## Contents

**Figures** ........................................... vi

**Tables** ............................................. vii

**Preface** ........................................... ix
- About this publication .................................. ix
- Access to publications and terminology .......... ix
- Accessibility ........................................ x
- Technical training .................................... x
- Support information ................................... x
- Statement of Good Security Practices ............ x

**Chapter 1. Desktop Password Reset**
**Assistant overview** ................................ 1
- Desktop Password Reset Assistant features .... 1
- Desktop Password Reset Assistant configuration 1
  - Basic configuration of the IBM Security Identity Manager and Desktop Password Reset Assistant 2
  - Enhanced configuration ............................ 2

**Chapter 2. Installation planning for the Desktop Password Reset Assistant** ....... 3
- Preinstallation roadmap .............................. 3
- Installation roadmap ................................. 3
- Installation prerequisites ........................... 3
- Software download .................................... 4

**Chapter 3. Desktop Password Reset Assistant installation** .......................... 5
- Desktop and automated deployment in the enterprise 5
  - Installing the Desktop Password Reset Assistant with the graphical user interface 5
  - Installing the Desktop Password Reset Assistant manually or by using an automated installation 6
  - Installing the CA Certificate for the SSL connection 8

**Chapter 4. First steps after installation** ............................................. 9
- Password reset and Windows account unlock with Desktop Password Reset Assistant 9
- Identifying yourself to the assistant ............................. 9
- Account selection ..................................... 9
- Unlocking or resetting a password ...................... 10
- Customization of the Desktop Password Reset Assistant 10
  - IBM logo customization ............................. 11
  - Product title logo customization .................. 11
  - Background bitmap customization ................ 11
  - User interface labels customization .............. 11
  - Response user interface behavior customization 12
  - Use of the Desktop Password Reset Assistant with Screen Saver Unlock 12

**Chapter 5. Problem troubleshooting for the Desktop Password Reset Assistant** .... 13
- Techniques for troubleshooting problems .......... 13
- Warnings and error messages ....................... 15

**Chapter 6. Adapter updates** ........................................... 17

**Chapter 7. Uninstalling the adapter** ........................................... 19

**Appendix A. Support information** ........................................... 21
- Searching knowledge bases ........................... 21
- Obtaining a product fix ............................... 22
- Contacting IBM Support ............................... 22

**Appendix B. Accessibility features for IBM Security Identity Manager** ........... 25

**Notices** ............................................. 27

**Index** ................................................ 31
Figures

1. Basic configuration for the Desktop Password Reset Assistant ............... 2
2. Enhanced configuration for the Desktop Password Reset Assistant ........ 2
### Tables

1. Preinstallation roadmap ............... 3
2. Installation roadmap ................. 3
3. Prerequisites to install the Desktop Password Reset Assistant ............... 3
4. ChallengeResponse registry values .... 7
5. Product title details ................. 11
6. Background bitmap details ............ 11
7. User interface labels details ........... 12
8. ShowResponses string details ........... 12
9. ShowOnUnlock string details ........... 12
10. Warning and error messages ............ 15
Preface

About this publication

The Desktop Password Reset Assistant Installation and Configuration Guide provides the basic information that you need to install and configure the Desktop Password Reset Assistant for use with IBM® Security Identity Manager.

The Desktop Password Reset Assistant enables connectivity between the IBM Security Identity Manager server and a Windows desktop. The IBM Security Identity Manager server is the server for your IBM Security Identity Manager product.

After the adapter is installed and configured, IBM Security Identity Manager manages access to RSA Authentication Manager resources with your site's security system. This information describes how to install and configure the Desktop Password Reset Assistant.

Access to publications and terminology

This section provides:
- A list of publications in the IBM Security Identity Manager library.
- Links to Online publications.
- A link to the IBM Terminology website on page x.

IBM Security Identity Manager library


Online publications

IBM posts product publications when the product is released and when the publications are updated at the following locations:

IBM Security Identity Manager library


IBM Security Systems Documentation Central

[IBM Security Systems Documentation Central](http://www-05.ibm.com/e-business/linkweb/publications/servlet/pbi.wss) provides an alphabetical list of all IBM Security Systems product libraries and links to the online documentation for specific versions of each product.

IBM Publications Center

IBM Terminology website


Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface. You can also use the keyboard instead of the mouse to operate all features of the graphical user interface.

Technical training

For technical training information, see the following IBM Education website at [http://www.ibm.com/software/tivoli/education](http://www.ibm.com/software/tivoli/education).

Support information

IBM Support provides assistance with code-related problems and routine, short duration installation or usage questions. You can directly access the IBM Software Support site at [http://www.ibm.com/software/support/probsub.html](http://www.ibm.com/software/support/probsub.html).

Appendix A, “Support information,” on page 21 provides details about:

- What information to collect before contacting IBM Support.
- The various methods for contacting IBM Support.
- How to use IBM Support Assistant.
- Instructions and problem-determination resources to isolate and fix the problem yourself.

Note: The Community and Support tab on the product information center can provide additional support resources.

Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.
Chapter 1. Desktop Password Reset Assistant overview

The Desktop Password Reset Assistant software enables Windows users to perform self-service password resets and self-service unlocks from their desktops.

The Desktop Password Reset Assistant allows users who forget their passwords and cannot log in to their Windows accounts to reset the passwords and unlock the accounts.

The Desktop Password Reset Assistant is distributed as a Credential Provider for Windows Vista, Windows 7, Windows 8, and Windows 2008 server and 2012 server. It is visible as a link under the password prompt when you are logged out or the computer is locked.

