

Using Group Policy Object Templates with RSA Authentication Agent 7.0 for Microsoft Windows



The Security Division of EMC

Contact Information

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

Trademarks

RSA and the RSA logo are registered trademarks of RSA Security Inc. in the United States and/or other countries. For the most up-to-date listing of RSA trademarks, go to www.rsa.com/legal/trademarks_list.pdf. EMC is a registered trademark of EMC Corporation. All other goods and/or services mentioned are trademarks of their respective companies.

License agreement

This software and the associated documentation are proprietary and confidential to RSA, 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 RSA.

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

Limit distribution of this document to trusted personnel.

Contents

Preface	5
About This Guide.....	5
RSA Authentication Agent 7.0 for Microsoft Windows Documentation.....	5
Related Documentation.....	6
Getting Support and Service	6
Before You Call Customer Support.....	6
Chapter 1: Understanding the Group Policy Object Templates	7
Overview of Authentication Agent for Microsoft Windows	7
Overview of the Group Policy Object Templates.....	8
Local Authentication Template.....	9
Credential Provider Settings	10
Local Authentication Settings.....	11
Chapter 2: Configuring Group Policy Object Template Settings ...	13
Preparing to Install the RSA Group Policy Object Templates.....	13
Installing the RSA Group Policy Object Templates	13
Defining the Local Authentication Preference Settings.....	15
Defining the Credential Provider Settings	18
Defining the Local Authentication Settings.....	19
Configuring Preference Settings Using Logon Scripts	25
Credential Provider Filtering Type Setting.....	25
Challenge Setting	26
Cached Challenge Setting	29
Windows Logon Setting	30
SecurID PIN Setting	31

Preface

About This Guide

This guide describes how administrators can use Group Policy Object templates to manage RSA Authentication Agent 7.0 for Microsoft Windows (Authentication Agent). When combined with RSA Authentication Manager 6.1 with Patch 2, Authentication Agent enhances native Windows security with strong, two-factor authentication using RSA SecurID tokens.

RSA Authentication Agent 7.0 for Microsoft Windows Documentation

For more information about RSA Authentication Agent 7.0 for Microsoft Windows, see the following documentation and Help:

Release Notes. Provides information about what is new and changed in this release, as well as workarounds for known issues. The latest *Release Notes* version is available from RSA SecurCare Online: <https://knowledge.rsasecurity.com>.

RSA Authentication Agent 7.0 for Microsoft Windows Installation and Administration Guide. Provides instructions on how to install, configure, troubleshoot, repair, or remove the product.

RSA Security Center Help. Describes the user options available in the RSA Security Center (the user interface of RSA Authentication Agent). All of the user options appear in the **Home** tab. To view the Help, click **Help** from the RSA Security Center menu or any dialog box.

RSA Security Center Administrator Help. Describes the configuration options available to administrators in the RSA Security Center (the user interface of RSA Authentication Agent). All of the administrator options appear in the **Configuration** tab. Any changes made through the Security Center only affect the local computer. To view the Help, click **Help** from the RSA Security Center menu or any dialog box.

Related Documentation

For more information about the products related to RSA Authentication Agent 7.0 for Microsoft Windows, see the following:

RSA Authentication Manager documentation set. The full documentation set for RSA Authentication Manager 6.1 (with the *RSA Authentication Manager 6.1.2 Readme*). To access a documentation set, go to <http://knowledge.rsasecurity.com>.

RSA Secured Partner Solutions directory. RSA has worked with a number of manufacturers to qualify software that works with RSA products. Qualified third-party products include virtual private network (VPN) and remote access servers (RAS), routers, web servers, and many more. To access the directory, including implementation guides and other information, go to <http://www.rsasecured.com>.

Getting Support and Service

RSA SecurCare Online	https://knowledge.rsasecurity.com
Customer Support Information	www.rsa.com/support
RSA Secured Partner Solutions Directory	www.rsasecured.com

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 Secured Partner Solutions Directory provides information about third-party hardware and software products that have been certified to work with RSA products. The directory includes Implementation Guides with step-by-step instructions and other information about using RSA products with these third-party products.

Before You Call Customer Support

Make sure that you have direct access to the computer running the RSA Authentication Agent 7.0 for Microsoft Windows software.

Please have the following information available when you call:

- Your RSA Customer/License ID for Authentication Manager.
- RSA Authentication Agent for Microsoft Windows software version number.
- The make and model of the machine.
- The name and version of the operating system.

1

Understanding the Group Policy Object Templates

This chapter describes the options you can set in the Group Policy Object templates to manage RSA Authentication Agent for Microsoft Windows. For details on installing the templates on the domain controller and setting the options, see Chapter 2, [“Configuring Group Policy Object Template Settings.”](#)

Overview of Authentication Agent for Microsoft Windows

RSA Authentication Agent 7.0 for Microsoft Windows works with RSA Authentication Manager 6.1 with Patch 2 to protect your company’s resources. Authentication Agent uses two-factor authentication to protect access to computers with a Windows Vista operating system. Two-factor authentication requires something you know (for example, an RSA SecurID PIN) and something you have (for example, a tokencode generated by an RSA SecurID token).

Note: You must use a hand-held RSA SecurID token with RSA Authentication Agent. For example, you cannot use a software token on your computer or a SecurID token connected to the USB port. But, you can use Authentication Agent with a software token installed on a portable device, for example, a Blackberry. For more information on software tokens, see the RSA documentation that came with your software token.

If you require a user to log on through Authentication Agent, the user may need to enter an RSA SecurID PIN followed by a tokencode to access the computer. The SecurID PIN and tokencode are known as the passcode. The first time users authenticate with passcodes, they create their SecurID PINs (automatically or manually). The tokencode appears as numbers on the front of a handheld SecurID token. The numbers change approximately every minute.

When a user enters a passcode, Authentication Agent sends the passcode to Authentication Manager for validation. If the passcode is correct, the user gains access to the desktop. Authentication Agent intercepts attempts to access local Windows desktops on users’ workstations and prompts users for RSA SecurID passcodes.

To deploy local authentication, you can use the configuration wizard to configure options and deploy it to multiple desktops. Once installed, you can manage Authentication Agent on individual computers through the RSA Security Center (user interface of Authentication Agent) or use the Group Policy Object templates to manage multiple computers. For more information on using the configuration wizard, see the *RSA Authentication Agent 7.0 for Microsoft Windows Installation and Administration Guide*. For more information on managing options for a local computer, see the RSA Security Center Administrator Help.

