to customers. Use the RSA Authentication Manager software version number as your Customer/License ID. To find this number:

  In the RSA Authentication Manager 6.1 Security Console, click:
  Help > About RSA Security Console > See Software Version Information.

  In the RSA Authentication Manager 7.1 Security Console, click:
  Help > About Database Administration > License Info
- ❑ The make and model of the machine on which the problem occurs.
- ❑ The name and version of the operating system.

1 Group Policy Object Templates

This chapter includes the following topics:

Group Policy Object Templates

RSA Group Policy Object (GPO) templates allow you to manage RSA Authentication Agent 7.2 for Microsoft Windows. The templates are part of the RSA Authentication Agent 7.2 software kit. The GPO templates allow you to:

- Manage policy settings for local authentication.
- Set the logon requirements for Windows operating systems.
- Manage password synchronization.
- Set an expiration warning message for RSA SecurID 800 Authenticators.

RSA Group Policy Object templates allow you to apply policy settings to the appropriate computers. Typically, you load the templates into the Group Policy Object Editor on your domain controller and then define the authentication policy settings in the templates. Each workstation within the domain automatically downloads the settings and loads them into the Microsoft Windows registry. Windows stores them in the Registry Editor keys under HKEY_LOCAL_MACHINE > Software > RSA > Policies.

Note: In addition to installing and defining the templates on your domain controller, if you want to use the templates on Windows computers that are not part of the domain, you must separately install the templates on those computers and define the template settings using the Local Group Policy Editor.

You can use the default policy settings or change the settings. If you change the policy settings, the new settings override any previous settings. In domain environments, all computers wait for specified refresh intervals before updating their settings. When the refresh process ends, the settings associated with the templates are loaded into the Windows registry.

Enforce the policy on the domain controller. Otherwise, users with administrator privileges can change the settings and the defaults in the local registry.

Template Files

You can install the following template files to manage the Authentication Agent. They are organized by operating system compatibility.

All Windows operating systems:

- **RSA_Authentication_Agent.adm**
- **RSA_Authentication_Agent_Password_Synchronization.adm**

Note: RSA_Authentication_Agent_Password_Synchronization.adm applies to domain controllers only.

- **RSA_SecurID_Expiration_Warning.adm**
- **RSADesktop_VerifyRSAComponents.adm**

Windows Vista, Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2, or Windows Server 2012 templates:

- **RSACredProviderFilter_Microsoft.adm**
- **RSACredProviderFilter_SecurID.adm**
- **RSACredProviderFilter_SmartCard.adm**
- **RSACredProviderFilter_ThirdParty.adm**

Policy Settings

You define the policy settings in each template by selecting one of the following options:

Not Configured. This is the default setting of an installed template.

Enabled. You activate a template setting by enabling it.

Disabled. When you select Disabled for a template, you deactivate the setting.

Disabled is not the same as Not Configured. Not Configured is the default setting. Review each policy setting carefully.

Note: RSA Authentication Agent honors the Microsoft token removal policy. The Microsoft policy defines the action the system takes when a user logs off or removes a token from a USB port. This Microsoft setting cannot be defined by the RSA Authentication Agent templates.

For information on defining policy settings for a template (including the defaults), see Chapter 3, "Defining the Policy Settings." For information on enforcing a policy, go to the Windows Server Group Policy page in the Microsoft Support Knowledge Base at **http://www.microsoft.com/grouppolicy/**.

RSA Local Authentication Settings Templates

The RSA Local Authentication Settings template files allow you to control how the RSA Authentication Agent logon prompts appear to users. The template files are:

- **RSA_Authentication_Agent.adm**
- **RSA_Authentication_Agent_Password_Synchronization.adm**

The following policy settings are available:

Cache Challenge Settings. Allows the Authentication Agent to retrieve the user's challenge settings from a local cache if the agent cannot determine the user's group membership from the domain controller. If Authentication Agent has not yet cached the challenge settings and the domain controller cannot be contacted, you can specify to either Challenge (passcode) or Do not challenge the user (allow Microsoft Windows password).

Note: Cache Challenge settings can be configured locally through the RSA Control Center. However, settings configured by Group Policy override settings configured in the RSA Control Center. For more information, see the Challenge Users topic in the RSA Authentication Agent (SecurID) Help.

Challenge Users. Specifies the users who will be challenged for RSA SecurID credentials (passcode). You can challenge all users, all users except those in a specified group, only users in a specified group, or no users.

Note: Challenge Users settings can be configured locally through the RSA Control Center. However, settings configured by Group Policy override settings configured in the RSA Control Center. For more information, see the Challenge Users topic in the RSA Authentication Agent (SecurID) Help.

Label for the Local Authentication Prompt. Specifies the label for the RSA SecurID authentication logon prompt: Passcode (PIN and tokencode) or Password (Microsoft Windows password). The label continues to display as pin for connected authenticators.

Offline Authentication Service. Prevents offline authentication from running on the client machine. You do not need to run this service if offline authentication is not configured on the RSA Authentication Manager server.

Reserve Password. The reserve password feature is an emergency access method that an administrator can use to allow an authorized user to authenticate to that user's protected computer without entering an RSA SecurID passcode.

Synchronize User Passwords. Set this policy on the domain controller, and select the users that should have automatic password synchronization. This allows the Agent to synchronize users' passwords with any password changes that took place on another computer or through the Active Directory. You can synchronize password changes for all users, all users in a specific group, or all users except those in a specific group, or no users.

Unlock with SecurID PIN or Password. Allows RSA SecurID users to unlock their computers with an RSA SecurID PIN or Windows password instead of an RSA SecurID passcode. You can also change the following settings:

- **RSA SecurID PIN or Password Attempts.** Specify the number of times RSA SecurID users can enter incorrect PINs or passwords before they are prompted for an RSA SecurID passcode.
- **RSA SecurID PIN or Password Time-out.** Specify the number of minutes after the computer locks when users can enter their RSA SecurID PINs or Windows password to unlock their computers.

For more information about configuring the Local Authentication settings, see "Defining the Local Authentication Settings" on page 27.

RSA Expiration Warning Message Template

The RSA Expiration Warning Message GPO template file, **RSA_SecurID_Expiration_Warning.adm**, contains a policy setting to configure a warning message to notify users of the number of days left before their RSA SecurID 800 Authenticators expire. Users can view the number of days before the expiration date from the RSA Security Center icon in the system tray.

The following policy setting is available:

Warning Message for Expiring Authenticators. Enable or disable a warning message to notify users that an authenticator is about to expire. Specify when the warning message displays.

For more information, see "Define the SecurID Authenticator Expiration Message" on page 36.

RSA Credential Provider Filter GPO Templates

The following RSA Credential Provider Filter GPO template files contain policy settings to define how Authentication Agent responds when users log on to Windows Vista, Windows 7, Windows 8, Windows Server 2008, or Windows Server 2012 computers:

- **RSACredProviderFilter_Microsoft.adm**
- **RSACredProviderFilter_SecurID.adm**
- **RSACredProviderFilter_SmartCard.adm**
- **RSACredProviderFilter_ThirdParty.adm**

The following policy settings are available:

- **Exclude all third-party Credential Providers.** Users cannot log on through a third-party Credential Provider tile.
- **Exclude the Microsoft Password Credential Providers.** Users cannot log on through the Microsoft Credential Provider tiles used for password logon (Windows account).
- **Exclude the Microsoft Smart Card Credential Providers.** Users cannot log on through the Microsoft Smart Card Credential Provider tiles used for certificate logon.
- **Exclude the Microsoft Picture Password Credential Providers.** Users cannot log on through the Microsoft Picture Password Credential Provider tile used for picture (with patterns) logon.
- **Exclude the Microsoft PIN Credential Providers.** Users cannot log on through the Microsoft PIN Credential Provider tile used for PIN connected to the local or Windows Live ID account logon.
- **Exclude the Microsoft Windows Live ID Credential Providers.** Users cannot log on through the Microsoft Windows Live ID Credential Provider tile used for Live ID account (e-mail address and password) logon.
- **Exclude the RSA SecurID Credential Provider for connected authenticators.** Users cannot log on with passcodes by entering the SecurID PINs with the application accessing the tokencodes from RSA SecurID authenticators connected to the USB port.
- **Exclude the RSA SecurID Credential Provider for disconnected authenticators.** Users cannot log on with a passcode (SecurID PIN and tokencode from a handheld RSA SecurID authenticator).
- **Exclude the RSA Smart Card Credential Providers.** Users cannot log on through the RSA Smart Card Credential Provider tile that allows them to log on with a smart card that contains a Windows account.

