

IBM MFA
Version 2 Release 0

*IBM Z Multi-Factor Authentication User's
Guide*



Note

Before using this information and the product it supports, read the information in [“Notices” on page 65.](#)

This edition applies to Version 2 Release 3 of z/OS (5650-ZOS) and to all subsequent releases and modifications until otherwise indicated in new editions.

Last updated: 2019-05-23

© **Copyright International Business Machines Corporation 2016, 2019.**

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

© **Rocket Software, Inc. 2016, 2019.**

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
Summary of changes as updated May, 2019.....	xiii
Chapter 1. Introduction to IBM MFA.....	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
PIN and token concepts: use of the password field.....	4
IBM TouchToken concepts.....	5
IBM TouchToken OTP.....	5
Preparing your Apple device for IBM TouchToken.....	6
IBM MFA Out-of-Band concepts.....	6
General logon approach.....	7
Chapter 2. IBM MFA Out-of-Band authentication.....	9
Enrolling your certificate for IBM MFA Certificate Authentication.....	10
Logging in to an application with IBM MFA Out-of-Band.....	11
Chapter 3. IBM MFA with SecurID in-band authentication.....	13
TSO/E.....	13
Fob-style hardware token.....	13
Hardware token with a PINpad.....	16
Soft token.....	18
CICS CESL transaction.....	21
Fob-style hardware token.....	21
Hardware token with a PINpad.....	22
Soft token.....	24
z/OS Management Facility.....	25
Logging in with a fob-style hardware token.....	25
Logging in with a hardware token with a PINpad.....	26
Logging in with a soft token.....	26
z/OS Management Facility with compound in-band authentication.....	26
IBM FTP.....	27
Logging in with a fob-style hardware token.....	28
Logging in with a hardware token with a PINpad.....	28
Logging in with a soft token.....	28
IBM FTP with compound in-band authentication.....	28
IBM OpenSSH.....	30
Logging in with a fob-style hardware token.....	30

Logging in with a hardware token with a PINpad.....	30
Logging in with a soft token.....	31
IBM OpenSSH with compound in-band authentication.....	31
Chapter 4. IBM TouchToken in-band authentication.....	35
Logging in to TSO with IBM TouchToken.....	35
Logging in to CICS CESL with IBM TouchToken.....	35
Logging in to z/OSMF with IBM TouchToken.....	35
Logging in to IBM FTP with IBM TouchToken.....	36
Logging in to IBM SSH with IBM TouchToken.....	36
Logging in with IBM TouchToken and compound in-band authentication.....	36
Logging in with generic TOTP.....	37
Chapter 5. IBM MFA for SafeNet RADIUS with TSO/E.....	39
TSO/E with Quick Log.....	39
TSO/E with Quick Log and compound in-band authentication.....	39
TSO/E with Challenge-Response.....	40
TSO/E with Challenge-Response and compound in-band authentication.....	41
Chapter 6. IBM MFA for generic RADIUS with TSO/E.....	43
Logging in with IBM MFA Compound In-Band when new PIN required.....	43
Chapter 7. Logging in with IBM MFA for LDAP	45
Logging in with IBM MFA for LDAP and compound in-band authentication.....	45
Chapter 8. Logging in with IBM MFA for YubiKey	47
Logging in with IBM MFA for YubiKey and compound in-band authentication.....	47
Chapter 9. IBM CL/SuperSession for z/OS.....	49
Chapter 10. IBM HTTP Server - Powered by Apache.....	51
Logging in with IBM TouchToken.....	51
Logging in with a fob-style hardware token.....	52
Logging in with a hardware token with a PINpad.....	52
Logging in with a soft token.....	52
Logging in with IBM MFA Out-of-Band.....	52
Chapter 11. Troubleshooting.....	55
Logging in with RSA SecurID "next token" mode.....	55
Logging in with Password Fallback.....	56
Chapter 12. Multi-Factor Authentication messages.....	57
Messages with AZF message numbers.....	57
AZF1001I.....	57
AZF1002I.....	57
AZF1003I.....	57
AZF1004I.....	57
AZF1005E.....	57
AZF1006E.....	58
AZF1007I.....	58
AZF1008E.....	58
AZF1009I.....	58
AZF1010E.....	58
AZF1011E.....	58
AZF1100E.....	58
AZF1101E.....	58

AZF1102I.....	58
AZF1103W.....	59
AZF1104I.....	59
AZF1105I.....	59
AZF5170E.....	59
AZF5171E.....	59
AZF5172E.....	59
AZF5173E.....	59
AZF5174E.....	59
AZF5175E.....	59
AZF5176E.....	59
Appendix A. Accessibility.....	61
Accessibility features.....	61
Consult assistive technologies.....	61
Keyboard navigation of the user interface.....	61
Dotted decimal syntax diagrams.....	61
Notices.....	65
Terms and conditions for product documentation.....	66
IBM Online Privacy Statement.....	67
Policy for unsupported hardware.....	67
Minimum supported hardware.....	68
Trademarks.....	68
Index.....	69

Tables

1. TSO/E Logon Options for a fob-style hardware token..... 14

2. TSO/E Logon Options for a hardware token with a PINpad..... 16

3. TSO/E Logon Options for a soft token..... 18

4. CICS Logon Options for a fob-style hardware token..... 21

5. CICS Logon Options for a hardware token with a PINpad..... 23

6. CICS Logon Options for a soft token..... 24

7. TSO/E Logon Options for SafeNet Quick Log..... 39

8. TSO/E Logon Options for SafeNet Quick Log with Compound In-Band..... 40

9. TSO/E Logon Options for SafeNet Challenge-Response..... 40

10. TSO/E Logon Options for SafeNet Challenge-Response with Compound In-Band..... 41

About this information

This book provides instructions for customizing and using IBM® Z Multi-Factor Authentication, 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.

For installation information, refer to *IBM Z Multi-Factor Authentication Program Directory*, which is included in the product package.

To find any supplemental information made available after publication, go to <http://www.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=ZSW03327USEN>.

To find the complete z/OS library, go to [IBM Knowledge Center \(www.ibm.com/support/knowledgecenter/SSLTBW/welcome\)](http://www.ibm.com/support/knowledgecenter/SSLTBW/welcome).

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](http://www.ibm.com/developerworks/rfe/) (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 mhvrfs@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 Multi-Factor Authentication for z/OS User's Guide, SC27-8448-30
- 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 right 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](http://support.ibm.com) (support.ibm.com).
- Contact your IBM service representative.
- Call IBM technical support.

Summary of changes

This information includes terminology, maintenance, and editorial changes. Technical changes or additions to the text and illustrations for the current edition are indicated by a vertical line to the left of the change.

Summary of changes as updated May, 2019

Changes made to IBM MFA for Version 2 Release 0 as updated May, 2019.

New

- Added IBM MFA for LDAP authentication, as described in [Chapter 7, “Logging in with IBM MFA for LDAP,”](#) on page 45.
- Added IBM MFA for YubiKey authentication, as described in [Chapter 8, “Logging in with IBM MFA for YubiKey,”](#) on page 47.

Chapter 1. Introduction to IBM MFA

IBM Z Multi-Factor Authentication, which is referred to in this document as IBM MFA, provides alternate authentication mechanisms for z/OS networks that are used in conjunction with RSA SecurID-based authentication systems, Apple Touch ID devices, certificate authentication options such as PIV/CAC cards, RADIUS, and more. IBM MFA allows RACF to use alternate authentication mechanisms in place of the standard z/OS password.

The most common method for authenticating users is by the use of passwords or password phrases. Unfortunately, passwords can present a relatively simple point of attack for exploitation. In order for systems that rely on passwords to be secure, they 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 an extremely powerful dedicated password cracking computer system has become trivial and low-cost. Clients are looking for ways to raise the assurance level of their systems by requiring additional authentication factors for users.

You can use IBM MFA with a large variety of applications. Some examples provided in this document include:

- TSO/E. Time Sharing Options (TSO/E) allows users to create an interactive session with the z/OS system. TSO provides a single-user logon capability and a basic command prompt interface to z/OS.
- CICS CESL. Customer Information Control System (CICS) is a family of application servers and connectors that provides industrial-strength, online transaction management and connectivity for mission-critical applications.
- z/OSMF. IBM z/OS Management Facility (z/OSMF) provides a web-based interface that allows you to manage various aspects of your z/OS systems through a browser.
- IBM OpenSSH. OpenSSH provides secure encryption for both remote login and file transfer.

Multi-factor authentication concepts

IBM MFA relies on multiple authentication factors.

A multi-factor authentication system requires that multiple authentication factors be presented during logon in order to verify a user's identity. Each authentication factor must be from a separate category of credential types.

Requiring multiple authentication factors improves the security of your user account.

You either present the credentials directly into the application (in-band) or out-of band:

- Out-of-band authentication allows you to authenticate on a user-specific web page with one or more factors to retrieve a cache token credential that you use to log in. Out-of-band authentication is described in “IBM MFA Out-of-Band concepts” on page 6. Out-of-band authentication methods are described in *Part 2: Out-of-Band Authentication*.
- For in-band authentication, you directly log on. In-band authentication methods are described in *Part 3: In-Band Authentication*.

IBM MFA with SecurID

In the simplest terms, for IBM MFA with SecurID, the RSA Authentication Manager determines whether the user's credentials are valid and, if so, returns success to RACF. RACF then resumes control and completes the authentication and authorization process as usual.

IBM MFA with SecurID requires:

- "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 with RADIUS

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/denied response. In all cases, the RADIUS server determines whether the user's credentials are valid and, if so, returns success to RACF. RACF then resumes control and completes the authentication and authorization process as usual.

IBM TouchToken

For IBM MFA with IBM TouchToken, you use the IBM TouchToken for iOS application on supported Apple devices to generate a hashed, timed one-time password (OTP), and then use this password together with your z/OS user name to log on to the z/OS system.

Note: If your system administrator configures your account for generic TOTP, you can log in by using common Quick Response (QR) codes on both Android and Apple iOS devices.

The OTP password generated by the IBM TouchToken for iOS application must match the OTP password generated by the IBM TouchToken component on the z/OS server. OTP passwords are regenerated at regular intervals.

IBM TouchToken requires:

- "Something you have." (The Apple Touch ID device, with the provisioned IBM TouchToken for iOS application.)
- "Something you are." (Your fingerprint.)

IBM MFA Certificate Authentication

IBM MFA Certificate Authentication is a general purpose certificate authentication that includes Common Access Card (CAC) and Personal Identification Verification (PIV) cards. Certificate authentication uses the client identity certificate to authenticate the user.

IBM MFA Certificate Authentication requires:

- "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 YubiKey

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

IBM MFA for YubiKey requires:

- "Something you have." (The hardware Yubikey token.)
- "Something you know." (IBM MFA for YubiKey should be used with compound in-band authentication or with IBM MFA Out-of-Band authentication.)

IBM MFA for LDAP

You can use your LDAP password to authenticate with IBM MFA.

IBM MFA for LDAP requires:

- "Something you know." (The LDAP password.)
- "Something else you know or have." (IBM MFA for LDAP should be used with compound in-band authentication or with IBM MFA Out-of-Band authentication.)

RSA Authentication Manager concepts

The RSA Authentication Manager includes token codes, PINs, and passcodes as described in this section.

SecurID token code

The SecurID token code is a continuously regenerated number used to prove your identity.

The token code is a pseudo-random 6- or 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 that a token code appears before the display is refreshed.

SecurID PIN

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

The Personal Identification Number (PIN) is a unique 4- to 8-digit identifier that only you know. Your PIN can be of your own choosing, or system generated by RSA Authentication Manager depending on your RSA token policy. If you create your own PIN, follow the locally established rules for creating a valid PIN, including the number of characters, the reuse policy, and so forth.

Your security administrator can clear and reset the PIN as needed, so it is possible that your current PIN is invalid and you need to change it.

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 your PIN followed by the token code and you must enter both. For example, if your PIN is 1234 and the token code is 567891, you enter the passcode as 1234567891.
- For SecurID PINpad hardware tokens and soft token applications, you enter your PIN on the pin pad 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. You then use the generated passcode when you log in.

Types of token devices

Several types of RSA SecurID token devices are supported for use with IBM Multi-Factor Authentication for z/OS.

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 in the LCD.

RSA SecurID PINpads

With an RSA SecurID PINpad token, you enter your PIN directly into the token, and the token generates a hash-encrypted six- or eight-digit passcode. For example, with the RSA SecurID 520 card-style PINpad, you enter 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.

You can use the PINpad token in two ways:

- If you have 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 you do not have a valid PIN, which can occur if the security administrator forces you to change it, use the token to generate a token code. You then use the generated token code to log in and change your PIN.

RSA SecurID soft tokens

RSA SecurID soft token applications reside on a computer or other smart device.

You can use the soft token application in two ways:

- If you have 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 you do not have a valid PIN, which can occur if the security administrator forces you to change it, use the token to generate a token code. You then use the generated token code to log in and change your PIN.

Support for MVS operator console logon

The MVS operator console logon does not support hard tokens. The MVS operator console logon does support soft tokens.

PIN and token concepts: use of the password field

Depending on the token type, IBM MFA uses the password field to contain the PIN and the token code.

Consider the following example:

User ID = Smith
PIN = 8888
Token = 123456
Soft token = 223344

As described in “Types of token devices” on page 3, hard tokens use a physical token and a PIN. Soft tokens use software to hash the PIN into the token and generate a passcode, so you do not use a separate PIN.

