iSecurity Multi Factor Authentication (MFA)

User Guide
Version 6.03

www.razlee.com

Introduction

Current security regulations recognize that passwords are not enough. The security of sensitive systems require that you need to verify more than *something you know* (such as a password). You also need to prove *something you have* (such as a phone that can receive SMS messages or an email address) or *something you are* (such as a biometric check, such as a fingerprint or retina scan). The checking of more than one of these values is known as **Multi- Factor Authentication (MFA)**.

iSecurity Multi-Factor Association implements this system for your IBM i. It can not only control logins but also connection attempts via FTP, ODBC, and other methods. When a user attempts to connect via one of these methods from an IP address that has not been explicitly pre-approved, iSecurity MFA sends a message to the user's cellphone, email, or both. If the user does not respond or does not authorize the connection, the attempt is logged and blocked.

Using the MFA management interface, as documented in this manual, administrators can specify the protocols for which specific users and groups require MFA, as well as the IP address ranges from which they do not need it. You can also specify how long the MFA passcodes need to be as well as how long the user has to respond to a confirmation message.

A user who requires MFA and tries to log on to a system from an IP address that has not been pre-approved receives an email, SMS message, or both containing a passcode. Entering the passcode completes the login.

When the user, or a job that the user runs, initiates a connection via several other protocols, the system sends a unique link to the user's SMS or email. The user must follow the link for the connection to continue.

Contents

About this Manual

This user guide is intended for system administrators and security administrators responsible for the implementation and management of security on IBM i systems. However, any user with basic knowledge of IBM i operations will be able to make full use of this product after reading this book.

Raz-Lee takes customer satisfaction seriously. Our products are designed for ease of use by personnel at all skill levels, especially those with minimal IBM i experience. The documentation package includes a variety of materials to get you familiar with this software quickly and effectively.

This user guide, together with the iSecurity Installation Guide, is the only printed documentation necessary for understanding this product. It is available in HTML form as well as in user-friendly PDF format, which may be displayed or printed using Adobe Acrobat Reader version 6.0 or higher. If you do not have Acrobat Reader, you can download it from the Adobe website: http://www.adobe.com/. You can also read and print pages from the manual using any modern web browser.

This manual contains concise explanations of the various product features as well as step-by-step instructions for using and configuring the product.

Raz-Lee's iSecurity is an integrated, state-of-the-art security solution for all System i servers, providing cutting-edge tools for managing all aspects of network access, data, and audit security. Its individual components work together transparently, providing comprehensive "out-of-the- box" security. To learn more about the iSecurity Suite, visit our website at http://www.razlee.com/.

Intended Audience

The Multi Factor Authentication (MFA)User Guide document was developed for users, system administrators and security administrators responsible for the implementation and management of security on IBM® AS/400 systems. However, any user with a basic knowledge of System i operations is able to make full use of this document following study of this User Guide.

NOTE: Deviations from IBM® standards are employed in certain circumstances in order to enhance clarity or when standard IBM® terminology conflicts with generally accepted industry conventions.

This document may also serve for new versions' upgrade approval by management.

Conventions Used in the Document

Menu options, field names, and function key names are written in **Courier New Bold**.

Links (internal or external) are emphasized with underline and blue color as follows: "About this Manual" on page 4.

Commands and system messages of IBM i® (OS/400®), are written in ***Bold Italic***.

Key combinations are in Bold and separated by a dash, for example: **Enter**, **Shift-Tab**.

Emphasis is written in **Bold.**

A sequence of operations entered via the keyboard is marked as

STRMFA **> 81 > 32**

meaning: Syslog definitions activated by typing ***STRMFA***and selecting option: **81** then option: **32**.

Data Entry Screens

Data entry screens include many convenient features such as:

- Pop-up selection windows
- Convenient option prompts
- Easy-to-read descriptions and explanatory text for all parameters and options
- Search and filtering with generic text support

The following describes the different data entry screens.

- To enter data in a field, type the desired text and then press Enter or Field Exit
- To move from one field to another without changing the contents press Tab
- To view options for a data field together with an explanation, press F4
- To accept the data displayed on the screen and continue, press Enter

The following function keys may appear on data entry screens.

- F1: **Help** Display context-sensitive help
- F3: **Exit** End the current task and return to the screen or menu from which the task was initiated
- F4: **Prompt** Display a list of valid options for the current field or command. For certain data items, a pop-up selection window appears
- F6: **Add New** Create a new record or data item
- F8: **Print** Print the current report or data item
- F9: **Retrieve** Retrieve the previously-entered command
- F12: **Cancel** Return to the previous screen or menu without updating

Legal Notice

This document is provided by Raz-Lee Security for information purposes only and is not a legal binding document.

While Raz-Lee is doing its best to coordinate between this document and Raz-Lee's products, changes might occur. In case a change has been encountered, please inform Raz-Lee. Raz-Lee keeps its right to modify the software or the document as per its sole discretion Usage of this document, and all information (including product information) provided within, are subject to the following terms and conditions, and all applicable laws. If you do not agree with these terms, please do not access or use the remainder of this document.