Default Behavior of the RSA Credential Provider Filter

The RSA Credential Provider filter is installed by the RSA Authentication Agent and RSA Authentication Client products and controls what logon tiles are available to the user. If none of the RSA Credential Provider Filter GPO templates are configured, certain credential providers are filtered by default, as shown in the following table:

RSA Products Installed	Credential Providers Filtered	Credential Providers Visible to the User
RSA Authentication Agent	Microsoft Password Credential Provider	• RSA SecurID Credential Provider for connected authenticators (if Connected Authenticator feature installed and user connects RSA SecurID 800 authenticator to USB port) • RSA SecurID Credential Provider for disconnected authenticators • Microsoft Smart Card Credential Provider (if user connects RSA SecurID 800 authenticator to USB port) • Other third-party credential providers
RSA Authentication Agent and RSA Authentication Client	Microsoft Password Credential Provider and RSA Smart Card Credential Provider	• RSA SecurID Credential Provider for connected authenticators* • RSA SecurID Credential Provider for disconnected authenticators • Microsoft Smart Card Credential Provider (if user connects RSA SecurID 800 authenticator to USB port) • Other third-party credential providers
RSA Authentication Client	RSA Smart Card Credential Provider	• Microsoft Password Credential Provider • Microsoft Smart Card Credential Provider (if user connects RSA SecurID 800 authenticator to USB port) • Other third-party credential providers

For more information, see "Configure the RSA Credential Provider Filter Settings" on page 37.

RSA Verify RSA Shared Components GPO Template

The Verify RSA Shared Components GPO template file, **RSADesktop_VerifyRSAComponents.adm**, contains policy settings to control whether RSA desktop applications verify the authenticity of shared RSA components. Verifying authenticity makes the system more secure, but verification may impact performance. Verification is on by default, however, you can turn off verification with the template.

For more information about defining verification settings, see "Verify RSA Shared Components" on page 44.

2 Installing Group Policy Object Templates

This chapter includes the following topics:

Prepare to Install the RSA Group Policy Object Templates

Group Policy is a feature of Microsoft Windows. RSA recommends that before you deploy the RSA Group Policy Object templates, you become familiar with Microsoft Windows Group Policy concepts and best practices. For more information, go to the Windows Server Group Policy page in the Microsoft Support Knowledge Base at **http://www.microsoft.com/grouppolicy/**.

For computers that are not part of your domain or subject to Group Policy, you must configure the template settings with the Local Group Policy Editor. For more information, see "Install the Templates on a Windows Computer" on page 23, and "Defining the Policy Settings" on page 25.

Map Preference Settings to Group Policy Object Templates

RSA Authentication Agent 7.2 uses Group Policy Object templates to configure policy settings. If you have RSA Authentication Agent 7.1 installed and you want to install RSA Authentication Agent 7.2, you do not need to redefine your policy settings. RSA Authentication Agent 7.2 holds on to your previous settings.

If you have RSA Authentication Agent 7.0 or earlier installed and you want to install Authentication Agent 7.2, you need to redefine the settings of your Group Policy Templates. (Earlier versions of RSA Authentication Agent used preference settings to configure the Authentication Agent instead of policy settings.) This section describes how to map your preferences so you can see what options changed and make notes of your current settings. Then you can redefine the setting after you install the latest version of Authentication Agent.

To map preference settings to GPO templates:

1. Use one of the following tools to view your current settings:
   - **RSA Control Center.**
   - **Group Policy Editor.** Use the Group Policy Management console to launch the Group Policy Editor.

   Note: Use the same tool that you used to configure your settings in a previous version of Authentication Agent to view your current settings.

2. Record your current settings. See the charts in "Map Preference Settings to Group Policy Object Templates" on page 15 for details on the settings for different versions of Authentication Agent for Microsoft Windows.
3. Install the RSA Authentication Agent 7.2 templates.

   Important: If you install Authentication Agent on the Windows Server where you plan to manage your RSA Group Policy Object templates, you do not need to manually install the templates. Authentication Agent automatically installs them in the Local Security Policy. If you want to install the templates on a computer other than the one where you installed Authentication Agent 7.2, see "Installing the RSA Group Policy Object Templates" on page 22.

4. Use the Group Policy Editor to configure the settings in RSA Authentication Agent 7.2. For more information, see Chapter 3, "Defining the Policy Settings."

Preference Settings and Agent Support

The following table lists the Local Authentication settings for Authentication Agent 7.2 for Microsoft Windows and earlier versions of the product.

Local Authentication Settings

Name	Description	Version Supported On			
		6.1	6.4	7.0	7.1 and 7.2
Challenge Users	Specifies which users (all users, users in a group, all users except those in a group, or no users) to challenge for RSA SecurID credentials. Includes Specify User Group and Send Domain and User Name to Authentication Manager	--	--	--	X
Challenge Groups	Specifies the group of users to challenge for RSA SecurID credentials. (You must select a group to select users from that group, or all users except those in a group to challenge for RSA SecurID credentials.)	X	X	X	In Challenge Users setting.
Cached Challenge Settings	Allows Authentication Agent to retrieve the user's challenge setting from a local cache if it cannot resolve the user's challenge status from the domain server. If the challenge setting is not found in the cache, use one of the following options: • Challenge the user for a passcode. • Do not challenge the user (allow Windows password).	X	X	X	X
Label for Local Authentication Prompt	Specifies the label for the RSA SecurID authentication prompt: Passcode or Password.	X	X	X	X
Allow Novell Password Update	Enables passwords in a Novell database to update whenever matching Microsoft Windows passwords are updated.	X	X	Not available	Not available
Synchronize user passwords	Specifies the users whose domain account password changes are automatically synchronized in matching accounts in the RSA Authentication Manager database. Includes Specify User Group and Send Domain and User Name to Authentication Manager.	--	--	--	X

Local Authentication Settings					
Name	**Description**	**Version Supported On**			
		6.1	**6.4**	**7.0**	**7.1 and 7.2**
Unlock with RSA SecurID PIN or Password	Allows RSA SecurID users to unlock their workstations with only an RSA SecurID PIN or Windows password instead of an RSA SecurID passcode	X (PIN only	X (PIN only)	X (PIN only)	X (7.1 PIN only, 7.2 PIN or Windows password)
RSA SecurID PIN or Password Time-out	Specifies the number of minutes after the workstation locks when RSA SecurID users can enter only their RSA SecurID PINs or Windows passwords to unlock their workstations.	X	X	X	Now in Unlock with RSA SecurID PIN or Password setting
RSA SecurID PIN or Password Attempts	Specifies the number of times RSA SecurID users can enter incorrect RSA SecurID PINs or Windows passwords before they are prompted for an RSA SecurID passcode.	X	X	X	Now in Unlock with RSA SecurID PIN or Password setting

The following table lists the Credential Provider Filter settings for Authentication Agent 7.2 for Microsoft Windows and earlier versions of the product.

Credential Provider Filter Settings

Name	Description	Version Supported On			
		6.1	6.4	7.0	7.1 or 7.2
Exclude all third-party Credential Providers	Users cannot log on through any third-party Credential Provider tiles.	--	--	--	X
Exclude the Microsoft Password Credential Providers	Users cannot log on through the Microsoft Credential Provider tiles that allow them to log on with a password (Windows account).	--	--	X	X
Exclude the Microsoft Smart Card Credential Providers	Users cannot log on through the Microsoft Smart Card Credential Provider that allows them to log on with a smart card that contains logon certificate.	--	--	--	X
Exclude the Microsoft Picture Password Credential Providers	Users cannot log on through the Microsoft Picture Password Credential Provider tile used for picture (with patterns) logon.	--	--	--	7.2 only
Exclude the Microsoft PIN Credential Providers	Users cannot log on through the Microsoft PIN Credential Provider tile used for PIN connected to the local or Windows Live ID account logon.	--	--	--	7.2 only
Exclude the Microsoft Windows Live ID	Credential Providers. Users cannot log on through the Microsoft Windows Live ID Credential Provider tile used for Live ID account (e-mail address and password) logon.	--	--	--	7.2 only
Exclude the RSA SecurID Credential Providers for connected authenticators	Users cannot log on with RSA SecurID connected authenticators.	--	--	--	X
Exclude the RSA SecurID Credential Providers for disconnected authenticators	Users cannot log on with RSA SecurID disconnected authenticators.	--	--	X	X
Exclude the RSA Smart Card Credential Providers	Users cannot log on through the RSA Smart Card Credential Provider tile that allows them to log on with a smart card that contains a Windows account.	--	--	--	X

The following table lists the Logon settings for Authentication Agent 7.2 for Microsoft Windows and earlier versions of the product.

Logon Settings					
Name	**Description**	**Version Supported On**			
		6.1	**6.4**	**7.0**	**7.1 or 7.2**
RSA Legal Notice Caption	Allows you to change the title of the legal notice that is displayed before the logon prompt. This legal notice is displayed only if a third-party legal notice is not defined in the system policy.	X	X	--	Now configured through Microsoft policy settings.
RSA Legal Notice Text	Allows you to change the text of the legal notice.	X	X	--	Now configured through Microsoft policy settings.

The following table lists the warning message you can set for expiring authenticators for Authentication Agent 7.2 for Microsoft Windows and earlier versions of the product.

