iSecurity Multi Factor Authentication (MFA)

User Guide
Version 7.01

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 5.

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)

MFA User Guide

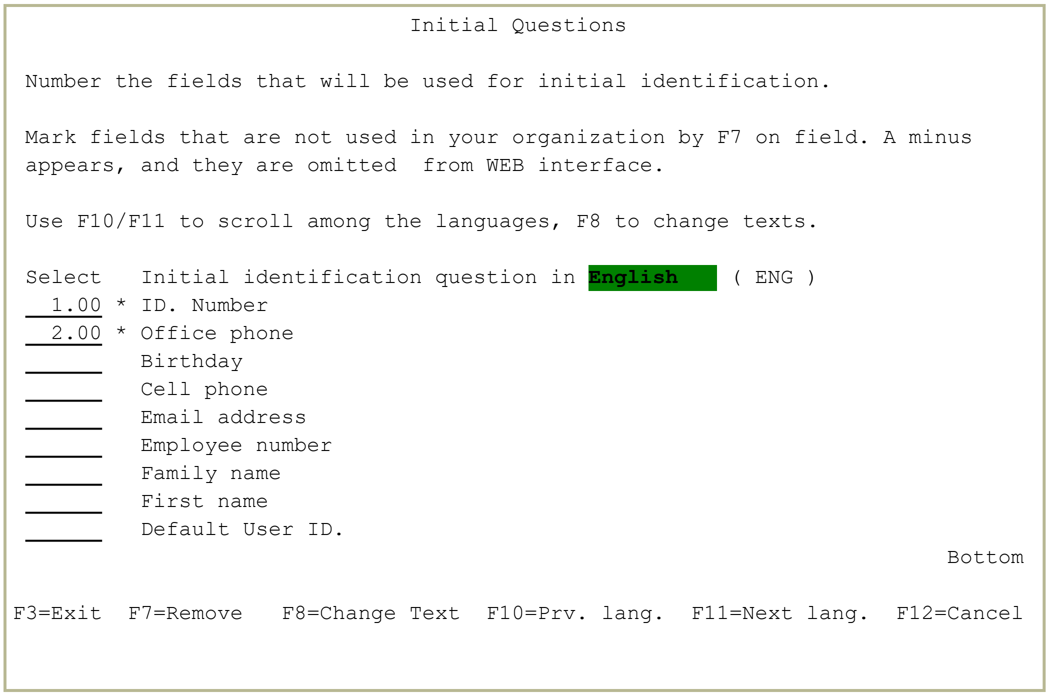
This User Guide is for end users, who will use Multi-Function Authentication to connect to the organization's systems.

The "MFA Administrator's Guide" on page 16, which follows, documents how to set up and administer MFA systems, and is of less interest to end users.

Setting up your MFA Access

When you first log in to the IBM i via the green screen (5250) interface after MFA has been implemented, you may be prompted to enter further information about yourself (such as phone numbers or company ID) or private questions and answers to be used if you would need to reset your password.

The screen that you are presented should resemble this, although your organization may customize the fields on it:



```
                              Initial Questions

 Number the fields that will be used for initial identification.

 Mark fields that are not used in your organization by F7 on field. A minus
 appears, and they are omitted  from WEB interface.

 Use F10/F11 to scroll among the languages, F8 to change texts.

 Select   Initial identification question in English     ( ENG )
 ___1.00 * ID. Number
 ___2.00 * Office phone
 ______    Birthday
 ______    Cell phone
 ______    Email address
 ______    Employee number
 ______    Family name
 ______    First name
 ______    Default User ID.
                                                                     Bottom

F3=Exit  F7=Remove   F8=Change Text  F10=Prv. lang.  F11=Next lang.  F12=Cancel
```

Once you have entered this information, you can continue to log in as before.

Soon afterward, you will receive an email containing the QR code and emergency codes for use with MFA, encrypted for security.

You will need to set up an authenticator app or device to use in MFA. MFA can work with, for example, Google Authenticator, Microsoft Authenticator, Authy, YubiKey, or the built-in iOS and MacOS authenticators. Adding your account to each involves a simple process, though there are slight differences between then. Instructions for the Microsoft Authenticator, for example, are online at https://support.microsoft.com/en-us/accountbilling/add-your-work-or-school-account-to-the-microsoft-authenticator-app-43a73ab5-b4e8-446d-9e54-2a4cb8e4e93c

Print your emergency codes and store them someplace secure.

Logging In with MFA

Once you have been set up with MFA and established a connection for it to an Authenticator, the Sign On screen for the IBM i includes an additional field, **MFA Token**, below the **Password** field.

```
                             Sign On

                                      System  . . . . . :   RLDEV
                                      Subsystem . . . . :   QINTER5
                                      Display . . . . . :   EVG02



User  . . . . . . . . . . . . . .
Password  . . . . . . . . . . . .
MFA Token . . . . . . . . . . . .
Program/procedure . . . . . . . .
Menu  . . . . . . . . . . . . . .
Current library . . . . . . . . .




               COPYRIGHT IBM CORP. 1980, 2018.
```

To sign in, enter your Username and Password as before. Open your Authenticator app or device and enter the six-digit code shown for your system in the **MFA Token** field.

NOTE: The value shown in the Authenticator changes every thirty seconds. If you see an error upon entering the value into the **MFA Token** field, there's a chance that it may have changed before you finished entering it. Check the Authenticator again and enter the new value.

Once you are authenticated, you can access the systems and exit points for which you have been authorized within the organization without further authentication for a predetermined amount of time.

Connecting to other Services with MFA

If you open a different connection to a system via FTP, ODBC, or other exit points, and are not currently authorized, the system sends you an email to confirm the connection.

The email may contain a link to click, which will confirm that you have initiated the connection. It may also require that you confirm the connection by entering the current six-digit code from your Authenticator or an emergency code.

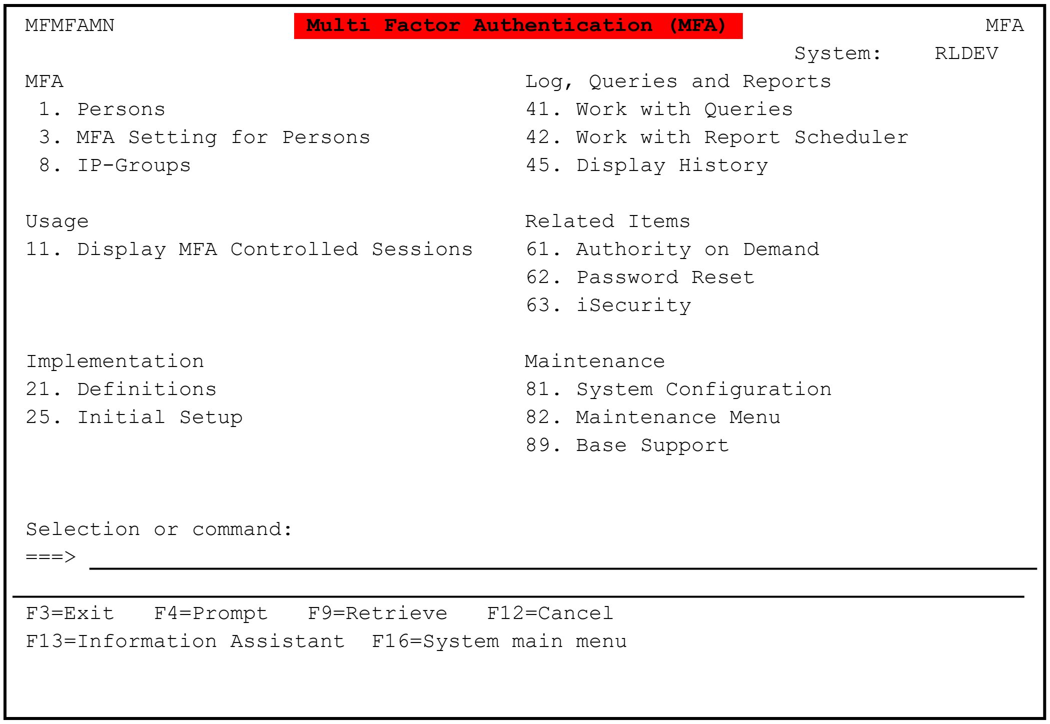
MFA Administrator's Guide

This Administrators' Guide documents how to set up and administer MFA systems.

The "MFA User Guide" on page 11, which precedes it, is for end users, who use Multi-Factor Authentication to connect to the organization's systems.

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:



```
MFMFAMN              Multi Factor Authentication (MFA)                  MFA
                                                      System:    RLDEV
MFA                                    Log, Queries and Reports
 1. Persons                            41. Work with Queries
 3. MFA Setting for Persons            42. Work with Report Scheduler
 8. IP-Groups                          45. Display History

Usage                                  Related Items
11. Display MFA Controlled Sessions    61. Authority on Demand
                                       62. Password Reset
                                       63. iSecurity

Implementation                         Maintenance
21. Definitions                        81. System Configuration
25. Initial Setup                      82. Maintenance Menu
                                       89. Base Support


Selection or command:
===> ____________________________________________________________________

F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
F13=Information Assistant  F16=System main menu
```

To **display and enter information concerning persons**, select **`1. Persons`** from the menu. The **Persons** screen appears, as shown in "Defining Persons" on page 59.

To **specify which users require Multi Factor Authentication**, select **`3. MFA Setting for Persons`** from the menu. The **Users Requiring MFA** screen appears, as shown in "MFA Settings for Persons" on page 82.

To **specify network IP addresses** from which particular users may access the system without added authentication, select **`8. IP-Groups`** from the menu. The **Work with IP-Groups** screen appears, as shown in "Specifying IP-Groups" on page 90"Specifying IP-Groups" on page 90.

To display sessions controlled by Multi Factor Authentication, select **11. Display MFA Controlled Sessions** from the menu. The Display MFA Active Jobs screen appears, as shown in "Displaying Sessions Controlled by MFA" on page 94.

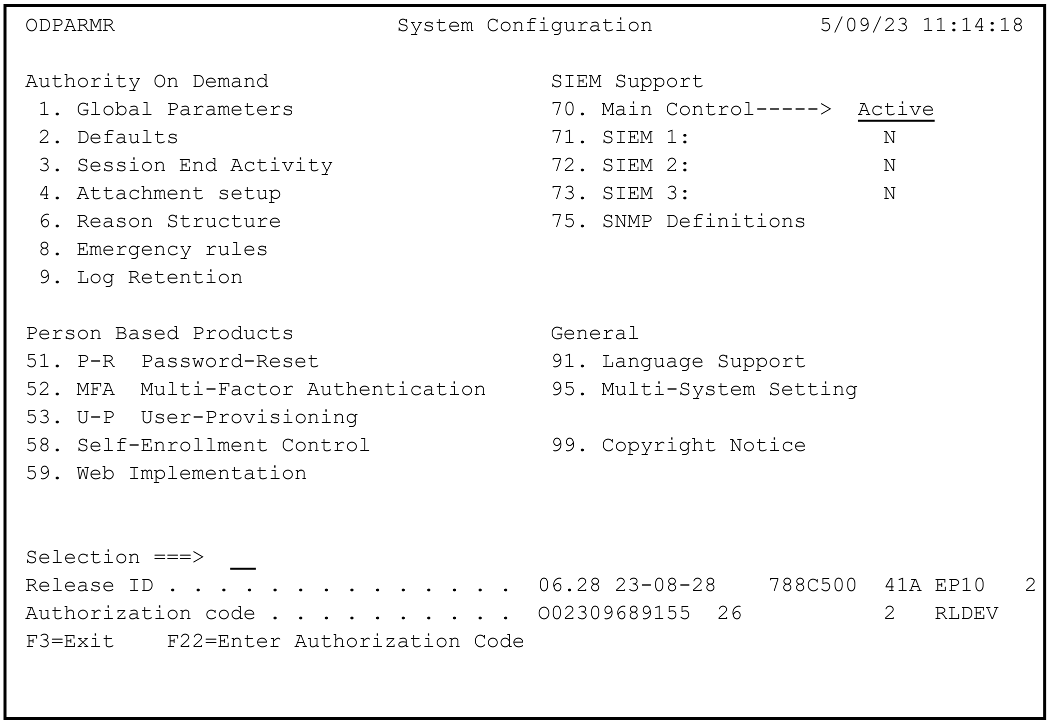
To change MFA Definitions, select **21. Definitions**, from the menu. The Definition screen appears, as shown in Definitions for MFA.

To run the Initial Setup, select **25. Initial Setup** from the menu. THe MFA Setup screen appears, as shown in "Setting Up Multi-Factor Authentication" on page 39.

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 facing page.

Defining General MFA Parameters

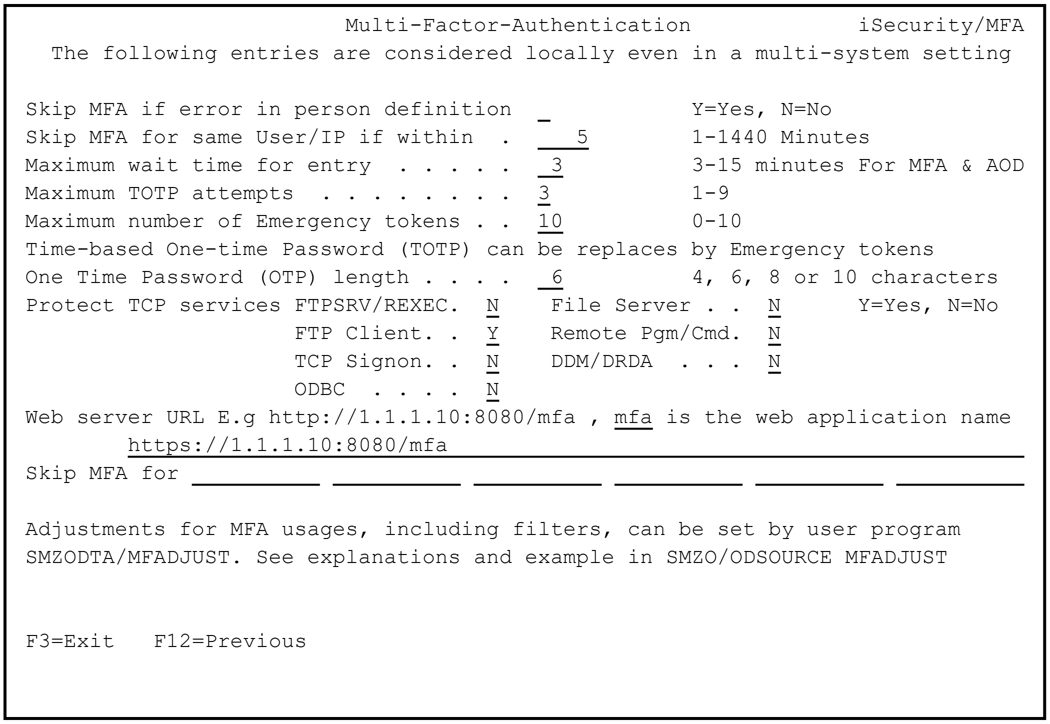
To **define general parameters for MFA**, select **`81. System Configuration`** from the main **`Multi-Factor Authentication (MFA)`** menu (as shown in "Starting Multi Factor Authentication (MFA)" on page 17). The **System Configuration** screen appears:



```
ODPARMR                      System Configuration             5/09/23 11:14:18

Authority On Demand                      SIEM Support
 1. Global Parameters                    70. Main Control----->  Active
 2. Defaults                             71. SIEM 1:               N
 3. Session End Activity                 72. SIEM 2:               N
 4. Attachment setup                     73. SIEM 3:               N
 6. Reason Structure                     75. SNMP Definitions
 8. Emergency rules
 9. Log Retention

Person Based Products                    General
51. P-R  Password-Reset                  91. Language Support
52. MFA  Multi-Factor Authentication     95. Multi-System Setting
53. U-P  User-Provisioning
58. Self-Enrollment Control              99. Copyright Notice
59. Web Implementation


Selection ===>  _
Release ID . . . . . . . . . . . . . .  06.28 23-08-28    788C500  41A EP10   2
Authorization code . . . . . . . . . .  002309689155  26           2   RLDEV
F3=Exit    F22=Enter Authorization Code
```

>

Select **`52. MFA Multi-Factor Authentication`** from the **`Person Based Products`** section of the **System Configuration** screen. The **Multi-Factor-Authentication** screen appears:



```
                        Multi-Factor-Authentication            iSecurity/MFA
  The following entries are considered locally even in a multi-system setting

Skip MFA if error in person definition  _           Y=Yes, N=No
Skip MFA for same User/IP if within  .     5        1-1440 Minutes
Maximum wait time for entry  . . . . .   3          3-15 minutes For MFA & AOD
Maximum TOTP attempts  . . . . . . . .  3           1-9
Maximum number of Emergency tokens . .  10          0-10
Time-based One-time Password (TOTP) can be replaces by Emergency tokens
One Time Password (OTP) length . . . .   6          4, 6, 8 or 10 characters
Protect TCP services FTPSRV/REXEC.  N    File Server . .  N      Y=Yes, N=No
                     FTP Client. .  Y    Remote Pgm/Cmd.  N
                     TCP Signon. .  N    DDM/DRDA  . . .  N
                     ODBC  . . . .  N
Web server URL E.g http://1.1.1.10:8080/mfa , mfa is the web application name
        https://1.1.1.10:8080/mfa
Skip MFA for __________ __________ __________ __________ __________ __________

Adjustments for MFA usages, including filters, can be set by user program
SMZODTA/MFADJUST. See explanations and example in SMZO/ODSOURCE MFADJUST


F3=Exit   F12=Previous
```

The body of the screen includes the following fields:

Skip MFA if error in person definition

If MFA encounters an error in a Person definition, You can skip authentication to let the user sign on without problems.

We log this information, so that you can review the MFA history in **STRMFA > 45 Display History**, or run a scheduled job using the job scheduler **STRMFA > 42 Work with Report Scheduler**, which contains a report of errors.

Skip MFA for same User/IP if 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 **1440**. If it is set to **999**, the system does not recheck connections from that user and IP if they have already been authenticated.

Maximum wait time for entry

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**. This item also affects Authority on Demand.

Maximum TOTP attempts

The maximum number of times that a person can try to enter TOTP codes before the connection is rejected. This can be between **0** and **5**. If set to zero, the connection is rejected immediately if the person enters an incorrect value.

Maximum number of Emergency tokens

The maximum number of token codes generated when MFA is set up for a person.

One Time Password (OTP) length

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).

Protect TCP Services

Services that MFA can protect. To activate MFA for the service, set its field to **Y**.