Overview of the Group Policy Object Templates

RSA Group Policy Object templates makes it easier for you manage Authentication Agent on many computers after you deploy it. To use the Group Policy Object templates, you load them into the Microsoft Policy Management tool on your domain controller and specify authentication policy settings in the templates. Each workstation within the domain automatically downloads the settings and then loads them into the Microsoft Registry.

In domain environments, all computers wait for specified refresh intervals before updating their settings. Once the refresh process ends, settings associated with the templates load into the Microsoft Registry. The settings specified in the Group Policy Object templates override the settings configured on individual workstations.

Important: The RSA templates are not policies. Windows stores RSA settings under **HKEY_LOCAL_MACHINE > Software > RSA** in the Registry Editor keys because they are preference settings instead of policy settings. For more information, see “[Local Authentication Template](#)” on page 9.

The Authentication Agent supports the Local Authentication template (**RSA_AuthAgent_LocalAuth.adm**). It allows you to define policy settings to control how Authentication Agent requires users to authenticate.

This template does not automatically come with the product. To obtain this Group Policy Object template, go to the Authentication Agent product page on the RSA web site (www.rsa.com) and see the download page. (Go to the RSA Authentication Agent [Try/Evaluate page](#) and click **Downloads** from the bottom of the page.)

Note: You cannot install RSA Authentication Agent 7.0 for Microsoft Windows on the domain controller. But if you have domain users, you can install RSA Authentication Agent 6.1 or 6.4 on the domain controller. To synchronize the password for a domain user, use the Password Synchronization template (**RSA_SID_PFC.adm**) from the Authentication Agent download page. (Go to the RSA Authentication Agent [Try/Evaluate page](#) and click **Downloads** from the bottom of the page.) For information on how to set the Password Synchronization template (**RSA_SID_PFC.adm**), see the *Using Group Policy Object Templates to Manage RSA Authentication Agent* guide for version 6.1 or 6.4 on the RSA Authentication Agent [download page](#).

Local Authentication Template

The Local Authentication template (**RSA_AuthAgent_LocalAuth.adm**) contains preference settings that you define to control how Authentication Agent appears to users. For example, you can specify what Credential Provider (logon prompt options) you want users to see, define challenge groups, set the logon field label, send the domain and user name to Authentication Manager, and define the ability to unlock the computer with an RSA SecurID PIN instead of a full passcode (PIN and tokencode). (You can also find these settings under the **Configuration** tab of the RSA Security Center.)

The Local Authentication template has the following two preference settings folders:

- Credential Provider Settings
- Local Authentication Settings

Important: The RSA templates are not policies. They are preference settings. Policies include settings that Windows stores in the Registry Editor keys under **Software > Policies**. Windows stores the RSA preference settings under **HKEY_LOCAL_MACHINE > Software > RSA** in the Registry Editor keys. You do not find them under **Policies**. If you configure a policy setting, the changes take effect as soon as they deploy to the computers in the domain. If you configure a preference setting, it also takes effect as soon it deploys through the domain. But, if you later decide to clear a preference setting and place it in an “unconfigured” state, Windows cannot apply the change (as it can with a policy setting). Instead, it retains the last setting you used. For example, if you enabled the Credential Provider filter setting and selected the **Show all available Credential Providers** options, users can see all the available logon tiles to log on to the computer. If you later access the preference again and select the **Not Configured** option, Windows retains the **Show all available Credential Providers** setting. Users will continue to see all the available logon tiles. You must select another option for the setting or select **Disable** to clear it.

Each preference folder contains subfolders. The subfolders contain preferences with settings that allow you to control different authentication components. For details on the Credential Provider Settings and Local Authentication Settings preferences, see [“Credential Provider Settings”](#) on page 10 or [“Local Authentication Settings”](#) on page 11.

Credential Provider Settings

As described in the previous section, the Local Authentication template (**RSA_AuthAgent_LocalAuth.adm**) contains the **Credential Provider Settings** and **Local Authentication Settings** preference folders. This section describes the Credential Provider Settings options. For details on the Local Authentication Settings options, see [“Local Authentication Settings”](#) on page 11.

The **Credential Provider Settings** folder contains a folder with the **Credential Provider Filter Type** setting. You can select one of the following for the setting:

- **Enable** (to activate)
- **Not Configured** (to leave inactive)
- **Disable** (to clear a previously enabled setting).

If you select **Enable**, you can select one of the following filtering types from the drop-down list:

- **Hide Microsoft Password Provider (default)**. Prevents users from logging on with Microsoft Windows passwords using the Microsoft Password Credential Provider. (Other Credential Providers remain available.) This is the default credential provider filter setting.
- **Only show RSA Authentication Agent Provider**. Prevents users from logging on using any method other than RSA SecurID passcodes.
- **Hide RSA Authentication Agent Provider**. Prevents users from logging on with RSA SecurID passcodes (PINs and tokencodes). (Other Credential Providers remain available.)
- **Show all available Credential Providers**. Allows users to log on using all available Credential Providers. Selecting this option ensures that users can log on to their workstations in case RSA SecurID is not available. For example, you may want to select this option until RSA SecurID is fully deployed throughout your company.

For more information on configuring the Credential Provider Filter Type preference, see [“Defining the Credential Provider Settings”](#) on page 18.

Local Authentication Settings

As described in [“Overview of the Group Policy Object Templates”](#) on page 8, the Local Authentication template (**RSA_AuthAgent_LocalAuth.adm**) contains the **Credential Provider Settings** and **Local Authentication Settings** preference folders. This section describes the Local Authentication Settings options. For details on the Credential Provider Settings options, see [“Credential Provider Settings”](#) on page 10.

The **Local Authentication Settings** folder contains the **Challenge**, **Authentication**, and **Unlocking Computer** folders.

These folders contain different preferences that you can set. For example, you can allow or deny the ability for a local administrator to define challenge groups. You can also define the users and groups that you want Authentication Agent to challenge for a SecurID passcode (PIN and tokencode). And, you can determine if you want to allow users to unlock their computer with a SecurID PIN instead of a full passcode.

The **Challenge** folder contains these preference settings:

- **Deny Access to Local Authentication Challenge Settings for Local Administrators**
- **Challenge Users**
- **Specify Challenge Group**
- **Allow Retrieval of Locally Cached Challenge Settings**

You can define the settings to allow or deny the ability for a local administrator to define challenge groups. You can also define users and groups you want Authentication Agent to challenge for a SecurID passcode (PIN and tokencode) and allow Authentication Agent to locate the local cached challenge setting from a local cache if it cannot determine the challenge status due to a network connection failure. For example, you can select one of the following for the **Deny Access to Local Authentication Challenge Settings for Local Administrators** setting:

- **Enable** (to activate)
- **Not Configured** (to leave inactive)
- **Disable** (to clear a previously enabled setting).