Warning Message for Expiring Authenticators Settings					
Name	**Description**	**Version Supported On**			
		6.1	**6.4**	**7.0**	**7.1 or 7.2**
Warning Message for Expiring Authenticators	Displays a warning message to notify users of the number of days left before an RSA SecurID 800 Authenticator expires.	--	--	--	X

The following table lists the password synchronization settings for Authentication Agent 7.2 for Microsoft Windows and earlier versions of the product.

Password Synchronization Settings

Name	Description	Version Supported On			
		6.1	6.4	7.0	7.1 on 7.2
Synchronize Users	Specifies categories of users whose password changes made to their domain accounts are synchronized with their corresponding accounts in the Authentication Manager database.	X	X	--	Now in Local Authentication settings, Synchronize User Passwords
Specify User Group	Specifies the group of users whose password changes made to their domain accounts are synchronized with their corresponding accounts in the Authentication Manager database.	X	X	--	Now in Local Authentication settings, Synchronize User Passwords
Send Domain and User Name to Authentication Manager	Directs the Authentication Agent to send both the domain name and user name, instead of just the user name, to the Authentication Manager during password synchronization. Enable this if you configured the Authentication Agent to send both the domain name and user name to the Authentication Manager during authentication.	X	X	--	Now in Local Authentication settings, Synchronize User Passwords

Installing the RSA Group Policy Object Templates

The RSA templates come with the product, but you can also access them through the product page on RSA SecurCare Online at **https://knowledge.rsasecurity.com**.

If you want to apply the template settings to all computers on your network, install the templates on the domain controller. If you do not want to apply the template settings to all of the computers in the domain, you can set up a group of computers for a domain. If you want to apply template settings to computers that are not subject to Group Policy from a domain controller, see "Install the Templates on a Windows Computer" on page 23.

The console you use to install the templates depends on your operating system. The following sections describe how to install the templates on Windows Server 2008 or Windows Server 2012 domain controllers. You can also find a section on how to install the templates on Windows computers other than domain controllers.

In domain environments, computers wait for specified refresh intervals before updating their settings. When the refresh process ends, settings associated with the templates are loaded into the Windows registry. The settings specified in the Group Policy Object templates override the settings configured on individual workstations.

Important: If you install Authentication Agent on the Windows Server where you plan to manage your RSA Group Policy Object templates, you do not need to manually install the templates. Authentication Agent automatically installs them in the Local Security Policy.

Install the Templates on Windows Server 2008 or 2012 Domain Controller

Install the templates in the Group Policy Editor through the Group Policy Management console. Templates are installed with the default setting of **Not Configured**. For more information about defining the settings, see Chapter 3, "Defining the Policy Settings."

Note: If you installed Windows Server 2012 in "Server Core" mode instead of "Server with GUI" mode, you do not use a user interface (GUI) to install applications and files as described in this document. You must use the command line. Refer to the Windows Server 2012 documentation for details on using Server Core mode.

To install the templates on Windows Server 2008 or Windows Server 2012:

1. Copy the templates to a local drive on the domain controller (server with the latest service packs).
2. Click **Start > Administrative Tools > Group Policy Management**.
3. Double-click the name of the domain where you want to install the templates.
4. Double-click **Group Policy Objects**.
5. Right-click the policy where you want to add the template, for example, **Default Domain Policy**, and click **Edit**.

6. Double-click **Computer Configuration**, and then double-click **Policies**.
7. Right-click **Administrative Template**, and click **Add/Remove Templates**.
8. Click **Add**.
9. Browse to the template files you want installed, and select the template files.
10. Click **Open**.
11. Click **Close**.

At the next refresh interval, template settings are loaded into the Windows registry of domain computers.

Install the Templates on a Windows Computer

For Windows computers that are not connected to your domain or subject to Group Policy, you can manually install and configure the templates with the Local Group Policy Editor.

If you install RSA Authentication Agent 7.2 for Microsoft Windows on the same computer you want to use to manage your templates. You do not need to manually install the templates. The application automatically installs the appropriate templates during installation in Local Security Policy.

The following list identifies the Group Policy Object Templates installed in Local Security Policy with RSA Authentication Agent 7.2 for Microsoft Windows. This applies to the supported operating systems (Windows Vista, Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2, or Windows Server 2012):

- RSA_Authentication_Agent.adm
- RSA_SecurID_Expiration_Warning.adm
- RSACredProviderFilter_Microsoft.adm
- RSACredProviderFilter_SecurID.adm
- RSACredProviderFilter_SmartCard.adm
- RSACredProviderFilter_ThirdParty.adm

For a complete list of available templates, see “Template Files,” on page 8.

To install the templates on a Windows computer:

1. Copy the templates to a local drive on the computer.
2. Click **Start** > **Run** > **gpedit.msc**.
3. Right-click **Administrative Templates**, and click **Add**.
4. Browse to the template files you want installed, and select the template files.
5. Click **Close**.

The templates install with the default setting of **Not Configured**. You can define the template settings immediately. For more information, see Chapter 3, “Defining the Policy Settings.”

3 Defining the Policy Settings

This chapter includes the following topics:

Accessing the Group Policy Object Templates

This section describes how to access the templates and define their settings. It includes instructions for domain controllers and Windows computers that are not joined to a domain or subject to Group Policy. The example procedures include screens from a Windows Server operating system.

Note: Make sure that you have installed the templates. For more information, see Chapter 2, "Installing Group Policy Object Templates."

Access the Templates on a Windows Server 2008 or 2012 Domain Controller

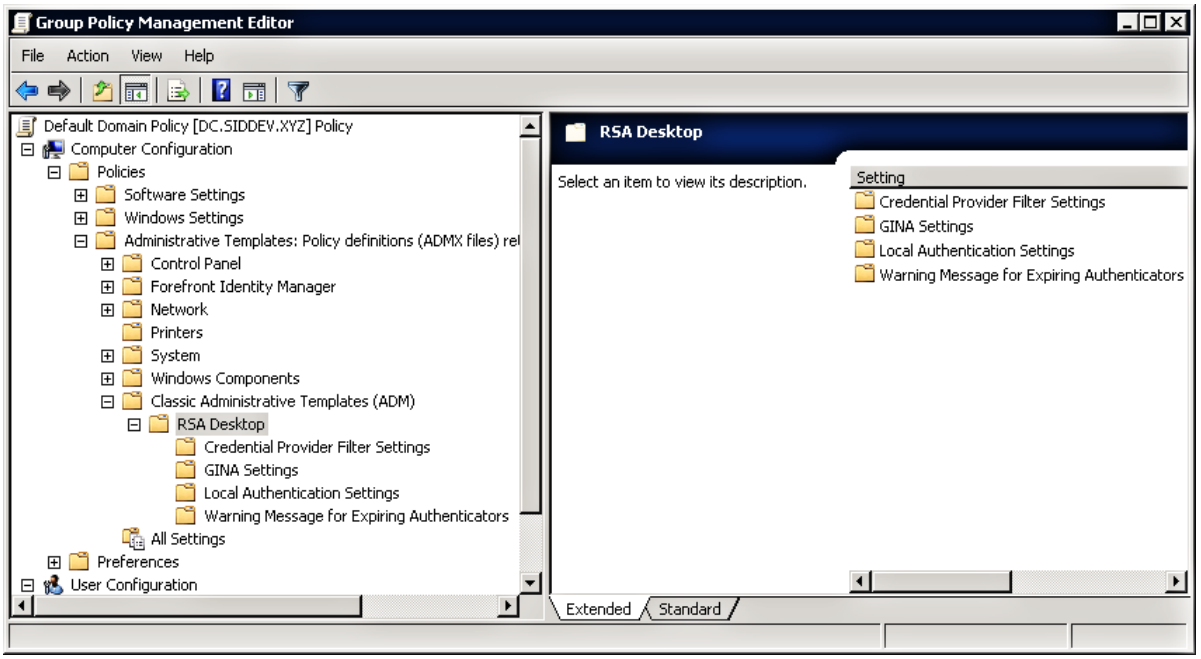
This section describes how to access the templates to view and define their settings.

To access the templates on a Windows Server 2008 or 2012 (with GUI) Domain Controller:

1. Click **Start** > **Administrative Tools** > **Group Policy Management**.
2. If necessary, double-click the name of the domain to expand it.
3. Right-click the policy with the template you need to edit, for example, **Default Domain Policy**, and click **Edit**.
4. Double-click **Policies** from **Computer Configuration**.
5. Double-click **Administrative Templates**.
6. Double-click **Classic Administrative Templates (ADM)**.

7. Double-click **RSA Desktop**.

   A screen similar to the screen below displays the policy folders of the templates you installed in the RSA Desktop folder. You can access the settings by double-clicking the folders.