Desktop Password Reset Assistant features

The Desktop Password Reset Assistant features are available to the user before logging into their Windows-based computer.

This provides the user a method for self-service password resets even if they have forgotten their Windows password. The Desktop Password Reset Assistant provides the ability for a user to perform the following functions:

- Self-service Windows password unlock without a password change
- Self-service password reset (change) and synchronization of all accounts
- Authentication using the secure challenge and response features of IBM Security Identity Manager
- Installation using a graphical user interface installer
- Compatibility with deployment tools such as Security Provisioning Manager or Microsoft SMS
- A translated user interface and support for double-byte languages
- A customizable user interface with support for company logos and backgrounds

Desktop Password Reset Assistant configuration

The IBM Security Identity Manager Desktop Password Reset Assistant can be installed in two configurations.

The first configuration is the basic configuration in which the IBM Security Identity Manager server and the Desktop Password Reset Assistant are installed on each user desktop computer. The second configuration is an enhanced solution that uses the basic configuration with optional IBM Security Access Manager for Enterprise Single Sign-On products.

Note: Both configurations require IBM Security Identity Manager adapters that are shipped separately. The Windows Active Directory Adapter and the IBM Security Access Manager for Enterprise Single Sign-On Adapter can be downloaded separately from the IBM Passport Advantage® site.
Basic configuration of the IBM Security Identity Manager and Desktop Password Reset Assistant

The basic configuration includes a single IBM Security Identity Manager server and the Desktop Password Reset Assistant installed on the Windows desktop of each user.

In this configuration, the Desktop Password Reset Assistant communicates to the IBM Security Identity Manager server to retrieve the user challenge questions and to validate the responses. After a successful authentication, the IBM Security Identity Manager generates password change, password reset, or password unlock commands to each account owned by the user.

Enhanced configuration

This configuration enhances the basic solution by including IBM Security Access Manager for Enterprise Single Sign-On products.

In this solution after a successful authentication, the IBM Security Access Manager for Enterprise Single Sign-On Adapter notifies the IBM Security Access Manager for Enterprise Single Sign-On IMS™ server, updating the passwords maintained in the IBM Security Access Manager for Enterprise Single Sign-On wallet for use with single sign-on features.
Chapter 2. Installation planning for the Desktop Password Reset Assistant

You must meet hardware, software, and authorization prerequisites before you install the Desktop Password Reset Assistant.

Verify that all of the prerequisites are met before you install the Desktop Password Reset Assistant.

Preinstallation roadmap

You must prepare the environment before you can install the Desktop Password Reset Assistant.

Table 1. Preinstallation roadmap

<table>
<thead>
<tr>
<th>What to do</th>
<th>Where to find more information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obtain the installation software</td>
<td>Download the software from Passport Advantage. See &quot;Software download&quot; on page 4.</td>
</tr>
<tr>
<td>Verify that the software and hardware requirements for the adapter that you want to install have been met.</td>
<td>See &quot;Installation prerequisites.&quot;</td>
</tr>
</tbody>
</table>

Installation roadmap

You must complete the necessary steps to install the Desktop Password Reset Assistant, including completing post-installation configuration tasks and verifying the installation.

Table 2. Installation roadmap

<table>
<thead>
<tr>
<th>What to do</th>
<th>Where to find more information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install the Desktop Password Reset Assistant.</td>
<td>See &quot;Desktop and automated deployment in the enterprise&quot; on page 5.</td>
</tr>
<tr>
<td>Install the certificates.</td>
<td>See &quot;Installing the CA Certificate for the SSL connection&quot; on page 8.</td>
</tr>
</tbody>
</table>

Installation prerequisites

Use this table to identify the software prerequisites to install the Desktop Password Reset Assistant. Verify that all of the prerequisites are satisfied before installing the Desktop Password Reset Assistant.

Table 3. Prerequisites to install the Desktop Password Reset Assistant

<table>
<thead>
<tr>
<th>Prerequisites</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>• Windows 7</td>
</tr>
<tr>
<td></td>
<td>• Windows 8</td>
</tr>
<tr>
<td></td>
<td>• Windows 2008 server</td>
</tr>
<tr>
<td></td>
<td>• Windows 2012 server</td>
</tr>
</tbody>
</table>
**Table 3. Prerequisites to install the Desktop Password Reset Assistant (continued)**

<table>
<thead>
<tr>
<th>Prerequisites</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Access Manager for Enterprise Single Sign-On products</td>
<td>Version 5.1 or later</td>
</tr>
<tr>
<td>Security Access Manager for Enterprise Single Sign-On Adapter</td>
<td>Version 5.1</td>
</tr>
<tr>
<td>IBM Security Identity Manager Windows Active Directory Adapter</td>
<td>Version 6.0</td>
</tr>
<tr>
<td>IBM Security Identity Manager Windows Local Account Adapter</td>
<td>Version 6.0</td>
</tr>
<tr>
<td>IBM Security Identity Manager server</td>
<td>Version 6.0</td>
</tr>
</tbody>
</table>

**Software download**

After you purchase IBM Security Identity Manager, you can download the Desktop Password Reset Assistant from your account in IBM Passport Advantage Online.

Use this website:

Chapter 3. Desktop Password Reset Assistant installation

The Desktop Password Reset Assistant has both a IBM Security Identity Manager server component (servlet) and the desktop component.

A certificate is also required at each user desktop to protect the secrecy of the passwords and challenge responses that are transmitted during the reset process.

Desktop and automated deployment in the enterprise

The Desktop Password Reset Assistant must be installed on each desktop in the enterprise. It can be installed either by using the graphical user interface or by using automated deployment products.

