

IBM Security Verify Governance  
10.0

*Desktop Password Reset Assistant  
Installation and Configuration Guide*





# Contents

<b>Tables.....</b>	<b>V</b>
<b>Chapter 1. Overview.....</b>	<b>1</b>
Desktop Password Reset Assistant features.....	1
Desktop Password Reset Assistant configuration.....	1
Basic configuration.....	1
Enhanced configuration.....	2
<b>Chapter 2. Planning.....</b>	<b>3</b>
Prerequisites.....	3
Software downloads.....	3
<b>Chapter 3. Installing.....</b>	<b>5</b>
Desktop and automated deployment in the enterprise.....	5
Installing Desktop Password Reset Assistant with the graphical user interface.....	5
Installing Desktop Password Reset Assistant manually or by using an automated installation.....	6
Installing the CA Certificate for the SSL connection.....	7
<b>Chapter 4. Upgrading.....</b>	<b>9</b>
<b>Chapter 5. Configuring.....</b>	<b>11</b>
Identifying yourself to the assistant.....	11
Account selection.....	11
Customization of the Desktop Password Reset Assistant.....	11
IBM logo customization.....	11
Product title logo customization.....	12
Background bitmap customization.....	12
User interface labels customization.....	12
Response user interface behavior customization.....	13
<b>Chapter 6. Troubleshooting.....</b>	<b>15</b>
Techniques for troubleshooting problems.....	15
<b>Chapter 7. Uninstalling.....</b>	<b>17</b>
<b>Index.....</b>	<b>19</b>



---

# Tables

1. Prerequisites to install the Desktop Password Reset Assistant.....	3
2. ChallengeResponse registry values.....	7
3. Product title details.....	12
4. Background bitmap details.....	12
5. User interface labels details.....	12
6. ShowResponses string details.....	13



---

## Chapter 1. Overview

An adapter is an interface between a managed resource and the Identity server. The Desktop Password Reset Assistant software enables Windows users to perform self-service password resets 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.

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 password reset (change) of all accounts
- Authentication using the secure challenge and response features of IBM Security Verify Governance
- Integration with Security Access Manager for Enterprise Single Sign-On through the Security Access Manager for Enterprise Single Sign-On Adapter
- 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

Desktop Password Reset Assistant can be installed in two configurations.

The first configuration is the basic configuration in which the IBM Security Verify Governance 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 Verify Governance 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

The basic configuration includes a single Identity 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 Identity server to retrieve the user challenge questions and to validate the responses. After a successful authentication, the IBM Security Verify Governance generates password change, password reset 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. Planning

Installing and configuring the adapter involves several steps that you must complete in a specific sequence. Follow the roadmap for the main tasks.

### Prerequisites

Verify that your environment meets the software and hardware requirements for the adapter.

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.

Prerequisites	Description
Operating System	<ul style="list-style-type: none"> <li>Windows 7</li> <li>Windows 8</li> <li>Windows 2008 server</li> <li>Windows 2012 server</li> </ul>
Security Access Manager for Enterprise Single Sign-On products	Version 5.1 or later
Security Access Manager for Enterprise Single Sign-On Adapter	Version 5.1
Windows Active Directory Adapter	Version 6.0, 7.0
Windows Local Account Adapter	Version 6.0, 7.0
Identity server	<p>The following servers are supported:</p> <ul style="list-style-type: none"> <li>Identity server Version 10.0</li> <li>Identity server Version 10.0</li> <li>Identity server Version 10.0</li> </ul>

### Software downloads

Log in to your account on the IBM Passport Advantage website and download the software.

Go to [IBM Passport Advantage](#). See the *IBM Security Verify Governance Download Document*.

**Note:** You can also obtain adapter information from IBM Support.



---

## Chapter 3. Installing

Installing the adapter mainly involves importing the adapter profile and creating an adapter service. Depending on the adapter, several other tasks can be involved to completely install it.

The Desktop Password Reset Assistant has both Identity 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 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 Identity server. You also must have a certificate authority (CA) installed on the desktop to protect the communication between the desktop and the Identity server.

#### About this task

The 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 Verify Governance server host name or IP address and IBM Security Verify Governance SSL port number, click **Next**.
8. Select a certificate file from your Identity 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 7](#).
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 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 Identity 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 `<language>.dll`, where `<language>` is the country language code. For example, the country code for Korean is `ko` and the county code for Brazilian Portuguese is `pt_BR`.
- To limit the list of language options, remove the corresponding `<language>.dll` file from the Windows system32 folder.

### About this task

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

### Procedure

1. Copy the files and `ItimCR.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\ITIM\ChallengeResponse, and set the following values:

Table 2. ChallengeResponse registry values		
Name	Type	Value
	String	Hostname or IP address of the Identity server
	String	SSL port number

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**.
12. Open **Certificates > Trusted root Certification Authorities**.
13. Right click **Certificates**.
14. Select **All Tasks\Import**.
15. Browse for or enter the name of the CA certificate for the Identity 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. Upgrading

Upgrading the adapter requires a full installation.

For information about installation, see [Chapter 3, “Installing,”](#) on page 5.