This document contains highly confidential information, which is proprietary to Raz-Lee Security Ltd. and/or its affiliates (hereafter, "Raz-Lee"). No part of this document's contents may be used, copied, disclosed or conveyed to any third party in any manner whatsoever without prior written permission from Raz-Lee. The information included in this document is intended for your knowledge and for negotiation purposes only. Raz-Lee makes no implicit representations or warranties with respect to such information. The information included in this document is subject to change without notice. Any decision to rely on the information contained herein shall be at your sole responsibility, and Raz-Lee will not accept any liability for your decision to use any information or for any damages resulting therefrom. Certain laws do not allow limitations on implied warranties or the exclusion or limitation of certain damages. If these laws apply to you, some or all of the above disclaimers, exclusions, or limitations may not apply to you.

All registered or unregistered trademarks, product names, logos and other service marks mentioned within this document are the property of Raz-Lee or their respective owners. Nothing contained herein shall be construed as conferring by implication, estoppels, or otherwise any license or right, either express or implied, under any patent or trademark of Raz-Lee or any third party. No use of any trademark may be made without the prior written authorization of Raz-Lee. This document and all of its contents are protected intellectual property of Raz-Lee. Any copying, reprinting, reuse, reproduction, adaptation, distribution or translation without the prior written permission of Raz-Lee is prohibited.

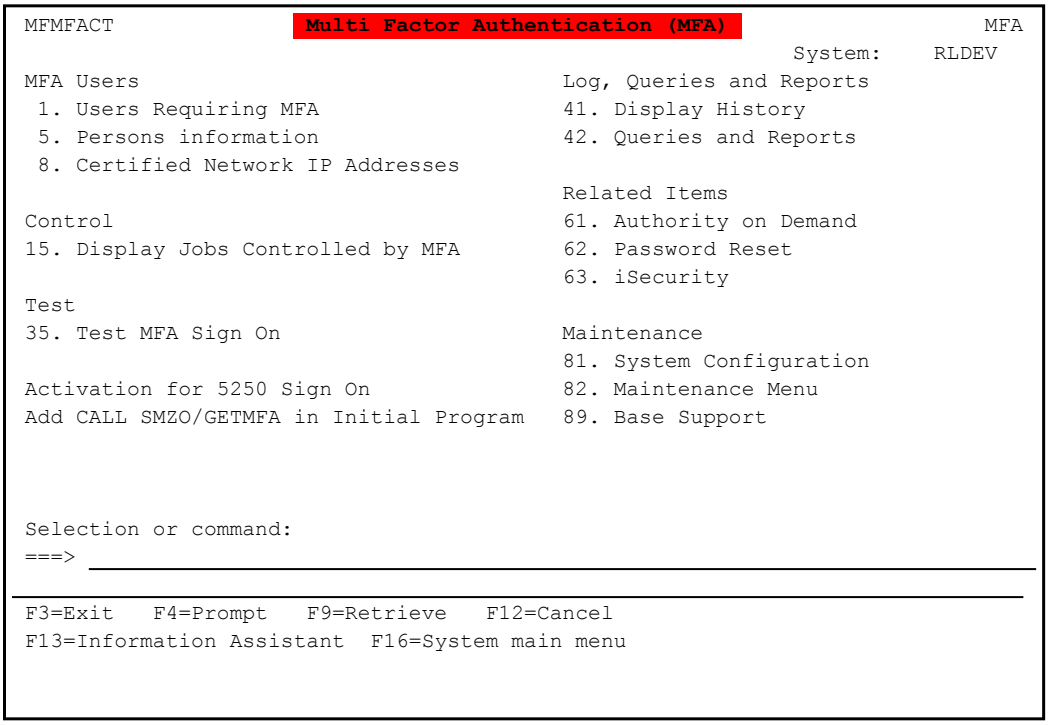
Please check your End User License Agreement (EULA) for terms and Conditions.

Contacts

Raz-Lee Security Inc. www.razlee.com
Marketing: marketing@razlee.com 1-888-RAZLEE-4 (1-888-7295334)
Support: support@razlee.com 1-888-RAZLEE-2 (1-888-7295332)

Starting Multi Factor Authentication (MFA)

To **start Multi Factor Authentication (MFA)**, enter the command **SMZO/STRMFA** on any command line. The main **Multi Factor Authentication (MFA)** screen appears:



To **specify which users require Multi Factor Authentication**, select **1. Users Requiring MFA** from the menu. The **Users Requiring MFA** screen appears, as shown in "Specifying Users Requiring Multi Factor Authentication" on page 14.

To **display and enter information concerning each user**, select **5. Person Information** from the menu. The **Work with Persons** screen appears, as shown in "Defining Persons" on page 16.

To specify network IP addresses from which particular users may access the system without added authentication, select **8. Certified Network IP Addresses** from the menu. The Work with Certified Network IP Addresses screen appears, as shown in "Specifying Certified Network IP Addresses" on page 22.

To define general parameters for MFA, select **81. System Configuration** from the menu, then select **61. General** from the **Multi-Factor Authentication** section of the System Configuration screen. The MFA General Definitions screen appears, as shown in "Defining General MFA Parameters" on the next page.

To display jobs controlled by Multi Factor Authentication, select **15. Display Jobs Controlled by MFA** from the menu. The Display MFA Active Jobs screen appears, as shown in "Displaying Jobs Controlled by MFA" on page 26.