Typical logon

Depending on the token type, IBM MFA uses the password field to contain the PIN and the token code.

With passphrase support (more than 8 characters allowed for the password):

- For a hard token, you enter 8888123456 in the password field.
- For a soft token, you enter 223344 in the password field.

Without passphrase support (maximum of 8 characters allowed for the password):

- For a hard token, you enter 123456 in the password field.
- For a hard token, you enter 8888 in the new password field.

Note: You may need to enter 8888 again in the validate change field.

- For a soft token, you enter 223344 in the password field.

PIN-change mode

Depending on the token type, IBM MFA uses the password field to contain the PIN and the token code.

PIN-change mode is similar to a password change in that after you complete the normal logon, you receive a "password expired" notification.

For example, assume that you want to use 9999 as the new hard token pin, or 229999 if using a soft token.

With passphrase support (more than 8 characters allowed for the password):

- For a hard token, you will be prompted to enter a new password. Enter 9999 in new password field.
- For a soft token, you will be prompted to enter a new password. Enter 229999 in new password field.

Without passphrase support (maximum of 8 characters allowed for the password):

- For a hard token, you enter
123456 in the password field (unless the underlying software does this for you).
9999 in the new password field.
9999 in the verify new password field.
- For a soft token, you enter:
223344 in the password field.
229999 in new password field.
229999 in the verify new password field.

Note:

After the PIN change is done, you then need to re-validate with the new codes using the normal logon steps.

IBM TouchToken concepts

IBM MFA with IBM TouchToken includes an IBM TouchToken for iOS application and an IBM TouchToken one-time-password (OTP) as described in this section.

IBM TouchToken provides strong authentication by combining something you have (your iOS device provisioned with an IBM TouchToken account) and something you are (your fingerprint.) When logging on to your z/OS account with IBM TouchToken, you use the IBM TouchToken for iOS application to generate a one-time password (a token code) and use that token code in place of your RACF password.

IBM TouchToken OTP

IBM TouchToken combines Touch ID fingerprint biometric technology with a hashed, timed one-time password (OTP) for secure multi-factor authentication. You can consider the IBM TouchToken OTP to be a token code.

The IBM TouchToken for iOS application on the Apple device uses a shared secret key and the current time to generate token code values. IBM TouchToken on the z/OS system then uses the same algorithm to validate user logons.

IBM TouchToken requires Apple Touch ID fingerprint technology.

The token code generated by the IBM TouchToken for iOS application must fall within an approved sequence of token codes generated by the IBM TouchToken component on the z/OS server.

Token codes are regenerated at regular intervals. One-time token codes that are generated from the same secret key are identical if they are generated within a predetermined "token period" time value, which your security administrator can set at intervals of 15, 30, or 60 seconds, and a "window", which your security administrator can set from 1 to 10.

Your security administrator will provide you with the URL of the IBM TouchToken registration server start page. You visit this URL from your iOS web browser.

Preparing your Apple device for IBM TouchToken

You need to download the IBM TouchToken for iOS application to your supported Apple device and then connect to the IBM TouchToken registration (HTTP) server to create an account.

Before you begin

You must satisfy the following prerequisites:

- IBM TouchToken for iOS requires Touch ID. To use Touch ID you must enable a passcode and enroll one or more fingerprints. You should also ensure that your iOS device uses a complex alphanumeric passcode.

If you do not already have a complex alphanumeric passcode set on your iOS device, use **Settings > Touch ID and Passcode > Turn Passcode On (or Change Passcode) > Passcode Options > Custom Alphanumeric Code** to set one.

- IBM TouchToken is secured with TLS. Depending on the TLS configuration of the IBM TouchToken registration server, your security administrator may instruct you to download and install an additional Root CA certificate to a Configuration Profile in the iOS device. Never do this without explicit guidance from your security administrator. You can then optionally view this profile from the iOS device **Settings > General > Profile** page.

Procedure

Perform the following steps:

1. Download and install the IBM TouchToken for iOS application from the App Store on your Apple Touch ID device.
2. Use Mobile Safari or a desktop browser to invoke the URL for the IBM TouchToken registration server. Your system administrator will provide you with this URL.
The page explains some basic information about IBM TouchToken, and contains both a QR code and a link that launch the IBM TouchToken for iOS application.
3. If using a desktop browser, scan the QR code with your iOS device camera. If using Mobile Safari, tap the "Launch URL" link.
This launches the IBM TouchToken for iOS application and begins registration for a new IBM TouchToken account.
4. Tap "Begin Account Registration."
5. Enter your RACF user ID and current RACF password or passphrase. Tap Done.
6. The Set Token Alias screen includes the user ID and the touch token realm name. For security purposes, enter an alternate alias and click Save. This step is not required, but it is a Best Practice.
7. Tap Done on the Account Added screen.
8. On the IBM TouchToken screen, tap the account you just created.
9. When prompted, enter your touch ID fingerprint.
10. The application negotiates with the IBM TouchToken registration server and creates an OTP token.
11. Use this OTP token to log on to the z/OS system.

IBM MFA Out-of-Band concepts

IBM MFA Out-of-Band authentication requires you to authenticate "out-of-band" with one or more factors to retrieve an in-band authentication code called a "cache token credential." Your security administrator must specifically configure your account for IBM MFA Out-of-Band.

In IBM MFA Out-of-Band authentication, you authenticate "out-of-band" with one or more authentication factors configured by your security administrator. A user-specific IBM MFA Out-of-Band login page prompts you for all of the authentication factors you must provide.

You follow the same process and provide the same information as you would for these factors without IBM MFA Out-of-Band, except that you enter the tokens on the login web page and not in your z/OS application.

You connect to the URL provided by your administrator and log on with your RACF user name and password or passphrase. You are then presented with a list of authentication policies. Each policy defines the factors you must supply and whether the cache token credentials can be reused and for how long they can be reused. When you select an authentication policy, you are then presented with the list of factors required to satisfy the policy.

The important thing to note is that **all** configured authentication factors must succeed for you to receive the in-band authentication code. For example, if your account were to be configured for IBM MFA with SecurID and IBM TouchToken, both must succeed.

If successful, you receive a *cache token credential (CTC)* that you use to log in to the z/OS application.

General logon approach

As a general rule, if you are presented with an in-band request for logon credentials, enter your IBM MFA credentials.

If you are presented with a request for in-band logon credentials, try your IBM MFA credentials first. This is true even if your account is configured to use PassTickets, because you may be required to first log on with IBM MFA.

For IBM MFA Out-of-Band, a user-specific web page prompts you for all of the authentication credentials you must provide.

Chapter 2. IBM MFA Out-of-Band authentication

IBM MFA Out-of-Band authentication requires you to authenticate "out-of-band" with one or more factors to retrieve a cache token credential, which you then use as your password with a z/OS application.

Your administrator must configure your account for IBM MFA Out-of-Band and will tell you whether you must use the IBM MFA Out-of-Band web page to log on.

The administrator will provide you with the URL to use.

When prompted by the IBM MFA Out-of-Band web page, you must provide the required token(s). How you obtain the required token varies by token type.

You follow the same process and provide the same information as you would for these factors without IBM MFA Out-of-Band, except that you enter the tokens on the login web page and not in your z/OS application.

IBM MFA with SecurID

1. For a SecurID token without a PINpad, get the 6- to 8-digit token code displayed by the token.
2. For a SecurID token with a PINpad (hardware or soft token), enter your PIN in the token and get the displayed passcode.
3. Provide it to the IBM MFA Out-of-Band web page when prompted.
4. Use the generated cache token credential as your password with the z/OS application.

IBM TouchToken

1. Follow the steps described in [“Preparing your Apple device for IBM TouchToken”](#) on page 6 to generate the OTP token.
2. Provide it to the IBM MFA Out-of-Band web page when prompted.
3. Use the generated cache token credential as your password with the z/OS application.

IBM MFA for generic RADIUS

How you log in depends entirely on how your administrator has configured the RADIUS server. You may need to supply a valid passcode, PIN, or some other credential. Your administrator will provide you with this information.

1. Provide the RADIUS credential to the IBM MFA Out-of-Band web page when prompted.
2. Use the generated cache token credential as your password with the z/OS application.

IBM MFA for SafeNet RADIUS

Your administrator will tell you which Gemalto SafeNet configuration applies to you.

1. In challenge-response mode, enter any single alphabetic character in the IBM MFA Out-of-Band passcode field. Copy the generated challenge and enter it in the MobilePASS application to generate a passcode.

In Quick Log mode, you do not have to perform this step.

2. Get the 6- to 8-digit token passcode displayed by the MobilePASS token.
3. For a "server-side user select" PIN, provide your PIN followed by the passcode to the IBM MFA Out-of-Band web page when prompted.

For a "user selected" PIN, provide only the passcode to the IBM MFA Out-of-Band web page when prompted.

4. Use the generated cache token credential as your password with the z/OS application.

IBM MFA Certificate Authentication

1. When prompted by the IBM MFA Out-of-Band web page, select the client certificate you want to use to authenticate yourself. Your security administrator will typically provide guidance on which certificate to use.

Note: If you are using Internet Explorer, be aware that the Windows Internet Options "Don't prompt for client certificate selection when only one certificate exists" setting can result in your not having to choose a certificate. The "Don't prompt for client certificate selection when only one certificate exists" setting is typically controlled by the system administrator.

2. For PIV/CAC cards, you must then enter your valid PIN.
3. Use the generated cache token credential as your password with the z/OS application.

IBM MFA for YubiKey

1. Use your YubiKey to generate an OTP in the **Yubico OTP credential** field
2. Use the generated cache token credential as your password with the z/OS application.

IBM MFA for LDAP

1. Use your LDAP in the **Enter LDAP password.** field
2. Use the generated cache token credential as your password with the z/OS application.

Enrolling your certificate for IBM MFA Certificate Authentication

If your administrator has configured your account for IBM MFA Certificate Authentication as part of IBM MFA Out-of-Band, you must enroll your certificate before you can use it to log on.

Before you begin

It is a Best Practice to clear your Windows system SSL state before enrolling your certificate. To do this, select **Control Panel > Internet Options > Content > Clear SSL State**.

In addition, from **Control Panel > Internet Options > Content > Advanced**, ensure that Use "SSL 2.0" and "Use SSL 3.0" are both unchecked.

About this task

You must enroll your certificate before you can use it to log on with IBM MFA Certificate Authentication. The process requires action by both the administrator and the user, and the actions must occur in the correct sequence. Perform these steps only as directed by your administrator.

Note: This procedure has been verified with Microsoft Internet Explorer and Google Chrome.

Procedure

1. Clear your Windows system SSL state.
2. When instructed to do so by your administrator, begin the IBM MFA Certificate Authentication logon process at the web server login page provided by the administrator, such as `https://servername:port/AZFCERT1/enroll`.

Use your RACF userid to access the IBM MFA Out of Band login interface.

User ID:
Password:

3. On the Enrollment page, click on "Begin Certificate Enrollment."

```
AZFCERT1 Enrollment
Ensure that you have a certificate available to enroll.
AZFCERT1
Begin Certificate Enrollment
```

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

Note: If you are using Internet Explorer, be aware that the Windows Internet Options "Don't prompt for client certificate selection when only one certificate exists" setting can result in your not having to choose a certificate. The "Don't prompt for client certificate selection when only one certificate exists" setting is typically controlled by the system administrator.

For PIV/CAC or other smart cards, you must then enter your valid PIN.

Note: If you receive an error indicating that the server certificate is invalid, it is more likely that the certificate you chose is invalid.

5. If successful, you receive a message indicating the certificate enrollment succeeded and to await further instruction from the administrator.

```
AZFCERT1 Enrollment
Ensure that you have a certificate available to enroll.

AZFCERT1 -[Succeeded]
Certificate enrollment succeeded. Your certificate is tagged for Review.
An administrator will notify you when it is Approved. Please close
your browser window.
```

The administrator will tell you when you can use the certificate to log on, as described in [“Logging in to an application with IBM MFA Out-of-Band”](#) on page 11.

6. Close the browser window to end the session.

Logging in to an application with IBM MFA Out-of-Band

You use the IBM MFA Out-of-Band logon web page to provide the required authentication tokens. Your security administrator has determined which tokens you must provide.

About this task

Your security administrator will tell you if you need to use IBM MFA Out-of-Band to log in. If you are required to use IBM MFA Out-of-Band to log in and you do not, you receive a reminder error message.

Note: This procedure has been verified with Microsoft Internet Explorer and Google Chrome.

Procedure

Perform the following steps:

1. Use a web browser to connect to the bookmark provided by your security administrator, typically `https://servername:port/mfa/policy-name`.
2. Follow the web interface to enter the required tokens.

Note: Your administrator determines the maximum amount of time you have to complete all authentication factors, starting from the time you successfully entered your RACF user name. If you do not complete all authentication factors within this time period, you must start over.

3. As you successfully enter the required tokens, the IBM MFA Out-of-Band web page prompts you for the next one.
4. When you have satisfied all of your token requirements, the IBM MFA Out-of-Band web page displays the cache token credential.

Cache Token Credential
You have satisfied the authentication policy.
CREDENTIAL
Click the above Cache Token Credential to copy it to Clipboard,
and use this in place of your password to access applications

5. Manually enter or copy/paste the cache token credential as your password, as appropriate.

Note: If you are using Internet Explorer and use the cache token credential copy feature, be aware that Windows Internet Options settings can affect its function. Specifically, the "Allow Programmatic Clipboard Access" setting in one or more applicable zones can disable this feature or require you to respond to an additional prompt. The "Allow Programmatic Clipboard Access" setting is typically controlled by the system administrator.