Access the Templates On a Windows Computer

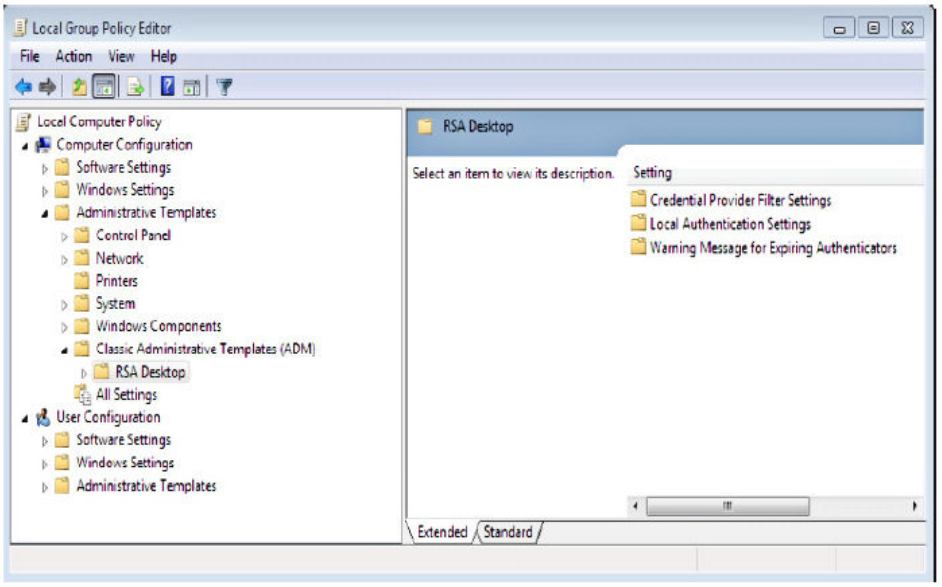
This section describes how to access the templates to view and define their settings with the Local Group Policy Editor.

To access the templates on a Windows Computer:

1. Click **Start** > **Run** > **gpedit.msc**.
2. Double-click **Administrative Templates**.
3. Double-click **Classic Administrative Templates (ADM)**.

4. Double-click **RSA Desktop**.

   A screen similar to the screen below displays the policy folders of the templates you installed in the RSA Desktop folder. You can access the settings by double-clicking the folders.



Defining the Local Authentication Settings

The **Local Authentication Settings** folder contains settings that allow you to control how users interact with Authentication Agent. You can:

- Specify the users to challenge with RSA SecurID credentials.
- Automatically synchronize user passwords.
- Enable retrieval of a user's challenge setting from a local cache.
- Set a reserve password emergency access method.

  Note: To securely establish a reserve password, you generate a hashed value of the reserve password using the RSA Authentication Agent Reserve Password Hash Generation utility that comes with the RSA Authentication Agent software installation kit.

- Set the label for the RSA SecurID local authentication logon prompt.
- Disable offline authentication locally.
- Allow users to unlock their computers with only an RSA SecurID PIN instead of an RSA SecurID passcode.

Specify Which Users to Challenge

RSA Authentication Agent protects resources by challenging users for RSA SecurID passcodes (PINs and tokencodes). You determine the degree of protection by specifying which users you want Authentication Agent to challenge (all users, no users, or specific groups of users). If this policy is disabled or not configured, no users are challenged.

You create challenge groups using the Microsoft Windows interface. For information about creating Windows groups, see your Windows documentation. If you do not want to create new groups through the Microsoft Windows options, use the default Windows groups.

If you create challenge groups for users' domain accounts, local authentication protects access to your company's domain in addition to protecting access to the local Windows desktop on users' computers. You can create challenge groups locally, or you can create them on the domain server.

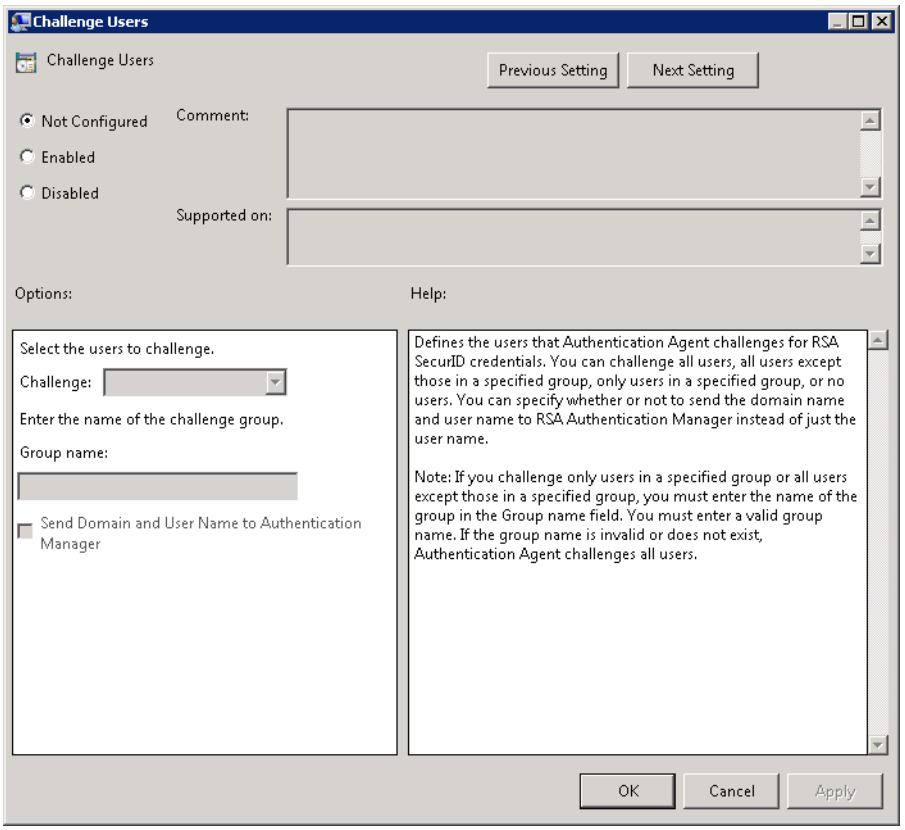
After you create the groups, you specify how Authentication Agent addresses the groups during authentication.

Important: You can configure challenge settings locally through the RSA Control Center. However, settings configured by Group Policy override settings configured in the RSA Control Center. For instructions and additional information, see the Challenge Users topic in the RSA Authentication Agent (SecurID) Help.

To specify which users to challenge:

1. Make sure that you have installed the templates as described in Chapter 2, "Installing Group Policy Object Templates."
2. Access the templates as described in "Accessing the Group Policy Object Templates."
3. Double-click the **Local Authentication Settings** folder.

4. In the right pane of the dialog box, double-click **Challenge Users**. A dialog box similar to below opens with a definition of the policy.



5. Select one of the following:
   - **Not Configured.** In this state, no users are challenged.
   - **Enabled.** This state allows you to challenge all users, members of a particular group, everyone except members of a particular group, or no users. See the next step.
   - **Disabled.** In this state, no users are challenged.
6. If you select **Enabled**, select which users you want to challenge.

Which Users to Challenge	How to Configure
Anyone who attempts to access the protected resource.	From the **Challenge** drop-down list, select **All users**.

Which Users to Challenge	How to Configure
Members of a particular group	a. From the **Challenge** drop-down list, select **Users in**. b. In the Group name field, enter the name of the group that you want in the format <domain name or machine name>\<group name>, or for the current machine, enter .\<group name>. You must enter a valid group name. If the group name is invalid or does not exist, Authentication Agent challenges all users.
Anyone except members of a particular group.	a. From the **Challenge** drop-down list, select **All users except**. b. In the Group name field, enter the name of the group that you want to exclude in the format <domain name or machine name>\<group name>, or for the current machine, enter .\<group name>. You must enter a valid group name. If the group name is invalid or does not exist, Authentication Agent challenges all users.
No one.	From the **Challenge** drop-down list, select **Off**.

7. If you set up the user account with a domain name and user name, (domain_name\user_name) in RSA Authentication Manager, select the checkbox **Send Domain and User Name to Authentication Manager**.
8. Click **Apply**, and then click **OK** to return to the **Local Authentication Settings** folder.
9. Close the Group Policy Management Editor.

If the policy was modified on the domain controller, the settings load into the Windows registry once the refresh interval ends in the domain.