Web server URL

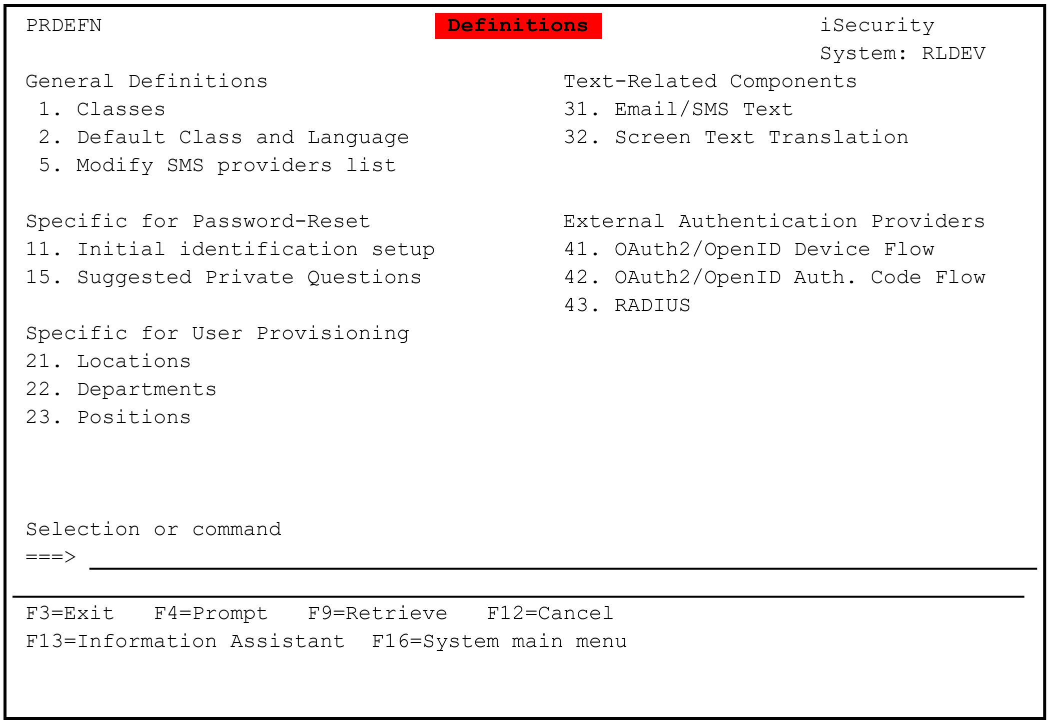
The URL at which the person enters MFA codes.

Skip MFA for

Up to five user profiles that should be excluded from MFA, regardless of the settings within MFA..

Definitions for MFA

To **specify definitions** for MFA (and other related modules), select **`21. Definitions`** from the **Multi Function Authentication** main screen, The **Definitions** screen appears:



```
PRDEFN                          Definitions                  iSecurity
                                                             System: RLDEV
General Definitions                         Text-Related Components
 1. Classes                                 31. Email/SMS Text
 2. Default Class and Language              32. Screen Text Translation
 5. Modify SMS providers list

Specific for Password-Reset                 External Authentication Providers
11. Initial identification setup            41. OAuth2/OpenID Device Flow
15. Suggested Private Questions             42. OAuth2/OpenID Auth. Code Flow
                                            43. RADIUS
Specific for User Provisioning
21. Locations
22. Departments
23. Positions



Selection or command
===> ____________________________________________________________________

F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
F13=Information Assistant  F16=System main menu
```

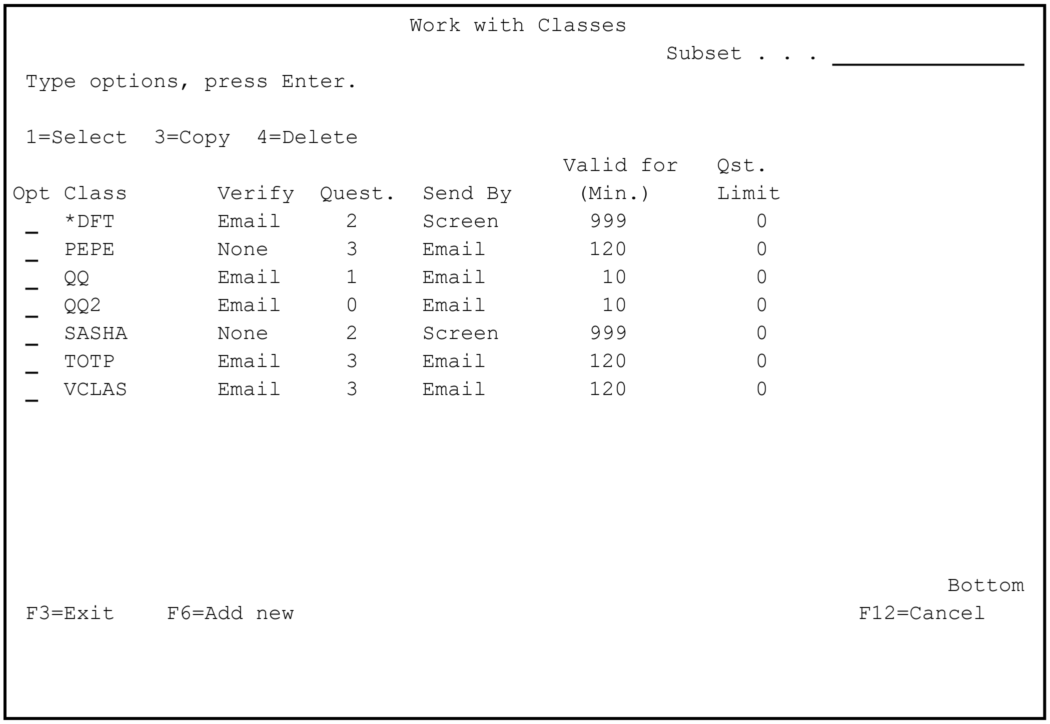
Users can be grouped into **Classes** for MFA. For example, users who have more control over the system might require more detailed MFA verification than others.

To **work with classes**, select **`1. Classes`** from the **Definitions** menu. The **Work with Classes** screen appears.

To **select external authorization providers**, see "External Authentication Providers" on page 29

Working with Classes

To **add, modify, copy, or delete classes**, select **`1. Classes`** from the **Definitions** screen (**`STRMFA > 21`**). The **Work with Classes** screen appears.



```
                               Work with Classes
                                                   Subset . . . _______________
 Type options, press Enter.

 1=Select  3=Copy  4=Delete
                                             Valid for   Qst.
Opt Class       Verify  Quest.  Send By      (Min.)      Limit
 _  *DFT        Email     2     Screen        999          0
 _  PEPE        None      3     Email         120          0
 _  QQ          Email     1     Email          10          0
 _  QQ2         Email     0     Email          10          0
 _  SASHA       None      2     Screen        999          0
 _  TOTP        Email     3     Email         120          0
 _  VCLAS       Email     3     Email         120          0







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

The body of the screen contains a line for each currently defined class. Each line contains these fields:

`Class`

The name of the class.

`Verify`

The class's preferred verification device. Values include **`Cell`**, **`Email`**, or **`None`** (for classes that do not use MFA).

`Quest.`

If using questions for verification, the number of questions asked.

`Send by`

How to send temporary passwords. Possible values are **`Cell`**, **`Email`**, and **`Screen`**.

`Valid for (Min.)`

The number of minutes for which temporary passwords are valid. The value can be between **`1`** and **`998`**. If set to **`999`**, the passwords do not expire.

`Qst. Limit`

The number of tries that the person may take to enter a correct answer to private questions. If set to **`0`**, this has no limit.

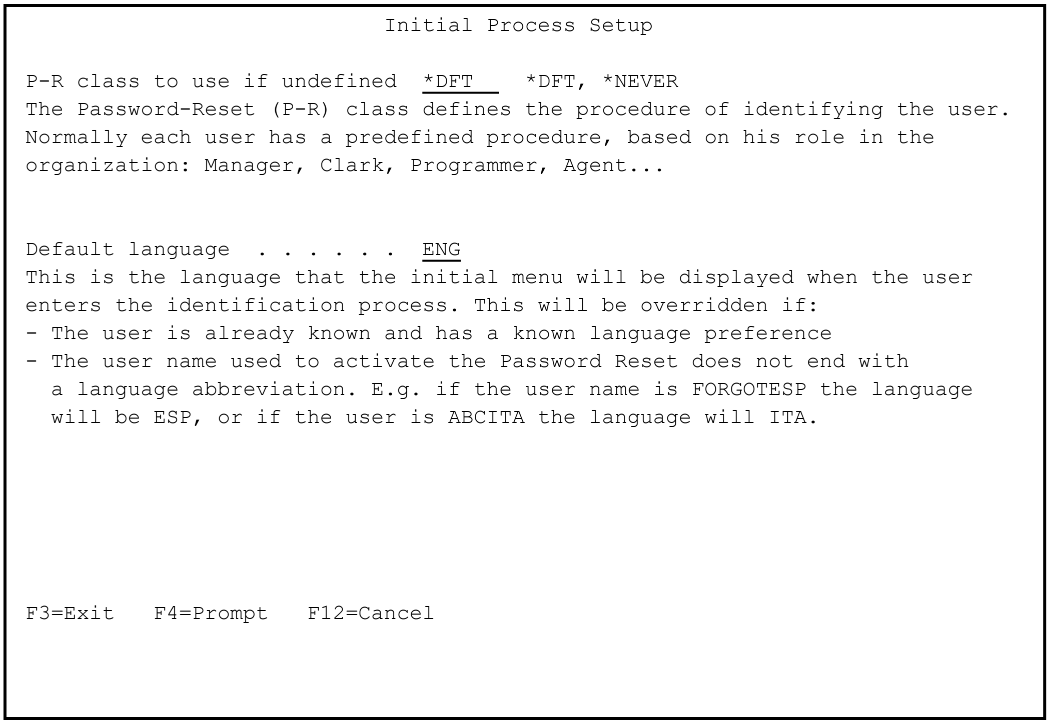
To **modify a class**, enter **`1`** in the **`Opt`** field for that class. The **Modify Class** screen appears, as shown in "Modifying Classes" on page 26.

To **copy a class**, enter **`3`** in the **`Opt`** field for that class. The **Copy Class** screen appears. Enter the name of the new class in the **`New class`** field of that screen, then press **Enter**.

To **delete a class**, enter **`4`** in the **`Opt`** field for that class. The **Delete Class** screen appears, displaying information about the class. Press **Enter** to delete that class. You can only delete classes that have no Persons as members.

To **add a class**, press the **F6** key. The **Add New Class** screen appears, with the same fields as the **Modify Class** screen shown in "Modifying Classes" on page 26.

To **set the default class and language** to use, select **`2. Default Class and Language`** from the **Definitions** menu. The **Initial Process Setup** screen appears:

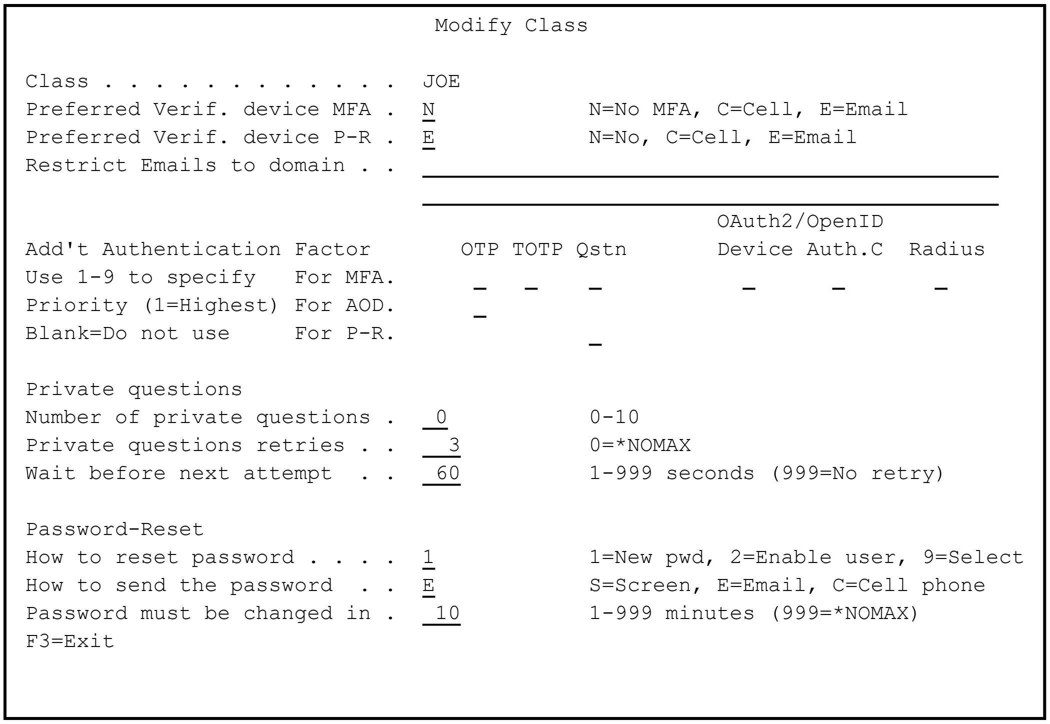


```
                            Initial Process Setup

P-R class to use if undefined  *DFT     *DFT, *NEVER
The Password-Reset (P-R) class defines the procedure of identifying the user.
Normally each user has a predefined procedure, based on his role in the
organization: Manager, Clark, Programmer, Agent...


Default language  . . . . . .  ENG
This is the language that the initial menu will be displayed when the user
enters the identification process. This will be overridden if:
- The user is already known and has a known language preference
- The user name used to activate the Password Reset does not end with
  a language abbreviation. E.g. if the user name is FORGOTESP the language
  will be ESP, or if the user is ABCITA the language will ITA.






F3=Exit   F4=Prompt   F12=Cancel
```

Enter the values as described on that page.

Modifying Classes

To **modify a class**, enter **`1`** in the **`Opt`** field for that class on the **Work with Classes** screen (**`STRFW > 21 > 1`**). The **Work with Classes** screen appears:



```
                                Modify Class

Class . . . . . . . . . . . .   JOE
Preferred Verif. device MFA .   N            N=No MFA, C=Cell, E=Email
Preferred Verif. device P-R .   E            N=No, C=Cell, E=Email
Restrict Emails to domain . .   _____________________________________________
                                _____________________________________________
                                                      OAuth2/OpenID
Add't Authentication Factor       OTP TOTP Qstn       Device Auth.C  Radius
Use 1-9 to specify   For MFA.      _   _    _           _      _       _
Priority (1=Highest) For AOD.      _
Blank=Do not use     For P-R.               _

Private questions
Number of private questions .    0           0-10
Private questions retries . .     3          0=*NOMAX
Wait before next attempt  . .    60          1-999 seconds (999=No retry)

Password-Reset
How to reset password . . . .   1            1=New pwd, 2=Enable user, 9=Select
How to send the password  . .   E            S=Screen, E=Email, C=Cell phone
Password must be changed in .    10          1-999 minutes (999=*NOMAX)
F3=Exit
```

The screen contains these fields:

`Class`

The name of the class. The default class is specified as **`*DFT`**.

`Preferred Verification Device`

The device to be used for verification. A user who connects to the system and requires MFA is sent a link for confirmation, either via email or via SMS to the user's smartphone.

Values include:

`C`: Cell phone

`E`: Email

`N`: The class does not use MFA.

Restrict emails by domain

The domains to which verification codes and new passwords can be sent by email. For example, they might be restricted to domains within the organization. If this field is left empty, the emails can go to any domain.

Add't Authentication Factor

The methods that MFA, Authority on Demand, and Password Reset use for additional authentication. When the user signs in using MFA and follows the link sent via email or SMS, the page displays a series of buttons on the lower right. The user can select those buttons to use alternate methods of verification. The values set here determine the order in which the buttons appear onscreen, from left to right. If no value is set for a method here, no button appears for that method.

The methods are:

OTP

A one-time password, sent via email or SMS, as set in the **Preferred Verification Device** field.

TOTP

A temporary one-time password, as shown in an authenticator app, such as the Microsoft Authenticator or Google Authenticator, installed on the user's smartphone. Users are set up with MFA (as shown in) receive a QR code by email. Scanning this code with an authenticator app connects the app and your MFA system. Users authenticating via TOTP enter the code shown for your system in their app. The codes change every thirty seconds. If a code expires while the user is entering it, they must enter the code that replaced it.

Qstn

A set of personal security questions that the user must answer correctly. The questions for each person are entered on the Modify Person Identification Questions screen (as shown in Questions and Answers).

OAuth2/OpenID Device Flow

The OAuth 2.0 Device Authorization Grant (formerly known as the Device Flow) is an OAuth 2.0 extension that enables devices with no browser or limited input capability to obtain an access token.

OAuth2/OpenID Auth. Code Flow

The authorization code grant type is used to obtain both access tokens and refresh tokens and is optimized for confidential clients. Since this is a redirection-based flow, the client must be capable of interacting with the resource owner's user-agent (typically a web browser) and capable of receiving incoming requests (via redirection) from the authorization server.

RSA/RADIUS

RADIUS authentication goes through a separate authentication server to authenticate users.

The three fields under **Private Questions** are relevant if **Qstn** has been selected as an additional authentication option.

Number of private questions

The number of private questions that the user is asked. The value can be between 0 and 10. The default is 0, meaning that Password Reset will skip the personal questions.

Private Questions retries

The number of times that a user gets to retry entering the answer to a private question if it fails. If set to **0**, there is no limit to the number of retries.

Wait before next attempt

The number of minutes that a user must wait after entering the maximum number of failed responses before trying again.

The number can be between **0** and **998**. A value of **999** means that there is no waiting time between failures.

External Authentication Providers

MFA can use a variety of methods of authentication provided by external companies or services. Some of these require setting up relationships between the organization and the external provider or installing of authentication apps on the users' devices. Once they are set up, the provider handles many of the complexities and much of the overhead of authentication.

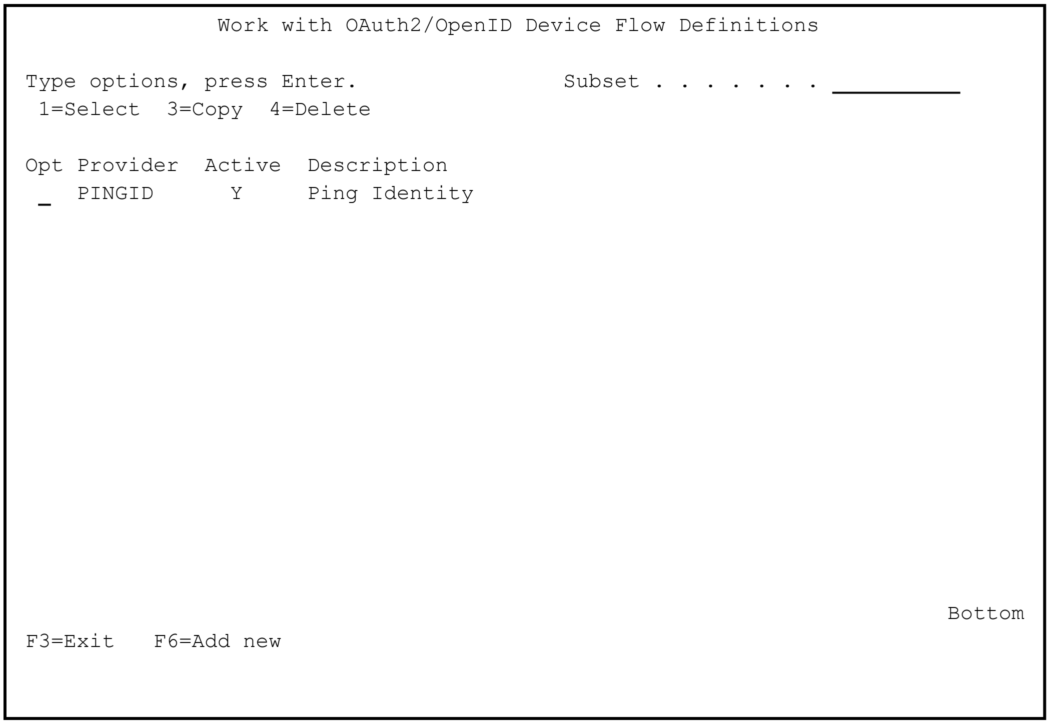
To set up OAuth2/OpenID Device Flow, select **`41. OAuth2/OpenID Device Flow`** from the Definitions menu (**`STRMFA > 21`**). The Work with OAuth2/OpenID Device Flow Definitions screen appears, as shown in "Setting Up OAuth2/OpenID Device Flow Authentication" on the next page.

To set up OAuth2/OpenID Authorization Code Flow, select **`42. OAuth2/OpenID Auth. Code Flow`** from the Definitions menu (**`STRMFA > 21`**). The Work with OAuth2/OpenID Auth. Code Flow Definitions screen appears, as shown in "Setting Up OAuth2/OpenID Authorization Code Flow Authentication" on page 33.

To set up RADIUS, used with systems such as Duo and RSA, select **`43. RADIUS`** from the Definitions menu (**`STRMFA > 21`**). The Work with Radius Definitions screen appears, as shown in "Setting Up RADIUS Authentication" on page 36.

Setting Up OAuth2/OpenID Device Flow Authentication

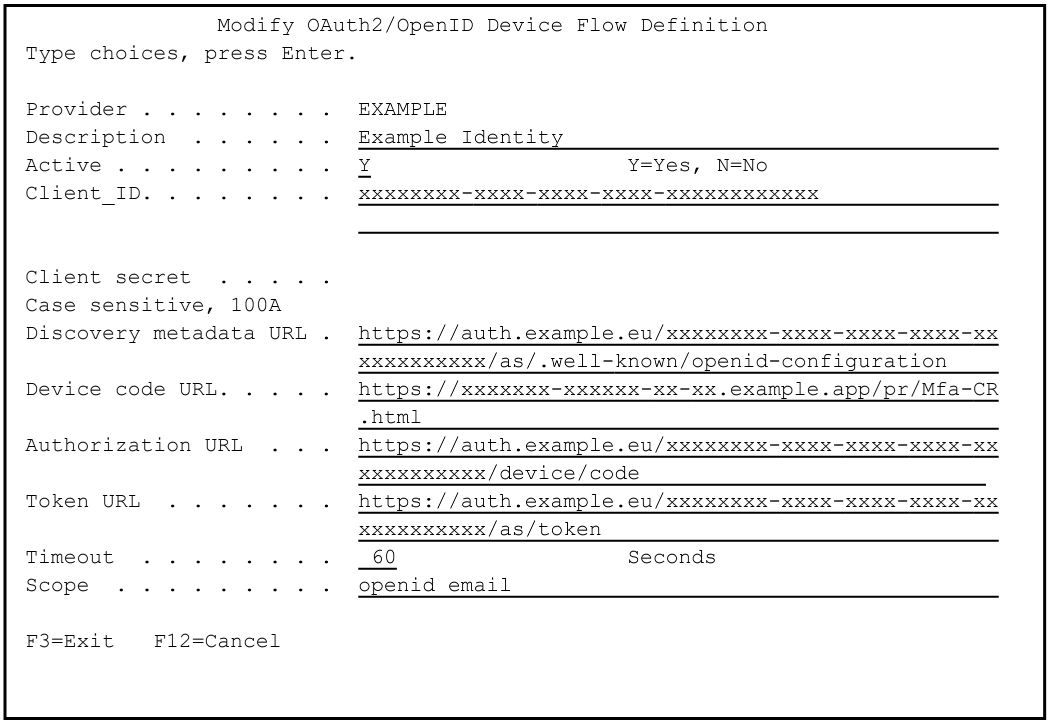
To set up OAuth2/OpenID Device Flow, select **41. OAuth2/OpenID Device Flow** from the Definitions menu (**STRMFA > 21**). The Work with OAuth2/OpenID Device Flow Definitions screen appears.