On the z/OS system, IBM MFA validates the cache token credential and allows or denies the logon.

Chapter 3. IBM MFA with SecurID in-band authentication

You can log in with your SecurID token. The steps you follow depend on the type of token you have.

TSO/E

How you log in to TSO/E with IBM MFA for SecurID enabled depends on the token type you are using, whether you have a valid PIN, and whether pass phrases are enabled.

IBM MFA SecurID

If the security administrator has enabled your account for IBM MFA, you no longer use your RACF password to log in. Instead, how you log in with TSO/E depends on the following SecurID token and TSO/E configuration choices made by your security administrator:

- What type of token do you have? See [“Types of token devices”](#) on page 3 for the supported token types.
- Whether you have a valid PIN, whether you must create a new one, or whether the system generates one for you. Your security administrator decides when you must change your PIN.
- Whether pass phrases are enabled. TSO/E passwords are typically a maximum of eight characters. However, it is possible for SecurID credentials to exceed eight characters. Therefore, your security administrator may have selected an alternate TSO/E logon panel that allows you to enter longer passwords called pass phrases in the Password field.

General guidelines

Observe the following guidelines:

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

Fob-style hardware token

Several TSO/E login options are available for use with IBM MFA if you are using a hardware token without a PINpad.

Consult [Table 1 on page 14](#) to determine which login option matches your specific configuration and then follow the link to the related section.

Table 1. TSO/E Logon Options for a fob-style hardware token.

Token type	Valid PIN?	Pass phrases enabled?	Use this login choice...
Fob-style hardware token	Yes	No	“Logging in with valid PIN, no passphrase” on page 14
	Yes	Yes	“Logging in with valid PIN, with passphrase” on page 14
	No	No	“Logging in without valid PIN or passphrase” on page 14
	No	Yes	“Logging in without valid PIN, with passphrase” on page 15

Logging in with valid PIN, no passphrase

You can log in to TSO/E with a valid PIN without using pass phrases. This use case requires a fob-style hardware token.

Procedure

Perform the following steps:

1. Begin to log in to TSO/E with your user name.
2. Get the 6- to 8-digit token code displayed by the SecurID token.
3. Enter the 6- to 8-digit token code displayed by the SecurID token in the Password field.
4. Enter your PIN in the New Password field and press Enter.
The LOGON panel appears again.
5. Re-enter your PIN to confirm it and press Enter.

Logging in with valid PIN, with passphrase

You can log in to TSO/E with a valid PIN when using pass phrases. This use case requires a fob-style hardware token.

Procedure

Perform the following steps:

1. Begin to log in to TSO/E with your user name.
2. Get the 6- to 8-digit token code displayed by the SecurID token.
3. Enter your PIN **followed by** the 6- to 8-digit token code displayed by the SecurID token in the Password field. For example, if your PIN is 4321 and your token code is 456789, enter 4321456789 in the Password field.
4. Press Enter.

Logging in without valid PIN or passphrase

You can log in to TSO/E without a currently valid PIN and without using pass phrases. This use case requires a fob-style hardware token.

Procedure

Perform the following steps:

1. Begin to log in to TSO/E with your user name.
2. Get the 6- to 8-digit token code displayed by the SecurID token.
3. Enter the 6- to 8-digit token code displayed by the SecurID token in the Password field. Leave the New Password field empty. Press Enter.
If the token code is accepted, a status message indicates that you must enter a new 4- to 8-digit PIN.

Note: Do not enter the new PIN on the status message page.

4. Press Enter.
The LOGON panel is displayed and you are prompted to enter a new password.
5. Enter a new PIN in the New Password field and press Enter. (If you are prompted with a system-generated PIN, use that PIN. You might also be prompted to use either the system-generated PIN or your own.)
6. Confirm the PIN.
If accepted, the "new PIN accepted" message is displayed.
7. Press Enter to return to the LOGON panel.
8. Because you changed the PIN, you must log in again. Wait for the token code displayed by the SecurID token to change and get the new token code.
9. Enter the token code displayed by the SecurID token in the Password field.
10. Enter the PIN in the New Password field and press Enter.

Logging in without valid PIN, with passphrase

You can log in to TSO/E without a currently valid PIN using pass phrases. This use case requires a fob-style hardware token.

Procedure

Perform the following steps:

1. Begin to log in to TSO/E with your user name.
2. Get the 6- to 8-digit token code displayed by the SecurID token.
3. Enter the 6- to 8-digit token code displayed by the SecurID token in the Password field. Press Enter.
If the token code is accepted, a status message indicates that you must enter a new 4- to 8-digit PIN.

Note: Do not enter the new PIN on the status message page.

4. Press Enter.
The LOGON panel is displayed and you are prompted to enter a new password.
5. Enter a new PIN in the Password field and press Enter. (If you are prompted with a system-generated PIN, use that PIN. You might also be prompted to use either the system-generated PIN or your own.)
6. Confirm the PIN.
If accepted, the "new PIN accepted" message is displayed.
7. Press Enter to return to the LOGON panel.
8. Because you changed the PIN, you must log in again. Wait for the token code displayed by the SecurID token to change. Get the new token code.
9. Enter your PIN **followed by** the 6- to 8-digit token code displayed by the SecurID token in the Password field. Press Enter.

Logging in with valid PIN and passphrase with compound in-band authentication

You can log in to TSO/E with a valid PIN when using pass phrases. Your administrator must have configured your account for IBM MFA Compound In-Band. This use case requires a fob-style hardware token.

About this task

Important: If your RACF password has expired, you are prompted during the compound in-band login session to change your RACF password. However, after attempting to change your password, the IBM MFA credentials are then replayed, which causes the password change operation to fail. In this case, begin a new TSO/E session, log in with your existing password and IBM MFA credentials, and then use the **-New Password** option on the panel to change your RACF password.

Procedure

Perform the following steps:

1. Begin to log in to TSO/E with your user name.
2. Get the 6- to 8-digit token code displayed by the SecurID token.
3. Enter your PIN **followed by** the 6- to 8-digit token code displayed by the SecurID token, **followed by the separator, followed by** your passphrase or password in the Password field.
For example, assume the separator is the colon (:). If your PIN is 4321 your token code is 456789, and your password is 12345678, enter 4321456789:12345678 in the Password field.
Note: Your security administrator can reverse the order in which you enter the credentials, so that you enter your passphrase or password first, followed by the separator. Consult your security administrator for guidance.
4. Press Enter.

Hardware token with a PINpad

Several TSO/E login options are available for use with IBM MFA if you are using a hardware token with a PINpad.

Consult Table 2 on page 16 to determine which login option matches your specific configuration and then follow the link to the related section.

Table 2. TSO/E Logon Options for a hardware token with a PINpad.			
Token type	Valid PIN?	Pass phrases enabled?	Use this login choice...
Hardware token (with PINpad)	Yes	No	“Logging in with valid PIN, no passphrase” on page 16
	Yes	Yes	“Logging in with valid PIN, with passphrase” on page 16
	No	No	“Logging in without valid PIN or passphrase” on page 17
	No	Yes	“Logging in without valid PIN, with passphrase” on page 17

Logging in with valid PIN, no passphrase

You can log in to TSO/E with a valid PIN without using pass phrases. This use case requires a hardware token with a PINpad.

Procedure

Perform the following steps:

1. Begin to log in to TSO/E with your user name.
2. Enter your PIN in the SecurID token and generate a passcode.
3. Enter the 6- to 8-digit passcode displayed by the SecurID token in the Password field.
4. Leave the New Password field empty.
5. Press Enter.

Logging in with valid PIN, with passphrase

You can log in to TSO/E with a valid PIN when using pass phrases. This use case requires a hardware token with a PINpad.

Procedure

Perform the following steps:

1. Begin to log in to TSO/E with your user name.

2. Enter your PIN in the SecurID token and generate a passcode.
3. Enter the 6- to 8-digit passcode displayed by the SecurID token in the Password field.
4. Press Enter.

Logging in without valid PIN or passphrase

You can log in to TSO/E without a currently valid PIN and without using pass phrases. This use case requires a hardware token with a PINpad.

Procedure

Perform the following steps:

1. Begin to log in to TSO/E with your user name.
2. Generate a token code on the SecurID token without entering a PIN.
3. Get the 6- to 8-digit token code displayed by the SecurID token.
4. Enter the 6- to 8-digit token code displayed by the SecurID token in the Password field. Leave the New Password field empty. Press Enter.
If the token code is accepted, a status message indicates that you must enter a new 4- to 8-digit PIN.

Note: Do not enter the new PIN on the status message page.

5. Press Enter.
The LOGON panel is displayed and you are prompted to enter a new password.
6. Enter a new PIN in the New Password field and press Enter. (If you are prompted with a system-generated PIN, use that PIN. You might also be prompted to use either the system-generated PIN or your own.)
7. Confirm the new PIN.
The "new PIN accepted" message is displayed.
8. Press Enter to return to the LOGON panel.
9. Because you changed the PIN, you must log in again. Wait for the token displayed by the SecurID token to change. Enter your PIN and generate a new passcode.
10. Enter the passcode displayed by the SecurID token in the Password field.
11. Leave the New Password field empty.
12. Press Enter.

Logging in without valid PIN, with passphrase

You can log in to TSO/E without a currently valid PIN using pass phrases. This use case requires a hardware token with a PINpad.

Procedure

Perform the following steps:

1. Begin to log in to TSO/E with your user name.
2. Generate a token code on the SecurID token without entering a PIN.
3. Get the 6- to 8-digit token code displayed by the SecurID token.
4. Enter the 6- to 8-digit token code displayed by the SecurID token in the Password field and press Enter.
If the token code is accepted, a status message indicates that you must enter a new 4- to 8-digit PIN.

Note: Do not enter the new PIN on the status message page.

5. Press Enter.
The LOGON panel is displayed and you are prompted to enter a new password.
6. Enter a new PIN in the Password field and press Enter. (If you are prompted with a system-generated PIN, use that PIN. You might also be prompted to use either the system-generated PIN or your own.)
7. Confirm the new PIN.
The "new PIN accepted" message is displayed.

8. Press Enter to return to the LOGON panel.
9. Because you changed the PIN, you must log in again. Wait for the token code displayed by the SecurID token to change. Enter your PIN and generate a passcode.
10. Enter the passcode displayed by the SecurID token in the Password field.
11. Press Enter.

Logging in with valid PIN and passphrase with compound in-band authentication

You can log in to TSO/E with a valid PIN when using pass phrases. Your administrator must have configured your account for IBM MFA Compound In-Band. This use case requires a hardware token with a PINpad.

About this task

Important: If your RACF password has expired, you are prompted during the compound in-band login session to change your RACF password. However, after attempting to change your password, the IBM MFA credentials are then replayed, which causes the password change operation to fail. In this case, begin a new TSO/E session, log in with your existing password and IBM MFA credentials, and then use the **-New Password** option on the panel to change your RACF password.

Procedure

Perform the following steps:

1. Begin to log in to TSO/E with your user name.
2. Enter your PIN in the SecurID token and generate a passcode.
3. Enter the 6- to 8-digit passcode displayed by the SecurID token, **followed by the separator, followed by** your passphrase or password in the Password field.

Note: Your security administrator can reverse the order in which you enter the credentials, so that you enter your passphrase or password first, followed by the separator. Consult your security administrator for guidance.

4. Press Enter.

Soft token

Several TSO/E login options are available for use with IBM MFA.

Consult [Table 3 on page 18](#) to determine which login option matches your specific configuration and then follow the link to the related section.

Table 3. TSO/E Logon Options for a soft token.			
Token type	Valid PIN?	Pass phrases enabled?	Use this login choice...
soft token	Yes	No	“Logging in with valid PIN, no passphrase” on page 19
	Yes	Yes	“Logging in with valid PIN, with passphrase” on page 19
	No	No	“Logging in without valid PIN or passphrase” on page 19
	No	Yes	“Logging in without valid PIN, with passphrase” on page 20

Logging in with valid PIN, no passphrase

You can log in to TSO/E with a valid PIN without using pass phrases. This use case requires a soft token.

Procedure

Perform the following steps:

1. Begin to log in to TSO/E with your user name.
2. Enter your PIN in the soft token application and generate a 6- to 8-digit passcode.
3. Use the copy feature to copy the passcode.
4. Paste the passcode displayed by the SecurID token in the Password field.
5. Leave the New Password field empty.
6. Press Enter.

Logging in with valid PIN, with passphrase

You can log in to TSO/E with a valid PIN when using pass phrases. This use case requires a soft token.

Procedure

Perform the following steps:

1. Begin to log in to TSO/E with your user name.
2. Enter your PIN in the soft token application and generate a 6- to 8-digit passcode.
3. Use the copy feature to copy the passcode.
4. Paste the passcode displayed by the SecurID token in the Password field.
5. Press Enter.

Logging in without valid PIN or passphrase

You can log in to TSO/E without a valid PIN and without using pass phrases. This use case requires a soft token.

Procedure

Perform the following steps:

1. Begin to log in to TSO/E with your user name.
2. Generate a token code on the SecurID token without entering a PIN. Use the copy feature to copy the token code.
3. Paste the 6- to 8-digit token code displayed by the SecurID token in the Password field. Leave the New Password field empty. Press Enter.
If the token code is accepted, a status message indicates that you must enter a new 4- to 8-digit PIN.

Note: Do not enter the new PIN on the status message page.