The **Authentication** folder contains these preference settings:

- **Label for the Local Authentication Prompt**
- **Send Domain and User Name to Authentication Manager**

With these preferences, you can set the logon label (**Password** or **Passcode**) and allow Authentication Agent to send the domain and user name to Authentication Manager to keep the accounts synchronized for online and offline authentication.

The **Unlocking Computer** folder has these preference settings:

- **Unlock with RSA SecurID PIN**
- **RSA SecurID PIN Time-Out**
- **RSA SecurID PIN Attempts**



With these preferences, you can set the option to allow the user to unlock the computer with a PIN instead of a full passcode, define the time allowed to enter a PIN before Authentication Agent requires a passcode, and specify the number of PIN attempts you want to allow.

For more information on configuring the Challenge, Authentication, and Unlocking computer preferences, see [“Defining the Local Authentication Settings”](#) on page 19.

2

Configuring Group Policy Object Template Settings

This chapter describes how to install and define the RSA Authentication Agent 7.0 for Microsoft Windows Group Policy Object settings.

Preparing 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 on Group Policy, go to the Windows Server Group Policy page in the Microsoft Support Knowledge Base at <http://www.microsoft.com/grouppolicy/>.

Important: The RSA templates are not policies. Policies include settings that Windows stores in the Registry Editor keys under **Software > Policies**. Windows stores RSA settings under **HKEY_LOCAL_MACHINE > Software > RSA** in the Registry Editor keys because they are preference settings instead of policy settings. This difference affects how Windows applies a setting if you define it and later want to set it to an “unconfigured” state. For more information, see “[Local Authentication Template](#)” on page 9.

As an alternative to using the RSA Group Policy Object templates, you can apply preference settings by incorporating them in logon scripts. For more information, see “[Configuring Preference Settings Using Logon Scripts](#)” on page 25.

Installing the RSA Group Policy Object Templates

As described in Chapter 1, “[Understanding the Group Policy Object Templates](#),” Authentication Agent supports the **Local Authentication template (RSA_AuthAgent_LocalAuth.adm)**. It allows you to define policy settings to control how Authentication Agent requires users to authenticate.

This template does not automatically come with the product. To obtain this Group Policy Object template, go to the Authentication Agent product page on the RSA web site (www.rsa.com) and see the download page. (Go to the RSA Authentication Agent [Try/Evaluate page](#) and click **Downloads** from the bottom of the page.)

Note: You cannot install RSA Authentication Agent 7.0 for Microsoft Windows on the domain controller. But if you have domain users, you can install RSA Authentication Agent 6.1 or 6.4 on the domain controller. To synchronize the password for a domain user, use the Password Synchronization template (**RSA_SID_PFC.adm**) from the Authentication Agent download page. (Go to the RSA Authentication Agent [Try/Evaluate page](#) and click **Downloads** from the bottom of the page.) For information on how to set the Password Synchronization template (**RSA_SID_PFC.adm**), see the *Using Group Policy Object Templates to Manage RSA Authentication Agent* guide for version 6.1 or 6.4 on the RSA Authentication Agent [download page](#).

To apply the template settings to computers on the network, install the template on the domain controller. You can set up groups of computers for a domain if you do not want to apply the template settings to all the computers on the domain.

The procedure for installing the templates varies, depending on the tool you use to launch the Group Policy Editor. The following procedures describe how to install the templates using the Active Directory Users and Computers Microsoft Management Console.

To install the templates on the domain controller:

1. Copy the Local Authentication template (**RSA_AuthAgent_LocalAuth.adm**) to a local drive on the domain controller (Windows Server 2000 or 2003 with latest service packs).
2. Click **Start > Administrative Tools > Active Directory Users and Computers**.
3. From the Active Directory Users and Computers console, right-click the name of the domain where you want to install the Local Authentication template, and click **Properties**.
4. In the Properties dialog box, click the **Group Policy** tab. Select the policy where you want to add the template, and click **Edit**.
5. Click **Computer Configuration**. Then right-click **Administrative Template** and click **Add/Remove Templates** to open the Add/Remove Templates dialog box.
6. Click **Add**.
7. Browse to the location of the **RSA_AuthAgent_LocalAuth.adm** file and click **Open**.
8. Click **Close**. Once you install a template on the domain controller, it applies the settings to all the computers on the domain. The preference settings default to a **Not Configured** state. To enable any of the settings, see the following sections.

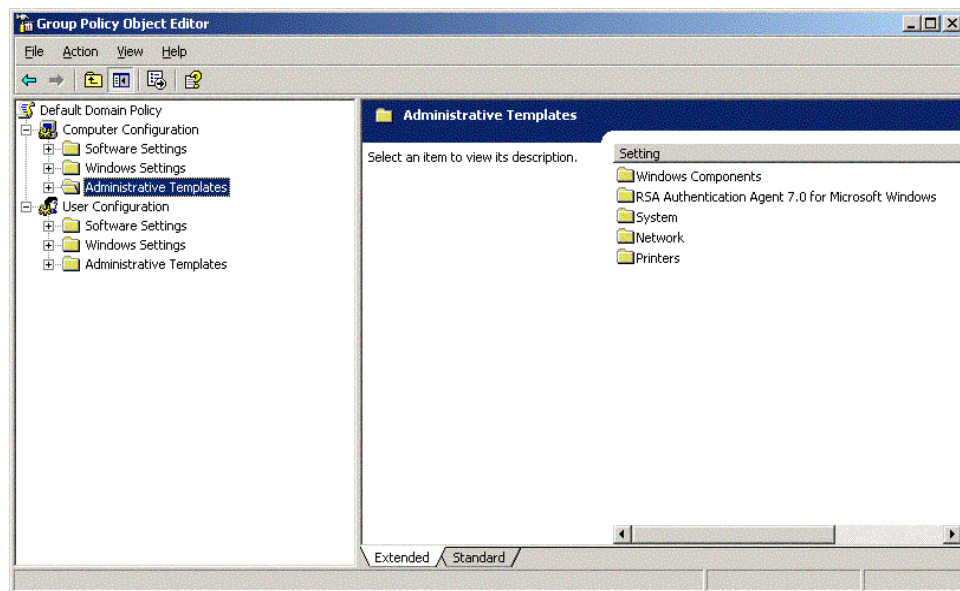
Note: In domain environments, all computers wait for specified refresh intervals before updating their settings. Once the refresh process ends, settings associated with the templates load into the Microsoft Registry. The settings specified in the Group Policy Object templates override the settings configured on individual workstations.

