IBM PowerSC Multi-Factor Authentication

Version 1.1.0

User's Guide

IBM PowerSC Multi-Factor Authentication

Version 1.1.0

User's Guide

Note
Before using this information and the product it supports, read the information in "Notices" on page 15.

This edition applies to IBM PowerSC Multi-Factor Authentication Version 1.1.0 and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright IBM Corporation 2017, 2018.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

© Copyright IBM Corp. 2017, 2018

About this document

This document provides information about how you can use IBM® PowerSC™ Multi-Factor Authentication.

Highlighting

The following highlighting conventions are used in this document:

Bold	Identifies commands, subroutines, keywords, files, structures, directories, and other items whose names are predefined by the system. Bold highlighting also identifies graphical objects, such as buttons, labels, and icons that the you select.
Italics	Identifies parameters for actual names or values that you supply.
`Monospace`	Identifies examples of specific data values, examples of text similar to what you might see displayed, examples of portions of program code similar to what you might write as a programmer, messages from the system, or text that you must type.

Case-sensitivity in IBM PowerSC Multi-Factor Authentication

Everything in the IBM PowerSC Multi-Factor Authentication software is case-sensitive, which means that it distinguishes between uppercase and lowercase letters. For example, you can use the **ls** command to list files. If you type `LS`, the system responds that the command `is not found`. Likewise, **FILEA**, **FiLea**, and **filea** are three distinct file names, even if they reside in the same directory. To avoid causing undesirable actions to be performed, always ensure that you use the correct case.

ISO 9000

ISO 9000 registered quality systems were used in the development and manufacturing of this product.

© Copyright IBM Corp. 2017, 2018

Introduction to IBM PowerSC Multi-Factor Authentication

IBM PowerSC Multi-Factor Authentication, which is referred to in this document as IBM PowerSC MFA, provides alternative authentication mechanisms for systems that are used with RSA SecurID-based authentication systems, and certificate authentication options such as Common Access Card (CAC) and Personal Identification Verification (PIV) cards. IBM PowerSC MFA allows the use of alternative authentication mechanisms instead of the standard password.

You can use IBM PowerSC MFA with a large variety of applications, such as Remote Shell (RSH), Telnet, and Secure Shell (SSH).

In-band and out-of-band login process

Your administrator might configure your account for the in-band or out-of-band authentication types. The login process is significantly different for these authentication types.

If you are using the in-band authentication type, you can generate a token or certificate by using IBM PowerSC MFA with SecurID or PIV/CAC cards and use that token or certificate directly to log in to the application. This is similar to logging into the application by using your password. Authentication is performed by using pluggable authentication modules (PAM).

If you are using the out-of-band authentication type, you can authenticate with one or more authentication methods that are configured by your security administrator to retrieve a cache token credential (CTC) that you can use to log in to the application. A user-specific out-of-band web page prompts you for all of the authentication methods you must specify.

Consider the following SSH example:

```
$ ssh user@system.your-domain.com

Available Policies:

1. SecurID 1

Select Policy or enter CTC: 1 2

Enter your SecurID passcode.

Policy Satisfied. CTC: IVn&/KO2^iB4QNHW 3
```

- **1** The available IBM PowerSC MFA policies are displayed.
- **2** You are presented with a choice of selecting a policy or entering a CTC.
  - If you select a policy, it indicates the in-band authentication type. You enter the token directly in the application.
  - If you choose to enter a CTC, it indicates the out-of-band authentication type. You must first authenticate on a user-specific web page with one or more factors to retrieve the CTC.
- **3** If the in-band authentication is successful, IBM PowerSC MFA generates a CTC that you can use to log in the next time if needed. In this scenario, you don't have to wait for a new token code to be displayed.

All configured authentication methods must succeed. For example, if your account is configured for IBM PowerSC MFA with SecurID and PIV/CAC authentication methods, both authentication methods must succeed.

© Copyright IBM Corp. 2017, 2018

Out-of-band authentication type

Your administrator must configure your account for the out-of-band authentication type and must notify you whether to use the out-of-band web page to get a cache token credential.

When prompted by the out-of-band web page, you must specify the required token or tokens. The procedure to obtain the required token varies based on the token type, as shown in the following sections.