```
               Work with OAuth2/OpenID Device Flow Definitions

Type options, press Enter.               Subset . . . . . . . __________
 1=Select  3=Copy  4=Delete

Opt Provider  Active  Description
 _  PINGID      Y     Ping Identity













                                                                    Bottom
F3=Exit   F6=Add new
```

For each provider, a line on the screen shows the **Provider** name, whether the provider is **Active**, and a plain text **Description** of the provider.

To modify an OAuth2/OpenID Device Flow, enter **1** in the **Opt** field for that provider. The Modify OAuth2/OpenID Device Flow Definition screen appears:



```
               Modify OAuth2/OpenID Device Flow Definition
Type choices, press Enter.

Provider . . . . . . . .  EXAMPLE
Description  . . . . . .  Example Identity
Active . . . . . . . . .  Y                     Y=Yes, N=No
Client_ID. . . . . . . .  xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx


Client secret  . . . . .
Case sensitive, 100A
Discovery metadata URL .  https://auth.example.eu/xxxxxxxx-xxxx-xxxx-xxxx-xx
                          xxxxxxxxxx/as/.well-known/openid-configuration
Device code URL. . . . .  https://xxxxxxx-xxxxxx-xx-xx.example.app/pr/Mfa-CR
                          .html
Authorization URL  . . .  https://auth.example.eu/xxxxxxxx-xxxx-xxxx-xxxx-xx
                          xxxxxxxxxx/device/code
Token URL  . . . . . . .  https://auth.example.eu/xxxxxxxx-xxxx-xxxx-xxxx-xx
                          xxxxxxxxxx/as/token
Timeout  . . . . . . . .   60                   Seconds
Scope  . . . . . . . . .  openid email

F3=Exit   F12=Cancel
```

The information for most of the fields is generated when you set up your organization's OpenID service with the provider. Copy the information for that provider to corresponding fields on this screen.

The remaining fields have these values:

Provider

A unique name for the provider.

Description

A free text description of the provider.

Active

Setting this to **Y** makes the service active. Setting it to **N** makes it inactive.

Timeout

The maximum number of seconds that the system waits for a response from the provider.

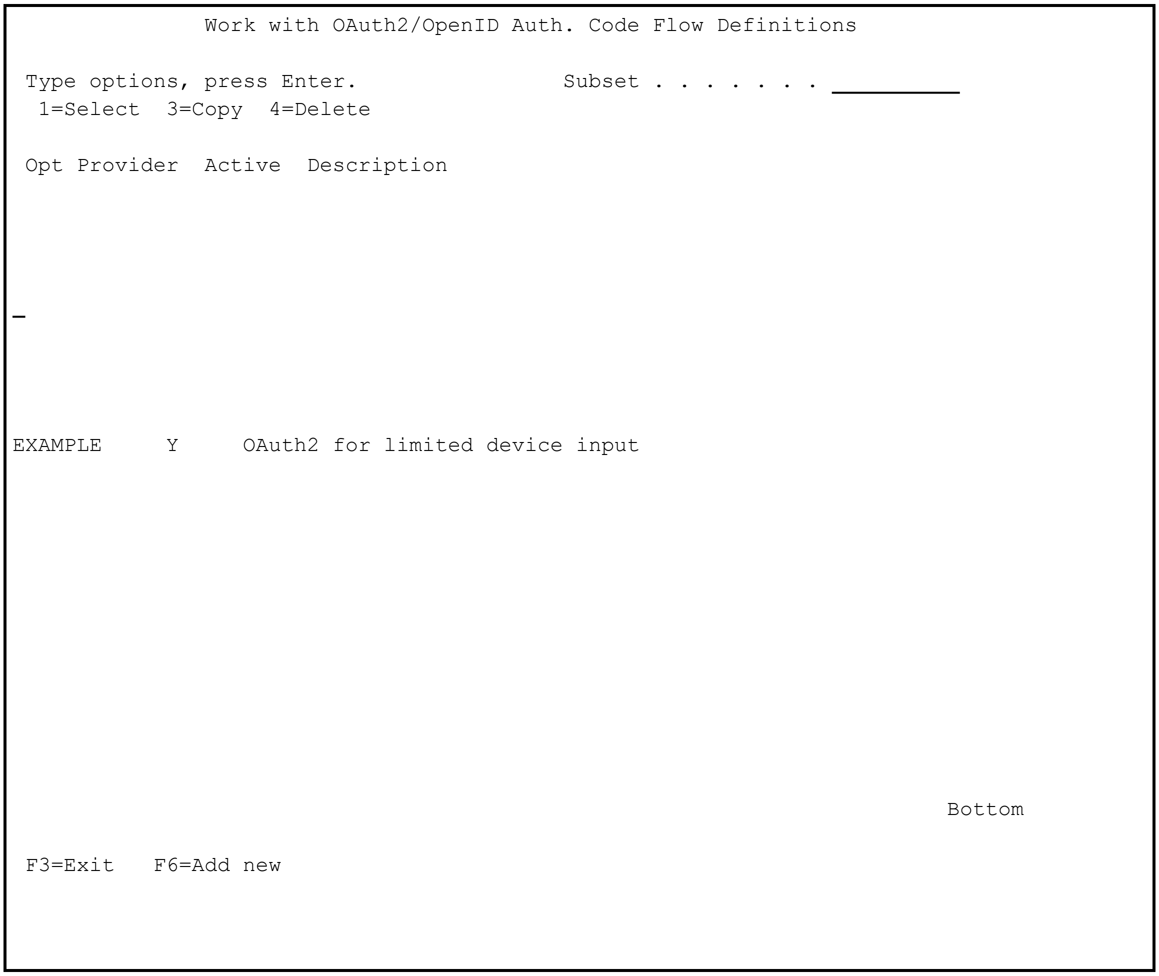
To **copy an OAuth2/OpenID Device Flow Definition**, enter **3** in the **`Opt`** field for that server on the **Work with OAuth2/OpenID Device Flow Definitions** screen. The **Copy OAuth2/OpenID Device Flow Definition** screen appears. Enter the name of the new server in the **`To: Definition`** field of that screen, then press **Enter**.

To **delete an OAuth2/OpenID Device Flow Definition**, enter **4** in the **`Opt`** field for that server on the **Work with OAuth2/OpenID Device Flow Definitions** screen. The **Delete OAuth2/OpenID Device Flow Definition** screen appears, displaying information about the server. Press **Enter** to delete that definition.

To **add an OAuth2/OpenID Device Flow Definition**, press the **F6** key on the **Work with OAuth2/OpenID Device Flow Definitions** screen. The **Add New OAuth2/OpenID Device Flow Definition** screen appears, with the same fields as the **Modify OOAuth2/OpenID Device Flow Definition** screen.

Setting Up OAuth2/OpenID Authorization Code Flow Authentication

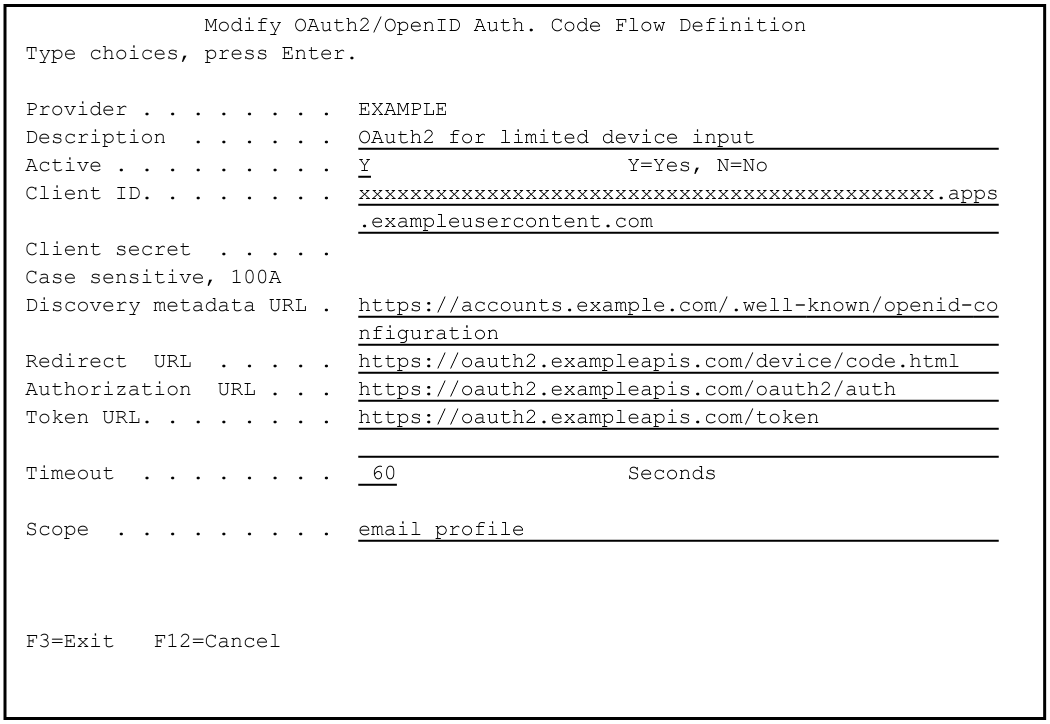
To **set up OAuth2/OpenID Authorization Code Flow Authentication**, select **`42. OAuth2/OpenID Auth. Code Flow`** from the **Definitions** menu (**`STRMFA > 21`**). The **Work with OAuth2/OpenID Auth. Code Flow Definitions** screen appears.



```
               Work with OAuth2/OpenID Auth. Code Flow Definitions

 Type options, press Enter.                Subset . . . . . . . __________
  1=Select   3=Copy   4=Delete

 Opt Provider  Active  Description



_



EXAMPLE     Y     OAuth2 for limited device input










                                                                      Bottom

 F3=Exit   F6=Add new
```

For each provider, a line on the screen shows the **`Provider`** name, whether the provider is **`Active`**, and a plain text **`Description`** of the provider.

To **modify an OAuth2/OpenID Auth. Code Flow definition**, enter **`1`** in the **`Opt`** field for that provider. The **Modify OAuth2/OpenID Auth. Code Flow Definition** screen appears:



```
              Modify OAuth2/OpenID Auth. Code Flow Definition
Type choices, press Enter.

Provider . . . . . . . .  EXAMPLE
Description  . . . . . .  OAuth2 for limited device input
Active . . . . . . . . .  Y                    Y=Yes, N=No
Client ID. . . . . . . .  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.apps
                          .exampleusercontent.com
Client secret  . . . . .
Case sensitive, 100A
Discovery metadata URL .  https://accounts.example.com/.well-known/openid-co
                          nfiguration
Redirect  URL  . . . . .  https://oauth2.exampleapis.com/device/code.html
Authorization  URL . . .  https://oauth2.exampleapis.com/oauth2/auth
Token URL. . . . . . . .  https://oauth2.exampleapis.com/token

Timeout  . . . . . . . .   60                  Seconds

Scope  . . . . . . . . .  email profile



F3=Exit   F12=Cancel
```

The information for most of the fields is generated on the provider's site when you establish your organization's relationship with the provider. Copy the information from their site to corresponding fields on this screen.

The remaining fields have these values:

Provider

A unique name for the provider.

Description

A free text description for the provider.

Active

Setting this to **Y** makes the service active. Setting it to **N** makes it inactive.

Timeout

The maximum number of seconds that the system waits for a response from the provider.

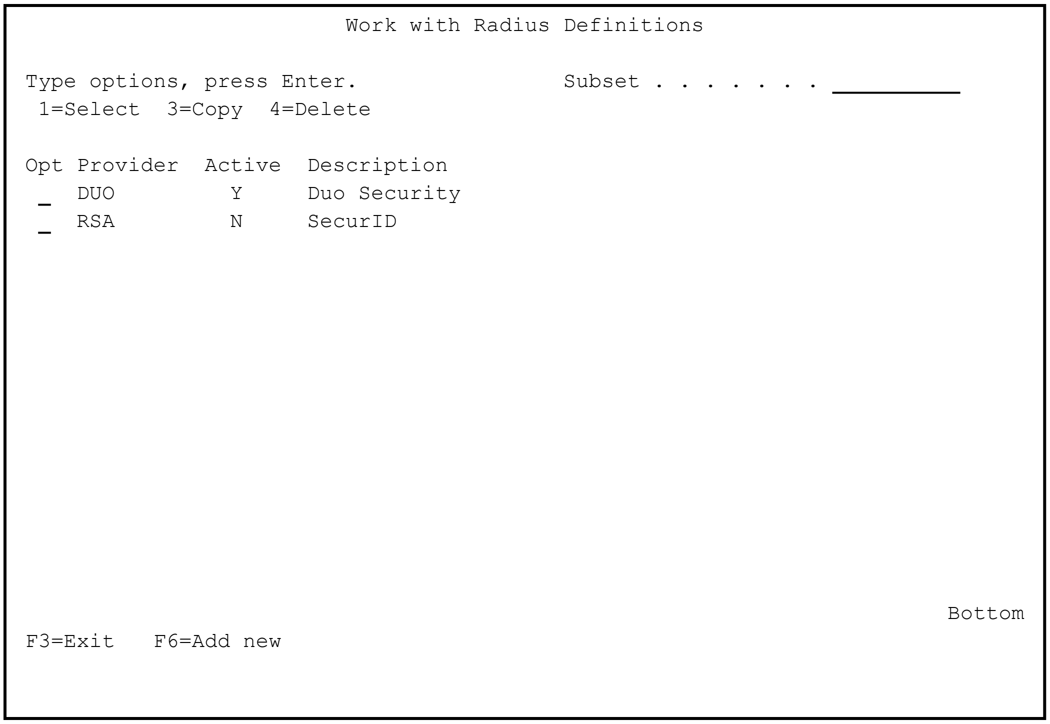
To **copy an OAuth2/OpenID Auth. Code Flow definition**, enter **`3`** in the **`Opt`** field for that provider on the **Work with OAuth2/OpenID Auth. Code Flow Definitions** screen. The **Copy OAuth2/OpenID Auth. Code Flow Definition** screen appears. Enter the name of the new provider in the **`To: Definition`** field of that screen, then press **Enter**.

To **delete an OAuth2/OpenID Auth. Code Flow definition**, enter **`4`** in the **`Opt`** field for that provider on the **Work with OAuth2/OpenID Auth. Code Flow Definitions** screen. The **Delete OAuth2/OpenID Auth. Code Flow Definition** screen appears, displaying information about the provider. Press **Enter** to delete that definition.

To **add an OAuth2/OpenID Auth. Code Flow definition**, press the **F6** key on the **Work with OAuth2/OpenID Auth. Code Flow Definitions** screen. The **Add New OAuth2/OpenID Auth. Code Flow Definition** screen appears, with the same fields as the **Modify OAuth2/OpenID Auth. Code Flow Definition** screen.

Setting Up RADIUS Authentication

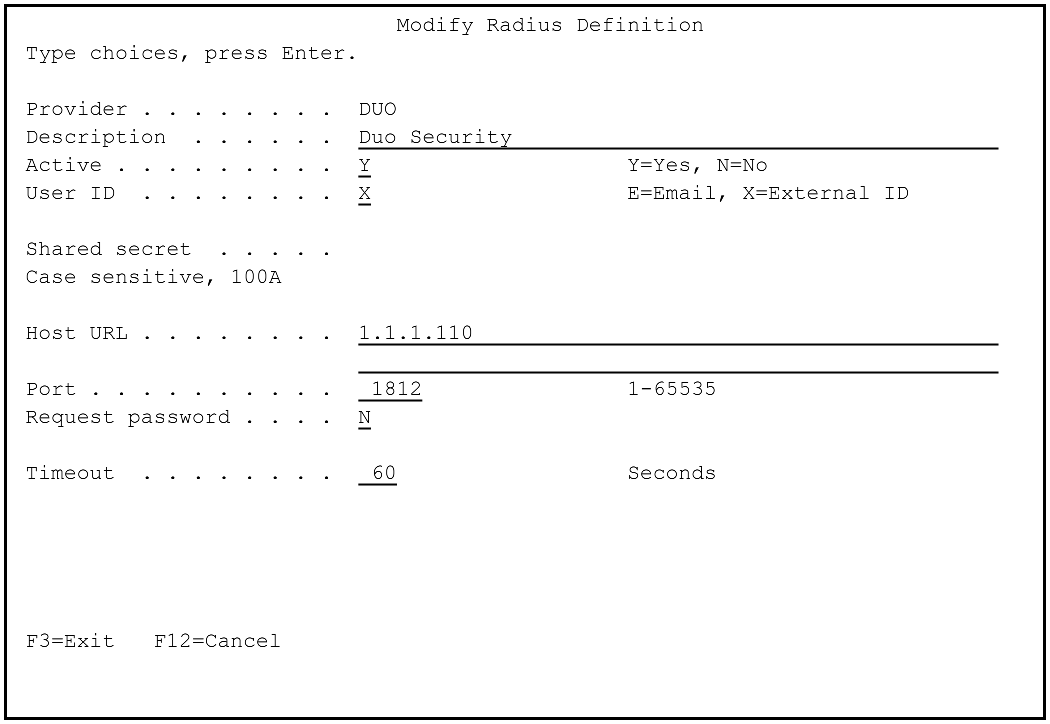
To **set up RADIUS**, select **`43. RADIUS`** from the **Definitions** menu (**`STRMFA > 21`**). The **Work with Radius Definitions** screen appears.