4. Press Enter.
The LOGON panel is displayed and you are prompted to enter a new password.
5. Enter a new PIN in the New Password field and press Enter. (If you are prompted with a system-generated PIN, use that PIN. You might also be prompted to use either the system-generated PIN or your own.)
6. Confirm the new PIN.
The "new PIN accepted" message is displayed.
7. Press Enter to return to the LOGON panel.
8. Because you changed the PIN, you must log in again. Wait for the token displayed by the SecurID token to change. Enter your PIN and generate a new passcode. Use the copy feature to copy the passcode.
9. Paste the passcode displayed by the SecurID token in the Password field.
10. Leave the New Password field empty.
11. Press Enter.

Logging in without valid PIN, with passphrase

You can log in to TSO/E without a currently valid PIN using pass phrases. This use case requires a soft token.

Procedure

Perform the following steps:

1. Begin to log in to TSO/E with your user name.
2. Generate a token code on the SecurID token without entering a PIN. Use the copy feature to copy the token code.
3. Paste the 6- to 8-digit token code displayed by the SecurID token in the Password field. Press Enter. If the token code is accepted, a status message indicates that you must enter a new 4- to 8-digit PIN.

Note: Do not enter the new PIN on the status message page.

4. Press Enter.
The LOGON panel is displayed and you are prompted to enter a new password.
5. Enter a new PIN in the Password field and press Enter. (If you are prompted with a system-generated PIN, use that PIN. You might also be prompted to use either the system-generated PIN or your own.)
6. Confirm the new PIN.
The "new PIN accepted" message is displayed.
7. Press Enter to return to the LOGON panel.
8. Because you changed the PIN, you must log in again. Wait for the token displayed by the SecurID token to change. Enter your PIN and generate a new passcode. Use the copy feature to copy the passcode.
9. Paste the passcode displayed by the SecurID token in the Password field.
10. Press Enter.

Logging in with valid PIN and passphrase with compound in-band authentication

You can log in to TSO/E with a valid PIN when using pass phrases. Your administrator must have configured your account for IBM MFA Compound In-Band. This use case requires a soft token.

About this task

Important: If your RACF password has expired, you are prompted during the compound in-band login session to change your RACF password. However, after attempting to change your password, the IBM MFA credentials are then replayed, which causes the password change operation to fail. In this case, begin a new TSO/E session, log in with your existing password and IBM MFA credentials, and then use the **-New Password** option on the panel to change your RACF password.

Procedure

Perform the following steps:

1. Begin to log in to TSO/E with your user name.
2. Enter your PIN in the soft token application and generate a 6- to 8-digit passcode.
3. Use the copy feature to copy the passcode.
4. Paste the passcode displayed by the SecurID token in the Password field, **followed by the separator, followed by** your passphrase or password.

Note: Your security administrator can reverse the order in which you enter the credentials, so that you enter your passphrase or password first, followed by the separator. Consult your security administrator for guidance.

5. Press Enter.

CICS CESL transaction

How you log in to a CICS CESL transaction with IBM MFA enabled depends on the token type you are using and whether you have a valid PIN.

IBM MFA SecurID

If the security administrator has enabled your account for IBM MFA, you no longer use your z/OS password to log in. Instead, how you log in with CICS depends on the following SecurID token and CICS configuration choices made by your security administrator.

- What type of token do you have? See “Types of token devices” on page 3 for the supported token types.
- Whether you have a currently valid PIN or whether you must create a new one. Your security administrator decides when you must change your PIN.

General guidelines

Observe the following guidelines:

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

Fob-style hardware token

Several CICS CESL login options are available for use with IBM MFA if you are using a fob-style hardware token.

Consult [Table 4 on page 21](#) to determine which login option matches your specific configuration and then follow the link to the related section.

Table 4. CICS Logon Options for a fob-style hardware token.		
Token type	Valid PIN?	Use this login choice...
Fob-style hardware token	Yes	“Logging in with valid PIN” on page 21
	No	“Logging in without valid PIN” on page 22

Logging in with valid PIN

You can log in to a CICS CESL transaction with a valid PIN. This use case requires a fob-style hardware token.

Procedure

Perform the following steps:

1. Begin to log in to the CICS CESL transaction with your user name.
2. Get the 6- to 8-digit token code displayed by the SecurID token.
3. Enter your PIN **followed by** the 6- to 8-digit token code displayed by the SecurID token in the Password field. For example, if your PIN is 4321 and your token code is 456789, enter 4321456789 in the Password field.
4. Leave the New Password field empty.
5. Press Enter.

Logging in without valid PIN

You can log in to a CICS CESL transaction without a currently valid PIN. This use case requires a fob-style hardware token.

Procedure

Perform the following steps:

1. Begin to log in to the CICS CESL transaction with your user name.
2. Get the 6- to 8-digit token code displayed by the SecurID token.
3. Enter the 6- to 8-digit token code displayed by the SecurID token in the Password field. Leave the New Password field empty. Press Enter.
The message "DFHCE3525 Your password has expired. Please type your new password." is displayed.
4. Enter a new PIN in the New Password field and press Enter. Confirm the new PIN.
The message "DFHCE3532 Your userid or password is invalid. Please retype both." is displayed.
5. Because you changed the PIN, you must log in again. Wait for the token code displayed by the SecurID token to change and get the new token code.
6. Enter your PIN **followed by** the 6- to 8-digit token code displayed by the SecurID token in the Password field.
7. Leave the New Password field empty.
8. Press Enter.

Logging in with valid PIN with compound in-band authentication

You can log in to a CICS CESL transaction with a valid PIN. Your administrator must have configured your account for IBM MFA Compound In-Band. This use case requires a fob-style hardware token.

Procedure

Perform the following steps:

1. Begin to log in to the CICS CESL transaction with your user name.
2. Get the 6- to 8-digit token code displayed by the SecurID token.
3. Enter your PIN **followed by** the 6- to 8-digit token code displayed by the SecurID token, **followed by the separator, followed by** your passphrase or password in the Password field. For example, assume that the separator is the colon (:). If your PIN is 4321, your token code is 456789, and your password is 12345678, enter 4321456789:12345678 in the Password field.

Note: Your security administrator can reverse the order in which you enter the credentials, so that you enter your passphrase or password first, followed by the separator. Consult your security administrator for guidance.

4. Leave the New Password field empty.
5. Press Enter.

Hardware token with a PINpad

Several CICS CESL login options are available for use with IBM MFA if you are using a hardware token with a PINpad.

Consult [Table 5 on page 23](#) to determine which login option matches your specific configuration and then follow the link to the related section.

Table 5. CICS Logon Options for a hardware token with a PINpad.

Token type	Valid PIN?	Use this login choice...
Hardware token (with PINpad)	Yes	“Logging in with valid PIN” on page 23
	No	“Logging in without valid PIN” on page 23

Logging in with valid PIN

You can log in to a CICS CESL transaction with a valid PIN. This use case requires a hardware token with a PINpad.

Procedure

Perform the following steps:

1. Begin to log in to a CICS CESL transaction with your user name.
2. Enter your PIN in the SecurID token and generate a passcode.
3. Enter the 6- to 8-digit passcode displayed by the SecurID token in the Password field.
4. Leave the New Password field empty.
5. Press Enter.

Logging in without valid PIN

You can log in to a CICS CESL transaction without a currently valid PIN. This use case requires a hardware token with a PINpad.

Procedure

Perform the following steps:

1. Begin to log in to a CICS CESL transaction with your user name.
2. Generate a token code on the SecurID token without entering a PIN.
3. Get the 6- to 8-digit token code displayed by the SecurID token.
4. Enter the 6- to 8-digit token code displayed by the SecurID token in the Password field. Leave the New Password field empty. Press Enter.
The message "DFHCE3525 Your password has expired. Please type your new password." is displayed.
5. Enter a new PIN in the New Password field and press Enter. Confirm the new PIN.
The message "DFHCE3532 Your userid or password is invalid. Please retype both." is displayed.
6. Because you changed the PIN, you must log in again. Wait for the token displayed by the SecurID token to change. Enter your PIN and generate a passcode.
7. Enter the passcode displayed by the SecurID token in the Password field.
8. Leave the New Password field empty.
9. Press Enter.

Logging in with valid PIN with compound in-band authentication

You can log in to a CICS CESL transaction with a valid PIN. Your administrator must have configured your account for IBM MFA Compound In-Band. This use case requires a hardware token with a PINpad.

Procedure

Perform the following steps:

1. Begin to log in to a CICS CESL transaction with your user name.
2. Enter your PIN in the SecurID token and generate a passcode.
3. Enter the 6- to 8-digit passcode displayed by the SecurID token, **followed by the separator, followed by** your passphrase or password in the Password field.

Note: Your security administrator can reverse the order in which you enter the credentials, so that you enter your passphrase or password first, followed by the separator. Consult your security administrator for guidance.

4. Leave the New Password field empty.
5. Press Enter.

Soft token

Several CICS CESL login options are available for use with IBM MFA.

Consult [Table 6 on page 24](#) to determine which login option matches your specific configuration and then follow the link to the related section.

Table 6. CICS Logon Options for a soft token.		
Token type	Valid PIN?	Use this login choice...
Soft Token	Yes	“Logging in with valid PIN” on page 24
	No	“Logging in without valid PIN” on page 24

Logging in with valid PIN

You can log in to a CICS CESL transaction with a valid PIN. This use case requires a soft token.

Procedure

Perform the following steps:

1. Begin to log in to a CICS CESL transaction with your user name.
2. Enter your PIN in the soft token application and generate a 6- to 8-digit passcode.
3. Use the copy feature to copy the passcode.
4. Paste the passcode displayed by the SecurID token in the Password field.
5. Leave the New Password field empty.
6. Press Enter.

Logging in without valid PIN

You can log in to a CICS CESL transaction without a currently valid PIN. This use case requires a soft token.

Procedure

Perform the following steps:

1. Begin to log in to a CICS CESL transaction with your user name.
2. Generate a token code on the SecurID token without entering a PIN. Use the copy feature to copy the token code.
3. Enter the 6- to 8-digit token code displayed by the SecurID token in the Password field. Leave the New Password field empty. Press Enter.
The message "DFHCE3525 Your password has expired. Please type your new password." is displayed.
4. Enter a new PIN in the New Password field and press Enter. Confirm the new PIN.
The message "DFHCE3532 Your userid or password is invalid. Please retype both." is displayed.
5. Because you changed the PIN, you must log in again. Wait for the token displayed by the SecurID token to change. Enter your PIN and generate a new passcode. Use the copy feature to copy the passcode.
6. Paste the passcode displayed by the SecurID token in the Password field.

7. Leave the New Password field empty.
8. Press Enter.

Logging in with valid PIN with compound in-band authentication

You can log in to a CICS CESL transaction with a valid PIN. Your administrator must have configured your account for IBM MFA Compound In-Band. This use case requires a soft token.

Procedure

Perform the following steps:

1. Begin to log in to a CICS CESL transaction with your user name.
2. Enter your PIN in the soft token application and generate a 6- to 8-digit passcode.
3. Use the copy feature to copy the passcode.
4. Paste the passcode displayed by the SecurID token, **followed by the separator, followed by** your passphrase or password in the Password field.

Note: Your security administrator can reverse the order in which you enter the credentials, so that you enter your passphrase or password first, followed by the separator. Consult your security administrator for guidance.

5. Leave the New Password field empty.
6. Press Enter.

z/OS Management Facility

How you log in to IBM z/OS Management Facility (z/OSMF) with IBM MFA enabled depends on the token type you are using. You must already have a valid PIN.

IBM MFA SecurID

If the security administrator has enabled your account for IBM MFA, you no longer use your z/OS password to log in. Instead, how you log in with z/OSMF depends on the type of token you have. See [“Types of token devices”](#) on page 3 for the supported token types.

General guidelines

Observe the following guidelines:

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

Logging in with a fob-style hardware token

You can log in to z/OSMF with a valid PIN. This use case requires a fob-style hardware token.

Procedure

Perform the following steps:

1. Begin to log in to z/OSMF with your user name.
2. Get the 6- to 8-digit token code displayed by the SecurID token.
3. Enter your PIN **followed by** the 6- to 8-digit token code displayed by the SecurID token in the Password field. For example, if your PIN is 4321 and your token code is 456789, enter 4321456789 in the Password field.
4. Press Enter.

Logging in with a hardware token with a PINpad

You can log in to z/OSMF with a valid PIN. This use case requires a hardware token with a PINpad.

Procedure

Perform the following steps:

1. Begin to log in to z/OSMF with your user name.
2. Enter your PIN in the SecurID token and generate a passcode.
3. Enter the 6- to 8-digit passcode displayed by the SecurID token in the Password field.
4. Press Enter.

Logging in with a soft token

You can log in to z/OSMF with a valid PIN. This use case requires a soft token.

Procedure

Perform the following steps:

1. Begin to log in to z/OSMF with your user name.
2. Enter your PIN in the soft token application and generate a 6- to 8-digit passcode.
3. Use the copy feature to copy the passcode.
4. Paste the passcode displayed by the SecurID token in the Password field.
5. Press Enter.

z/OS Management Facility with compound in-band authentication

How you log in to IBM z/OS Management Facility (z/OSMF) with IBM MFA Compound In-Band enabled depends on the token type you are using. You must already have a valid PIN.

IBM MFA SecurID

If the security administrator has enabled your account for IBM MFA, you no longer use your z/OS password to log in. Instead, how you log in with z/OSMF depends on the type of token you have. See [“Types of token devices” on page 3](#) for the supported token types.