Defining the Local Authentication Preference Settings

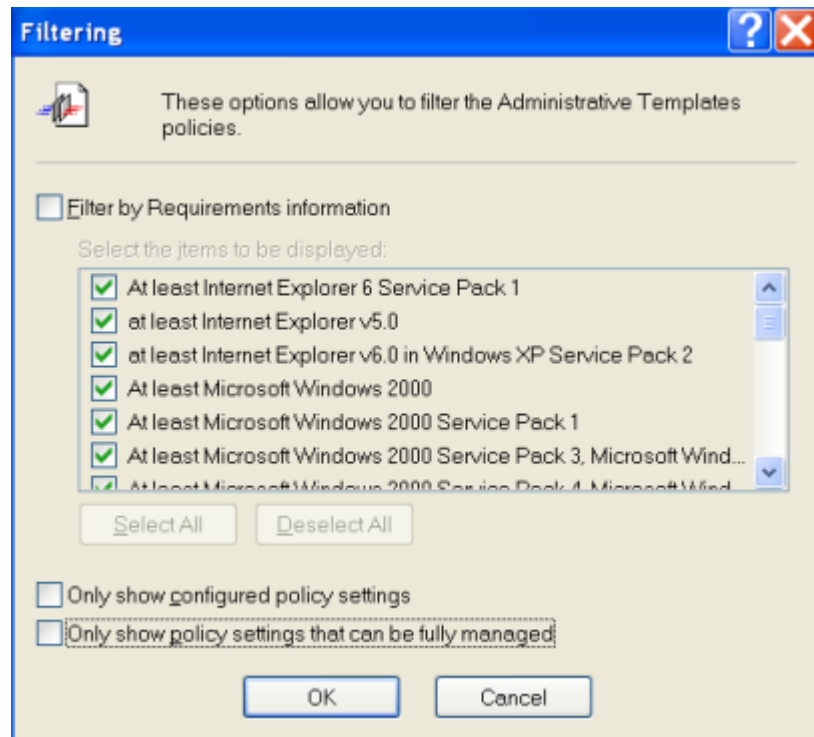
This section describes how to define the preference settings in the Local Authentication template (**RSA_AuthAgent_LocalAuth.adm**).

To define the settings in the Local Authentication template:

1. On the domain controller, click **Start > Administrator Tools > Active Directory Users and Computers**.
2. In the Active Directory Users and Computers dialog box, right-click the name of the domain, and click **Properties**.
3. Click the **Group Policy** tab.
4. In the Group Policy dialog box, click **Default Domain Policy**, then click **Edit**.
5. In the left pane of the Group Policy window, click **Administrative Templates**. Right-click **Administrative Templates > View > Filtering**.



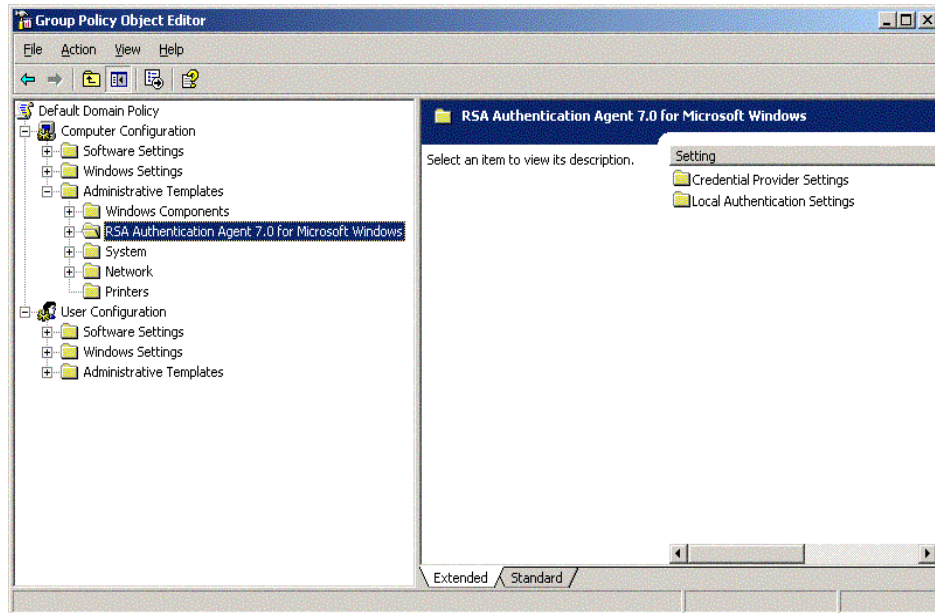
- In the Filtering dialog box, clear **Only show policy settings that can be fully managed**.



Because the RSA group policies are preferences and not true policies, you must clear this option to view the RSA Group Policy Object templates.

- Click **OK**.

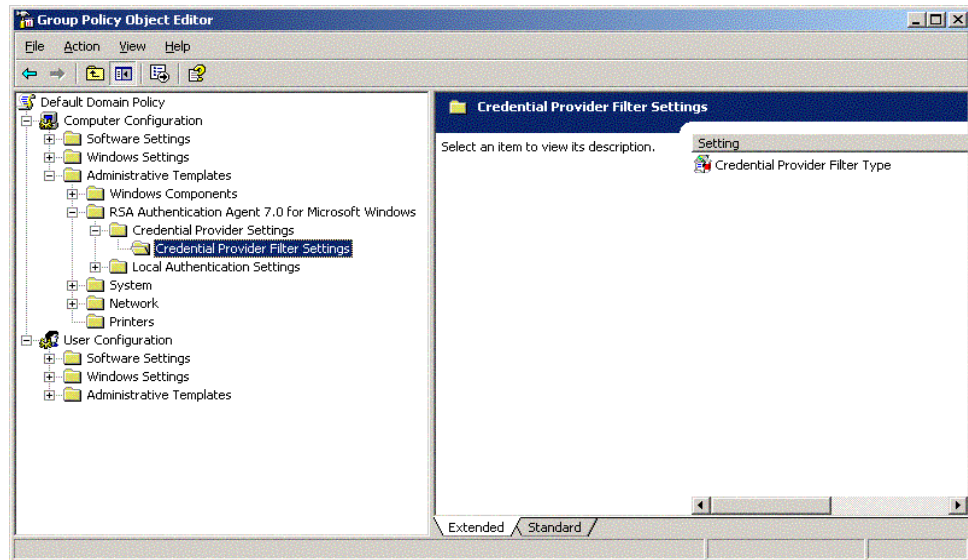
8. Double-click **Computer Configuration > Administrative Templates > RSA Authentication Agent 7.0 for Microsoft Windows**. You see the **Credential Provider Settings** and **Local Authentication Settings** preference folders as shown:



9. Click on the folders to access the preferences. For details on defining the Credential Provider Settings, see [“Defining the Credential Provider Settings”](#) on page 18. For details on defining the Local Authentication settings, see [“Defining the Local Authentication Settings”](#) on page 19.