```
                         Work with Radius Definitions

Type options, press Enter.                Subset . . . . . . . __________
 1=Select  3=Copy  4=Delete

Opt Provider  Active  Description
 _  DUO         Y     Duo Security
 _  RSA         N     SecurID















                                                                      Bottom
F3=Exit   F6=Add new
```

For each provider, a line on the screen shows the **`Provider`** name, whether the provider is **`Active`**, and a plain text **`Description`** of the provider.

To **modify a RADIUS definition**, enter **`1`** in the **`Opt`** field for that provider. The **Modify Radius Definition** screen appears:



```
                          Modify Radius Definition
Type choices, press Enter.

Provider . . . . . . . .  DUO
Description  . . . . . .  Duo Security
Active . . . . . . . . .  Y                   Y=Yes, N=No
User ID  . . . . . . . .  X                   E=Email, X=External ID

Shared secret  . . . . .
Case sensitive, 100A

Host URL . . . . . . . .  1.1.1.110


Port . . . . . . . . . .   1812               1-65535
Request password . . . .  N

Timeout  . . . . . . . .   60                 Seconds





F3=Exit   F12=Cancel
```

The information for most of the fields is generated when you set up your organization's RADIUS authentication server. Copy the information for that server to corresponding fields on this screen.

The remaining fields have these values:

Provider

A unique name for the provider.

Description

A free text description of the provider.

Active

Setting this to **Y** makes the service active. Setting it to **N** makes it inactive.

User ID

It is possible to set an External ID for a person in addition to the mandatory email address, as shown in "Modifying a Person" on page 66. Set this field to **X** to use the External ID or **E** to use the email address.

`Timeout`

The maximum number of seconds that the system waits for a response from the provider.

To **copy a RADIUS definition**, enter **`3`** in the **`Opt`** field for that server on the **Work with Radius Definitions** screen. The **Copy Radius Definition** screen appears. Enter the name of the new server in the **`To: Definition`** field of that screen, then press **Enter**.

To **delete a RADIUS definition**, enter **`4`** in the **`Opt`** field for that server on the **Work with Radius Definitions** screen. The **Delete Radius Definition** screen appears, displaying information about the server. Press **Enter** to delete that definition.

To **add a RADIUS definition**, press the **F6** key on the **Work with Radius Definitions** screen. The **Add New Radius Definition** screen appears, with the same fields as the **Modify Radius Definition** screen.

Setting Up Multi-Factor Authentication

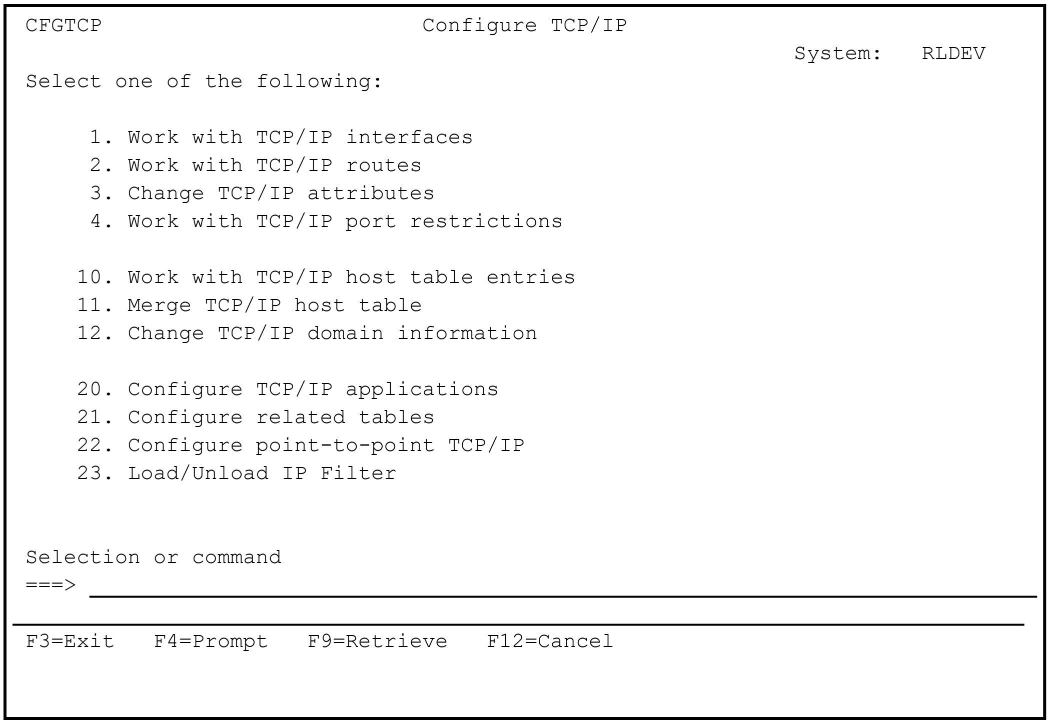
Setting up MFA can include the following steps:

- "Setting Up Email" on the next page
- "Setting Up SMS Text Messaging" on page 43
- "Setting a Local or Centralized Server" on page 44
- "Setting Up the Web Server for MFA" on page 50
- "Enabling MFA Checking for 5250 Sign-ons" on page 51
- "Setting Whether MFA Runs Alongside Other Security Programs" on page 55

Setting Up Email

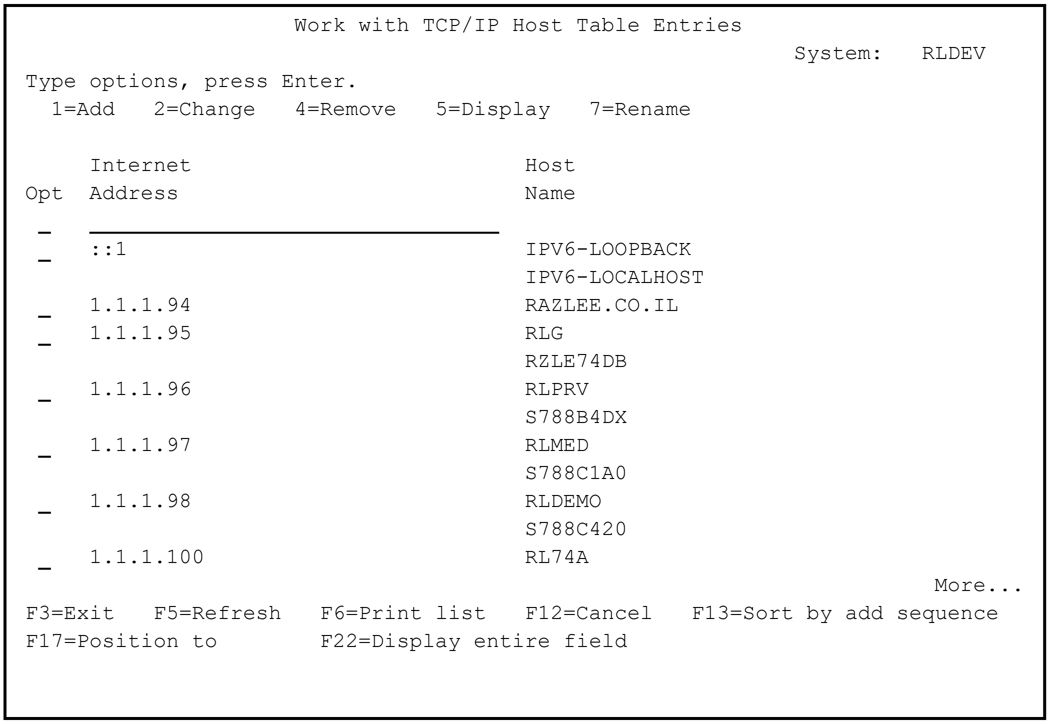
To **specify the email server** that Multi-Factor Authentication uses:

Open the **Configure TCP/IP** screen by entering the ***CFGTCP*** command.



```
CFGTCP                         Configure TCP/IP
                                                            System:   RLDEV
Select one of the following:

     1. Work with TCP/IP interfaces
     2. Work with TCP/IP routes
     3. Change TCP/IP attributes
     4. Work with TCP/IP port restrictions

    10. Work with TCP/IP host table entries
    11. Merge TCP/IP host table
    12. Change TCP/IP domain information

    20. Configure TCP/IP applications
    21. Configure related tables
    22. Configure point-to-point TCP/IP
    23. Load/Unload IP Filter


Selection or command
===> ____________________________________________________________________________

F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
```

Select **`10. Work with TCP/IP host table entries`**. The **Work with TCP/IP Host Table Entries** screen appears.

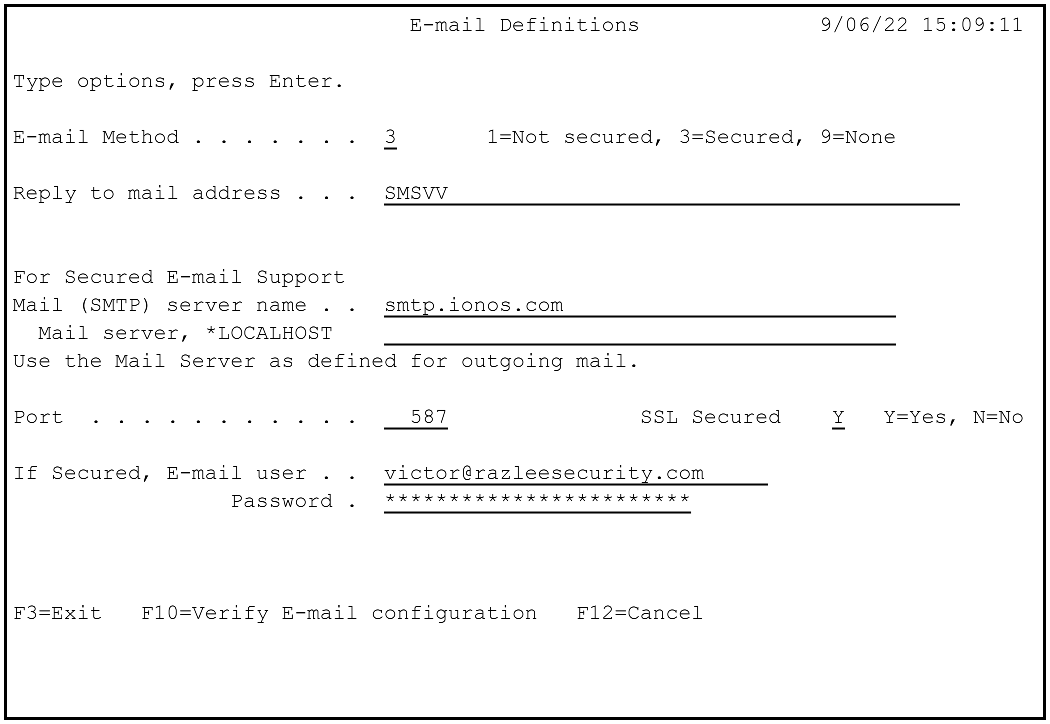


```
                     Work with TCP/IP Host Table Entries
                                                            System:   RLDEV
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display   7=Rename

     Internet                          Host
Opt  Address                           Name

 _   ________________________________
 _   ::1                               IPV6-LOOPBACK
                                       IPV6-LOCALHOST
 _   1.1.1.94                          RAZLEE.CO.IL
 _   1.1.1.95                          RLG
                                       RZLE74DB
 _   1.1.1.96                          RLPRV
                                       S788B4DX
 _   1.1.1.97                          RLMED
                                       S788C1A0
 _   1.1.1.98                          RLDEMO
                                       S788C420
 _   1.1.1.100                         RL74A
                                                                       More...
F3=Exit   F5=Refresh   F6=Print list   F12=Cancel   F13=Sort by add sequence
F17=Position to        F22=Display entire field
```

Locate the **Internet Address** and **Host Name** values for your email server.

NOTE: If the server is not listed, enter **1** in the **Opt** field for the first line on the body of the screen to open the **Add TCP/IP Host Table Entry (ADDTCPHTE) screen**, and enter its **Internet address**, **Host Names** and a free text **Description** there.

Open the Base System **E-mail Definitions** screen (***STRAUD*> 89 > 2**).



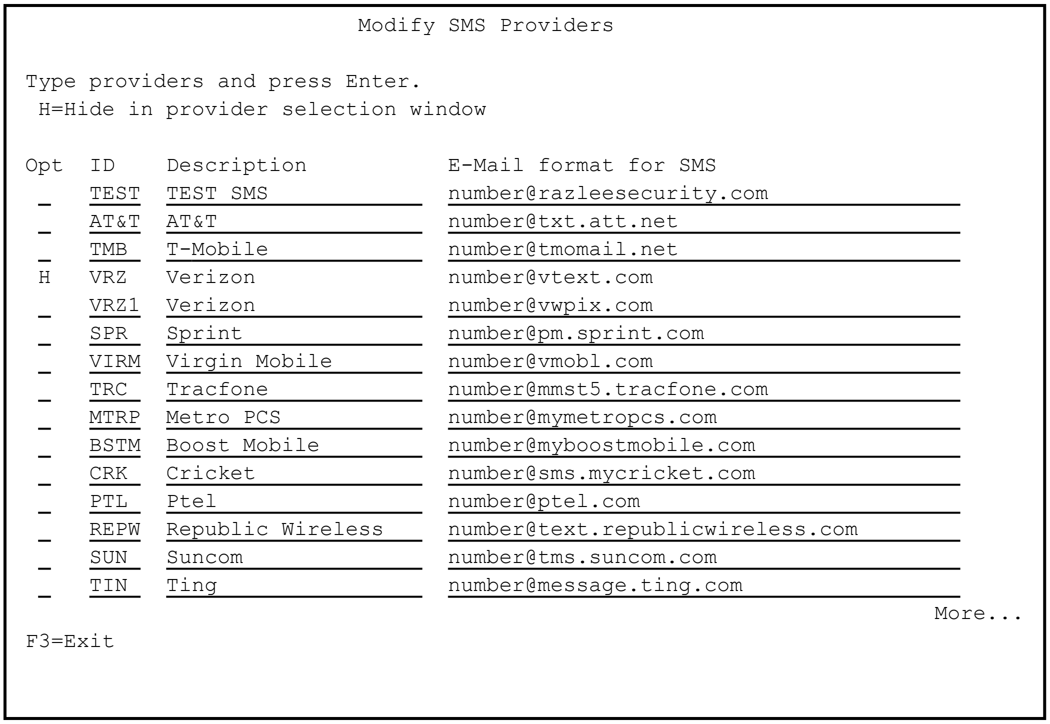
```
                               E-mail Definitions             9/06/22 15:09:11

Type options, press Enter.

E-mail Method . . . . . . .  3       1=Not secured, 3=Secured, 9=None

Reply to mail address . . .  SMSVV


For Secured E-mail Support
Mail (SMTP) server name . .  smtp.ionos.com
  Mail server, *LOCALHOST
Use the Mail Server as defined for outgoing mail.

