IBM MFA
2.1

IBM Z Multi-Factor Authentication for z/VM

SC27-4938-40

Note

Before using this information and the product it supports, read the information in "Notices" on page 147.

This edition applies to Version *2* Release *1* of IBM Z Multi-Factor Authentication (product number 5655-MA1) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Tables... vii

About this information... ix

How to send your comments to IBM...xi

If you have a technical problem..xi

Summary of changes..xiii

Chapter 1. IBM MFA concepts...1

IBM MFA features for z/VM..1

Multi-factor authentication concepts...1

RSA Authentication Manager concepts...3

SecurID token code...3

SecurID PIN..3

SecurID passcode...3

Types of token devices...3

Chapter 2. IBM MFA Prerequisites... 5

Chapter 3. Installing IBM MFA..7

IBM MFA requirements..7

Installing and initializing postgres on SUSE Linux Enterprise Server on IBM Z......................................8

Installing and initializing postgres on Red Hat Enterprise Linux Server on IBM Z.................................8

Obtaining the PKCS#12 file and certificate password...8

Configuring a PKCS#11 token..9

Installing openCryptoki on SUSE Linux Enterprise Server on IBM Z..9

Installing openCryptoki on Red Hat Enterprise Linux Server on IBM Z...9

Using pkcsslotd and pkcsconf to configure a PKCS#11 token..10

Installing IBM MFA server and GUI..11

Completing the server setup...12

Managing IBM MFA administrator IDs..13

Adding IBM MFA administrator IDs..13

Listing IBM MFA administrator IDs..14

Deleting IBM MFA administrator IDs...14

Resuming IBM MFA administrator IDs...15

Editing the `/etc/pam.d` files on Red Hat Enterprise Linux Server on IBM Z.....................................15

Editing the `/etc/pam.d` files on SUSE Linux Enterprise Server on IBM Z..15

Starting the IBM MFA server..16

Locating the IBM MFA server log file...17

Restarting the IBM MFA server...17

Starting the IBM MFA database...17

Updating IBM MFA server and GUI..18

Chapter 4. Using the IBM MFA GUI... 21

Navigating the IBM MFA GUI 21

Chapter 5. Configuring server options..23

Enabling strict PCI compliance mode...25

Chapter 6. Configuring IBM MFA authentication methods 27
Configuring the RSA SecurID authentication method.. 27
Prerequisites for using the RSA SecurID authentication method 27
Configuring the RSA SecurID authentication method.. 28
Configuring the IBM MFA for PIV/CAC or X.509 Certificate authentication method.............................. 29
Creating the server truststore... 29
Configuring IBM MFA for PIV/CAC or X.509 Certificate authentication...................................... 30
Enabling OCSP validation.. 31
Configuring the TOTP authentication method... 33
Configuring the IBM MFA for generic RADIUS authentication method.. 35
Configuring the IBM MFA for SafeNet RADIUS authentication method.. 37
Configuring the RSA SecurID RADIUS authentication method.. 38
Configuring IBM MFA for Yubico OTP authentication... 40
Configuring IBM MFA for LDAP Simple Bind authentication... 41
Configuring IBM MFA for IBM Security Access Manager authentication..................................... 42
Configuring the PAM authentication method... 44

Chapter 7. Configuring IBM MFA policies.. 45
Creating IBM MFA policies... 45
Displaying IBM MFA policies... 45
Associating IBM MFA policies with authentication methods... 46
Setting policy token timeout.. 46
Setting the cache token credential to be reusable... 46
Deleting IBM MFA policies... 47

Chapter 8. Provisioning IBM MFA users.. 49
Provisioning users in bulk for IBM MFA.. 49
Enabling users for IBM MFA... 52
Enabling users for RSA SecurID authentication.. 52
Enabling users for IBM MFA for PIV/CAC or X.509 Certificate authentication.............................. 53
Enabling users for TOTP authentication... 55
Enabling users for IBM MFA for generic RADIUS authentication.. 56
Enabling users for IBM MFA for SafeNet RADIUS authentication.. 57
Enabling users for RSA SecurID RADIUS authentication.. 59
Enabling users for IBM MFA for Yubico OTP authentication... 60
Enabling users for IBM MFA for LDAP Simple Bind 65
Enabling users for IBM MFA for IBM Security Access Manager authentication............................ 66
Enabling users for IBM MFA Password Authentication... 68
Assigning policies and authentication methods to users.. 69
Displaying users.. 69
Checking and updating user information... 70
Suspending or resuming a user account... 70
Enabling a TOTP suspended user... 71
Setting or resetting a user's MFA password... 71
Changing a user's MFA password... 72
Checking and updating user information... 72
Removing policies for a user.. 73

Chapter 9. Adding z/VM clients... 75

Chapter 10. Removing z/VM clients.. 77

Chapter 11. Backing up and restoring the IBM MFA database............................... 79

Chapter 12. Updating postgres.. 81

Chapter 13. Preparing user devices for IBM TouchToken for iOS authentication..... 83

Chapter 14. Troubleshooting IBM MFA 85

Chapter 15. Optional: Creating test root and server certificates.............................87

Chapter 16. IBM MFA messages.. 91
IBM MFA ssl messages...140

Chapter 17. Translating IBM MFA messages and HTML..143

Appendix A. Accessibility..145

Notices...147
Terms and conditions for product documentation.. 148
IBM Online Privacy Statement... 149
Policy for unsupported hardware..149
Minimum supported hardware...149
Trademarks...150

Index.. 151

Tables

1. Required Ports........ 5

2. IBM MFA Requirements........ 7

3. Server Options 23

4. IBM MFA for PIV/CAC or X.509 Certificate Authentication Method........ 30

5. TOTP Factor Attributes........ 33

6. IBM MFA for generic RADIUS Authentication Method Attributes........ 35

7. IBM MFA for SafeNet RADIUS Authentication Method Attributes........ 37

8. RSA SecurID RADIUS Authentication Method Attributes........ 39

9. IBM MFA for Yubico OTP Authentication Method Attributes........ 40

10. IBM MFA for LDAP Simple Bind Authentication Method Attributes........ 41

11. IBM MFA for IBM Security Access Manager Authentication Method Attributes........ 43

12. PAM Authentication Method Attributes........ 44

13. azfbulk Parameters........ 50

14. Authentication-Method-Specific Parameters........ 50

15. User-specific TOTP settings........ 55

16. Login Options for SafeNet Quick Log........ 58

17. Login Options for SafeNet Challenge-Response........ 59

18. azfyubi1_ingest Parameters........ 62

About this information

This book provides instructions for customizing and using IBM® Z Multi-Factor Authentication for z/VM, which is referred to in this document as IBM MFA. The book is designed to help system administrators, security administrators, and operators customize the product following installation.

This book assumes that readers have a working knowledge of:

- The Linux for Z operating system
- Authentication mechanisms
- OpenSSL
- PKCS#11 tokens

Related z/VM documentation

Refer to the following documentation to configure and use z/VM with IBM MFA:

- GC24-6292 *z/VM: Installation Guide*
- SC24-6271 *z/VM: CP Planning and Administration*
- SC24-6331 *z/VM: TCP/IP Planning and Customization*
- SC24-6311 *z/VM: RACF Security Server Security Administrator's Guide*
- SC24-6312 *z/VM: RACF Security Server System Programmer's Guide*

To find the complete z/VM library, go to https://www.ibm.com/support/knowledgecenter/SSB27U.

How to send your comments to IBM

We invite you to submit comments about the z/OS® product documentation. Your valuable feedback helps to ensure accurate and high-quality information.

Important: If your comment regards a technical question or problem, see instead "If you have a technical problem" on page xi.

Submit your feedback by using the appropriate method for your type of comment or question:

Feedback on z/OS function

If your comment or question is about z/OS itself, submit a request through the IBM RFE Community (www.ibm.com/developerworks/rfe/).

Feedback on IBM Knowledge Center function

If your comment or question is about the IBM Knowledge Center functionality, for example search capabilities or how to arrange the browser view, send a detailed email to IBM Knowledge Center Support at ibmkc@us.ibm.com.

Feedback on the z/OS product documentation and content

If your comment is about the information that is provided in the z/OS product documentation library, send a detailed email to mhvrcfs@us.ibm.com. We welcome any feedback that you have, including comments on the clarity, accuracy, or completeness of the information.

To help us better process your submission, include the following information:

- Your name, company/university/institution name, and email address
- The following deliverable title and order number: IBM Z Multi-Factor Authentication for z/VM, SC27-4938-40
- The section title of the specific information to which your comment relates
- The text of your comment.

When you send comments to IBM, you grant IBM a nonexclusive authority to use or distribute the comments in any way appropriate without incurring any obligation to you.

IBM or any other organizations use the personal information that you supply to contact you only about the issues that you submit.

If you have a technical problem

If you have a technical problem or question, do not use the feedback methods that are provided for sending documentation comments. Instead, take one or more of the following actions:

- Go to the IBM Support Portal (support.ibm.com).
- Contact your IBM service representative.
- Call IBM technical support.

Summary of changes

Changes made to IBM MFA for Version 2 Release 1.

New

The following information is new.

November 2021 refresh

- The section Chapter 12, “Updating postgres,” on page 81 is added in this release.
- The section “Updating IBM MFA server and GUI” on page 18 is added in this release.

April 2021 refresh

- The IBM MFA server installs the mfa.service, which has dependencies on postgresql and pkcsslotd systemd services. The systemd service ensures that the dependent services are running before starting IBM MFA server. Multiple sections have been updated to reflect this change.
- The **azf_administrator_util** command is enhanced in this release, as described in “Managing IBM MFA administrator IDs” on page 13.
- “Approving user certificates” on page 54 and “Preparing user devices for generic TOTP authentication” on page 56 are updated with easier to use enrollment URLs.

January 2021 refresh

- Added editorial improvements and cross-reference link updates.

November 2020 refresh

- The Consecutive Failures Before TOTP Suspension setting is added, as described in “Configuring the TOTP authentication method” on page 33. This setting was not previously documented.
- Clarified that generic RADIUS uses UDP only.
- The section Chapter 11, “Backing up and restoring the IBM MFA database,” on page 79 has been added to the documentation.

July 2020 refresh

- The IBM MFA for LDAP Simple Bind authentication method has been added to the documentation.
- The change MFA password feature has been added to the documentation.
- Several product names have been updated.

June 2020 refresh

- IBM Z Multi-Factor Authentication for z/VM is introduced in this release.

Chapter 1. IBM MFA concepts

IBM Z Multi-Factor Authentication for z/VM®, which is referred to in this document as IBM MFA, provides alternative authentication mechanisms for systems. You can use IBM MFA with a large variety of applications.

The most common method for authenticating users to applications is by the use of passwords. Unfortunately, passwords can present a relatively simple point of attack for exploitation. For systems that rely on passwords to be secure, the system administrator must enforce password controls and provide user education. Users tend to pick common passwords, write down passwords, and unintentionally install malware that can log passwords. Additionally, building a powerful dedicated password cracking computer system has become trivial and low cost. IBM MFA provides a method to raise the assurance level of systems by requiring extra authentication factors for users.

IBM MFA features for z/VM

IBM MFA provides a multifactor authentication solution with the typical z/VM user experience.

The IBM MFA multifactor authentication solution minimizes additional administration and maintenance, supports single or shared database environments, and includes support for RACF® and other external security managers (ESMs) for z/VM.

IBM MFA provides the following features:

- The IBM MFA server runs on a Linux® on IBM Z® system.
- Uses TLS encryption to guarantee security and privacy of the data.
- Uses a TCPIP-based protocol to communicate between the z/VM systems and the IBM MFA server.
- Allows multiple z/VM systems to connect to one IBM MFA instance.
- Allows specified users to log on without IBM MFA for disaster recovery and emergency.

Multi-factor authentication concepts

IBM MFA relies on multiple authentication factors.

Multi-factor authentication is a method of computer access control in which a user is granted access only after successfully providing several authentication factors to an authentication mechanism. The authentication factors are typically from at least two of the following categories: knowledge (*something they know*), possession (*something they have*), and inheritance (*something they are*).

Multiple authentication factors improves the security of user accounts.

Consider the following IBM MFA authentication flow:

1. You create an IBM MFA authentication policy for users and provide them with the policy URL.
2. The user navigates to the policy URL and provides credentials that satisfy the authentication methods of the policy.
3. The IBM MFA server provides an authentication token called a *cache token credential (CTC)*.
4. The user navigates to the z/VM LOGON screen.
5. The user enters their user ID and pastes the authentication token in to the password field.
6. The ESM communicates with the IBM MFA server to verify the authentication token.
7. If verification is successful, the ESM authorizes the logon.

IBM MFA for RSA SecurID authentication method

While authenticating by using the IBM MFA for RSA SecurID authentication method, the RSA Authentication Manager determines whether the user's credentials are valid, and if valid returns success to IBM MFA. The operating system then resumes control and completes the authentication and authorization process as usual.

The IBM MFA for RSA SecurID authentication method requires the following credentials:

- *Something you have*: The hardware or software RSA SecurID token.
- *Two things you know*: An RSA SecurID Personal Identification Number (PIN), and *something you know*.

IBM MFA for PIV/CAC or X.509 Certificate method

The IBM MFA for PIV/CAC or X.509 Certificate method is a general-purpose certificate authentication that includes Personal Identification Verification (PIV) and Common Access Card (CAC) cards. Certificate authentication uses the client identity certificate to authenticate the user.

The IBM MFA for PIV/CAC or X.509 Certificate method requires the following credentials:

- *Something you have*: The approved certificate, typically from a PIV or CAC card or other smart card.
- *Something you know*: The Personal Identification Number (PIN).

IBM MFA for RADIUS authentication methods

IBM MFA includes support for "generic" RADIUS, SafeNet RADIUS, and RSA SecurID RADIUS. Generic RADIUS refers to the RADIUS server of your choice that returns a simple allowed or denied response. In all cases, the RADIUS server determines whether the user's credentials are valid, and if so, returns success. The operating system then resumes control and completes the authentication and authorization process as usual.

IBM MFA for TOTP authentication method

The two methods of generating a hashed, timed one-time password (TOTP) are generic TOTP and IBM TouchToken for iOS.

If you configure a user's account for generic TOTP, the user can log in by using common Quick Response (QR) codes on both Android and Apple iOS devices. The user installs a QR code application such as IBM Verify, Google Authenticator, or Duo Mobile on their device. The user then uses the generated timed one-time password (OTP) with their user name to log in.

For IBM TouchToken for iOS, the user uses the IBM TouchToken for iOS application on supported Apple devices to generate a hashed, timed one-time password (OTP), and then uses this password together with their user name to log in.

For both generic TOTP and IBM TouchToken for iOS, the OTP password must match the OTP password generated on the IBM MFA server. OTP passwords are regenerated at regular intervals.

TOTP requires:

- *Something you have*: The Apple Touch ID device with the provisioned IBM TouchToken for iOS application, or a QR code application on an Android and Apple iOS device.
- *Something you are*: Your fingerprint.

IBM MFA for Yubico OTP authentication method

The OTP password generated by the Yubikey token must match the OTP password generated by the IBM MFA for Yubico OTP component on the IBM MFA server. OTP passwords are generated when you trigger the Yubikey token.

IBM MFA for Yubico OTP requires:

- *Something you have*: The hardware Yubikey token.
- *Something you know*: IBM MFA for Yubico OTP should be used with another authentication method.

IBM MFA for IBM Security Access Manager authentication method

IBM MFA for IBM Security Access Manager requires:

- *Something you know*: The IBM MFA for IBM Security Access Manager verification one-time password, if configured.
- *Something you know*: The IBM MFA for IBM Security Access Manager user ID and password.

RSA Authentication Manager concepts

The RSA Authentication Manager includes token codes, PINs, and passcodes.

SecurID token code

The SecurID token code is a continuously regenerated number used to prove the user's identity.

The token code is a pseudo-random 6-8 digit number (PRN), based on the current time, that is displayed on the RSA SecurID token device. It is presumed that only an authorized user possesses the token device.

The token code is a one-time password (OTP). It is valid only while it is displayed, and it can be used only once. The token device generates a new token code at regular intervals, typically every 60 seconds. The display frequency for the token device determines the amount of time for which a token code appears before the display is refreshed.

SecurID PIN

The SecurID PIN is conceptually similar to a PIN that the user might use for financial transactions. It is a number that only the user knows that helps to identify the user.

The Personal Identification Number (PIN) is a unique 4-8 digit identifier that only the user knows. The PIN can be of the user's choosing, or system-generated by RSA Authentication Manager depending on the RSA token policy. If the user creates their own PIN, they should follow the locally established rules for creating a valid PIN, such as the number of characters and the reuse policy.

The RSA security administrator can clear and reset the PIN and the user's current PIN becomes invalid.

SecurID passcode

A SecurID passcode is the combination of a PIN and token code.

Similar to the token code, a passcode is a one-time password (OTP). It is valid only while it is displayed, and it can be used only once.

There are two types of passcodes:

- For hardware fob-style tokens without a PINpad, the SecurID passcode consists of the user's PIN followed by the token code and the user must enter both. For example, if the PIN is 1234 and the token code is 567891, the user enters the passcode as 1234567891.
- For SecurID PINpad hardware tokens and software token applications, the user enters the PIN on the PINpad and the token generates a hash-encrypted passcode from the PIN and the generated token. The token generates a new passcode at regular intervals, typically every 60 seconds. The user then uses the generated passcode to log in.

Types of token devices

Several types of RSA SecurID token devices are supported.

RSA SecurID card-style tokens and key fobs

These devices generate a token code. Card-style tokens (such as the RSA SecurID 200) and key fobs (such as the RSA SecurID 800) function identically, with both displaying the token code on the LCD.

RSA SecurID PINpads

The user enters the PIN directly into the token, and the token generates a hash-encrypted 6-8 digit passcode. For example, by using the RSA SecurID 520 card-style PINpad, the user enters the PIN via a 10-digit numeric pad that is contained on the card. The passcode displayed is a hash-encrypted combination of the PIN and the current token code.

The user can use the PINpad token in the following ways:

- If the user has a valid PIN, the user can enter the PIN and the token generates a hash-encrypted passcode. The passcode displayed is a hash-encrypted combination of the PIN and the current token code. The passcode can be six or eight digits, depending on the profile.
- If the user does not have a valid PIN, which can occur if the security administrator forces the user to change it, use the token to generate a token code. The user then uses the generated token code to log in and change the PIN.

RSA SecurID software token applications

RSA SecurID software token applications are available on a computer or other smart device.

The user can use the software token application in the following ways:

- If the user has a valid PIN, enter the PIN and the token generates a hash-encrypted passcode. The passcode displayed is a hash-encrypted combination of the PIN and the current token code. The passcode can be six or eight digits, depending on the profile.
- If the user does not have a valid PIN, which can occur if the security administrator forces the user to change it, use the token to generate a token code. The user then uses the generated token code to log in and change the PIN.

Chapter 2. IBM MFA Prerequisites

Before you customize IBM MFA, consider the following prerequisites.

You might need to coordinate with other systems-level and network support staff to satisfy these prerequisites.

Maintenance

Apply all software updates that are available for IBM MFA from the IBM website at http://www.ibm.com/support/mysupport.

Required ports

Determine whether you need to allocate the ports that are shown in Table 1 on page 5. Both the ports must be different.

Table 1. Required Ports

Port Name	Description	When Needed
Server Authentication Port	This is the port number on which the IBM MFA web server listens.	This port is required for the IBM MFA GUI and for IBM MFA user interaction.
Mutual Authentication Port	This is the port for client (mutual) authentication.	You must allocate this port before you can use PIV/CAC cards.

General configuration prerequisites

- If you plan to use IBM MFA with SecurID:
  - Configure an RSA Authentication Agent for each system that is running IBM MFA. For more information, see your Authentication Manager documentation.
  - Create accounts for the users in RSA Authentication Manager and assign RSA tokens.
- If you plan to use IBM MFA with RADIUS:
  - Configure the RADIUS server to accept communication from the system that is running the IBM MFA server. See your RADIUS documentation for configuration information.
  - Create user accounts in the RADIUS server and assign tokens.

Chapter 3. Installing IBM MFA

The IBM MFA components are installed separately.

A post-installation step allows you to log in as the initial IBM MFA user.

IBM MFA requirements

This section describes the hardware and software requirements for installing IBM MFA.

Software requirements

You can install the IBM MFA components as described in Table 2 on page 7.

Table 2. IBM MFA Requirements

Component	Requirement
IBM MFA server and GUI components	The Red Hat Enterprise Linux Server on IBM Z must be at the following versions: • 8.x or later The SUSE Linux Enterprise Server on IBM Z must be at the following versions: • SLES 15 or later
postgres database	For SUSE Linux Enterprise Server on IBM Z: • libpq5 • postgresql10-server For Red Hat Enterprise Linux Server on IBM Z: • postgresql-server
openCryptoki	For SUSE Linux Enterprise Server on IBM Z: • openCryptoki • openCryptoki-64bit For Red Hat Enterprise Linux Server on IBM Z: • openCryptoki • opencryptoki-swtok
openssl	Red Hat Enterprise Linux Server on IBM Z • 1.1.1 SUSE Linux Enterprise Server on IBM Z • 1.1.0

Installing and initializing postgres on SUSE Linux Enterprise Server on IBM Z

You must install and initialize the postgres database if it is not already installed.

Procedure

1. Run **zypper** or **yast** to see if libpq5 and postgresql10-server are already installed. For example with **zypper**:

```
zypper se --provides libpq5
zypper se --provides postgresql10-server
```

2. Install libpq5 and postgresql10-server if they are not already installed. For example, with **zypper**:

```
zypper install libpq5
zypper install postgresql10-server
```

Installing and initializing postgres on Red Hat Enterprise Linux Server on IBM Z

You must install and initialize the postgres database if it is not already installed.

Procedure

1. Check to see if the **postgresql-server** package is already installed. For example, with **yum**:

```
# yum list postgresql-server
```

2. Install the **postgresql-server** package if it is not already installed. For example, with **yum**:

```
yum install postgresql-server
```

Obtaining the PKCS#12 file and certificate password

Obtain the PKCS#12 file and the server certificate password for your IBM MFA server system from your security administrator.

About this task

Note: If you are configuring IBM MFA in a test environment that does not have official certificates, you can create a PKCS#12 file as described in Chapter 15, “Optional: Creating test root and server certificates,” on page 87. However, it is strongly recommended that you use a server certificate issued by a well-known certificate authority.

The PKCS#12 file includes the server certificate, any intermediate certificates, and the private key in a single file. You must have the password for the server certificate.

After you obtain the PKCS#12 file and the password for the server certificate, use the secure copy (**scp**) command to copy the resulting file to the `/etc/security/mfa/certificates` directory on the IBM MFA server system. You must create this directory.

Configuring a PKCS#11 token

You must configure a PKCS#11 token.

About this task

openCryptoki is an implementation of the PKCS#11 API standard. It provides an interface to the functions of underlying cryptographic tokens. Use the **pkcsconf** utility to further configure openCryptoki after the daemon is running.

Installing openCryptoki on SUSE Linux Enterprise Server on IBM Z

You must install openCryptoki if it is not already installed.

About this task

Procedure

1. Run **zypper** or **yast** to see if openCryptoki and openCryptoki-64bit are already installed. For example with **zypper**:

   ```
   zypper se --provides openCryptoki
   zypper se --provides openCryptoki-64bit
   ```

2. Install openCryptoki and openCryptoki-64bit if they are not already installed. For example, with **zypper**:

   ```
   zypper install openCryptoki
   zypper install openCryptoki-64bit
   ```

Installing openCryptoki on Red Hat Enterprise Linux Server on IBM Z

You must install openCryptoki if it is not already installed.

About this task

Procedure

1. Check to see if the **openCryptoki** package is already installed. For example, with **yum**:

   ```
   # yum list opencryptoki
   Installed Packages
   opencryptoki.s390x               3.10.0-3.el8               @InstallMedia-BaseOS
   #
   ```

2. Install the **openCryptoki** package if it is not already installed. For example, with **yum**:

   ```
   yum install opencryptoki
   ```

3. Check to see if the **opencryptoki-swtok** package is already installed. For example, with **yum**:

   ```
   # yum list opencryptoki-swtok    Installed Packages
   opencryptoki-swtok.s390x                 3.10.0-3.el8    @InstallMedia-BaseOS
   #
   ```

4. Install the **opencryptoki-swtok** package if it is not already installed. For example, with **yum**:

   ```
   yum install opencryptoki-swtok
   ```

Using pkcsslotd and pkcsconf to configure a PKCS#11 token

You must configure a PKCS#11 token.

About this task

Procedure

1. Run the **`pkcsslotd`** command to start daemon. The daemon reads the `/etc/opencryptoki/opencryptoki.conf` file to collect information about the tokens and their slots.
2. Run the **`pkcsconf -tis`** command to see which slot is available. In this example, the default token is available in slot #3.

```
# pkcsconf -tis
PKCS#11 Info
        Version 2.20
        Manufacturer: IBM
        Flags: 0x0
        Library Description: Meta PKCS11 LIBRARY
        Library Version 3.10
Token #3 Info:
        Label: IBM OS PKCS#11
        Manufacturer: IBM Corp.
        Model: IBM SoftTok
        Serial Number: 123
        Flags: 0x880045 (RNG|LOGIN_REQUIRED|CLOCK_ON_TOKEN|USER_PIN_TO_BE_CHANGED|
SO_PIN_TO_BE_CHANGED)
        Sessions: 0/18446744073709551614
        R/W Sessions: 18446744073709551615/18446744073709551614
        PIN Length: 4-8
        Public Memory: 0xFFFFFFFFFFFFFFFF/0xFFFFFFFFFFFFFFFF
        Private Memory: 0xFFFFFFFFFFFFFFFF/0xFFFFFFFFFFFFFFFF
        Hardware Version: 1.0
        Firmware Version: 1.0
        Time: 12:35:01
Slot #3 Info
        Description: Linux
        Manufacturer: IBM
        Flags: 0x1 (TOKEN_PRESENT) 1
        Hardware Version: 0.0
        Firmware Version: 0.0
```

3. Run the **`pkcsconf -I -c 3`** command to initialize the token, in this example in slot #3. Enter the SO PIN and a token label. Remember this label, you will need it later.

   Important: The default SO PIN is 87654321. You can use the **`pkcsconf -P`** command to change this value.

```
# pkcsconf -I -c 3
Enter the SO PIN:
Enter a unique token label: azf
```

4. Run the **`pkcsconf -tis`** command to verify the token is created:

```
# pkcsconf -tis
PKCS#11 Info
        Version 2.20
        Manufacturer: IBM
        Flags: 0x0
        Library Description: Meta PKCS11 LIBRARY
        Library Version 3.10
Token #3 Info: 2
        Label: azf
        Manufacturer: IBM Corp.
        Model: IBM SoftTok
        Serial Number: 123
        Flags: 0x880445 (RNG|LOGIN_REQUIRED|CLOCK_ON_TOKEN|TOKEN_INITIALIZED|
USER_PIN_TO_BE_CHANGED|SO_PIN_TO_BE_CHANGED)
        Sessions: 0/18446744073709551614
        R/W Sessions: 18446744073709551615/18446744073709551614
        PIN Length: 4-8
        Public Memory: 0xFFFFFFFFFFFFFFFF/0xFFFFFFFFFFFFFFFF
        Private Memory: 0xFFFFFFFFFFFFFFFF/0xFFFFFFFFFFFFFFFF
        Hardware Version: 1.0
        Firmware Version: 1.0
        Time: 12:38:05
Slot #3 Info
        Description: Linux
        Manufacturer: IBM
        Flags: 0x1 (TOKEN_PRESENT)
        Hardware Version: 0.0
        Firmware Version: 0.0
```

Installing IBM MFA server and GUI

IBM MFA can run on any Red Hat Enterprise Linux Server on IBM Z or SUSE Linux Enterprise Server on IBM Z operating system that meets the minimum requirements.

About this task

You must install the IBM MFA server and GUI on one instance of a Red Hat Enterprise Linux Server on IBM Z or SUSE Linux Enterprise Server on IBM Z operating system.

The IBM MFA server installs the mfa.service, which has dependencies on postgresql and pkcsslotd systemd services. systemd ensures that the dependent services are running before starting IBM MFA server.

Important: Special considerations for SELinux

The IBM MFA installer determines whether SELinux is enabled. (You can also use the **`sestatus`** command to determine this state.) If SELinux is enabled, IBM MFA service dependencies are not set to ensure compatibility, in a manner similar to the following:

```
Is server running?
Last login: Thu Apr 15 09:36:16 EDT 2021
waiting for server to start.... done
server started
Last login: Thu Apr 15 09:36:16 EDT 2021
0
MFA DB initialization complete.
SELinux active: exiting. mfa.service installed with no dependencies.
SELinux active: mfadb files must be registered according to installed policy.
SELinux active: See /opt/IBM/MFA/db/db-selinux-rhel.sh for example
```

If SELinux is enabled in your environment, perform the following steps:

1. Review the process context and tags associated with the postgresql and pkcsslotd services before enabling mfa.service dependencies on the postgresql and pkcsslotd services.
2. After you have identified the required SELinux tags, implement the sample scripts in `/opt/IBM/MFA/db/db-selinux-rhel.sh` and `/opt/IBM/MFA/db/db-selinux-sles.sh`, respectively, to update the MFA SELinux settings and enable dependencies in mfa.service.

Procedure

1. Ensure that you are logged in as the root user.
2. Enter one of the following commands depending on the platform on which you are installing:

```
rpm -i mfa-server-2.1.0.latest.rhel8.s390x.rpm
rpm -i mfa-server-2.1.0.latest.sles15.s390x.rpm
```

```
:
waiting for server to start.... done
server started
Last login: Thu Apr 15 10:48:10 EDT 2021
0
MFA DB initialization complete.
SELinux NOT active - proceeding with service enablement of MFA and postgresql
SELinux NOT active: add MFA DB to postgresql service
Attempting stop of standalone postgres server
Last login: Thu Apr 15 10:48:10 EDT 2021
waiting for server to shut down.... done
```

```
server stopped
Starting postgresql.service
/var/run/postgresql:5432 - accepting connections
MFA DB service enablement complete.
```

3. If applicable, you can update a previously installed version of IBM MFA with the following command run with root privileges:

   ```
   rpm -U product
   ```

4. If needed, you can uninstall the RPM with the following command run with root privileges:

   ```
   rpm -e product
   ```

Completing the server setup

You must run the **azf_webserver_config** utility to complete the IBM MFA server setup.

About this task

Important: The **azf_webserver_config** utility accepts the values you specify and does not perform additional validation. If you make typing mistakes or enter invalid values, the IBM MFA daemon might not start.

To finish the IBM MFA server setup, complete the following steps:

Procedure

1. Log in to the IBM MFA server system by using SSH.
2. Change directory (cd) to /opt/IBM/MFA/bin.
3. Create an input file of the following format. A sample file is provided in /opt/IBM/MFA/conf/azfserver_setup.conf.

   ```
   # initial trace level for MFA server
   INITIAL TRACE LEVEL=0

   # location of the P12 identity certificate for the server
   P12 LOCATION=/etc/security/certificates/secsrv.p12

   # PKCS11 token used while encrypting P12 password
   PKCS11 TOKEN NAME=mfazvm

   # directory or PEM file containing CAs that will be trusted by the MFA server
   # CAS LOCATION=/etc/security/mfa/certificates/cas

   # port to use for server authentication
   SERVER AUTH PORT=6793

   # port to use for mutual authentication
   MUTUAL AUTH PORT=6794

   # port to use for ZVM Host communications
   ZVM PORT=6787
   ```

   where:

   - INITIAL TRACE LEVEL sets the IBM MFA server initial trace level. Valid values are 0 - 3, where the higher number increases the level of verbosity. You should generally accept the default value of 0.

     The IBM MFA server logs informational and error messages to the /var/log/MFA/mfa_latest-server-log.log file.
   - P12 LOCATION is the PKCS#12 certificate you obtained by completing the procedure in "Obtaining the PKCS#12 file and certificate password" on page 8.
   - PKCS11 TOKEN NAME is the PKCS#11 token you created in "Configuring a PKCS#11 token" on page 9.

- `CAS LOCATION`: You need to specify this location only if you plan to use the IBM MFA for PIV/CAC or X.509 Certificate method. For more information, see "Creating the server truststore" on page 29.
- `SERVER AUTH PORT` is the port number on which you want the web server to listen.
- `MUTUAL AUTH PORT` is the port number you want to use for mutual authentication.
- `ZVM PORT` is the port to use for z/VM host communications.