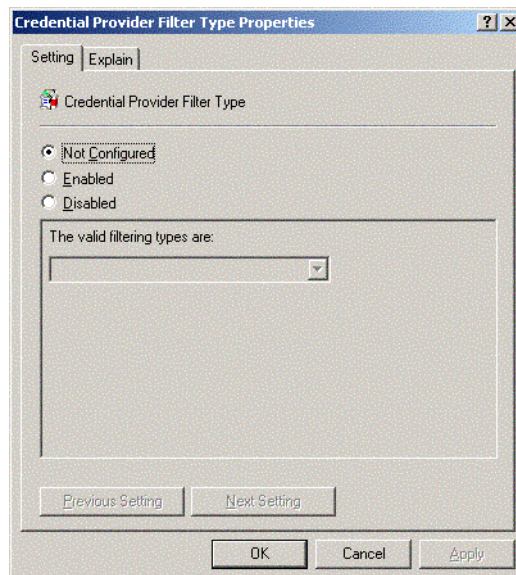
Defining the Credential Provider Settings

The **Credential Provider Filter Settings** folder contains the **Credential Provider Filter Type** preference as shown:



To define the **Credential Provider Filter Type** setting:

1. Double-click **Credential Provider Filter Type** to open the Credential Filter Type Properties dialog box. For example:

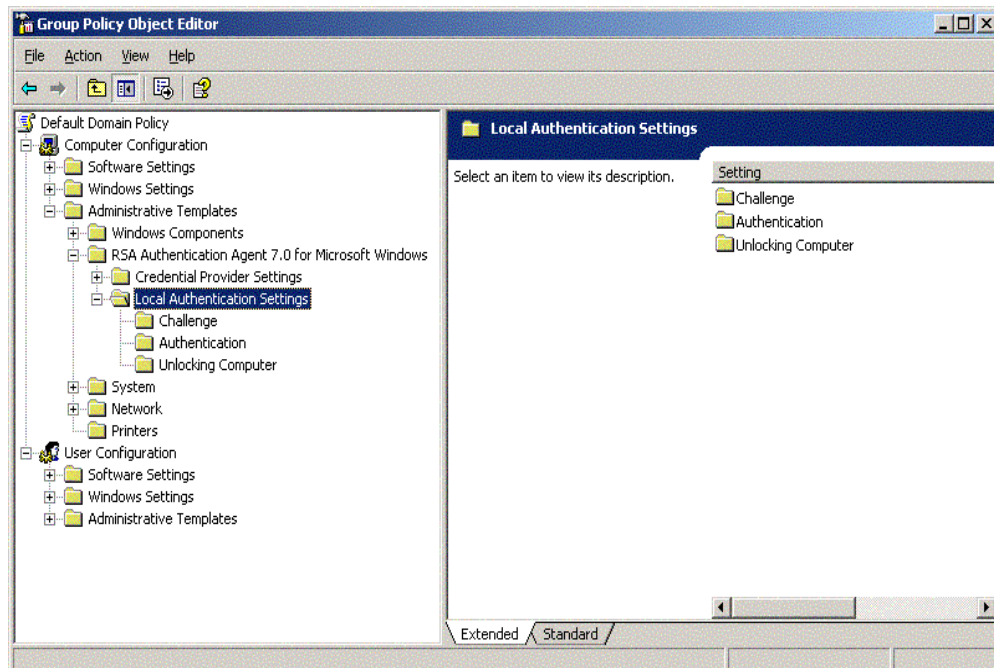


Note: Click the **Explain** tab to review a definition of the preference setting.

2. In the **Setting** tab, do one of the following:
 - Leave the default of **Not Configured** to leave the setting inactive.
 - Select **Enable** to activate the field setting. Then select one of the following from the drop-down list:
 - **Hide Microsoft Password Provider (default)**. Prevents users from logging on with Microsoft Windows passwords using the Microsoft Password Credential Provider. (Other Credential Providers remain available.) This is the default credential provider filter setting.
 - **Only show RSA Authentication Agent Provider**. Prevents users from logging on using any method other than RSA SecurID passcodes.
 - **Hide RSA Authentication Agent Provider**. Prevents users from logging on with RSA SecurID passcodes (PINs and tokencodes). (Other Credential Providers remain available.)
 - **Show all available Credential Providers**. Allows users to log on using all available Credential Providers. Selecting this option ensures that users can log on to their workstations in case RSA SecurID is not available. For example, you may want to select this option until RSA SecurID is fully deployed throughout your company.
 - Select **Disable** to clear the setting.
3. Click **Apply** to apply your changes. Then click **OK** to return to the **Credential Provider Filter Type** preference.

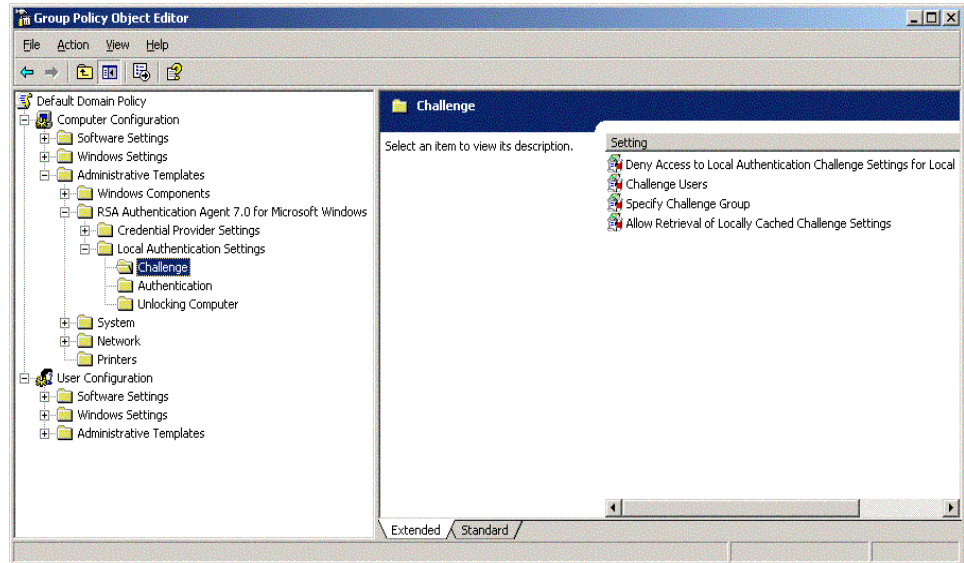
Defining the Local Authentication Settings