Defining General MFA Parameters

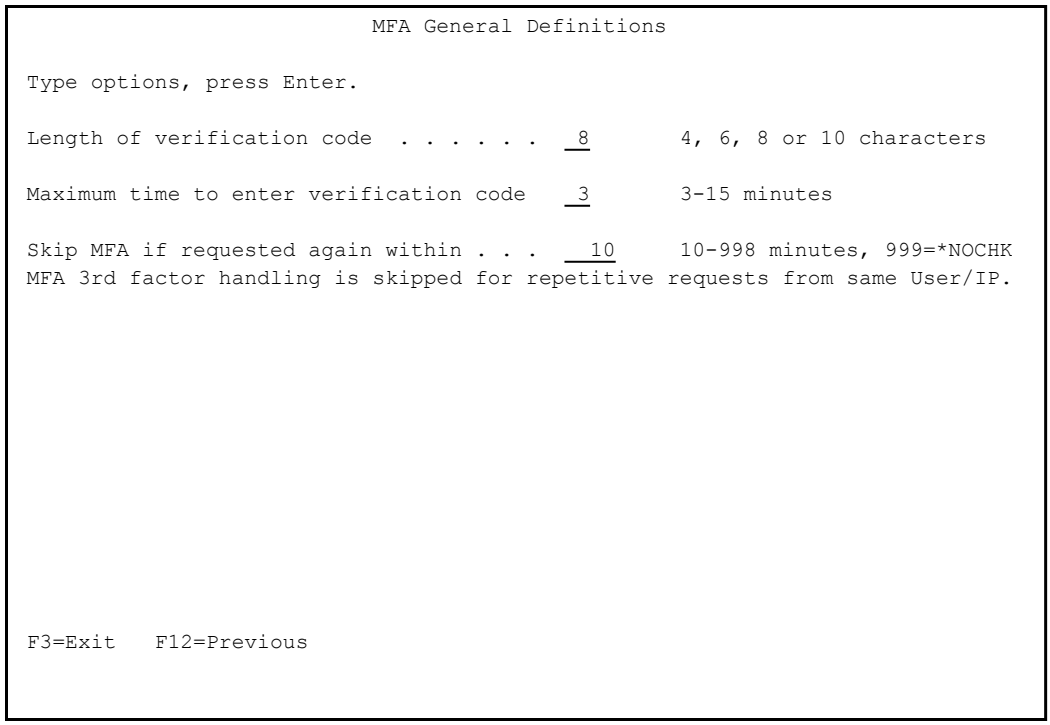
To **define general parameters for MFA**, select **81. System Configuration** from the main **Multi-Factor Authentication (MFA)** menu (as shown in "Starting Multi Factor Authentication (MFA)" on page 10). The **System Configuration** screen appears:

```
ODPARMR                        System Configuration              3/10/21 13:22:47

Authority On Demand                        Multi-Factor Authentication
 1. Global Parameters                      61. General
 2. Exit programs
 3. Session End Activity                   SIEM Support
 4. Attachment setup                       70. Main Control-----> Active
 5. Defaults                               71. SIEM 1: Syslog #1     N
 6. Reason Structure                       72. SIEM 2: Syslog #2     N
 7. Multi-System LPAR Support              73. SIEM 3: Syslog #3     N
 8. Emergency rules                        75. SNMP Definitions
 9. Log Retention
                                           Person Data
Password Reset                             81. Copy Attributes
51. Control & Self-Registration
52. Initial Process Defaults               General
55. Customizing web interface              91. Language Support
                                           99. Copyright Notice

Selection ===>
Release ID . . . . . .  06.03 21-09-12    788C500  41A EP10   2
Authorization code . . . . . .  O02111694776              2   RLDEV
F3=Exit    F22=Enter Authorization Code
```

Select **61. General** from the **Multi-Factor Authentication** section of the **System Configuration** screen. The **MFA General Definitions** screen appears:



The body of the screen includes the following fields:

Length of verification code

The length of the verification code that is sent to the user. The value may be **4**, **6**, **8**, or **10** (so that a code may be split evenly when sent to a combination of the user's cell phone and email).

Maximum time to enter verification code

The number of minutes that the system waits for the user to respond after it sends a verification code. If that time is exceeded, the verification attempt fails. The value may be from **3** to **15**.

Skip MFA if requested again within

Do not request authentication again if the same user, connecting from the same IP address, has been authenticated within the given number of minutes. The value may be from **10** to **998**. If it is set to **999**, the system does not recheck connection from that user and IP if they have already been authenticated.