Automatically Synchronize User Passwords

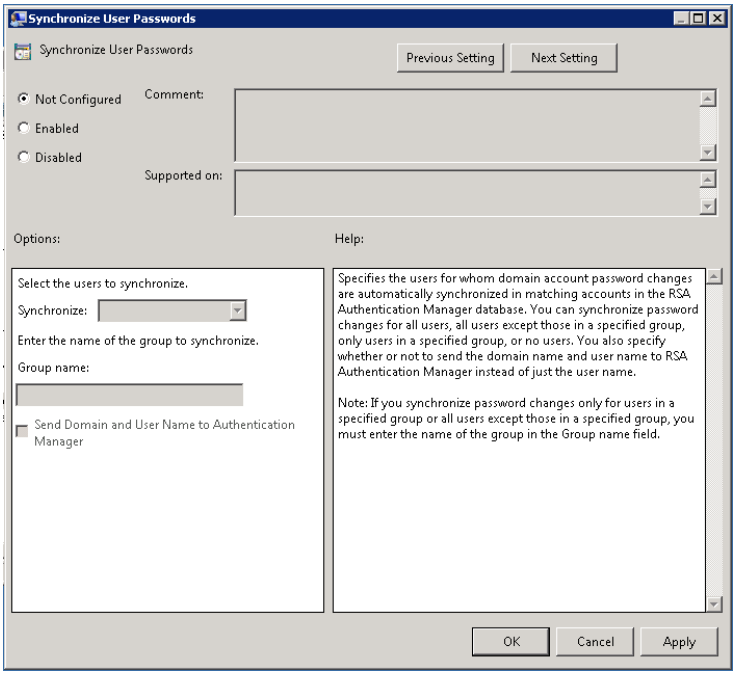
The Synchronize User Passwords setting is used to automatically synchronize domain user passwords on domain controllers that have Authentication Agent installed if you do not want to require an RSA SecurID challenge on the domain controllers. If users are challenged on the domain controller, passwords will be synchronized for all challenged users. If you use both the Synchronize User Passwords template and the Challenge Users template on the domain controller, passwords will be synchronized for users in either group.

Typically, you specify the same group of users for password synchronization as the group of users that you challenge for RSA SecurID credentials. If, however, you install Authentication Agent on the domain controllers, but do not use the password synchronization setting to specify which users should have their passwords synchronized, challenge settings on the domain controller determine the users for whom passwords are synchronized. For example, if you set the challenge for all users, but you do not set up password synchronization, passwords are synchronized for all users.

Configure the Synchronize User Passwords settings only on the domain controller. The domain controller must be running the Offline Authentication Service.

To synchronize user passwords automatically:

1. Make sure that you have installed the templates. For more information, see Chapter 2, "Installing Group Policy Object Templates."
2. Access the templates. For more information, see "Accessing the Group Policy Object Templates."
3. Double-click the **Local Authentication Settings** folder.
4. From the right pane, double-click **Synchronize User Passwords**. A dialog box similar to below opens with a definition of the setting.



5. Select one of the following:
   - **Not Configured.** In this state, user passwords are synchronized with the Challenge Users template.
   - **Enabled.** In this state, you can synchronize password changes for all users, all users in a specific group, all users except those in a specific group, or no users. See the next step.
   - **Disabled.** In this state, user passwords are synchronized with the Challenge Users template.
6. If you select **Enabled**, select the users for whom you want automatic password synchronization.

Whose Passwords to Synchronize	How to Specify
Anyone who attempts to access the protected resource.	From the **Synchronize** drop-down list, select **All users**.
Members of a particular group.	a. From the **Synchronize** drop-down list, select **Users in**. b. In the Group name field, enter the name of the group that you want synchronization for as <domain name>\<group name>, or for the current machine, enter .\<group name>. You must enter a valid group name. If the group name is invalid or does not exist, Authentication Agent synchronizes passwords for all challenged users.
Anyone except members of a particular group.	a. From the **Synchronize** drop-down list, select **All users except**. b. In the Group name field, enter the name of the group that you want to exclude. You must enter a valid group name. If the group name is invalid or does not exist, Authentication Agent synchronizes passwords for all users.
No one.	From the **Synchronize** drop-down list, select **Off**.

7. If you or the RSA Authentication Manager administrator set up the user account with a domain name and user name (domain_name\user_name) in RSA Authentication Manager, select **Send Domain and User Name to Authentication Manager**.
8. Click **Apply**, and then click **OK** to return to the **Local Authentication Settings** folder.
9. Close the Group Policy Management Editor.

If the policy was modified on the domain controller, the settings load into the Windows registry once the refresh interval ends in the domain.

Enable Retrieval of Locally Cached Challenge Settings

You specify challenge status by using the Microsoft Windows interface to create challenge groups. You can create the groups locally or on your company's domain server. For more information, see "Specify Which Users to Challenge" on page 28.

When a user attempts to log on to a local Windows desktop using a domain account, RSA Authentication Agent contacts the domain controller to determine the user's challenge status. If Authentication Agent cannot determine the challenge status (for example, if the connection to the domain server fails), Authentication Agent challenges the user for an RSA SecurID passcode. Users who have been issued RSA SecurID tokens can authenticate successfully, but users who are not required to authenticate using RSA SecurID are locked out of their computers.

You can configure Authentication Agent so that when the challenge status is not available from the domain server, Authentication Agent searches for a cached challenge setting on the user's local computer.

If a locally cached policy setting exists, Authentication Agent uses it to determine whether or not to challenge the user for an RSA SecurID passcode. If a locally cached setting does not exist, Authentication Agent challenges the user for an RSA SecurID passcode.

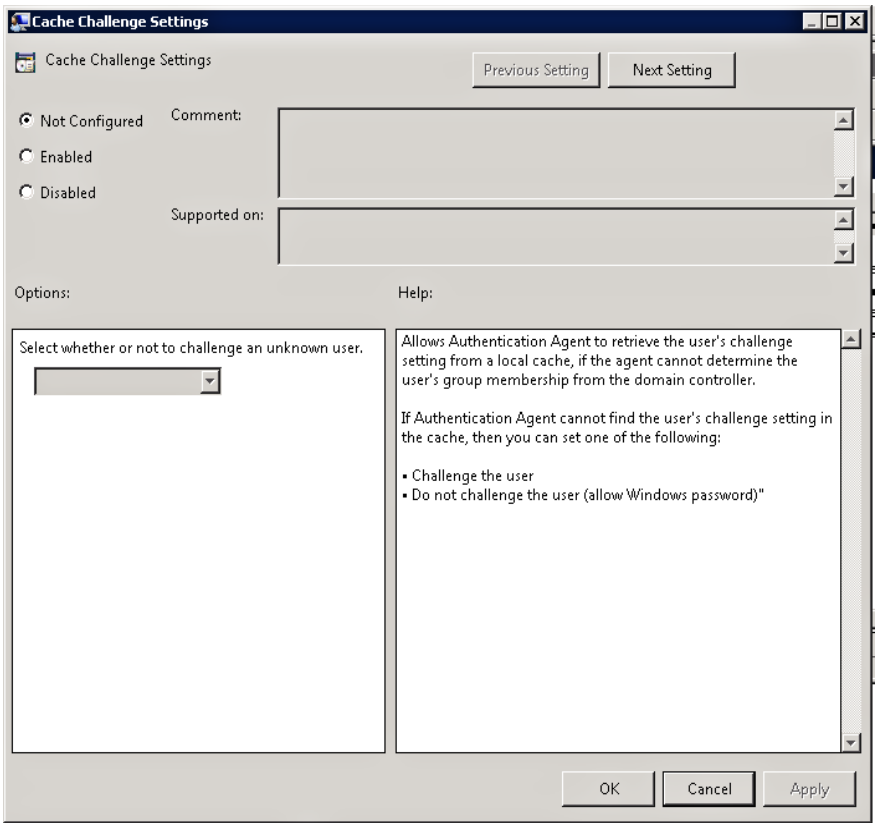
If this policy is not configured or is disabled, Authentication Agent does not use the local cache to determine group membership. If Authentication Agent cannot determine group membership, the user is challenged for RSA SecurID credentials.

Important: You can configure Cache Challenge settings locally through the RSA Control Center. However, settings configured by Group Policy override local settings configured in the RSA Control Center. For instructions and more information, see the Challenge Users topic in the RSA Authentication Agent (SecurID) Help.

To enable retrieval of locally cached challenge settings:

1. Make sure that you have installed the templates. For more information, see Chapter 2, "Installing Group Policy Object Templates."
2. Access the templates. For more information, see "Accessing the Group Policy Object Templates."
3. Double-click the **Local Authentication Settings** folder.

4. In the right pane, double-click **Cache Challenge Settings**. A dialog box similar to below opens with a definition of the setting.



5. Select one of the following:
   - **Not Configured.** This state challenges users for their RSA SecurID credentials if a user's group membership cannot be determined. Authentication Agent does not use the local cache to determine group membership.
   - **Enabled.** This state enables Authentication Agent to use the local cache to determine group membership if the domain controller is unavailable. See the next step.
   - **Disabled.** This state challenges users for their RSA SecurID credentials if the user's group membership cannot be determined. Authentication Agent does not use the local cache to determine group membership.
6. If you select **Enabled**, do one of the following:
   - To require a passcode when group membership cannot be determined, select **Challenge users**.
   - To allow the Windows password when group membership cannot be determined, select **Do not challenge user**.
7. Click **Apply**, and then click **OK** to return to the **Local Authentication Settings** folder.

8. Close the Group Policy Management Editor.

If the policy was modified on the domain controller, the settings load into the Windows registry once the refresh interval ends in the domain.