The **Local Authentication Settings** folder contains the **Challenge**, **Authentication**, and **Unlocking Computer** subfolders as shown:

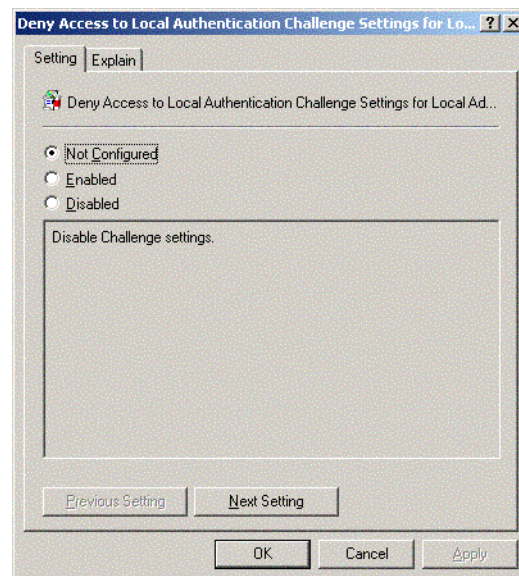


To define the Challenge setting:

1. Double-click the **Challenge** folder. You see the **Deny Access to Local Authentication Challenge Settings for Local Administrators, Challenge Users, Specify Challenge Group, and Allow Retrieval of Locally Cached Challenge Settings** preferences as shown:



2. Click the preference you want to set. For example, if you want to set the **Deny Access to Local Authentication Challenge Settings for Local Administrators** preference, click it to open the Deny Access to Local Authentication Challenge Settings for Local Administrators Properties dialog box:

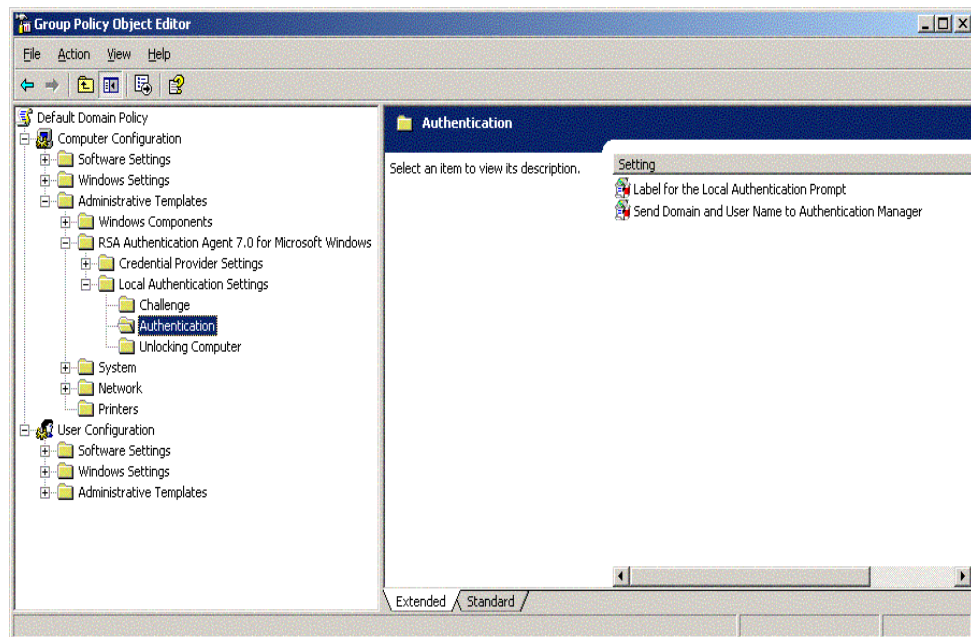


Note: Click the **Explain** tab to review a definition of the preference setting.

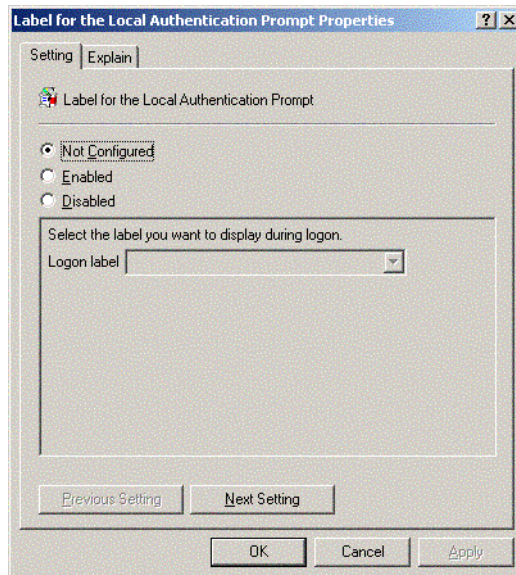
3. In the **Setting** tab, do one of the following:
 - Leave the default of **Not Configured** to leave the setting inactive.
 - Select **Enabled** to activate the field setting. This allows local administrators to define challenge users and groups.
 - Select **Disabled** to clear the setting.
4. Click **Apply** to apply your changes. Then click **OK** to return to the **Challenge** preferences.
5. Repeat the steps in this procedure for each preference you want to set. For example, if you to enable the **Challenge Users** preference, select **Off, Users In, All users**, or **All users except** from the drop-down list. Then enable the **Specific Challenge Group** preference and enter the name of the group you want to challenge in the **Group name** field. If you want to all allow Authentication Agent to locate the user's challenge setting from a local cache if it cannot determine the challenge status due to a network connection failure, enable the **Allow Retrieval of Locally Cached Challenge Settings** preference.