Important: Ensure that your firewall does not prevent access to the `SERVER AUTH PORT` , `MUTUAL AUTH PORT`, and `ZVM PORT` ports. Otherwise, the server will be listening on these ports but will not receive any connections, making troubleshooting difficult.

One possible method to check the firewall status is with the **`systemctl status firewalld`** command:

```
systemctl status firewalld
firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset:
enabled)
   Active: inactive (dead) since Fri 2019-12-13 12:43:29 EST; 47min ago
```

4. Ensure that the **`pkcsslotd`** daemon is running:

```
# ps -ef | grep pkcsslotd
root      3441     1  0 Jan28 ?        00:00:01 pkcsslotd
```

5. Run the following command as root.

```
./azf_webserver_config input-file
Enter password for P12 Identity Certificate:
Successfully configured AZF Webserver.
```

Managing IBM MFA administrator IDs

You must run the **`azf_administrator_util`** utility to manage IBM MFA administrator IDs. Only IBM MFA administrators can access the IBM MFA GUI.

Adding IBM MFA administrator IDs

You must run the **`azf_administrator_util`** utility to add one or more IBM MFA administrator IDs.

About this task

To add one or more IBM MFA administrator IDs, complete the following steps:

Procedure

1. Log in to the IBM MFA server system by using SSH.
2. Change directory (cd) to `/opt/IBM/MFA/bin`.
3. Run the **`azf_administrator_util`** command as root with the **add** parameter and provide the required access level to the user. The allowable access is as follows:

Access Level	Allowed Access
NONE	Nothing is allowed for the provided user ID.
READ	The user ID is allowed to get entity (user, method, and policy) information.
ADD	The user ID is allowed to add entity (user, method, and policy) information.
UPDATE	The user ID is allowed to update entity (user, method, and policy) information.

Access Level	Allowed Access
DELETE	The user ID is allowed to delete entity (user, method, and policy) information.
CONTROL	Includes READ+ADD+UPDATE+DELETE entity (user, method, and policy) access.
SUPERADMIN	Includes CONTROL plus the ability to edit the IBM MFA server options and restart the IBM MFA server through the GUI.

Specify **SUPERADMIN** to be able to perform all IBM MFA administrative functions.

```
./azf_administrator_util add username SUPERADMIN
```

An output that is similar to the following example is displayed:

```
Successfully added administrator user username with permission SUPERADMIN
```

Listing IBM MFA administrator IDs

You run the **azf_administrator_util** utility to list one or more IBM MFA administrator IDs.

About this task

To list one or more IBM MFA administrator IDs, complete the following steps:

Procedure

1. Log in to the IBM MFA server system by using SSH.
2. Change directory (cd) to /opt/IBM/MFA/bin.
3. Run the **azf_administrator_util** command as root with the **list** parameter:

```
./azf_administrator_util list
```

An output that is similar to the following example is displayed:

```
adminuser: SUPERADMIN
user1: DELETE,UPDATE,READ
```

Deleting IBM MFA administrator IDs

You run the **azf_administrator_util** utility to delete IBM MFA administrator IDs.

About this task

To delete IBM MFA administrator IDs, complete the following steps:

Procedure

1. Log in to the IBM MFA server system by using SSH.
2. Change directory (cd) to /opt/IBM/MFA/bin.
3. Run the **azf_administrator_util** command as root with the **delete** parameter:

```
./azf_administrator_util delete username
```

Resuming IBM MFA administrator IDs

You run the **azf_administrator_util** utility to resume suspended IBM MFA administrator IDs. This function may be needed if you use the **Server Options** pane to set an administrator suspension threshold. This suspension is separate and distinct from any operating system suspension mechanism.

About this task

To resume IBM MFA suspended administrator IDs, complete the following steps:

Procedure

1. Log in to the IBM MFA server system by using SSH.
2. Change directory (cd) to `/opt/IBM/MFA/bin`.
3. Run the **azf_administrator_util** command as root with the **unsuspend** parameter:

```
./azf_administrator_util unsuspend username
```

Editing the /etc/pam.d files on Red Hat Enterprise Linux Server on IBM Z

This section describes how to edit azfserver in the `/etc/pam.d` directory to use IBM MFA. You can also use the **authconfig** tool to configure PAM instead of manually editing the PAM configuration files, as described in the Red Hat Enterprise Linux Server on IBM Z documentation.

About this task

To use the IBM MFA PAM module, complete the following steps:

Procedure

1. Create (**touch**) the file `/etc/pam.d/azfserver`.
2. Edit `/etc/pam.d/azfserver` and add a site-specific version of the following entry:

```
#%PAM-1.0
auth required pam_sepermit.so
auth substack password-auth
auth include postlogin
account     required      pam_nologin.so
account     include       system-auth
```

3. Save the changes.

Editing the /etc/pam.d files on SUSE Linux Enterprise Server on IBM Z

This section describes how to edit azfserver in the `/etc/pam.d` directory to use IBM MFA. You can also use the **pam-config** tool to configure PAM instead of manually editing the PAM configuration files, as described in the SUSE Linux Enterprise Server on IBM Z documentation

About this task

To use IBM MFA, complete the following steps:

Procedure

1. Create (**touch**) the file `/etc/pam.d/azfserver`.
2. Edit `/etc/pam.d/azfserver` and add a site-specific version of the following entry:

```
#%PAM-1.0
auth     required      pam_nologin.so
auth     include        common-auth
account  include        common-account
password include        common-password
```

3. Save the changes.

Starting the IBM MFA server

The IBM MFA server supports authentication of users, validation of factors at runtime, and the IBM MFA GUI.

Before you begin

Before you start the IBM MFA server, ensure that the following requirements are satisfied:

- The **pkcsslotd** service is running.

```
# systemctl status pkcsslotd
pkcsslotd.service - Daemon which manages cryptographic hardware tokens for the openCryptoki
package
   Loaded: loaded (/usr/lib/systemd/system/pkcsslotd.service; disabled; vendor preset:
disabled)
   Active: active (running) since Thu 2021-04-15 11:22:17 EDT; 1s ago
  Process: 15381 ExecStart=/usr/sbin/pkcsslotd (code=exited, status=0/SUCCESS)
 Main PID: 15382 (pkcsslotd)
    Tasks: 1 (limit: 50303)
   Memory: 5.4M
   CGroup: /system.slice/pkcsslotd.service
           └─15382 /usr/sbin/pkcsslotd
```

  If the service is not running, start it with the following command:

```
systemctl start pkcsslotd
```

- If a firewall is running, make sure that it allows access to the SERVER AUTH PORT and MUTUAL AUTH PORT ports. One possible method to check the firewall status is with the **systemctl status firewalld** command:

```
systemctl status firewalld
firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
   Active: inactive (dead) since Fri 2019-12-13 12:43:29 EST; 47min ago
```

About this task

To start the IBM MFA server as a service, complete the following steps:

Procedure

1. Enter the following command as root:

```
systemctl start mfa
```

2. Verify that the service started:

```
systemctl status mfa
```

Locating the IBM MFA server log file

The IBM MFA server logs informational and error messages to the /var/log/MFA/mfa_*latest-server*.log file. The log file contains detailed information about the function of the IBM MFA server and is intended for use by IBM support in the event of a problem.

About this task

The INITIAL TRACE LEVEL you specified in "Completing the server setup" on page 12 sets the IBM MFA server initial trace level in the log file. The default value of 0 logs standard and unconditional messages.

Note: You should generally accept the default value of 0. You should not set a trace level higher than 2 unless a problem can be reproduced and you receive specific instructions from IBM support. Lower the trace level to 0 or 1 after the problem has been reproduced and the data has been collected.

When you first start the IBM MFA server and have not yet configured any authentication methods, the log file includes information about the unconfigured authentication methods. This is expected behavior and will change as you configure the authentication methods.

To view the IBM MFA server log file:

Procedure

1. Change directory (cd) to /var/log/MFA/.
2. Find the most recent log file:

```
ls -l
```

Restarting the IBM MFA server

You must stop and restart the IBM MFA server if you change any of the settings in the **Server Options** or **Authentication Methods** panes of the IBM MFA GUI.

About this task

To restart the IBM MFA server, complete the following steps:

Procedure

1. Select **Restart MFA Server** from the **Settings** control at the top of the IBM MFA main page.
2. Instead of using the **Restart MFA Server** control, if you prefer, you can enter the following commands as root:

```
systemctl stop mfa
systemctl start mfa
```

Starting the IBM MFA database

The IBM MFA postgres database is started when you install IBM MFA. Starting IBM MFA with the systemd mfa.service dependent specification also starts the postgresql.service if it is stopped. If you need to restart the database, follow the steps in this section.

About this task

To start the IBM MFA postgres database in an SELinux environment where the postgres database is running under systemd's control, complete the following steps:

Procedure

1. Enter the following command as root to check the service status:

   ```
   systemctl status postgresql
   ```

2. Enter the following command as root to start the postgres service:

   ```
   systemctl start postgresql
   ```

To start the IBM MFA postgres database in an SELinux environment where the postgres database is not running under systemd's control, complete the following steps:

3. Enter the following commands:

   ```
   su - postgres
   pg_ctl -D /opt/IBM/MFA/mfadb start
   ```

4. Verify that the service started:

   ```
   # ps -ef | grep postgres
   postgres  6906     1  0 11:16 pts/1    00:00:00 /usr/bin/postgres -D /opt/IBM/MFA/mfadb
   ```

5. Exit the postgres user account:

   ```
   # exit
   ```

Updating IBM MFA server and GUI

If you update to a newer version of IBM MFA, your existing database and configuration settings are maintained.

Before you begin

Before you update IBM MFA, ensure that your IBM MFA server system meets the minimum system requirements described in "IBM MFA requirements" on page 7.

When you update to a newer version of IBM MFA, your existing database and configuration settings are maintained. However, as a general best practice, you should back up your database before any update, as described in Chapter 11, "Backing up and restoring the IBM MFA database," on page 79.

About this task

The IBM MFA server installs the mfa.service, which has dependencies on postgresql and pkcsslotd systemd services. systemd ensures that the dependent services are running before starting IBM MFA server.

Important: Special considerations for SELinux

The IBM MFA installer determines whether SELinux is enabled. (You can also use the **sestatus** command to determine this state.) If SELinux is enabled, IBM MFA service dependencies are not set to ensure compatibility, in a manner similar to the following:

```
Is server running?
Last login: Thu Apr 15 09:36:16 EDT 2021
waiting for server to start.... done
server started
Last login: Thu Apr 15 09:36:16 EDT 2021
0
MFA DB initialization complete.
SELinux active: exiting. mfa.service installed with no dependencies.
SELinux active: mfadb files must be registered according to installed policy.
SELinux active: See /opt/IBM/MFA/db/db-selinux-rhel.sh for example
```

If SELinux is enabled in your environment, perform the following steps:

1. Review the process context and tags associated with the postgresql and pkcsslotd services before enabling mfa.service dependencies on the postgresql and pkcsslotd services.
2. After you have identified the required SELinux tags, implement the sample scripts in `/opt/IBM/MFA/db/db-selinux-rhel.sh` and `/opt/IBM/MFA/db/db-selinux-sles.sh`, respectively, to update the MFA SELinux settings and enable dependencies in mfa.service.

Procedure

1. Ensure that you are logged in as the root user.

```
# whoami
root
```

2. Enter one of the following commands depending on the platform on which you are installing:

```
rpm -U mfa-server-2.1.0.latest.rhel8.s390x.rpm
rpm -U mfa-server-2.1.0.latest.sles15.s390x.rpm
```

3. Verify that the IBM MFA server started and remained active:

```
systemctl status mfa
● mfa.service - AZF MFA Server
   Loaded: loaded (/etc/systemd/system/mfa.service; enabled; vendor preset: disabled)
   Active: active (running) since Thu 2021-10-14 13:55:22 EDT; 1min 51s ago
 Main PID: 46413 (azfd)
    Tasks: 2 (limit: 50303)
   Memory: 3.5M
   CGroup: /system.slice/mfa.service
           ├─46413 /bin/bash /opt/IBM/MFA/bin/azfd
           └─46418 /opt/IBM/MFA/bin/azfServer
```

Chapter 4. Using the IBM MFA GUI

You can use the IBM MFA GUI to configure authentication factors and policies, and to apply the authentication factors and policies to users.

After you complete the postinstallation steps, the IBM MFA GUI is available at https://*login-server-hostname*:*port*/mfaadmin/index.html, where:

- *login-server-hostname* is the host name or IP address of the system where you installed IBM MFA server.
- *port* is the port number on which the IBM MFA web server listens.

The main page of the IBM MFA GUI contains the following four tabs:

- The **User Provisioning** tab. The **User Provisioning** tab allows the following operations:
  - Enroll a new IBM MFA user.
  - Start the provisioning wizard to assign policies and authentication methods to users.
  - Delete an existing IBM MFA user.
  - Show all users.
  - Display detailed information for a specific user.
- The **Policy Definitions** tab. The **Policy Definitions** tab shows the following policy attributes:
  - The available policies.
  - The factors that are applied to the policy.
  - The duration for which the associated cache token credential is valid before it times out.
  - Whether the cache token credential is re-usable.

  Click a policy name to display a new page with additional policy-specific settings.
- The **Authentication Methods** tab displays all of the possible authentication factors and whether they are enabled. Click an authentication method name to display a new page with more specific settings.
- The **ZVM clients** tab displays the settings for the ZVM clients that you configure.

The **Settings** control includes the following choices:

- **Server Options** displays the settings for the IBM MFA daemon.
- **Restart MFA Server** restarts the IBM MFA server.

Navigating the IBM MFA GUI

You can use the IBM MFA GUI for all interaction with IBM MFA.

Before you begin

To navigate the IBM MFA GUI, complete the following steps:

Procedure

1. Open the IBM MFA GUI at https://*login-server-hostname*:*port*/mfaadmin, where:
   - *login-server-hostname* is the host name or IP address of the system where you installed IBM MFA server.
   - *port* is the port number on which the IBM MFA web server listens.

   The IBM MFA GUI displays the main page.
2. The IBM MFA GUI main page includes the following panes:

- Select the **User Provisioning** tab to provision a user with a policy, or to add or remove a policy for a user.
- Select the **Policy Definitions** tab to add a new policy, delete an existing policy, or to display policy attributes. Click a policy name to display a new page with more policy-specific settings and to add or remove an authentication method from the policy.
- Select the **Authentication Methods** tab to configure and display all of the possible authentication method. Click an authentication method name to display a new page with more specific settings that apply to all users of that authentication method.

3. To configure and display the settings for the IBM MFA server, select **Settings** > **Server Options**.
4. To restart IBM MFA services, select **Settings** > **Restart MFA Server**.

Chapter 5. Configuring server options

Most of the initial settings for the IBM MFA server are derived from running the **`mfa_webserver_config`** utility. You must configure the remaining settings on the IBM MFA GUI **Server Options** pane.

About this task

If you make a change to the IBM MFA server settings, the GUI immediately reflects the change but the change does not take effect until you restart the IBM MFA server. In this instance, the GUI indicates the runtime value that is currently in use.

To configure the server options, complete the following steps:

Procedure

1. In the IBM MFA GUI, click **Settings**.
2. Select **Server Options**.
3. Specify the following settings to configure the IBM MFA server.

Table 3. Server Options

Setting	Allowed Values	Description
Initial Trace Level	0 - 3	Choose the initial trace level. Valid values are 0 - 3, where the higher number increases the level of verbosity. The default value is 0.
Prefer client-side CTC display	On or Off	When this setting is On, the CTC is displayed. When this setting is Off, the CTC is masked for additional security to prevent it from being observed. The default is On. The user has the option to display a masked CTC on the IBM MFA Out-of-Band page if needed.
Enable Certificate Services	On or Off	Set this to On if you plan to use the certificate authentication method. The default value is Off.
Enable TOTP Services	On or Off	Enable this setting if you plan to use TOTP or generic TOTP as described in "Configuring the TOTP authentication method" on page 33.
Enable Yubico enrollment services	On or Off	Enable this setting if you plan to enable users for IBM MFA for Yubico OTP authentication from an existing `.csv` configuration file.

Table 3. Server Options (continued)

Setting	**Allowed Values**	**Description**
Enable MFA Password Services	On or Off	Enables the MFA password setting for all users. The MFA password is a special password that allows the user to log in to the IBM MFA server for IBM MFA-specific actions, such as enrolling TOTP and IBM MFA for Yubico OTP tokens. This password is unique to the IBM MFA server.
Enable Strict PCI mode	On or Off	Enable this setting if you plan to use strict PCI mode, as described in "Enabling strict PCI compliance mode" on page 25.
PKCS#11 Token Name	Actual PKCS#11 token name	Enter the name of the PKCS#11 token you created by completing the procedure in "Configuring a PKCS#11 token" on page 9. The PKCS#11 token name is required.
Max Administrator Login Failures Before Suspension	Integer value	This setting is intended to prevent brute force attacks. If the maximum failure value is exceeded, the IBM MFA administrator account is suspended until you re-enable the account with the **azf_administrator_util** command, as described in "Resuming IBM MFA administrator IDs" on page 15.
Max CTC Check Failures Before Suspension	Integer value	This setting is intended to prevent brute force CTC attacks. If the maximum failure value is exceeded, the IBM MFA user account is suspended until you re-enable the account on the **User Provisioning** tab. If the user already has a valid CTC when the failure count is exceeded, that CTC is invalidated. If you set this value, choose a value high enough that the user does not unintentionally exceed it in the course of normal actions. For example, 50. A value of 0 indicates that brute force CTC protection is not enabled.
CTC Style	Select from the drop-down list	Choose the CTC type that you want to use from the drop-down list. All generated CTCs will use this type.

Table 3. Server Options (continued)

Setting	Allowed Values	Description
Password Hash Iteration	Select from the drop-down list	The number of hash iterations made when setting, and therefore validating, IBM MFA-specific passwords. The default is 4000 hash iterations. Higher numbers of iterations result in more secure password handling at a cost of additional processing time.
Trust Store Path	Valid file specification	You need to specify this setting only if you plan to use the IBM MFA for PIV/CAC or X.509 Certificate authentication method. See "Creating the server truststore" on page 29.
PKCS#12 Server Identity Path	Valid file specification	Enter the file specification of the server PKCS#12 file.
PKCS#12 Server Identity Passphrase	Valid passphrase	Enter the passphrase of the server PKCS#12 file.
Server Auth Port	Valid port number	Enter the port number on which the web server is listening.
Mutual Auth Port	Valid port number	Enter the port number, or zero. The mutual authentication port is required only if **Enable Certificate Services** is set to On.
ZVM Listener Port	Valid port number	Enter the port number to use for z/VM host communications.

4. Click **Save** to save your changes.
5. Restart the IBM MFA daemon, as described in "Restarting the IBM MFA server" on page 17.

Enabling strict PCI compliance mode

IBM MFA supports the Payment Card Industry Data Security Standard (PCI DSS) standard through the Enable Strict PCI Compliance Mode setting. It is recommended that you do not enable this setting unless you are fully aware of the ramifications.

About this task

The following actions are taken for IBM MFA authentication when you enable Strict PCI Compliance Mode:

- The web page prompts for all factors before validating the user's response and returning a status. If there is a failure, the user does not know which factor failed.
- Messages returned to the user for an authentication request are suppressed. The user does not know which factor caused the authentication to fail. However, need more information messages generated after a successful authentication are displayed.
- A cache token credential is always returned, even if the authentication request failed. The user cannot determine which part of the authentication failed.

Chapter 6. Configuring IBM MFA authentication methods

The **Authentication Methods** tab displays all of the possible authentication methods. Click an authentication method name to display a new page with more specific settings.

The **Authentication Methods** tab contains all of the possible authentication methods that can be applied to a policy:

- IBM MFA for PIV/CAC or X.509 Certificate is a general-purpose certificate authentication mechanism that uses the client identity certificate to authenticate the user.
- RSA SecurID is an RSA SecurID-based authentication mechanism.
- TOTP is the timed one-time-password authentication mechanism.
- IBM MFA for generic RADIUS is the generic RADIUS authentication mechanism.
- IBM MFA for SafeNet RADIUS is the SafeNet RADIUS authentication mechanism.
- RSA SecurID RADIUS is the SecurID RADIUS authentication mechanism.
- IBM MFA Password Authentication is the password authentication mechanism.
- IBM MFA for Yubico OTP is the Yubikey authentication mechanism.
- IBM MFA for IBM Security Access Manager is the IBM Security Access Manager authentication mechanism.
- IBM MFA for LDAP Simple Bind is the LDAP authentication mechanism.

Configuring the RSA SecurID authentication method

You must define the file names of the `sdconf.rec` file and the node secret, set the initial trace level, and optionally define the file name of the `sdopts.rec` file.

The RSA node secret is a shared secret known to IBM MFA and the RSA Authentication Manager. A new node secret is created by the RSA Authentication Manager during the first successful login by any user. The RSA Authentication Manager then sends the node secret to IBM MFA. You must provide the location for this file.

Prerequisites for using the RSA SecurID authentication method

You must satisfy several prerequisites before you can use the RSA SecurID authentication method.

Note: The RSA SecurID authentication method requires network access to a functioning RSA SecurID configuration. You must have already configured an RSA Authentication Agent for the system that is running the IBM MFA server, created accounts for the users in RSA Authentication Manager, and assigned RSA tokens. For more information, see your Authentication Manager documentation.

Copying the `sdconf.rec` file

The `sdconf.rec` file is the configuration file for connecting to the RSA Authentication Manager. Obtain the `sdconf.rec` file from the RSA Authentication Manager (or the RSA Authentication Manager administrator).

About this task

To copy the `sdconf.rec` file, complete the following steps:

Procedure

1. Log in as administrator to the RSA Authentication Manager.

2. Click **Access** > **Authentication Agents** > **Generate Configuration File**.
3. Select **Generate Config File**.

   The message "The configuration file was successfully generated and is ready to download" is displayed.
4. Select **Download Now**.
5. Unzip the resulting file to get the `sdconf.rec` file.
6. Use your tool of choice to copy the `sdconf.rec` file to a location of your choice on the IBM MFA server system. Copy the file in binary mode.

Creating an `sdopts.rec` file

In some environments, you might need to use an `sdopts.rec` file to ensure that the SecurID plug-in can correctly communicate with RSA Authentication Manager.

About this task

In some cases, the host IP address that is auto-detected by the SecurID authentication method does not match the IP address used for outgoing traffic. In such cases, use the **`CLIENT_IP`** parameter to manually specify the IP address that the SecurID authentication method should use. Currently, only IPV4 addresses are supported in the `sdopts.rec` file.

The `sdopts.rec` file uses the following syntax:

```
CLIENT_IP=<IP v4 Address Override>
CLIENT_IP=<IP v4 Address Override for second system>
```

To create the `sdopts.rec` file, complete the following steps:

Procedure

1. Create `sdopts.rec` with the required parameters.
2. Save your changes.

Configuring the RSA SecurID authentication method

Navigate to the RSA SecurID authentication method to define the file names of the `sdconf.rec` file, node secret, and optional `sdopts.rec` files, and the initial trace level.

About this task

To configure the RSA SecurID authentication method, complete the following steps:

Procedure

1. In the IBM MFA GUI, select the **Authentication Methods** tab.
2. Click on the **RSA SecurID** method.
3. Choose the initial trace level. Move the slider to increase the tracing level. Valid values are 0 - 3, where the higher number increases the level of verbosity. The default value is zero.
4. Enter the following file names:
   - The location of the `sdconf.rec` file.
   - The location of the file that will contain the node secret. This file is created by IBM MFA.
   - Optionally, the location of the `sdopts.rec` file.
5. Verify the changes and click **Save**.
6. Restart the IBM MFA daemon, as described in "Restarting the IBM MFA server" on page 17.

Clear the node secret (if needed)

The RSA node secret is a shared secret known to IBM MFA and the RSA Authentication Manager. If this secret must be established (or re-established), your RSA Authentication Manager administrator will request that the node secret be cleared from the IBM MFA server.

Procedure

1. In the IBM MFA GUI, select the **Authentication Methods** tab.
2. Click on the **RSA SecurID** method.
3. Click **Clear Node Secret**.
4. The RSA Authentication Manager generates a new node secret on the first successful logon.

Configuring the IBM MFA for PIV/CAC or X.509 Certificate authentication method

If you want to use certificate authentication, you must first create the server truststore so that the server trusts the client certificates.

The server truststore is a single file that contains the client issuing certificate chain.

Creating the server truststore

If you want to use certificate authentication, you must create the server truststore so that the server trusts the client certificates. You do not need to create the server truststore for any other authentication method. The server truststore of trusted Certificate Authority (CA) certificates is a single file in the `/etc/security/mfa/certificates` directory that contains the client PIV/CAC card issuing certificate chain in Privacy Enhanced Mail (PEM) format.

About this task

The client certificate issuing chain, including any intermediate certificates and the root CA, must be in PEM format.

Note: The procedure to obtain the certificate chain of the PIV/CAC card varies by the vendor and application.

To create the truststore, complete the following steps:

Procedure

1. If the certificates are not already in the PEM format, convert them. For example, if the certificates are currently in the Distinguished Encoding Rules (DER) format, you can use the **`openssl x509`** command to convert them. The following example converts one intermediary certificate and the root CA certificate.

   ```
   openssl x509 -in inter_key.cer -inform der -outform pem -out inter_key.pem
   openssl x509 -in ca_key.cer -inform der -outform pem -out ca_key.pem
   ```

2. Concatenate the certificate `.pem` files into a single file.

   ```
   cat inter_key.pem > client.pem
   cat ca_key.pem >> client.pem
   ```

3. Use the secure copy (**scp**) command to copy the resulting file to the `/etc/security/mfa/certificates` directory in the IBM MFA server system.
4. Specify the location of the file in the **`Trust Store Path`** field of the IBM MFA server configuration, as described in Chapter 5, “Configuring server options,” on page 23.
5. Optionally, edit the server configuration input file you created in “Completing the server setup” on page 12 to include the server truststore.

```
# initial trace level for MFA server
INITIAL TRACE LEVEL=0

# location of the P12 identity certificate for the server
P12 LOCATION=/etc/security/mfa/certificates/secsrv.p12


# PKCS11 token used while encrypting P12 password
PKCS11 TOKEN NAME=azf

# directory or PEM file containing CAs that will be trusted by the server
# CAS LOCATION=/etc/security/mfa/certificates/client.pem


# port to use for server authentication
SERVER AUTH PORT=6793

# port to use for mutual authentication
MUTUAL AUTH PORT=6794

# port to use for ZVM Host communications
ZVM PORT=6787
```

where:

- `<CAS LOCATION>` is the truststore (`client.`pem in the example) you created.

6. After you set the **`Trust Store Path`** field of the IBM MFA server configuration, you need to stop and restart the IBM MFA daemon. However, you will probably find it more convenient to first configure the certificate authentication method as described in "Configuring IBM MFA for PIV/CAC or X.509 Certificate authentication" on page 30 and then restart the IBM MFA server.

Configuring IBM MFA for PIV/CAC or X.509 Certificate authentication

You must configure the certificate settings to use this authentication method.

About this task

You can optionally configure the settings to notify an administrator by email when a user enrolls a certificate.

To configure the IBM MFA for PIV/CAC or X.509 Certificate authentication method, complete the following steps:

Procedure

1. In the IBM MFA GUI, select the **Authentication Methods** tab.
2. Click on the **IBM MFA for PIV/CAC or X.509 Certificate** method.
3. Use the following table to specify the **IBM MFA for PIV/CAC or X.509 Certificate** authentication method:

Table 4. IBM MFA for PIV/CAC or X.509 Certificate Authentication Method

Setting	Description
Initial Trace Level	The trace level used for tracing events within the plug-in. Valid values are 0 - 3, where the higher number increases the level of verbosity. The default value is zero.

Table 4. IBM MFA for PIV/CAC or X.509 Certificate Authentication Method (continued)

Setting	Description
Require Exact Certificate	The possible settings are on and off. By default, the client certificate must match the Subject DN and Issuer DN of the root CA certificate and a hash is created. This parameter addresses the scenario where the user gets a new certificate and the hash does not match. If set to On, the user certificate must match the hash, the Subject DN, and Issuer DN of the root CA certificate.
SMTP Server Address	Enter the host name or IP address of the Simple Mail Transfer Protocol (SMTP) server for outbound email.
SMTP Server Port	Enter the port number of the SMTP server.
SMTP Login User Id	Enter the user ID you want to use to log in to the SMTP server.
SMTP Login Password	Enter the password for the user ID you want to use to log in to the SMTP server.
Recipient Email Address	Enter the email address to be notified when a user enrolls a certificate.
Email Reply-to Address	Enter the email address used to send the email notification.

4. Click **Save**.
5. Select the **Settings** > **Server Options**.
6. Set the **Enable certificate services** control.
7. Restart the IBM MFA daemon, as described in "Restarting the IBM MFA server" on page 17.

Enabling OCSP validation

Online Certificate Status Protocol (OCSP) tests whether a certificate has been revoked since it was issued. You can enable OCSP validation to test the certificates used for IBM MFA IBM MFA for PIV/CAC or X.509 Certificate authentication. When OCSP validation is enabled, OCSP validation is performed as an additional security measure, after other certificate validation steps are performed. OCSP validation is attempted only for certificates that have passed the other validation steps.

Before you begin

If you want to use OCSP validation, you must create the OCSP truststore in Privacy Enhanced Mail (PEM) format. The certificates in the OCSP truststore must be a single-file concatenation of:

- The direct issuing certificate in the chain (not necessarily the Root CA) for each certificate you want to check via OCSP.
- The root CA for each OCSP response you expect to receive. This is typically the same as the root CA for the certificate, but is not technically required to be the same.

Important: You may find that the server truststore you created in "Creating the server truststore" on page 29 satisfies all the requirements of the OCSP truststore. In this case, you can simply specify the location of the server truststore as the location of the OCSP truststore.

About this task

The responder URI provides timely information regarding the revocation status of certificates. There are two ways to specify which responder URI to use:

- You embed (or they already exist) one or more OCSP responder URIs in the certificates to be used for client authentication. The specific steps required to use this method are dependent on the process and products you use to issue client certificates in your organization.

  You can use the **openssl** command to view the OCSP information for the certificate. For example:

  ```
  openssl x509 -in your-cert.pem -text
  :
  Authority Information Access:
            OCSP - URI:http://some-url
  ```

- You can specify the responder URI in the **Default Responder URI** field. The **Default Responder URI** setting is used only if the certificate does not contain any responder URIs.

Handling the OCSP response

By default, IBM MFA assumes that the certificate is valid unless the responder URI returns an explicit revoked status. Any other status fails "open" and the certificate is accepted.

Important: You can change the default fail open status by enabling the **Deny Access on Any OCSP Error** control. You should not enable this control unless you are aware of the possible reasons for OCSP errors and accept the ramifications of denying access based on these errors.

For example, if the IBM MFA server does not have network connectivity to the responder URI, the default status fails "open" and the certificate is accepted. If you set an elevated trace level, the following message is printed to the IBM MFA server log file:

```

(A remote host refused an attempted connect operation.)
AZFCERT1:OCSP: Failed to init http session for
    Responder URI: http://some-uri
```

As another example, if OCSP is enabled, but the certificate does not contain one or more responder URIs and if you have not configured a default responder URI, by default the certificate is accepted. If you set an elevated trace level, the following message is printed to the IBM MFA server log file:

```
AZFCERT1:OCSP: No embedded or default Responder URI; granting access
```

Enabling OCSP validation

To enable OCSP validation, complete the following steps. You do not need to complete Steps 1-4 if the server truststore you created in “Creating the server truststore” on page 29 satisfies all the requirements of the OCSP truststore.

Procedure

1. Obtain the certificate chain of the user's certificate. The procedure to obtain the certificate chain of the user's certificate varies by the vendor and application.
2. If the certificates are not already in the PEM format, convert them. For example, if the certificates are currently in the Distinguished Encoding Rules (DER) format, you can use the **openssl x509** command to convert them. The following example converts one intermediary certificate and the root CA certificate.

   ```
   openssl x509 -in inter_key.cer -inform der -outform pem -out inter_key.pem
   openssl x509 -in ca_key.cer -inform der -outform pem -out ca_key.pem
   ```

3. Concatenate the certificate `.pem` files into a single file.

   ```
   cat inter_key.pem > ocspTrustStore.pem
   cat ca_key.pem >> ocspTrustStore.pem
   ```

4. If needed, use the secure copy (**scp**) command to copy the resulting file to the IBM MFA server system.
5. Specify the location of the file in the **Trust Store Path** field of the IBM MFA for PIV/CAC or X.509 Certificate configuration.
6. Restart the IBM MFA server, as described in "Restarting the IBM MFA server" on page 17.