Obtaining a token for IBM PowerSC MFA with SecurID

To obtain a token for IBM PowerSC MFA with SecurID, complete the following steps:

1. Access the out-of-band web page on a supported web browser. For example, https://*hostname*:6793/mfa.
2. For a SecurID token without a PINpad, get the 6-8 digit token code displayed by the token.
3. For a SecurID token with a PINpad (hardware or software token), enter your PIN in the token and note the displayed passcode.
4. Specify the token code or passcode in the out-of-band web page when prompted.
5. Use the generated cache token credential as your password with the application.

Obtaining a token for PIV/CAC cards

To obtain a token for PIV/CAC cards, complete the following steps:

1. Access the out-of-band web page on a supported browser. For example, https://*hostname*:6793/mfa.
2. When prompted by the out-of-band web page, select the client certificate you want to use to authenticate yourself. Your security administrator will typically provide guidance on which certificate to use.

   Note: If you are using Internet Explorer, the Windows Internet Options "Don't prompt for client certificate selection when only one certificate exists" setting might not prompt you to choose a certificate. The "Don't prompt for client certificate selection when only one certificate exists" setting is typically controlled by the system administrator.
3. For PIV/CAC cards, you must then enter your valid PIN.
4. Use the generated cache token credential as your password with the application.

Enrolling your certificates

Your security administrator might require you to enroll your certificate before you can use it to log in by using a PIV/CAC card for the out-of-band authentication type.

If you are using a Windows system to access the certificate enrollment web page, you must clear the Windows system SSL state before enrolling the certificate. Select **Control Panel** > **Internet Options** > **Content** > **Clear SSL State**.

Select **Control Panel** > **Internet Options** > **Content** > **Advanced** and clear the **Use SSL 2.0** and **Use SSL 3.0** check boxes.

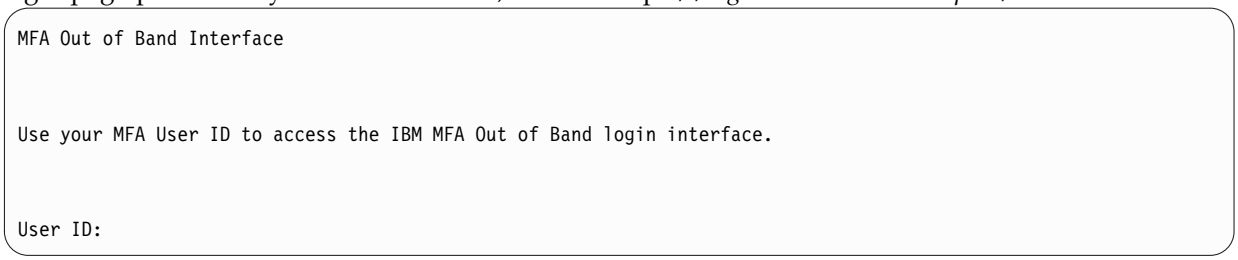
The steps requires action by both the administrator and the user, and the actions must occur in the correct sequence. Perform the following steps only as directed by your administrator.

© Copyright IBM Corp. 2017, 2018

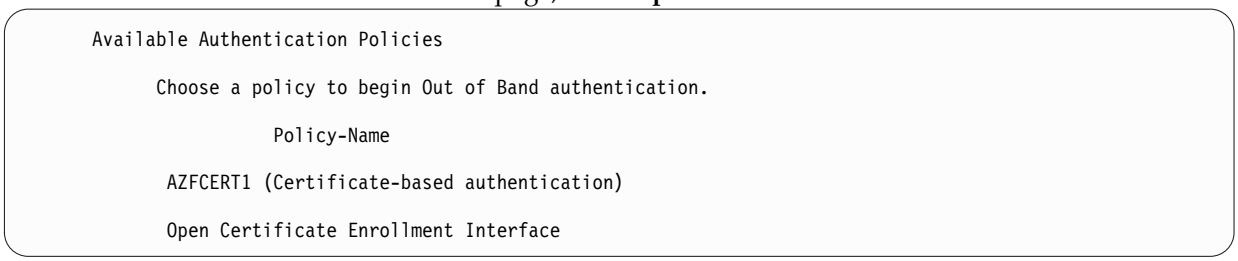
Note: This procedure has been verified on the Microsoft Internet Explorer and Google Chrome web browsers.