Specifying Users Requiring Multi Factor Authentication

To **specify which users require Multi Factor Authentication**, select **1 . Users Requiring MFA** from the main **Multi Factor Authentication (MFA) menu**. The **Users Requiring MFA** screen appears.

```
                              Users Requiring MFA

Type options, press Enter.                        Position:
 4=Delete

                 MFA  Sign  FTP     FTP     SQL  File
Opt  User*       By   On    Server  Client       Server
     *ALL
 _   A*          2    Y     _       _       _    _
 _   AA*         2    Y     _       _       _    _
 _   ALEX        3          _       _       _    _
 _   AODSPC      2    Y     _       _       _    _
 _   AU          _    O     _       _       _    _
 _   AVICTOR     2    Y     _       _       _    _
 _   DAVID       _    Y     _       _       _    _
 _   DB          2    Y     _       _       _    _
 _   DS          2    Y     _       _       _    _
 _   EL*         2    Y     _       _       _    _
                                                          More...
Require MFA: Y=Yes, O=Outside of certified network
MFA type: 1=Cell, 2=Email, 3=Cell+Email

F3=Exit    F6=Add new    F12=Cancel
```

The body of the screen contains lines for specific users or groups.

For each items, the **MFA by** column indicates the medium to which the system sends codes for verification. Possible values include:

- **1**: SMS
- **2**: Email
- **3**: Split the code between SMS and Email

The remaining fields specify the connection types for which MFA is required. The connections include:

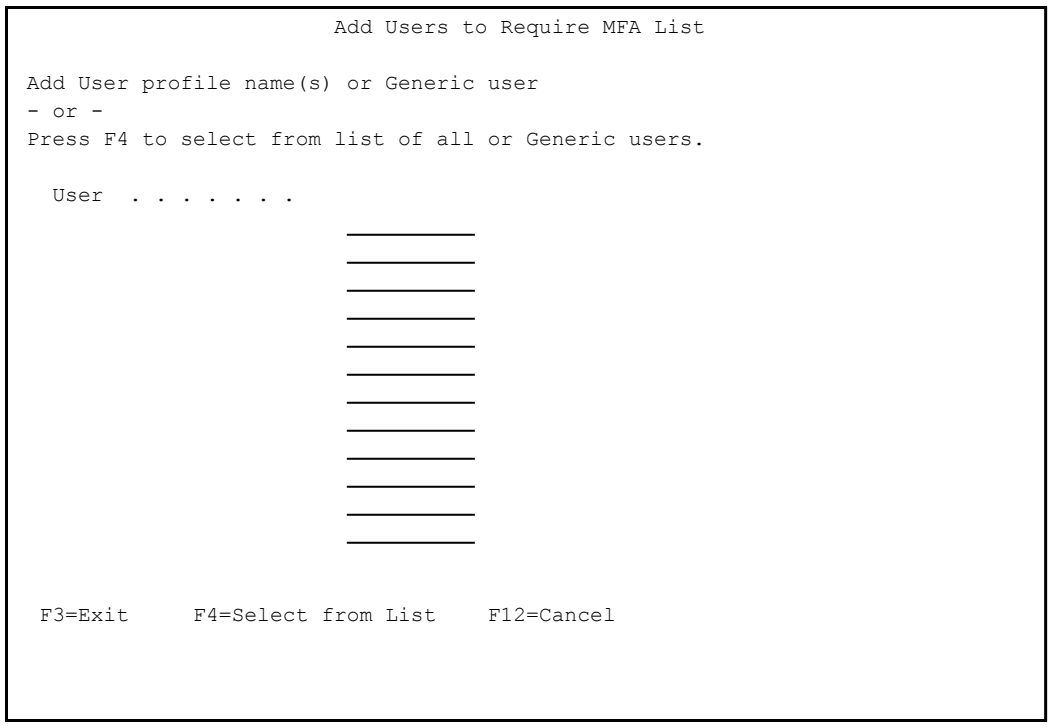
- **Sign-on**
- **FTP Server**

- **FTP Client**
- **SQL**
- **File Server**

For each, you can specify

- **Y**: MFA always required.
- **O**: MFA required when connecting from outside certified networks (as shown in)
- **(blank)** : MFA is never required

To add a new person to the list of users, press the F6 key. The Add Users to Require MFA List screen appears:



Enter the profile names or Generic names of one or more users in the fields on this screen. To select from a list of known users, press the F4 key.

To remove a person from the list, enter **4** in the **Opt** field for that person on the Users Requiring MFA screen, as shown above..

Defining Persons

To **display and enter information concerning each user**, select **5. Person Information** from the Multi Factor Authentication (MFA) main menu. The **Work with Persons** screen appears:

```
                          Work with Persons
                                                Subset . . . _______________
 Type options, press Enter.
 1=Work with   3=Copy   4=Delete   7=Questions

Opt Person     Name                 Role
 _  ALEX       sdfgdf safsdfsf      *NA-*NA-*NA
 _  ALEXANDER  Muchnik Alex         *NA-*NA-*NA
 _  ALEX2      Mudfdf alexxx        *NA-*NA-*NA
 _  ALEX22     muchnik alex         *NA-*NA-*NA
 _  ALEX22ENG  Kan Emmanuil         *NA-*NA-*NA
 _  ALEX22H    KIMKHI ALEX          *NA-*NA-*NA
 _  ALEX22HEBB ELI SHATS            *NA-*NA-*NA
 _  ALEX22HEBC shats elka           *NA-*NA-*NA
 _  ALEX22HEBD ÕÑ ¡ÈÅ               *NA-*NA-*NA
 _  ALEX22HEBF ¡ÈÅ ÕÑ               *NA-*NA-*NA
 _  ALEX3      d d                  *NA-*NA-*NA
 _  BOGON001   Bogon John           IL-ACCOUNTS PAYABLE-MANAGER
 _  ELI        test alex            *NA-*NA-*NA
 _  GEORGETEST Test George          NY-CASHIER-MANAGER
                                                                      More...
F3=Exit    F6=Add new    F12=Cancel
```

The body of the screen contains a line for each user. Each contains the following fields:

Person

A unique identifier for the Person.