Configuring the TOTP authentication method

You must configure the TOTP settings to use this authentication method.

About this task

You can use generic TOTP as an alternative to the IBM TouchToken for iOS app. Generic TOTP supports common Quick Response (QR) codes on both Android and Apple iOS devices. Generic TOTP uses the TOTP authentication method, but the procedure to provision the user is different.

To configure the TOTP authentication method, complete the following steps:

Procedure

1. In the IBM MFA GUI, click the **Authentication Methods** tab.
2. Click the **TOTP** authentication method.
3. Use the following table to specify an TOTP authentication method:

Table 5. TOTP Factor Attributes

Setting	Description
Consecutive Failures Before TOTP Suspension	Limits the number of times a user consecutively fails to provide a valid TOTP code. Valid values are 0 through 255. A value of 0 indicates that revoke count protection is not enabled for the TOTP authentication method. Any numeric value greater than zero is treated as the number of times a user may consecutively fail to provide a valid TOTP code. If a user fails exactly this number of times and then provides a valid TOTP code: • Authentication succeeds. • Their failure count is reset to zero. If the user fails more than this number of times: • Authentication fails. • Their suspension status is set to YES. • Their failure count is reset to zero.
Initial Trace Level	The trace level used for tracing events within the TOTP authentication method. Valid values are 0 through 3, in which the higher indicates an increased the level of verbosity.
Web Services Trace Level	The initial trace level for TOTP web services. Valid values are 0 through 3, where the higher number increases the level of verbosity. The default is zero.

Table 5. TOTP Factor Attributes (continued)

Setting	Description
Realm Name	Enter the realm name for your web services server. You can choose the name. This setting is used in combination with the user ID to generate a default label for a user's TOTP account. The generated label takes the form `<user ID>@<Realm Name>`. For example, a user with user ID "user1" provisioned with a TOTP account using the realm name of "myrealm" would receive the default TOTP account label of "user1@myrealm".
Digest Algorithm	Choose the default digest algorithm. TOTP uses the digest algorithm, the shared secret key, and the current time to generate the TOTP value. Possible values are SHA1 (generic TOTP only), SHA256, SHA384, and SHA512. The default value is SHA256.
Token Digits	Choose the number of digits in the generated token. Possible values are 6, 7, and 8. The default value is 8.
Authentication Window	Enter the skew intervals of the algorithm. The skew interval accommodates any possible synchronization delay between the server and the client that generates the one-time password. For example, a skew interval of 2 means that a one-time password generated in up to two intervals in the past, or two intervals in the future, are also valid. Therefore, if it is interval 563, and intervals are 30 seconds, then one-time passwords for intervals 561- 565 are computed and checked within a range of 2.5 minutes. The maximum value is 10.
Token Period Seconds	Choose the time (in seconds) between changes in the token value. This number determines how long a one-time password is active before the next one-time password is generated. Possible values are 15, 30, and 60. The default value is 30 seconds.

4. Click **Save**.
5. Select the **Settings** > **Server Options**.
6. Set the **Enable TOTP services** control.
7. Restart the IBM MFA daemon, as described in "Restarting the IBM MFA server" on page 17.

Configuring the IBM MFA for generic RADIUS authentication method

You must configure the IBM MFA for generic RADIUS settings to use this authentication method.

Before you begin

The IBM MFA for generic RADIUS authentication method requires network access to a RADIUS server configuration that is functioning properly. You must have already configured communication between the RADIUS server and the system that is running the IBM MFA server, created accounts for the users in the RADIUS server, and assigned tokens. For more information, see your RADIUS server documentation

About this task

Note: If you are using the SafeNet RADIUS server, as a general rule, you should use IBM MFA for SafeNet RADIUS, as described in "Configuring the IBM MFA for SafeNet RADIUS authentication method" on page 37.

To configure the IBM MFA for generic RADIUS authentication method, complete the following steps:

Procedure

1. In the IBM MFA GUI, click the **Authentication Methods** tab.
2. Select the **IBM MFA for generic RADIUS** method.
3. Use the following table to specify an IBM MFA for generic RADIUS authentication method:

Table 6. IBM MFA for generic RADIUS Authentication Method Attributes

Setting	**Allowed Values**	**Description**
Initial Trace Level	0 through 3	Choose the initial trace level. Valid values are 0 through 3, where the higher value indicates a higher level of verbosity. The default value is 0.
RADIUS Primary Server	Valid host name or IP address	Enter the host name or IP address for the primary RADIUS server. The host name must be sufficiently qualified for web clients to resolve the host name. This attribute must be set.
RADIUS Primary Server Port	Valid port number	The port number of the primary RADIUS server. The default value is 1812.
RADIUS Secondary Server	Valid host name or IP address	Enter the host name or IP address for the secondary RADIUS server, if applicable. This value is required only if you have multiple servers. The host name must be sufficiently qualified for web clients to resolve the host name.
RADIUS Secondary Server Port	Valid port number	The port number of the secondary RADIUS server, if applicable. This value is required only if you have multiple servers.

Table 6. IBM MFA for generic RADIUS Authentication Method Attributes (continued)

Setting	Allowed Values	Description
RADIUS Tertiary Server	Valid host name or IP address	Enter the host name or IP address for the tertiary RADIUS server, if applicable. This value is required only if you have multiple servers. The host name must be sufficiently qualified for web clients to resolve the host name.
RADIUS Tertiary Server Port	Valid port number	The port number of the tertiary RADIUS server, if applicable. This value is required only if you have multiple servers.
RADIUS Shared Secret	Actual shared secret	The shared secret (case-sensitive password) that is used by the RADIUS server to recognize the IBM MFA RADIUS client. The RADIUS client uses the same shared secret while communicating with the RADIUS primary server or RADIUS replica servers.
Receive Timeout	Number of seconds, from 1 through 30	The time duration for which the connection between IBM MFA and the RADIUS server can remain inactive before the session is timed out. The default value is 10 seconds.
Retry Count	Integer, from 1 through 15	The number of times IBM MFA attempts to contact the RADIUS server if the connection becomes inactive.
PKCS#11 Key Label	Actual PKCS#11 key label	The name of the Key Label that is used to encrypt the shared secret. The PKCS#11 key label has a limit of 32 characters. **Note:** If you change the PKCS#11 key label, you must also re-enter the existing shared secret.

4. Click **Save**.
5. Restart the IBM MFA daemon, as described in "Restarting the IBM MFA server" on page 17.
6. Ensure that the RADIUS server accepts communication from the system that is running the IBM MFA server. See your RADIUS documentation for configuration information.

Configuring the IBM MFA for SafeNet RADIUS authentication method

You must configure the IBM MFA for SafeNet RADIUS settings to use the IBM MFA for SafeNet RADIUS authentication method.

Before you begin

The IBM MFA for SafeNet RADIUS authentication method requires network access to a RADIUS server configuration that is functioning properly. You must have already configured communication between the RADIUS server and the system that is running the IBM MFA server, created accounts for the users in the RADIUS server, and assigned tokens. For more information, see your RADIUS server documentation

About this task

To configure the IBM MFA for SafeNet RADIUS authentication method, complete the following steps:

Procedure

1. In the IBM MFA GUI, click the **Authentication Methods** tab.
2. Select the **IBM MFA for SafeNet RADIUS** method.
3. Use the following table to specify an IBM MFA for SafeNet RADIUS authentication method:

Table 7. IBM MFA for SafeNet RADIUS Authentication Method Attributes

Setting	**Allowed Values**	**Description**
Initial Trace Level	0 through 3	Choose the initial trace level. Valid values are 0 through 3, where the higher value indicates a higher level of verbosity. The default value is 0.
RADIUS Primary Server	Valid host name or IP address	Enter the host name or IP address for the primary RADIUS server. The host name must be sufficiently qualified for web clients to resolve the host name. This attribute must be set.
RADIUS Primary Server Port	Valid port number	The port number of the primary RADIUS server. The default value is 1812.
RADIUS Secondary Server	Valid host name or IP address	Enter the host name or IP address for the secondary RADIUS server, if applicable. This value is required only if you have multiple servers. The host name must be sufficiently qualified for web clients to resolve the host name.
RADIUS Secondary Server Port	Valid port number	The port number of the secondary RADIUS server, if applicable. This value is required only if you have multiple servers.

Table 7. IBM MFA for SafeNet RADIUS Authentication Method Attributes (continued)

Setting	Allowed Values	Description
RADIUS Tertiary Server	Valid host name or IP address	Enter the host name or IP address for the tertiary RADIUS server, if applicable. This value is required only if you have multiple servers. The host name must be sufficiently qualified for web clients to resolve the host name.
RADIUS Tertiary Server Port	Valid port number	The port number of the tertiary RADIUS server, if applicable. This value is required only if you have multiple servers.
RADIUS Shared Secret	Actual shared secret	The shared secret (case-sensitive password) that is used by the RADIUS server to recognize the IBM MFA RADIUS client. The RADIUS client uses the same shared secret while communicating with the RADIUS primary server or RADIUS replica servers.
Receive Timeout	Number of seconds, from 1 through 30	The time duration for which the connection between IBM MFA and the RADIUS server can remain inactive before the session is timed out. The default value is 10 seconds.
Retry Count	Integer, from 1 through 15	The number of times IBM MFA attempts to contact the RADIUS server if the connection becomes inactive.
PKCS#11 Key Label	Actual PKCS#11 key label	The name of the Key Label that is used to encrypt the shared secret. The PKCS#11 key label has a limit of 32 characters. **Note:** If you change the PKCS#11 key label, you must also re-enter the existing shared secret.

4. Click **Save**.
5. Restart the IBM MFA daemon, as described in "Restarting the IBM MFA server" on page 17.
6. Ensure that the RADIUS server accepts communication from the system that is running the IBM MFA server. See your RADIUS documentation for configuration information.

Configuring the RSA SecurID RADIUS authentication method

You must configure the RSA SecurID RADIUS settings to use this authentication method.

Before you begin

The RSA SecurID RADIUS authentication method requires network access to a RADIUS server configuration that is functioning properly. You must have already configured communication between the RADIUS server and the system that is running the IBM MFA server, created accounts for the users in the RADIUS server, and assigned tokens. For more information, see your RADIUS server documentation

About this task

To configure the RSA SecurID RADIUS authentication method, complete the following steps:

Procedure

1. In the IBM MFA GUI, click the **Authentication Methods** tab.
2. Select the **RSA SecurID RADIUS** method.
3. Use the following table to specify the RSA SecurID RADIUS authentication method:

Table 8. RSA SecurID RADIUS Authentication Method Attributes

Setting	Allowed Values	Description
Initial Trace Level	0 through 3	Choose the initial trace level. Valid values are 0 through 3, where the higher value indicates a higher level of verbosity. The default value is 0.
RADIUS Primary Server	Valid host name or IP address	Enter the host name or IP address for the primary RADIUS server. The host name must be sufficiently qualified for web clients to resolve the host name. This attribute must be set.
RADIUS Primary Server Port	Valid port number	The port number of the primary RADIUS server. The default value is 1812.
RADIUS Secondary Server	Valid host name or IP address	Enter the host name or IP address for the secondary RADIUS server, if applicable. This value is required only if you have multiple servers. The host name must be sufficiently qualified for web clients to resolve the host name.
RADIUS Secondary Server Port	Valid port number	The port number of the secondary RADIUS server, if applicable. This value is required only if you have multiple servers.
RADIUS Tertiary Server	Valid host name or IP address	Enter the host name or IP address for the tertiary RADIUS server, if applicable. This value is required only if you have multiple servers. The host name must be sufficiently qualified for web clients to resolve the host name.
RADIUS Tertiary Server Port	Valid port number	The port number of the tertiary RADIUS server, if applicable. This value is required only if you have multiple servers.

Table 8. RSA SecurID RADIUS Authentication Method Attributes (continued)

Setting	Allowed Values	Description
RADIUS Shared Secret	Actual shared secret	The shared secret (case-sensitive password) that is used by the RADIUS server to recognize the IBM MFA RADIUS client. The RADIUS client uses the same shared secret while communicating with the RADIUS primary server or RADIUS replica servers.
Receive Timeout	Number of seconds, from 1 through 30	The time duration for which the connection between IBM MFA and the RADIUS server can remain inactive before the session is timed out. The default value is 10 seconds.
Retry Count	Integer, from 1 through 15	The number of times IBM MFA attempts to contact the RADIUS server if the connection becomes inactive.
PKCS#11 Key Label	Actual PKCS#11 key label	The name of the Key Label that is used to encrypt the shared secret. The PKCS#11 key label has a limit of 32 characters. **Note:** If you change the PKCS#11 key label, you must also re-enter the existing shared secret.

4. Click **Save**.
5. Restart the IBM MFA daemon, as described in "Restarting the IBM MFA server" on page 17.
6. Ensure that the RADIUS server accepts communication from the system that is running the IBM MFA server. See your RADIUS documentation for configuration information.

Configuring IBM MFA for Yubico OTP authentication

You must configure the IBM MFA for Yubico OTP settings to use this authentication method.

About this task

To configure the IBM MFA for Yubico OTP authentication method, complete the following steps:

Procedure

1. In the IBM MFA GUI, click the **Authentication Methods** tab.
2. Select the **IBM MFA for Yubico OTP** authentication method.
3. Use the following table to specify the IBM MFA for Yubico OTP authentication method:

Table 9. IBM MFA for Yubico OTP Authentication Method Attributes

Setting	Allowed Values	Description
Initial Trace Level	0 through 3	Choose the initial trace level. Valid values are 0 through 3, where the higher value indicates a higher level of verbosity. The default value is 0.

Table 9. IBM MFA for Yubico OTP Authentication Method Attributes (continued)

Setting	Allowed Values	Description
PKCS#11 Key Label	Actual PKCS#11 key label	The name of the Key Label that is used to encrypt the shared secret. The PKCS#11 key label has a limit of 32 characters.

4. Click **Save**.
5. Restart the IBM MFA daemon, as described in "Restarting the IBM MFA server" on page 17.

Configuring IBM MFA for LDAP Simple Bind authentication

You must configure the IBM MFA for LDAP Simple Bind settings to use this authentication method.

About this task

To configure the IBM MFA for LDAP Simple Bind authentication method, complete the following steps:

Procedure

1. In the IBM MFA GUI, click the **Authentication Methods** tab.
2. Select the **IBM MFA for LDAP Simple Bind** authentication method.
3. Use the following table to specify the IBM MFA for LDAP Simple Bind authentication method:

Table 10. IBM MFA for LDAP Simple Bind Authentication Method Attributes

Setting	Allowed Values	Description
Initial Trace Level	0 through 3	The trace level used for tracing events. Valid values are 0 through 3, where the higher number increases the level of verbosity. The default is zero.
LDAP Primary Server	Valid host name or IP address	The hostname (or IP address) of the primary LDAP server. The hostname must be sufficiently qualified for web clients to resolve the hostname.
LDAP Primary Server Port	Valid port number	The port number used on the primary LDAP server for authentication. Default: 636.
LDAP Secondary Server	Valid host name or IP address	The hostname (or IP address) of the secondary LDAP server. This is required only if you have multiple servers. The default is blank. The hostname must be sufficiently qualified for web clients to resolve the hostname.

Table 10. IBM MFA for LDAP Simple Bind Authentication Method Attributes (continued)

Setting	Allowed Values	Description
LDAP Secondary Server Port	Valid port number	The port number used on the secondary LDAP server for authentication. This is required only if you have multiple servers. The default is 0.
LDAP Tertiary Server	Valid host name or IP address	The hostname (or IP address) of the tertiary LDAP server. This is required only if you have multiple servers. The default is blank. The hostname must be sufficiently qualified for web clients to resolve the hostname.
LDAP Tertiary Server Port	Valid port number	The port number used on the secondary LDAP server for authentication. This is required only if you have multiple servers. The default is 0.
Receive Timeout	Number of seconds, from 1 through 30	The number of seconds a server is allowed to take before a retry will occur if there is no response. The default is 3 seconds.
Trusted CAs Path	Valid path name	The location of the PEM file containing the LDAP server CAs that will be trusted by the server.

4. Click **Save**.
5. Restart the IBM MFA daemon, as described in "Restarting the IBM MFA server" on page 17.

Configuring IBM MFA for IBM Security Access Manager authentication

You must configure the IBM MFA for IBM Security Access Manager settings to use this authentication method.

Before you begin

- If you have not already installed the IBM Security AppX Installer, navigate to https://exchange.xforce.ibmcloud.com/hub/extension/ad8f86525d3a9c1186c1bce524edc9c3 in a browser and download and install it. Log in with an IBM ID if you have not already done so.

  The IBM Security AppX Installer enables configuration of your IBM Security Access Manager appliance for use with partner applications published on the IBM Security App Exchange.
- Navigate to IBM Security Verify Access Extension for Multi-factor Authentication API in a browser. Log in with an IBM ID if you have not already done so.

  Follow the provided links on the page to download the software and review the documentation.

  Pay close attention to the documented **`Oauth`** configuration parameters for running the installer script. These parameters begin with the prefix `--oauth` (for example `--oauthproxy`) and they define the back channel interface that is used by IBM MFA to perform OTP authentication.

- Ensure that `backchannelcomplete.json` complies with the following syntax:

  ```
  {"username":"@USERNAME@","status":"success"}
  ```

  The following syntax is also valid. (The example is wrapped for format requirements.)

  ```
  {"username":"@USERNAME@","authenticationMechanismTypes":"@AUTHNMECHTYPES@",
  "status":"success"}
  ```

- Obtain the root CA public certificate of the IBM Security Access Manager server in .pem format.

About this task

To configure the IBM MFA for IBM Security Access Manager authentication method, complete the following steps:

Procedure

1. Log in to the IBM MFA for IBM Security Access Manager local management interface (LMI).
2. Navigate to **Secure Access Control** > **Global Settings** > **Template Files** > **C** > **authsvc** > **authenticator** > **apimfa** > **browser.html**.
3. Configure the authentication context in the `browser.html` file:

   ```
   <td>
         <select name="authnctx">
         <option value="server-auth-ctx">Arbitrary text that describes your server</option>
         </select>
       </td>
   ```

   where *server-auth-ctx* must match that of the **`Authentication Context`** on the IBM MFA server.
4. A pending change message is displayed at the top of the main pane. Click **Click here** to review the changes or apply them to the system.
5. In the Deploy Pending Changes page:
   a) To view the details of changes that are made to a particular module, click the link to that module.
   b) To deploy the changes, click **Deploy**.
   c) To abandon the changes, click **Roll Back**.
   d) To close the pop-up page without any actions against the changes, click **Cancel**.
6. In the IBM MFA GUI, click the **Authentication Methods** tab.
7. Select the **IBM MFA for IBM Security Access Manager** authentication method.
8. Use the following table to specify the IBM MFA for IBM Security Access Manager authentication method:

Table 11. IBM MFA for IBM Security Access Manager Authentication Method Attributes

Setting	Allowed Values	Description
Initial Trace Level	0 through 3	Choose the initial trace level. Valid values are 0 through 3, where the higher value indicates a higher level of verbosity. The default value is 0.
Key Label	Actual PKCS#11 key label	The name of the Key Label that is used to encrypt the client secret. The PKCS#11 key label has a limit of 32 characters.
Client ID	Actual client ID	User ID that is used to obtain an access or bearer token.
Client Secret	Actual value	Password for Client ID.

Table 11. IBM MFA for IBM Security Access Manager Authentication Method Attributes (continued)

Setting	Allowed Values	Description
Authentication Context	Default application context	Enables specific OTP generations for an authentication context. Must match that of the IBM MFA for IBM Security Access Manager server unless the application context is included as a user tag.
Access Token URL	URL	The URL to which to send the client ID and secret to obtain the access or bearer token.
One-Time Passcode Validation URL	URL	URL to which to send user authentication requests.
Trusted CA Path	Valid file specification	The file specification of the root CA public certificate of the IBM Security Access Manager server in .pem format.
Timeout	Number of seconds, from 1 through 30	The amount of time the connection can remain inactive before the session is timed out.

9. Click **Save**.
10. Restart the IBM MFA daemon, as described in "Restarting the IBM MFA server" on page 17.

Configuring the PAM authentication method

You can configure IBM MFA for password authentication to the IBM MFA server system. You must configure the PAM authentication settings to use this authentication method.

About this task

Important: The authentication is performed against the user's IBM MFA-specific password.

Password authentication is a weak authentication method and cannot be used alone. You must use it in combination with another authentication method.

To configure the Password authentication method, complete the following steps:

Procedure

1. In the IBM MFA GUI, click the **Authentication Methods** tab.
2. Select the **PAM Authentication** method.
3. Use the following table to specify a PAM authentication method:

Table 12. PAM Authentication Method Attributes

Setting	Allowed Values	Description
Initial Trace Level	0 through 3	Choose the initial trace level. Valid values are 0 through 3, where the higher value indicates a higher level of verbosity. The default value is 0.

4. Click **Save**.
5. Stop and restart the IBM MFA daemon, as described in "Restarting the IBM MFA server" on page 17.

Chapter 7. Configuring IBM MFA policies

You must associate a policy with a user to apply one or more authentication methods to that user.

The **Policy Definitions** tab displays the configured policy definitions.

Creating IBM MFA policies

To use IBM MFA, you must create authentication policies.

About this task

To create authentication policies, complete the following steps:

Procedure

1. In the IBM MFA GUI, click the **Policy Definitions** tab.
2. Click **+** to add a new policy.

   The new policy settings page is displayed.
3. Enter a description for the policy.
4. Enter a descriptive name for the policy.
5. Enter the CTC timeout for the policy, which is the number of seconds for which the associated cache token credential is valid before it times out.
6. Set the **CTC Reuse** control if you want the cache token credential to be re-usable during the token timeout period.
7. Click **+** to add authentication methods to the policy.

   The available methods pop-up is displayed.
8. Select the authentication methods you want to associate with this policy.
9. Click **OK**.
10. Click **Save**.

Displaying IBM MFA policies

You can display the existing IBM MFA policies.

About this task

To display the existing IBM MFA policies, complete the following steps:

Procedure

1. Open the IBM MFA GUI. The IBM MFA GUI displays the main page.
2. Select the **Policy Definitions** tab.

   The **Policy Definitions** tab displays the currently available policies with the following policy attributes:

   - The policy name.
   - The methods that are applied to the policy.
   - The duration for which the associated cache token credential is valid before it times out.
   - Whether the cache token credential is reusable.

Associating IBM MFA policies with authentication methods

You must associate an IBM MFA policy with one or more authentication methods.

About this task

To associate an IBM MFA policy with one or more authentication methods, complete the following steps:

Procedure

1. In the IBM MFA GUI, click the **Policy Definitions** tab.
2. Select an existing policy.

   The policy settings page is displayed.
3. Click **trash** to remove an existing method from the policy.
4. Click **+** to add a method to the policy.

   The available authentication methods pop-up is displayed.
5. Select the authentication methods you want to associate with this policy.
6. Click **OK**.
7. Click **Save**.

Setting policy token timeout

The policy token timeout is the number of seconds for which the associated cache token credential is valid before it times out.

About this task

To set the policy token timeout, complete the following steps:

Procedure

1. In the IBM MFA GUI, click the **Policy Definitions** tab.
2. Select an existing policy.

   The policies setting page is displayed.
3. Enter the token timeout value for the policy, in seconds.
4. Click **Save**.

Setting the cache token credential to be reusable

You can set the cache token credential to be reusable within the token timeout period. Setting the cache token credential to be reusable allows you to use the cache token credential in cases where the application replays the user password. If the authentication policy specifies that the cache token credential is reusable, it is usable until the first time the cache is cleared after it expires.

About this task

To set the cache token credential to be reusable, complete the following steps:

Procedure

1. In the IBM MFA GUI, click the **Policy Definitions** tab.
2. Select an existing policy.

   The policies setting page is displayed.
3. Set the **Re-usable** control for the policy.

4. Click **Save**.

Deleting IBM MFA policies

You can delete an existing IBM MFA policy, whether or not users are associated with the IBM MFA policy.

About this task

To delete one or more existing policies, complete the following steps:

Procedure

1. In the IBM MFA GUI, click the **Policy Definitions** tab.
2. Select one or more existing IBM MFA policies.
3. Click **trash** to delete the selected IBM MFA policies.
4. Click **Save**.

Chapter 8. Provisioning IBM MFA users

You must provision users for IBM MFA. Although you can use the IBM MFA GUI for this purpose, the bulk provisioning feature is faster and more efficient than the GUI if you have a large number of users.

The **User Provisioning** tab displays the provisioned users.

Using keyboard navigation

In the **User Provisioning** tab, the following keyboard navigation options are available:

- The Enter key selects a user row.
- Ctrl+Enter opens the selected user's information page.
- The Delete key deletes a user row.

Provisioning users in bulk for IBM MFA

IBM MFA provides programs and shell scripts that you can use to provision users with policies and authentication methods for IBM MFA.

About this task

The user names you provision must match the user names associated with the effective client user ID. For example, if you provision user *USERA*, *USERA* must exist on the IBM MFA client system.

IBM MFA includes the following program:

- The **azfbulk** program reads the user-created text file to provision users and optionally add them to the repository. The **azfbulk** program reads the contents of the text file, and generates two shell scripts that you then run to provision the users.

  The **azfbulk** parameters are shown in Table 13 on page 50.

  The parameter usage is as follows:

  ```
  azfbulk input-file (COMMIT)
  ```

Table 13. ***azfbulk*** *Parameters*

Parameter	Description
input-file	A user-created text file of user names, policies, authentication methods, and authentication method-specific parameters. The format of this file must be as follows: • Each entry starts on a new line. • Each field is separated by a space. • The only validation performed is on the authentication method name. All other entries are assumed to be valid. The fields are as follows: • **userID**. This is required. • **policy name**. This is required. The **policy name** field must be the name of an existing policy. **policy name** is case sensitive. • **authentication method**. This is required. **authentication method** is case sensitive. • **ADD**. Adds the user ID to the repository. This is optional and is not needed if you have already added the user ID to the repository. You can further enhance the **ADD** parameter with **USERNAME**=*user name* parameter to add the user's full name to the repository. • Any authentication method-specific parameters shown in Table 14 on page 50.
COMMIT	Commits the changes. You can run the **azfbulk** program with or without the **COMMIT** parameter. It is recommended that you run the **azfabulk** program the first time without the **COMMIT** parameter and then examine the output shell scripts. If the output shell scripts are correct, run the **azfbulk** program a second time and specify the **COMMIT** parameter.

Table 14 on page 50 describes the authentication method-specific parameters.

Table 14. Authentication-Method-Specific Parameters

Authentication Method	Parameters
IBM MFA for PIV/CAC or X.509 Certificate (AZFCERT1)	The file specification of the user certificate. The **azfbulk** program performs the certificate enrollment and approval process on your behalf.
RSA SecurID (AZFSIDP1) and SecurID RADIUS (AZFSIDR1)	The associated RSA user ID.
Generic RADIUS (AZFRADP1) and SafeNet RADIUS (AZFSFNP1)	The RADIUS user ID.
TOTP (AZFTOTP1)	Does not accept any parameters. The user registration state is set to OPEN.

Table 14. Authentication-Method-Specific Parameters (continued)

Authentication Method	**Parameters**
PAM Authentication (AZFPASS1)	Does not accept any parameters.
IBM MFA for Yubico OTP (AZFYUBI1)	The complete string from the `.csv` file enclosed in quotation marks.
IBM MFA for LDAP Simple Bind (AZFLDAP1)	The user DN enclosed in quotation marks.
IBM MFA for IBM Security Access Manager (AZFISAM1)	The user ID and the authentication context.

An example of the input file follows:

```
usera   CERTONLY AZFCERT1  /u/usera/certificates/useracert.cer
userb   SIDPONLY AZFSIDP1 ADD USERNAME=userb rsauserb
userc   SIDPONLY  AZFSIDP1  rsauserc
```

The **azfbulk** program creates two shell scripts, `azfprov1.sh` and `azfprov2.sh` from the input file:

- `azfprov1.sh` associates the users with the policies and authentication methods.
- `azfprov2.sh` calls factor-specific utility programs to set the user factor data. `azfprov2.sh` commits the changes.

To provision users in bulk, complete the following steps:

Procedure

1. Add the `/opt/IBM/MFA/bin` directory to your PATH.

   ```
   export PATH=/opt/IBM/MFA/bin:${PATH}
   ```

2. Create your input file.
3. Run the **azfbulk** program without the **COMMIT** parameter.

   ```
   ./azfbulk input-file
   ```

4. Check the resulting `azfprov1.sh` and `azfprov2.sh` files.
5. Correct any errors in your input file and re-run the **azfbulk** command.
6. Run the **azfbulk** program with the **COMMIT** parameter.

   ```
   ./azfbulk input-file COMMIT
   ```

7. Run the `azfprov1.sh` shell script.

   ```
   sh azfprov1.sh
   ```

8. Run the `azfprov2.sh` shell script.

   ```
   sh azfprov2.sh
   ```

9. Verify the provisioned users in the IBM MFA GUI.

Enabling users for IBM MFA

You must enable existing users with the IBM MFA policies that you require. Although you can use the IBM MFA GUI for this purpose, the bulk provisioning feature can be used if you have a large number of users.

Enabling users for RSA SecurID authentication

To enable a user for RSA SecurID authentication you need the user's RSA user ID.

About this task

To enable users for RSA SecurID authentication, complete the following steps:

Procedure

1. In the IBM MFA GUI, click the **User Provisioning** tab.
2. Click the plus sign (**+**) control.
3. Enter the ID for the user. The ID is the user name associated with the effective client user ID. IBM MFA automatically saves the user ID in lowercase.
4. Enter the Name for the user. This is a name of your choice.
5. Enter an MFA password of your choice, if applicable. The MFA password is a special password that allows the user to log in to the IBM MFA server for IBM MFA-specific actions. This password is unique to the IBM MFA server.

   Note: In this release of IBM MFA, the IBM MFA password is needed only for enrolling tokens for TOTP and IBM MFA for Yubico OTP, and for password authentication with the PAM authentication method. If the user is not using these authentication methods, you can leave this password blank.
6. Click **Save**.
7. The Policies table shows all of the policies assigned to the user. Click **+** in the Policies section.

   The All Policies table shows all of the available policies.
8. Select one or more policies.
9. Click **Confirm**.

   The Authentication Methods table shows the configured authentication methods for the policy.
10. Select the SecurID authentication method.
11. Click the **Edit** icon.
12. You are prompted for the user-specific authentication method settings. Specify the RSA user ID for this user. If you do not specify an RSA user ID, the MFA ID is used by default.
13. Click **Confirm**.
14. Set **Active** to On for the authentication method.
15. Click **Confirm**.
16. The **CTC Failure Count** is the number of times a user consecutively fails to provide a valid credential, based on the **Max CTC Check Failures Before Suspension** setting in Chapter 5, "Configuring server options," on page 23. If the user exceeds this limit, the **Suspended** control it set. You must disable the **Suspended** control before the user can log in.
17. Inform users to use the IBM MFA Out-of-Band web server login page that you configured, such as

    ```
    https://server:port/mfa/policy-name
    ```

    where *port* is the server authentication port you configured and *policy-name* is the policy the user must use. You may want to have the user bookmark this URL.
18. When the user visits the IBM MFA Out-of-Band web login page,

    user-specific information about the methods required for the user to log in is displayed.

Enabling users for IBM MFA for PIV/CAC or X.509 Certificate authentication

To enable a user for IBM MFA for PIV/CAC or X.509 Certificate authentication you need to have the user's PIV/CAC card public certificate in a location that is accessible from your browser.

About this task

To enable users for IBM MFA for PIV/CAC or X.509 Certificate authentication, complete the following steps:

Procedure

1. In the IBM MFA GUI, click the **User Provisioning** tab.
2. Click the plus sign (**+**) control.
3. Enter the ID for the user. The ID is the user name associated with the effective client user ID. IBM MFA automatically saves the user ID in lowercase.
4. Enter the Name for the user. This is a name of your choice.
5. Enter an MFA password of your choice, if applicable. The MFA password is a special password that allows the user to log in to the IBM MFA server for IBM MFA-specific actions. This password is unique to the IBM MFA server.