General guidelines

Observe the following guidelines:

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

Logging in with a fob-style hardware token

You can log in to z/OSMF with a valid PIN. Your administrator must have configured your account for IBM MFA Compound In-Band. This use case requires a fob-style hardware token.

Procedure

Perform the following steps:

1. Begin to log in to z/OSMF with your user name.
2. Get the 6- to 8-digit token code displayed by the SecurID token.
3. Enter your PIN **followed by** the 6- to 8-digit token code displayed by the SecurID token, **followed by the separator, followed by** your passphrase or password in the Password field. For example, assume the separator is the colon (:). If your PIN is 4321, your token code is 456789, and your password is 12345678, enter 4321456789:12345678 in the Password field.

Note: Your security administrator can reverse the order in which you enter the credentials, so that you enter your passphrase or password first, followed by the separator. Consult your security administrator for guidance.

4. Press Enter.

Logging in with a hardware token with a PINpad

You can log in to z/OSMF with a valid PIN. Your administrator must have configured your account for IBM MFA Compound In-Band. This use case requires a hardware token with a PINpad.

Procedure

Perform the following steps:

1. Begin to log in to z/OSMF with your user name.
2. Enter your PIN in the SecurID token and generate a passcode.
3. Enter the 6- to 8-digit passcode displayed by the SecurID token, **followed by the separator, followed by** your passphrase or password in the Password field.

Note: Your security administrator can reverse the order in which you enter the credentials, so that you enter your passphrase or password first, followed by the separator. Consult your security administrator for guidance.

4. Press Enter.

Logging in with a soft token

You can log in to z/OSMF with a valid PIN. Your administrator must have configured your account for IBM MFA Compound In-Band. This use case requires a soft token.

Procedure

Perform the following steps:

1. Begin to log in to z/OSMF with your user name.
2. Enter your PIN in the soft token application and generate a 6- to 8-digit passcode.
3. Use the copy feature to copy the passcode.
4. Paste the passcode displayed by the SecurID token in the Password field, **followed by the separator, followed by** your passphrase or password.

Note: Your security administrator can reverse the order in which you enter the credentials, so that you enter your passphrase or password first, followed by the separator. Consult your security administrator for guidance.

5. Press Enter.

IBM FTP

How you log in to IBM FTP with IBM MFA enabled depends on the token type you are using. You must already have a valid PIN.

IBM MFA SecurID

If the security administrator has enabled your account for IBM MFA, you no longer use your z/OS password to log in. Instead, how you log in with IBM FTP depends on the type of token you have. See [“Types of token devices” on page 3](#) for the supported token types.

General guidelines

Observe the following guidelines:

- It is a best practice to wait until the token code changes before attempting to log in.
- You can use the token code only once.

- If you receive an authentication failure, wait until the token code changes before attempting to log in again.

Logging in with a fob-style hardware token

You can log in to IBM FTP with a valid PIN. This use case requires a fob-style hardware token.

Procedure

Perform the following steps:

1. Open an IBM FTP connection and enter your user name.
2. Press Enter.
3. Get the 6- to 8-digit token code displayed by the SecurID token.
4. Enter your PIN **followed by** the 6- to 8-digit token code displayed by the SecurID token in the password field. For example, if your PIN is 4321 and your token code is 456789, enter 4321456789 in the password field.
5. Press Enter.
If successful, IBM FTP displays PASS.

Logging in with a hardware token with a PINpad

You can log in to IBM FTP with a valid PIN. This use case requires a hardware token with a PINpad.

Procedure

Perform the following steps:

1. Open an IBM FTP connection and enter your user name.
2. Press Enter.
3. Enter your PIN in the SecurID token and generate a passcode.
4. Enter the 6- to 8-digit passcode displayed by the SecurID token in the password field.
5. Press Enter.
If successful, IBM FTP displays PASS.

Logging in with a soft token

You can log in to IBM FTP with a valid PIN. This use case requires a soft token application.

Procedure

Perform the following steps:

1. Open an IBM FTP connection and enter your user name.
2. Press Enter.
3. Enter your PIN in the soft token and generate a passcode. Use the copy feature to copy the passcode.
4. Paste the 6- to 8-digit passcode displayed by the soft token in the password field.
5. Press Enter.
If successful, IBM FTP displays PASS.

IBM FTP with compound in-band authentication

How you log in to IBM FTP with IBM MFA Compound In-Band enabled depends on the token type you are using. You must already have a valid PIN.

IBM MFA SecurID

If the security administrator has enabled your account for IBM MFA, you no longer use your z/OS password to log in. Instead, how you log in with IBM FTP depends on the type of token you have. See [“Types of token devices” on page 3](#) for the supported token types.

General guidelines

Observe the following guidelines:

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

Logging in with a fob-style hardware token

You can log in to IBM FTP with a valid PIN. Your administrator must have configured your account for IBM MFA Compound In-Band. This use case requires a fob-style hardware token.

Procedure

Perform the following steps:

1. Open an IBM FTP connection and enter your user name.
2. Press Enter.
3. Get the 6- to 8-digit token code displayed by the SecurID token.
4. Enter your PIN **followed by** the 6- to 8-digit token code displayed by the SecurID token, **followed by the separator, followed by** your passphrase or password in the password field. For example, assume that the separator is the vertical bar (|). If your PIN is 4321, your token code is 456789, and your password is 12345678, enter 4321456789|12345678 in the password field.

Note: Your security administrator can reverse the order in which you enter the credentials, so that you enter your passphrase or password first, followed by the separator. Consult your security administrator for guidance.

5. Press Enter.
If successful, IBM FTP displays PASS.

Logging in with a hardware token with a PINpad

You can log in to IBM FTP with a valid PIN. Your administrator must have configured your account for IBM MFA Compound In-Band. This use case requires a hardware token with a PINpad.

Procedure

Perform the following steps:

1. Open an IBM FTP connection and enter your user name.
2. Press Enter.
3. Enter your PIN in the SecurID token and generate a passcode.
4. Enter the 6- to 8-digit passcode displayed by the SecurID token, **followed by the separator, followed by** your passphrase or password in the password field.

Note: Your security administrator can reverse the order in which you enter the credentials, so that you enter your passphrase or password first, followed by the separator. Consult your security administrator for guidance.

5. Press Enter.
If successful, IBM FTP displays PASS.

Logging in with a soft token

You can log in to IBM FTP with a valid PIN. Your administrator must have configured your account for IBM MFA Compound In-Band. This use case requires a soft token application.

Procedure

Perform the following steps:

1. Open an IBM FTP connection and enter your user name.
2. Press Enter.

3. Enter your PIN in the soft token and generate a passcode. Use the copy feature to copy the passcode.
4. Paste the 6- to 8-digit passcode displayed by the soft token in the password field, **followed by the separator, followed by** your passphrase or password.

Note: Your security administrator can reverse the order in which you enter the credentials, so that you enter your passphrase or password first, followed by the separator. Consult your security administrator for guidance.

5. Press Enter.
If successful, IBM FTP displays PASS.

IBM OpenSSH

How you log in to IBM OpenSSH with IBM MFA enabled depends on the token type you are using. You must already have a valid pin.

IBM MFA SecurID

If the security administrator has enabled your account for IBM MFA, you no longer use your z/OS password to log in. Instead, how you log in with IBM OpenSSH utilities depends on the type of token you have. See [“Types of token devices” on page 3](#) for the supported token types.

General guidelines

Observe the following guidelines:

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

Logging in with a fob-style hardware token

You can log in to IBM OpenSSH with a valid PIN. This use case requires a fob-style hardware token.

Procedure

Perform the following steps:

1. Open an OpenSSH utility connection to the z/OS system. Consider the following examples:

```
ssh user-name@your-host
```

```
scp files.txt user-name@your-host:/home/user-name
```

You are prompted for the password.

2. Get the 6- to 8-digit token code displayed by the SecurID token.
3. Enter your PIN **followed by** the 6- to 8-digit token code displayed by the SecurID token in the password field. For example, if your PIN is 4321 and your token code is 456789, enter 4321456789 in the password field.
4. Press Enter.
If successful, the OpenSSH command succeeds.

Logging in with a hardware token with a PINpad

You can log in to IBM OpenSSH with a valid PIN. This use case requires a hardware token with a PINpad.

Procedure

Perform the following steps:

1. Open an OpenSSH utility connection to the z/OS system. Consider the following examples:

```
ssh user-name@your-host
```

```
scp files.txt user-name@your-host:/home/user-name
```

You are prompted for the password.

2. Enter your PIN in the SecurID token and generate a passcode.
3. Enter the 6- to 8-digit passcode displayed by the SecurID token in the password field.
4. Press Enter.
If successful, the OpenSSH command succeeds.

Logging in with a soft token

You can log in to IBM OpenSSH with a valid PIN. This use case requires a soft token application.

Procedure

Perform the following steps:

1. Open an OpenSSH utility connection to the z/OS system. Consider the following examples:

```
ssh user-name@your-host
```

```
scp files.txt user-name@your-host:/home/user-name
```

You are prompted for the password.

2. Enter your PIN in the soft token and generate a passcode. Use the copy feature to copy the passcode.
3. Paste the 6- to 8-digit passcode displayed by the soft token in the password field.
4. Press Enter.
If successful, the OpenSSH command succeeds.

IBM OpenSSH with compound in-band authentication

How you log in to IBM OpenSSH with IBM MFA Compound In-Band enabled depends on the token type you are using. You must already have a valid pin.

IBM MFA SecurID

If the security administrator has enabled your account for IBM MFA, you no longer use your z/OS password to log in. Instead, how you log in with IBM OpenSSH utilities depends on the type of token you have. See [“Types of token devices” on page 3](#) for the supported token types.

General guidelines

Observe the following guidelines:

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

Logging in with a fob-style hardware token

You can log in to IBM OpenSSH with a valid PIN. Your administrator must have configured your account for IBM MFA Compound In-Band. This use case requires a fob-style hardware token.

Procedure

Perform the following steps:

1. Open an OpenSSH utility connection to the z/OS system. Consider the following examples:

```
ssh user-name@your-host
```

```
scp files.txt user-name@your-host:/home/user-name
```

You are prompted for the password.

2. Get the 6- to 8-digit token code displayed by the SecurID token.
3. Enter your PIN **followed by** the 6- to 8-digit token code displayed by the SecurID token, **followed by the separator, followed by** your passphrase or password in the password field. For example, assume that the separator is the colon(:). If your PIN is 4321, your token code is 456789, and your password is 12345678, enter 4321456789:12345678 in the password field.

Note: Your security administrator can reverse the order in which you enter the credentials, so that you enter your passphrase or password first, followed by the separator. Consult your security administrator for guidance.

4. Press Enter.
If successful, the OpenSSH command succeeds.

Logging in with a hardware token with a PINpad

You can log in to IBM OpenSSH with a valid PIN. Your administrator must have configured your account for IBM MFA Compound In-Band. This use case requires a hardware token with a PINpad.

Procedure

Perform the following steps:

1. Open an OpenSSH utility connection to the z/OS system. Consider the following examples:

```
ssh user-name@your-host
```

```
scp files.txt user-name@your-host:/home/user-name
```

You are prompted for the password.

2. Enter your PIN in the SecurID token and generate a passcode.
3. Enter the 6- to 8-digit passcode displayed by the SecurID token, **followed by the separator, followed by** your passphrase or password in the password field.

Note: Your security administrator can reverse the order in which you enter the credentials, so that you enter your passphrase or password first, followed by the separator. Consult your security administrator for guidance.

4. Press Enter.
If successful, the OpenSSH command succeeds.

Logging in with a soft token

You can log in to IBM OpenSSH with a valid PIN. Your administrator must have configured your account for IBM MFA Compound In-Band. This use case requires a soft token application.

Procedure

Perform the following steps:

1. Open an OpenSSH utility connection to the z/OS system. Consider the following examples:

```
ssh user-name@your-host
```

```
scp files.txt user-name@your-host:/home/user-name
```

You are prompted for the password.

2. Enter your PIN in the soft token and generate a passcode. Use the copy feature to copy the passcode.

3. Paste the 6- to 8-digit passcode displayed by the soft token in the password field, **followed by the separator, followed by** your passphrase or password.

Note: Your security administrator can reverse the order in which you enter the credentials, so that you enter your passphrase or password first, followed by the separator. Consult your security administrator for guidance.

4. Press Enter.
If successful, the OpenSSH command succeeds.

Chapter 4. IBM TouchToken in-band authentication

You can log in in-band with a valid IBM TouchToken OTP token code. This use case requires the IBM TouchToken for iOS application.

Logging in to TSO with IBM TouchToken

You can log in to TSO/E with a valid IBM TouchToken OTP token code. This use case requires the IBM TouchToken for iOS application.

Procedure

Perform the following steps:

1. Begin to log in to TSO/E with your user name.
2. Run the IBM TouchToken for iOS application.
3. Tap the account you created to select it.
4. Use your Touch ID fingerprint on the IBM TouchToken for iOS application to generate the IBM TouchToken OTP. This OTP is valid for 15, 30, or 60 seconds as determined by your security administrator and can be used only once.
5. Manually enter or copy/paste the OTP as the password as appropriate.
On the z/OS system, IBM TouchToken validates the OTP and allows or denies the logon.

Logging in to CICS CESL with IBM TouchToken

You can log in to a CICS CESL transaction with a valid IBM TouchToken OTP token code. This use case requires the IBM TouchToken for iOS application.