To enroll your certificate, complete the following steps:

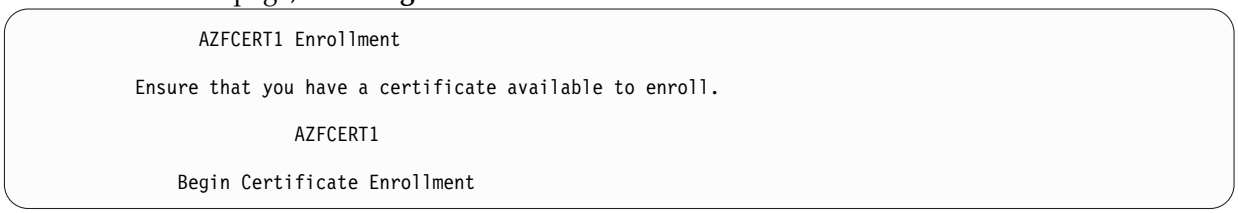
1. When instructed to do so by your administrator, begin the PIV/CAC logon process on the web server login page provided by the administrator, such as https://*login-server-hostname:port*/mfa.



2. On the Available Authentication Policies page, click **Open Certificate Enrollment Interface**.



3. Log in with your user name and password.
4. On the Enrollment page, click **Begin Certificate Enrollment.**



5. Select the certificate you want to use and click **OK**. Your security administrator will typically provide guidance on which certificate to use.

   Note: If you are using Internet Explorer, the Windows Internet Options "Don't prompt for client certificate selection when only one certificate exists" setting might block you from choosing a certificate. The "Don't prompt for client certificate selection when only one certificate exists" setting is typically controlled by the system administrator.
   For PIV/CAC cards or other smart cards, you must then enter your valid PIN.

   Note: If you receive an error message indicating that the server certificate is invalid, it is more likely that the certificate you chose is invalid.
6. Upon successful completion, you will receive a message indicating that the certificate enrollment succeeded and to await further instruction from the administrator.

```
            AZFCERT1 Enrollment

    Ensure that you have a certificate available to enroll.



    AZFCERT1 -[Succeeded]

Certificate enrollment succeeded. Your certificate is tagged for Review.

An administrator will notify you when it is Approved. Please close

your browser window.
```

The administrator notifies you about when you can use the certificate to log in. For instructions, see "Logging in to an application by using the out-of-band authentication type."

7. Close the browser window to end the session.

Logging in to an application by using the out-of-band authentication type

You can use the out-of-band login web page to provide the required authentication tokens. Your security administrator determines which tokens you must specify.

Your security administrator notifies you if you need to use the out-of-band authentication type to log in. If you are required to use the out-of-band authentication type and you do not use it, you receive a reminder error message.

Note: This procedure has been verified on Microsoft Internet Explorer and Google Chrome web browsers.

Perform the following steps to log in to an application:

1. Use a web browser to connect to the URL provided by your security administrator. For example, https://*login-server-hostname:port*/mfa.

```
MFA Out of Band Interface

Use your MFA User ID to access the IBM MFA Out of Band login interface.
                User ID:
```

2. Enter your user name. If your account is provisioned, a user-specific authentication page is displayed.
3. Choose your policy and follow the web interface. If more than one policy is displayed, your security administrator notifies you about which policy to use.

   Note: When you choose a policy for a login session, that policy is enforced for that session. If you need to choose another policy, log off and log in again to start a new session.
4. Follow the web interface to enter the required tokens.

   Note: The method of generating a token depends on your token type, as described in "Out-of-band authentication type" on page 3.
5. After you successfully enter the first required token, the out-of-band web page prompts you to enter the next required token.
6. After you have completed the token requirements, the out-of-band web page displays the cache token credential.

```
Cache Token Credential

You have satisfied the authentication policy.

                CREDENTIAL
Click the above Cache Token Credential to copy it to Clipboard,
and use this in place of your password to access applications
```

7. Manually enter or copy and paste the cache token credential as your password in your application, as appropriate. For example, for Telnet on the AIX® operating system, paste in your cache token credential when prompted.

```
telnet hostname
Trying...
Connected to hostname.
Escape character is '^]'.

AIX Version 7
Copyright IBM Corporation, 1982, 2017.
login: user-name
Available Policies:
1. test5
Select Policy or enter CTC: CTC


*******************************************************************************
*                                                                             *
*                                                                             *
*  Welcome to AIX Version 7.1!
```

   Note: If you are using Internet Explorer and use the cache token credential copy feature, the Windows Internet Options settings can affect its function. Specifically, the "Allow Programmatic Clipboard Access" setting in one or more applicable zones can disable this feature or require you to respond to an additional prompt. The "Allow Programmatic Clipboard Access" setting is typically controlled by the system administrator.
   On the AIX operating system, IBM PowerSC MFA validates the cache token credential and allows or denies the login attempt.
8. If your administrator has configured the CTC to be reusable, you can reuse it to log in for the period of time determined by your administrator. If the CTC is not reusable, you must generate a new CTC if you need to log in again.