To define the Authentication setting:

1. Double-click the **Authentication** folder. You see you see the **Label for the Local Authentication Prompt** and the **Send Domain and User Name to Authentication Manager** preferences as shown:



2. Click the preference you want to set. For example, if you want to set the **Label for the Local Authentication Prompt** preference, click it to open the Label for the Local Authentication Prompt Properties dialog box:

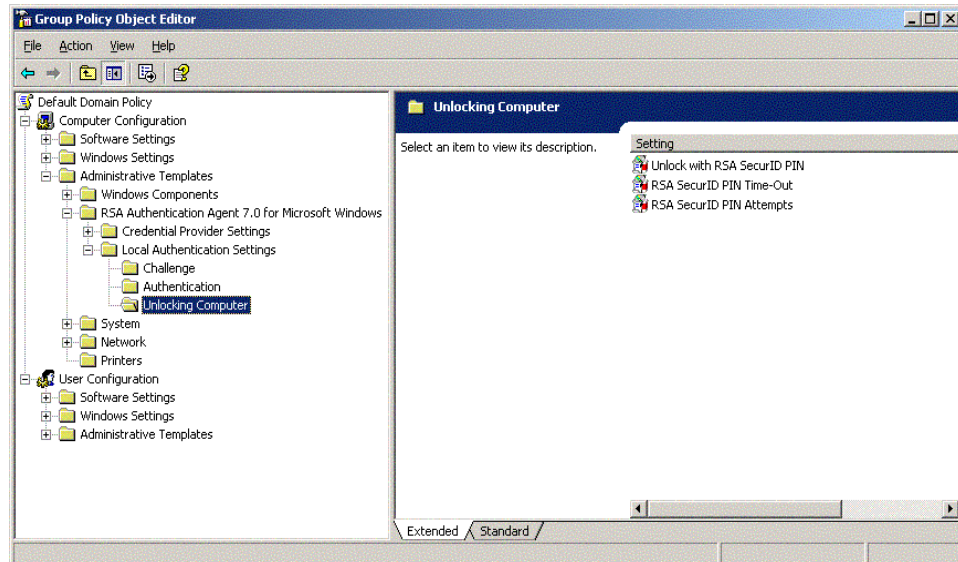


Note: Click the **Explain** tab to review a definition of the preference setting.

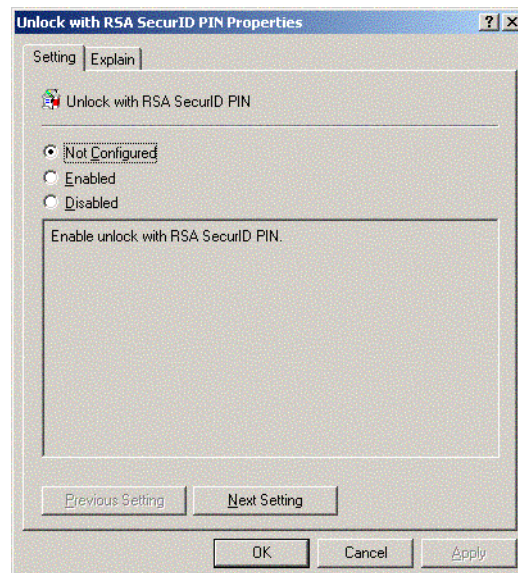
3. In the **Setting** tab, do one of the following:
 - Leave the default of **Not Configured** to leave the setting inactive.
 - Select **Enabled** to activate the field setting. This allows local administrators to define challenge users and groups.
 - Select **Disabled** to clear the setting.
4. If you select **Enabled**, select **Passcode** or **Password** from the **Logon label** field.
5. Click **Apply** to apply your changes. Then click **OK** to return to the **Authentication** preferences.
6. Repeat the steps in this procedure for the **Send Domain and User Name to Authentication Manager** preference. For example, you may want to enable this preference if you want to send the domain name and the user name to Authentication Manager instead of just the user name. This provides Authentication Manager with more account information to ensure security.

To define the Unlocking Computer setting:

1. Double-click the **Unlocking Computer** folder. You see the **Unlock with RSA SecurID PIN**, **RSA SecurID PIN Time-Out**, and **RSA SecurID PIN Attempts** preferences as shown:



2. Click the preference you want to set. For example, if you want to set the **Unlock with RSA SecurID PIN** preference, click it to open the Unlock with RSA SecurID PIN Properties dialog box:



Note: Click the **Explain** tab to review a definition of the preference setting.

3. In the **Setting** tab, do one of the following:
 - Leave the default of **Not Configured** to leave the setting inactive.
 - Select **Enabled** to activate the field setting. This allows local administrators to define challenge users and groups.
 - Select **Disabled** to clear the setting.
4. Click **Apply** to apply your changes. Then click **OK** to return to the **Authentication** preferences.
5. Repeat the steps in this procedure for each preference you want to set. For example, if you enabled the **Unlock with RSA SecurID PIN** preference, you may want to set the **RSA SecurID PIN Time-Out** and **RSA SecurID PIN Attempts** preferences. You can enable **RSA SecurID PIN Time-Out** to define the time allowed to enter a PIN to unlock the computer in the **Time-out** field. (The preference uses a default of 75 minutes. You can enter a time between 1 to 480 minutes.) Once the time elapses, the user must enter a PIN and tokencode to unlock the computer.
 If you enable the **RSA SecurID PIN Attempts** preference, you can set the number of attempts you want to allow the user to enter the PIN in the **Attempts** field. The preference uses a default of three (3) attempts. You can enter a value of 3 to 10.

Configuring Preference Settings Using Logon Scripts

As an alternative to using the RSA Group Policy Object template, you can apply preference settings by incorporating them in logon scripts.

The following charts provide details on the location of the root key and the registry settings associated with each Local Authentication preference template.

Credential Provider Filtering Type Setting

The following charts list the key, value name, value type, and options for the Credential Provider filtering type preference setting. They also include descriptions of the key and options.

Key	HKEY_LOCAL_MACHINE\SOFTWARE\RSA\RSA Authentication Agent\CurrentVersion\Settings\Credential Providers
Value Name	FilterType
Value Type	REG_DWORD
Description	Hides or shows the Credential Providers users can access to log on to computers.

Option	Value	Description
Hide Microsoft Password Provider	0	Prevents users from logging on with Microsoft Windows passwords using the Microsoft Password Credential Provider. (Other Credential Providers remain available.) This is the default credential provider filter setting.
Only show RSA Authentication Agent Provider	1	Prevents users from logging on using any method other than RSA SecurID passcodes.
Hide RSA Authentication Agent Provider	2	Prevents users from logging on with RSA SecurID passcodes (PINs and tokencodes). (Other Credential Providers remain available.)
Show all available Credential Providers	3	Allows users to log on using all available Credential Providers. Selecting this option ensures that users can log on to their workstations in case RSA SecurID is not available. For example, you may want to select this option until RSA SecurID is fully deployed throughout your company.

Challenge Setting

The following charts list the keys, value names, value types, and options for the Challenge preference setting. They also include descriptions of the keys and options.