Set a Reserve Password Emergency Access Method

A reserve password is an emergency access method that allows an administrator to assist a user who is unable to log on, for example, because the user has run out of offline day files. The reserve password allows an administrator to bypass the challenge for an RSA SecurID passcode under these circumstances. For example, if you set the reserve password option, the user is prompted to enter a reserve password to log on if the following applies:

- The Offline Authentication Service (RSA Authentication Agent Offline Local) is not running on the local computer.
- There are no offline days on the local computer.
- The computer cannot connect to RSA Authentication Manager.

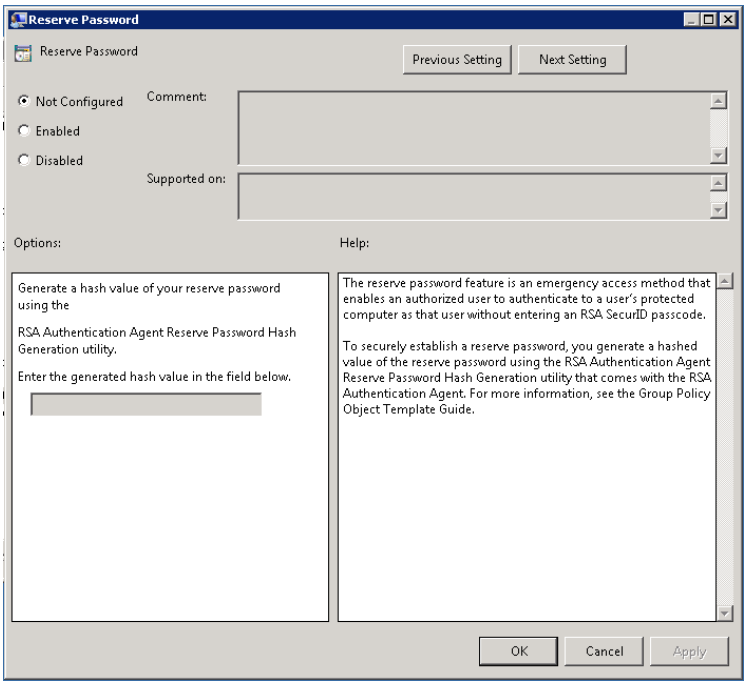
Only an administrator knows the reserve password. If a user is prompted for a reserve password, the user must contact the appropriate administrator for assistance. Once the administrator enters the reserve password, Authentication Agent prompts for the Windows password. (It cannot access the Windows password stored on Authentication Manager.) If approved, the administrator can access the desktop.

Set a reserve password or use the Cached Challenge Setting options to avoid getting locked out of the computer. For example, if you select All Users as the Select users to challenge setting for local authentication and the network connection fails, no one, including an administrator, can logon to that computer. You can also use another emergency access method. For example, you can set the system to allow users to log on with one-time or fixed passwords if they forget their SecurID tokens. For more information, see “Enable Retrieval of Locally Cached Challenge Settings” on page 33 and the *Installation and Administration Guide*.

Important: The reserve password is less secure than other emergency access methods. It does not require a SecurID PIN, and it remains valid unless an administrator changes it. With a one-time password, a user must include the SecurID PIN, and the user can only use it once.

To set a reserve password:

1. Make sure that you have installed the templates. For more information, see Chapter 2, "Installing Group Policy Object Templates."
2. Access the templates. For more information, see "Accessing the Group Policy Object Templates."
3. Double-click the **Local Authentication Settings** folder.
4. In the right pane, double-click **Reserve Password**. A dialog box similar to below opens with a definition of the setting.



5. Do one of the following:
   - **Not Configured.** With this setting, authorized users cannot log on with a reserve password.
   - **Enabled.** With this setting, authorized users can log on with a reserve password. For details, see the next step.
   - **Disabled.** With this setting, authorized users cannot log on with a reserve password.
6. If you select **Enabled**, generate a hash value of the reserve password using the RSA Authentication Agent Reserve Password Hash Generation utility that comes with the RSA Authentication Agent software installation kit, and enter the hash value of the reserve password in the **Enter the generated hash value** field.
7. Click **Apply**. Click **OK** to return to the **Local Authentication Settings** folder.
8. Close the Group Policy Management Editor.

If the policy was modified on the domain controller, the settings load into the Windows registry once the refresh interval ends in the domain.

Set the Label for the RSA SecurID Local Authentication Logon Prompt

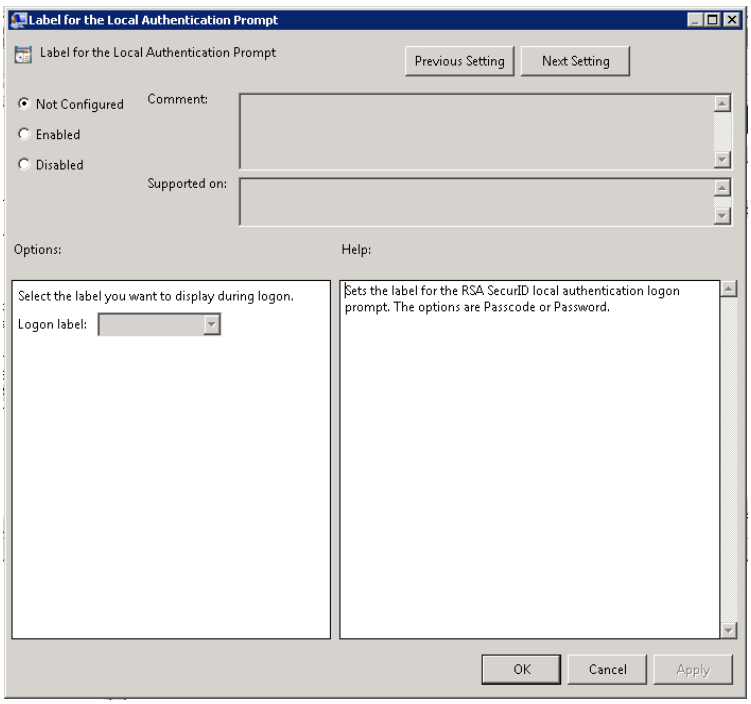
You can customize the RSA SecurID local authentication logon prompt to request a Windows password or an RSA SecurID passcode.

If a user is required to authenticate with RSA SecurID, configure the Authentication Agent to prompt for a passcode. If a user is not required to authenticate with RSA SecurID, configure the Authentication Agent to prompt for a Windows password. By default, the Authentication Agent prompts for passcodes. If the policy is not configured or is disabled, the user is prompted for the Windows password.

Note: The option you select applies to all users of the computer. For example, if you select passcode for a computer that is shared by more than one user, the logon prompt requests passcodes from all users, including those who have not been set up for RSA SecurID authentication.

To set the label for the logon prompt:

1. Make sure that you have installed the templates. For more information, see Chapter 2, "Installing Group Policy Object Templates."
2. Access the templates. For more information, see "Accessing the Group Policy Object Templates."
3. Double-click the **Local Authentication Settings** folder.
4. In the right pane, double-click **Label for the Local Authentication Prompt**. A dialog box similar to below opens with a definition of the setting.



5. Select one of the following:
   - **Not Configured.** With this setting, users must enter their Windows Password.
   - **Enabled.** With this setting, users are prompted for their Passcode or Windows Password. See the next step.
   - **Disabled.** With this setting, users must enter their Windows Password.
6. If you select **Enabled**, select **Passcode** or **Password**.
7. Click **Apply**, and then click **OK** to return to the **Local Authentication Settings** folder.
8. Close the Group Policy Management Editor.

If the policy was modified on the domain controller, the settings load into the Windows registry once the refresh interval ends in the domain.

Disable Offline Authentication Locally

The offline authentication policy specifies whether the offline authentication service should run on the local machine. If you are not using offline authentication, you can disable the service on the local machine. If this policy is not configured or enabled, the offline authentication service runs on the local machine. If this policy is disabled, offline authentication does not run on the local machine. Setting this policy to Disabled stops the service from running the next time the machine is rebooted.

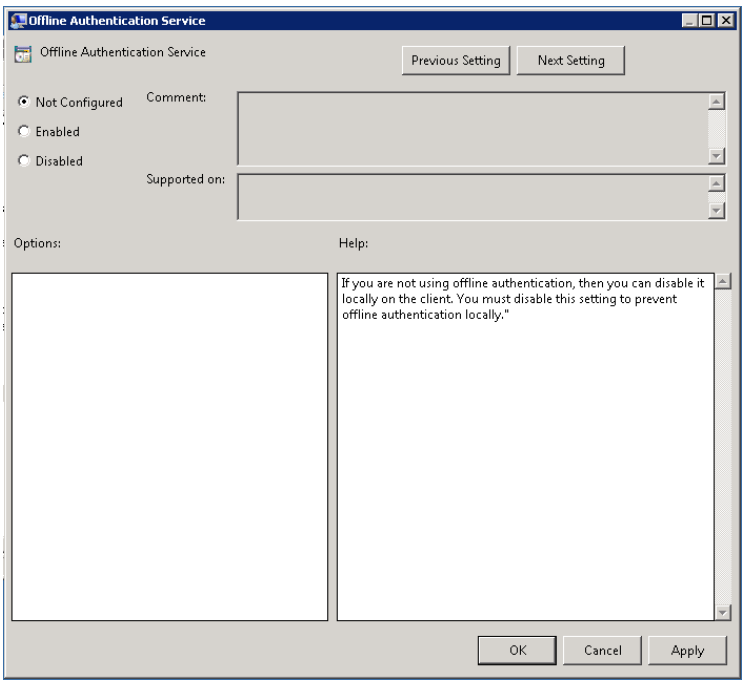
You can enable offline authentication per user through settings in the Authentication Manager server. If offline authentication is enabled for the user but the offline authentication service is not running on the local machine, the user cannot perform an RSA SecurID authentication offline.