Port  . . . . . . . . . . .    587              SSL Secured    Y   Y=Yes, N=No

If Secured, E-mail user . .  victor@razleesecurity.com
                 Password .  ************************



F3=Exit   F10=Verify E-mail configuration   F12=Cancel
```

Enter the **`Mail (SMTP) server name`** and other details for your email server.

To **test your email settings**, press the **F10** key from the **Email Definitions** screen. Enter your email address and press **Enter**. If the email settings have been entered correctly, you should receive a test email. If you do not receive the email, check the details in your job log (***DSPJOBLOG*** > **F10** > **F18**).

Setting Up SMS Text Messaging

To **set up SMS text messaging**, open the **Modify SMS Providers** screen (*STRMFA* **> 21 > 5**),



```
                          Modify SMS Providers

Type providers and press Enter.
 H=Hide in provider selection window

Opt  ID    Description           E-Mail format for SMS
 _   TEST  TEST SMS              number@razleesecurity.com
 _   AT&T  AT&T                  number@txt.att.net
 _   TMB   T-Mobile              number@tmomail.net
 H   VRZ   Verizon               number@vtext.com
 _   VRZ1  Verizon               number@vwpix.com
 _   SPR   Sprint                number@pm.sprint.com
 _   VIRM  Virgin Mobile         number@vmobl.com
 _   TRC   Tracfone              number@mmst5.tracfone.com
 _   MTRP  Metro PCS             number@mymetropcs.com
 _   BSTM  Boost Mobile          number@myboostmobile.com
 _   CRK   Cricket               number@sms.mycricket.com
 _   PTL   Ptel                  number@ptel.com
 _   REPW  Republic Wireless     number@text.republicwireless.com
 _   SUN   Suncom                number@tms.suncom.com
 _   TIN   Ting                  number@message.ting.com
                                                                      More...
F3=Exit
```

You can send SMS messages to users of many SMS providers by sending email to a specific address at the provider's domain.

For each provider, one line on the screen shows a unique **`ID`**, a **`Description`** of the provider, and the **`Email format for SMS`**. The email format often is the string **`number@`** followed by the provider's domain.

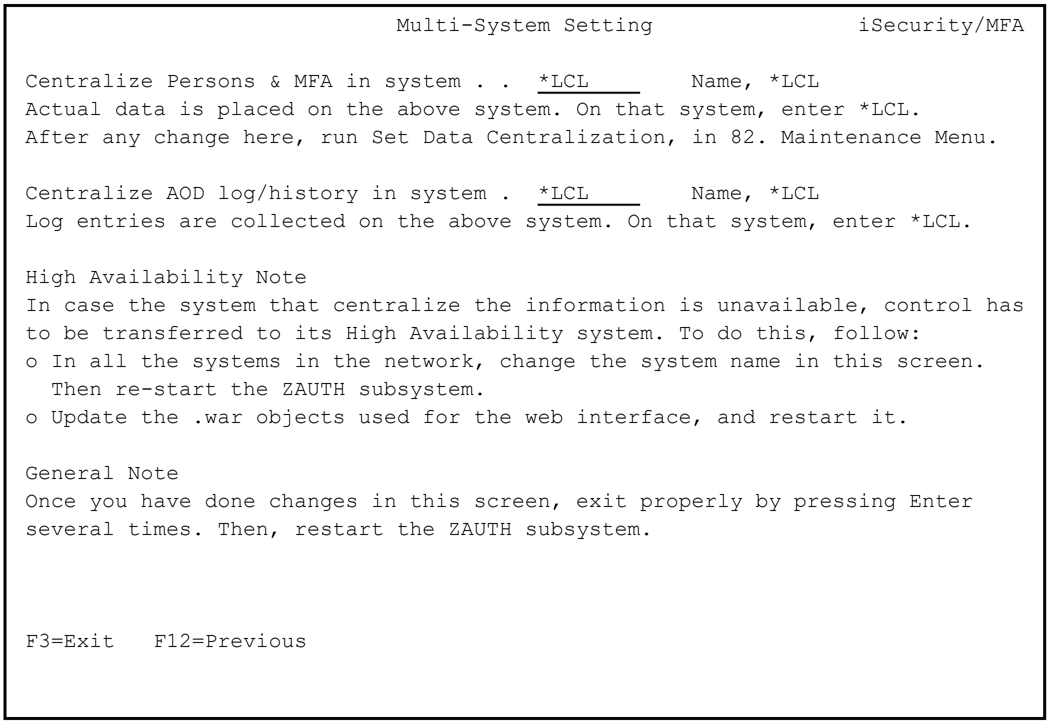
Thus, for example, to send an SMS to a user with the phone number **555-345-6789** from a provider using the domain **text.example.com**, you would send the email to the address **`5553456789@text.example.com`**.

Setting a Local or Centralized Server

You can set Multi-Factor Authentication to work locally, from the IBM i on which you are installing it, or from a different Centralized server.

Running locally

To run **locally**, open the **Multi-System Setting** screen (***STRMFA*> 81 > 95**).

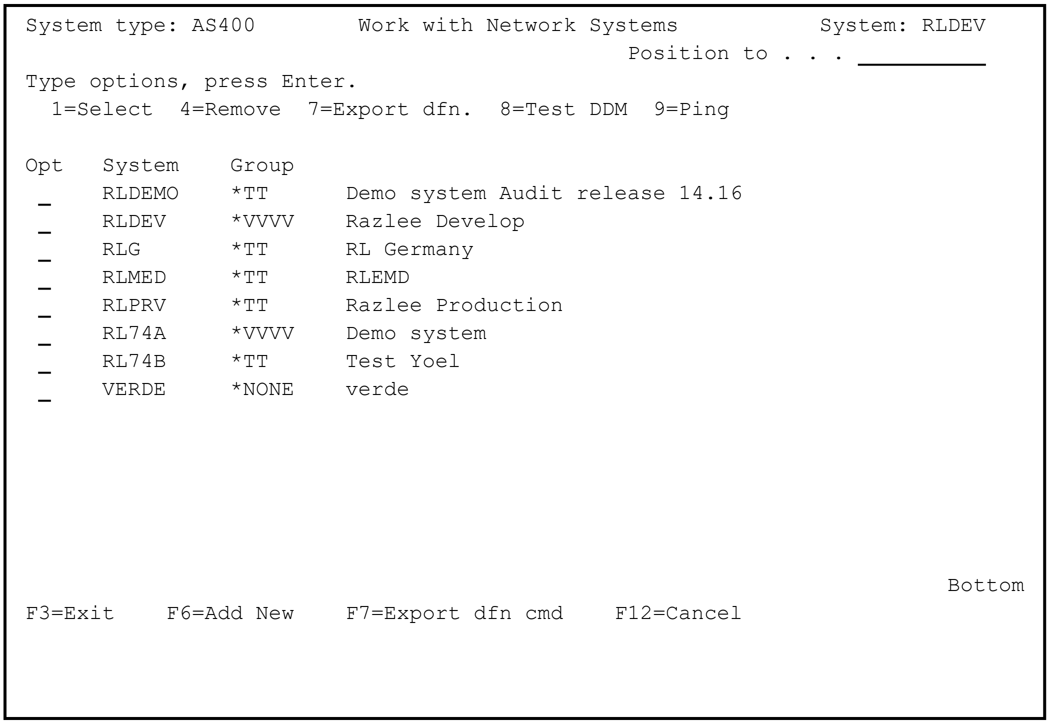


```
                             Multi-System Setting               iSecurity/MFA

Centralize Persons & MFA in system . .  *LCL        Name, *LCL
Actual data is placed on the above system. On that system, enter *LCL.
After any change here, run Set Data Centralization, in 82. Maintenance Menu.

Centralize AOD log/history in system .  *LCL        Name, *LCL
Log entries are collected on the above system. On that system, enter *LCL.

High Availability Note
In case the system that centralize the information is unavailable, control has
to be transferred to its High Availability system. To do this, follow:
o In all the systems in the network, change the system name in this screen.
  Then re-start the ZAUTH subsystem.
o Update the .war objects used for the web interface, and restart it.

General Note
Once you have done changes in this screen, exit properly by pressing Enter
several times. Then, restart the ZAUTH subsystem.



F3=Exit   F12=Previous
```

Set the **`Centralize Persons & MFA in system`** field to **`*LCL`**, then exit the screen and restart the ZAUTH subsystem.

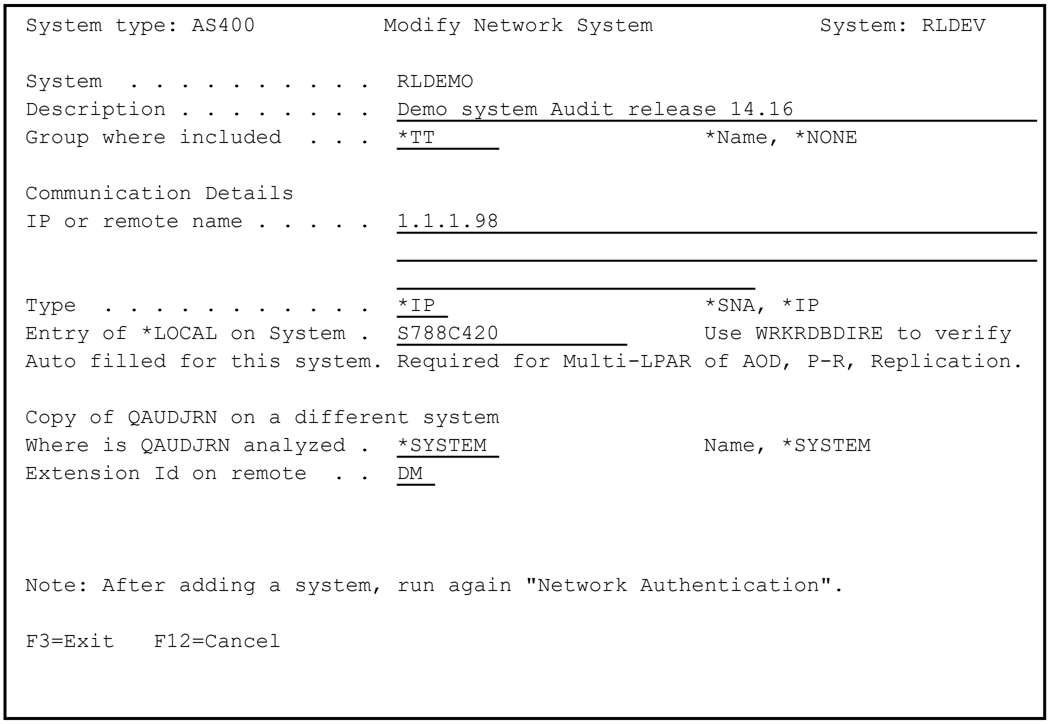
Running from a Centralized Server

To run from a centralized server, open the **Work with Network Systems** screen (***STRAUD*****> 89 > 71**)



```
System type: AS400        Work with Network Systems          System: RLDEV
                                                Position to . . . __________
Type options, press Enter.
  1=Select  4=Remove  7=Export dfn.  8=Test DDM  9=Ping

Opt   System    Group
 _    RLDEMO    *TT      Demo system Audit release 14.16
 _    RLDEV     *VVVV    Razlee Develop
 _    RLG       *TT      RL Germany
 _    RLMED     *TT      RLEMD
 _    RLPRV     *TT      Razlee Production
 _    RL74A     *VVVV    Demo system
 _    RL74B     *TT      Test Yoel
 _    VERDE     *NONE    verde






                                                                      Bottom
F3=Exit    F6=Add New    F7=Export dfn cmd    F12=Cancel
```

If the centralized server is **shown** on the screen, open the **Modify Network System** screen by entering **`1`** in the **`Opt`** field for that server.



```
System type: AS400          Modify Network System            System: RLDEV

System  . . . . . . . . . .  RLDEMO
Description . . . . . . . .  Demo system Audit release 14.16
Group where included  . . .  *TT                     *Name, *NONE

Communication Details
IP or remote name . . . . .  1.1.1.98



Type  . . . . . . . . . . .  *IP                     *SNA, *IP
Entry of *LOCAL on System .  S788C420                Use WRKRDBDIRE to verify
Auto filled for this system. Required for Multi-LPAR of AOD, P-R, Replication.

Copy of QAUDJRN on a different system
Where is QAUDJRN analyzed .  *SYSTEM                 Name, *SYSTEM
Extension Id on remote  . .  DM



Note: After adding a system, run again "Network Authentication".

F3=Exit   F12=Cancel
```

The screen contains these fields:

System

A unique name for the system

Description

A free text description of the system

Group where included

The name of a group of system that includes it. The name must begin with an asterisk ("*****").

IP or Remote Name

The IP address or remote name of the server

Type

***SNA** if the previous field shows a Remote Name; ***!P** if it shows an IP address.

Entry of *LOCAL on System

What ***LOCAL** is set to on that system. Use *WRKRDBDIRE* to verify the value.

Where is QAUDJRN analyzed

Where QAUDJRN is analyzed for that system.

Extension ID on Remote

When QAUDJRN is analysed, the extension added to the string "SMZ4DTA" to name the library containing the analysis. More information can be found at ***STRAUD* > 2 > 41 > 1**.

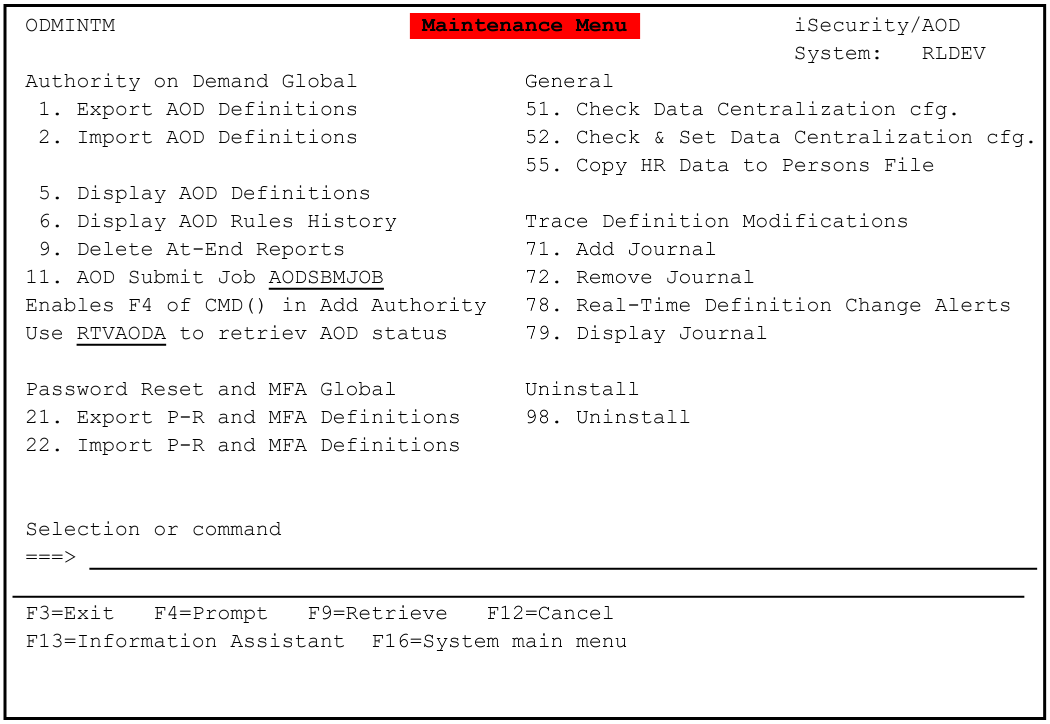
If the Centralized server is **not yet shown** on the screen, open the **Add Network System** screen by pressing the **F6** key from the **Work with Network Systems** screen.

Open the **Multi-System Setting** screen (***STRMFA* > 81 > 95**), shown above.

Set the **Centralize Persons & MFA in system** field to the system name of the centralized server.

Checking the Server Setting

Open the **Maintenance** Menu (*STRMFA* > 82)



```
ODMINTM                      Maintenance Menu               iSecurity/AOD
                                                            System:   RLDEV
Authority on Demand Global              General
 1. Export AOD Definitions              51. Check Data Centralization cfg.
 2. Import AOD Definitions              52. Check & Set Data Centralization cfg.
                                        55. Copy HR Data to Persons File
 5. Display AOD Definitions
 6. Display AOD Rules History           Trace Definition Modifications
 9. Delete At-End Reports               71. Add Journal
11. AOD Submit Job AODSBMJOB            72. Remove Journal
Enables F4 of CMD() in Add Authority    78. Real-Time Definition Change Alerts
Use RTVAODA to retriev AOD status       79. Display Journal

Password Reset and MFA Global           Uninstall
21. Export P-R and MFA Definitions      98. Uninstall
22. Import P-R and MFA Definitions



Selection or command
===> ____________________________________________________________________________

F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
F13=Information Assistant  F16=System main menu
```

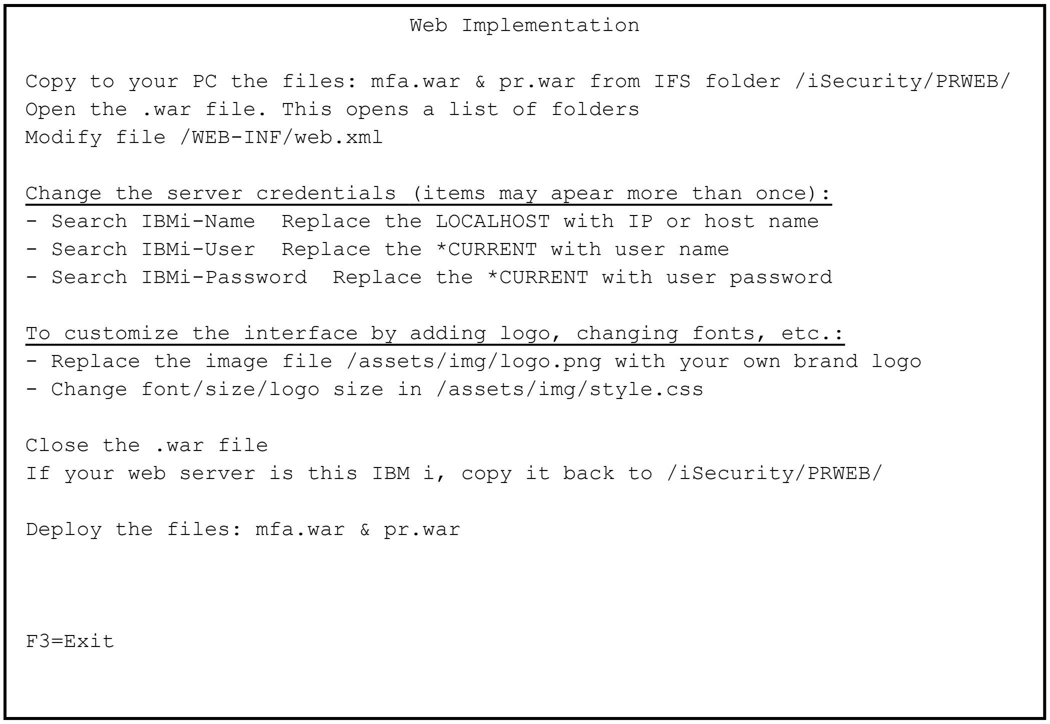
Select **`52. Check & Set Data Centralization cfg.`**
The bottom line of the screen displays "**`Person/MFA files are properly set`**".

Setting Up the Web Server for MFA

Install the TOMCAT 10 web server or the integrated Application Server on the IBM i.

Add the MFA application to the WEBAPPS directory within the TOMCAT or Application server.

Open the Web Implementation and Customization screen (*STRMFA*> **81 > 59**)



```
                               Web Implementation

Copy to your PC the files: mfa.war & pr.war from IFS folder /iSecurity/PRWEB/
Open the .war file. This opens a list of folders
Modify file /WEB-INF/web.xml

Change the server credentials (items may apear more than once):
- Search IBMi-Name  Replace the LOCALHOST with IP or host name
- Search IBMi-User  Replace the *CURRENT with user name
- Search IBMi-Password  Replace the *CURRENT with user password

To customize the interface by adding logo, changing fonts, etc.:
- Replace the image file /assets/img/logo.png with your own brand logo
- Change font/size/logo size in /assets/img/style.css

Close the .war file
If your web server is this IBM i, copy it back to /iSecurity/PRWEB/

Deploy the files: mfa.war & pr.war



F3=Exit
```

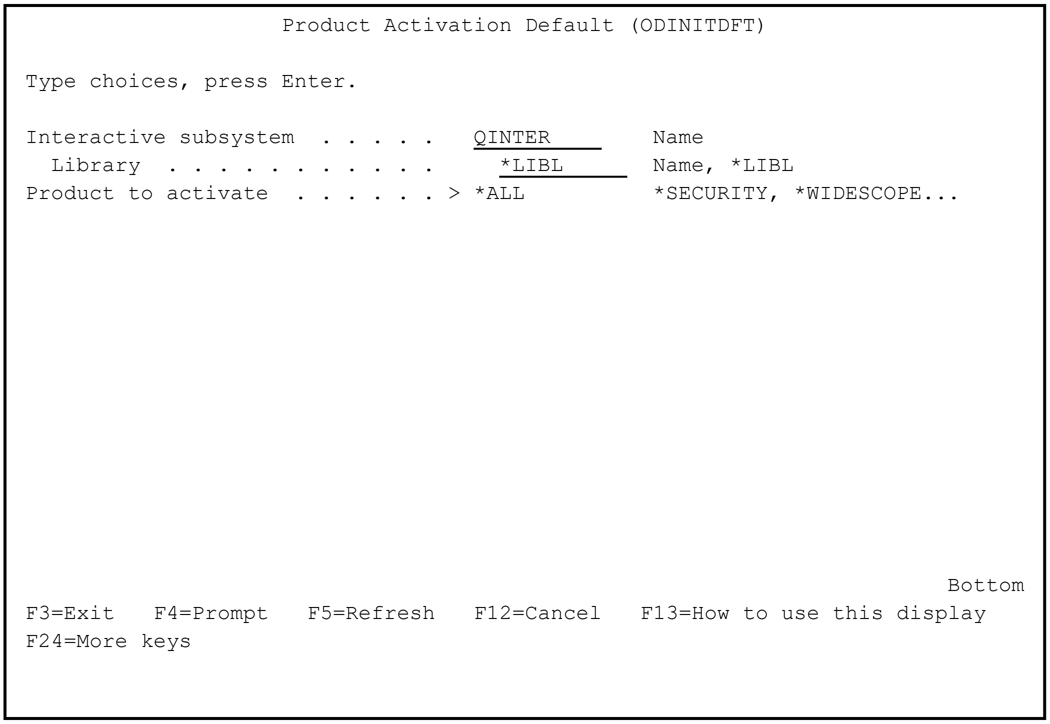
Follow the instructions shown on the screen.

Enabling MFA Checking for 5250 Sign-ons

MFA must be enabled both for the subsystems for which it is needed and for the users requiring authentication

Enabling MFA by Subsystem

Open the **Product Activation Default (ODINITDFT)** screen (***STRMFA*** **> 25 > 11**).