Name

The family name and first name of the user.

Role

A set of three fields determining the Person's role within the organization, combining the Person's Location, Department, and Position.

To **add a new person**, press the **F6** key. The **Add New Person** screen appears, as shown in "Adding a New Person" on page 18.

To **modify a person**, enter **1** in the **Opt** field for the person. The **Modify Person** screen appears, as shown in "Modifying a Person" on page 20.

Adding a New Person

To **add a new person** to the list of users, press the **F6** key on the **Working with Persons** screen (as shown in "Defining Persons" on page 16). The **Add New Person** screen appears.

```
Screen 1/2                      Add New Person

Person  . . . . . .  __________
ID. Number  . . . . . .  ____________________________
Birth date  . . . . . .  010101______________________
Cell phone  . . . . . .  ____________________________ F4=SMS provider
Email address . . . . . .  _________________________
                         _________________________
Employee number . . . . .  _________________________
Family name . . . . . .  ___________________________
First name  . . . . . .  ___________________________
Preferred language  . . .  ENG______________________
Office phone  . . . . . .  _________________________
Default User ID.  . . . .  _________________________
Password Reset Class  . .  *DFT_____________________ Name, *DFT, *NEVER




Highlighted fields are mandatory. Email or Cell# is required.

F3=Exit    F4=Prompt    F7=Choose fields    F12=Cancel
```

The body of the screen contains these fields:

Person

A unique identifier for the Person.

ID. Number

The National ID number of the Person.

Birth date

The Person's birth date in the standard national format as set for the system. In the USA, for example, it would be "MM/DD/YY", so December 31st, 1970 would be "12/31/70". In much of Europe, it would be "DD/MM/YY", so December 31st, 1970 would be "31/12/70".

Cell phone

The cell phone number of the Person. SMS notifications of new passwords would go to this number. To select a mobile phone provider from a list, press the F4 key.

Email address

The email address of the person. Email notifications of new passwords would go to this email address.

Employee number

The employee number of the Person within the organization

Family name

The family name or surname of the Person

First name

The first name of the Person.

Preferred language

The language in which the Person will receive verification questions. To select the language from a list, press the F4 key.

Office phone

The office phone number of the Person

Default user ID

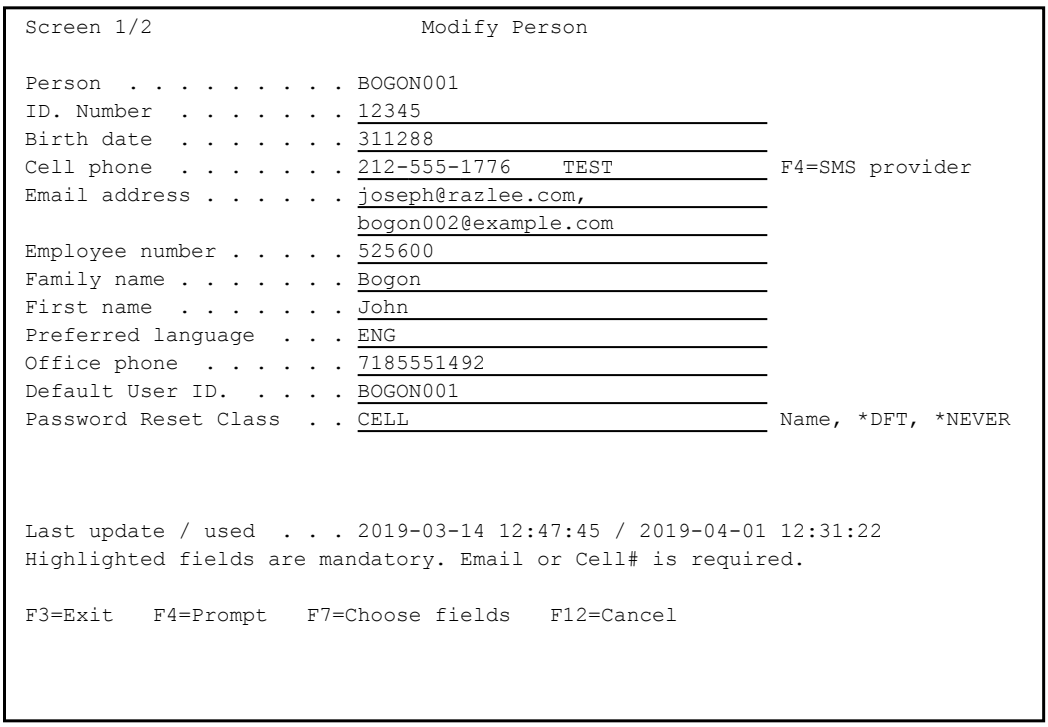
The preferred User ID of the Person on the IBM i. It is used to create the User Profiles for the Person.