   Note: In this release of IBM MFA, the IBM MFA password is needed only for enrolling tokens for TOTP and IBM MFA for Yubico OTP, and for password authentication with the PAM authentication method. If the user is not using these authentication methods, you can leave this password blank.
6. Click **Save**.
7. The Policies table shows all of the policies assigned to the user. Click **+** in the Policies section.

   The All Policies table shows all of the available policies.
8. Select one or more policies.
9. Click **Confirm**.

   The Authentication Methods table shows the configured authentication methods for the policy.
10. Select the certificate authentication method.
11. Click the **Edit** icon.
12. You are prompted for the user-specific authentication method settings. Upload the user's PIV/CAC card public certificate. You can browse to the file in `.cer` or `.pem` format.

    Note: You can optionally have users register their own certificates. In this case, you must approve the certificate before the user can use it to log in, as described in "Approving user certificates" on page 54. This process requires the user to log in to the IBM MFA server system with a user name and password, which may not be appropriate for all users.
13. Click **Confirm**.
14. Set **Active** to On for the authentication method.
15. Click **Confirm**.
16. The **CTC Failure Count** is the number of times a user consecutively fails to provide a valid credential, based on the **Max CTC Check Failures Before Suspension** setting in Chapter 5, "Configuring server options," on page 23. If the user exceeds this limit, the **Suspended** control it set. You must disable the **Suspended** control before the user can log in.
17. Inform users to use the IBM MFA Out-of-Band web server login page that you configured, such as

    ```
    https://server:port/mfa/policy-name
    ```

    where *port* is the server authentication port you configured and *policy-name* is the policy the user must use. You may want to have the user bookmark this URL.
18. When the user visits the IBM MFA Out-of-Band web login page,

    user-specific information about the methods required for the user to log in is displayed.

Approving user certificates

If you choose to have the user register their own certificates, you must approve the certificate before the user can use it to log in.

About this task

Note: This procedure requires the user to log in to the IBM MFA server system with a user name and password, which may not be appropriate for all users. In this case, register the certificate on behalf of the user, as described in "Enabling users for IBM MFA for PIV/CAC or X.509 Certificate authentication" on page 53.

You must approve the certificate that is presented by a user to be sure it is correct and approved for the specific user. The user cannot use the certificate to log in with the PIV/CAC card until you complete this process. The user can enroll only one certificate.

To approve user certificates, complete the following steps:

Procedure

1. In the IBM MFA GUI, click the **User Provisioning** tab.
2. Select an existing user.
3. Click **Check user information**.

   The Policies table shows all of the policies that are assigned to the user.
4. Click **+** in the Policies section.

   The All Policies table shows all of the available policies.
5. Select a policy that has the certificate authentication method.
6. Click **Confirm**.

   The Authentication Methods table shows the configured authentication methods for the policy.
7. Select the certificate authentication method.
8. Click **Check provisioning information**.
9. You are prompted for the user-specific authentication method settings. Do not upload a certificate.
10. Click **Confirm**.

    The registration state is set to OPEN.
11. Set **Active** to On for the authentication method.
12. Instruct the user to begin the IBM MFA certificate authentication logon process at the web server login page:

    ```
    https://server:port/AZFCERT1/enroll
    ```

    where port is the server authentication port.
13. On the Available Authentication Policies page, instruct the user to click **Open Certificate Enrollment Interface**.
14. On the Certificate AZFCERT1 Enrollment page, instruct the user to click **Begin Certificate Enrollment**.
15. The user must select the certificate they want to use to log in and enter their valid PIN.
16. If successful, the user receives a message indicating the certificate enrollment succeeded and to await further instruction from the administrator.
17. In the IBM MFA GUI, select the user again.
18. Click **Check user information**.
19. Select the certificate authentication method.
20. Click **Check provisioning information**.
21. Examine the user certificate and set the registration state to APPROVED if it is correct.

22. Click **Confirm**.
23. Set **Active** to On for the authentication method.
24. Instruct the user to return to the web server login page and log in.
25. On the Available Authentication Policies page, instruct the user to now click **Begin Certificate-based Authentication**.
26. The user must select the certificate they want to use to log in and enter their valid PIN.
27. On the Cache Token Credential page, instruct the user to copy the generated cache token credential and use it to log in to the application.

Enabling users for TOTP authentication

To enable a user for TOTP authentication you must provision users with the TOTP policy and prepare the user's device.

Configuring users for TOTP authentication

You must enable existing users with the IBM MFA policies that you require.

About this task

To enable users for TOTP authentication, complete the following steps:

Procedure

1. In the IBM MFA GUI, click the **User Provisioning** tab.
2. Click the plus sign (**+**) control.
3. Enter the ID for the user. The ID is the user name associated with the effective client user ID. IBM MFA automatically saves the user ID in lowercase.
4. Enter the Name for the user. This is a name of your choice.
5. Enter an MFA password of your choice, if applicable. The MFA password is a special password that allows the user to log in to the IBM MFA server for IBM MFA-specific actions. This password is unique to the IBM MFA server.

   Note: In this release of IBM MFA, the IBM MFA password is needed only for enrolling tokens for TOTP and IBM MFA for Yubico OTP, and for password authentication with the PAM authentication method. If the user is not using these authentication methods, you can leave this password blank.
6. Click **Save**.
7. The Policies table shows all of the policies assigned to the user. Click **+** in the Policies section.

   The All Policies table shows all of the available policies.
8. Select one or more policies.
9. Click **Confirm**.

   The Authentication Methods table lists the configured authentication methods for the policy.
10. Select the TOTP authentication method.
11. Click the **Edit** icon.
12. You are prompted for the user-specific authentication method settings.

Table 15. User-specific TOTP settings

Tag	**Description**
Registration state	Set this to OPEN.
Digest algorithm	Select the digest algorithm.
Number of Digits	Select the number of digits in the generated token.

13. Click **Confirm**.

14. Set **Active** to On for the authentication method.
15. Click **Confirm**.
16. The **CTC Failure Count** is the number of times a user consecutively fails to provide a valid credential, based on the **Max CTC Check Failures Before Suspension** setting in Chapter 5, “Configuring server options,” on page 23. If the user exceeds this limit, the **Suspended** control it set. You must disable the **Suspended** control before the user can log in.

Preparing user devices for generic TOTP authentication

Generic TOTP uses the TOTP authentication method. You must prepare each user's device for generic TOTP.

Procedure

1. Instruct users to install a QR code application such as IBM Verify, Google Authenticator, or Duo Mobile on their device.
2. Instruct the user to open the generic TOTP start page in a desktop web browser and to log in with their user name and their MFA password. The MFA password is a special password that allows the user to log in to the IBM MFA server for IBM MFA-specific actions. For example:

   ```
   https://hostname:6793/AZFTOTP1/genericStart
   ```

   A page that contains the **AuthURL** URL and the encoded QR code is displayed.
3. Instruct the user to point their device at the generated QR code and scan it with the application.

   The application displays the TOTP code.
4. Instruct the user to enter the TOTP code on the web page and click **Generic TOTP Enrollment**.
5. If an error occurs, the user is prompted to retry enrollment. In this case, for the greatest compatibility with QR applications, first set the following parameter values:

   - **Digest Algorithm** SHA1
   - **Token Digits** 6
   - **Token Period Seconds** 30

   If an error occurs, instruct the user to click **Retry enrollment**.
6. If the enrollment is successful, the message "New TOTP token has been confirmed and is ready to use." is displayed. The user must now use this TOTP token code to log in.
7. Inform users to use the IBM MFA Out-of-Band web server login page that you configured, such as

   ```
   https://server:port/mfa/policy-name
   ```

   where *port* is the server authentication port you configured and *policy-name* is the policy the user must use. You may want to have the user bookmark this URL.
8. When the user visits the IBM MFA Out-of-Band web login page,

   user-specific information about the methods required for the user to log in is displayed.

Enabling users for IBM MFA for generic RADIUS authentication

To enable a user for IBM MFA for generic RADIUS authentication you need the user's RADIUS user ID. Generic RADIUS refers to the RADIUS server of your choice that returns a simple allowed or denied response. IBM MFA supports Password Authentication Protocol (PAP) only.

About this task

To enable users for IBM MFA for generic RADIUS authentication, complete the following steps:

Procedure

1. In the IBM MFA GUI, click the **User Provisioning** tab.
2. Click the plus sign (**+**) control.
3. Enter the ID for the user. The ID is the user name associated with the effective client user ID. IBM MFA automatically saves the user ID in lowercase.
4. Enter the Name for the user. This is a name of your choice.
5. Enter an MFA password of your choice, if applicable. The MFA password is a special password that allows the user to log in to the IBM MFA server for IBM MFA-specific actions. This password is unique to the IBM MFA server.

   Note: In this release of IBM MFA, the IBM MFA password is needed only for enrolling tokens for TOTP and IBM MFA for Yubico OTP, and for password authentication with the PAM authentication method. If the user is not using these authentication methods, you can leave this password blank.
6. Click **Save**.
7. The Policies table shows all of the policies assigned to the user. Click **+** in the Policies section.

   The All Policies table shows all of the available policies.
8. Select one or more policies.
9. Click **Confirm**.

   The Authentication Methods table lists the configured authentication methods for the policy.
10. Select the IBM MFA for generic RADIUS authentication method.
11. Click the **Edit** icon.
12. You are prompted for the user-specific authentication method settings. Specify the RADIUS user ID for this user. If you do not specify a user ID, the MFA ID is used by default.
13. Click **Confirm**.
14. Set **Active** to On for the authentication method.
15. Click **Confirm**.
16. The **CTC Failure Count** is the number of times a user consecutively fails to provide a valid credential, based on the **Max CTC Check Failures Before Suspension** setting in Chapter 5, “Configuring server options,” on page 23. If the user exceeds this limit, the **Suspended** control it set. You must disable the **Suspended** control before the user can log in.
17. Inform users to use the IBM MFA Out-of-Band web server login page that you configured, such as

    ```
    https://server:port/mfa/policy-name
    ```

    where *port* is the server authentication port you configured and *policy-name* is the policy the user must use. You may want to have the user bookmark this URL.
18. When the user visits the IBM MFA Out-of-Band web login page,

    user-specific information about the methods required for the user to log in is displayed.

Enabling users for IBM MFA for SafeNet RADIUS authentication

To enable a user for IBM MFA for SafeNet RADIUS authentication you need the user's RADIUS user ID. IBM MFA supports Password Authentication Protocol (PAP) only.

About this task

To enable users for IBM MFA for SafeNet RADIUS authentication, complete the following steps:

Procedure

1. In the IBM MFA GUI, click the **User Provisioning** tab.
2. Click the plus sign (**+**) control.

3. Enter the ID for the user. The ID is the user name associated with the effective client user ID. IBM MFA automatically saves the user ID in lowercase.
4. Enter the Name for the user. This is a name of your choice.
5. Enter an MFA password of your choice, if applicable. The MFA password is a special password that allows the user to log in to the IBM MFA server for IBM MFA-specific actions. This password is unique to the IBM MFA server.

   Note: In this release of IBM MFA, the IBM MFA password is needed only for enrolling tokens for TOTP and IBM MFA for Yubico OTP, and for password authentication with the PAM authentication method. If the user is not using these authentication methods, you can leave this password blank.
6. Click **Save**.
7. The Policies table shows all of the policies assigned to the user. Click **+** in the Policies section.

   The All Policies table shows all of the available policies.
8. Select one or more policies.
9. Click **Confirm**.

   The Authentication Methods table lists the configured authentication methods for the policy.
10. Select the IBM MFA for SafeNet RADIUS authentication method.
11. Click the **Edit** icon.
12. You are prompted for the user-specific authentication method settings. Specify the RADIUS user ID for this user. If you do not specify a user ID, the MFA ID is used by default.
13. Click **Confirm**.
14. Set **Active** to On for the authentication method.
15. Click **Confirm**.
16. The **CTC Failure Count** is the number of times a user consecutively fails to provide a valid credential, based on the **Max CTC Check Failures Before Suspension** setting in Chapter 5, “Configuring server options,” on page 23. If the user exceeds this limit, the **Suspended** control it set. You must disable the **Suspended** control before the user can log in.
17. Inform users to use the IBM MFA Out-of-Band web server login page that you configured, such as

    ```
    https://server:port/mfa/policy-name
    ```

    where *port* is the server authentication port you configured and *policy-name* is the policy the user must use. You may want to have the user bookmark this URL.
18. When the user visits the IBM MFA Out-of-Band web login page,

    user-specific information about the methods required for the user to log in is displayed.

Understanding login options for IBM MFA for SafeNet RADIUS

How the user logs on to the application depends on how you have configured the Token Templates and the Server-Side PIN policies. Inform the users about the procedure they must follow.

About this task

Important: IBM MFA supports the MobilePASS token, and has been tested with the SafeNet Authentication Service Token Templates and Server-Side PIN policies. Consult your SafeNet documentation for configuration information.

How the user logs on to the application depends on how you have configured the Token Templates and the Server-Side PIN policies, as shown in Table 16 on page 58 and Table 17 on page 59.

Table 16. Login Options for SafeNet Quick Log

PIN	You Enter...
No PIN	Enter the MobilePASS passcode in the password field.

Table 16. Login Options for SafeNet Quick Log (continued)

PIN	You Enter...
Server-side User Select	Enter your PIN followed by the MobilePASS passcode in the password field.
User-selected PIN	Enter the MobilePASS passcode in the password field.
New PIN required	1. Enter your current PIN followed by the MobilePASS passcode in the password field. (The PIN is not required in the User-selected PIN mode.) 2. When prompted, enter a new PIN in the password field. 3. Confirm the PIN.

Table 17. Login Options for SafeNet Challenge-Response

PIN	You Enter...
No PIN	1. Enter any single alphabetic character in the password field and press Enter. 2. Copy the challenge, paste it in MobilePASS, and generate a passcode. 3. Enter the MobilePASS passcode in the password field.
Server-side User Select	1. Enter any single alphabetic character in the password field and press Enter. 2. Copy the challenge, paste it in MobilePASS and generate a passcode. 3. Enter the PIN followed by the MobilePASS passcode in the password field.
User-selected PIN	1. Enter any single alphabetic character in the password field and press Enter. 2. Copy the challenge, paste it in MobilePASS, and generate a passcode. 3. Enter the passcode in the password field.
New PIN required	1. Enter any single alphabetic character in the password field and press Enter. 2. Copy the challenge, paste it in MobilePASS, and generate a passcode. 3. Enter the PIN followed by the passcode in the password field. (The PIN is not required in the User-selected PIN mode.) 4. Respond to the prompts to enter a new PIN.

Important: If the user enters an incorrect PIN more times than your SafeNet configuration allows, the SafeNet server might lock the token. In this case, the user receives an authentication error. The IBM MFA server shows the following error message, but does not specifically indicate that the token is locked:

```
MFAPOL:AZF2604I User user-name denied by factor AZFSFNP1
```

Check your SafeNet server log file for `User's token is locked.` messages and manage the token according to your security policy.

Enabling users for RSA SecurID RADIUS authentication

To enable a user for RSA SecurID RADIUS authentication you need the user's RADIUS user ID. IBM MFA supports Password Authentication Protocol (PAP) only.

About this task

To enable users for RSA SecurID RADIUS authentication, complete the following steps:

Procedure

1. In the IBM MFA GUI, click the **User Provisioning** tab.
2. Click the plus sign (**+**) control.
3. Enter the ID for the user. The ID is the user name associated with the effective client user ID. IBM MFA automatically saves the user ID in lowercase.
4. Enter the Name for the user. This is a name of your choice.
5. Enter an MFA password of your choice, if applicable. The MFA password is a special password that allows the user to log in to the IBM MFA server for IBM MFA-specific actions. This password is unique to the IBM MFA server.

   Note: In this release of IBM MFA, the IBM MFA password is needed only for enrolling tokens for TOTP and IBM MFA for Yubico OTP, and for password authentication with the PAM authentication method. If the user is not using these authentication methods, you can leave this password blank.
6. Click **Save**.
7. The Policies table shows all of the policies assigned to the user. Click **+** in the Policies section.

   The All Policies table shows all of the available policies.
8. Select one or more policies.
9. Click **Confirm**.

   The Authentication Methods table lists the configured authentication methods for the policy.
10. Select the RSA SecurID RADIUS authentication method.
11. Click the **Edit** icon.
12. You are prompted for the user-specific authentication method settings. Specify the RADIUS user ID for this user. If you do not specify a user ID, the MFA ID is used by default.
13. Click **Confirm**.
14. Set **Active** to On for the authentication method.
15. Click **Confirm**.
16. The **CTC Failure Count** is the number of times a user consecutively fails to provide a valid credential, based on the **Max CTC Check Failures Before Suspension** setting in Chapter 5, “Configuring server options,” on page 23. If the user exceeds this limit, the **Suspended** control it set. You must disable the **Suspended** control before the user can log in.
17. Inform users to use the IBM MFA Out-of-Band web server login page that you configured, such as

    ```
    https://server:port/mfa/policy-name
    ```

    where *port* is the server authentication port you configured and *policy-name* is the policy the user must use. You may want to have the user bookmark this URL.
18. When the user visits the IBM MFA Out-of-Band web login page,

    user-specific information about the methods required for the user to log in is displayed.

Enabling users for IBM MFA for Yubico OTP authentication

Follow the steps in this section to provision users and start up and administer IBM MFA for Yubico OTP authentication.

Before you begin

There are two possible scenarios when provisioning users for IBM MFA for Yubico OTP authentication:

- Allow the users to self-enroll their own tokens. This method allows you to activate a large number of users for IBM MFA for Yubico OTP authentication without being concerned with which user has which specific YubiKey token.
- Enroll tokens for users. This methods is more time consuming and is best suited to activate a small number of users. It allows you to control which user has which specific token.

Creating a .csv configuration file

If you already have a `.csv` configuration file from your YubiKey provider, you can skip this section. You can create a `.csv` configuration file that contains the YubiKey token key material if you do not have one from your YubiKey provider. Yubico OTP is the only supported Yubico format.

About this task

Note: As described in the YubiKey documentation, the Yubico OTP generated by the Yubikey token represents a single authentication method. It is recommended that you use IBM MFA for Yubico OTP with another authentication method.

To prepare the IBM MFA for Yubico OTP token, complete the following steps:

Procedure

1. Download and install the YubiKey Personalization Tool from the Yubico website https://www.yubico.com/.
2. Insert the Yubikey token in a USB slot on a Windows system.
3. Run the YubiKey Personalization Tool.
4. Select the **Settings** tab.
5. In the **Log configuration output** control, select **Yubico format**. This is the only supported format.
6. Select the **Yubico OTP** tab.
7. Click **Quick**.
8. Select **Configuration Slot 2**.
9. Click **Write Configuration**.

   The configuration information is stored in a format similar to the following example:

   ```
   7699966,tvhcjlhgucln,ba29fe0f63b4,3ae7fa1cd82885153a2ae8dea864a22b,
   000000000000,2018-08-23T16:06:21,
   ```

   where the first field is the serial number of the Yubikey token and the key material follows.
10. Save the configuration file (`.csv` file) to a secure location of your choice that is accessible to the IBM MFA server system.

    Important: The configuration `.csv` file contains important key material. Save the file only in a secure location. A malicious actor could attempt to use the key material to gain system access.

Allowing users to self-enroll their tokens

Allowing users to self-enroll their YubiKey token on the web enrollment page lets you activate users for IBM MFA for Yubico OTP. Use the self-enrollment process when you do not need to control which user has which specific YubiKey token. Yubico OTP is the only supported Yubico format.

Before you begin

Note: As described in the YubiKey documentation, the Yubico OTP generated by the YubiKey token represents a single authentication factor. It is recommended that you use IBM MFA for Yubico OTP authentication together with another authentication method.

About this task

The **`azfyubi1_ingest`** command has the parameters shown in Table 18 on page 62.

Table 18. azfyubi1_ingest Parameters

Parameter	Description
SCAN	Iterates over the entire input file, attempts to validate each line as a Yubico format token descriptor, and determines whether a IBM MFA record already exists for the parsed token Public ID. Must be uppercase.
INGEST mode without COMMIT	Includes the SCAN behavior, and indicates which IBM MFA record additions would have been made. Must be uppercase.
INGEST mode with COMMIT	Includes the SCAN behavior, and indicates which IBM MFA record additions were made. Must be uppercase.
CLEAN mode without COMMIT	Includes the SCAN behavior, and indicates which IBM MFA record deletions would have been made. Must be uppercase.
CLEAN mode with COMMIT	Includes the SCAN behavior, and indicates which IBM MFA record deletions were made. Must be uppercase.

Procedure

1. **Enable Yubico enrollment services** must be enabled, as described in Chapter 5, “Configuring server options,” on page 23.
2. Add the `/opt/IBM/MFA/bin` directory to your PATH.

   ```
   export PATH=/opt/IBM/MFA/bin:${PATH}
   ```

3. Run the **`./azfyubi1_ingest`** program with the **`SCAN`** parameter and check for errors.

   Note: The output is for example purposes and contains only one CSV record.

   The message `AZFDB:PubId not found` is informational and indicates that the public IDs of the Yubikey tokens are not already in the IBM MFA database.

   ```
   ./azfyubi1_ingest yubikey.csv SCAN
   Proceeding in SCAN mode
   2019-08-08-12-58-39.410906 AZFDB:PubId not found
   AZF Yubico OTP Settings:
     PKCS#11 Token Name: azf
     PKCS#11 Key Label:  AZFYUBI1.AESKEY

   Ingest Utility Results:
     Valid CSV records in input file:       1
       Those with PubID already in DB:    0
     Number of DB records written:        0
     Number of DB records deleted:        0
   Total input file lines processed: 1
   ```

4. Run the **`./azfyubi1_ingest`** program with the **`INGEST`** parameter without the **`COMMIT`** parameter and check for errors.

   ```
   ./azfyubi1_ingest yubikey.csv INGEST
   Proceeding in INGEST mode with committing OFF
   2019-08-08-13-13-23.345807 AZFDB:PubId not found
   Skipped attempt to create a new DB record for token with public ID vvjkeehkbkuj
   AZF Yubico OTP Settings:
     PKCS#11 Token Name: azf
     PKCS#11 Key Label:  AZFYUBI1.AESKEY

   Ingest Utility Results:
     Valid CSV records in input file:       1
       Those with PubID already in DB:    0
     Number of DB records written:        0
     Number of DB records deleted:        0
   Total input file lines processed: 1
   ```

5. Run the **`./azfyubi1_ingest`** program with the **`INGEST`** parameter with the **`COMMIT`** parameter.

```
./azfyubi1_ingest yubikey.csv INGEST
COMMITProceeding in INGEST mode with committing ON
2019-08-08-13-15-59.207569 AZFDB:PubId not found
Added a new DB record for token with public ID vvjkeehkbkuj
AZF Yubico OTP Settings:
  PKCS#11 Token Name: azf
  PKCS#11 Key Label:  AZFYUBI1.AESKEY

Ingest Utility Results:
  Valid CSV records in input file:       1
    Those with PubID already in DB:    0
  Number of DB records written:        1
  Number of DB records deleted:        0
Total input file lines processed: 1
```

6. Create an input file in the following format:

   Note: The bulk provisioning feature is described in "Provisioning users in bulk for IBM MFA" on page 49. The IBM MFA for Yubico OTP-specific steps are summarized here for your convenience.

   ```
   user-name policy-name AZFYUBI1
   ```

   For example:

   ```
   USERA YUBI AZFYUBI1
   USERB YUBI AZFYUBI1
   USERC YUBI AZFYUBI1
   USERD YUBI AZFYUBI1
   USERE YUBI AZFYUBI1
   USERF YUBI AZFYUBI1
   USERG YUBI AZFYUBI1 ADD USERNAME=USERG
   ```

   In this example, USERA through USERF are existing IBM MFA users. USERG is a new user being added to the IBM MFA database.
7. Run the **`azfbulk`** program without the **`COMMIT`** parameter.

   ```
   ./azfbulk input-file
   ```

8. Check the resulting `azfprov1.sh` files.

   Important: `azfbulk` generates a `azfprov2.sh` file that is not needed or functional in this workflow. Do not run the `azfprov2.sh` file.
9. Correct any errors in your input file and re-run the **`azfbulk`** command.
10. Run the **`azfbulk`** program with the **`COMMIT`** parameter.

    ```
    ./azfbulk input-file COMMIT
    ```

11. Run the `azfprov1.sh` shell script.

    ```
    sh azfprov1.sh
    ```

12. Instruct the user to insert the YubiKey into a USB port on their Windows system.
13. Instruct the user to launch the YubiKey enrollment page:

    ```
    https://server-name:port/AZFYUBI1/enroll
    ```

    Instruct the user to provide their user name and MFA password, and tap the YubiKey to generate an OTP in the YubiKey OTP field. The MFA password is a special password that allows the user to log in to the IBM MFA server for IBM MFA-specific actions.

    The user receives a message that the YubiKey was associated with their account.

    ```
    Information
    Your YubiKey device was successfully associated with your account.
    ```

14. Verify the provisioned users in the IBM MFA GUI.

    Note that the authentication method state changes to **`ACTIVE`**.

15. The user must now use the YubiKey token to log in.
16. Inform users to use the IBM MFA Out-of-Band web server login page that you configured, such as

    ```
    https://server:port/mfa/policy-name
    ```

    where *port* is the server authentication port you configured and *policy-name* is the policy the user must use. You may want to have the user bookmark this URL.
17. When the user visits the IBM MFA Out-of-Band web login page,

    user-specific information about the methods required for the user to log in is displayed.

Enrolling tokens for users

Enroll the tokens for users when you need to control which user has which specific YubiKey token.

Before you begin

Note: As described in the YubiKey documentation, the Yubico OTP generated by the YubiKey token represents a single authentication factor. It is recommended that you use IBM MFA for Yubico OTP authentication together with another authentication method.

About this task

The bulk provisioning feature is described in "Provisioning users in bulk for IBM MFA" on page 49. The IBM MFA for Yubico OTP-specific steps are summarized here for your convenience.

To configure the IBM MFA for Yubico OTP authentication method, complete the following steps:

Procedure

1. Add the `/opt/IBM/MFA/bin` directory to your PATH.

   ```
   export PATH=/opt/IBM/MFA/bin:${PATH}
   ```

2. Create an input file in the following format:

   ```
   user-name policy-name AZFYUBI1 csv-data
   ```

   where *csv-data* is the complete string from the configuration file (`.csv` file) that you want to assign to this user enclosed in quotation marks.

   For example:

   ```
   USERA YUBI AZFYUBI1 "7699966,tvhcjlhgucln,ba29fe0f63b4,3ae7fa1cd82885153a2ae8dea864a
   22b,000000000000,2018-08-23T16:06:21,"
   ```

   In this example, USERA is an existing IBM MFA user.
3. Run the **`azfbulk`** program without the **`COMMIT`** parameter.

   ```
   ./azfbulk input-file
   ```

4. Check the resulting `azfprov1.sh` and `azfprov2.sh` files.
5. Correct any errors in your input file and re-run the **`azfbulk`** command.
6. Run the **`azfabulk`** program with the **`COMMIT`** parameter.

   ```
   ./azfbulk input-file COMMIT
   ```

7. Run the `azfprov1.sh` shell script.

   ```
   sh azfprov1.sh
   ```

8. Run the `azfprov2.sh` shell script.

```
sh azfprov2.sh
```

9. Verify the provisioned users in the IBM MFA GUI.

   Note that the registration state changes to **WANTSYNC** and the authentication method state changes to **ACTIVE**.
10. Instruct the user to insert the YubiKey into a USB port on their Windows system.
11. Instruct the user to log in to the application and press the YubiKey token to generate a token in the password field. Remind the users that a YubiKey token in **Configuration Slot 2** requires the long press.

    Note that the registration state changes to **CONFIRMED**.
12. The user must now use the YubiKey token to log in.
13. Inform users to use the IBM MFA Out-of-Band web server login page that you configured, such as

    ```
    https://server:port/mfa/policy-name
    ```

    where *port* is the server authentication port you configured and *policy-name* is the policy the user must use. You may want to have the user bookmark this URL.
14. When the user visits the IBM MFA Out-of-Band web login page,

    user-specific information about the methods required for the user to log in is displayed.

Enabling users for IBM MFA for LDAP Simple Bind

To enable a user for IBM MFA for LDAP Simple Bind authentication you need the user's fully-qualified domain name.

About this task

Note: You need the fully-qualified domain name for each user you want to authenticate with IBM MFA for LDAP Simple Bind. For example, the Windows `whoami /fqdn` command returns results similar to the following:

```
C:\Users\juser>whoami /fqdn
CN=J User,OU=Users,OU=Company Offices,DC=companyname,DC=com
```

To enable users for IBM MFA for LDAP Simple Bind, complete the following steps:

Procedure

1. In the IBM MFA GUI, click the **User Provisioning** tab.
2. Click the plus sign (**+**) control.
3. Enter the ID for the user. The ID is the user name associated with the effective client user ID. IBM MFA automatically saves the user ID in lowercase.
4. Enter the Name for the user. This is a name of your choice.
5. Enter an MFA password of your choice, if applicable. The MFA password is a special password that allows the user to log in to the IBM MFA server for IBM MFA-specific actions. This password is unique to the IBM MFA server.

   Note: In this release of IBM MFA, the IBM MFA password is needed only for enrolling tokens for TOTP and IBM MFA for Yubico OTP, and for password authentication with the PAM authentication method. If the user is not using these authentication methods, you can leave this password blank.
6. Click **Save**.
7. The Policies table shows all of the policies assigned to the user. Click **+** in the Policies section.

   The All Policies table shows all of the available policies.
8. Select one or more policies.
9. Click **Confirm**.

The Authentication Methods table lists the configured authentication methods for the policy.

10. Select the IBM MFA for LDAP Simple Bind authentication method.
11. Click the **Edit** icon.
12. You are prompted for the user-specific authentication method settings. Specify the fully qualified DN for this user.
13. Click **Confirm**.
14. Set **Active** to On for the authentication method.
15. Click **Confirm**.
16. The **CTC Failure Count** is the number of times a user consecutively fails to provide a valid credential, based on the **Max CTC Check Failures Before Suspension** setting in Chapter 5, "Configuring server options," on page 23. If the user exceeds this limit, the **Suspended** control it set. You must disable the **Suspended** control before the user can log in.
17. Inform users to use the IBM MFA Out-of-Band web server login page that you configured, such as

```
https://server:port/mfa/policy-name
```

where *port* is the server authentication port you configured and *policy-name* is the policy the user must use. You may want to have the user bookmark this URL.

18. When the user visits the IBM MFA Out-of-Band web login page,

user-specific information about the methods required for the user to log in is displayed.

Enabling users for IBM MFA for IBM Security Access Manager authentication

To enable a user for IBM MFA for IBM Security Access Manager authentication you need the user's user ID and the application context.

About this task

To enable users for IBM MFA for IBM Security Access Manager authentication, complete the following steps:

Procedure

1. In the IBM MFA GUI, click the **User Provisioning** tab.
2. Click the plus sign (**+**) control.
3. Enter the ID for the user. The ID is the user name associated with the effective client user ID. IBM MFA automatically saves the user ID in lowercase.
4. Enter the Name for the user. This is a name of your choice.
5. Enter an MFA password of your choice, if applicable. The MFA password is a special password that allows the user to log in to the IBM MFA server for IBM MFA-specific actions. This password is unique to the IBM MFA server.

   Note: In this release of IBM MFA, the IBM MFA password is needed only for enrolling tokens for TOTP and IBM MFA for Yubico OTP, and for password authentication with the PAM authentication method. If the user is not using these authentication methods, you can leave this password blank.
6. Click **Save**.
7. The Policies table shows all of the policies assigned to the user. Click **+** in the Policies section.

   The All Policies table shows all of the available policies.
8. Select one or more policies.
9. Click **Confirm**.

   The Authentication Methods table lists the configured authentication methods for the policy.
10. Select the IBM MFA for IBM Security Access Manager authentication method.
11. Click the **Edit** icon.