```
                    Product Activation Default (ODINITDFT)

Type choices, press Enter.

Interactive subsystem  . . . . .   QINTER        Name
  Library  . . . . . . . . . . .     *LIBL       Name, *LIBL
Product to activate  . . . . . . > *ALL          *SECURITY, *WIDESCOPE...

















                                                                      Bottom
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys
```

The screen includes default values for the **`Interactive subsystem`** and **`Library`**, and the **`Product to activate`** fields.

Press **Enter** to accept the values and enable MFA.

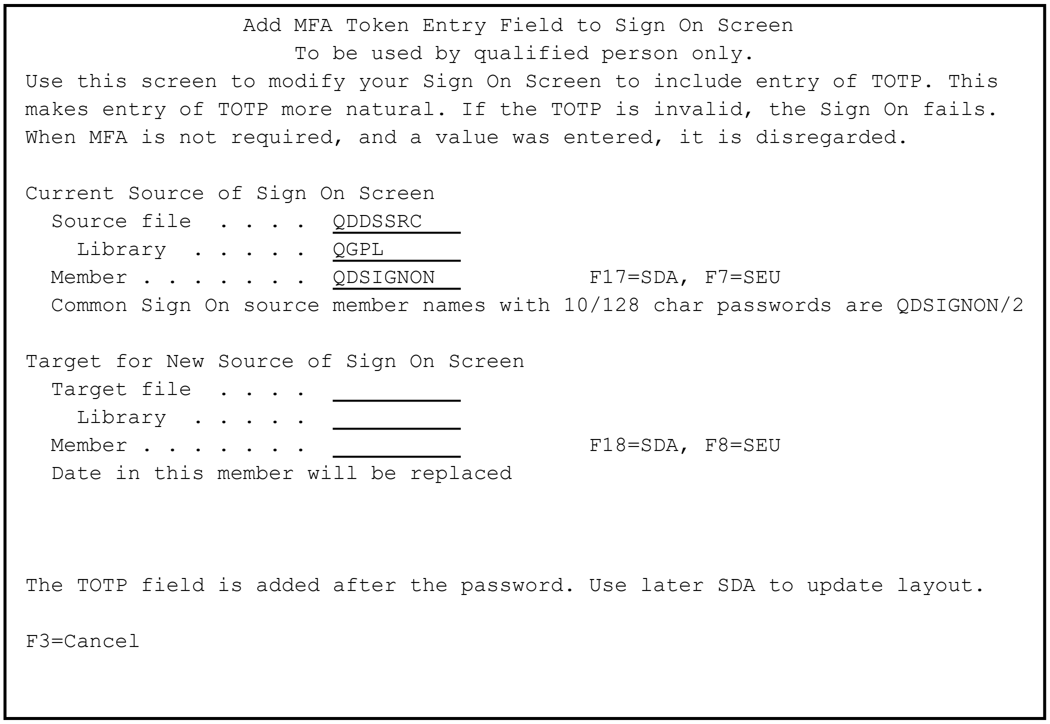
Enabling MFA by User

To enable MFA for users, add the ***SMZO/GETMFA*** command as the initial program of each of those users.

Adding the MFA Token to the 5250 Sign-On Screen

The **MFA token** field on the 5250 sign-on screen enables secure single-step authentication, in which the user enters the username, password, and MFA token at the same time.

To add the field. open the Add MFA Token Entry Field to Sign On Screen screen (*STRMFA*> 25 > 9).



```
                 Add MFA Token Entry Field to Sign On Screen
                     To be used by qualified person only.
Use this screen to modify your Sign On Screen to include entry of TOTP. This
makes entry of TOTP more natural. If the TOTP is invalid, the Sign On fails.
When MFA is not required, and a value was entered, it is disregarded.

Current Source of Sign On Screen
  Source file  . . . .  QDDSSRC
    Library  . . . . .  QGPL
  Member . . . . . . .  QDSIGNON            F17=SDA, F7=SEU
  Common Sign On source member names with 10/128 char passwords are QDSIGNON/2

Target for New Source of Sign On Screen
  Target file  . . . .  __________
    Library  . . . . .  __________
  Member . . . . . . .  __________          F18=SDA, F8=SEU
  Date in this member will be replaced



The TOTP field is added after the password. Use later SDA to update layout.

F3=Cancel
```

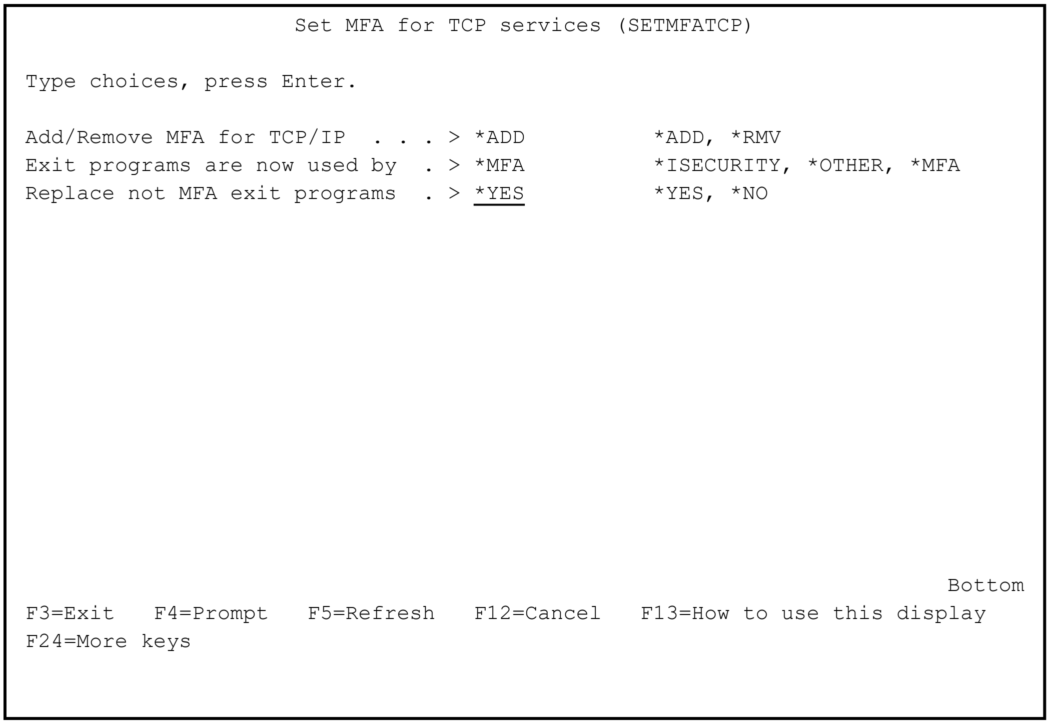
The screen creates a new member file for the sign on screen or replaces an existing one. Enter the new **Target file**, **Library**, and **Member** values.

Setting Whether MFA Runs Alongside Other Security Programs

MFA can run in addition to existing exit programs. If this is enabled, the existing exit program handles the connection request. If the program accepts the connection, MFA then prompts the user to confirm the connection or enter an MFA token.

Running MFA on Its Own

Open the **Set MFA for TCP services (SETMFATCP)** screen with options set for stand-alone operation (***STRMFA*> 25 > 21**).

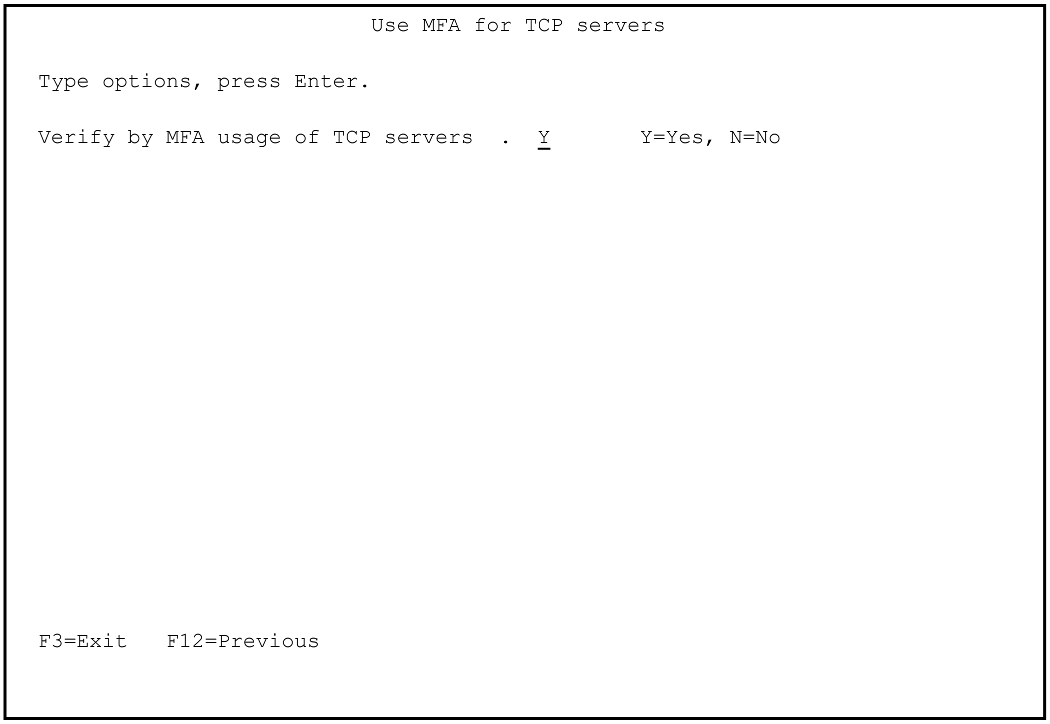


```
                     Set MFA for TCP services (SETMFATCP)

Type choices, press Enter.

Add/Remove MFA for TCP/IP  . . . > *ADD          *ADD, *RMV
Exit programs are now used by  . > *MFA          *ISECURITY, *OTHER, *MFA
Replace not MFA exit programs  . > *YES          *YES, *NO















                                                                       Bottom
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys
```

Press **Enter** to accept the options.

Running MFA alongside iSecurity/Firewall

Open the iSecurity/Firewall U**se MFA for TCP Servers** screen (***STRFW*** **> 81 > 41**).

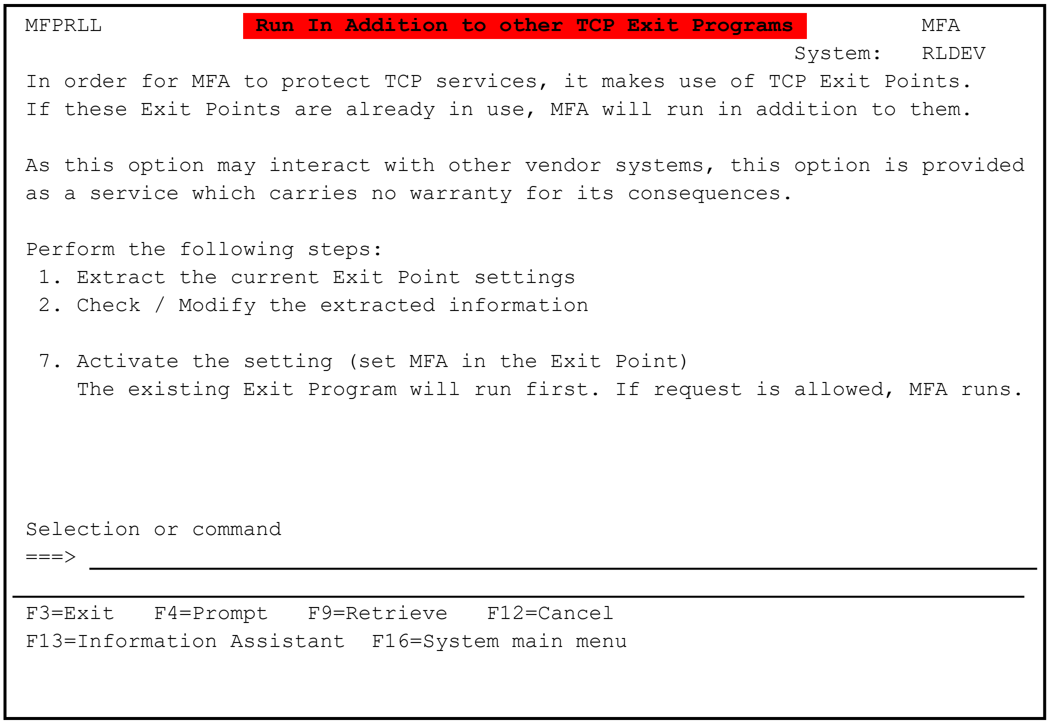


```
                             Use MFA for TCP servers

 Type options, press Enter.

 Verify by MFA usage of TCP servers  .  Y       Y=Yes, N=No
















 F3=Exit   F12=Previous
```

Set the **`Verify by MFA usage of TCP servers`** field to **`Y`**.

Running MFA in Addition to Other Programs

Open the **Run In Addition to other TCP Exit Programs screen** (***STRMFA* > 25 > 23**).



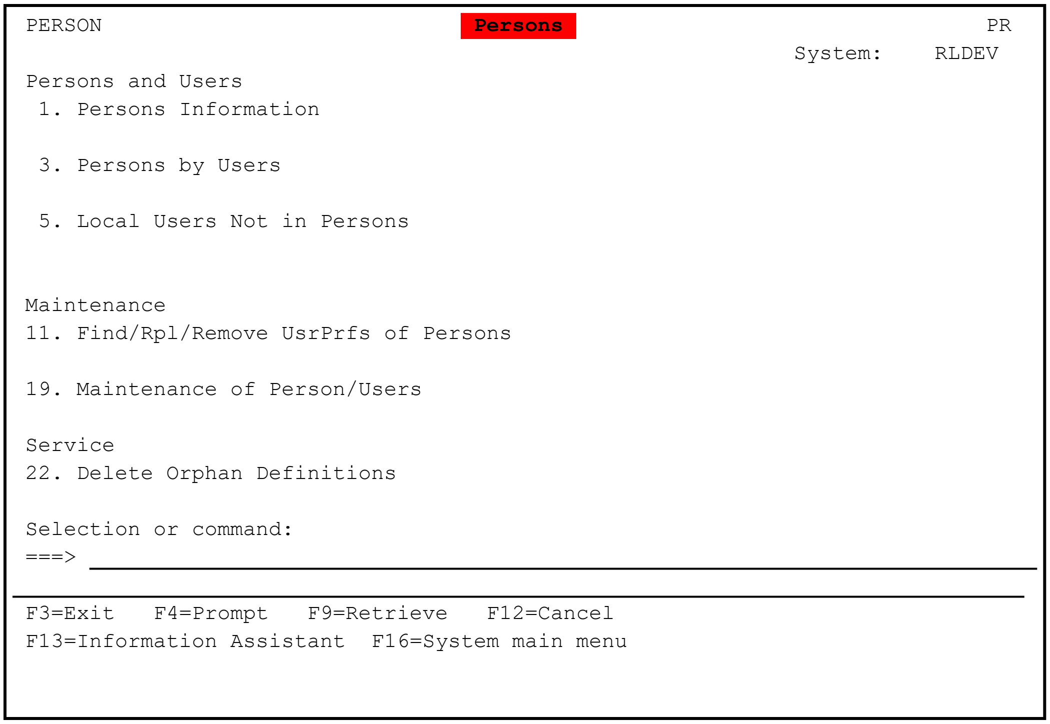
```
MFPRLL              Run In Addition to other TCP Exit Programs           MFA
                                                            System:   RLDEV
In order for MFA to protect TCP services, it makes use of TCP Exit Points.
If these Exit Points are already in use, MFA will run in addition to them.

As this option may interact with other vendor systems, this option is provided
as a service which carries no warranty for its consequences.

Perform the following steps:
 1. Extract the current Exit Point settings
 2. Check / Modify the extracted information

 7. Activate the setting (set MFA in the Exit Point)
    The existing Exit Program will run first. If request is allowed, MFA runs.