Typically, the graphical user interface is used for demonstration purposes or for small enterprises with a limited number of desktops. For large enterprise systems, use an automated deployment product such as Security Provisioning Manager or Microsoft SMS.

Installing the Desktop Password Reset Assistant with the graphical user interface

You might install the Desktop Password Reset Assistant by using the graphical user interface.

Before you begin

Before you start, you must know the IP address and port number to communicate to the IBM Security Identity Manager server. You also must have a certificate authority (CA) installed on the desktop to protect the communication between the desktop and the IBM Security Identity Manager server.

About this task

The IBM Security Identity Manager Desktop Password Reset Assistant installation program is available for download from the IBM website. Contact your IBM account representative for the web address and download instructions.

To install the Desktop Password Reset Assistant, complete the following steps.

Procedure

1. Download the Desktop Password Reset Assistant compressed file from the IBM website.
2. Extract the contents of the compressed file into a temporary directory and change location to that directory.
   The content of the compressed file includes several files.
   • An install.htm file that describes how to download and run the adapter installer to unpack the encrypted adapter (.enc) file.
   • The compressed, encrypted .enc adapter file.
3. Open the install.htm file and use its instructions to run the adapter installer, which decrypts the files that you extracted and provides the License Agreement window.
4. In the License Agreement window, review the license agreement. To decrypt the installer package, the installation program requires that you accept the license agreement. If you do, select Accept and click Next.

5. Start the installation program by using the SetupDPRA.exe file in the temporary directory. For example, select Run from the Start menu, and type C:\TEMP\SetupDPRA.exe in the Open field.

6. In the Welcome window, click Next.

7. Enter the IBM Security Identity Manager server host name or IP address and IBM Security Identity Manager SSL port number, click Next.

8. Select a certificate file from your IBM Security Identity Manager server, if one exists, and click Next.

   **Note:** If you do not install the CA during the installation of the Desktop Password Reset Assistant, you can install it by using the manual instructions. See “Installing the CA Certificate for the SSL connection” on page 8.

9. In the Install Summary window, review the installation settings. Click Back to change any of these settings. Otherwise, click Next to begin the installation.

10. In the Install Completed window, click Finish to exit the program.

### What to do next

Regenerate the WebSphere® Application Server plug-in, plugin-cfg.xml, so the configuration changes can take effect. You can regenerate the plug-in by navigating to the WebSphere Application Server Console > Environment page > Update global Web server plug-in configuration > OK.

### Installing the Desktop Password Reset Assistant manually or by using an automated installation

The Desktop Password Reset Assistant can be installed manually or by using automated deployment products such as Security Provisioning Manager or Microsoft SMS.

### Before you begin

You must also install a CA certificate to ensure secure communications between the IBM Security Identity Manager server and the desktop.

**Note:** If you use a language other than English, you must install the option DLLs. Copy the DLLs to the Windows system32 folder. The DLL file names are formatted as IsimCR<language>.dll, where <language> is the country language code. For example, the country code for Korean is ko and the country code for Brazilian Portuguese is pt_BR.

### About this task

Include the following manual steps in your installation script for an automated installation.

### Procedure

1. Copy the files IsimCRCredentialProvider.dll and IsimCR.dll to the system32 folder. For support of languages other than English, you must install the optional language DLLs.
2. Open the Windows Registry key HKEY_LOCAL_MACHINE\SOFTWARE\Windows\CurrentVersion\Authentication\Credential Providers\ directory. Create a key called 61CF0CFE-8846-460a-B49D-66B3C81A5BC2, and set the value of the string Default to ItimCRCredentialProvider.

Additionally, open the Windows Registry key HKEY_LOCAL_MACHINE\SOFTWARE\Windows\CurrentVersion\Authentication\Credential Provider Filters\ directory. Create a key called A235EEA1-2109-4933-9A25-FDD6602EBE27, and set the value of the string Default to ItimCRCredentialProvider.

3. Open the Windows Registry key HKEY_CLASSES_ROOT\CLSID\ directory.
   a. Create a key called 61CF0CFE-8846-460a-B49D-66B3C81A5BC2, and set the value of the string Default to ItimCRCredentialProvider.

   Additionally, create a key called A235EEA1-2109-4933-9A25-FDD6602EBE27, and set the value of the string Default to ItimCRCredentialProvider.

   b. Create a key called InprocServer32 under the key 61CF0CFE-8846-460a-B49D-66B3C81A5BC2, and set the value of the string ThreadingModel to Apartment.

   Additionally, create a key called InprocServer32 under the key A235EEA1-2109-4933-9A25-FDD6602EBE27, and set the value of the string ThreadingModel to Apartment.

4. Alternatively, you can create a text file filename.reg with the following text. Run regedit.exe filename.reg to import the values into the registry.