12. You are prompted for the user-specific authentication method settings. Specify the IBM MFA for IBM Security Access Manager user ID for this user and the authentication context. If you do not specify a user ID, the MFA ID is used by default.
13. Click **Confirm**.
14. Set **Active** to On for the authentication method.
15. Click **Confirm**.
16. The **CTC Failure Count** is the number of times a user consecutively fails to provide a valid credential, based on the **Max CTC Check Failures Before Suspension** setting in Chapter 5, “Configuring server options,” on page 23. If the user exceeds this limit, the **Suspended** control it set. You must disable the **Suspended** control before the user can log in.
17. Inform users to use the IBM MFA Out-of-Band web server login page that you configured, such as

    ```
    https://server:port/mfa/policy-name
    ```

    where *port* is the server authentication port you configured and *policy-name* is the policy the user must use. You may want to have the user bookmark this URL.
18. When the user visits the IBM MFA Out-of-Band web login page,

    user-specific information about the methods required for the user to log in is displayed.

IBM MFA for IBM Security Access Manager login flow

This section describes the typical user login flow. The exact steps the user must follow depend on your IBM MFA for IBM Security Access Manager configuration.

About this task

As part of the login flow, provide the user with the following:

- The URL of the IBM Security Access Manager server login page.
- Their user name on the IBM Security Access Manager server.
- The name of the application to use on the Generate application one-time password page.

Important: As part of the login flow, the user registers and uses a device such as a smart phone, tablet, and so forth, that is running the IBM Verify application. This device must have network connectivity to the IBM Security Access Manager server.

Procedure

1. Navigate to the web page provided by your administrator and log in with your IBM Security Access Manager user name.

   The API Multi-factor authentication page is displayed.
2. Click on **Manage / Register IBM Verify and FIDO U2F**. This step is needed only on your first access.
   a) Under **Authenticators::Register new authenticator**, select **AuthenticatorClient** in the drop-down menu.
   b) Click **register new authenticator**.
   c) Launch IBM Verify on the device and point the camera at the displayed QR code.
   d) IBM Verify connects with API Multi-factor authentication and creates a new account.
   e) Click **Home** on the web page to return to the API Multi-factor authentication page.
3. Click **Obtain application OTP**. The Mobile Multi Factor Device Selection page is displayed.
   a) Click the radio button corresponding to the device you registered.
   b) Click **Submit**. This device will receive a notification.
   c) The Mobile Multi Factor Pending Authentication page is displayed.

   d) Accept the **Please log me in: user name** notification on your device. Click the check mark and verify with your fingerprint if you configured Touch ID.
   e) If the Mobile Multi Factor Pending Authentication page does not disappear, click **Verify**.

4. On the Generate application one-time password page:
   a) Select the application the administrator instructs you to use from the **Application** drop-down menu.
   b) Click **Generate OTP**. The OTP is displayed:

```
Application One-time Password
Username    username
Application    app-name
One-time password    OTP
Expires In (hh:mm:ss)
```

   c) Copy the OTP to the clipboard.
5. Log in to the IBM MFA Out-of-Band login page provided by your administrator with your IBM MFA user ID.
6. Paste the OTP from the clipboard as your password.

Enabling users for IBM MFA Password Authentication

The IBM MFA Password Authentication is performed against the user's IBM MFA-specific password. Password authentication is a weak authentication method and you must use it in addition to at least one other authentication method.

About this task

To enable users for IBM MFA Password Authentication, complete the following steps:

Procedure

1. In the IBM MFA GUI, click the **User Provisioning** tab.
2. Click the plus sign (**+**) control.
3. Enter the ID for the user. The ID is the user name associated with the effective client user ID. IBM MFA automatically saves the user ID in lowercase.
4. Enter the Name for the user. This is a name of your choice.
5. Enter an MFA password of your choice.
6. Click **Save**.
7. The Policies table shows all of the policies assigned to the user. Click **+** in the Policies section.

   The All Policies table shows all of the available policies.
8. Select one or more policies.
9. Click **Confirm**.

   The Authentication Methods table lists the configured authentication methods for the policy.
10. Select the IBM MFA Password Authentication authentication method.
11. Set **Active** to On for the authentication method.
12. Click **Confirm**.
13. The **CTC Failure Count** is the number of times a user consecutively fails to provide a valid credential, based on the **Max CTC Check Failures Before Suspension** setting in Chapter 5, “Configuring server options,” on page 23. If the user exceeds this limit, the **Suspended** control it set. You must disable the **Suspended** control before the user can log in.
14. Inform users to use the IBM MFA Out-of-Band web server login page that you configured, such as

```
https://server:port/mfa/policy-name
```

where *port* is the server authentication port you configured and *policy-name* is the policy the user must use. You may want to have the user bookmark this URL.

15. When the user visits the IBM MFA Out-of-Band web login page,

    user-specific information about the methods required for the user to log in is displayed. Remind the user to use their MFA password. The MFA password is a special password that allows the user to log in to the IBM MFA server for IBM MFA-specific actions.

Assigning policies and authentication methods to users

You must assign one or more policies to a user and specify the user-specific authentication method settings, either by using the GUI or by using the bulk provisioning feature. Note that the bulk provisioning feature is more efficient if you have a large number of users.

About this task

To assign one or more policies to a user and to specify the user-specific authentication method settings, complete the following steps:

Procedure

1. In the IBM MFA GUI, click the **User Provisioning** tab.
2. Select an existing user.
3. Click **Check user information**.

   The Policies table shows all of the policies that are assigned to the user.
4. Click **+** in the Policies section.

   The All Policies table shows all of the available policies.
5. Select one or more policies.
6. Click **Confirm**.

   The Authentication Methods table shows the configured authentication methods for the policy.
7. Select an authentication methods.
8. Click **Check provisioning information**.
9. You are prompted for the user-specific authentication methods settings.
10. Click **Confirm**.
11. Set **Active** to **On** for the authentication methods
12. Click **Confirm**.
13. Inform users to use the IBM MFA Out-of-Band web server login page that you configured, such as

    ```
    https://server:port/mfa/policy-name
    ```

    where *port* is the server authentication port you configured and *policy-name* is the policy the user must use. You may want to have the user bookmark this URL.
14. When the user visits the IBM MFA Out-of-Band web login page,

    user-specific information about the methods required for the user to log in is displayed.

Displaying users

You can display the users in the repository.

About this task

To display the users in the IBM MFA repository, complete the following steps:

Procedure

1. In the IBM MFA GUI, click the **User Provisioning** tab.
2. Click the **Users** icon.

   The users in the repository are listed.
3. Click the column labels to sort the users by MFA ID and Name.
4. Enter a search string in the **Search by MFA ID or Name** field to find a specific user.

Checking and updating user information

You can check and update the MFA password, policy, and authentication method information for a specific user.

About this task

To check the user information, complete the following steps:

Procedure

1. In the IBM MFA GUI, click the **User Provisioning** tab.
2. Enter a search string in the **Search by MFA ID or Name** field to find the required user.
3. Select the required user.
4. Click **Check user information**.

   The user-specific information page is displayed. From this page you can:

   a. View the current user information.

   b. Set or reset an IBM MFA password.

   c. Reset the suspension state.

   d. Add or delete a policy.

   e. Add or delete an authentication method.

   f. Set the authentication method to be active or inactive.

   g. Check the user suspension state if you enabled **Consecutive Failures Before TOTP Suspension** for TOTP.
5. If you make a change, confirm your selection and click **Save**.

Suspending or resuming a user account

You can use the **Suspended** control to prevent a user from logging in with an IBM MFA policy. The **Suspended** control is separate and distinct from any z/VM revocation mechanism.

About this task

The **Suspended** control is typically used in conjunction with the **CTC Failure Count**, as described in Chapter 5, “Configuring server options,” on page 23. However, you can also set the **Suspended** control to prevent the user from logging in with IBM MFA authentication for any reason.

Note: If you set the **Suspended** control for a user and the user attempts to log in, the user receives the message `This User ID is unable to authenticate via the specified policy.` The IBM MFA server log in `/var/log/MFA` contains the message `MFAPOL:Userid` *`name`* `is suspended.`

To set or clear the **Suspended** control:

Procedure

1. In the IBM MFA GUI, click the **User Provisioning** tab.
2. Enter a search string in the **Search by MFA ID or Name** field to find the required user.

3. Select the required user.

   The user-specific information page is displayed.
4. Set the **SUSPENDED** control to suspend the user account.
5. Clear the **SUSPENDED** control to resume the user account.

Enabling a TOTP suspended user

If the user exceeds the TOTP **Consecutive Failures Before TOTP Suspension** limit, you must set the **Suspension Status** control to NO before the user can log in.

About this task

To enable a suspended user, complete the following steps:

Procedure

1. In the IBM MFA GUI, click the **User Provisioning** tab.
2. Enter a search string in the **Search by ID or Name** field to find the required user.
3. Select the required user.

   The user-specific information page is displayed.
4. Select the TOTP authentication method.

   The current suspension status is displayed.
5. Click the edit (pencil) icon.
6. Change Suspension Status to NO.
7. Click **Confirm**.

Setting or resetting a user's MFA password

You can set or reset the user's MFA password. The MFA password is a special password that allows the user to log in to the IBM MFA server for IBM MFA-specific actions. This password is unique to the IBM MFA server.

About this task

To set or reset the MFA password, complete the following steps:

Procedure

1. In the IBM MFA GUI, click the **User Provisioning** tab.
2. Enter a search string in the **Search by MFA ID or Name** field to find the required user.
3. Select the required user.

   The user-specific information page is displayed. From this page you can:

   a. View the current user information.

   b. Set or reset an IBM MFA password.

   c. Add or delete a policy.

   d. Add or delete an authentication method.

   e. Set the authentication method to be active or inactive.
4. Click **Set password** to set an initial MFA password.
5. Click **Reset password** to reset the MFA password.
6. If you make a change, confirm your selection and click **Confirm**.

Changing a user's MFA password

You can change a user's MFA password, or allow the user to change it themselves. The MFA password is a special password that allows the user to log in to the IBM MFA server for IBM MFA-specific actions. This password is unique to the IBM MFA server.

About this task

To change the MFA password, complete the following steps:

Procedure

1. Open the following URL, or provide it to your users:

   ```
   https://server-name:port/pwChange
   ```

2. Enter the following information:
   - User Name
   - Password
   - New Password
   - Confirm New Password
3. Click **Change Password**.

Checking and updating user information

You can check and update the MFA password, policy, and authentication method information for a specific user.

About this task

To check the user information, complete the following steps:

Procedure

1. In the IBM MFA GUI, click the **User Provisioning** tab.
2. Enter a search string in the **Search by MFA ID or Name** field to find the required user.
3. Select the required user.
4. Click **Check user information**.

   The user-specific information page is displayed. From this page you can:

   a. View the current user information.

   b. Set or reset an IBM MFA password.

   c. Reset the suspension state.

   d. Add or delete a policy.

   e. Add or delete an authentication method.

   f. Set the authentication method to be active or inactive.

   g. Check the user suspension state if you enabled **Consecutive Failures Before TOTP Suspension** for TOTP.
5. If you make a change, confirm your selection and click **Save**.

Removing policies for a user

You can remove one or more policies that are assigned to a user.

About this task

To remove one or more policies that are assigned to a user, complete the following steps:

Procedure

1. In the IBM MFA GUI, click the **User Provisioning** tab.
2. Select an existing user.

   The Policies table shows all of the policies applied to this user.
3. Select a policy.
4. Click **Delete policy** to remove a policy from this user.
5. Confirm your selection.

Chapter 9. Adding z/VM clients

Use the IBM MFA GUI to add the z/VM systems that interact with the IBM MFA server.

Procedure

1. In the IBM MFA GUI, select the **z/VM Clients** tab.
2. Click the plus sign (+) control.
3. Specify the **Client ID**, **Client Description**, and **Client Secret** of the z/VM systems that interact with the IBM MFA server.
4. Click **Save**.

Chapter 10. Removing z/VM clients

You can use the IBM MFA GUI to remove z/VM clients.

Procedure

1. In the IBM MFA GUI, select the **z/VM Clients** tab.
2. Select the z/VM client you want to remove.
3. Click the trash can control.
4. Click **Save**.

Chapter 11. Backing up and restoring the IBM MFA database

The IBM MFA database includes details about the system configuration, details about all registered users, their configured policies, and authentication methods. You should regularly back up the IBM MFA database.

Before you begin

As a general best practice, you should back up the IBM MFA database at the following times:

- After configuring users, policies, or authentication methods.
- Before performing maintenance activity on the system.
- Periodically, following your local policies and procedures.

About this task

To back up the IBM MFA database, complete the following steps:

Procedure

1. Enter the following command as root to back up the database. The resulting `/opt/IBM/MFA/mfadb.sql` file contains all of the commands that are needed to re-create the database until that time.

   ```
   /usr/bin/pg_dump -f /opt/IBM/MFA/mfadb.sql -d mfadb
   ```

2. If you need to restore the database from the backup, enter the following command as root to restore the database:

   ```
   /usr/bin/psql -U root -d mfadb -f /opt/IBM/MFA/mfadb.sql
   ```

   The command populates the database by running all of the commands in the `/opt/IBM/MFA/mfadb.sql` file.

   Important: If the existing database is not empty, commands will fail because the entries already exist in the database. If you need to restore the database from the backup and the existing database is not empty, you must first delete the existing database:

   a. Ensure that you have a valid `mfadb.sql` file before you continue:

   ```
    ls -l /opt/IBM/MFA/mfadb.sql
   ```

   b. Enter the following command as root to delete the existing database:

   ```
   dropdb mfadb
   ```

   c. Become the **`postgres`** user and enter the following command to create the database:

   ```
   su - postgres
   createdb -O root mfadb
   ```

   d. Exit the **`postgres`** user account:

   ```
   exit
   ```

   e. Enter the following command as root to restore the database:

   ```
   /usr/bin/psql -U root -d mfadb -f /opt/IBM/MFA/mfadb.sql
   ```

Chapter 12. Updating postgres

The IBM MFA database includes details about the system configuration, details about all registered users, their configured policies, and authentication methods. You must back up the IBM MFA database before updating postgres.

Before you begin

As a general best practice, you should back up the IBM MFA database at the following times:

- After configuring users, policies, or authentication methods.
- Before performing maintenance activity on the system.
- Periodically, following your local policies and procedures.

About this task

To update postgres, complete the following steps:

Procedure

1. Stop the IBM MFA server:

   ```
   systemctl stop mfa
   ```

2. Enter the following command as root to back up the database. The resulting `/opt/IBM/MFA/mfadb.sql` file contains all of the commands that are needed to re-create the database until that time.

   ```
   /usr/bin/pg_dump -f /opt/IBM/MFA/mfadb.sql -d mfadb
   ```

3. Enter the following command as root to delete the existing database:

   ```
   dropdb mfadb
   ```

4. Upgrade postgres. Enter the following commands depending on the platform on which you are installing, or use your method of choice to update the packages.

   ```
   For RHEL:
   yum update postgresql-server

   For SLES:
   zypper update libpq5
   zypper update postgresql10-server
   ```

5. Become the postgres user and enter the following command to create the database:

   ```
   su - postgres
   createdb -O root mfadb
   ```

6. Exit the postgres user account:

   ```
   exit
   ```

7. Enter the following command as root to restore the database:

   ```
   /usr/bin/psql -U root -d mfadb -f /opt/IBM/MFA/mfadb.sql
   ```

8. Start the IBM MFA server:

   ```
   systemctl start mfa
   ```

Chapter 13. Preparing user devices for IBM TouchToken for iOS authentication

You can use the IBM TouchToken for iOS application as an alternative to Generic TOTP. You must prepare each user's Apple device for TOTP authentication.

About this task

This procedure assumes that you are using a public certificate authority (CA). It is strongly recommended that you use a certificate issued by a well-known CA. If you are not using a CA that is trusted by default by Apple iOS, ensure that all IBM TouchToken for iOS devices have a Configuration Profile installed that allows the devices to establish TLS connections with the IBM MFA server.

Important: If your IBM MFA server certificate was not issued by a well-known CA, do not instruct users to visit the IBM MFA server start page until they have a Configuration Profile installed that allows them to establish TLS connections with the IBM MFA server. If users accept the server certificate in Mobile Safari as an SSL exception, the IBM TouchToken for iOS application still cannot trust the CA that issued the certificate. Users will be able to view the enrollment launch URL, but will not be able to complete the enrollment.

Procedure

1. Ensure that the user's Apple iOS device has network connectivity to the IBM MFA server.
2. Instruct users to install the IBM TouchToken for iOS application on their iOS device.
3. Instruct users to open the IBM MFA server start page, by using either Mobile Safari on their iOS device or a desktop browser. For example:

   ```
   https://hostname:6793/AZFTOTP1/start
   ```

   The page explains some basic information about TOTP to the user, and contains both a QR code and a link that launch the IBM TouchToken for iOS application on the user's device.
4. Instruct the user to use either the QR code or the link to launch the IBM TouchToken for iOS application on the Apple device. Note that after the TOTP account is set up on the Apple device, the registration state changes to **PROVISIONED** and the state of the authentication method changes to **ACTIVE**.
5. Instruct the user to tap the new TOTP account. You may want to have the user rename this account to remove any system-specific information.
6. When prompted, the user must supply their Apple TouchID fingerprint.

   If successful, the TOTP token code is displayed. The user must now use this OTP token code to log in.
7. Inform users to use the IBM MFA Out-of-Band web server login page that you configured, such as

   ```
   https://server:port/mfa/policy-name
   ```

   where *port* is the server authentication port you configured and *policy-name* is the policy the user must use. You may want to have the user bookmark this URL.
8. When the user visits the IBM MFA Out-of-Band web login page,

   user-specific information about the methods required for the user to log in is displayed.

Chapter 14. Troubleshooting IBM MFA

The troubleshooting steps you perform depend on which system has failed.

Browser shows incorrect or stale data

If your web browser shows incorrect or stale data, refresh the browser window. The browser cache might be out-of-sync with the IBM MFA server.

IBM MFA certificate authentication not working

If the user receives an "There was an error connecting to the server." error when attempting to log in with certificate authentication, ensure that **Enable out-of-band Services** and **Enable certificate services** are both enabled, as described in Chapter 5, “Configuring server options,” on page 23.

The user receives an "Error processing MFA request" error

There are several possible causes of this error:

- The authentication methods configured for the user must match the policy. The policy is not satisfiable if the user is not configured for all of the authentication methods required by the policy.
- No preceding or trailing spaces must exist in the IBM MFA GUI configuration. For example, if an extraneous space exists in the **Radius Primary Server** field, IBM MFA will not be able to resolve the host name or IP address.
- No preceding or trailing spaces must exist in an entry in the pam.d files, as described in “Editing the /etc/pam.d files on Red Hat Enterprise Linux Server on IBM Z” on page 15 and “Editing the /etc/pam.d files on SUSE Linux Enterprise Server on IBM Z” on page 15.

Chapter 15. Optional: Creating test root and server certificates

This section describes the optional case of creating your own certificate authority (CA) root certificate and server certificate if needed for testing purposes. However, it is strongly recommended that you use a server certificate issued by a well-known certificate authority. If you use a server certificate issued by a well-known certificate authority, you can skip this section.

About this task

To create the certificate authority (CA) root certificate and server certificate, complete the following steps:

Procedure

1. Generate a private key:

   ```
   openssl genrsa -des3 -out myCA.key 2048
   ```

2. Generate a root certificate. For convenience, identify the certificate as the root certificate in the **Common Name** field:

   ```
   openssl req -x509 -new -nodes -key myCA.key -sha256 -days
   1825 -out myCA.pem
   ```

   ```
   Enter pass phrase for myCA.key:
   You are about to be asked to enter information that will be incorporated
   into your certificate request.
   What you are about to enter is what is called a Distinguished Name or a DN.
   There are quite a few fields but you can leave some blank
   For some fields there will be a default value,
   If you enter '.', the field will be left blank.
   -----
   Country Name (2 letter code) [AU]:US
   State or Province Name (full name) [Some-State]:Massachusetts
   Locality Name (eg, city) []:Waltham
   Organization Name (eg, company) [Internet Widgits Pty Ltd]:Company Name
   Organizational Unit Name (eg, section) []:MFA
   Common Name (e.g. server FQDN or YOUR name) []:MFA Root Certificate
   Email Address []:user@company.com
   ```

3. Create a private key:

   ```
   openssl genrsa -out test-server.key 2048
   ```

4. Create a certificate signing request (CSR). For convenience, identify the certificate as the server certificate in the **Common Name** field:

   ```
   openssl req -new -key test-server.key -out test-server.csr
   ```

   ```
   You are about to be asked to enter information that will be incorporated
   into your certificate request.
   What you are about to enter is what is called a Distinguished Name or a DN.
   There are quite a few fields but you can leave some blank
   For some fields there will be a default value,
   If you enter '.', the field will be left blank.
   -----
   Country Name (2 letter code) [AU]:US
   State or Province Name (full name) [Some-State]:Massachusetts
   Locality Name (eg, city) []:Waltham
   Organization Name (eg, company) [Internet Widgits Pty Ltd]:Company Name
   Organizational Unit Name (eg, section) []:MFA
   Common Name (e.g. server FQDN or YOUR name) []:Test Server Certificate
   Email Address []:user@company.com

   Please enter the following 'extra' attributes
   ```

```
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

5. Use an editor to create an extension file for the server certificate. Ensure that you specify subject alternate names that cover all names that a user might enter in the browser to access the server.

   ```
   authorityKeyIdentifier=keyid,issuer
   basicConstraints=CA:FALSE
   keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment
   subjectAltName = @alt_names

   [alt_names]
   DNS.1 = fully-qualified-host-name
   DNS.2 = short-name
   DNS.3 = IP address
   ```

6. Create the server certificate using the CSR, the CA private key, the CA certificate, and the extension file:

   ```
   openssl x509 -req -in test-server.csr -CA myCA.pem -CAkey myCA.key
   -CAcreateserial -out test-server.pem -days 1825 -sha256 -extfile test-server.ext
   ```

   ```
   Signature ok
   subject=/C=US/ST=Massachusetts/L=Waltham/O=Company/OU=MFA/CN=Test Server Certificate/
   emailAddress=user@company.com
   Getting CA Private Key
   Enter pass phrase for myCA.key:
   ```

7. Display the server certificate. Note that it is issued by the CA root, with the subject alternate names from the extension file.

   ```
   openssl x509 -in test-server.pem -text
   ```

   ```
   Certificate:
       Data:
           Version: 3 (0x2)
           Serial Number:
               e8:e4:50:85:c4:eb:b5:ba
       Signature Algorithm: sha256WithRSAEncryption
           Issuer: C=US, ST=Massachusetts, L=Waltham, O=Compant, OU=MFA, CN=MFA Root
   Certificate/
   emailAddress=user@company.com
           Validity
               Not Before: Dec  1 19:30:02 2017 GMT
               Not After : Nov 30 19:30:02 2022 GMT
           Subject: C=US, ST=Massachusetts, L=Waltham, O=Company, OU=MFA, CN=Test Server
   Certificate/
   emailAddress=user@company.com
           Subject Public Key Info:
               Public Key Algorithm: rsaEncryption
                   Public-Key: (2048 bit)
                   Modulus:
                       00:ac:ed:13:11:8e:34:dd:98:03:19:1c:03:d9:1e:
                       f1:9b:c6:74:00:ce:36:3a:b1:fc:f7:c8:0c:c6:bf:
                       33:91:dc:c5:31:d1:2f:07:03:1b:62:9f:aa:64:d9:
                       e2:1e:ae:6c:d2:ab:4d:29:2b:0e:4b:dc:ef:43:b2:
                       59:14:97:d0:db:ca:fc:d8:67:fa:51:5f:a4:0d:93:
                       d3:ab:b1:e8:cd:24:62:c4:c8:b9:69:f1:f8:e1:8a:
                       49:72:d9:c7:1f:c4:30:31:f7:c9:0a:65:fe:3c:3a:
                       54:cf:9e:de:98:64:8d:04:53:09:08:95:67:10:ba:
                       7e:b6:46:1c:1c:4a:00:75:7c:1c:0d:6e:0e:dd:19:
                       7d:12:c3:be:f7:9d:04:a0:32:92:9d:f2:5e:58:87:
                       95:da:8e:5f:6e:5f:d6:f6:22:74:4d:a5:02:4b:d8:
                       8e:07:98:f9:93:5e:11:67:83:27:dd:3b:90:4c:c1:
                       25:c5:1f:c9:60:fb:0c:02:5d:a5:ed:87:eb:d5:9e:
                       14:fe:12:6a:06:52:34:37:b9:73:70:2b:c4:16:cc:
                       cd:ed:21:d5:3a:3b:12:f1:21:6e:01:ab:51:3d:c9:
                       c7:9e:12:62:b3:8f:53:97:f7:2b:57:f0:2a:52:fe:
                       b7:55:54:d7:fa:05:2d:8a:a9:f2:6a:43:d3:8c:c3:
                       39:31
                   Exponent: 65537 (0x10001)
           X509v3 extensions:
               X509v3 Authority Key Identifier:
                   keyid:F5:B2:B7:0E:D7:1A:C3:9B:7B:66:3A:C7:17:1F:42:B5:07:71:FF:94
   ```

```
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Key Usage:
                Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment
            X509v3 Subject Alternative Name:
                DNS:fully-qualified-hostname, DNS:hostname,
DNS:IP address
    Signature Algorithm: sha256WithRSAEncryption
         46:25:e4:db:d9:24:93:b7:18:31:c1:96:d0:dd:82:c5:e8:2c:
         da:c3:79:cd:8a:a4:7e:6d:83:62:cc:07:e2:87:9d:2e:2f:54:
         12:9e:a7:47:ce:f3:09:6d:23:6c:8d:4d:b7:19:ca:63:da:92:
         bc:e5:9f:e3:91:92:a5:10:f3:47:56:ca:1f:ec:fe:5c:b6:d2:
         0c:03:a7:49:ee:7d:69:35:44:3d:1b:ce:10:01:d2:0a:5c:51:
         3a:e5:97:93:61:b3:6e:ca:6e:63:cd:44:79:7c:d7:4e:2b:cf:
         40:d3:25:fb:16:9d:49:8b:a8:11:9e:d0:79:3c:5f:9e:51:eb:
         49:6e:62:77:fb:93:fc:2d:a1:b2:e7:77:20:a4:07:4d:6f:c8:
         8e:ff:14:fc:5a:4a:16:c0:9c:21:de:3e:72:8b:16:e7:0e:15:
         00:d5:16:db:2e:8c:e4:0d:e8:9e:d8:de:10:d8:91:4c:df:a5:
         4a:0d:c2:14:03:46:d2:9e:a2:f6:a4:e8:62:58:a5:86:bd:7f:
         de:ed:d7:41:b6:91:c6:1c:cc:cb:85:bb:6a:f3:84:ec:00:d0:
         45:fa:dd:84:73:39:04:12:f9:9d:aa:cc:85:3a:7d:7f:7b:ed:
         01:5f:23:95:3c:a5:11:5d:7e:96:01:64:6c:66:8c:e3:d7:a8:
         af:0e:12:6a
-----BEGIN CERTIFICATE-----
MIIEXzCCA0egAwIBAgIJAOjkUIXE67W6MA0GCSqGSIb3DQEBCwUAMIGoMQswCQYD
VQQGEwJVUzEWMBQGA1UECAwNTWFzc2FjaHVzZXR0czEQMA4GA1UEBwwHV2FsdGhh
bTEYMBYGA1UECgwPUm9ja2V0IFNvZnR3YXJlMQ0wCwYDVQQLDARQTUZBMR4wHAYD
VQQDDBVQTUZBIFJvb3QgQ2VydGlmaWNhdGUxJjAkBgkqhkiG9w0BCQEWF3VzZXJA
cm9ja2V0c29mdHdhcmUuY29tMB4XDTE3MTIwMTE5MzAwMloXDTIyMTEzMDE5MzAw
MlowgaoxCzAJBgNVBAYTAlVTMRYwFAYDVQQIDA1NYXNzYWNodXNldHRzMRAwDgYD
VQQHDAdXYWx0aGFtMRgwFgYDVQQKDA9Sb2NrZXQgU29mdHdhcmUxDTALBgNVBAsM
BFBNRkExIDAeBgNVBAMMF1Rlc3QgU2VydmVyIENlcnRpZmljYXRlMSYwJAYJKoZI
hvcNAQkBFhd1c2VyQHJvY2tldHNvZnR3YXJlLmNvbTCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBAKztExGONN2YAxkcA9ke8ZvGdADONjqx/PfIDMa/M5Hc
xTHRLwcDG2KfqmTZ4h6ubNKrTSkrDkvc70OyWRSX0NvK/Nhn+lFfpA2T06ux6M0k
YsTIuWnx+OGKSXLZxx/EMDH3yQpl/jw6VM+e3phkjQRTCQiVZxC6frZGHBxKAHV8
HA1uDt0ZfRLDvvedBKAykp3yXliHldqOX25f1vYidE2lAkvYjgeY+ZNeEWeDJ907
kEzBJcUfyWD7DAJdpe2H69WeFP4SagZSNDe5c3ArxBbMze0h1To7EvEhbgGrUT3J
x54SYrOPU5f3K1fwKlL+t1VU1/oFLYqp8mpD04zDOTECAwEAAaOBhzCBhDAfBgNV
HSMEGDAWgBT1srcO1xrDm3tmOscXH0K1B3H/lDAJBgNVHRMEAjAAMAsGA1UdDwQE
AwIE8DBJBgNVHREEQjBAgiF3YWxkZXZwc2NhaXgzOC5yb2NrZXRzb2Z0d2FyZS5j
b22CDndhbGRldnBzY2FpeDM4ggsxMC4xNy41Ni44MzANBgkqhkiG9w0BAQsFAAOC
AQEARiXk29kkk7cYMcGW0N2Cxegs2sN5zYqkfm2DYswH4oedLi9UEp6nR87zCW0j
bI1NtxnKY9qSvOWf45GSpRDzR1bKH+z+XLbSDAOnSe59aTVEPRvOEAHSClxROuWX
k2GzbspuY81EeXzXTivPQNMl+xadSYuoEZ7QeTxfnlHrSW5id/uT/C2hsud3IKQH
TW/Ijv8U/FpKFsCcId4+cosW5w4VANUW2y6M5A3ontjeENiRTN+lSg3CFANG0p6i
9qToYlilhr1/3u3XQbaRxhzMy4W7avOE7ADQRfrdhHM5BBL5narMhTp9f3vtAV8j
lTylEV1+lgFkbGaM49eorw4Sag==
-----END CERTIFICATE-----
```

8. Convert the server certificate and private key to PKCS #12 format. Enter a password of your choice when prompted.

   ```
   openssl pkcs12 -export -chain -inkey test-server.key -CAfile
   myCA.pem -in test-server.pem -out test-server.pfx
   ```

   ```

   Enter Export Password:
   Verifying - Enter Export Password:
   ```

9. Configure the IBM MFA server to use this PKCS #12 server identity and passphrase.

   a) Use the secure copy (**scp**) command to copy the resulting file to the `/etc/security/mfa/certificates` directory on the IBM MFA server system.

   b) Change directory (cd) to /opt/IBM/MFA/bin.

   c) Create an input file of the following format:

   ```
   # initial trace level for MFA server
   INITIAL TRACE LEVEL=0

   # location of the P12 identity certificate for the MFA server
   P12 LOCATION=/etc/security/mfa/certificates/test-server.pfx

   # PKCS11 token used while encrypting P12 password
   PKCS11 TOKEN NAME=mfa

   # directory or PEM file containing CAs that will be trusted by the MFA server
   ```

```
CAS LOCATION=/etc/security/mfa/certificates/client.pem

# port to use for server-authentication
SERVER AUTH PORT=6793

# port to use for mutual authentication
MUTUAL AUTH PORT=6794

# port to use for ZVM Host communications
ZVM PORT=6787
```

d) Run the following command as root.

```
./azf_webserver_config input-file
```

See “Completing the server setup” on page 12 for complete information on the **azf_webserver_config** utility parameters.

10. Use the CA root certificate (*myCA.pem* in the examples) for the client trust store you create.