Selection or command
===> ___________________________________________________________________________

F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
F13=Information Assistant  F16=System main menu
```

Follow the numbered steps on that screen.

Defining Persons

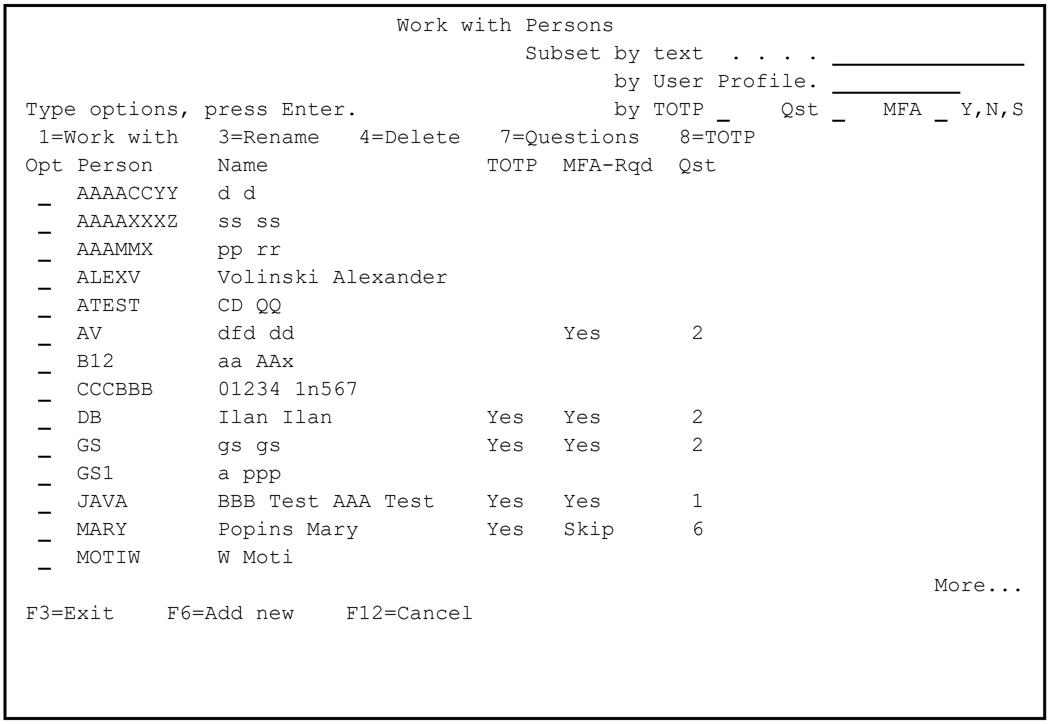
Multi-Factor Authentication, as well as iSecurity Authority on Demand and Password Reset, manages user information in terms of **Persons**. Since multiple users on multiple system might all be the same person, MFA groups them together. Thus, for example, if a person has been successfully authenticated as a particular user on one system, attempts to access related systems by that same person using other user names in a allotted period of time will also be accepted without needing to be authenticated again.

To **define and work with persons**, select **`1. Persons`** from the **Multi Factor Authentication (MFA)** main menu. The **Persons** menu appears.



```
PERSON                          Persons                               PR
                                                        System:     RLDEV
Persons and Users
 1. Persons Information

 3. Persons by Users

 5. Local Users Not in Persons


Maintenance
11. Find/Rpl/Remove UsrPrfs of Persons

19. Maintenance of Person/Users

Service
22. Delete Orphan Definitions

Selection or command:
===> ____________________________________________________________________

F3=Exit    F4=Prompt    F9=Retrieve    F12=Cancel
F13=Information Assistant   F16=System main menu
```

To **display and enter information concerning each user**, select **`1. Person Information`** from the **Persons** menu (*STRMFA* **>** **`1`**). The **Work with Persons** screen appears:



```
                              Work with Persons
                                        Subset by text  . . . . ______________
                                               by User Profile. __________
Type options, press Enter.                     by TOTP _    Qst _    MFA _ Y,N,S
 1=Work with   3=Rename   4=Delete   7=Questions   8=TOTP
Opt Person     Name                 TOTP  MFA-Rqd  Qst
 _  AAAACCYY   d d
 _  AAAAXXXZ   ss ss
 _  AAAMMX     pp rr
 _  ALEXV      Volinski Alexander
 _  ATEST      CD QQ
 _  AV         dfd dd                     Yes       2
 _  B12        aa AAx
 _  CCCBBB     01234 1n567
 _  DB         Ilan Ilan            Yes   Yes       2
 _  GS         gs gs                Yes   Yes       2
 _  GS1        a ppp
 _  JAVA       BBB Test AAA Test    Yes   Yes       1
 _  MARY       Popins Mary          Yes   Skip      6
 _  MOTIW      W Moti
                                                                      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.

TOTP

If set to **Yes**, a Temporary One-Time Password is defined for this person.

MFA-Rqd

Whether MFA is required for this person.

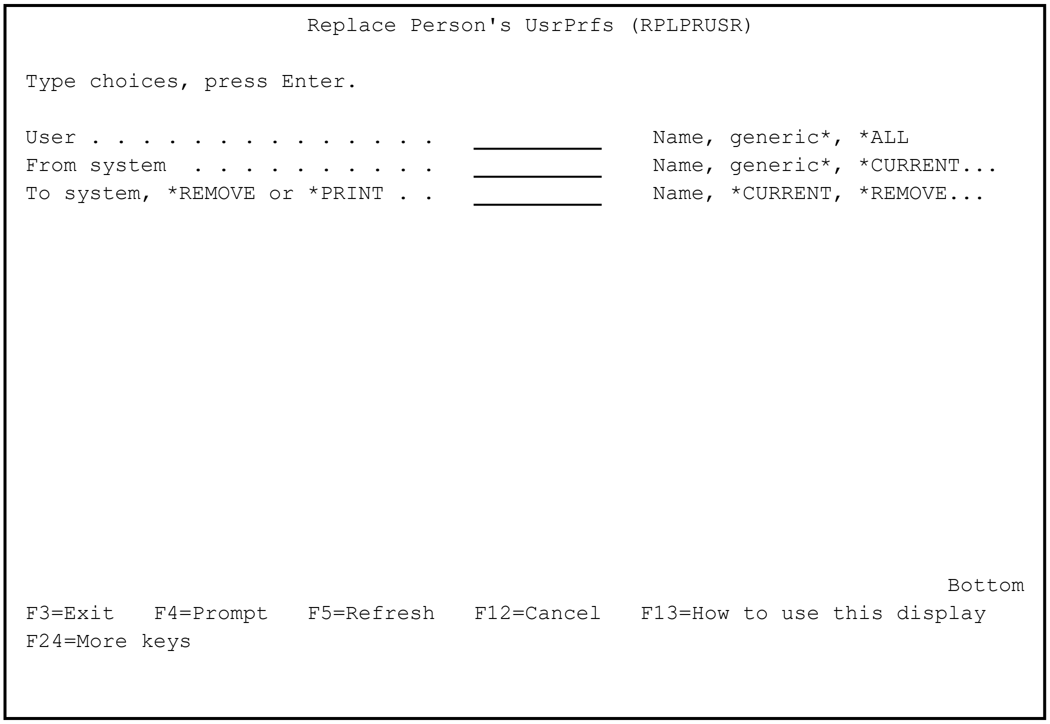
Qst

The number of personal questions and answers defined for this person.

To **add a new person**, press the **F6** key from the **Work with Persons** screen (*STRMFA* **> 1 > 1**). The **Add New Person** screen appears, as shown in "Adding a New Person" on page 63.

To **modify a person**, enter **`1`** in the **`Opt`** field for the person on the **Work with Persons** screen (*STRMFA* **>** **`1 > 1`**). The **Modify Person** screen appears, as shown in "Modifying a Person" on page 66.

To **find, remove, or replace a Person's user profiles**, select **`11. Find/Rpl/Remove UsrPrfs of Persons`** from the **Persons** menu (*STRMFA* **>** **`1`**). The **Replace Person's UsrPrfs (RPLPRUSR)** screen appears.



```
                      Replace Person's UsrPrfs (RPLPRUSR)

Type choices, press Enter.

User . . . . . . . . . . . . . .   __________    Name, generic*, *ALL
From system  . . . . . . . . . .   __________    Name, generic*, *CURRENT...
To system, *REMOVE or *PRINT . .   __________    Name, *CURRENT, *REMOVE...

                                                                       Bottom
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys
```

This command could be useful in duplicating a person's user profiles from one system to another.

The body of the screen has three fields:

`User`

The name of the person or persons. It can be a name, a generic* name, or *ALL.

`From system`

The system containing the original user profiles. It can be a name, a generic* name, *CURRENT, or *ALL.

To system, *REMOVE or *PRINT

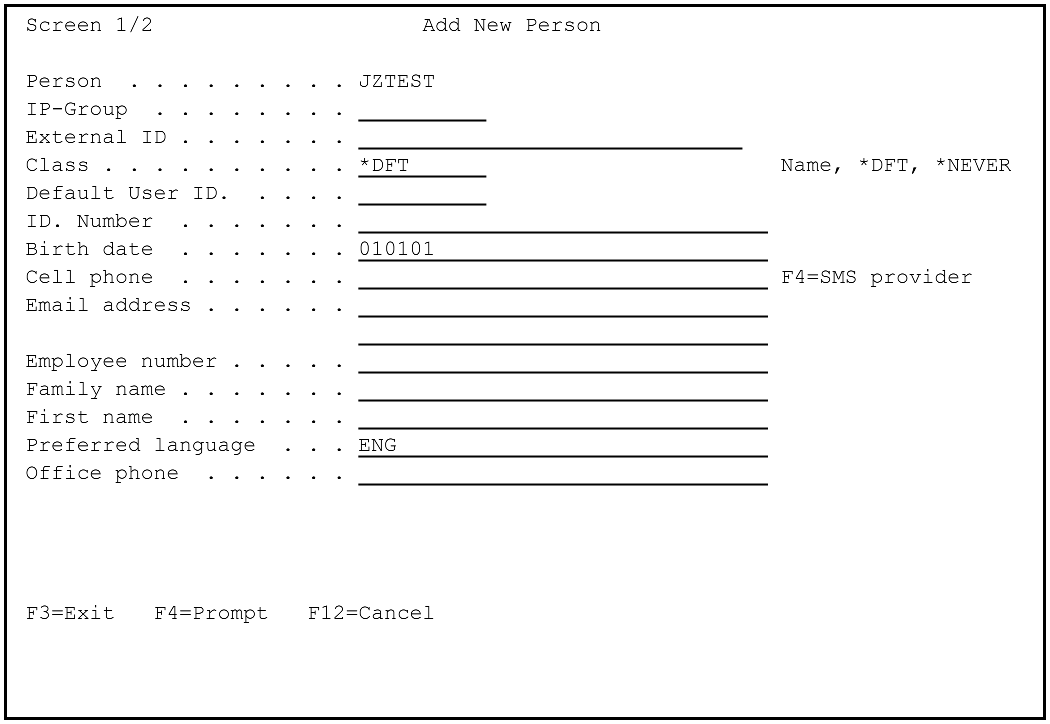
If you are **replacing** user profiles, the name of the system to which they should be copied from the system in the previous field.

To **remove** user profiles from the system in the previous field, the string *REMOVE.

To **print a listing** of user profiles from the system in the previous field.

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 59). The **Add New Person** screen appears.



```
Screen 1/2                     Add New Person

Person  . . . . . . . . . . JZTEST
IP-Group  . . . . . . . . . __________
External ID . . . . . . . . ______________________________
Class . . . . . . . . . . . *DFT______                     Name, *DFT, *NEVER
Default User ID.  . . . . . __________
ID. Number  . . . . . . . . ________________________________
Birth date  . . . . . . . . 010101__________________________
Cell phone  . . . . . . . . ________________________________ F4=SMS provider
Email address . . . . . . . ________________________________
                            ________________________________
Employee number . . . . . . ________________________________
Family name . . . . . . . . ________________________________
First name  . . . . . . . . ________________________________
Preferred language  . . . . ENG_____________________________
Office phone  . . . . . . . ________________________________




F3=Exit   F4=Prompt   F12=Cancel
```

The body of the screen contains these fields:

`Person`

A unique identifier for the Person.

`IP-Group`

The name of an IP Group of which the person is a member, as described in "Defining IP Groups" on page 86

`External ID`

A different unique identifier for the Person, if one has been established.

`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.

`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.

`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.

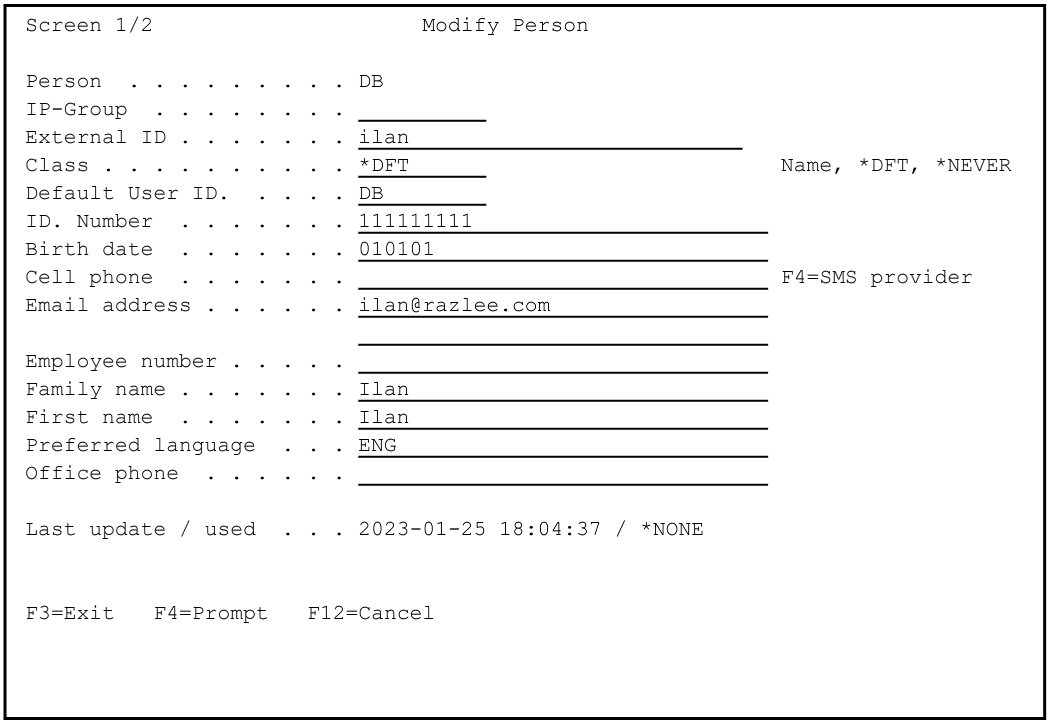
`Office phone`

The office phone number of the Person

Press **Enter** to complete the entry. The **Work with Users of a Person** screen appears, as shown in "Setting Up Users for a Person" on page 78

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 59. The **Modify Person** screen appears:



```
Screen 1/2                    Modify Person

Person  . . . . . . . . . DB
IP-Group  . . . . . . . . __________
External ID . . . . . . . ilan
Class . . . . . . . . . . *DFT                            Name, *DFT, *NEVER
Default User ID.  . . . . DB
ID. Number  . . . . . . . 111111111
Birth date  . . . . . . . 010101
Cell phone  . . . . . . . ________________________________ F4=SMS provider
Email address . . . . . . ilan@razlee.com
                          ________________________________
Employee number . . . . . ________________________________
Family name . . . . . . . Ilan
First name  . . . . . . . Ilan
Preferred language  . . . ENG
Office phone  . . . . . . ________________________________

Last update / used  . . . 2023-01-25 18:04:37 / *NONE


F3=Exit   F4=Prompt   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=Prompt key.

Office phone

The office phone number of the Person

Default user ID

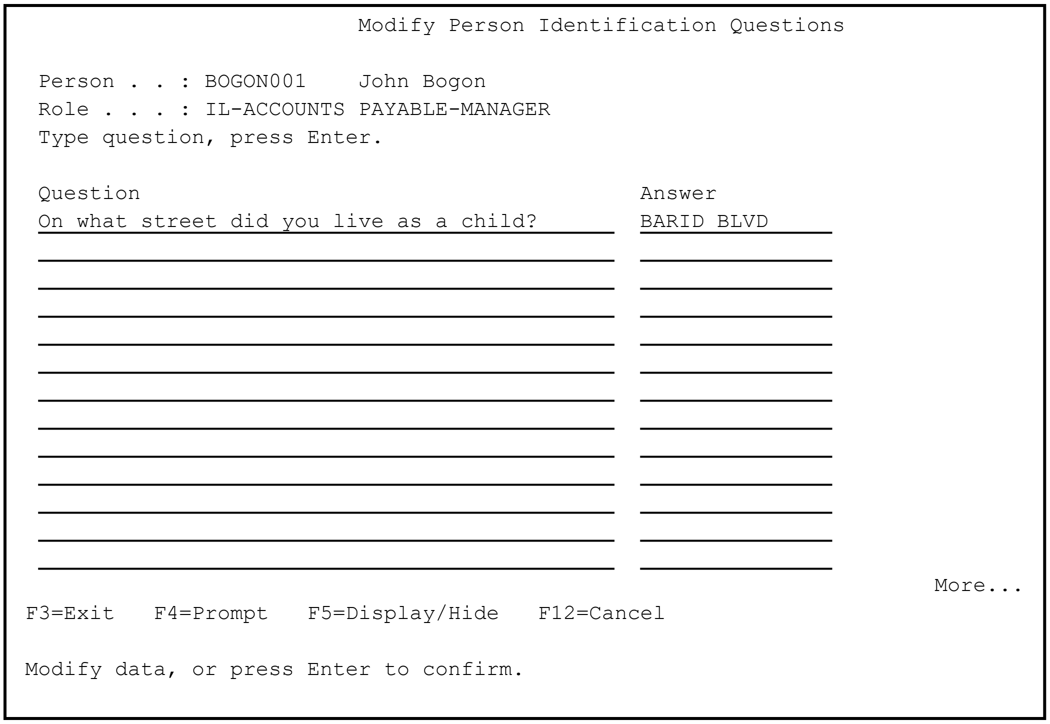
The preferred User ID of the Person on the IBM i. It is used to create the User Profiles for the Person.

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.

Modifying Person Identification Questions

To **set or modify a Person's identification questions and answers**, enter **`7`** in the **`Opt`** field for that Person on the **Work with Persons** screen (*STRMFA* **`> 1 > 1`**). The **Modify Person Identification Questions** screen appears.



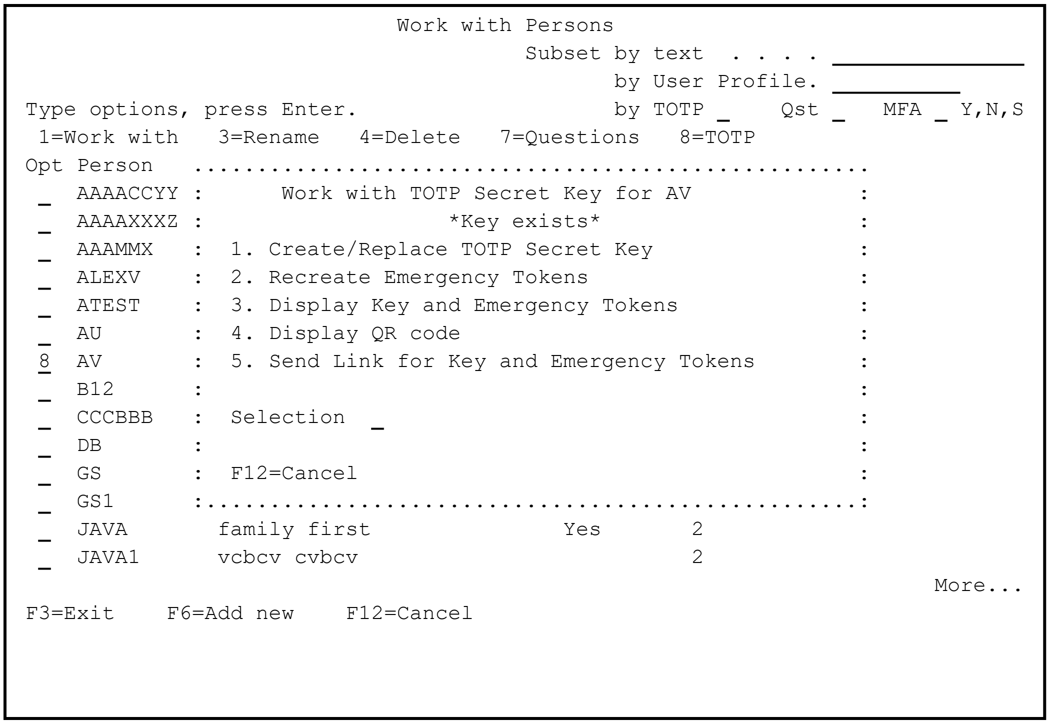
```
                           Modify Person Identification Questions

  Person . . : BOGON001    John Bogon
  Role . . . : IL-ACCOUNTS PAYABLE-MANAGER
  Type question, press Enter.