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\{61CF0CFE-8846-460a-B49D-66B3C81A5BC2}\]
"@"="ItimCRCredentialProvider"

[HKEY_CLASSES_ROOT\CLSID\{61CF0CFE-8846-460a-B49D-66B3C81A5BC2}\]
"@"="ItimCRCredentialProvider"

[HKEY_CLASSES_ROOT\CLSID\{61CF0CFE-8846-460a-B49D-66B3C81A5BC2]\InprocServer32]
"@="ItimCRCredentialProvider.dll"
"ThreadingModel"="Apartment"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider Filters\{A235EEA1-2109-4933-9A25-FDD6602EBE27}\]
"@="ItimCRCredentialProvider"

[HKEY_CLASSES_ROOT\CLSID\{A235EEA1-2109-4933-9A25-FDD6602EBE27]\]
"@="ItimCRCredentialProvider"

[HKEY_CLASSES_ROOT\CLSID\{A235EEA1-2109-4933-9A25-FDD6602EBE27]\InprocServer32]
"@="ItimCRCredentialProvider.dll"
"ThreadingModel"="Apartment"
```

5. Create a key called HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISIM\ChallengeResponse, and set the following values:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IsimHost</td>
<td>String</td>
<td>Hostname or IP address of the IBM Security Identity Manager server</td>
</tr>
<tr>
<td>IsimPort</td>
<td>String</td>
<td>SSL port number</td>
</tr>
</tbody>
</table>

6. Restart the system for the changes to take effect.
What to do next

Regenerate the WebSphere Application Server plug-in, plugin-cfg.xml, so the configuration changes can take effect. You can regenerate the plug-in by navigating to the WebSphere Application Server Console > Environment page > Update global Web server plug-in configuration > OK.

Installing the CA Certificate for the SSL connection

Use the MMC Certificate plug-in to install the CA Certificate for the SSL connection.

Procedure

1. Go to Start > Run.
2. Type mmc and click OK.
3. Select File/Add/Remove Snap-in.
4. Click Add.
5. Select Certificates.
6. Click Add.
7. Select Computer.
8. Click Next.
9. Click Finish.
10. Click Close.
11. Click OK.
13. Right click Certificates.
14. Select All Tasks \ Import.
15. Browse for or enter the name of the CA certificate for the IBM Security Identity Manager server.
16. Click Next.
17. Click Next.
18. Click Finish.

Automated installations can use the Certificate Manager utility, CertMgr.exe.
The command line is:

```
certmgr -add -c certificate file -s -r localMachine root
```

Where certificate file is the complete path to the certificate file.
Chapter 4. First steps after installation

After you install the Desktop Password Reset Assistant, you can do more tasks.

Password reset and Windows account unlock with Desktop Password Reset Assistant

You can reset your password and unlock your Windows account from your workstation by using the Desktop Password Reset Assistant software.

The Desktop Password Reset Assistant is visible as a link on the password screen whenever:
- You restart the workstation.
- You log off from your account.

Note: By default, the Desktop Password Reset Assistant link is not displayed when you unlock your workstation.

To specify whether the credential provider is displayed when you unlock your workstation, modify the value of the ShowOnUnlock registry setting.

Identifying yourself to the assistant

Use the Desktop Password Reset Assistant and answer some personalized challenge questions in case you forgot your password.

Procedure
1. Select the IBM Password Reset Assistant.
2. Type in your IBM Security Identity Manager user ID and click Next.

Note: You might want to synchronize your IBM Security Identity Manager ID with your Windows Active Directory user name.

The IBM Security Identity Manager ID entered on the previous screen is used to retrieve your personalized challenge questions. The Desktop Password Reset Assistant leads you through the questions one at a time, collecting your responses and providing a visual indicator for your progress.
3. Type in the answer to each of the challenge questions and click Next.
4. Type in the answer to the last challenge question and click Submit. If any of the responses are incorrect, an error message is displayed. Use the <<Back and Next>> buttons to navigate through the questions to verify your responses.

Account selection

After you identify yourself to the assistant by entering the correct answers to the challenge response questions, you can select accounts to unlock or reset. The account selection step can vary.

The step depends on whether you have Windows accounts, that is, Windows Local or Windows Active Directory accounts that are managed by IBM Security Identity Manager. The step also depends on the IBM Security Identity Manager security settings to enable or disable password synchronization.
Enabled
Displays a list of all accounts that are owned by the ISIM user account. The option to select accounts is disabled because all accounts will be synchronized to the new password.

Disabled
Displays a list of Windows accounts that are owned by the ISIM user. You can select which accounts to reset. After your selection, you can reset the passwords or unlock the accounts, maintaining the existing password.

If password synchronization is disabled, you can select which Windows accounts to reset or unlock. If it is enabled, all accounts are selected. You cannot selectively reset or unlock them. After making the selection, click Next to go to the password step.

Unlocking or resetting a password
You can unlock or reset a password.

About this task
Your choices depend on whether password synchronization is enabled or disabled. If enabled, you see only your Windows accounts and the Unlock only button is enabled. If password synchronization is disabled, the Unlock only button is disabled. Your only choice is to enter a new password.

Procedure
• Reset your password.
  1. Enter the new password.
     Optionally, you can select Unlock only (Windows Accounts) to unlock your Windows accounts without resetting the password. If password synchronization is enabled, this option is disabled.
  2. Click Submit to initiate the password reset process.
• To unlock your Windows accounts and keep your existing password, follow these steps:
  1. Click Unlock only (Windows Accounts).
  2. Click Submit. Your accounts are unlocked and you can log in using your existing password.

Note: Clicking Submit sends the new password, or the unlock request, to the IBM Security Identity Manager server for processing. The actual password change or unlock is performed by the IBM Security Identity Manager server through the adapters. There might be a delay before the password change or unlock request is completed.

Customization of the Desktop Password Reset Assistant
You can customize the Desktop Password Reset Assistant screen, including logos, labels, and other elements.
• “IBM logo customization” on page 11
• “Product title logo customization” on page 11
• “Background bitmap customization” on page 11
• “User interface labels customization” on page 11
IBM logo customization
You can replace the IBM logo in the upper right corner of the screen with the logo of your company by using the Desktop Password Reset Assistant.

When a logo of an organization is supplied, the adapter replaces the IBM logo with the logo of the organization. The Desktop Password Reset Assistant searches for the updated logo in the `c:\windows\system32` directory.

Note: You cannot resize the customized logo.

Product title logo customization
You can replace the IBM Security Identity Manager product title logo with the product title logo of your company by using the Desktop Password Reset Assistant.

The product title logo is displayed as the full title bar of the dialog. When a product title logo of an organization is supplied, the adapter replaces the IBM product title logo with the logo of the organization. The Desktop Password Reset Assistant searches for the updated logo at the following location.

Table 5. Product title details

<table>
<thead>
<tr>
<th>File name</th>
<th>DPRA_title.bmp</th>
</tr>
</thead>
<tbody>
<tr>
<td>File location</td>
<td><code>c:\windows\system32</code></td>
</tr>
<tr>
<td>Attributes</td>
<td>Width = 459, Height = 39</td>
</tr>
</tbody>
</table>

Note: You cannot resize the customized product title logo. Therefore, it must be approximately of the same dimensions as specified in Table 5.

Background bitmap customization
You can replace the background bitmap by using the Desktop Password Reset Assistant.

When a new background bitmap is supplied, the adapter replaces the existing background of the Desktop Password Reset Assistant dialog. The Desktop Password Reset Assistant searches for the updated bitmap at the following location.

Table 6. Background bitmap details

<table>
<thead>
<tr>
<th>File name</th>
<th>DPRA_Back.bmp</th>
</tr>
</thead>
<tbody>
<tr>
<td>File location</td>
<td><code>c:\windows\system32</code></td>
</tr>
<tr>
<td>Attributes</td>
<td>You can resize the background bitmap depending on the dimensions of the dialog window, which is approximately 450 x 275.</td>
</tr>
</tbody>
</table>

User interface labels customization
You can replace the user interface labels by using the Desktop Password Reset Assistant.
When you replace the labels, you must add the labels that you want to override. The Desktop Password Reset Assistant searches for the updated labels at the following location.

Table 7. User interface labels details

<table>
<thead>
<tr>
<th>File name</th>
<th>DPRA_Str.txt</th>
</tr>
</thead>
<tbody>
<tr>
<td>File location</td>
<td>c:\windows\system32</td>
</tr>
<tr>
<td>Format</td>
<td>&lt;id number&gt;,&lt;newstring&gt;</td>
</tr>
</tbody>
</table>

The complete list of ID numbers and default strings is described in the DPRAstringIDs.txt file and is supplied for your reference. A sample DPRA_Str.txt is also supplied as a reference.

Note: The DPRA_Str.txt file must be a Unicode file.

Response user interface behavior customization

You can configure the behavior of the Response attribute by using the Desktop Password Reset Assistant.

By default, the Responses are mapped to the Password field. However, you can control this behavior through the registry key string ShowResponses. This string enables the Responses to be displayed in clear text when the Responses are set to TRUE.

Table 8. ShowResponses string details

<table>
<thead>
<tr>
<th>Key</th>
<th>HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISIM\ChallengeResponse</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>ShowResponses</td>
</tr>
<tr>
<td>Value</td>
<td>TRUE</td>
</tr>
</tbody>
</table>