Password Reset Class

The Password Reset class to which the person belongs. The class determines how the user's identity is verified when resetting passwords. To select the class from a list, press the F4 key. You can also enter either "***DFT**" to use default settings or "***NEVER**" to define that the Password Reset class will never be used.

Modifying a Person

To **modify a person**, enter **1** in the **Opt** field for the person on the **Working with Persons** screen, as shown in "Defining Persons" on page 16. The **Modify Person** screen appears:



The body of the screen contains these fields:

Person

A unique identifier for the Person.

ID. Number

The National ID number of the Person.

Birth date

The Person's birth date in the standard national format as set for the system. In the USA, for example, it would be "MM/DD/YY", so December 31st, 1970 would be "12/31/70". In much of Europe, it would be "DD/MM/YY", so December 31st, 1970 would be "31/12/70".

Cell phone

The cell phone number of the Person. SMS notifications of new passwords would go to this number. To select a mobile phone provider from a list, press the F4 key.

Email address

The email address of the person. Email notifications of new passwords would go to this email address.

Employee number

The employee number of the Person within the organization

Family name

The family name or surname of the Person

First name

The first name of the Person.

Preferred language

The language in which the Person will receive verification questions. To select the language from a list, press the F4=Prompt key.

Office phone

The office phone number of the Person

Default user ID

The preferred User ID of the Person on the IBM i. It is used to create the User Profiles for the Person.

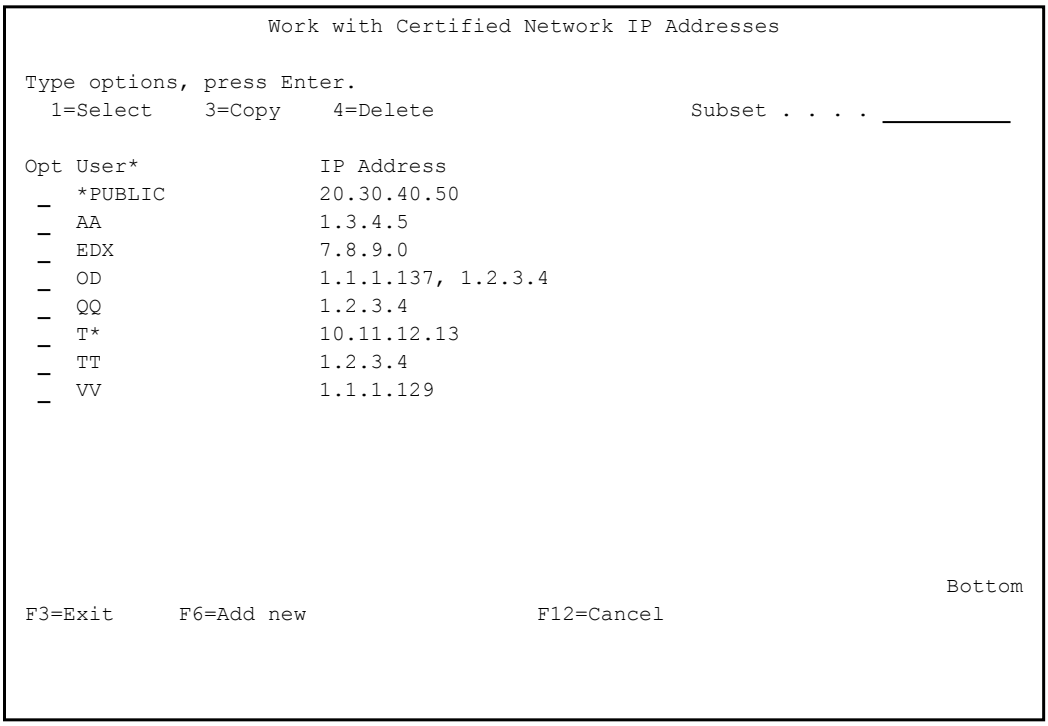
Password Reset Class

The Password Reset class to which the person belongs. The class determines how the user's identity is verified when resetting passwords. To select the class from a list, press the F4 key. You can also enter either "***DFT**" to use default settings or "***NEVER**" to define that the Password Reset class will never be used.

Specifying Certified Network IP Addresses

You can specify (on the **Users Requiring MFA** screen, shown in "Specifying Users Requiring Multi Factor Authentication" on page 14) that users may bypass Multi Factor Authentication if they are connecting from certified network IP addresses.

To **specify network IP addresses** from which particular users may access the system without added authentication, select **`8. Certified Network IP Addresses`** from the main **Multi Factor Authentication (MFA)** menu. The **Work with Certified Network IP Addresses** screen appears:



The body of the screen contains lines for each user or Generic* user. Each line contains the fields:

`User`

The username or Generic* name of the users

IP Addresses

Certified IP addresses for the user. If they connect from these IP Addresses, and the user is set not to require MFA when connecting via that protocol via certified addresses (by setting the field for that user and protocol to the letter **O** on the **Users Requiring MFA** screen), MFA is not required.

To **modify the certified IP addresses** for a user, enter **1** in the **Opt** field for that user. The **Modify User of Certified Network IP Addresses** screen appears, as shown in "Modifying Certified Network IP Addresses" on page 25.