Procedure

Perform the following steps:

1. Begin to log in to the CICS CESL transaction with your user name.
2. Run the IBM TouchToken for iOS application.
3. Tap the account you created to select it.
4. Use your Touch ID fingerprint on the IBM TouchToken for iOS application to generate the IBM TouchToken OTP. This OTP is valid for 15, 30, or 60 seconds as determined by your security administrator and can be used only once.
5. Manually enter or copy/paste the OTP password as appropriate.
On the z/OS system, IBM TouchToken validates the OTP and allows or denies the logon.

Logging in to z/OSMF with IBM TouchToken

You can log in to z/OSMF with a valid IBM TouchToken OTP password. This use case requires the IBM TouchToken for iOS application.

Procedure

Perform the following steps:

1. Begin to log in to z/OSMF with your user name.
2. Run the IBM TouchToken for iOS application.
3. Tap the account you created to select it.

4. Use your Touch ID fingerprint on the IBM TouchToken for iOS application to generate the IBM TouchToken OTP. This OTP is valid for 15, 30, or 60 seconds as determined by your security administrator and can be used only once.
5. Manually enter or copy/paste the OTP password as appropriate.
On the z/OS system, IBM TouchToken validates the OTP and allows or denies the logon.

Logging in to IBM FTP with IBM TouchToken

You can log in to IBM FTP with a valid IBM TouchToken OTP token code. This use case requires the IBM TouchToken for iOS application.

Procedure

Perform the following steps:

1. Begin to log in to IBM FTP with your user name.
2. Run the IBM TouchToken for iOS application.
3. Tap the account you created to select it.
4. Use your Touch ID fingerprint on the IBM TouchToken for iOS application to generate the IBM TouchToken OTP. This OTP is valid for 15, 30, or 60 seconds as determined by your security administrator and can be used only once.
5. Manually enter or copy/paste the OTP password as appropriate.
On the z/OS system, IBM TouchToken validates the OTP and allows or denies the logon.

Logging in to IBM SSH with IBM TouchToken

You can log in to IBM SSH with a valid IBM TouchToken OTP token code. This use case requires the IBM TouchToken for iOS application.

Procedure

Perform the following steps:

1. Begin to log in to IBM SSH with your user name.
2. Run the IBM TouchToken for iOS application.
3. Tap the account you created to select it.
4. Use your Touch ID fingerprint on the IBM TouchToken for iOS application to generate the IBM TouchToken OTP. This OTP is valid for 15, 30, or 60 seconds as determined by your security administrator and can be used only once.
5. Manually enter or copy/paste the OTP password as appropriate.
On the z/OS system, IBM TouchToken validates the OTP and allows or denies the logon.

Logging in with IBM TouchToken and compound in-band authentication

You can log in with a valid IBM TouchToken OTP token code and a passphrase or password. Your administrator must have configured your account for IBM MFA Compound In-Band.

About this task

Important: If your RACF password has expired and you are using TSO/E, you are prompted during the compound in-band login session to change your RACF password. However, after attempting to change your password, the IBM MFA credentials are then replayed, which causes the password change operation to fail. In this case, begin a new TSO/E session, log in with your existing password and IBM MFA credentials, and then use the **-New Password** option on the panel to change your RACF password.

Procedure

Perform the following steps:

1. Begin to log in with your user name.
2. Run the IBM TouchToken for iOS application.
3. Tap the account you created to select it.
4. Use your Touch ID fingerprint on the IBM TouchToken for iOS application to generate the IBM TouchToken OTP. This OTP is valid for 15, 30, or 60 seconds as determined by your security administrator and can be used only once.
5. Manually enter or copy/paste the OTP as the password as appropriate, **followed by the separator, followed by** your passphrase or password.

Note: Your security administrator can reverse the order in which you enter the credentials, so that you enter your passphrase or password first, followed by the separator. Consult your security administrator for guidance.

Logging in with generic TOTP

If your system administrator configures your account for generic TOTP, you can log in by using common Quick Response (QR) codes on both Android and Apple iOS devices.

Procedure

1. Install a QR code application such as IBM Verify, Google Authenticator, Duo Mobile, and so forth on your device as directed by your system administrator.
2. When instructed by your system administrator, open the generic TOTP start page in a desktop web browser. For example, <https://hostname:6789/AZFTOTP1/genericStart>.
3. Log in with your z/OS user name and password.
A page that contains the **AuthURL** and the encoded QR code is displayed.
4. Point your device at the generated QR code and scan it with the application.
The application displays the TOTP code.
5. Enter the TOTP code on the web page and click **Generic TOTP Enrollment**.
6. If an error occurs, you are prompted to retry enrollment. If the error persists, your administrator may need to make additional tag settings changes to your account.
7. If the enrollment is successful, the message "New TOTP token has been confirmed and is ready to use." is displayed.
8. You must now use this TOTP token code to log on to the z/OS application.

Chapter 5. IBM MFA for SafeNet RADIUS with TSO/E

How you log in to TSO/E with IBM MFA for SafeNet RADIUS enabled depends on how your administrator has configured the Gemalto SafeNet token templates, the server-side PIN policies, and whether passphrases are enabled in TSO/E. Your administrator will provide you with this information.

This section describes specific approaches to two authentication modes: Quick Log, and Challenge-Response.

TSO/E with Quick Log

In SafeNet Quick Log mode, no challenge-response is required. You provide the MobilePASS passcode to TSO/E without having to first respond to a challenge.

Consult [Table 7 on page 39](#) to determine which login option matches your specific configuration and then follow the steps.

Table 7. TSO/E Logon Options for SafeNet Quick Log.		
PIN	Passphrase Accepted?	You enter...
No PIN	Yes	Enter the MobilePASS passcode in the TSO/E Password field.
Server-side User Select	Yes	Enter your PIN followed by the MobilePASS passcode in the TSO/E Password field.
User-selected PIN	Yes	Enter the MobilePASS passcode in the TSO/E Password field.
New PIN required	Yes	1. Enter your current PIN followed by the MobilePASS passcode in the TSO/E Password field. (The PIN is not needed in User-selected PIN mode.) 2. When prompted, enter a new PIN in the Password field. 3. Confirm the PIN.

TSO/E with Quick Log and compound in-band authentication

In SafeNet Quick Log mode, no challenge-response is required. You provide the MobilePASS passcode to TSO/E without having to first respond to a challenge. Your administrator must have configured your account for IBM MFA Compound In-Band.

Consult [Table 8 on page 40](#) to determine which login option matches your specific configuration and then follow the steps.

Note: Your security administrator can reverse the order in which you enter the credentials, so that you enter your passphrase or password first, followed by the separator. Consult your security administrator for guidance.

Important: If your RACF password has expired and you are using TSO/E, you are prompted during the compound in-band login session to change your RACF password. However, after attempting to change your password, the IBM MFA credentials are then replayed, which causes the password change operation to fail. In this case, begin a new TSO/E session, log in with your existing password and IBM MFA credentials, and then use the **-New Password** option on the panel to change your RACF password.

Table 8. TSO/E Logon Options for SafeNet Quick Log with Compound In-Band.		
PIN	Passphrase Accepted?	You enter...
No PIN	Yes	Enter the MobilePASS passcode in the TSO/E Password field, followed by the separator , followed by your passphrase or password.
Server-side User Select	Yes	Enter your PIN followed by the MobilePASS passcode in the TSO/E Password field, followed by the separator , followed by your passphrase or password.
User-selected PIN	Yes	Enter the MobilePASS passcode in the TSO/E Password field, followed by the separator , followed by your passphrase or password.
New PIN required	Yes	1. Enter your current PIN followed by the MobilePASS passcode in the TSO/E Password field, followed by the separator, followed by your passphrase or password. (The PIN is not needed in User-selected PIN mode.) 2. When prompted, enter a new PIN in the Password field. 3. Confirm the PIN.

TSO/E with Challenge-Response

In SafeNet Challenge-Response mode, you are presented with a challenge in your TSO/E session. You provide this challenge to the MobilePASS application, which in turn generates a passcode. You then use the generated passcode to log on to TSO/E.

Consult Table 9 on page 40 to determine which login option matches your specific configuration and then follow the steps.

Table 9. TSO/E Logon Options for SafeNet Challenge-Response.		
PIN	Passphrase Accepted?	You enter...
No PIN	Yes	1. Enter any single alphabetic character in the TSO/E Password field and press Enter. 2. Copy the challenge, paste it in MobilePASS, and generate a passcode. 3. Enter the MobilePASS passcode in the TSO/E Password field.
Server-side User Select	Yes	1. Enter any single alphabetic character in the TSO/E 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 TSO/E Password field.
User-selected PIN	Yes	1. Enter any single alphabetic character in the TSO/E Password field and press Enter. 2. Copy the challenge, paste it in MobilePASS, and generate a passcode. 3. Enter the passcode in the TSO/E Password field.

Table 9. TSO/E Logon Options for SafeNet Challenge-Response. (continued)

PIN	Passphrase Accepted?	You enter...
New PIN required	Yes	1. Enter any single alphabetic character in the TSO/E 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 TSO/E Password field. (The PIN is not needed in User-selected PIN mode.) 4. Respond to the prompts to enter a new PIN.

TSO/E with Challenge-Response and compound in-band authentication

In SafeNet Challenge-Response mode, you are presented with a challenge in your TSO/E session. You provide this challenge to the MobilePASS application, which in turn generates a passcode. You then use the generated passcode to log on to TSO/E. Your administrator must have configured your account for IBM MFA Compound In-Band.

Consult [Table 10 on page 41](#) to determine which login option matches your specific configuration and then follow the steps.

Note: Your security administrator can reverse the order in which you enter the credentials, so that you enter your passphrase or password first, followed by the separator. Consult your security administrator for guidance.

Important: If your RACF password has expired and you are using TSO/E, you are prompted during the compound in-band login session to change your RACF password. However, after attempting to change your password, the IBM MFA credentials are then replayed, which causes the password change operation to fail. In this case, begin a new TSO/E session, log in with your existing password and IBM MFA credentials, and then use the **-New Password** option on the panel to change your RACF password.

Table 10. TSO/E Logon Options for SafeNet Challenge-Response with Compound In-Band.

PIN	Passphrase Accepted?	You enter...
No PIN	Yes	1. Enter any single alphabetic character in the TSO/E Password field and press Enter. 2. Copy the challenge, paste it in MobilePASS, and generate a passcode. 3. Enter the MobilePASS passcode in the TSO/E Password field, followed by the separator, followed by your passphrase or password.
Server-side User Select	Yes	1. Enter any single alphabetic character in the TSO/E 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 TSO/E Password field, followed by the separator, followed by your passphrase or password.

Table 10. TSO/E Logon Options for SafeNet Challenge-Response with Compound In-Band. (continued)

PIN	Passphrase Accepted?	You enter...
User-selected PIN	Yes	1. Enter any single alphabetic character in the TSO/E Password field and press Enter. 2. Copy the challenge, paste it in MobilePASS, and generate a passcode. 3. Enter the passcode in the TSO/E Password field, followed by the separator, followed by your passphrase or password.
New PIN required	Yes	1. Enter any single alphabetic character in the TSO/E 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 TSO/E Password field, followed by the separator, followed by your passphrase or password. (The PIN is not needed in User-selected PIN mode.) 4. Respond to the prompts to enter a new PIN.

Chapter 6. IBM MFA for generic RADIUS with TSO/E

How you log in to TSO/E with IBM MFA for generic RADIUS depends entirely on how your administrator has configured the RADIUS server. You may need to supply a valid passcode, PIN, or some other credential. Your administrator will provide you with this information.

IBM MFA Compound In-Band

If your administrator has configured your account for IBM MFA Compound In-Band, you log in with your RADIUS credential, the required separator, and your passphrase or password in the password field. Your administrator will provide you with this information. For example:

```
credential:passphrase
```

Note: Your security administrator can reverse the order in which you enter the credentials, so that you enter your passphrase or password first, followed by the separator. Consult your security administrator for guidance.

Important: If your RACF password has expired and you are using TSO/E, you are prompted during the compound in-band login session to change your RACF password. However, after attempting to change your password, the IBM MFA credentials are then replayed, which causes the password change operation to fail. In this case, begin a new TSO/E session, log in with your existing password and IBM MFA credentials, and then use the **-New Password** option on the panel to change your RACF password.

Logging in with IBM MFA Compound In-Band when new PIN required

This section describes how you log in with IBM MFA for generic RADIUS and IBM MFA Compound In-Band when a new PIN is required.

Procedure

If you receive a new PIN required message, perform the following steps:

Note: Your security administrator can reverse the order in which you enter the credentials, so that you enter your passphrase or password first, followed by the separator. Consult your security administrator for guidance.

1. Enter your new PIN, **followed by the separator, followed by** your passphrase or password.
2. Press Enter. You are prompted to re-enter the new PIN.

```
ICH70008I IBM MFA Message:
      ::Please re-enter new PIN:
***
```

3. Re-enter your new PIN, **followed by the separator, followed by** your passphrase or password. If the PIN is accepted, the following message is displayed:

```
ICH70008I IBM MFA Message:
      ::PIN Accepted.::Wait for the token code to change,::then en
      ter the new passcode:
```

4. Wait for the SecurID token code to change.
5. Enter the new SecurID credential using the new PIN, **followed by the separator, followed by** your passphrase or password. How you generate the new SecurID credential depends on the token type you are using: fob-style hardware token, hardware token with a PINpad, or Soft token.