Use of the Desktop Password Reset Assistant with Screen Saver Unlock

By default, the Desktop Password Reset Assistant screen is displayed only when you log on to the workstation.

You can configure this behavior through the registry key string ShowOnUnlock. When you want the Desktop Password Reset Assistant to resume locked sessions, set this registry key to TRUE.

Table 9. ShowOnUnlock string details

<table>
<thead>
<tr>
<th>Key</th>
<th>HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISIM\ChallengeResponse</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>ShowOnUnlock</td>
</tr>
<tr>
<td>Value</td>
<td>TRUE</td>
</tr>
</tbody>
</table>
Chapter 5. Problem troubleshooting for the Desktop Password Reset Assistant

Troubleshooting is the process of determining why a product does not function as it is designed to function.

Use this information to identify and resolve problems that are related to the Desktop Password Reset Assistant, including errors that might occur during installation.

Techniques for troubleshooting problems

Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem. Certain common techniques can help with the task of troubleshooting.

The first step in the troubleshooting process is to describe the problem completely. Problem descriptions help you and the IBM technical-support representative know where to start to find the cause of the problem. This step includes asking yourself basic questions:

- What are the symptoms of the problem?
- Where does the problem occur?
- When does the problem occur?
- Under which conditions does the problem occur?
- Can the problem be reproduced?

The answers to these questions typically lead to a good description of the problem, which can then lead you to a problem resolution.

What are the symptoms of the problem?

When starting to describe a problem, the most obvious question is “What is the problem?” This question might seem straightforward; however, you can break it down into several more-focused questions that create a more descriptive picture of the problem. These questions can include:

- Who, or what, is reporting the problem?
- What are the error codes and messages?
- How does the system fail? For example, is it a loop, hang, crash, performance degradation, or incorrect result?

Where does the problem occur?

Determining where the problem originates is not always easy, but it is one of the most important steps in resolving a problem. Many layers of technology can exist between the reporting and failing components. Networks, disks, and drivers are only a few of the components to consider when you are investigating problems.

The following questions help you to focus on where the problem occurs to isolate the problem layer:
- Is the problem specific to one platform or operating system, or is it common across multiple platforms or operating systems?
- Is the current environment and configuration supported?
- Do all users have the problem?
- (For multi-site installations.) Do all sites have the problem?

If one layer reports the problem, the problem does not necessarily originate in that layer. Part of identifying where a problem originates is understanding the environment in which it exists. Take some time to completely describe the problem environment, including the operating system and version, all corresponding software and versions, and hardware information. Confirm that you are running within an environment that is a supported configuration; many problems can be traced back to incompatible levels of software that are not intended to run together or have not been fully tested together.

**When does the problem occur?**

Develop a detailed timeline of events leading up to a failure, especially for those cases that are one-time occurrences. You can most easily develop a timeline by working backward: Start at the time an error was reported (as precisely as possible, even down to the millisecond), and work backward through the available logs and information. Typically, you need to look only as far as the first suspicious event that you find in a diagnostic log.

To develop a detailed timeline of events, answer these questions:
- Does the problem happen only at a certain time of day or night?
- How often does the problem happen?
- What sequence of events leads up to the time that the problem is reported?
- Does the problem happen after an environment change, such as upgrading or installing software or hardware?

Responding to these types of questions can give you a frame of reference in which to investigate the problem.

**Under which conditions does the problem occur?**

Knowing which systems and applications are running at the time that a problem occurs is an important part of troubleshooting. These questions about your environment can help you to identify the root cause of the problem:
- Does the problem always occur when the same task is being performed?
- Does a certain sequence of events need to happen for the problem to occur?
- Do any other applications fail at the same time?

Answering these types of questions can help you explain the environment in which the problem occurs and correlate any dependencies. Remember that just because multiple problems might have occurred around the same time, the problems are not necessarily related.

**Can the problem be reproduced?**

From a troubleshooting standpoint, the ideal problem is one that can be reproduced. Typically, when a problem can be reproduced you have a larger set of
tools or procedures at your disposal to help you investigate. Consequently, problems that you can reproduce are often easier to debug and solve.

However, problems that you can reproduce can have a disadvantage: If the problem is of significant business impact, you do not want it to recur. If possible, re-create the problem in a test or development environment, which typically offers you more flexibility and control during your investigation.

- Can the problem be re-created on a test system?
- Are multiple users or applications encountering the same type of problem?
- Can the problem be re-created by running a single command, a set of commands, or a particular application?

For information about obtaining support, see Appendix A, “Support information,” on page 21.

---

## Warnings and error messages

A warning or error might be displayed in the user interface to provide information that the user needs to know about the adapter or when an error occurs.

Table 10 contains warnings or errors which might be displayed in the user interface if the Desktop Password Reset Assistant is installed on your system.

### Table 10. Warning and error messages

<table>
<thead>
<tr>
<th>Warning or error message</th>
<th>Try the following actions:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Winhttp cannot connect</td>
<td>Verify that the IBM Security Identity Manager server is running. If it is not, restart the server. See the IBM Security Identity Manager product documentation if you need information about how to perform these tasks.</td>
</tr>
<tr>
<td>Internal error on ISIM server - jndiCommunicationException.</td>
<td>Verify that the IBM Security Identity Manager server is running. If it is not, restart the server. See the IBM Security Identity Manager product documentation if you need information about how to perform these tasks.</td>
</tr>
</tbody>
</table>
| ISIM user not found      | Ensure that the specified IBM Security Identity Manager user ID on the Desktop Password Reset Assistant screen is typed correctly and that the same user exists on the IBM Security Identity Manager server. To verify that the user account exists, complete these steps:  
1. From the navigation tree, select Manage Users.  
2. On the Select a User page, type information about the user in the Search information field, select an attribute from the Search by list, and then click Search.  
3. In the Users table, locate the user account. If the user account does not exist, you can either create the user account or specify a valid user account in the Desktop Password Reset Assistant screen. |
| Invalid response         | Ensure that the answer to each of the challenge questions is correct. Use the <<Back and Next>> buttons to navigate through the questions to verify the responses. |