SecurID in-band authentication method

The method of logging in by using IBM PowerSC MFA with SecurID authentication depends on your RSA token type. The token type can be a fob-style hardware token, a hardware token with a PINpad, or a software token. If you are not sure about the RSA token type you are using, ask your system administrator.

This section describes how to log in to several sample applications by using IBM PowerSC MFA with the SecurID authentication method. Examples included in this section include Remote Shell (RSH), Telnet, and Secure Shell (SSH). The actual applications for which you must use IBM PowerSC MFA with the SecurID authentication method are determined by your system administrator.

Logging in to RSH by using IBM PowerSC MFA with SecurID

The method of logging into RSH by using IBM PowerSC MFA with SecurID depends on the token type you are using. You must already have a valid PIN.

If the security administrator has enabled your account for IBM PowerSC MFA, you do not need to use your password to log in. Instead, the method of logging in to RSH depends on the type of token you have.

General guidelines

Observe the following guidelines:

- It is a best practice to wait until the token code changes before attempting to log in.
- You can use the token code only once.
- If you receive an authentication failure, wait until the token code changes before attempting to log in again.

Logging in to RSH by using a fob-style hardware token

You can log in to RSH on the IBM PowerSC MFA system by using a valid PIN. This scenario requires a fob-style hardware token.

Perform the following steps to log in to RSH by using a fob-style hardware token:

1. Open an RSH connection to the IBM PowerSC MFA client system.
2. Press Enter.
3. Enter the number of the IBM PowerSC MFA policy you want to use. This policy must be active for the AZFSIDP1 factor on the IBM PowerSC MFA system.
4. Get the 6-8 digit token code that is displayed by the SecurID token.
5. Enter your PIN **followed by** the 6-8 digit token code displayed by the SecurID token in the password field. For example, if your PIN is 4321 and your token code is 456789, enter 4321456789 in the password field.
6. Press Enter.
7. As a convenience, IBM PowerSC MFA generates a CTC that you can use to log in a second time if needed. If your administrator has set the CTC to be reusable, you can reuse it to log in for the period of time determined by your administrator.

© Copyright IBM Corp. 2017, 2018

Logging in to RSH by using a hardware token with a PINpad

You can log in to RSH on the IBM PowerSC MFA system by using a valid PIN. This scenario requires a hardware token with a PINpad.

Perform the following steps to log in to RSH by using a hardware token with a PINpad:

1. Open an RSH connection to the IBM PowerSC MFA client system.
2. Press Enter.
3. Enter the number of the IBM PowerSC MFA policy you want to use. This policy must be active for the AZFSIDP1 factor on the IBM PowerSC MFA system.
4. Enter your PIN in the SecurID token and generate a passcode.
5. Enter the 6-8 digit passcode displayed by the SecurID token in the password field.
6. Press Enter.
7. As a convenience, IBM PowerSC MFA generates a CTC that you can use to log in a second time if needed. If your administrator has set the CTC to be reusable, you can reuse it to log in for the period of time determined by your administrator.

Logging in to RSH by using a software token

You can log in to RSH on the IBM PowerSC MFA system by using a valid PIN. This scenario requires a software token application.

Perform the following steps to log in to RSH by using a software token:

1. Open an RSH connection to the IBM PowerSC MFA client system.
2. Press Enter.
3. Enter the number of the IBM PowerSC MFA policy you want to use. This policy must be active for the AZFSIDP1 factor on the IBM PowerSC MFA system.
4. Enter your PIN in the software token application and generate a passcode. Use the copy feature to copy the passcode.
5. Paste the 6-8 digit passcode displayed by the software token in the password field.
6. Press Enter.
7. As a convenience, IBM PowerSC MFA generates a CTC that you can use to log in a second time if needed. If your administrator has set the CTC to be reusable, you can reuse it to log in for the period of time determined by your administrator.

Logging in to SSH by using IBM PowerSC MFA with SecurID

The method of logging into SSH by using IBM PowerSC MFA with SecurID depends on the token type you are using. You must already have a valid PIN.

If the security administrator has enabled your account for IBM PowerSC MFA, you do not need to use your password to log in. Instead, the method of logging in to SSH depends on the type of token you have.