**Note:** Restart the workstation after you install the Desktop Password Reset Assistant.





---

## Chapter 5. Configuring

After you install the adapter, configure it to function correctly. Configuration is based on your requirements or preference.

### 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 Verify Governance user ID and click **Next**.

**Note:** You might want to synchronize your IBM Security Verify Governance ID with your Windows Active Directory user name.

The IBM Security Verify Governance 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 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 Verify Governance.

Verify Governance Windows accounts are listed and you can select any number of accounts to have the password reset.

### 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

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 Verify Governance 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.

<i>Table 3. Product title details</i>	
File name	DPRA_title.bmp
File location	c:\windows\system32
Attributes	<ul style="list-style-type: none"> <li>• Width = 552</li> <li>• Height = 48</li> </ul> <p><b>Note:</b> For Windows 8 and 10:</p> <ul style="list-style-type: none"> <li>• Width = 449</li> <li>• Height = 39</li> </ul>

**Note:** You cannot resize the customized product title logo. Therefore, it must be approximately of the same dimensions as specified in [Table 3 on page 12](#).

## 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.

<i>Table 4. Background bitmap details</i>	
File name	DPRA_Back.bmp
File location	c:\windows\system32
Attributes	You can resize the background bitmap depending on the dimensions of the dialog window, which is approximately 450 x 275.

## 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.

<i>Table 5. User interface labels details</i>	
File name	DPRA_Str.txt
File location	c:\windows\system32
Format	<id number>,<newstring>

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.

<i>Table 6. ShowResponses string details</i>	
Key	HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ITIM\ChallengeResponse
String	<b>ShowResponses</b>
Value	TRUE



---

## Chapter 6. Troubleshooting

*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. This topic provides information and techniques for identifying and resolving problems that are related to the adapter, including troubleshooting errors that might occur during the adapter installation.

---

### Techniques for troubleshooting problems

---

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 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 you start 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 operating system, or is it common across multiple 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 are not fully tested together.

## **When does the problem occur?**

Develop a detailed timeline of events that lead 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 use 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 done?
- Is a certain sequence of events required 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 occur 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. 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?
- Do multiple users or applications have the same type of problem?
- Can the problem be re-created by running a single command, a set of commands, or a particular application?

---

## Chapter 7. Uninstalling

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**.

**Note:** If a JRE is present on the workstation where DPRA is installed, the standard DPRA uninstall fails. Complete either of the following two options:

- Run the uninstaller from the command line and specify the `jvm` as a command line argument. For example,

```
C>"Uninstall Desktop Password Reset Assistant.exe"  
LAX_VM "c:\Program Files (x86)\Java\jre1.8.0_31\bin\java.exe"
```

- Manually update the `installvariables.properties` after the installation to point to a valid `jvm`.





# Index

## A

architectural overview [1](#)  
 attributes  
   customization [12](#), [12](#), [13](#)

## B

background bitmap customization [12](#)

## C

CA Certificate  
   installation [7](#)  
   SSL connection [7](#)  
 configuration  
   supported [1](#), [1](#)  
 customization  
   background bitmap [11](#), [12](#)  
   bitmap resizing [12](#)  
   label file format [12](#)  
   options [11](#)  
   product logo [11](#)  
   response user interface behavior [13](#)  
   screen saver unlock [11](#)  
   user interface labels [11](#)  
   Windows credential tile [11](#)

## D

Desktop Password Reset Assistant  
   background bitmap [11](#)  
   customization [11](#)  
   installation [5](#)  
   overview [1](#)  
   product logo [11](#)  
   screen saver unlock [11](#)  
   user interface labels [11](#)  
   Windows credential tile [11](#)  
 download, software [3](#)

## E

enterprise, user interface label file format [12](#)

## F

features [1](#)  
 first steps, post installation [11](#)

## G

GINA [1](#)  
 graphical identification and authentication [1](#)  
 graphical user interface  
   installation [5](#)

## I

IBM  
   logo customization [11](#)  
 installation  
   adapter [5](#)  
   automated [6](#)  
   desktop password reset assistant [5](#)  
   enterprise [6](#)  
   graphical user interface [5](#)  
   manual [6](#)  
   planning roadmaps [3](#)  
   prerequisites [3](#)  
   problems [15](#)  
   required certificate [5](#)  
   restart [9](#)  
   security [5](#)

## L

logo  
   customization [12](#)  
   IBM [11](#)

## P

password  
   forgotten [11](#)  
   personalized challenge questions [11](#)  
   reset [11](#)  
 post-installation first steps [11](#)  
 prerequisites  
   operating system [3](#)  
   per version [3](#)  
 product integration  
   features [1](#)

## R

registry key string  
   ShowResponses [13](#)  
 registry settings [6](#)  
 remove programs [17](#)  
 response user interface customization [13](#)  
 roadmaps  
   planning [3](#)

## S

ShowResponses [13](#)  
 software  
   download [3](#)  
   website [3](#)  
 supported configurations [1](#)

## T

troubleshooting  
   identifying problems [15](#)  
   installation problem [15](#)  
   techniques for [15](#)  
 troubleshooting and support  
   troubleshooting techniques [15](#)

## **U**

uninstallation [17](#)

user interface label customization [12](#)

## **V**

version update [9](#)