To **add users and their certified IP addresses**, press the **F6** key. The **Add User of Certified Network Addresses** screen appears, as shown in "Adding Users of Certified Network IP Addresses" on the next page.

Adding Users of Certified Network IP Addresses

To **add users of certified IP addresses**, press the **F6** key from the **Work with Certified Network IP Addresses** screen (as shown in "Specifying Certified Network IP Addresses" on page 22). The **Add User of Certified Network Addresses** screen appears:

```
                Add User of Certified Network Addresses

Type information, press Enter.
User  . . . . . .  _________          Name, generic*
                                        F4 for list

  Certified Network
IP Address        Subnet Mask       Text
  _______________   _______________   ____________________________
_______________   _______________   ____________________________
_______________   _______________   ____________________________
_______________   _______________   ____________________________
_______________   _______________   ____________________________
_______________   _______________   ____________________________
_______________   _______________   ____________________________
_______________   _______________   ____________________________
_______________   _______________   ____________________________
_______________   _______________   ____________________________
_______________   _______________   ____________________________
_______________   _______________   ____________________________
     More...

F3=Exit    F4=Prompt    F11=Alternate view    F12=Cancel
```

The **User** field, near the top of the screen, is for the name of the user for whom you are specifying the addresses. This can be a single name or a Generic* name. Press the **F4** key to select a name from a list of known users.

The body of the screen contains lines for the IP address ranges from which the user's connections do not need MFA. Each line includes these fields:

Certified Network IP Address

An IP address in the certified range.

Subnet Mask

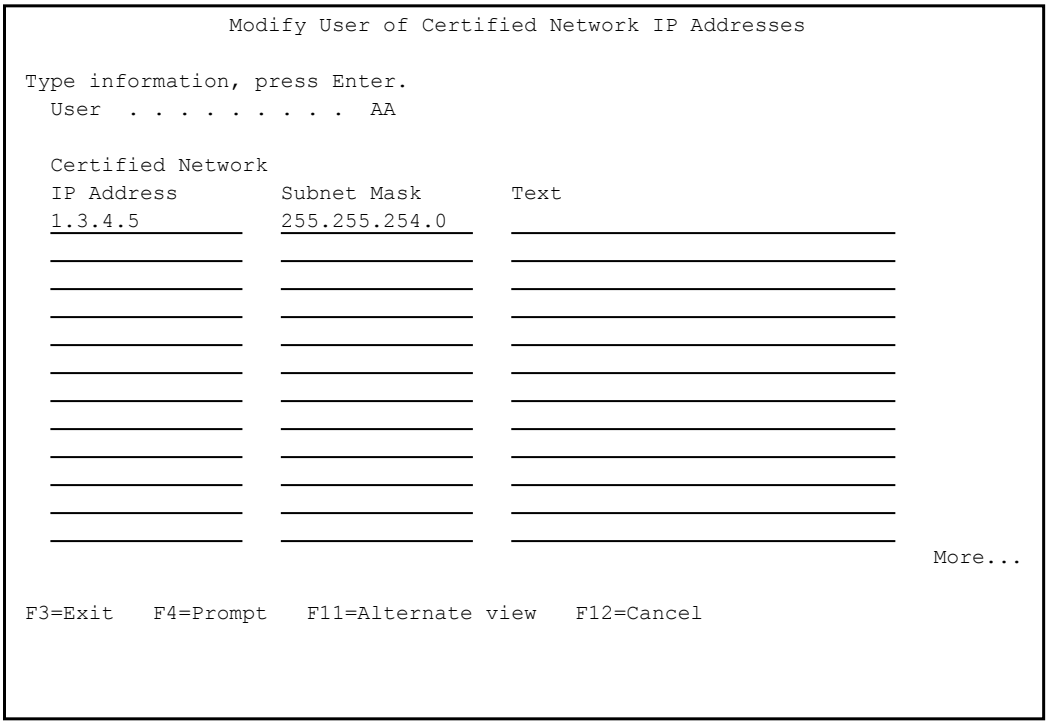
A subnet mask indicating the range of addresses including that address.

Text

A text description of the range.

Modifying Certified Network IP Addresses

To **modify the certified IP addresses** for a user, enter **1** in the **Opt** field for that user on the **Work with Certified Network IP Addresses** screen (shown in "Specifying Certified Network IP Addresses" on page 22). The **Modify User of Certified Network IP Addresses** screen appears:



The body of the screen contains lines for the IP address ranges from which the user's connections do not need MFA. Each line includes these fields:

Certified Network IP Address

An IP address in the certified range.