Note: You create challenge groups using the Windows interface. For details on 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 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.

Key	HKEY_LOCAL_MACHINE\SOFTWARE\RSA\RSA Security Center
Value Name	DisableChallenge
Value Type	REG_DWORD
Description	Prevents local administrators from accessing the Deny Access to Local Authentication Challenge Settings for Local Administrators option to determine who Authentication Agent challenges for a SecurID passcode on the local computer.

Option	Value	Description
Disabled	0	Allows local administrators access to the Deny Access to Local Authentication Challenge Settings for Local Administrators option.
Enabled	1	Prevents local administrators from accessing the Deny Access to Local Authentication Challenge Settings for Local Administrators option.

Key	HKEY_LOCAL_MACHINE\SOFTWARE\RSA\RSA Authentication Agent\CurrentVersion\Settings\SDGINA
Value Name	Enabled
Value Type	REG_DWORD
Description	Activates the challenge group setting for you to define who Authentication Agent challenges for a SecurID passcode (PIN and tokencode) before allowing access to the computer.

Option	Value	Description
None	0	Prevents Authentication Agent from challenging any users.
Users in	1	Allows Authentication Agent to challenge users in a group for a passcode. Note: You also need to set the ChallengeGroup value to the name of the challenge group. See the following charts for details.
All users	2	Allows Authentication Agent to challenge all users, including administrators, for a passcode.
All users except	3	Allows Authentication Agent to challenge all users for a passcode except for those in a particular group. Note: You also need to set the ChallengeGroup value to the name of the group exception. See the following charts for details.

Key	HKEY_LOCAL_MACHINE\SOFTWARE\RSA\RSA Authentication Agent\CurrentVersion\Settings\SDGINA
Value Name	ChallengeGroup
Value Type	REG_SZ
Description	Allows you to specify the group that Authentication Agent challenges for a SecurID passcode (PIN and tokencode) before allowing access to the computer.

Option	Value	Description
Users in	\\ComputerName\ GroupName	Allows Authentication Agent to challenge users in a particular group for a passcode. Note: You need to enable the setting to define the users in a group for a SecurID passcode. See the previous charts for details.
All users except	\\ComputerName\ GroupName	Allows Authentication Agent to challenge all users, including administrators, for a passcode except for those in a particular group.

Key	HKEY_LOCAL_MACHINE\SOFTWARE\RSA\RSA Authentication Agent\CurrentVersion\Settings\SDGINA
Value Name	SendDomainName
Value Type	REG_SZ
Description	Allows the Agent to send the domain and user name to RSA Authentication Manager after authenticating with a SecurID passcode.

Option	Value	Description
Disabled	0	Prevents Authentication Agent from sending the domain and user name to RSA Authentication Manager.
Enabled	1	Allows Authentication Agent to send the domain and user name to RSA Authentication Manager.

Cached Challenge Setting

The following charts list the keys, value names, and value types for the Cached Challenge preference setting. They also include descriptions of the keys and values.

Key	HKEY_LOCAL_MACHINE\SOFTWARE\RSA\RSA Authentication Agent\CurrentVersion\Local\OASVC
Value Name	FailOpenPolicy
Value Type	REG_DWORD
Description	Allows Authentication Agent to use the locally cached policy setting to determine if it should challenge the user for SecurID passcode or not. When you enable the retrieval of challenge settings from the local cache, you must specify how you want the Agent to respond when a cached setting does not exist.

Option	Value	Description
Disabled	0	Prevents Authentication Agent from retrieving the challenge setting from the local cache.
Enabled	1	Allows Authentication Agent to retrieve the challenge setting from the local cache.

Key	HKEY_LOCAL_MACHINE\SOFTWARE\RSA\RSA Authentication Agent\CurrentVersion\Local\OASVC
Value Name	UnknownUsersChallengePolicy
Value Type	REG_DWORD
Description	Allows Authentication Agent to challenge the user for a SecurID passcode if the cached settings do not exist.

Option	Value	Description
Do not challenge	0	Prevents Authentication Agent from challenging the user for a SecurID passcode. Note: If set to 0, you must set FailOpenPolicy to 1.
Challenge	1	Allows Authentication Agent to challenge the user for a SecurID passcode.

Windows Logon Setting

The following charts list the keys, value names, and value types for the Windows Logon preference setting. They also include descriptions of the keys and values.

Key	HKEY_LOCAL_MACHINE\SOFTWARE\RSA\RSA Authentication Agent\CurrentVersion\Settings\SDGINA
Value Name	LogonPromptPassword
Value Type	REG_DWORD
Description	Sets the logon label for the Authentication Agent Credential Provider to Password or Passcode . Users see the field label you set when they attempt to log on to the computer.

Option	Value	Description
Passcode	0	Shows a logon field label of Passcode .
Password	1	Shows a logon field label of Password .

SecurID PIN Setting

The following charts list the keys, value names, and value types for the SecurID PIN setting. They also include descriptions of the keys and values.

Key	HKEY_LOCAL_MACHINE\SOFTWARE\RSA\RSA Authentication Agent\CurrentVersion\Settings\SDGINA
Value Name	EnablePinUnlock
Value Type	REG_DWORD
Description	Allows the user to unlock the computer by entering a SecurID PIN within a set amount of time after locking the computer. Once that time expires, users must enter a passcode to unlock the computer. For example, if you do not set this option, users must always enter full passcode (PIN and tokencode) instead of just a PIN to unlock the computer.

Option	Value	Description
Disabled	0	Requires the user to enter a passcode to unlock the computer.
Enabled	1	Allows the user to unlock the computer with a PIN within a set amount of time.

Key	HKEY_LOCAL_MACHINE\SOFTWARE\RSA\RSA Authentication Agent\CurrentVersion\Settings\SDGINA
Value Name	PinLifetime
Value Type	REG_DWORD
Description	Number of minutes a user has to unlock the computer with a PIN before the Agent requires a full passcode.

Option	Value	Description
Time-out	1 to 480 minutes (default = 75 minutes)	Number of minutes between 1 to 480 before the Agent requires a passcode instead of a PIN to unlock the computer.



Key	HKEY_LOCAL_MACHINE\SOFTWARE\RSA\RSA Authentication Agent\CurrentVersion\Settings\SDGINA
Value Name	PinAttempts
Value Type	REG_DWORD
Description	Number of times a user can enter an invalid PIN before the Agent requires a full passcode.

Option	Value	Description
Attempts	3 to 10 attempts (default = 3 attempts)	Number of invalid PIN attempts between 3 and 10 (default of 3) before the Agent requires a passcode to unlock the computer.