Table 10. Warning and error messages (continued)

<table>
<thead>
<tr>
<th>Warning or error message</th>
<th>Try the following actions:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal error on ISIM server - CHALLENGE_RESPONSE_CONFIG_CHANGE</td>
<td>Ensure that the challenge response is configured for the user on IBM Security Identity Manager. From the IBM Security Identity Manager navigation tree, select <strong>Set System Security &gt; Configure Forgotten Password Settings</strong> and select the Enable forgotten password authentication check box. See the IBM Security Identity Manager product documentation if you need information about how to perform these tasks.</td>
</tr>
<tr>
<td>Internal error on ISIM server - ACCOUNT_NOT_ACTIVE</td>
<td>Ensure that the IBM Security Identity Manager user is active (not suspended). To view or change account details for a user, complete these steps:</td>
</tr>
<tr>
<td></td>
<td>1. From the navigation tree, select <strong>Manage Users</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. On the Select a User page, complete these steps:</td>
</tr>
<tr>
<td></td>
<td>a. Type information about the user in the Search information field, select an attribute from the Search by list, and then click <strong>Search</strong>.</td>
</tr>
<tr>
<td></td>
<td>b. In the Users table, locate the user account and verify if its status is active</td>
</tr>
<tr>
<td></td>
<td>c. If the status is inactive, in the Users table, click the icon adjacent to the name of the user account, and click <strong>Restore</strong>.</td>
</tr>
<tr>
<td></td>
<td>d. On the Restore Users &gt; Schedule page, click <strong>Submit</strong>.</td>
</tr>
<tr>
<td></td>
<td>e. On the Restore Users &gt; Success page click <strong>Close</strong>.</td>
</tr>
<tr>
<td></td>
<td>f. On the Select a User page in the User table, click <strong>Refresh</strong> and verify that the account is now active.</td>
</tr>
<tr>
<td></td>
<td>See the IBM Security Identity Manager product documentation if you need information on how to perform these tasks.</td>
</tr>
<tr>
<td>Internal error on ISIM server - OPERATION_NOT_ALLOWED</td>
<td>Ensure that the user has the privilege to unlock their accounts without changing the password.</td>
</tr>
<tr>
<td></td>
<td>Create or modify an ACL that has permission for <strong>Account Locked Out</strong>. To verify the permissions, go to <strong>Set System Security &gt; Change Access Control items &gt; Permissions</strong>.</td>
</tr>
<tr>
<td>Invalid Certificate authority</td>
<td>Ensure that the CA certificate is correctly installed.</td>
</tr>
<tr>
<td></td>
<td>Perform the following steps using the MMC Certificate plugin: See “Installing the CA Certificate for the SSL connection” on page 8.</td>
</tr>
</tbody>
</table>
Chapter 6. Adapter updates

You can install the updated version of the Desktop Password Reset Assistant on an existing version.

For information about installation, see Chapter 3, “Desktop Password Reset Assistant installation,” on page 5.

**Note:** Restart the workstation after you install the Desktop Password Reset Assistant.
Chapter 7. Uninstalling the adapter

You can uninstall the Desktop Password Reset Assistant from the Control Panel.

Procedure
1. Go to the Control Panel and double-click Add or Remove Programs.
2. On the Add or Remove Programs page, select Desktop Password Reset Assistant from the list, and click Remove.
Appendix A. Support information

You have several options to obtain support for IBM products.

- “Searching knowledge bases”
- “Obtaining a product fix” on page 22
- “Contacting IBM Support” on page 22

Searching knowledge bases

You can often find solutions to problems by searching IBM knowledge bases. You can optimize your results by using available resources, support tools, and search methods.

About this task

You can find useful information by searching the product documentation for IBM Security Identity Manager. However, sometimes you must look beyond the product documentation to answer your questions or resolve problems.

Procedure

To search knowledge bases for information that you need, use one or more of the following approaches:

1. Search for content by using the IBM Support Assistant (ISA).
   ISA is a no-charge software serviceability workbench that helps you answer questions and resolve problems with IBM software products. You can find instructions for downloading and installing ISA on the ISA website.

2. Find the content that you need by using the IBM Support Portal.
   The IBM Support Portal is a unified, centralized view of all technical support tools and information for all IBM systems, software, and services. The IBM Support Portal lets you access the IBM electronic support portfolio from one place. You can tailor the pages to focus on the information and resources that you need for problem prevention and faster problem resolution. Familiarize yourself with the IBM Support Portal by viewing the demo videos (https://www.ibm.com/blogs/SPNA/entry/the_ibm_support_portal_videos) about this tool. These videos introduce you to the IBM Support Portal, explore troubleshooting and other resources, and demonstrate how you can tailor the page by moving, adding, and deleting portlets.

3. Search for content about IBM Security Identity Manager by using one of the following additional technical resources:
   - IBM Security Identity Manager version 6.0 technotes and APARs (problem reports)
   - IBM Security Identity Manager Support website
   - IBM Redbooks®
   - IBM support communities (forums and newsgroups)

4. Search for content by using the IBM masthead search. You can use the IBM masthead search by typing your search string into the Search field at the top of any ibm.com® page.

5. Search for content by using any external search engine, such as Google, Yahoo, or Bing. If you use an external search engine, your results are more likely to
include information that is outside the ibm.com domain. However, sometimes you can find useful problem-solving information about IBM products in newsgroups, forums, and blogs that are not on ibm.com.

**Tip:** Include “IBM” and the name of the product in your search if you are looking for information about an IBM product.

### Obtaining a product fix

A product fix might be available to resolve your problem.

**About this task**

You can get fixes by following these steps:

**Procedure**

1. Obtain the tools that are required to get the fix. You can obtain product fixes from the Fix Central Site. See [http://www.ibm.com/support/fixcentral/](http://www.ibm.com/support/fixcentral/)
2. Determine which fix you need.
3. Download the fix. Open the download document and follow the link in the “Download package” section.
4. Apply the fix. Follow the instructions in the “Installation Instructions” section of the download document.

### Contacting IBM Support

IBM Support assists you with product defects, answers FAQs, and helps users resolve problems with the product.

**Before you begin**

After trying to find your answer or solution by using other self-help options such as technotes, you can contact IBM Support. Before contacting IBM Support, your company or organization must have an active IBM software subscription and support contract, and you must be authorized to submit problems to IBM. For information about the types of available support, see the Support portfolio topic in the “Software Support Handbook”.

**Procedure**

To contact IBM Support about a problem:

1. Define the problem, gather background information, and determine the severity of the problem. For more information, see the Getting IBM support topic in the Software Support Handbook.
2. Gather diagnostic information.
3. Submit the problem to IBM Support in one of the following ways:
   - Using IBM Support Assistant (ISA):
     Any data that has been collected can be attached to the service request. Using ISA in this way can expedite the analysis and reduce the time to resolution.
     b. Open ISA.
c. Click Collection and Send Data.
d. Click the Service Requests tab.
e. Click Open a New Service Request.

- Online through the [IBM Support Portal](#) You can open, update, and view all of your service requests from the Service Request portlet on the Service Request page.