Note: The password integration, password synchronization, and Unlock with SecurID PIN features require that offline authentication be enabled on both the Agent and the server. If you are using these features, do not disable offline authentication.

To disable offline authentication locally:

1. Make sure that you have installed the templates. For more information, see Chapter 2, "Installing Group Policy Object Templates."
2. Access the templates. For more information, see "Accessing the Group Policy Object Templates."
3. Double-click the **Local Authentication Settings** folder.

4. In the right pane, double-click **Offline Authentication Service**. A dialog box similar to below opens with a definition of the setting.



5. Select **Disabled** to disable offline authentication locally.
6. Click **Apply**, and then click **OK** to return to the **Local Authentication Settings** folder.
7. Close the Group Policy Management Editor.

   If the policy was modified on the domain controller, the settings are loaded into the Windows registry once the refresh interval ends in the domain.

Set Computers to Unlock with an RSA SecurID PIN or Windows Password

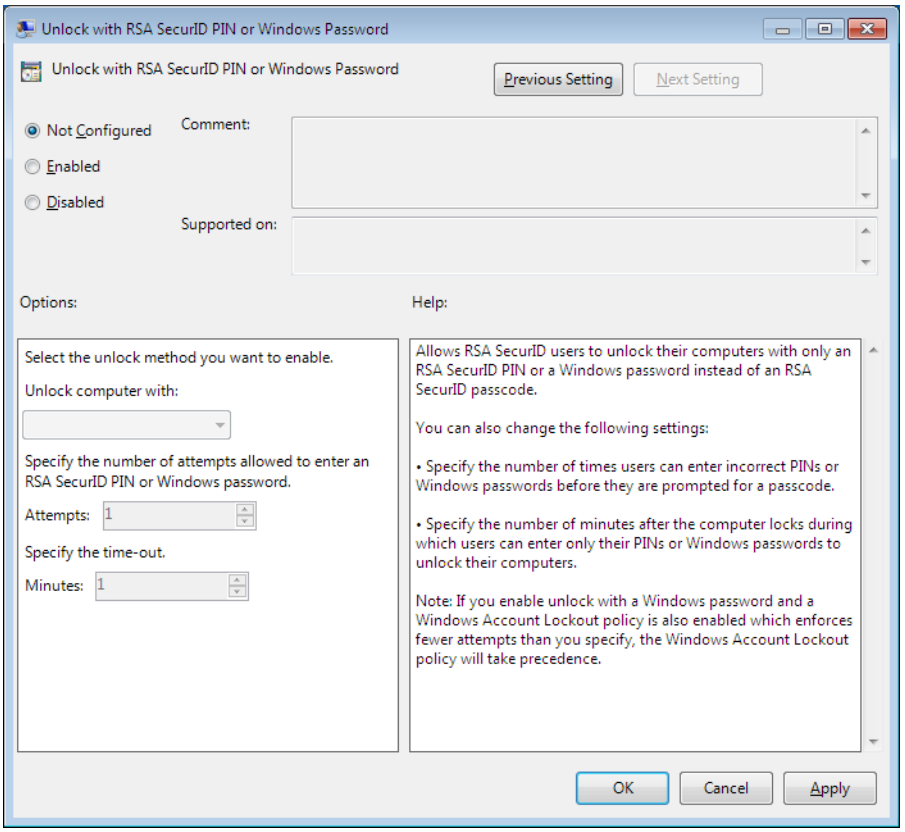
If a user can log on to the desktop with a passcode (RSA SecurID PIN and tokencode) or a passcode and a Windows password, you can allow the user to unlock the computer with only an RSA SecurID PIN or Windows password instead of needing to enter the full passcode.

If this policy is not configured or is disabled, users are not allowed to unlock their computers with only an RSA SecurID PIN or password. If this policy is enabled, you can specify the number of times users can enter incorrect PINs or passwords before they are prompted for a passcode. You can also specify the number of minutes when users can enter just PINs or passwords before their computers lock.

Note: The Unlock with SecurID PIN or Windows password feature also requires that the offline authentication feature be enabled on both the Agent and the server. If you allow users to unlock their computers with only a SecurID PIN or Windows password, do not disable offline authentication. The Authentication Agent for Windows does not support using this feature with software tokens.

To set computers to unlock with an RSA SecurID PIN or Windows password:

1. Make sure that you have installed the templates. For more information, see Chapter 2, "Installing Group Policy Object Templates."
2. Access the templates. For more information, see "Accessing the Group Policy Object Templates."
3. Double-click the **Local Authentication Settings**.
4. In the right pane, double-click **Unlock Computer with RSA SecurID PIN or Windows Password**. A dialog box opens with a definition of the setting.



5. Do one of the following:
   - **Not Configured.** Users must enter a passcode to unlock their computer.
   - **Enabled.** Users can unlock their computer with a pin instead of a passcode. See the next step.
   - **Disabled.** Users must enter a passcode to unlock their computer.
6. If you select **Enabled**, set the number of minutes (defaults to 75 minutes) when users can unlock their computers by entering SecurID PINs (no tokencode required) or Windows passwords. The maximum time-out period is 480 minutes.

   Then set the number of times users can enter incorrect PINs or passwords (defaults to three) before they are prompted for an RSA SecurID passcode. The maximum number of attempts is 10.

7. Click **Apply**, and then click **OK** to return to the **Local Authentication Settings** folder.
8. Close the Group Policy Management Editor.

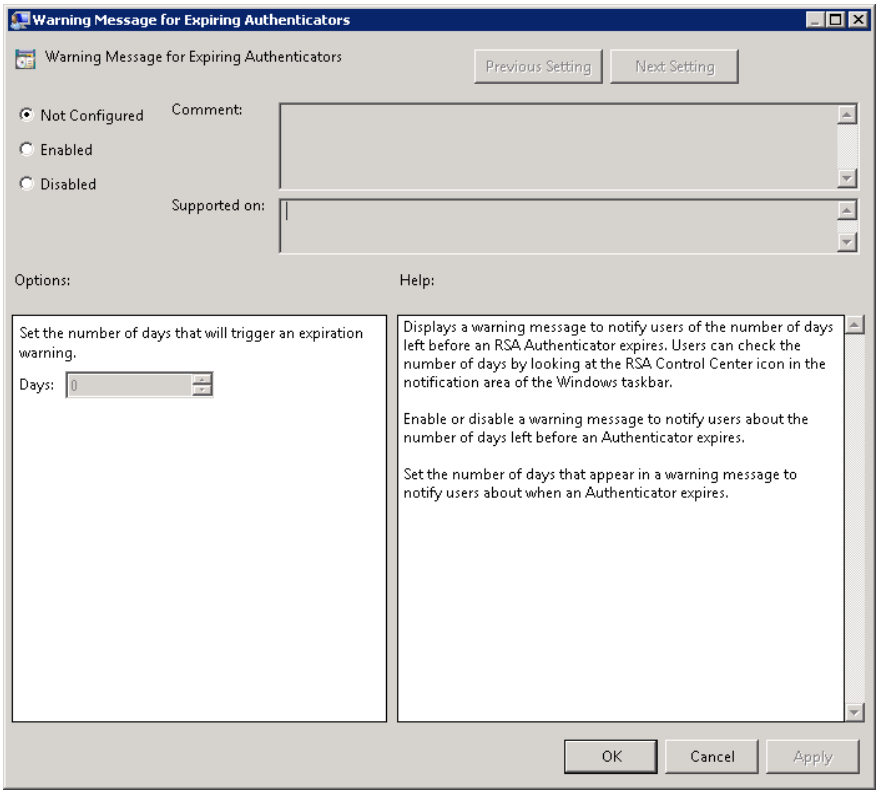
If the policy was modified on the domain controller, the settings load into the Windows registry once the refresh interval ends in the domain.

Define the SecurID Authenticator Expiration Message

The **Warning Message for Expiring Authenticators** folder contains a setting to configure a warning message to notify users of the number of days left before the expiration of an RSA SecurID authenticator connected to the USB port. Users can view the number of days before the expiration date from the RSA Security Center icon in the Windows task bar.