```

TRUSTEDCAS = /etc/security/mfa/certificates/myCA.pem
```

Chapter 16. IBM MFA messages

This section describes messages issued with IBM MFA message numbers.

A letter following the message number indicates the severity of the message:

I
Information.

W
Warning.

E
Error.

S
Severe

AZF1010E Supported tags: SIDUSERID

Explanation:
Invalid tag name specified. The supported tag name is the RSA User ID.

User response

Retry with valid tag.

AZF1011E SIDUSERID length must be <= 50

Explanation:
The RSA User ID must be fewer than 50 characters long.

User response

Retry with valid length.

AZF1100E TOTP PROVISIONING ERROR - NOTIFY ADMINISTRATOR

Explanation:
Your account is not correctly configured for TOTP.

User response

Notify your system administrator of the error.

AZF1101E TOTP CRYPTO ERROR - NOTIFY ADMINISTRATOR

Explanation:
Your account is not correctly configured for TOTP.

User response

Notify your system administrator of the error.

AZF1102E TOTP USER SUSPENDED - NOTIFY ADMINISTRATOR

Explanation:
Your user account is suspended.

User response

Notify your system administrator of the error.

AZF1103I TOTP PASSCODE REJECTED

Explanation:
This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF1103W TOTP REPLAY DENIED

Explanation:
Your TOTP OTP token cannot be reused. This message indicates that someone attempted to reuse the OTP token.

User response

Notify your system administrator of the error.

AZF1104I TOTP PASSCODE REJECTED

Explanation:
This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF1110I Various Messages

Explanation

This is a multiple-purpose message for configuration issues.

User response

Refer to the message text, and see the related chapter for configuration information.

AZF1112I **Valid REGSTATE changes: unset to OPEN; REVIEW to APPROVED**

Explanation

You specified an invalid REGSTATE value.

User response

Specify valid tag names.

AZF1300E **Valid tag names are REGSTATE, SUBJECT, and ISSUER**

Explanation

You specified an invalid tag name.

User response

Specify valid tag names.

AZF1301I **Certificate validation succeeded**

Explanation

This is an informational message.

User response

No response is required.

AZF1302E **Certificate validation failed**

Explanation

The certificate validation failed. The certificate must be valid. The complete client certificate chain must be present in the server's trust store.

User response

Import the complete client certificate chain.

AZF1303E **Your AZFCERT1 factor data is improperly configured, or missing tag data required for enrollment or certificate authentication**

Explanation

Your AZFCERT1 factor data is improperly configured.

User response

Configure IBM MFA for PIV/CAC or X.509 Certificate as described in "Configuring IBM MFA for PIV/CAC or X.509 Certificate authentication" on page 30.

AZF2100I **AZF main task started**

Explanation

The main task started. This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF2101I **Initialized recovery routine**

Explanation

The recovery routine was initialized. This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF2102I **Loaded authenticator**

Explanation

The authenticator was loaded. This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF2103I **Initialized PC routine**

Explanation

The PC routine was initialized. This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF2104I **Started web server**

Explanation

The web server has started.

User response

No response is required.

AZF2105I **Authentication request (*PC*)**

Explanation

This message contains the PC of the authentication request. This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF2106I **Tag validation request**

Explanation

Tag validation request. This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF2107I **Web request**

Explanation

The web services server received a request.

User response

No response is required.

AZF2108I **Authenticator entry point invoked**

Explanation

The authenticator entry point was invoked. This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF2109I **Authenticator initialized**

Explanation

The authenticator is initialized. This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF2110I **Started console receiver**

Explanation

The console receiver started. This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF2111I **Console received stop request**

Explanation

The console received a stop request. This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF2112I **Console received modify command**

Explanation

The console received a modify command. This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF2113I **Console command action**

Explanation

The console received a command action. This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF2114E **Unrecognized command**

Explanation

The user entered an unrecognized command.

User response

Correct the command and retry.

AZF2115I **Authenticator command**

Explanation

An authenticator command was entered. This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF2116E **Command processing failed**

Explanation

The user entered an invalid command.

User response

Correct the command and retry.

AZF2117E **Invalid trace level specified (valid levels are 0-3)"**

Explanation

You specified an invalid trace level.

User response

Valid trace levels are 0-3.

AZF2118I **AZF main task startup complete**

Explanation

The main task startup is complete. This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF2119I **Strict PCI compliant mode is enabled**

Explanation

IBM MFA supports the Payment Card Industry Data Security Standard (PCI DSS) standard through the Enable Strict PCI Compliance Mode setting. It is recommended that you do not enable this setting unless you are fully aware of the ramifications.

This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF2120I **Auth continuation requested (*network*)**

Explanation

The authentication continuation was requested at *network*. This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF2121I **Auth continuation requested (*PC*)**

Explanation

The authentication continuation was requested at *PC*. This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF2122I **AuthTxn Socket timeout**

Explanation

The authentication request timed out. This could be caused by load conditions.

User response

No response is required.

AZF2123I **Auth continued (*network*)**

Explanation

The authentication continues at *network*. This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF2124I **Auth continued (*PC*)**

Explanation

The authentication continues at *PC*. This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF2130I AuthTxn pruned from SocketTable

Explanation

An auth transaction was pruned, typically because a timeout occurred. This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF2131I AuthTxn pruned from PCTable

Explanation

An auth transaction was pruned, typically because a timeout occurred. This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF2132I WorkElement pruned

Explanation

A work element was pruned, typically because a timeout occurred. This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF2133E Entered purgeRequest

Explanation

A request was pruned, typically because a timeout occurred.

User response

No response is required.

AZF2134I Invoked sweep of expired Cache Token Credentials

Explanation

This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF2201I In-band auth success

Explanation

The authentication is successful. This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF2202W In-band auth failed

Explanation

The authentication request failed.

User response

Correct your credentials and retry the authentication request.

AZF2203E Auth eval failed (*missing authenticator*)

Explanation

The authentication evaluation failed.

User response

Contact IBM support.

AZF2204E Auth eval failed (*error from authenticator*)

Explanation

Authentication evaluation failed.

User response

Contact IBM support.

AZF2205E Auth eval failed (*R_Factor error*)

Explanation

Authentication evaluation failed.

User response

Contact IBM support.

AZF2207E Auth eval failed (*User MFA parse*)

Explanation

Authentication evaluation failed.

User response

Contact IBM support.

AZF2208E **Auth eval failed (*socket read*)**

Explanation

Authentication evaluation failed.

User response

Contact IBM support.

AZF2209E **Auth eval failed (*user has no active factors*)**

Explanation

The factor may have been deleted from the user after the authentication started, but before the server processed it.

User response

Make sure that the authentication factors are present.

AZF2210S **Authenticator returned an invalid code**

Explanation

Authenticator returned an invalid code

User response

Contact IBM support.

AZF2211E **Auth preparation failed, cannot evaluate**

Explanation

The factor may have been deleted from the user after the authentication started, but before the server processed it.

User response

Make sure that the authentication factors are present.

AZF2216E **Factor data or plugin not found for specified out-of-band factor**

Explanation

If you apply a policy to a user, the user must have all the factors defined in the policy, and those factors must be active for the user.

User response

Activate the user for the policy.

AZF2217E **Out-of-band factor inactive for user**

Explanation

If you apply a policy to a user, the user must have all the factors defined in the policy, and those factors must be active for the user.

User response

Activate the user for the policy.

AZF2221I **Out-of-band factor auth success**

Explanation

The authentication was successful.

User response

No response is required.

AZF2222W **Out-of-band factor auth failed**

Explanation

The authentication was unsuccessful.

User response

Activate the user for the policy.

AZF2223I **Out-of-band factor auth continuation requested (NMI)**

Explanation

"Need more information" messages indicate that additional information is needed after a successful authentication, such as the next token in next token mode. This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF2225I **Out-of-band factor auth continued (NMI)**

Explanation

"Need more information" messages indicate that additional information is needed after a successful authentication, such as the next token in next token mode. This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF2226I **User *%s* authenticated in-band with factor *%s***

Explanation

The in-band authentication was successful.

User response

No response is required.

AZF2227I **User *%s* denied access in-band by factor *%s***

Explanation

The in-band authentication was unsuccessful.

User response

Provision the user for IBM MFA as described in Chapter 8, “Provisioning IBM MFA users,” on page 49.

AZF2228I **AUTHENTICATION SUCCESSFUL**

Explanation

The user was successfully authenticated.

User response

No response is required.

AZF2229W **AUTHENTICATION FAILED**

Explanation

The user authentication failed.

User response

Verify the user credentials and retry the operation.

AZF2301I **Tag validation: valid**

Explanation

The tag validation is valid. This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF2303E **Tag eval failed (missing authenticator)**

Explanation

The tag evaluation failed.

User response

Contact IBM support.

AZF2304E **Tag eval failed (*error from authenticator*)**

Explanation

Tag evaluation failed.

User response

Contact IBM support.

AZF2305E **Tag eval failed (*R_Factor error*)**

Explanation

Tag evaluation failed.

User response

Contact IBM support.

AZF2306E **Tag eval failed (*TMFA parse*)**

Explanation

Tag evaluation failed.

User response

Contact IBM support.

AZF2307E **Tag eval failed (*User MFA parse*)**

Explanation

Tag evaluation failed.

User response

Contact IBM support.

AZF2308E **Tag eval: Unexpected MFAR function code**

Explanation

An internal error occurred.

User response

Contact IBM support.

AZF2309E Tag validation init failed in STC

Explanation

An internal error occurred.

User response

Examine the preceding messages in the log for additional details. Contact IBM support.

AZF2310E Tag validation detected duplicate tag names

Explanation

You entered duplicate tags.

User response

Correct the tags and re-enter.

AZF2401S Failed to initialize recovery routine

Explanation

The recovery routine initialization failed.

User response

Contact IBM support.

AZF2403E Failed to load authenticator

Explanation

The authenticator failed to load.

User response

Contact IBM support.

AZF2404E Failed to start web server

Explanation

The web server failed to start.

User response

Configure the IBM MFA server, as described in "Completing the server setup" on page 12.

AZF2405E Authenticator initialize failed

Explanation

The authenticator failed to initialize.

User response

Contact IBM support.

AZF2408I Authenticator not defined (MFADEF profile not defined)

Explanation

A supported plug-in is not enabled.

User response

No response is required.

AZF2409S No authenticators were initialized

Explanation

No authenticators were initialized.

User response

Contact IBM support.

AZF2416S No Multi-Factor authenticators were initialized

Explanation

No strong factors were initialized.

User response

Contact IBM support.

AZF2501S Entered recovery routine

Explanation

Informational message for the recovery routine.

User response

Capture output information and contact IBM support.

AZF2502S Out of memory

Explanation

This is a general memory error.

User response

Increase the memory and restart the IBM MFA server. If the problem persists, contact IBM support.

AZF2503S **Internal structure integrity**

Explanation

There is an issue with the internal structure of IBM MFA.

User response

Contact IBM support.

AZF2504S **Hashtable write error**

Explanation

There is an issue with the internal structure of IBM MFA.

User response

Contact IBM support.

AZF2505S **Hashtable remove error (item not present)**

Explanation

There is an issue with the internal structure of IBM MFA.

User response

Contact IBM support.

AZF2506S **Unexpected route**

Explanation

There is an issue with the internal structure of IBM MFA.

User response

Contact IBM support.

AZF2601E **No factors are active for the specified User ID**

Explanation

If you apply a policy to a user, the user must have all the factors defined in the policy, and those factors must be active.

User response

Configure the user as described in Chapter 8, "Provisioning IBM MFA users," on page 49.

AZF2603I **User *%s* authenticated to factor *%s***

Explanation

The authentication was successful.

User response

No response is required.

AZF2604I **User *%s* denied by factor *%s***

Explanation

The authentication was unsuccessful.

User response

Provision the user as described in Chapter 8, "Provisioning IBM MFA users," on page 49.

AZF2606E **Failed to listen on loopback address**

Explanation

A return code of 1115 indicates that the port is already in use by another application.

User response

Assign either the application or the IBM MFA server a different port number.

AZF2607I **Listening on loopback address**

Explanation

This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF2608E **Cannot respond without internal txnid**

Explanation

An internal error occurred that prevented the plug-in from processing the transaction.

User response

Contact IBM support.

AZF2609E **Failed to generate CTC**

Explanation

An internal error occurred that prevented the plug-in from generating a CTC.

User response

Contact IBM support.

AZF2610E Policy %s contains unusable factor %s

Explanation

Your factor data is improperly configured.

User response

Correct or clear the factor data for the affected user.

AZF3001E Error communicating with RSA Server

Explanation

Unable to send or receive messages to the RSA Authentication Manager and its replicas.

User response

Ensure that the RSA Authentication Manager is running and is reachable. For example, try pinging the Authentication Manager from the server system. If there are firewalls present, ensure the rules do not block traffic. If using VIPA (Virtual IP Address), make any necessary network configuration changes.

AZF3002W User must provide next tokencode

Explanation

After *n* number of failed login attempts followed by a successful login, where *n* is determined by your local RSA Authentication Manager security policy, the user may be prompted to also enter the next displayed token code for extra security. By successfully entering the next token code, the RSA Authentication Manager is able to verify that the user has possession of the assigned token.

Next token code mode requires the user to enter the **next** token code (or passcode) that is displayed. That is, the user must enter two successive codes to log in. If the user does not enter the next displayed token code or passcode, the login fails.

Note: Not all login applications indicate when the RSA SecurID "next token" mode is in effect. Because the number of unsuccessful login attempts that trigger "next token" mode can vary, the user may not know that the next token is also required.

User response

1. Wait for the token code you just used to change. If you are using a hardware token with a PINpad or a soft token, wait for the passcode you just used to change.
2. Get the 6- to 8-digit token code (or passcode) displayed by the SecurID token.
3. Enter the token code (or passcode) where prompted.
4. Press Enter.

AZF3003W User must create new PIN (*user generated only*)

Explanation

The RSA Authentication Manager is in "new PIN required" mode. The user must enter a new user-generated PIN.

Note: Not all login applications indicate when the RSA SecurID "new PIN required" mode is in effect. The user may not know that a new PIN is required.

User response

The user should follow the locally established rules for creating a valid PIN, including the number of characters, the reuse policy, and so forth. The PIN typically must be between four and eight characters.

After the user enters and confirms the new PIN, the user must log in again.

AZF3004W User must create new PIN (*system generated only*)

Explanation

The RSA Authentication Manager is in "new PIN required" mode and is set to require a system-generated PIN. The user must enter the system-generated PIN that is displayed.

Note: Not all login applications display the new system-generated PIN. The user may not know that this specific system-generated PIN is required.

User response

The user must enter and confirm the new system-generated PIN. The user must then log in again.

AZF3005W User must create new PIN (*user or system generated*)

Explanation

The RSA Authentication Manager is in "new PIN required" mode. The user must enter either a new user-generated or system-generated PIN.

Note: Not all login applications indicate when the RSA SecurID "new PIN required" mode is in effect. The user may not know that a new PIN is required, or see the system-generated PIN.

User response

The user should either use the system-generated PIN or follow the locally established rules for creating a valid PIN, including the number of characters, the reuse policy, and so forth. The PIN typically must be between four and eight characters.

The user must enter and confirm the new PIN. The user must then log in again.

AZF3006W **New PIN rejected**

Explanation

The new PIN the user entered was rejected.

User response

The user must follow the locally established rules for creating a valid PIN, including the number of characters, the reuse policy, and so forth. The PIN typically must be between four and eight characters.

AZF3007I **New PIN canceled**

Explanation

The new PIN operation was canceled.

User response

No response is required.

AZF3008I **New PIN accepted**

Explanation

The new PIN the user entered was accepted.

User response

Because the user changed the PIN, the user must log in again. The user should wait for the token code or passcode) displayed by the SecurID token to change.

AZF3012I **Authentication successful**

Explanation

The user was successfully authenticated.

User response

No response is required.

AZF3013W **Authentication successful (next tokencode)**

Explanation

After *n* number of failed login attempts followed by a successful login, where *n* is determined by your local RSA Authentication Manager security policy, the user was prompted to also enter the next displayed token code for extra security. By successfully entering the next token code, the RSA Authentication Manager is able to verify that the user has possession of the assigned token.

Next token code mode requires the user to enter the **next** token code (or passcode) that is displayed. That is, the user must enter two successive codes to log in. If the user does not enter the next displayed token code or passcode, the login fails.

Note: Not all login applications indicate when the RSA SecurID "next token" mode is in effect. Because the number of unsuccessful login attempts that trigger "next token" mode can vary, the user may not know that the next token is also required.

User response

1. Wait for the token code to change. If using a hardware token with a PINpad or a soft token, wait for the passcode to change.
2. Get the 6- to 8-digit token code (or passcode) displayed by the SecurID token.
3. Enter the token code (or passcode) where prompted.
4. Press Enter.

AZF3014W **Authentication denied**

Explanation

The RSA Authentication Manager has denied the authentication request.

User response

Verify the user credentials and retry the operation.

AZF3017I **Need new node secret**

Explanation

No node secret was found for this system. A new node secret will be created automatically after the first successful authentication.

User response

No response is required.

AZF3018S Failed to read SDCONF file

Explanation

Unable to read the SDCONF.REC file specified.

User response

Make sure that a valid SDCONF.REC file has been transferred to the server system in binary mode, and that it is present in the location specified. It must be readable by the IBM MFA server.

AZF3019I Successfully parsed SDCONF file

Explanation

The IBM MFA server successfully parsed the SDCONF.REC file specified.

User response

No response is required.

AZF3020S Failed to parse SDCONF file

Explanation

Unable to parse the SDCONF.REC file specified.

User response

Make sure that a valid SDCONF.REC file has been transferred to the IBM MFA server in binary mode, that it is present in the location specified, and that it is readable by the IBM MFA server.

AZF3021I AZFSIDP1 Initializing

Explanation

The AZFSIDP1 profile is initializing.

User response

No response is required.

AZF3022E New PIN protocol states mismatch, access denied

Explanation

Internal error during new PIN processing.

User response

Retry authentication.

AZF3023I Canceling authentication transaction

Explanation

The user canceled the authentication transaction.

User response

No response is required.

AZF3024E Internal error, bad plugin data

Explanation

An internal error occurred while processing the authentication.

User response

Restart the IBM MFA server.

AZF3025E Internal error, bad authTxn data

Explanation

An internal error occurred while processing the authentication.

User response

Restart the IBM MFA server.

AZF3026I Node secret was cleared

Explanation

The RSA node secret was cleared.

The RSA node secret is a shared secret known to IBM MFA and the RSA Authentication Manager. If this secret must be established (or re-established), your RSA Authentication Manager administrator will request that the node secret be cleared from the IBM MFA server.

User response

No response is required.

AZF3027W Potential node secret mismatch with server

Explanation

There is a potential node secret mismatch with the RSA Authentication Manager.

User response

Clear the node secret for this agent host in Authentication Manager and the IBM MFA server.

AZF3028S Failed to read SDOPTS file

Explanation

Unable to read the SDOPTS.REC file specified.

User response

Make sure that a valid SDOPTS.REC file has been transferred to the IBM MFA server in binary mode, and that it is present in the location specified. It must be readable by theIBM MFA server.

AZF3029I Successfully parsed SDOPTS file

Explanation

The IBM MFA server successfully parsed the SDOPTS.REC file specified.

User response

No response is required.

AZF3030S Failed to parse SDOPTS file

Explanation

Unable to parse the SDOPTS.REC file specified.

User response

Make sure that a valid SDOPTS.REC file has been transferred to the IBM MFA server in binary mode, that it is present in the location specified, and that it is readable by the IBM MFA server.

AZF3031S Unexpected transition from SEND_INIT

Explanation

Internal error.

User response

Contact IBM support.

AZF3032S Time packet synchronization failed

Explanation

Internal error.

User response

Contact IBM support.

AZF3033S No SDCONF.REC file specified in settings

Explanation

No SDCONF.REC file specified in settings.

User response

See "Configuring the RSA SecurID authentication method" on page 27.

AZF3034S No Node Secret file specified in settings

Explanation

No Node Secret file specified in settings

User response

See "Configuring the RSA SecurID authentication method" on page 27.

AZF3035S AZFSIDP1 failed to initialize

Explanation

Internal error.

User response

Contact IBM support.

AZF3036S Failed to initialize Node Secret

Explanation

The Node Secret was not initialized.

User response

Make sure the Node Secret file is specified in settings. See "Configuring the RSA SecurID authentication method" on page 27.

AZF3037E Settings required by AZFSIDP1 are missing

Explanation

Settings required by AZFSIDP1 are missing. One of the settings was not set correctly in the configuration.

User response

Configure IBM MFA for SecurID, as described in "Configuring the RSA SecurID authentication method" on page 27.

AZF3038E **Internal error, missing plugin state**

Explanation

An internal error occurred that prevented the plug-in from processing the transaction.

User response

Contact IBM support.

AZF3039E **Failed to build txn-specific state**

Explanation

An internal error occurred that prevented the plug-in from processing the transaction.

User response

Contact IBM support.

AZF3040E **Internal error, missing txn-specific state**

Explanation

An internal error occurred that prevented the plug-in from processing the transaction.

User response

Contact IBM support.

AZF3041E **Failed to restart network flow in response to a timeout**

Explanation

The plug-in was unable to communicate with the RSA Authentication Manager server.

User response

Check your network configuration, and ensure there is a viable network path between the host machine and the RSA Authentication Manager. Ensure that the RSA Authentication Manager is properly configured and available.

AZF3042E **Denying access due to a socket error**

Explanation

An internal error occurred that prevented the plug-in from processing the transaction.

User response

Contact IBM support.

AZF3043E **Failed to get network data or sender info**

Explanation

An internal error occurred that prevented the plug-in from correctly reading network data.

User response

Contact IBM support.

AZF3044E **CheckResponse returned FALSE**

Explanation

The response from the Authentication Manager was not correctly formatted. Refer to the message for more details.

User response

Ensure that the Authentication Manager is correctly configured, and that the node secret state is the same in both the plug-in and on the Authentication Manager.

AZF3045E **Internal error, state mismatch**

Explanation

An internal error occurred that prevented the plug-in from processing the transaction. Refer to the messages for more details.

User response

Contact IBM support.

AZF3046E **Failed to retry a network send**

Explanation

The plug-in was unable to communicate with the Authentication Manager. Refer to the message for more details.

User response

Check your network configuration, and ensure there is a viable network path between the host machine and the Authentication Manager. Ensure that the Authentication Manager is properly configured and available.

AZF3047E AZFSIDP1 statistics unavailable

Explanation

Statistics are available only if at least one authentication request has been processed.

User response

Perform at least one authentication before requesting statistics.

AZF3048E Suspect or invalid credential syntax

Explanation

An internal error occurred that caused the plug-in to create an invalid authentication request.

User response

Contact IBM support.

AZF3049E Unable to register transaction socket

Explanation

An internal error prevented the plug-in from creating a new network socket.

User response

Contact IBM support.

AZF3050I No node secret found for this system

Explanation

No node secret was found for this system. A new node secret will be created automatically after the first successful authentication.

User response

No response is required.

AZF3051S Unable to determine local IP Address, no SDOPTS override present

Explanation

The AZFSIDP1 factor cannot determine the IP address of the local system and is unable to read the IP address from the SDOPTS.REC file. In certain situations, such as a multi-homed LPAR, or a VIPA, it is possible that the host IP address that is auto-detected by the AZFSIDP1 plug-in does not match the IP address actually used for outgoing traffic. In such cases, use the CLIENT_IP override to manually specify the IP address that AZFSIDP1 should use.

User response

Make sure that a valid SDOPTS.REC file has been transferred to the IBM MFA server in binary mode, and that it is present in the location specified. It must be readable by the IBM MFA server.

AZF3054I AZFSIDP1 settings follow

Explanation

The AZFSIDP1 factor-wide settings are printed when the AZFSIDP1 factor is initialized during IBM MFA server startup, and are preceded by this message.

User response

No response is required.

AZF4001I AZFTOTP1 Authenticator init

Explanation

The AZFTOTP1 plug-in is initializing.

User response

No response is required.

AZF4002I AZFTOTP1 Authenticator deactivated

Explanation

The AZFTOTP1 plug-in is stopped.

User response

No response is required.

AZF4003I AZFTOTP1 Entry point

Explanation

This progress message is intended for use by support in the event of a problem.

User response

No response is required.

AZF4004E AZFTOTP1 Authenticator initialization failed

Explanation

The AZFTOTP1 plug-in could not initialize.

User response

Contact IBM support.

AZF4100E TOTP AuthTransactions cannot be canceled or continued

Explanation

This message indicates incorrect message routing inside the IBM MFA server and is not seen in normal circumstances.

User response

Shut down and restart the IBM MFA server.

AZF4101S Structure integrity check failed

Explanation

This message indicates memory corruption inside the IBM MFA server.

User response

Shut down and restart the IBM MFA server.

AZF4102I Starting TOTP auth processing

Explanation

This is an informational message that AZFTOTP1 authentication is starting.

User response

No response is required.

AZF4104I Finished TOTP auth processing

Explanation

This is an informational message that AZFTOTP1 authentication is finished.

User response

No response is required.

AZF4105E Failed to create TOTP User object

Explanation

The AZFTOTP1 factor data for a particular user ID is invalid.

User response

Correct or clear the AZFTOTP1 factor data for the affected user.

AZF4107I TOTP Passcode Rejected

Explanation

The TOTP passcode the user entered was rejected, most likely because the passcode was entered incorrectly or was outside of the authentication window.

User response

The user should wait for the TOTP passcode to change and try again.

AZF4108W TOTP Replay prevention

Explanation

The AZFTOTP1 plug-in prevented a previously-used TOTP passcode from being reused.

User response

Ensure that the passcode reuse was a user error and not the result of a replay attack.

AZF4110E TOTP User object validation failed

Explanation

The AZFTOTP1 factor data for a particular user ID is invalid.

User response

Clear and re-provision the AZFTOTP1 factor data for the affected user, as described in Chapter 8, “Provisioning IBM MFA users,” on page 49.

AZF4111E TOTP User object has invalid REGSTATE

Explanation

When you register a user for TOTP, you set the registration state to OPEN. (Case is sensitive.) TOTP then changes the registration state to PROVISIONED when an TOTP account is created for the user on the iOS device.

User response

Specify a valid registration state.

AZF4112E **TOTP User object is missing KEYLABEL**

Explanation

When TOTP changes the registration state to PROVISIONED, a keylabel is created automatically. This message can occur if you deactivated the user for TOTP and cleared all tags for that user.

User response

Re-register the user as described in Chapter 8, "Provisioning IBM MFA users," on page 49.

AZF4113E **TOTP User object has invalid ALG**

Explanation

When you configure a user for TOTP, you can set the digest algorithm used to generate the one-time password. Valid options include SHA1, SHA256, SHA384, and SHA512. (Case is sensitive.) This overrides the default settings.

User response

Set a valid digest algorithm, as described in "Configuring the TOTP authentication method" on page 33.

AZF4114E **TOTP User object has invalid NUMDIGITS**

Explanation

When you configure a user for TOTP, you can set the number of digits used to generate the one-time password. Valid options are 6 - 8 digits. This overrides the default settings.

User response

Set a valid number of digits, as described in "Configuring the TOTP authentication method" on page 33.

AZF4115E **TOTP User object has invalid PERIOD**

Explanation

When you configure a user for TOTP, you can set the number of seconds an interval lasts. This number determines how long a one-time password is active before the next one-time password generates. Valid values are 15 seconds, 30 seconds, and 60 seconds. This overrides the default settings.

User response

Set a valid period, as described in "Configuring the TOTP authentication method" on page 33.

AZF4116E **Error validating TOTP passcode**

Explanation

A user's TOTP passcode could not be validated due to an underlying library error. This message will include the relevant PKCS#11 return and reason codes, if applicable.

User response

See the PKCS#11 return and reason codes.

AZF4117I **TOTP Passcode Accepted**

Explanation

The TOTP passcode the user entered was accepted.

User response

No response is required.

AZF4118W **User's tags are now invalid; verify AZFTOTP1 is INACTIVE**

Explanation

You specified an invalid tag name.

User response

Set AZFTOTP1 to INACTIVE for the user until you specify valid tag names, as described in "Configuring users for TOTP authentication" on page 55.

AZF4120I **Defaulting TOTP algorithm**

Explanation

When you configure a user for TOTP, you can set the digest algorithm used to generate the one-time password. Valid options include SHA1, SHA256, SHA384, and SHA512. (Case is sensitive.) This overrides the default settings. If you do not set the digest algorithm, the default setting is used.

User response

No response is required.

AZF4121I **Defaulting TOTP digits**

Explanation

When you configure a user for TOTP, you can set the number of digits used to generate the one-time password. If you do not set the number of digits, the default setting is used.

User response

No response is required.

AZF4122I **Defaulting TOTP period**

Explanation

When you configure a user for TOTP, you can set the number of seconds an interval lasts. This number determines how long a one-time password is active before the next one-time password generates. If you do not set the period, the default setting is used.

User response

No response is required.

AZF4123I **Defaulting TOTP window**

Explanation

When you configure a user for TOTP, you can set the window skew interval. If you do not set the window, the default setting is used.

User response

No response is required.

AZF4124E **AZFTOTP1 factor-wide settings are missing or invalid**

Explanation

The AZFTOTP1 factor-wide settings are missing or invalid.

User response

Configure the AZFTOTP1 factor-wide settings, as described in “Configuring the TOTP authentication method” on page 33.

AZF4125W **Failed to update user's CVALUE, replay protection inop**

Explanation

After validating a user’s TOTP passcode, AZFTOTP1 failed to update the user’s factor data to indicate their latest CVALUE. This value is updated to prevent a passcode from being reused by an attacker.

User response

Contact IBM support.

AZF4126I **AZFTOTP1 settings follow**

Explanation

The AZFTOTP1 factor-wide settings are printed when the AZFTOTP1 factor is initialized during IBM MFA server startup, and are preceded by this message.

User response

No response is required.

AZF4127E **Failed to read AZFTOTP1 settings**

Explanation

AZFTOTP1 settings could not be retrieved.

User response

Configure AZFTOTP1, as described in “Configuring the TOTP authentication method” on page 33.

AZF4128W **Runtime settings were not changed**

Explanation

If it is determined during command processing that incoming AZFTOTP1 settings are invalid, those settings will not be applied.

User response

Correct the invalid settings.

AZF4131I **Validated TOTP User**

Explanation

The user was validated.

User response

No response is required.

AZF4132I **Matched TOTP counter value**

Explanation

This is an informational message.

User response

No response is required.

AZF4140E PKCS#11 token name is missing from AZFTOTP1 settings

Explanation

The PKCS#11 token name is missing from the IBM MFA server settings.

User response

Configure the IBM MFA server.

AZF4141E Failed to get PKCS#11 environment info

Explanation:
The PKCS#11 environment could not be obtained.

User response:
Configure the PKCS#11 token, as described in“Configuring a PKCS#11 token” on page 9.

AZF4142E The named PKCS#11 token was not accessible

Explanation

The PKCS#11 token name specified in the IBM MFA server settings is not accessible.

User response

Configure the PKCS#11 token, as described in “Configuring a PKCS#11 token” on page 9.

AZF4143I Description of accessible PKCS#11 environment follows:

Explanation

This is an informational message generated as part of normal processing.

User response

No response is required.

AZF4144E A user's TOTP key object was not found

Explanation

When TOTP changes the registration state to PROVISIONED, a keylabel is created automatically. This message can occur if you deactivated the user for TOTP and cleared all tags for that user.

User response

Re-register the user, as described in “Enabling users for TOTP authentication” on page 55.

AZF4145E Multiple TOTP key objects were found for the same KEYLABEL

Explanation

When TOTP changes the registration state to PROVISIONED, a keylabel is created automatically.

User response

Re-register the user, as described in “Enabling users for TOTP authentication” on page 55.

AZF4146W Failed to delete a key object from the PKCS#11 token