General guidelines

Observe the following guidelines:

- It is a best practice to wait until the token code changes before attempting to log in.
- You can use the token code only once.
- If you receive an authentication failure, wait until the token code changes before attempting to log in again.

Logging in to SSH by using a fob-style hardware token

You can log in to SSH on the IBM PowerSC MFA system by using a valid PIN. This scenario requires a fob-style hardware token.

Perform the following steps to log in to SSH by using a fob-style hardware token:

1. Open an SSH connection to the IBM PowerSC MFA client system. Consider the following example:
   ```
   ssh user-name@your-host
   ```
2. Enter the number of the IBM PowerSC MFA policy you want to use. This policy must be active for the AZFSIDP1 factor on the IBM PowerSC MFA system.
3. Get the 6-8 digit token code displayed by the SecurID token.
4. Enter your PIN **followed by** the 6-8 digit token code displayed by the SecurID token in the password field. For example, if your PIN is 4321 and your token code is 456789, enter 4321456789 in the password field.
5. Press Enter. If successful, the SSH command succeeds.
6. As a convenience, IBM PowerSC MFA generates a CTC that you can use to log in a second time if needed. If your administrator has set the CTC to be reusable, you can reuse it to log in for the period of time determined by your administrator.

Logging in to SSH by using a hardware token with a PINpad

You can log in to SSH on the IBM PowerSC MFA system by using a valid PIN. This scenario requires a hardware token with a PINpad.

Perform the following steps to log in to SSH by using a hardware token with a PINpad:

1. Open an SSH connection to the IBM PowerSC MFA client system. Consider the following example:
   ```
   ssh user-name@your-host
   ```
2. Enter the number of the IBM PowerSC MFA policy you want to use. This policy must be active for the AZFSIDP1 factor on the IBM PowerSC MFA system.
3. Enter your PIN in the SecurID token and generate a passcode.
4. Enter the 6-8 digit passcode displayed by the SecurID token in the password field.
5. Press Enter. If successful, the SSH command succeeds.
6. As a convenience, IBM PowerSC MFA generates a CTC that you can use to log in a second time if needed. If your administrator has set the CTC to be reusable, you can reuse it to log in for the period of time determined by your administrator.

Logging in to SSH by using a software token

You can log in to SSH on the IBM PowerSC MFA system by using a valid PIN. This scenario requires a software token application.

Perform the following steps to log in to SSH by using a software token:

1. Open an SSH connection to the IBM PowerSC MFA client system. Consider the following example:
   ```
   ssh user-name@your-host
   ```
2. Enter the number of the IBM PowerSC MFA policy you want to use. This policy must be active for the AZFSIDP1 factor on the IBM PowerSC MFA system.
3. Enter your PIN in the software token application and generate a passcode. Use the copy feature to copy the passcode.
4. Paste the 6-8 digit passcode displayed by the software token in the password field.
5. Press Enter. If successful, the SSH command succeeds.

6. As a convenience, IBM PowerSC MFA generates a CTC that you can use to log in a second time if needed. If your administrator has set the CTC to be reusable, you can reuse it to log in for the period of time determined by your administrator.

Logging in to Telnet by using IBM PowerSC MFA with SecurID

The method of logging in to Telnet by using IBM PowerSC MFA with SecurID depends on the token type you are using. You must already have a valid PIN.

If the security administrator has enabled your account for IBM PowerSC MFA, you no longer use your password to log in. Instead, how you log in with Telnet depends on the type of token you have.

General guidelines

Observe the following guidelines:

- It is a best practice to wait until the token code changes before attempting to log in.
- You can use the token code only once.
- If you receive an authentication failure, wait until the token code changes before attempting to log in again.

Logging in to Telnet by using a fob-style hardware token

You can log in to Telnet on the IBM PowerSC MFA system by using a valid PIN. This scenario requires a fob-style hardware token.

Perform the following steps to log in to Telnet by using a fob-style hardware token:

1. Open a Telnet connection to the IBM PowerSC MFA client system. Consider the following examples:
   ```
   telnet your-host
   ```
2. Enter your user name.
3. Enter the number of the IBM PowerSC MFA policy you want to use. This policy must be active for the AZFSIDP1 factor on the IBM PowerSC MFA system.
4. Get the 6-8 digit token code displayed by the SecurID token.
5. Enter your PIN **followed by** the 6-8 digit token code displayed by the SecurID token in the password field. For example, if your PIN is 4321 and your token code is 456789, enter 4321456789 in the password field.
6. Press Enter. If successful, the Telnet command succeeds.
7. As a convenience, IBM PowerSC MFA generates a CTC that you can use to log in a second time if needed. If your administrator has set the CTC to be reusable, you can reuse it to log in for the period of time determined by your administrator.