To configure an expiration warning message for an RSA SecurID authenticator:

1. Make sure that you have installed the templates. For more information, see Chapter 2, "Installing Group Policy Object Templates."
2. Access the templates. For more information, see "Accessing the Group Policy Object Templates."
3. Double-click the **Warning Message for Expiring Authenticators**.
4. In the right pane, double-click the **Warning Message for Expiring Authenticators**. A dialog box opens with a definition of the setting:



5. Select one of the following:
   - **Not Configured.** This state is the default behavior. Users are not notified that their token may expire soon.
   - **Enabled.** This state notifies users of the number of days left before their connected USB token expires. See the next step.
   - **Disabled.** This state notifies the user that the USB token will expire within 15 days of expiration.
6. If you select **Enabled**, set the number of days to trigger an expiration warning message in the Options field.
7. Click **Apply**.
8. Click **OK**.
9. Close the Group Policy Management Editor.

If the policy was modified on the domain controller, the settings load into the Windows registry once the refresh interval ends in the domain.

Configure the RSA Credential Provider Filter Settings

The **Credential Provider Filter Options** folder contains settings to define how Authentication Agent responds when users log on to Windows 7, Windows Vista, or Windows Server 2008 computers.

When you install the RSA Credential Provider Filter template, RSA Authentication Agent allows users to log on by default through the RSA SecurID Credential Provider or another third-party credential providers that you install and configure.

Note: To ensure that users cannot change the default (or another setting), you must install the template, make any changes, and enforce the policy on the domain controller. For more information about enforcing a policy, go to the Windows Server Group Policy page in the Microsoft Support Knowledge Base at **http://www.microsoft.com/grouppolicy/**.

To configure the Credential Provider filter settings:

1. Make sure that you have installed the templates. For more information, see Chapter 2, "Installing Group Policy Object Templates."
2. Access the templates. For more information, see "Accessing the Group Policy Object Templates."
3. Double-click the **Credential Provider Filter Settings** folder, and locate the settings in the right pane of the dialog box.
4. Double-click one of the following settings to exclude (hide) the associated Credential Provider tile from users:

- **Exclude the Microsoft Password Credential Provider.** Hides the Microsoft Credential Provider tiles that allow users to log on with their Windows accounts. If this policy is disabled, the Microsoft Password Credential Provider is presented at logon and in the User Account Control (UAC) dialog.
- **Exclude the Smart Card Credential Provider.** Hides the Credential Provider tiles that allow users to log on with their logon certificates on their smart cards. If this policy is disabled and the RSA SecurID 800 Authenticator is connected, the RSA Smart Card Credential Provider is presented at logon, in the UAC dialog, and in the Windows Security dialog.
- **Exclude the Microsoft Picture Password Credential Providers.** Hides the Credential Provider tiles that allow users to log on through the Microsoft Picture Password Credential Provider tile (picture with patterns). If this policy is disabled, the Picture Password Credential Provider is not excluded. The users can create pictures to use as their logon credentials.
- **Exclude the Microsoft PIN Credential Providers**. Hides Credential Provider tiles that allow users to log on through the Microsoft PIN Credential Provider tile. This is the PIN connected to the local or Windows Live ID account logon. If this policy is disabled, the Microsoft PIN Credential Provider tile is not excluded. If users have Windows Live ID accounts, they can create PINs for those accounts.
- **Exclude the Microsoft Windows Live ID Credential Providers.** Hides Credential Provider tiles that allow users to log on through the Microsoft Windows Live ID Credential Provider tile used for Live ID accounts (e-mail addresses and passwords). If this policy is disabled, the Microsoft Windows Live ID Credential Provider tile is not excluded. Users can create and log on with Windows Live ID accounts.
- **Exclude the RSA SecurID Credential Provider for connected authenticators.** Hides the RSA SecurID Credential Provider that allows users to log on with RSA SecurID using an authenticator connected to the USB port. If this policy is disabled, the Connected SecurID Credential Provider is not excluded and is presented to the user at logon, in the UAC dialog, and in the Windows Security dialog.
- **Exclude the RSA SecurID Credential Provider for disconnected authenticators.** Hides the RSA SecurID Credential Provider that allows users to log on with RSA SecurID using an authenticator not connected to the USB port. If this policy is disabled, the Disconnected SecurID Credential Provider is not excluded and is presented to the user at logon, in the UAC dialog, and in the Windows Security dialog.

  Important: If only this policy is enabled, users do not see any Credential Provider tiles until they have connected an RSA SecurID 800 Authenticator.

- **Exclude the RSA Smart Card Credential Provider.** Hides the RSA Credential Provider tile that allows users to log on with their Windows accounts on their smart cards. If this policy is not configured or is disabled, the RSA Credential Provider tile is available at logon, in the UAC dialog, and in the Windows Security dialog.

- **Exclude All Third-Party Credential Providers.** Hides any third-party Credential Provider tiles that allow users to log on with other log on methods. If this policy is not configured or is disabled, no third-party credential providers are excluded.

5. For each of the Credential Provider settings, select one of the following:
   - **Not Configured.** The associated Credential Provider tile or tiles are available for users at logon.
   - **Enabled.** The associated Credential Provider tile or tiles are unavailable for users at logon.
   - **Disabled.** This deactivates the setting.
6. Click **Apply**.
7. Do one of the following:
   - To access the next Credential Provider setting, click **Next Setting**. Then repeat steps 4 and 5. (If necessary, click **Previous Setting**.)
   - Click **OK** to return to the **Credential Provider Filter Settings** folder.
8. Close the Group Policy Management Editor.

   If the policy was modified on the domain controller, the settings are loaded into the Windows registry once the refresh interval ends in the domain.

Verify RSA Shared Components

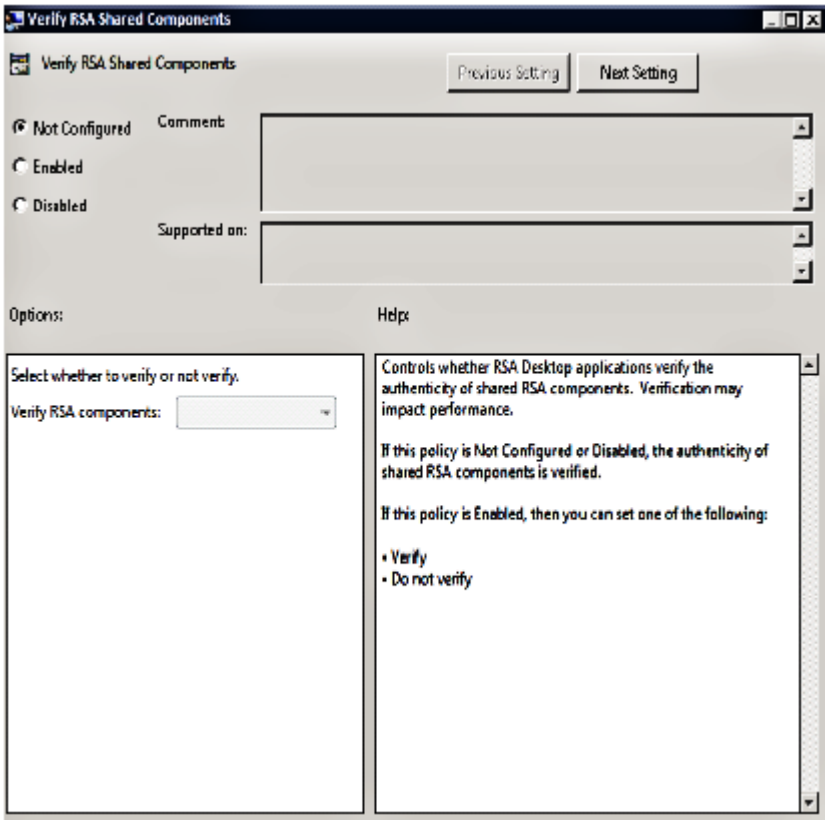
The **Common Settings** folder contains a template for controlling whether or not RSA Desktop applications verify the authenticity of shared RSA components. Verifying authenticity makes the system more secure, but verification may impact system performance.

The default state of this template is Not Configured. If the policy setting is Not Configured or Disabled, the authenticity of shared RSA components is verified. If you do not want applications to verify the authenticity of shared RSA components, select the **Enabled** state, and then select **Do not verify**.

To set verification settings of RSA shared components:

1. Make sure that you have installed the templates. For more information, see Chapter 2, “Installing Group Policy Object Templates.”
2. Access the templates. For more information, see “Accessing the Group Policy Object Templates.”
3. Double-click the **Common Settings** folder.

4. In the right pane, double-click **Verify RSA Shared Components**. A dialog box similar to below opens with a definition of the setting.



5. Select one of the following:
   - **Not Configured.** The authenticity of shared RSA components **is** verified.
   - **Enabled.** Select **Verify** or **Do not verify**.
   - **Disabled.** The authenticity of shared RSA components **is** verified.
6. Click **Apply**.
7. Click **OK**.
8. Close the Group Policy Management Editor.

   If the policy was modified on the domain controller, the settings are loaded into the Windows registry once the refresh interval ends in the domain.