Chapter 7. Logging in with IBM MFA for LDAP

If your administrator configures your account for IBM MFA for LDAP, you use your LDAP password to log in to applications.

Procedure

Enter your LDAP password when prompted for your passphrase or password.

Logging in with IBM MFA for LDAP and compound in-band authentication

If your administrator configures your account for IBM MFA for LDAP, you use your LDAP password to log in to applications.

Procedure

Enter your LDAP password, **followed by the separator, followed by** your RACF passphrase or password.

Note: Your security administrator can reverse the order in which you enter the credentials, so that you enter your passphrase or password first, followed by the separator. Consult your security administrator for guidance.

Chapter 8. Logging in with IBM MFA for YubiKey

If your administrator configures your account for IBM MFA for YubiKey, you use your YubiKey to log in to applications.

Procedure

1. If instructed by your administrator, launch the YubiKey enrollment page provided by the administrator.
2. Provide your user name and password.
3. Tap the YubiKey to generate an OTP in the YubiKey OTP field.

You receive a message that the YubiKey was associated with your account.

Information
Your YubiKey device was successfully associated with your account.

4. You must now use the YubiKey to generate an OTP in the password field of applications.

Logging in with IBM MFA for YubiKey and compound in-band authentication

If your administrator configures your account for IBM MFA for YubiKey, you use your YubiKey to log in to applications.

Procedure

1. If instructed by your administrator, launch the YubiKey enrollment page provided by the administrator.
2. Provide your user name and password.
3. Tap the YubiKey to generate an OTP in the YubiKey OTP field.

You receive a message that the YubiKey was associated with your account.

Information
Your YubiKey device was successfully associated with your account.

4. You must now use the YubiKey to generate an OTP in the password field of applications.
5. Tap the YubiKey to generate an OTP in the password field, **followed by the separator, followed by** your RACF passphrase or password.

Note: Your security administrator can reverse the order in which you enter the credentials, so that you enter your passphrase or password first, followed by the separator. Consult your security administrator for guidance.

Chapter 9. IBM CL/SuperSession for z/OS

IBM CL/SuperSession for z/OS, V2.1 provides efficient management of VTAM® sessions for mainframe applications.

You can use IBM MFA to log in to IBM CL/SuperSession for z/OS, V2.1 in the following ways:

- In-band using a passphrase or password.
- Via IBM MFA Out-of-Band with a cache token credential.
- Your administrator can configure IBM CL/SuperSession for z/OS, V2.1 to use PassTickets to authenticate to downstream applications after a successful IBM MFA authentication to IBM CL/SuperSession for z/OS, V2.1.

See [IBM CL/SuperSession for z/OS Version 2 Release 1](#) for configuration information and other product documentation.

Chapter 10. IBM HTTP Server - Powered by Apache

How you log in to IBM HTTP Server - Powered by Apache with IBM MFA enabled depends on the token type you are using.

For IBM MFA SecurID, you must already have a valid PIN. For IBM MFA with IBM TouchToken, you need the generated IBM TouchToken OTP.

IBM TouchToken

If the security administrator has enabled your account for IBM MFA with IBM TouchToken, you no longer use your RACF password to log in. Instead, you must use your supported Apple device to generate an IBM TouchToken OTP and then use that to log in.

IBM MFA SecurID

If the security administrator has enabled your account for IBM MFA, you no longer use your z/OS password to log in. Instead, how you log in depends on the type of token you have. See [“Types of token devices” on page 3](#) for the supported token types.

General guidelines

Observe the following guidelines:

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

Note: If you are using IBM HTTP Server - Powered by Apache with compound in-band authentication, the possible separator values are a colon (:) and a vertical bar (|). The forward slash (/) is not supported as a separator.

Logging in with IBM TouchToken

You can log in to IBM HTTP Server - Powered by Apache with a valid IBM TouchToken OTP token code. This use case requires the IBM TouchToken for iOS application.

Procedure

Perform the following steps:

1. Begin to log in to IBM HTTP Server - Powered by Apache with your user name.
2. Run the IBM TouchToken for iOS application.
3. Tap the account you created to select it.
4. Use your Touch ID fingerprint on the IBM TouchToken for iOS application to generate the IBM TouchToken OTP. This OTP is valid for 15, 30, or 60 seconds as determined by your security administrator and can be used only once.
5. Manually enter or copy/paste the OTP password as appropriate.
On the z/OS system, IBM TouchToken validates the OTP and allows or denies the logon.

Logging in with a fob-style hardware token

You can log in to IBM HTTP Server - Powered by Apache with a valid PIN. This use case requires a fob-style hardware token.

Procedure

Perform the following steps:

1. Open an IBM HTTP Server - Powered by Apache application and enter your user name.
2. Get the 6- to 8-digit token code displayed by the SecurID token.
3. Enter your PIN **followed by** the 6- to 8-digit token code displayed by the SecurID token in the password field. For example, if your PIN is 4321 and your token code is 456789, enter 4321456789 in the password field.
4. Press Enter.

Logging in with a hardware token with a PINpad

You can log in to IBM HTTP Server - Powered by Apache with a valid PIN. This use case requires a hardware token with a PINpad.

Procedure

Perform the following steps:

1. Open an IBM HTTP Server - Powered by Apache application and enter your user name.
2. Enter your PIN in the SecurID token and generate a passcode.
3. Enter the 6- to 8-digit passcode displayed by the SecurID token in the password field.
4. Press Enter.

Logging in with a soft token

You can log in to IBM HTTP Server - Powered by Apache with a valid PIN. This use case requires a soft token application.

Procedure

Perform the following steps:

1. Open an IBM HTTP Server - Powered by Apache application and enter your user name.
2. Enter your PIN in the soft token and generate a passcode. Use the copy feature to copy the passcode.
3. Paste the 6- to 8-digit passcode displayed by the soft token in the password field.
4. Press Enter.

Logging in with IBM MFA Out-of-Band

You can log in to IBM HTTP Server - Powered by Apache with a IBM MFA Out-of-Band cache token credential.

About this task

Your security administrator will tell you if you need to use IBM MFA Out-of-Band to log in. If you are required to use IBM MFA Out-of-Band to log in and you do not, you receive a reminder error message.

Note: This procedure has been verified with Microsoft Internet Explorer and Google Chrome.

Procedure

Perform the following steps:

1. Use a web browser to connect to the URL provided by your security administrator, typically `https://login-server-hostname:port/mfa/policy-name`.
2. Follow the web interface to enter the required token.

Note: Your administrator determines the maximum amount of time you have to complete all authentication factors.

3. As you successfully enter the required tokens, the IBM MFA Certificate Authentication web page prompts you for the next one.
4. When you have satisfied all of your token requirements, the IBM MFA Certificate Authentication web page displays the cache token credential.
5. Open an IBM HTTP Server - Powered by Apache application and enter your user name.
6. Manually enter or copy/paste the cache token credential as your password, as appropriate.

Note: If you are using Internet Explorer and use the cache token credential copy feature, be aware that Windows Internet Options settings can affect its function. Specifically, the "Allow Programmatic Clipboard Access" setting in one or more applicable zones can disable this feature or require you to respond to an additional prompt. The "Allow Programmatic Clipboard Access" setting is typically controlled by the system administrator.

Chapter 11. Troubleshooting

If you are unable to successfully log in using IBM MFA, your next steps depend on which program you are using to log in.

Before you begin

Not all programs display the messages described in [Chapter 12, “Multi-Factor Authentication messages,” on page 57](#). Therefore, the cause of a login failure might not be totally obvious.

For example, because the number of unsuccessful login attempts that trigger RSA SecurID “next token” mode can vary due to local security policy, it is possible that you are in the “next token” mode without being aware of it. (RSA SecurID “next token” mode is described in [“Logging in with RSA SecurID “next token” mode” on page 55](#).)

As another example, if the RSA Authentication Manager is configured for system-generated PINs, the new PIN may not be displayed. Similarly, in the unlikely event that your PIN is invalid and you are not aware of it, the cause of the login failure might not be obvious to you if your application does not display the messages.

Note: If the application you are using stores and reuses password information, this method is incompatible with IBM MFA because a token can be used only once. For example, HTTP Basic authentication works this way. To resolve these types of issues, contact your system programming support.

Procedure

Perform the following steps:

1. If your program displays the messages, see [Chapter 12, “Multi-Factor Authentication messages,” on page 57](#) for more information about how to resolve the issue.
2. If you have previously been able to log in with IBM MFA, but now receive an error, the most likely cause is you made a typing error.
3. Wait until the token code (or passcode) changes before attempting to log in, then take your time. Reusing a token code or passcode is a common mistake.
4. Make sure that your PIN is correct.
5. Make sure you are using token codes and passcodes correctly. There is a difference between a token code and a passcode, as described in [“Multi-factor authentication concepts” on page 1](#). If you use one instead of the other, your login will fail.
6. Do not keep trying. If you are unable to log in after several attempts, ask your security administrator for guidance.

Logging in with RSA SecurID “next token” mode

Next token code mode requires you to enter two successive codes to log in. After n number of failed login attempts followed by a successful login, where n is determined by your local security policy, you may be prompted to also enter the next displayed token code for extra security. If you do not enter the next displayed token code or passcode, the login fails.

Before you begin

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 due to local security policy, it may not be obvious that the next token is also required. Ask your security administrator for guidance if you are unable to log in after several attempts.

Procedure

Perform the following steps:

1. If prompted to enter the next token code, 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.

Note: In compound authentication mode, you enter the token code (or passcode) **followed by the separator, followed by** your passphrase or password.

Note: Your security administrator can reverse the order in which you enter the credentials, so that you enter your passphrase or password first, followed by the separator. Consult your security administrator for guidance.

4. Press Enter.

Logging in with Password Fallback

IBM MFA password fallback allows you to log in using your z/OS password if the RSA Authentication Manager, RADIUS server, or IBM MFA server are down.

About this task

If your security administrator has configured your account with the password fallback parameter, password fallback provides a mechanism to log in with your z/OS password instead of your IBM MFA credentials. The password fallback mechanism is provided as a fail safe authentication method, and is not something you typically use.

If after several attempts you are unable to log in using your IBM MFA credentials, and you are certain that you are using your approved login process, PIN, and token, ask your security administrator if there is a system problem and whether you should use your z/OS password.

Procedure

Perform the following steps:

1. Log in with your user name.
2. Enter your z/OS password, not your IBM MFA credentials.
3. If your z/OS password has expired, you are prompted to enter a new password.

Chapter 12. Multi-Factor Authentication messages

This topic explains the messages that IBM MFA issues to the user.

Messages with AZF message numbers

This section describes messages issued with IBM MFA AZF message numbers.

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

- I** Information.
- W** Warning.
- E** Error.

AZF1001I ENTER NEXT TOKENCODE

Explanation

After n number of failed login attempts followed by a successful login, where n is determined by your local security policy, you may be prompted to also enter the next displayed token code for extra security. By successfully entering the next token code, the system is able to verify that you have possession of the token assigned to you.

Next token code mode requires you to enter the **next** token code (or passcode) that is displayed. That is, you must enter two successive codes to log in. If you do not enter the next displayed token code or passcode, the login fails.

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.

AZF1002I CONFIRM SYSGEN PIN: *PIN*

Explanation

The RSA Authentication Manager generated a system-generated PIN.

User response

Confirm the system-generated PIN.

AZF1003I USER OR SYSGEN PIN: *PIN*

Explanation

The RSA Authentication Manager is configured to allow you to use either a system-generated PIN or a PIN of your choice. The message is displayed with a system-generated PIN appended, but you can choose something else.

User response

Accept the system-generated PIN or choose your own.

AZF1004I NEW PIN ACCEPTED

Explanation

The new PIN you entered was accepted.

User response

Because you changed the PIN, you must log in again. Wait for the token code (or passcode) displayed by the SecurID token to change.

AZF1005E NEW PIN REJECTED

Explanation

The new PIN you entered was rejected.

User response

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.

AZF1006E ACCESS DENIED

Explanation

Your PIN, token code, or both were rejected.

User response

- If you are unable to log in after several attempts, ask your security administrator for guidance. If you continue to try to log in you will probably lock your account.
- It is a best practice to wait until the token code or passcode changes before attempting to log in. That way, you do not have to rush to enter it before it expires.
- You can use the token code or passcode only once.
- If you receive an authentication failure, wait until the token code or passcode changes before attempting to log in again.
- Remember that there is a difference between a token code and a passcode, as described in [“Multi-factor authentication concepts” on page 1](#). If you use one instead of the other, your login will fail.

AZF1007I ENTER NEW PIN - MIN 4 MAX 8

Explanation

You must enter a new PIN before you can log in.

User response

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 you enter and confirm the new PIN, you must log in again.

AZF1008E NEW PIN CANCELLED

Explanation

You must enter a new PIN before you can log in.

User response

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 you enter and confirm the new PIN, you must log in again.

AZF1009I AZFSIDP1 AUTHENTICATION SUCCESSFUL

Explanation

The authentication was successful.

User response

No response is required.

AZF1010E Supported tags: SIDUSERID

Explanation

The AZFSIDP1 factor accepts the SIDUSERID as a valid tag, where SIDUSERID is the user ID on the RSA Authentication Manager system.

User response

Enter a valid tag value.

AZF1011E SIDUSERID length must be <= 50

Explanation

The AZFSIDP1 factor accepts the SIDUSERID as a valid tag, where SIDUSERID is the user ID on the RSA Authentication Manager system.

User response

Enter a valid SIDUSERID.