Explanation

A user’s factor data contained a label tag value, and multiple PKCS#11 key records were returned for the specified label value.

User response

Clear the user’s factor data, return them to REGSTATE:OPEN state, and instruct them to re-enroll their IBM TouchToken for iOS account, as described in “Enabling users for TOTP authentication” on page 55.

AZF4147I Deleted tags include KEYLABEL

Explanation

When TOTP changes the registration state to PROVISIONED, a keylabel is created automatically. This message can occur if you deactivated the user for TOTP and cleared all tags for that user.

User response

Re-register the user, as described in “Enabling users for TOTP authentication” on page 55.

AZF4150W Tag eval failed to translate a local status to PC return/reason pair

Explanation

The local error cannot be translated to be more meaningful.

User response

Check your inputs to make sure you specified tags and values as documented.

AZF4160I Suspending TOTP user for consecutive failures

Explanation

The user has exceeded the revoke count that you configured.

User response

The user is unable to authenticate with TOTP until you reset them.

AZF4161E Failed to update TOTP user data; brute-force protection inoperative

Explanation

The revoke count could not be configured.

User response

Configure the revoke count.

AZF5001I IBM TouchToken Registration Web Services

Explanation

This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF5002I Server base init success

Explanation

The IBM MFA server is successfully initializing.

User response

No response is required.

AZF5003E Server base init error

Explanation

The IBM MFA server did not successfully initialize.

User response

Contact IBM support.

AZF5004S Failed to initialize the services shared context

Explanation

Fatal error on startup, possibly due to missing or invalid AZFTOTP1 settings.

User response

Configure TOTP as described in "Configuring the TOTP authentication method" on page 33.

AZF5006S AZFTOTP1 or IBM MFA server settings could not be read; Cannot start Registration Services

Explanation

The AZFTOTP1 or IBM MFA server settings are missing or invalid.

User response

Configure the IBM MFA server settings, as described in Chapter 5, "Configuring server options," on page 23. Configure the AZFTOTP1 settings, as described in "Configuring the TOTP authentication method" on page 33.

AZF5007S A required parameter is missing from the IBM MFA server settings, or PKCS#11 init failed

Explanation

An IBM MFA server setting is missing or is invalid, or the PKCS#11 initialization failed.

User response

Configure PKCS#11 as described in "Configuring a PKCS#11 token" on page 9. Configure the IBM MFA server settings, as described in Chapter 5, "Configuring server options," on page 23.

AZF5008S Failed to initialize one or more web services

Explanation

Fatal error on startup, possibly due to missing or invalid AZFTOTP1 settings.

User response

Configure TOTP as described in "Configuring the TOTP authentication method" on page 33.

AZF5009I **AZFTOTP1 settings follow:**

Explanation

This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF5011E **Server-auth TLS port number is missing from IBM MFA server settings**

Explanation

The server authentication port setting is missing.

User response

Configure the server authentication port, as described in Chapter 5, "Configuring server options," on page 23.

AZF5012E **PKCS#11 token name is missing from IBM MFA server settings**

Explanation

The PKCS#11 token name is missing.

User response

Enter the PKCS#11 token name, as described in "Configuring a PKCS#11 token" on page 9.

AZF5014I **Will declare the following Realm name to clients**

Explanation

AZFTOTP1 will use this realm name for your IBM MFA server. This is an arbitrary name of your choosing.

User response

No response is required.

AZF5015I **web services server using trace level**

Explanation

The IBM MFA server is using the trace level. Valid values are 0 through 3, where the higher number increases the level of verbosity.

User response

No response is required.

AZF5020E **The enrollCheck service saw a request with zero content length**

Explanation

A request was made to a valid registration web server URL, but the body of the request was invalid because it was empty. Either a connection to a valid client was dropped by the network infrastructure, or an unexpected client is issuing requests to the web services server.

User response

Make sure that the user's Apple iOS device has network connectivity to the web services server, as described in "Enabling users for TOTP authentication" on page 55.

AZF5021E **Received an enrollCheck request that was malformed or missing parameters**

Explanation

A request was made to a valid registration web server URL, but the body of the request was invalid because it was empty. Either a connection to a valid client was dropped by the network infrastructure, or an unexpected client is issuing requests to the web services server.

User response

Make sure that the user's Apple iOS device has network connectivity to the web services server, as described in "Enabling users for TOTP authentication" on page 55.

AZF5023E **Enrollment check returning Not Authorized**

Explanation

A client contacted the IBM MFA server to determine whether a user may enroll a new account, but the client provided an invalid combination of User ID and Password or Passphrase.

User response

Instruct users to open the IBM MFA server start page using Mobile Safari on their iOS device and log in with their user name and password.

AZF5024E Enrollment check responding with following error

Explanation

A client contacted the IBM MFA server to determine whether a user may enroll a new TouchToken Account, and the IBM MFA server is responding as described.

User response

See the accompanying error for more information.

AZF5025I Enrollment check responding success

Explanation

A client contacted the IBM MFA server to determine whether a user may enroll a new account, and the IBM MFA server is responding that the user in question may proceed with enrollment.

User response

No response is required.

AZF5026I Found existing invitation

Explanation

A client contacted the IBM MFA server to retrieve TOTP token details, and the server located a preexisting internal structure describing a partial token for the given user.

User response

No response is required.

AZF5027I Created new invitation

Explanation

A client contacted the IBM MFA server to retrieve TOTP token details, and the server created a new internal structure describing a partial token for the given user.

User response

No response is required.

AZF5028E Failed to retrieve AZFTOTP user object

Explanation

A client contacted the IBM MFA server to determine whether a user may enroll a new account, and the IBM MFA server failed to locate valid AZFTOTP1 configuration for that user.

User response

Configure the user account, as described in "Enabling users for TOTP authentication" on page 55.

AZF5029I Invite code

Explanation

This is an internal progress message to aid support in the event that a problem requires diagnosis.

User response

No response is required.

AZF5031I Generated candidate keylabel

Explanation

This message displays the label to be applied to the PKCS#11 key record for a user's newly-enrolled account.

User response

No response is required.

AZF5032E Base64 encoding failed

Explanation

This is unlikely to occur unless there is an out of memory issue. If the server is still up and emitting this message, restart it.

User response

Restart the IBM MFA server.

AZF5033E Invitation not found

Explanation

A client tried to retrieve an account specification from the server, but specified an account identifier that did not match any specification pending output in the server. Something other than the IBM TouchToken for iOS application may be issuing requests to the server URL space.

User response

Determine which application is trying to connect to the IBM MFA server.

AZF5034I **Retrieved an invitation and will promote it**

Explanation

This is a progress message to aid in support in the event of a problem.

User response

No response is required.

AZF5035E **Invitation in invalid state will be destroyed; user must restart enrollment**

Explanation

A previous error caused an account specification to become unusable, so it will not be used.

User response

The user attempting to enroll a new IBM TouchToken for iOS account should restart the enrollment process in the application.

AZF5036E **Invitation promotion failed**

Explanation

The server failed to infuse a IBM TouchToken for iOS account specification with required data.

User response

See other errors in the log.

AZF5037E **JSON encoding failed**

Explanation

Unlikely to occur unless out of memory.

User response

If the IBM MFA server is still up and emitting this message, restart it.

AZF5038I **Tokenspec retrieval responding success**

Explanation

Progress message to aid in support in the event of a problem.

User response

No response is required.

AZF5040I **Entered preflight**

Explanation

Progress message to aid in support in the event of a problem.

User response

No response is required.

AZF5041E **Preflight account metadata not found**

Explanation

A client attempted to contact the preflight service URL space, but provided no valid short-lived account identifier. An internal error has occurred, a network error has occurred, or a client other than the IBM TouchToken for iOS application may be contacting the registration server.

User response

Contact IBM support.

AZF5042E **Preflight saw invalid account metadata**

Explanation

A client attempted to contact the preflight service URL space, but provided no valid short-lived account identifier. An internal error has occurred, a network error has occurred, or a client other than the IBM TouchToken for iOS application may be contacting the registration server.

User response

Contact IBM support.

AZF5043E **Preflight failed to match the provided token code**

Explanation

The TOTP value provided by the client did not match any of the allowed values, possible due to clock skew between the client application and the server.

User response

Consider increasing the default Window value in the AZFTOTP1 factor, then instruct the affected user to re-attempt IBM TouchToken for iOS account enrollment.

AZF5043I **If using a short PERIOD value, try increasing WINDOW to reduce clock skew effects**

Explanation

Token Period is the time (in seconds) between changes in value for the token. This number determines how long a one-time password is active before the next one-time password generates. The Window skew interval considers any possible synchronization delay between the server and the client that generates the one-time password. If Token Period and Window are both short, the user may not have sufficient time to enter the passcode.

User response

Increase the Window value if needed.

AZF5044I **Preflight will commit and activate AZFTOTP1**

Explanation

A user has completed IBM TouchToken for iOS account enrollment and should begin using this account to access IBM MFA-protected systems.

User response

No response is required.

AZF5046E **Failed to convert user secret to session HMAC key (*rc=*, *rsn=*)**

Explanation

The hash message authentication code (HMAC) key could not be created.

User response

Configure the PKCS#11 token.

AZF5050I **Console listener task starting up**

Explanation

The console listener task is starting up. This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF5051I **Stop command received**

Explanation

This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF5052I **Modify command received**

Explanation

This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF5053E **Modify command was not recognized**

Explanation

The **`Modify`** command was not recognized.

User response

Use the IBM MFA server configuration settings to set the trace level.

AZF5054E **Invalid trace level specified (valid levels are 0-3)**

Explanation

You specified an invalid trace level.

User response

Enter a valid trace level.

AZF5055E **Modify command processing failed**

Explanation

The **`Modify`** command processing failed.

User response

Use the IBM MFA server configuration settings to set the trace level.

AZF5056I **Modify command action**

Explanation

This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF5101S Structure integrity check failed

Explanation

A serious internal error has occurred.

User response

Restart the IBM MFA server.

AZF5105E Failed to create AZFTOTP User object

Explanation

A user's AZFTOTP1 factor data was not present, or contained values that prevented the creation of a validated user object.

User response

Clear the user's AZFTOTP1 factor data and set their REGSTATE tag to OPEN, as described in "Enabling users for TOTP authentication" on page 55.

AZF5107I TOTP Passcode Rejected

Explanation

The TOTP passcode the user entered was rejected, most likely because the passcode was entered incorrectly or was outside of the Window skew interval, as described in "Configuring the TOTP authentication method" on page 33.

User response

The user should wait for the TOTP passcode to change and try again.

AZF5108W TOTP Replay prevention

Explanation

The AZFTOTP1 plug-in prevented a previously-used TOTP passcode from being reused.

User response

Ensure that the passcode reuse was a user error and not the result of a replay attack.

AZF5110E TOTP User object validation failed

Explanation

A user's AZFTOTP1 factor data contained values that prevented the creation of a validated user object.

User response

Clear the user's AZFTOTP1 factor data and set their REGSTATE tag to OPEN, as described in "Enabling users for TOTP authentication" on page 55.

AZF5111E TOTP User object has invalid REGSTATE

Explanation

When you register a user for TOTP, you set the registration state to OPEN. (Case is sensitive.) TOTP then changes the registration state to PROVISIONED when an TOTP account is created for the user on the iOS device.

User response

Specify a valid registration state.

AZF5112E TOTP User object is missing KEYLABEL

Explanation

When TOTP changes the registration state to PROVISIONED, a keylabel is created automatically. This message can occur if you deactivated the user forTOTP and cleared all tags for that user.

User response

Re-register the user as described in "Enabling users for TOTP authentication" on page 55.

AZF5113E TOTP User object has invalid ALG

Explanation

When you configure a user for TOTP, you can set the digest algorithm used to generate the one-time password. Valid options include SHA256, SHA384, and SHA512. (Case is sensitive.) This overrides the default settings.

User response

Set a valid digest algorithm, as described in "Configuring the TOTP authentication method" on page 33.

AZF5116E **Error validating TOTP passcode**

Explanation

A client accessed the preflight service, but the server was unable to verify whether the supplied TOTP passcode was matched by one of the allowed values. This indicates a configuration problem or a serious error in an underlying service.

User response

Check the AZFTOTP1 configuration, restart the server, and contact IBM support if the problem persists.

AZF5117I **TOTP Passcode Accepted**

Explanation

The TOTP passcode the user entered was accepted.

User response

No response is required.

AZF5120I **Defaulting TOTP algorithm**

Explanation

When you configure a user for TOTP, you can set the digest algorithm used to generate the one-time password. Valid options include SHA256, SHA384, and SHA512. (Case is sensitive.) This overrides the default settings. If you do not set the digest algorithm, the default setting is used.

User response

No response is required.

AZF5121I **Defaulting TOTP digits**

Explanation

When you configure a user for TOTP, you can set the number of digits used to generate the one-time password. If you do not set the number of digits, the default setting is used.

User response

No response is required.

AZF5122I **Defaulting TOTP period**

Explanation

When you configure a user for TOTP, you can set the number of seconds an interval lasts. This number determines how long a one-time password is active before the next one-time password generates. If you do not set the period, the default setting is used.

User response

No response is required.

AZF5123I **Defaulting TOTP window**

Explanation

When you configure a user for TOTP, you can set the window skew interval. If you do not set the window, the default setting is used.

User response

No response is required.

AZF5124E **AZFTOTP1 factor-wide settings are missing or invalid**

Explanation

The AZFTOTP1 factor-wide settings are missing or invalid.

User response

Configure the AZFTOTP1 settings, as described in "Configuring the TOTP authentication method" on page 33.

AZF5141E **Failed to get PKCS#11 environment info**

Explanation

This is a serious error that will prevent the web services server from functioning.

User response

Check the AZFTOTP1 configuration and restart the IBM MFA server.

AZF5142E **The named PKCS#11 token was not accessible**

Explanation

The named PKCS#11 token is not accessible.

User response

Check the token name configured in the IBM MFA server settings.

AZF5143I **Description of accessible PKCS#11 environment follows:**

Explanation

Subsequent messages in the log describe which PKCS#11 tokens were accessible by the registration server.

User response

See the following messages in the log for a description of which PKCS#11 tokens were accessible by the IBM MFA server. If the displayed list does not contain the configured PKCS#11 token name, the IBM MFA server will not function.

AZF5144E **A required PKCS#11 key object was not found**

Explanation

A user's factor data contained a label tag value, but a PKCS#11 key record with that label was not found. The PKCS#11 token name in the settings may have recently been changed to an invalid value.

User response

Configure the PKCS#11 token name in the IBM MFA settings.

AZF5145E **Multiple TOTP key objects were found for the same label**

Explanation

A user's factor data contained a label tag value, and multiple PKCS#11 key records were returned for the specified label value.

User response

Clear the user's factor data, return them to REGSTATE:OPEN state, and instruct them to re-enroll their IBM TouchToken for iOS account, as described in "Enabling users for TOTP authentication" on page 55.

AZF5146W **Failed to delete a key object from the PKCS#11 token**

Explanation

A user's factor data contained a label tag value, and multiple PKCS#11 key records were returned for the specified label value.

User response

Clear the user's factor data, return them to REGSTATE:OPEN state, and instruct them to re-enroll their IBM TouchToken for iOS account, as described in "Enabling users for TOTP authentication" on page 55.

AZF5153E **Failed to generate random bytes**

Explanation

The PKCS#11 token was deleted after the task successfully started.

User response

Configure a PKCS#11 token, as described in "Configuring a PKCS#11 token" on page 9.

AZF5154E **Failed to create a PKCS#11 HMAC key from raw bytes**

Explanation

The hash message authentication code (HMAC) key could not be created.

User response

Configure the PKCS#11 token, as described in "Configuring a PKCS#11 token" on page 9.

AZF5155E **Error checking token code**

Explanation

The PKCS#11 AES key could not be created.

User response

Configure the PKCS#11 token, as described in "Configuring a PKCS#11 token" on page 9.

AZF5156I **Created PKCS#11 AES key successfully**

Explanation

The PKCS#11 AES key was created. This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF5157I **Found PKCS#11 token**

Explanation

The PKCS#11 token was found. This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF5158I Found PKCS#11 AES key

Explanation

The PKCS#11 AES key was found. This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF5160E Failed to commit a user's AZFTOTP1 factor data

Explanation

TOTP was unable to commit the user's factor data.

User response

Contact IBM support.

AZF5161E Service unavailable

Explanation

You may have entered an invalid user ID on the IBM MFA Out-of-Band login page.

User response

Verify the user ID and retry.

AZF5161I Committed AZFTOTP1 user factor data, and set ACTIVE

Explanation

TOTP committed the user's factor data and set the factor to active. This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF5170E Required data was missing from the request

Explanation

The user is not correctly configured for TOTP.

User response

See “Enabling users for TOTP authentication” on page 55 for the steps to follow to register a user.

AZF5171E Authentication failed

Explanation

The AZFTOTP1 factor must be marked NOACTIVE for registration. The IBM MFA server checks the user's password. If AZFTOTP1 is active at the time the password check occurs, it will fail.

User response

See “Enabling users for TOTP authentication” on page 55 for the steps to follow to register a user.

AZF5172E An internal error prevented the server from verifying user eligibility

Explanation

An internal error occurred.

User response

Contact IBM support.

AZF5173E The specified User ID is not currently eligible for TouchToken Account enrollment

Explanation

The specified user ID cannot currently be enrolled due to a configuration error.

User response

See “Enabling users for TOTP authentication” on page 55 for the steps to follow to register a user.

AZF5174E Existing AZFTOTP1 factor data for the specified User ID failed validation

Explanation

The specified user ID failed validation, possibly due to a configuration error.

User response

See “Enabling users for TOTP authentication” on page 55 for the steps to follow to register a user.

AZF5175I The specified User ID has already enrolled a TouchToken Account; existing Account details must be cleared by an administrator before a new Account may be enrolled

Explanation

The user attempted to create a TOTP account and one already exists.

User response

You typically do not need to re-register a user for TOTP. If you do need to do so, follow the steps described in "Enabling users for TOTP authentication" on page 55.

AZF5176E The specified User ID is eligible for TouchToken enrollment, but an internal server error prevented enrollment from proceeding

Explanation

An internal server error prevented the user account from being enrolled.

User response

Contact IBM support.

AZF5177E An internal server error prevented enrollment of your new TouchToken Account

Explanation

An internal server error prevented the user account from being enrolled.

User response

Contact IBM support.

AZF5178E The token code sent to the server was invalid or out of range, retry enrollment and contact an administrator if this problem persists

Explanation

The token code provided by the user is invalid, possibly due to a configuration error.

User response

See "Enabling users for TOTP authentication" on page 55 for the steps to follow to register a user.

AZF6001I IBM Multi-Factor Authentication Web Services

Explanation

This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF6002I Server base init success

Explanation

The IBM MFA server is successfully initializing.

User response

No response is required.

AZF6003E Server base init error

Explanation

The IBM MFA server did not successfully initialize.

User response

Contact IBM support.

AZF6004S Failed to initialize the services shared context

Explanation

Fatal error on startup, possibly due to missing or invalid settings.

User response

Configure IBM MFA server, as described in Chapter 5, "Configuring server options," on page 23.

AZF6006S AZFTOTP1 token registration services disabled

Explanation

The AZFTOTP1 settings are missing or invalid.

User response

Configure the AZFTOTP1 settings, as described in "Configuring the TOTP authentication method" on page 33.

AZF6007S **A required parameter is missing from the settings, or PKCS#11 init failed**

Explanation

A factor-wide setting is missing or is invalid, or the PKCS#11 initialization failed.

User response

Configure PKCS#11 as described in "Configuring a PKCS#11 token" on page 9. Configure the IBM MFA server settings, as described in Chapter 5, "Configuring server options," on page 23.

AZF6008S **Failed to initialize one or more web services**

Explanation

Fatal error on startup, possibly due to missing or invalid settings.

User response

Configure the IBM MFA server settings, as described in Chapter 5, "Configuring server options," on page 23.

AZF6009I **Settings follow:**

Explanation

This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF6010E **Failed to read AZF settings**

Explanation

The IBM MFA server settings are missing.

User response

Configure IBM MFA server as described in Chapter 5, "Configuring server options," on page 23.

AZF6011E **No web services are enabled in the AZF settings; shutting down**

Explanation

The IBM MFA settings are missing.

User response

Configure IBM MFA server as described in Chapter 5, "Configuring server options," on page 23.

AZF6012I **IBM Multi-Factor Authentication Web Services startup complete**

Explanation

The main IBM MFA server startup is complete. This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF6012E **PKCS#11 token name is missing from AZFSTC settings**

Explanation

The PKCS#11 token name is missing.

User response

Enter the PKCS#11 token name, as described in "Configuring a PKCS#11 token" on page 9.

AZF6012W **The auto-detected hostname did not match the configured hostname**

Explanation

The auto-detected hostname did not match the configured hostname.

User response

Check the log for the IBM MFA server to determine which host name was used. Contact IBM support if the host name is configured correctly.

AZF6013W **IP address for the autodetected hostname did not match the IP address for the configured hostname**

Explanation

The auto-detected IP address did not match the configured hostname

User response

Check the log for the IBM MFA server to determine which host name was used. Contact IBM support if the configured IP address is correct.

AZF6014I IP address for the autodetected hostname matched the IP address for the configured hostname

Explanation

The IP address for the auto-detected hostname matched the IP address for the configured hostname.

User response

No response is required.

AZF6020E Failed to initialize OOBSvcsClient

Explanation

The IBM MFA Out-of-Band services failed to initialize.

User response

Make sure that the IBM MFA server is configured.

AZF6030I Console listener task starting up

Explanation

This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF 6031I Stop command received

Explanation

This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF 6032I Modify command received

Explanation

This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF 6033E Modify command was not recognized

Explanation

The **`Modify`** command was not recognized.

User response

Use the server configuration settings to set the trace level.

AZF6034E Invalid trace level specified (valid levels are 0-3)

Explanation

You specified an invalid trace level.

User response

Enter a valid trace level.

AZF6035E Modify command processing failed

Explanation

The **`Modify`** command processing failed.

User response

Correct the format of the **`Modify`** command.

AZF6036I Modify command action

Explanation

This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF6050I Console listener task starting up

Explanation

The console listener task is starting up. This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF6051I Stop command received

Explanation

This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF6052I Modify command received

Explanation

This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF6053E Modify command was not recognized

Explanation

The **`Modify`** command was not recognized.

User response

Set the trace level as described in Chapter 5, “Configuring server options,” on page 23.

AZF6054E Invalid trace level specified (valid levels are 0-3)

Explanation

You specified an invalid trace level.

User response

Enter a valid trace level.

AZF6055E Modify command processing failed

Explanation

The **`Modify`** command processing failed.

User response

Set the trace level as described in Chapter 5, “Configuring server options,” on page 23.

AZF6056I Modify command action

Explanation

This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF6141E Failed to get PKCS#11 environment info

Explanation

This is a serious error that will prevent the IBM MFA server from functioning.

User response

Check the IBM MFA configuration and restart the IBM MFA server.

AZF6142E The named PKCS#11 token was not accessible

Explanation

The named PKCS#11 token is not accessible.

User response

Check the token name configured in the IBM MFA settings.

AZF6143I Description of accessible PKCS#11 environment follows:

Explanation

Subsequent messages in the log describe which PKCS#11 tokens were accessible by the registration server.

User response

See the following messages in the log for a description of which PKCS#11 tokens were accessible by the IBM MFA server. If the displayed list does not contain the configured PKCS#11 token name, the IBM MFA server will not function.

AZF6144E A required PKCS#11 key object was not found

Explanation

A user’s factor data contained a label tag value, but a PKCS#11 key record with that label was not found. The PKCS#11 token name in the settings may have recently been changed to an invalid value.

User response

Configure the PKCS#11 token name in the IBM MFA settings.

AZF6145E Multiple PKCS#11 key objects were found for the same label

Explanation

A user’s factor data contained a label tag value, and multiple PKCS#11 key records were returned for the specified label value.

User response

Check the configured key label in the associated factor.

AZF6146W Failed to delete a key object from the PKCS#11 token

Explanation

A user’s factor data contained a label tag value, and multiple PKCS#11 key records were returned for the specified label value.

User response

Clear the user's factor data for the affected factor. For TOTP, clear the user's factor data for the affected factor, return them to REGSTATE:OPEN state, and instruct them to re-enroll their IBM TouchToken for iOS account, as described in “Enabling users for TOTP authentication” on page 55.

AZF6153E Failed to generate random bytes

Explanation

The PKCS#11 token was deleted after the task successfully started.

User response

Configure a PKCS#11 token, as described in “Configuring a PKCS#11 token” on page 9.

AZF6154E Failed to create a PKCS#11 HMAC key

Explanation

The hash message authentication code (HMAC) key could not be created.

User response

Configure the PKCS#11 token, as described in “Configuring a PKCS#11 token” on page 9.

AZF6155E Failed to create a PKCS#11 AES key

Explanation

The PKCS#11 AES key could not be created.

User response

Configure the PKCS#11 token, as described in “Configuring a PKCS#11 token” on page 9.

AZF6156I Created PKCS#11 AES key successfully

Explanation

The PKCS#11 AES key was created. This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF6157I Found PKCS#11 token

Explanation

The PKCS#11 token was found. This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF6158I Found PKCS#11 AES key

Explanation

The PKCS#11 AES key was found. This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF6160E Error while authenticating user

Explanation

IBM MFA was unable to authenticate the user.

User response

Contact IBM support.

AZF6161E Service unavailable

Explanation

You may have entered an invalid user ID on the IBM MFA Out-of-Band login page.

User response

Verify the user ID and retry.

AZF6162E Failed to authentication user via PAM

Explanation

You might have entered an invalid user ID on the IBM MFA Out-of-Band login page.

User response

Verify the user ID and retry.

AZF6165I Yubikey enrollment services initialized

Explanation

This is an informational message generated as part of processing.

User response

No response is required.

AZF6166W Yubikey enrollment services init failed

Explanation

AZFYUBI1 plug-in could not initialize.

User response

Contact IBM support.

AZF6170E No factors are active for the specified User ID

Explanation

If you apply a policy to a user, the user must have all the factors defined in the policy, and those factors must be active.

User response

Configure the user as described in Chapter 8, “Provisioning IBM MFA users,” on page 49.

AZF6171E Session expired or otherwise not found

Explanation

The user exceeded the amount of time allowed to satisfy all authentication factors.

User response

The user must begin the logon process again.

AZF6172E The specified policy name is invalid

Explanation

The policy name associated with the user ID is invalid.

User response

Specify the policy name as described in “Assigning policies and authentication methods to users” on page 69.

AZF6173E Failed to create a Cache Token Credential

Explanation

A cache token credential is created every time a user successfully logs on with IBM MFA Out-of-Band. IBM MFA Out-of-Band could not create the cache token credential.

User response

Make sure that the IBM MFA server is configured.

AZF6174E No policies are bound to the specified user or session

Explanation

A policy name is not associated with the user ID.

User response

Associate a policy name with the user ID as described in “Assigning policies and authentication methods to users” on page 69.

AZF6175I None of the user's policies are satisfiable

Explanation

If you apply a policy to a user, the user must have all the factors defined in the policy, and those factors must be active.

User response

Configure the user as described in Chapter 8, “Provisioning IBM MFA users,” on page 49.

AZF6176E **An internal error occurred**

Explanation

An internal server error prevented the user account from authenticating.

User response

Contact IBM support.

AZF6177E **Your account is not provisioned for MFA**

Explanation

The user account is not provisioned for IBM MFA Out-of-Band.

User response

Configure the user as described in Chapter 8, “Provisioning IBM MFA users,” on page 49.

AZF6180E **Mutual Authentication port must be different from Server Authentication port**

Explanation

The mutual authentication port you configure must be different from the server authentication port.

User response

Configure the mutual authentication port.

AZF7001E **Internal error, bad plugin data**

Explanation

An internal error occurred while processing the authentication.

User response

Restart the IBM MFA server.

AZF7002E **Internal error, bad authTxn data**

Explanation

An internal error occurred while processing the authentication.

User response

Restart the IBM MFA server.

AZF7003E **Internal error, missing plugin state**

Explanation

An internal error occurred while initializing the plug-in.

User response

Contact IBM support.

AZF7009E **Bad settings data**

Explanation

An internal error occurred while initializing the plug-in.

User response

Contact IBM support.

AZF7012I **Applying user-specific eval policy**

Explanation

The user-specific settings are different than the defaults.

User response

No response is required.

AZF8001E **Internal error, bad plugin data**

Explanation

An internal error occurred while processing the authentication.

User response

Restart the IBM MFA server.

AZF8002E **Internal error, bad authTxn data**

Explanation

An internal error occurred while processing the authentication.

User response

Restart the IBM MFA server.

AZF8003E **Internal error, missing plugin state**

Explanation

An internal error occurred that prevented the plug-in from processing the transaction.

User response

Contact IBM support.

AZF8004E Invalid AZFCERT1 settings data

Explanation

An internal error occurred while initializing the plug-in.

User response

Contact IBM support.

AZF8005I AZFCERT1 Initializing

Explanation

The AZFCERT1 plug-in is initializing.

User response

No response is required.

AZF8006I Result of certificate evaluation

Explanation

This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF8007E Invalid tag name

Explanation

You specified an invalid tag name.

User response

Enter a valid AZFCERT1 setting, as described in "Configuring IBM MFA for PIV/CAC or X.509 Certificate authentication" on page 30.

AZF8008E Failed to read AZFCERT1 settings

Explanation

AZFCERT1 settings could not be retrieved.

User response

Verify the AZFCERT1 settings, as described in "Configuring IBM MFA for PIV/CAC or X.509 Certificate authentication" on page 30.

AZF8009W Runtime settings were not changed

Explanation

If it is determined during REFRESH command processing that incoming AZFCERT11 settings are invalid, those settings will not be applied.

User response

Correct the invalid settings.

AZF8010I AZFCERT1 settings follow

Explanation

The AZFCERT1 factor-wide settings are printed when the AZFCERT1 factor is initialized during IBM MFA server startup, and are preceded by this message.

User response

No response is required.

AZF8011I Password expired. Enter and confirm a New Password.

Explanation:
This is an informational message generated as part of IBM MFA processing.

User response

Enter and confirm a new password.

AZF8012I New Password not accepted. Enter and confirm a different New Password.

Explanation:
This is an informational message generated as part of IBM MFA processing.

User response

Enter and confirm a new password.

AZF8013I New Password validation failed. Re-enter and confirm the New Password.

Explanation:
This is an informational message generated as part of IBM MFA processing.

User response

Enter and confirm a new password.

AZF8014I **Password accepted.**

Explanation:
This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF8015I **Password rejected.**

Explanation:
This is an informational message generated as part of IBM MFA processing.

User response

Enter and confirm a new password.

AZF8016I **Password expired. Enter and confirm a New Password, using a response of the form: password/newPassword/newPassword**

Explanation:
This is an informational message generated as part of IBM MFA processing.

User response

Enter and confirm a new password.

AZF8017I **New Password not accepted. Enter and confirm a different New Password, using a response of the form: password/newPassword/newPassword**

Explanation:
This is an informational message generated as part of IBM MFA processing.

User response

Enter and confirm a new password.

AZF8018I **New Password validation failed. Re-enter and confirm the New Password, using a response of the form: password/newPassword/newPassword**

Explanation:
This is an informational message generated as part of IBM MFA processing.

User response

Enter and confirm a new password.

AZF8020I **Authenticator initialized**

Explanation

The authenticator is initialized. This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF8021E **Authenticator init failed**

Explanation

AZFCERT1 plug-in could not initialize.

User response