Logging in to Telnet by using a hardware token with a PINpad

You can log in to Telnet on the IBM PowerSC MFA system with a valid PIN. This scenario requires a hardware token with a PINpad.

Perform the following steps to log in to Telnet by using a hardware token with a PINpad:

1. Open a Telnet connection to the IBM PowerSC MFA client system. Consider the following examples:
   ```
   telnet your-host
   ```
2. Enter your user name.
3. Enter the number of the IBM PowerSC MFA policy you want to use. This policy must be active for the AZFSIDP1 factor on the IBM PowerSC MFA system.
4. Enter your PIN in the SecurID token and generate a passcode.
5. Enter the 6-8 digit passcode displayed by the SecurID token in the password field.

6. Press Enter. If successful, the Telnet command succeeds.
7. As a convenience, IBM PowerSC MFA generates a CTC that you can use to log in a second time if needed. If your administrator has set the CTC to be reusable, you can reuse it to log in for the period of time determined by your administrator.

Logging in to Telnet by using a software token

You can log in to Telnet on the IBM PowerSC MFA system with a valid PIN. This scenario requires a software token application.

Perform the following steps:

1. Open a Telnet connection to the IBM PowerSC MFA client system. Consider the following examples:
   ```
   telnet your-host
   ```
2. Enter your user name.
3. Enter the number of the IBM PowerSC MFA policy you want to use. This policy must be active for the AZFSIDP1 factor on the IBM PowerSC MFA system.
4. Enter your PIN in the software token application and generate a passcode. Use the copy feature to copy the passcode.
5. Paste the 6-8 digit passcode displayed by the software token in the password field.
6. Press Enter. If successful, the Telnet command succeeds.
7. As a convenience, IBM PowerSC MFA generates a CTC that you can use to log in a second time if needed. If your administrator has set the CTC to be reusable, you can reuse it to log in for the period of time determined by your administrator.

PIV/CAC in-band authentication method

You can use the PIV/CAC authentication method in-band to log in to the AIX operating system that has a smart card reader directly attached to the USB port, or to an application on that system.

Your system administrator must have configured the AIX operating system for the IBM PowerSC MFA PIV/CAC authentication method.

Attention: Make sure the smart card is not in the reader when the session is locked and any of following conditions occur. Otherwise, the login may try to use the smart card PIN as the password and thereby invalidate the smart card after some number of failed attempts.

- Password fallback is enabled and the login falls back to your password.
- You need to use your password to log in.
- The root user logs in with a password to unlock the session.

Perform the following steps to log in to the AIX operating system that has a smart card reader directly attached to the USB port:

1. Enroll your certificate as instructed by your system administrator. Your administrator might perform this step on your behalf.
2. Log in to the AIX operating system that has a smart card reader attached to the USB port, or to a local application on that system, and enter your user name.
3. Press Enter.

```
Smartcard authentication starts
Smart card found.
Welcome OT AWP (User PIN)!
Smart card PIN:
```

4. Enter the PIN for the certificate.
5. Press Enter.

```
verifying certificate
Checking signature
*******************************************************************************
*                                                                             *
*                                                                             *
*  Welcome to AIX Version 7.2!                                                *
```

© Copyright IBM Corp. 2017, 2018

Notices

This information was developed for products and services offered in the US.

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 grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing

IBM Corporation

North Castle Drive, MD-NC119

Armonk, NY 10504-1785

US

For license inquiries regarding double-byte character set (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

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 jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may 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 websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

© Copyright IBM Corp. 2017, 2018

IBM may use or distribute any of the information you provide 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 Director of Licensing

IBM Corporation

North Castle Drive, MD-NC119

Armonk, NY 10504-1785

US

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.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

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.

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

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

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 actual people or business enterprises 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. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

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

© (your company name) (year).

Portions of this code are derived from IBM Corp. Sample Programs.

© Copyright IBM Corp. _enter the year or years_.

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, 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 the 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.

For more information about the use of various technologies, including cookies, for these purposes, see IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM’s Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled “Cookies, Web Beacons and Other Technologies” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at http://www.ibm.com/software/info/product-privacy.

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 www.ibm.com/legal/copytrade.shtml.

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

Index

© Copyright IBM Corp. 2017, 2018

Printed in USA