Subnet Mask

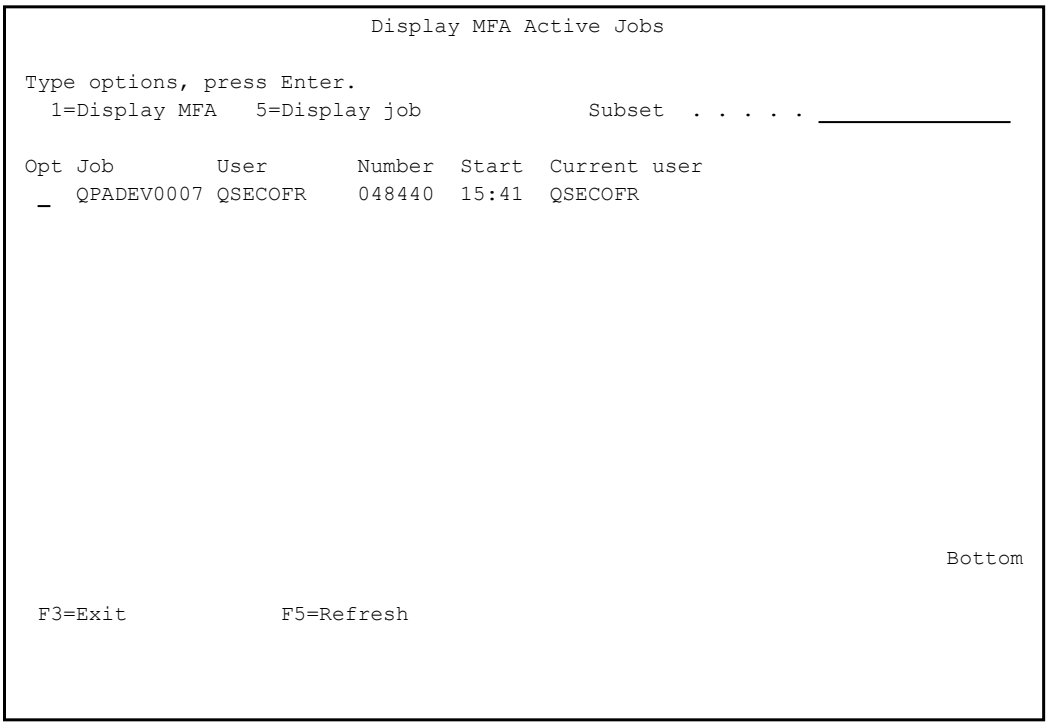
A subnet mask indicating the range of addresses including that address.

Text

A text description of the range.

Displaying Jobs Controlled by MFA

To display jobs controlled by Multi Factor Authentication, select **15. Display Jobs Controlled by MFA** from the main Multi-Factor Authentication (MFA) menu (as shown in "Starting Multi Factor Authentication (MFA)" on page 10). The Display MFA Active Jobs screen appears:



The body of the screen contain lines for each job being run from a connection that used Multi Factor Authentication. The fields include:

Job

The name of the job

User

The user who started the job

Number

The number of the job

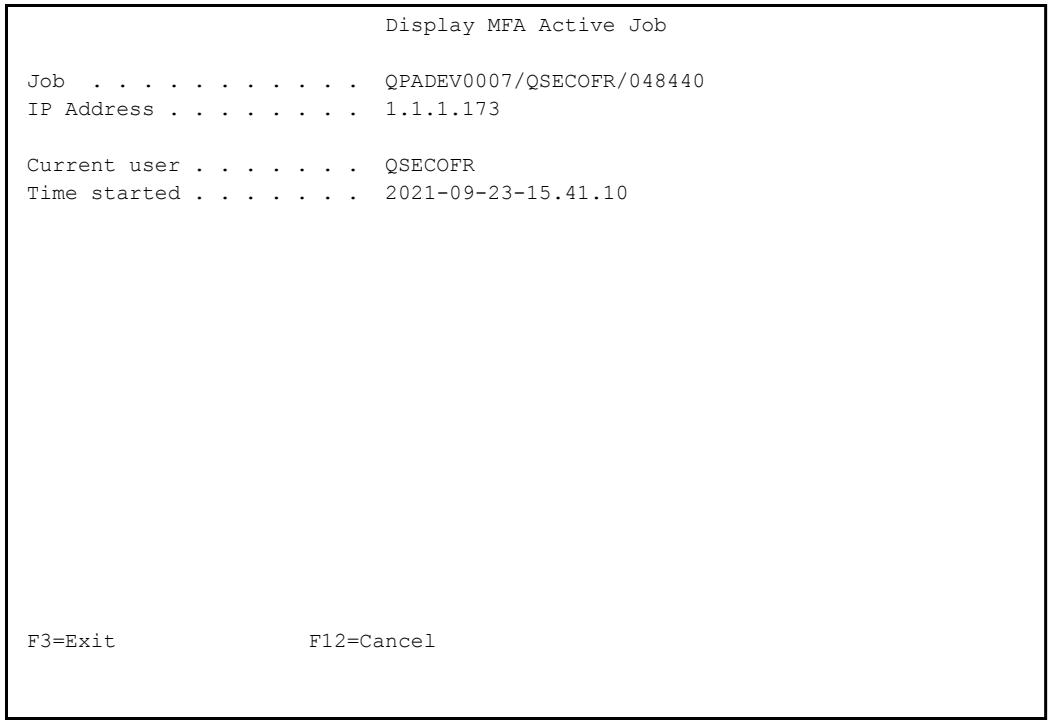
Start

The time at which the job was started

Current user

The user currently using the job

To display further information about a job, enter **5** in the **Opt** field for that job. The Display MFA Active Job screen appears.



In addition to the information on the previous screen, this screen includes:

- the **IP Address** from which the connection was made
- the date on which the job was started, in the **Time started** field.