- By telephone for critical, system down, or severity 1 issues: For the telephone number to call in your region, see the [Directory of worldwide contacts](#) web page.

**Results**

If the problem that you submit is for a software defect or for missing or inaccurate documentation, IBM Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Support provides a workaround that you can implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the IBM Support website daily, so that other users who experience the same problem can benefit from the same resolution.
Appendix B. Accessibility features for IBM Security Identity Manager

Accessibility features help users who have a disability, such as restricted mobility or limited vision, to use information technology products successfully.

**Accessibility features**

The following list includes the major accessibility features in IBM Security Identity Manager.

- Support for the Freedom Scientific JAWS screen reader application
- Keyboard-only operation
- Interfaces that are commonly used by screen readers
- Keys that are discernible by touch but do not activate just by touching them
- Industry-standard devices for ports and connectors
- The attachment of alternative input and output devices

The IBM Security Identity Manager library, and its related publications, are accessible.

**Keyboard navigation**

This product uses standard Microsoft Windows navigation keys.

**Related accessibility information**

The following keyboard navigation and accessibility features are available in the form designer:

- You can use the tab keys and arrow keys to move between the user interface controls.
- You can use the Home, End, Page Up, and Page Down keys for more navigation.
- You can launch any applet, such as the form designer applet, in a separate window to enable the Alt+Tab keystroke to toggle between that applet and the web interface, and also to use more screen workspace. To launch the window, click **Launch as a separate window**.
- You can change the appearance of applets such as the form designer by using themes, which provide high contrast color schemes that help users with vision impairments to differentiate between controls.

**IBM and accessibility**

See the [IBM Human Ability and Accessibility Center](https://www.ibm.com/able) for more information about the commitment that IBM has to accessibility.
Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.
IBM may use or distribute any of the information you supply in any way it
believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose
of enabling: (i) the exchange of information between independently created
programs and other programs (including this one) and (ii) the mutual use of the
information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions,
including in some cases payment of a fee.

The licensed program described in this document and all licensed material
available for it are provided by IBM under terms of the IBM Customer Agreement,
IBM International Program License Agreement or any equivalent agreement
between us.

Any performance data contained herein was determined in a controlled
environment. Therefore, the results obtained in other operating environments may
vary significantly. Some measurements may have been made on development-level
systems and there is no guarantee that these measurements will be the same on
generally available systems. Furthermore, some measurement may have been
estimated through extrapolation. Actual results may vary. Users of this document
should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of
those products, their published announcements or other publicly available sources.
IBM has not tested those products and cannot confirm the accuracy of
performance, compatibility or any other claims related to non-IBM products.
Questions on the capabilities of non-IBM products should be addressed to the
suppliers of those products.

All statements regarding IBM’s future direction or intent are subject to change or
withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business
operations. To illustrate them as completely as possible, the examples include the
names of individuals, companies, brands, and products. All of these names are
fictitious and any similarity to the names and addresses used by an actual business
enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which
illustrate programming techniques on various operating platforms. You may copy,
modify, and distribute these sample programs in any form without payment to
IBM, for the purposes of developing, using, marketing or distributing application
programs conforming to the application programming interface for the operating
platform for which the sample programs are written. These examples have not
been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or
imply reliability, serviceability, or function of these programs. You may copy,
modify, and distribute these sample programs in any form without payment to
IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

If you are viewing this information softcopy, the photographs and color illustrations might not appear.

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

**Trademarks**

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at [http://www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Cell Broadband Engine and Cell/B.E. are trademarks of Sony Computer Entertainment, Inc., in the United States, other countries, or both and is used under license therefrom.
Privacy Policy Considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, and to tailor interactions with the end user or for other purposes. In many cases, no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

Index

A
accessibility x, 25
account, inactive 15
architectural overview 1
attributes
customization 11, 12

B
background bitmap customization 11

C
CA Certificate
installation 8
SSL connection 8
configuration
adapter-server communication 2
adapter-server connectivity ix
basic 2
supported 1
connectivity error 15
customization
background bitmap 10, 11
bitmap resizing 11
label file format 12
options 10
product logo 10
response user interface behavior 12
screen saver unlock 10
user interface labels 10
Windows credential tile 10

D
Desktop Password Reset Assistant
background bitmap 10
customization 10
installation 5
overview 1
product logo 10
screen saver unlock 10
user interface labels 10
Windows credential tile 10

E
education x
enterprise, user interface label file format 12
error
inactive account 15
ISIM server 15
messages 15
operation not allowed 15

F
features 1
first steps, post installation 9

G
GINA 1
graphical identification and authentication 1
graphical user interface
installation 5

I
IBM
logo customization 11
Software Support 4
Support Assistant 4
IBM Security Access Manager for Enterprise Single Sign-On
product integration 2
IBM Security Identity Manager
configuration enhancement 2
product integration 2
IBM Support Assistant 22
inactive account error 15
installation
adapter 5
automated 6
basic installation and configuration information ix
desktop password reset assistant 5
enterprise 6
graphical user interface 5
manual 6
plan 3
prerequisites 3
problems 13
required certificate 5
restart 17
roadmap 3
security 5
software download 4
invalid certificate authority error 15
ISA 22
ISIM server internal error 15

K
knowledge bases 21

L
logo
customization 11
IBM 11

N
notices 27

O
online
publications ix
terminology ix
operation not allowed error 15

P
Passport Advantage Online 4
password
forgotten 9
personalized challenge questions 9
reset 9, 10
unlock 10
unlock account 9
post-installation first steps 9
preinstallation roadmap 3
prerequisites
operating system 3
per version 3
problem-determination x
product integration
configure 2
features 1
publications
accessing online ix
list of ix

R
registry key string
ShowOnUnlock 12
ShowResponses 12
registry settings 6
remove programs 19
reset password 10
response user interface customization 12
roadmap
installation 3
preinstallation 3

S
screen saver
customization 12
unlock 12
ShowOnUnlock 12
ShowResponses 12
software problems, troubleshooting 13
support contact information 22
supported configurations 1