Contact IBM support.

AZF8022I **Authenticator teardown invoked**

Explanation

This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF8023E **Unsupported API invoked**

Explanation

An internal error occurred.

User response

Contact IBM support.

AZF8030E **A Base64 decode operation failed**

Explanation

This is unlikely to occur unless there is an out of memory issue. If the IBM MFA server is still up and emitting this message, restart it.

User response

Restart the IBM MFA server.

AZF8031E **Failed to create AZFCERT1 User object**

Explanation

A user's AZFCERT1 factor data was not present, or contained values that prevented the creation of a validated user object.

User response

Clear the user's AZFCERT1 factor data and configure the user as described in "Enabling users for IBM MFA for PIV/CAC or X.509 Certificate authentication" on page 53.

AZF8032E **Error evaluating AZFCERT1 User object changes**

Explanation

Changing the user AZFCERT1 factor data resulted in an error.

User response

See additional log messages for details.

AZF8033E **Tag eval failed to translate local status to PC rc/reason pair**

Explanation

The local error cannot be translated to be more meaningful.

User response

Check your input to make sure you specified values as documented.

AZF9001I ***factor-name* Authenticator initialized**

Explanation:
This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF9002I ***factor-name* Authenticator deactivated**

Explanation:
This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF9004E ***factor-name* Authenticator init failed**

Explanation

The plug-in could not initialize.

User response

Contact IBM support.

AZF9005E **Internal error, bad plugin data**

Explanation

An internal error occurred while processing the authentication.

User response

Restart the IBM MFA server.

AZF9006E **Internal error, bad authTxn data**

Explanation

An internal error occurred while processing the authentication.

User response

Restart the IBM MFA server.

AZF9007E **Internal error, missing plugin state**

Explanation

An internal error occurred that prevented the plug-in from processing the transaction.

User response

Contact IBM support.

AZF9008E **Failed to build txn-specific state**

Explanation

An internal error occurred that prevented the plug-in from processing the transaction.

User response

Contact IBM support.

AZF9009E **Internal error, missing txn-specific state**

Explanation

An internal error occurred that prevented the plug-in from processing the transaction.

User response

Contact IBM support.

AZF9010E **Error communicating with RADIUS Server**

Explanation

Unable to send or receive messages to the RADIUS server and its replicas.

User response

Ensure that the RADIUS server is running and is reachable from the IBM MFA server system. For example, try pinging the RADIUS server. If there are firewalls present, ensure the rules do not block traffic. If using VIPA (Virtual IP Address), make any necessary network configuration changes.

AZF9011E **Failed to send RADIUS packet**

Explanation

This is a socket error. This is typically followed by a retry, or a "could not evaluate" error. Additional errors will follow.

User response

Verify connectivity between the RADIUS server and IBM MFA.

AZF9012E **Denying access due to a socket error**

Explanation

An internal error occurred that prevented the plug-in from processing the transaction.

User response

Contact IBM support.

AZF9013E **Failed to get network data or sender info**

Explanation

An internal error occurred that prevented the plug-in from correctly reading network data.

User response

Contact IBM support.

AZF9015I **Canceling authentication in flight**

Explanation:
This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF9016I **Retrying RADIUS communication**

Explanation

This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF9017E **Unable to retry sending RADIUS packet**

Explanation

No RADIUS servers are available, or the specified number of retries has been reached.

User response

Add additional RADIUS servers or increase the number of retries. Verify connectivity to the RADIUS servers.

AZF9018I ***factor-name* Initializing**

Explanation

The *factor-name* plug-in is initializing.

User response

No response is required.

AZF9020E **Tag validation error - Invalid tag name**

Explanation

Invalid tag name specified.

User response

Retry with valid tag.

AZF9021E **Tag validation error - Invalid tag value**

Explanation

Invalid tag value specified.

User response

Retry with valid tag.

AZF9124E AZFRADP1 factor-wide settings are missing or invalid

Explanation

The AZFRADP1 factor-wide settings are missing or invalid.

User response

Configure the AZFRADP1 factor-wide settings, as described in "Configuring the IBM MFA for generic RADIUS authentication method" on page 35.

AZF9126I AZFRADP1 settings follow

Explanation

The AZFRADP1 factor-wide settings are printed when the AZFRADP1 factor is initialized during IBM MFA server startup, and are preceded by this message.

User response

No response is required.

AZF9129E AZFRADP1 failed to read settings

Explanation

The IBM MFA server settings could not be determined.

User response

Configure IBM MFA server as described in Chapter 5, "Configuring server options," on page 23.

AZF9130E RADIUS initialization failed

Explanation

The RADIUS plug-in could not initialize.

User response

Contact IBM support.

AZF9131E Session initialization failed

Explanation

The attempt to use the RADIUS factor was unsuccessful because the factor was not initialized successfully.

User response

Contact IBM support.

AZF9132E RADIUS packet preparation failed

Explanation

RADIUS packet preparation failed.

User response

Verify that the PKCS#11 token name still exists.

AZF9133E Failed to receive or validate RADIUS response

Explanation

An unexpected response was received from the RADIUS server. This could be the result of a protocol error or there could be a mismatch in the shared secret. IBM MFA supports Password Authentication Protocol (PAP) only.

User response

Verify the shared secret. Verify that the RADIUS server supports Password Authentication Protocol (PAP).

AZF9200E Failed to access PKCS#11 token

Explanation

The PKCS#11 token name specified in the IBM MFA server settings is not accessible.

User response

Configure the IBM MFAsettings, as described in Chapter 5, "Configuring server options," on page 23.

AZF9201I Accessible PKCS#11 environment description follows:

Explanation

This is an informational message generated as part of normal processing.

User response

No response is required.

AZF9202E Required PKCS#11 token key not found

Explanation

The PKCS#11 token key is not found.

User response

Check the token name configured in the IBM MFA server settings.

AZF9203E Failed to create PKCS#11 token AES key

Explanation

The PKCS#11 AES key could not be created.

User response

Configure the PKCS#11 token, as described in "Configuring a PKCS#11 token" on page 9.

AZF9204E Settings do not contain shared secret ciphertext

Explanation

The shared secret (case-sensitive password) is used by the RADIUS server to recognize the IBM MFA RADIUS client. The RADIUS client uses the same shared secret when communicating with the RADIUS primary server or RADIUS replica servers.

User response

Configure the shared secret.

AZF9205E Failed to decrypt the shared secret

Explanation

The shared secret (case-sensitive password) is used by the RADIUS server to recognize the IBM MFA RADIUS client. The RADIUS client uses the same shared secret when communicating with the RADIUS primary server or RADIUS replica servers.

User response

Configure the shared secret for the authentication factor.

AZF9206E One or more required RADIUS settings is missing

Explanation

Settings required by RADIUS are missing. One of the settings was not set correctly in the configuration.

User response

Configure the RADIUS authentication factor.

AZF9207E Failed to initialize RADIUS server entry

Explanation

This message follows AZF9215E, and additional server-specific messages follow. One possible reason for this error is that the RADIUS server entry address can't be resolved.

User response

Verify connectivity to the RADIUS servers.

AZF9208E Failed to connect to TCP server

Explanation

The generic RADIUS factor failed to connect to the TCP server. Generic RADIUS supports both User Datagram Protocol (UDP) and Transmission Control Protocol (TCP).

User response

Configure the generic RADIUS factor, as described in "Configuring the IBM MFA for generic RADIUS authentication method" on page 35.

AZF9209E Failed to get UDP peer socket

Explanation

The generic RADIUS factor failed to get the UDP peer socket. Generic RADIUS supports both User Datagram Protocol (UDP) and Transmission Control Protocol (TCP).

User response

Configure the generic RADIUS factor, as described in "Configuring the IBM MFA for generic RADIUS authentication method" on page 35.

AZF9211I Failed to get local hostname

Explanation

There is a problem obtaining the local host name and its IP address.

User response

Verify that TCP/IP is started before IBM MFA.

AZF9212E Failed to get local address

Explanation

Failed to get local address

User response

Start IBM MFA server after TCP/IP is running.

AZF9213E Failed to send complete RADIUS packet

Explanation

This is a socket error. This is typically followed by a retry, or a "could not evaluate" error. Additional errors will follow.

User response

Verify connectivity between the RADIUS server and IBM MFA.

AZF9214E Error validating received RADIUS packet

Explanation

An unexpected response was received from the RADIUS server. This could be the result of a protocol error or there could be a mismatch in the shared secret. IBM MFA supports Password Authentication Protocol (PAP) only.

User response

Verify the shared secret. Verify that the RADIUS server supports Password Authentication Protocol (PAP).

AZF9215E Failed to resolve hostname entry

Explanation

The hostname for the RADIUS server cannot be resolved. The hostname must be sufficiently qualified for web clients to resolve the hostname.

User response

Configure the RADIUS server hostname.

AZF9301I AZFISAM1 Authenticator initialized

Explanation

The authenticator is initialized. This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF9302I AZFISAM1 Authenticator deactivated

Explanation:
This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF9304E AZFISAM1 Authenticator init failed

Explanation

The AZFISAM1 plug-in could not initialize.

User response

Contact IBM support.

AZF9305E Internal error, bad plugin data

Explanation

An internal error occurred while processing the authentication.

User response

Restart the IBM MFA server.

AZF9306E Internal error, bad authTxn data

Explanation

An internal error occurred while processing the authentication.

User response

Restart the IBM MFA server.

AZF9307E Internal error, bad authTxn data

Explanation

An internal error occurred while processing the authentication.

User response

Restart the IBM MFA server.

AZF9308E Failed to build txn-specific state

Explanation

An internal error occurred that prevented the plug-in from processing the transaction.

User response

Contact IBM support.

AZF9309E Internal error, missing txn-specific stat

Explanation

An internal error occurred that prevented the plug-in from processing the transaction.

User response

Contact IBM support.

AZF9310E Error communicating with HTTP server

Explanation

Unable to send or receive messages to the HTTP server.

User response

Ensure that the HTTP server is running and is reachable. For example, try pinging the HTTP server from the system. If there are firewalls present, ensure the rules do not block traffic. If using VIPA (Virtual IP Address), make any necessary network configuration changes.

AZF9311E Failed to send HTTP request

Explanation

Unable to send or receive messages to the HTTP server.

User response

Ensure that the HTTP server is running and is reachable from the system. For example, try pinging the HTTP server from the system. If there are firewalls present, ensure the rules do not block traffic. If using VIPA (Virtual IP Address), make any necessary network configuration changes.

AZF9312E Denying access due to a socket error

Explanation

An internal error occurred that prevented the plug-in from processing the transaction.

User response

Contact IBM support.

AZF9313E Failed to get network data or sender info

Explanation

An internal error occurred that prevented the plug-in from correctly reading network data.

User response

Contact IBM support.

AZF9314E HTTP response validation failed

Explanation

An invalid HTTP response was received from the remote server.

User response

Set trace level 3 in the AZFISAM1 plug-in and repeat the failing operation. Ensure that the AZFISAM1 settings configuration contains the correct Access Token URL and One-time Passcode Validation URL. Check for errors on the remote server.

AZF9315I Canceling authentication in flight

Explanation:
This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF9316E Failed to interpret HTTP response (denying access)

Explanation

An unsupported response was received from the remote server, and the user was not authenticated.

User response

Set trace level 3 for the AZFISAM1 factor and retry the failing operation. Ensure that the AZFISAM1 settings configuration contains the correct Access Token URL and One-time Passcode Validation URL. Check for errors on the remote server.

AZF9320E **Tag validation error - Invalid tag name**

Explanation

Invalid tag name specified in ALTUSER command.

User response

Retry with valid tag.

AZF9321E **Tag validation error - Invalid tag value**

Explanation

Invalid tag value specified in ALTUSER command.

User response

Retry with valid tag.

AZF9324E **AZFISAM1 settings are missing or invalid**

Explanation

The AZFISAM1 factor-wide settings are missing or invalid.

User response

Configure the AZFISAM1 factor-wide settings.

AZF9326I **AZFISAM1 settings follow**

Explanation

The AZFISAM1 factor-wide settings are printed when the AZFISAM1 factor is initialized during AZF started task startup, and are preceded by this message.

User response

No response is required.

AZF9329E **AZFISAM1 failed to read AZFSTC settings**

Explanation

The STC settings could not be determined.

User response

Configure the STC settings.

AZF9330E **HTTP client initialization failed**

Explanation

The AZFISAM1 factor failed to initialize an HTTP client context, and will be unable to authenticate users.

User response

Set trace level 3 in the AZFISAM1 settings and restart the IBM MFA server to view any additional error context. Check the AZFISAM1 settings to ensure that valid URLs are specified for the Access Token URL and the One-time Passcode Validation URL

AZF9330I **AZFISAM1 Initializing**

Explanation

The *factor-name* plug-in is initializing.

User response

No response is required.

AZF9331E **HTTP session initialization failed**

Explanation

The attempt to use the AZFISAM1 factor was unsuccessful because the factor was not initialized successfully.

User response

Contact IBM support.

AZF9332E **HTTP session failed to stage request**

Explanation

The AZFISAM1 factor attempted to build an Access Token request or One-time Password Validation request, but was unable to do so completely.

User response

Set trace level 3 for the AZFISAM1 factor and retry the failing operation. Check the AZFISAM1 settings to ensure that valid PKCS#11 Token Name, Key Label, Client Id, and Authentication Context values are specified. If the task log indicates an error reading the Client Secret, ensure that the Client Secret is set.

AZF9335E **failed to parse Access token URL setting**

Explanation

The Access Token URL in the AZFISAM1 factor settings cannot be parsed.

User response

Verify the AZFISAM1 factor settings.

AZF9336E **failed to parse OTP validation URL setting**

Explanation

The One-time Passcode Validation URL in the AZFISAM1 factor settings cannot be parsed.

User response

Verify the AZFISAM1 factor settings.

AZF9340E **Missing or unsupported ISAM AUTHMECH setting**

Explanation

The Authentication Context in the AZFISAM1 factor settings cannot be parsed.

User response

Verify the AZFISAM1 factor settings.

AZF9341E **Failed to access PKCS#11 token**

Explanation

The PKCS#11 token name specified in the IBM MFA settings is not accessible.

User response

Verify the IBM MFA server settings.

AZF9342I **Accessible PKCS#11 environment description follows:**

Explanation

This is an informational message generated as part of normal processing.

User response

No response is required.

AZF9343E **Required PKCS#11 token key not found**

Explanation

The PKCS#11 token key is not found.

User response

Check the token name configured in the IBM MFA server settings.

AZF9344E **Failed to create PKCS#11 token AES key**

Explanation

The PKCS#11 AES key could not be created.

User response

Configure the PKCS#11 token.

AZF9345E **Settings do not contain client secret ciphertext**

Explanation

The **Client Secret** setting is not configured.

User response

Configure the **Client Secret** setting on the AZFISAM1 factor panel.

AZF9346E **Failed to decrypt the client secret**

Explanation

The **Client Secret** setting is not configured or does not match that of the client.

User response

Verify the **Client Secret** setting on the AZFISAM1 factor panel.

AZF9351E **ACCESS DENIED**

Explanation

This is a general authentication failed error.

User response

See the SYSLOG for additional errors.

AZF9353I **ISAM AUTHENTICATION SUCCESSFUL**

Explanation

The user was successfully authenticated.

User response

No response is required.

AZF9360E **Supported tags: ISAMUSERID, AUTHMECH**

Explanation

You specified an invalid tag name.

User response

Retry with valid tag.

AZF9361E **ISAMUSERID length must be <= 128**

Explanation

ISAMUSERID must be less than or equal to 128 characters.

User response

Retry with valid length.

AZF9370I **AZFISAM1 USER IS SUSPENDED - NOTIFY ADMINISTRATOR**

Explanation:
The user account is suspended.

User response

Notify your system administrator of the error.

AZF9501I **AZFYUBI1 Authenticator initialized**

Explanation

This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF9502I **AZFYUBI1 Authenticator deactivated**

Explanation

The AZFYUBI1 plug-in is stopped.

User response

No response is required.

AZF9503I **AZFYUBI1 Authenticator deactivated**

Explanation

This progress message is intended for use by support in the event of a problem.

User response

No response is required.

AZF9504E **AZFYUBI1 Authenticator init failed**

Explanation

AZFYUBI1 plug-in could not initialize.

User response

Contact IBM support.

AZF9505E **Internal error, bad plugin data**

Explanation

An internal error occurred while processing the authentication.

User response

Restart the server.

AZF9506E **Internal error, bad authTxn data**

Explanation

An internal error occurred while processing the authentication.

User response

Restart the server.

AZF9507E **Internal error, missing plugin state**

Explanation

An internal error occurred that prevented the plug-in from processing the transaction.

User response

Contact IBM support.

AZF9508E **Failed to build txn-specific state**

Explanation

An internal error occurred that prevented the plug-in from processing the transaction.

User response

Contact IBM support.

AZF9509E Internal error, missing txn-specific state

Explanation

An internal error occurred that prevented the plug-in from processing the transaction.

User response

Contact IBM support.

AZF9511E AZFYUBI1 AuthTransactions cannot be canceled or continued

Explanation

This message indicates incorrect message routing inside the server and is not seen in normal circumstances.

User response

Shut down and restart the server.

AZF9512E Failed to create AZFYUBI1 User object

Explanation

The AZFYUBI1 factor data for a particular user ID is invalid.

User response

Correct or clear the AZFYUBI1 factor data for the affected user.

AZF9513E Error validating Yubico OTP

Explanation

A user’s OTP passcode could not be validated due to an underlying library error. This message will include the relevant PKCS#11 return and reason codes, if applicable.

User response

See the PKCS#11 return and reason codes.

AZF9515E Yubico OTP replay detected

Explanation

The AZFYUBI1 plug-in prevented a previously-used OTP passcode from being reused.

User response

Ensure that the passcode reuse was a user error and not the result of a replay attack.

AZF9514I Yubico OTP accepted

Explanation

This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF9524E AZFYUBI1 settings are missing or invalid

Explanation

The AZFYUBI1 factor-wide settings are missing or invalid.

User response

Configure the AZFYUBI1 factor-wide settings.

AZF9526I AZFYUBI1 settings follow

Explanation

The AZFYUBI1 factor-wide settings are printed when the AZFYUBI1 factor is initialized during AZF started task startup, and are preceded by this message.

User response

No response is required.

AZF9530I AZFYUBI1 Initializing

Explanation

This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF9530E AZFYUBI1 User secret missing

Explanation

The user's AZFYUBI1 settings are missing or invalid.

User response

Configure the user's AZFYUBI1 settings.

AZF9531E AZFYUBI1 User secret decode error

Explanation

The user's AZFYUBI1 settings are invalid.

User response

Configure the user's AZFYUBI1 settings.

AZF9542I Description of accessible PKCS#11 environment follows:

Explanation

This is an informational message generated as part of normal processing.

User response

No response is required.

AZF9551E ACCESS DENIED

Explanation

The authentication failed.

User response

Check the system log for additional reasons for the failure.

AZF9553I YUBICO OTP AUTHENTICATION SUCCESS

Explanation

The user was successfully authenticated.

User response

No response is required.

AZF9801I AZFLDAP1 Authenticator initialized

Explanation

The authenticator is initialized. This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF9802I AZFLDAP1 Authenticator deactivated

Explanation:
This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF9803I AZFLDAP1 Entry point

Explanation

This progress message is intended for use by support in the event of a problem.

User response

No response is required.

AZF9804E AZFLDAP1 Authenticator init failed

Explanation

The AZFLDAP1 plug-in could not initialize.

User response

Contact IBM support.

AZF9810E Failed to create AZFLDAP1 User object

Explanation

A user’s AZFLDAP1 factor data was not present, or contained values that prevented the creation of a validated user object.

User response

Verify the user's AZFLDAP1 configuration.

AZF9811E Failed to stage LDAP bind request

Explanation

The AZFLDAP1 factor attempted to build an LDAP simple bind request packet, but was unable to do so completely.

User response

Set trace level 3 in the AZFLDAP1 factor and retry the failing operation. Check the AZFLDAP1 user factor data of the user ID, and ensure that the value in the DN tag is a valid DN string.

AZF9812E **Error communicating with LDAP server**

Explanation

Unable to send or receive messages to the LDAP server.

User response

Ensure that the LDAP server is running and is reachable from the system. For example, try pinging the LDAP server.

AZF9813E **Error receiving or parsing BER response**

Explanation

The AZFLDAP1 factor issued a simple bind request to the remote LDAP server, and received no response or an invalid response.

User response

Set trace level 3 in the AZFLDAP1 factor and retry the failing operation. Check the AZFLDAP1 settings and ensure all specified Server Host Name and Server Port entries are valid and point to LDAP servers. Check for errors on the LDAP server.

AZF9814I **Canceling auth transaction**

Explanation:
This is an informational message generated as part of IBM MFA processing.

User response

No response is required.

AZF9815E **Failed to retry bind attempt**

Explanation

The AZFLDAP1 factor issued a simple bind request to a remote LDAP server, and the request timed out. Upon attempting to retry the request against another server, no additional servers were available or the AZFLDAP1 factor failed to open a connection to the next server.

User response

Set trace level 3 in the AZFLDAP1 factor and retry the failing operation. Check the AZFLDAP1 settings and ensure all specified Server Host Name and Server Port entries are valid and point to LDAP servers.

AZF9816I **Retrying bind request**

Explanation

The AZFLDAP1 factor retried a simple bind request to a remote LDAP server.

User response

This is an informational message and no response is required.

AZF9817E **Failed to stage LDAP unbind request**

Explanation

The AZFLDAP1 factor issued a simple bind request, the server responded, and user authentication succeeded or failed based on the server's response. The AZFLDAP1 factor then attempted to issue a standard unbind request, but was unable to do so completely.

User response

Set trace level 3 in the AZFLDAP1 factor and retry the failing operation.

AZF9824E **AZFLDAP1 settings are missing or invalid**

Explanation

The AZFLDAP1 factor-wide settings are missing or invalid.

User response

Configure the AZFLDAP1 factor-wide settings.

AZF9826I **AZFLDAP1 settings follow**

Explanation

The AZFLDAP1 factor-wide settings are printed when the AZFLDAP1 factor is initialized during AZF started task startup, and are preceded by this message.

User response

No response is required.

AZF9830I ***factor-name* Initializing**

Explanation

The *factor-name* plug-in is initializing.

User response

No response is required.

AZF9830E **Connection reinitialization failed**

Explanation

None of the configured LDAP servers could be reached on the network, or the maximum number of allowed retries was exceeded. The related authentication attempt fails with Could Not Evaluate.

User response

Ensure that the configured LDAP servers are available and reachable.

AZF9851E **ACCESS DENIED**

Explanation

The authentication failed.

User response

Check the system log for additional reasons for the failure.

AZF9853I **LDAP AUTHENTICATION SUCCESSFUL**

Explanation

The user was successfully authenticated.

User response

No response is required.

IBM MFA ssl messages

This section describes messages issued with IBM MFA ssl message numbers.

1180061 **TRUSTED CA HAS NO STATUS**

Explanation

The **TRUSTEDCAS** field is required. It specifies the fully-qualified path to the file containing a concatenation of PEM-format X.509 certificates. The path or file you specified is not valid or cannot be accessed for some reason.

User response

Configure **TRUSTEDCAS**.

1180062 **LOAD VERIFY LOCATION FAILED**

Explanation

The **TRUSTEDCAS** field is required. It specifies the fully-qualified path to the file containing a concatenation of PEM-format X.509 certificates. The path or file you specified cannot be found.

User response

Configure **TRUSTEDCAS**.

1180063 **TRUSTED CA IS REQUIRED**

Explanation

The **TRUSTEDCAS** field is required. It specifies the fully-qualified path to the file containing a concatenation of PEM-format X.509 certificates.

User response

Configure **TRUSTEDCAS**.

1180064 **P12 OPEN FAILED**

Explanation

IBM MFA cannot open the server's PKCS#12 file.

User response

Configure the server's PKCS#12 file as described in “Obtaining the PKCS#12 file and certificate password” on page 8.

1180065 **P12 READ FAILED**

Explanation

IBM MFA cannot read the server's PKCS#12 file.

User response

Configure the server's PKCS#12 file as described in "Obtaining the PKCS#12 file and certificate password" on page 8.

1180066 P12 PARSE FAILED

Explanation

IBM MFA cannot parse the server's PKCS#12 file.

User response

Configure the server's PKCS#12 file as described in "Obtaining the PKCS#12 file and certificate password" on page 8.

1180067 P12 EXTRACT FAILED

Explanation

IBM MFA cannot extract needed information from the server's PKCS#12 file.

User response

Configure the server's PKCS#12 file as described in "Obtaining the PKCS#12 file and certificate password" on page 8.

1180068 USE CERT FAILED

Explanation

IBM MFA cannot use the certificate from the server's PKCS#12 file.

User response

Configure the server's PKCS#12 file as described in "Obtaining the PKCS#12 file and certificate password" on page 8.

1180069 USE PRIVATE KEY FAILED

Explanation

IBM MFA cannot use the private key from the server's PKCS#12 file.

User response

Configure the server's PKCS#12 file as described in "Obtaining the PKCS#12 file and certificate password" on page 8.

1180070 CHECK PRIVATE KEY FAILED

Explanation

IBM MFA cannot use the private key from the server's PKCS#12 file.

User response

Configure the server's PKCS#12 file as described in "Obtaining the PKCS#12 file and certificate password" on page 8.

1180071 USE CERTIFICATE FILE FAILED

Explanation

IBM MFA cannot use the certificate file from the server's PKCS#12 file.

User response

Configure the server's PKCS#12 file as described in "Obtaining the PKCS#12 file and certificate password" on page 8.

1180072 USE PRIVATE KEY FILE FAILED

Explanation

IBM MFA cannot use the private key file from the server's PKCS#12 file.

User response

Configure the server's PKCS#12 file as described in "Obtaining the PKCS#12 file and certificate password" on page 8.

1180073 PEM READ X509 FAILED

Explanation

IBM MFA cannot read the certificate from the server's truststore.

User response

Configure the server truststore as described in "Creating the server truststore" on page 29.

1180074 GET CERTIFICATE INFO FAILED

Explanation

IBM MFA cannot read the certificate information from the server's truststore.

User response

Configure the server truststore as described in "Creating the server truststore" on page 29.

1180075 NO PEER CERT

Explanation

IBM MFA cannot find the client's PIV/CAC card issuing certificate chain in the server's truststore.

User response

Configure the server truststore as described in "Creating the server truststore" on page 29.

Chapter 17. Translating IBM MFA messages and HTML

IBM MFA allows you to provide translated versions of IBM MFA messages and HTML text that are displayed in the language specified by the web browser.

Procedure

1. Change directory (cd) to `/opt/IBM/MFA/mfa/i18n`.
2. In the i18n subdirectory, create a language (for example, en or fr) or language-locale (for example, en-US or fr-BE) translation subdirectory. For example, `/opt/IBM/MFA/mfa/i18n/fr`.
3. Copy `/opt/IBM/MFA/mfa/i18n/translate.json` to `/opt/IBM/MFA/mfa/i18n/fr/translate.json` and edit the strings as needed, using exactly the same value:pair format.

   ```
   {
     "IBM MFA Out of Band Interface": "IBM MFA Out of Band Interface",
     "IBM TouchToken Enrollment": "IBM TouchToken Enrollment",
     "Certificate Enrollment via Mutually-Authenticated TLS":"Certificate Enrollmen
   t via Mutually-Authenticated TLS",
     "Authentication Token": "Authentication Token",
     "Please wait, request is being processed": "Please wait, request is being proc
   essed",
     "Please input the policy name": "Please input the policy name",
     "INTERACTIVE": "Interactive",
     "Policy Name": "Policy Name",
     "Enter your SecurID passcode": "Enter your SecurID passcode",
     "Passcode": "Passcode",
     "RSA SecureID": "RSA SecureID",
     "Password Authentication": "Password Authentication",
   :
   :
   ```

4. In the i18n subdirectory, create an HTML subdirectory. For example, `/opt/IBM/MFA/mfa/i18n/fr/html`.
5. Copy the HTML pages from `/opt/IBM/MFA/mfa/html` to `/opt/IBM/MFA/mfa/i18n/fr/html/` and edit as needed.
6. IBM MFA finds `/opt/IBM/MFA/mfa/i18n/fr/translate.json` and `/opt/IBM/MFA/mfa/i18n/fr/html/*.html` and serves them as needed.

   `/opt/IBM/MFA/mfa/i18n/translate.json` is the default file if a client-specific translation file is not available.

Appendix A. Accessibility

z/VM is accessible by people with disabilities.

The following features support use by people with disabilities:

- Operation by keyboard alone
- Optional font enlargement and high-contrast display settings
- Screen readers and screen magnifiers tested for use by people with visual impairment

Notices

This information was developed for products and services that are offered in the USA or elsewhere.

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
United States of America

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

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 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.

This information could include missing, incorrect, or broken hyperlinks. Hyperlinks are maintained in only the HTML plug-in output for the Knowledge Centers. Use of hyperlinks in other output formats of this information is at your own risk.

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.

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
Site Counsel
2455 South Road

Poughkeepsie, NY 12601-5400
USA

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 measurements 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. 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.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

IBM Online Privacy Statement

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.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user's name, email address, phone number, or other personally identifiable information for purposes of enhanced user usability and single sign-on configuration. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

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.

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

Policy for unsupported hardware

Various z/OS elements, such as DFSMSdfp, JES2, JES3, and MVS™, contain code that supports specific hardware servers or devices. In some cases, this device-related element support remains in the product even after the hardware devices pass their announced End of Service date. z/OS may continue to service element code; however, it will not provide service related to unsupported hardware devices. Software problems related to these devices will not be accepted for service, and current service activity will cease if a problem is determined to be associated with out-of-support devices. In such cases, fixes will not be issued.

Minimum supported hardware

The minimum supported hardware for z/OS releases identified in z/OS announcements can subsequently change when service for particular servers or devices is withdrawn. Likewise, the levels of other software products supported on a particular release of z/OS are subject to the service support lifecycle of those products. Therefore, z/OS and its product publications (for example, panels, samples, messages, and product documentation) can include references to hardware and software that is no longer supported.

- For information about software support lifecycle, see: IBM Lifecycle Support for z/OS (www.ibm.com/software/support/systemsz/lifecycle)
- For information about currently-supported IBM hardware, contact your IBM representative.

Trademarks

Index

Special Characters

/etc/pam.d
  editing 15

A

accessibility
  contact IBM 145
activate and deactivate users
  IBM MFA 52, 53, 55–59, 65–68
  IBM MFA for Yubico OTP 60, 61, 64
additional SecurID steps 27, 29
administrator IDs
  adding 13
  listing 14
  removing 14, 15
approving certificates
  IBM MFA for PIV/CAC or X.509 Certificate 54
assign policies to users
  IBM MFA 69
assistive technologies 145
authentication methods
  associating with policies 46
  configuring 27
AZF messages 91

B

backing up
  database 79
bulk provision users
  IBM MFA 49

C

CA root certificate
  creating for testing 87
cache token credential
  setting reusable 46
Certificate
  configuring panel 30
change password
  IBM MFA 72
check user information
  IBM MFA 70, 72
configuring IBM MFAauthentication methods 27
configuring SecurID parameters 28
copying sdconf.rec 27

D

daemon
  starting for server 16
  stopping for server 17
database
  backing up 79
  starting for server 17
deleting
  multi-factor authentication policies 47
disaster recovery
  SecurID 85
displaying users
  IBM MFA 69

E

editing
  /etc/pam.d 15

F

feedback xi

G

generic TOTP
  prepare device 56
GUI interface
  installing 7
  navigating 21
  using 21

I

IBM MFA
  activate and deactivate users 52, 53, 55–59, 65–68
  assign policies to users 69
  bulk provision users 49
  change MFA password 72
  check user information 70, 72
  configure PCI mode 25
  configure PKCS#11 token 9, 10
  configure server options 23
  displaying users 69
  install postgres 8
  requirements 7
  set or reset MFA password 71
  setting suspended flag 70
  suspension status 71
  z/VM clients 75, 77
IBM MFA for generic RADIUS
  configuring panel 35
IBM MFA for IBM Security Access Manager
  configure 42
IBM MFA for LDAP Simple Bind
  configure 41
IBM MFA for PIV/CAC or X.509 Certificate
  approving certificates 54
IBM MFA for SafeNet RADIUS

IBM MFA for SafeNet RADIUS *(continued)*
- configuring panel 37

IBM MFA for Yubico OTP
- activate and deactivate users 60, 61, 64
- configure 40
- prepare token 61

K

keyboard
- navigation 145
- PF keys 145
- shortcut keys 145

L

log file
- location 16, 17

M

multi-factor authentication
- authentication factors 1
- introduction 1
- RSA Authentication Manager concepts 3
- SecurID passcode 3
- SecurID PIN 3
- SecurID token code 3
- types of token devices 3

multi-factor authentication policies
- applying to users 45
- associating with authentication methods 46
- creating 45
- deleting 47
- displaying 45
- provisioning users 49
- setting policy token timeout 46

N

navigation
- keyboard 145

node secret
- clear for SecurID 29

P

parameters
- configuring for SecurID 28

Password
- configuring panel 44

PCI mode
- configure 25

PCS#11 token
- configure 9, 10

PKCS#12 file
- obtaining 8

policies
- removing from users 73

postgres
- installing 8
- updating 81

prepare token

prepare token *(continued)*
- IBM MFA for Yubico OTP 61

preparing for IBM MFA 5

R

removing policies
- from users 73

RSA Authentication Manager concepts 3

S

sdconf.rec
- copying for SecurID 27

sdopts.rec file 28

SecurID
- clear node secret 29
- configuring 27–29
- copying sdconf.rec 27
- prerequisites 27
- sdopts.rec file 28

SecurID disaster recovery 85

SecurID RADIUS
- configuring panel 38

sending to IBM
- reader comments xi

server
- log file 17
- starting daemon 16
- starting database 17
- stopping daemon 17

server and GUI interface
- installing 11, 18

server certificate
- creating for testing 87

server logging
- location of log file 16, 17

server options
- configure 23

server setup
- completing 12

server truststore
- creating 29, 31

set password
- IBM MFA 71

shortcut keys 145

ssl messages 140

summary of changes xiii

suspended control
- IBM MFA 70

suspension status
- IBM MFA 71

T

TOTP
- configure user profile 83
- configuring panel 33

trademarks 150

translation
- configure 143

U

updating
  postgres 81
user interface
  ISPF 145
  TSO/E 145
user profile
  configure for generic TOTP 56
  configure for TOTP 83
users
  provisioning 49

Z

z/VM clients
  adding 75
  removing 77

Product Number: 5655-MA1

SC27-4938-40