AZF1100E TOTP PROVISIONING ERROR - NOTIFY ADMINISTRATOR

Explanation

IBM TouchToken cannot provision successfully.

User response

Notify your Security Administrator of this error.

AZF1101E TOTP CRYPTO ERROR - NOTIFY ADMINISTRATOR

Explanation

IBM TouchToken detected a cryptographic error.

User response

Notify your Security Administrator of this error.

AZF1102I TOTP USER SUSPENDED - NOTIFY ADMINISTRATOR

Explanation

IBM TouchToken has suspended the user account.

User response

Notify your Security Administrator of this error.

AZF1103W TOTP REPLAY DENIED

Explanation

IBM TouchToken has prevented an attempt to reuse the OTP password.

User response

Notify your Security Administrator of this error.

AZF1104I TOTP PASSCODE REJECTED

Explanation

IBM TouchToken has rejected the OTP token.

User response

You may have incorrectly entered the OTP token. Wait for the next OTP token to be displayed and retry.

AZF1105I TOTP PASSCODE ACCEPTED

Explanation

IBM TouchToken has accepted the OTP token.

User response

No response is required.

AZF5170E No factors are active for the specified User ID

Explanation

When the administrator applies 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. There are no active factors.

User response

Your administrator must set the required factors to be active.

AZF5171E Session expired or is otherwise not found

Explanation

The session is valid for 10 minutes, starting from when you log on with your RACF credentials. The session has expired.

User response

Log in again with your RACF credentials and start another session.

AZF5172E The specified policy name is invalid

Explanation

When the administrator applies a policy to a user, the policy must exist and be valid.

User response

Your administrator must apply a valid policy to your user account.

AZF5173E Failed to create a Cache Token Credential

Explanation

IBM MFA Out-of-Band authentication was unable to create a cache token credential.

User response

Seek guidance and additional, related error messages from your administrator.

AZF5174E No policies are bound to the specified user or session

Explanation

There are no IBM MFA Out-of-Band policies bound to your user account.

User response

Your administrator must associate your user ID with a valid policy.

AZF5175E None of the user's policies are satisfiable

Explanation

When the administrator applies 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

Your administrator must associate your user ID with a valid policy.

AZF5176E An internal error occurred

Explanation

An internal error occurred.

User response

Seek guidance and additional, related error messages from your administrator.

Appendix A. Accessibility

Accessible publications for this product are offered through [IBM Knowledge Center \(www.ibm.com/support/knowledgecenter/SSLTBW/welcome\)](http://www.ibm.com/support/knowledgecenter/SSLTBW/welcome).

If you experience difficulty with the accessibility of any z/OS information, send a detailed email message to mhvrfs@us.ibm.com.

Accessibility features

Accessibility features help users who have physical disabilities such as restricted mobility or limited vision use software products successfully. The accessibility features in z/OS can help users do the following tasks:

- Run assistive technology such as screen readers and screen magnifier software.
- Operate specific or equivalent features by using the keyboard.
- Customize display attributes such as color, contrast, and font size.

Consult assistive technologies

Assistive technology products such as screen readers function with the user interfaces found in z/OS. Consult the product information for the specific assistive technology product that is used to access z/OS interfaces.

Keyboard navigation of the user interface

You can access z/OS user interfaces with TSO/E or ISPF. The following information describes how to use TSO/E and ISPF, including the use of keyboard shortcuts and function keys (PF keys). Each guide includes the default settings for the PF keys.

- [*z/OS TSO/E Primer*](#)
- [*z/OS TSO/E User's Guide*](#)
- [*z/OS ISPF User's Guide Vol I*](#)

Dotted decimal syntax diagrams

Syntax diagrams are provided in dotted decimal format for users who access IBM Knowledge Center with a screen reader. In dotted decimal format, each syntax element is written on a separate line. If two or more syntax elements are always present together (or always absent together), they can appear on the same line because they are considered a single compound syntax element.

Each line starts with a dotted decimal number; for example, 3 or 3.1 or 3.1.1. To hear these numbers correctly, make sure that the screen reader is set to read out punctuation. All the syntax elements that have the same dotted decimal number (for example, all the syntax elements that have the number 3.1) are mutually exclusive alternatives. If you hear the lines 3.1 USERID and 3.1 SYSTEMID, your syntax can include either USERID or SYSTEMID, but not both.

The dotted decimal numbering level denotes the level of nesting. For example, if a syntax element with dotted decimal number 3 is followed by a series of syntax elements with dotted decimal number 3.1, all the syntax elements numbered 3.1 are subordinate to the syntax element numbered 3.

Certain words and symbols are used next to the dotted decimal numbers to add information about the syntax elements. Occasionally, these words and symbols might occur at the beginning of the element itself. For ease of identification, if the word or symbol is a part of the syntax element, it is preceded by the backslash (\) character. The * symbol is placed next to a dotted decimal number to indicate that the syntax element repeats. For example, syntax element *FILE with dotted decimal number 3 is given the format 3 * FILE. Format 3* FILE indicates that syntax element FILE repeats. Format 3* * FILE indicates that syntax element * FILE repeats.

Characters such as commas, which are used to separate a string of syntax elements, are shown in the syntax just before the items they separate. These characters can appear on the same line as each item, or on a separate line with the same dotted decimal number as the relevant items. The line can also show another symbol to provide information about the syntax elements. For example, the lines 5.1*, 5.1 LASTRUN, and 5.1 DELETE mean that if you use more than one of the LASTRUN and DELETE syntax elements, the elements must be separated by a comma. If no separator is given, assume that you use a blank to separate each syntax element.

If a syntax element is preceded by the % symbol, it indicates a reference that is defined elsewhere. The string that follows the % symbol is the name of a syntax fragment rather than a literal. For example, the line 2.1 %OP1 means that you must refer to separate syntax fragment OP1.

The following symbols are used next to the dotted decimal numbers.

? indicates an optional syntax element

The question mark (?) symbol indicates an optional syntax element. A dotted decimal number followed by the question mark symbol (?) indicates that all the syntax elements with a corresponding dotted decimal number, and any subordinate syntax elements, are optional. If there is only one syntax element with a dotted decimal number, the ? symbol is displayed on the same line as the syntax element, (for example 5? NOTIFY). If there is more than one syntax element with a dotted decimal number, the ? symbol is displayed on a line by itself, followed by the syntax elements that are optional. For example, if you hear the lines 5 ?, 5 NOTIFY, and 5 UPDATE, you know that the syntax elements NOTIFY and UPDATE are optional. That is, you can choose one or none of them. The ? symbol is equivalent to a bypass line in a railroad diagram.

! indicates a default syntax element

The exclamation mark (!) symbol indicates a default syntax element. A dotted decimal number followed by the ! symbol and a syntax element indicate that the syntax element is the default option for all syntax elements that share the same dotted decimal number. Only one of the syntax elements that share the dotted decimal number can specify the ! symbol. For example, if you hear the lines 2? FILE, 2.1! (KEEP), and 2.1 (DELETE), you know that (KEEP) is the default option for the FILE keyword. In the example, if you include the FILE keyword, but do not specify an option, the default option KEEP is applied. A default option also applies to the next higher dotted decimal number. In this example, if the FILE keyword is omitted, the default FILE (KEEP) is used. However, if you hear the lines 2? FILE, 2.1, 2.1.1! (KEEP), and 2.1.1 (DELETE), the default option KEEP applies only to the next higher dotted decimal number, 2.1 (which does not have an associated keyword), and does not apply to 2? FILE. Nothing is used if the keyword FILE is omitted.

*** indicates an optional syntax element that is repeatable**

The asterisk or glyph (*) symbol indicates a syntax element that can be repeated zero or more times. A dotted decimal number followed by the * symbol indicates that this syntax element can be used zero or more times; that is, it is optional and can be repeated. For example, if you hear the line 5.1* data area, you know that you can include one data area, more than one data area, or no data area. If you hear the lines 3* , 3 HOST, 3 STATE, you know that you can include HOST, STATE, both together, or nothing.

Notes:

1. If a dotted decimal number has an asterisk (*) next to it and there is only one item with that dotted decimal number, you can repeat that same item more than once.
2. If a dotted decimal number has an asterisk next to it and several items have that dotted decimal number, you can use more than one item from the list, but you cannot use the items more than once each. In the previous example, you can write HOST STATE, but you cannot write HOST HOST.

3. The * symbol is equivalent to a loopback line in a railroad syntax diagram.

+ indicates a syntax element that must be included

The plus (+) symbol indicates a syntax element that must be included at least once. A dotted decimal number followed by the + symbol indicates that the syntax element must be included one or more times. That is, it must be included at least once and can be repeated. For example, if you hear the line 6.1+ data area, you must include at least one data area. If you hear the lines 2+, 2 HOST, and 2 STATE, you know that you must include HOST, STATE, or both. Similar to the * symbol, the + symbol can repeat a particular item if it is the only item with that dotted decimal number. The + symbol, like the * symbol, is equivalent to a loopback line in a railroad syntax diagram.

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 DFSMS, 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 \(www.ibm.com/software/support/systemsz/lifecycle\)](http://www.ibm.com/software/support/systemsz/lifecycle)
- For information about currently-supported IBM hardware, contact your IBM representative.

Trademarks

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

Index

A

- accessibility
 - contact IBM [61](#)
 - features [61](#)
- Apple device
 - preparing for IBM TouchToken [6](#)
- Applications
 - logging in with IBM MFA Out-of-Band [9](#), [11](#), [52](#)
- assistive technologies [61](#)

C

- CAC card
 - configure [10](#)
- CICS CESL
 - logging in with IBM TouchToken [35](#)
- CICS CESL transaction
 - fob-style hardware token [21](#)
 - PINpad hardware token [22](#)
 - soft token [24](#)
- contact
 - z/OS [61](#)

F

- feedback [xi](#)
- fob-style token
 - TSO login [13](#)

G

- generic TOTP
 - logging in [37](#)

I

- IBM FTP
 - fob-style hardware token [28](#), [29](#)
 - logging in with IBM TouchToken [36](#)
 - PINpad hardware token [28](#), [29](#)
 - soft token [28](#), [29](#)
- IBM HTTP Server - Powered by Apache
 - fob-style hardware token [52](#)
 - logging in with IBM TouchToken [51](#)
 - out-of-band [52](#)
 - PINpad hardware token [52](#)
 - soft token [52](#)
- IBM MFA Certificate Authentication
 - register certificates [10](#)
- IBM OpenSSH
 - fob-style hardware token [30](#), [31](#)
 - logging in with IBM TouchToken [36](#)
 - PINpad hardware token [30](#), [32](#)
 - soft token [31](#), [32](#)
- IBM TouchToken

- IBM TouchToken (*continued*)
 - OTP password [5](#)
 - preparing Apple device [6](#)
- IBM TouchToken concepts [5](#)

K

- keyboard
 - navigation [61](#)
 - PF keys [61](#)
 - shortcut keys [61](#)

M

- messages [57](#)
- Multi-Factor Authentication
 - authentication factors [1](#)
 - CICS login, fob-style token [21](#), [22](#)
 - CICS login, PINpad token [23](#)
 - CICS login, soft token [24](#), [25](#)
 - introduction [1](#)
 - logging in with password fallback [56](#)
 - logon approach [7](#)
 - OTP concepts [5](#)
 - PIN-change mode [4](#)
 - RSA Authentication Manager concepts [3](#)
 - RSA SecurID next token mode [55](#)
 - SecurID passcode [3](#)
 - SecurID PIN [3](#)
 - SecurID token code [3](#)
 - troubleshooting [55](#)
 - types of token devices [3](#)
 - typical logon [4](#)
 - use of password field [4](#)
 - with PIN, with pass phrase [21–25](#)
 - without PIN, with pass phrase [22–24](#)

N

- navigation
 - keyboard [61](#)

O

- out-of-band authentication
 - concepts [6](#)

P

- PINpad token
 - TSO login [16](#)
- PIV card
 - configure [10](#)

R

register certificates
 IBM MFA Certificate Authentication [10](#)
RSA Authentication Manager concepts [3](#)

S

sending to IBM
 reader comments [xi](#)
shortcut keys [61](#)
summary of changes
 as updated May 2019 [xiii](#)

T

trademarks [68](#)
troubleshooting [55](#), [56](#)
TSO
 logging in with IBM MFA for generic RADIUS and IBM
 MFA Compound In-Band [43](#)
 logging in with IBM MFA for LDAP [45](#)
 logging in with IBM MFA for YubiKey [47](#)
 logging in with IBM TouchToken [35](#), [36](#)
TSO login, fob-style token
 with PIN, no pass phrase [14](#)
 with PIN, with pass phrase [14](#), [15](#)
 without PIN or pass phrase [14](#)
 without PIN, with pass phrase [15](#)
TSO login, Pinpad token
 with PIN, no pass phrase [16](#)
 with PIN, with pass phrase [16](#), [18](#)
 without PIN or pass phrase [17](#)
 without PIN, with pass phrase [17](#)
TSO login, soft token
 with PIN, no pass phrase [19](#)
 with PIN, with pass phrase [19](#), [20](#)
 without PIN or pass phrase [19](#)
 without PIN, with pass phrase [20](#)

U

user interface
 ISPF [61](#)
 TSO/E [61](#)

Z

z/OSMF
 fob-style hardware token [25](#), [26](#)
 logging in with IBM TouchToken [35](#)
 PINpad hardware token [26](#), [27](#)
 soft token [26](#), [27](#)



SC27-8448-30