  Question                                       Answer
  On what street did you live as a child?______  BARID BLVD_____
  _____________________________________________  _______________
  _____________________________________________  _______________
  _____________________________________________  _______________
  _____________________________________________  _______________
  _____________________________________________  _______________
  _____________________________________________  _______________
  _____________________________________________  _______________
  _____________________________________________  _______________
  _____________________________________________  _______________
  _____________________________________________  _______________
  _____________________________________________  _______________
  _____________________________________________  _______________
                                                                        More...
 F3=Exit   F4=Prompt   F5=Display/Hide   F12=Cancel

 Modify data, or press Enter to confirm.
```

The body of the screen contains lines in which you can enter multiple questions, used to identify a Person, and their corresponding answers. The questions can be up to 45 characters long. The answers can be up to 15 characters long.

By default, the answers are hidden. To reveal or hide them press the **F5** key.

Setting Up TOTP for a Person

To **set up Temporary One Time Passwords (TOTP) for a person**, enter **8** in the **`Opt`** field for that person on the **Work with Persons** screen (*STRMFA* **> `1` > `1`**).



```
                              Work with Persons
                                        Subset by text  . . . . _______________
                                               by User Profile. __________
Type options, press Enter.                     by TOTP _    Qst _    MFA _ Y,N,S
 1=Work with   3=Rename   4=Delete   7=Questions   8=TOTP
Opt Person   ..................................................
 _  AAAACCYY :      Work with TOTP Secret Key for AV            :
 _  AAAAXXXZ :                   *Key exists*                   :
 _  AAAMMX   :  1. Create/Replace TOTP Secret Key               :
 _  ALEXV    :  2. Recreate Emergency Tokens                    :
 _  ATEST    :  3. Display Key and Emergency Tokens             :
 _  AU       :  4. Display QR code                              :
 8  AV       :  5. Send Link for Key and Emergency Tokens       :
 _  B12      :                                                  :
 _  CCCBBB   :  Selection  _                                    :
 _  DB       :                                                  :
 _  GS       :  F12=Cancel                                      :
 _  GS1      :..................................................:
 _  JAVA       family first               Yes       2
 _  JAVA1      vcbcv cvbcv                          2
                                                                    More...
F3=Exit    F6=Add new    F12=Cancel
```

To **create or replace a TOTP secret key** for the Person, enter **1** in the **`Selection`** field within the window, The **Create New TOTP Secret Key** window appears, as shown in "Creating or Replacing a TOTP Secret Key" on page 71.

To **recreate the emergency tokens** for the Person, enter **2** in the **`Selection`** field within the window, The **Recreate Emergency Tokens** window appears, as shown in "Recreating Emergency Tokens for TOTP" on page 76.

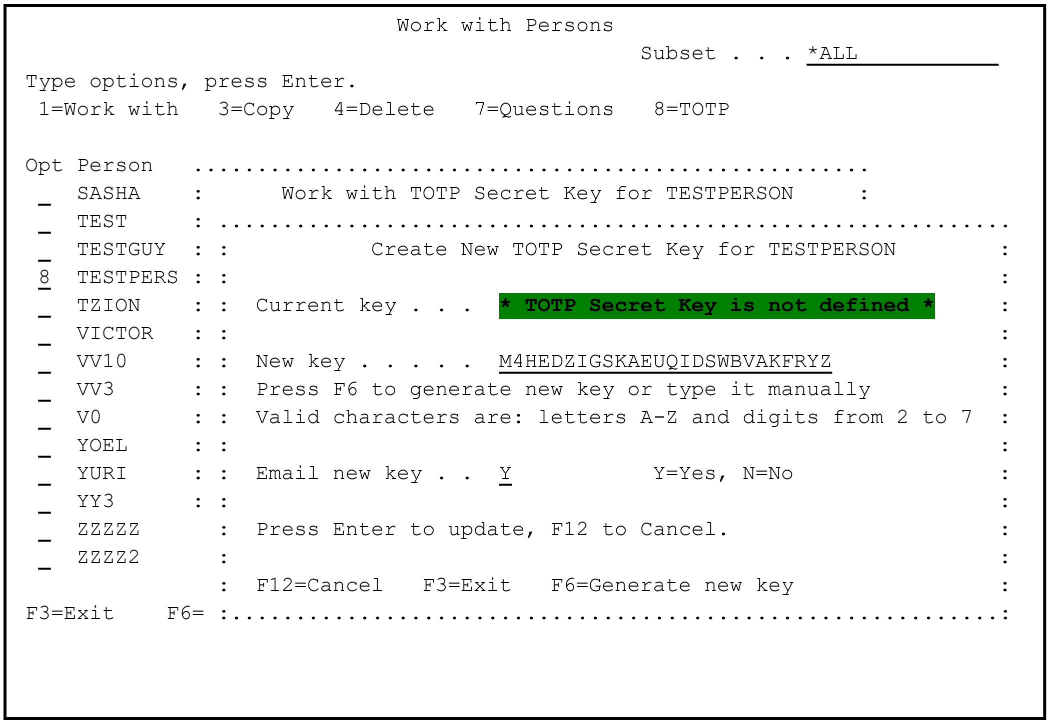
To **display the TOTP key and emergency tokens** for the Person, enter **3** in the **`Selection`** field within the window. The **TOTP Keys** window appears, as shown in "Displaying a TOTP Key and Emergency Tokens" on page 77.

To **display a QR code** that can be used with authentication apps, enter **4** in the **`Selection`** field within the window. A tab opens within the local browser, containing the QR code.

To **email the TOTP key and emergency tokens** to the Person, enter **5** in the **`Selection`** field within the window. A window opens,, showing the email address set for the user. To email the key and tokens to the user, press **Enter**. To cancel sending the email, press **F12**.

Creating or Replacing a TOTP Secret Key

To **create or replace a TOTP secret key** for the Person, enter **`1`** in the **`Selection`** field within the **Work with TOTP Secret Key** window (*STRMFA* **> `1` > `1`, `1`**), The **Create New TOTP Secret Key** window appears:



```
                              Work with Persons
                                                   Subset . . . *ALL
Type options, press Enter.
 1=Work with   3=Copy   4=Delete   7=Questions   8=TOTP

Opt Person    ....................................................
 _  SASHA    :      Work with TOTP Secret Key for TESTPERSON     :
 _  TEST     : ..............................................................
 _  TESTGUY  : :           Create New TOTP Secret Key for TESTPERSON        :
 8  TESTPERS : :                                                            :
 _  TZION    : :  Current key . . .  * TOTP Secret Key is not defined *     :
 _  VICTOR   : :                                                            :
 _  VV10     : :  New key . . . . .  M4HEDZIGSKAEUQIDSWBVAKFRYZ             :
 _  VV3      : :  Press F6 to generate new key or type it manually          :
 _  V0       : :  Valid characters are: letters A-Z and digits from 2 to 7  :
 _  YOEL     : :                                                            :
 _  YURI     : :  Email new key . .  Y           Y=Yes, N=No                :
 _  YY3      : :                                                            :
 _  ZZZZZ      :  Press Enter to update, F12 to Cancel.                     :
 _  ZZZZ2      :                                                            :
               :  F12=Cancel   F3=Exit   F6=Generate new key                :
F3=Exit    F6= :............................................................:
```

If the Person currently has a secret key, it appears in the **`Current key`** field.

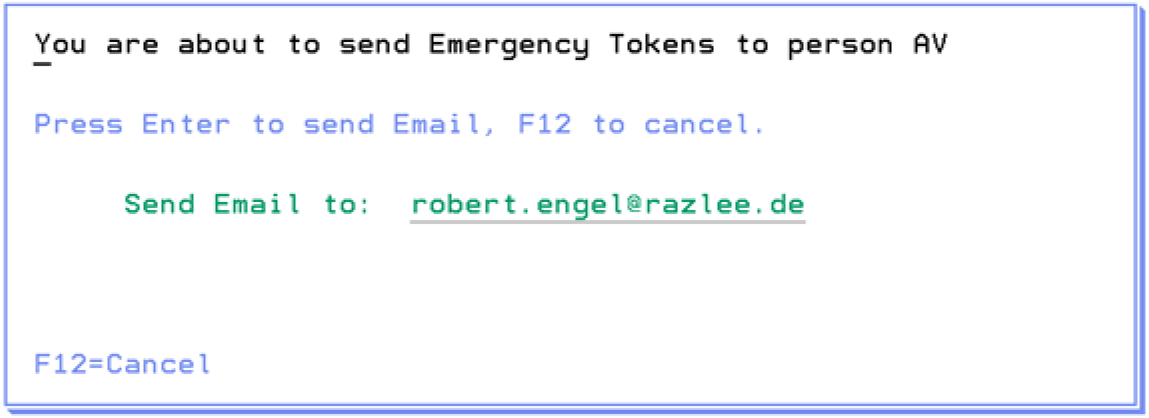
To **cancel the entry** and continue to use the current key, press **F12**.

To **automatically generate a new valid key**, press the **F6** key. The new key appears in the **`New key`** field.

You can also **enter a new key manually** in the **`New key`** field. It must be 32 characters long, and may only contain capital letters and digits from **2** to **7**.

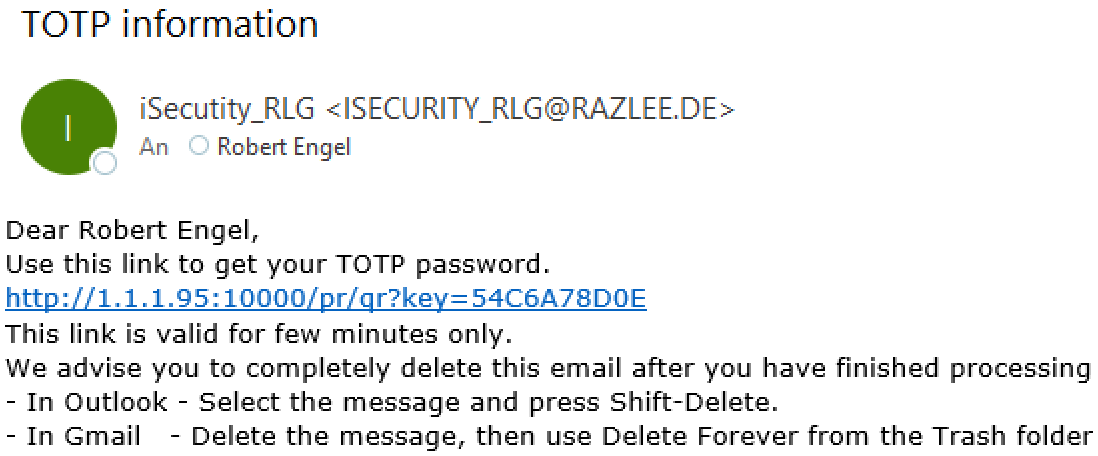
To **email the new key** to the email address set for the Person, set the **`Email new key`** field to Y.

A window appears, confirming your email address:



```
You are about to send Emergency Tokens to person AV

Press Enter to send Email, F12 to cancel.

     Send Email to:   robert.engel@razlee.de



F12=Cancel
```

A new email is sent with the link to the TOTP password:

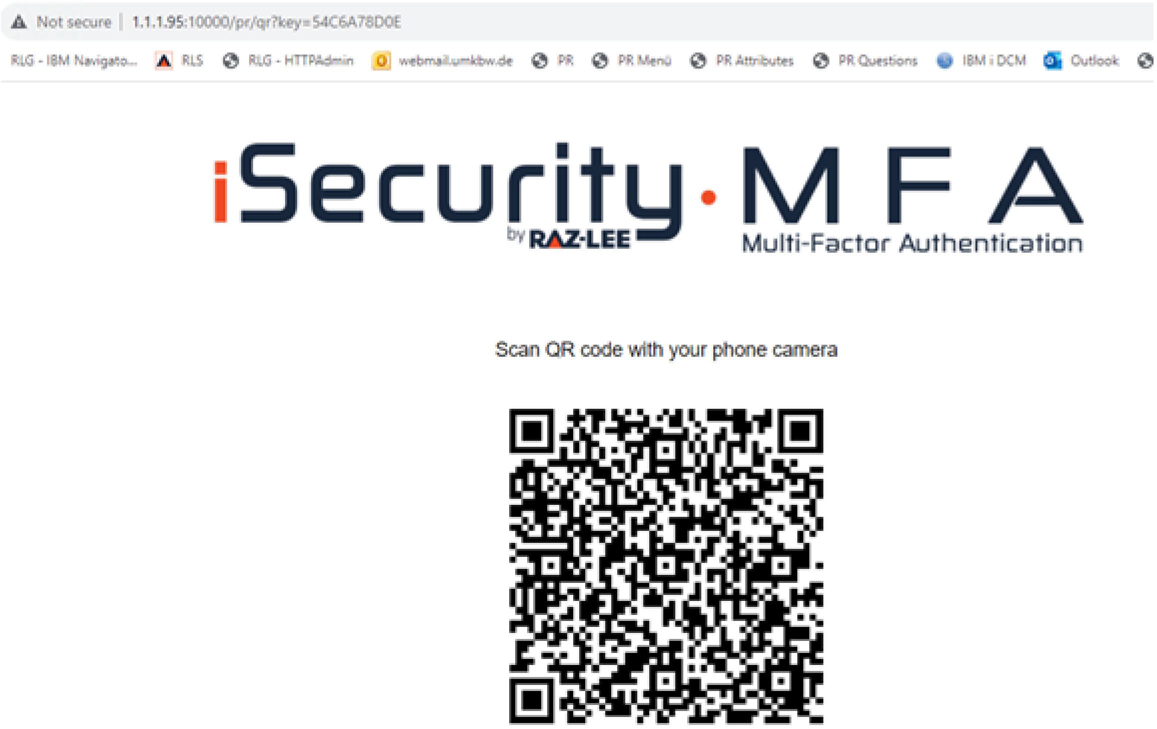


TOTP information

iSecutity_RLG <ISECURITY_RLG@RAZLEE.DE>
An ○ Robert Engel

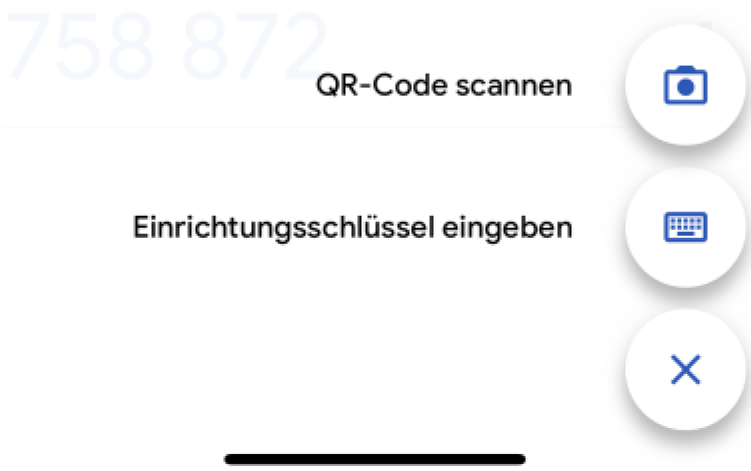
Dear Robert Engel,
Use this link to get your TOTP password.
http://1.1.1.95:10000/pr/qr?key=54C6A78D0E
This link is valid for few minutes only.
We advise you to completely delete this email after you have finished processing
- In Outlook - Select the message and press Shift-Delete.
- In Gmail - Delete the message, then use Delete Forever from the Trash folder

To see the website with the QR code, click on the link in the email. A web page with the QR code appears in your browser:

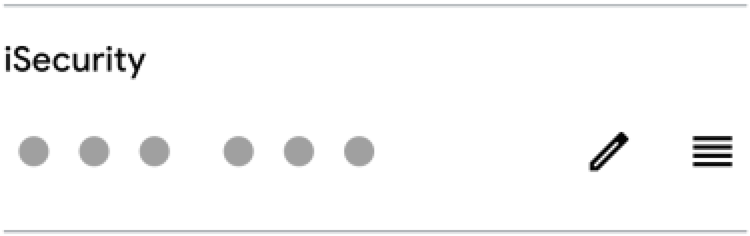


Scan QR code with your phone camera

You can then add the account to an authenticator app on your mobile device. For example, in Google Authenticator, you would select the plus-sign icon to add the account, then select the icon to scan a QR code:

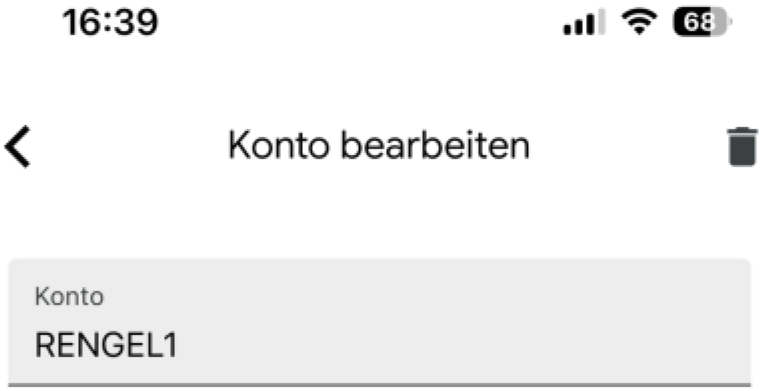


Scan the QR code. A new account appears in the app named "iSecurity".



iSecurity

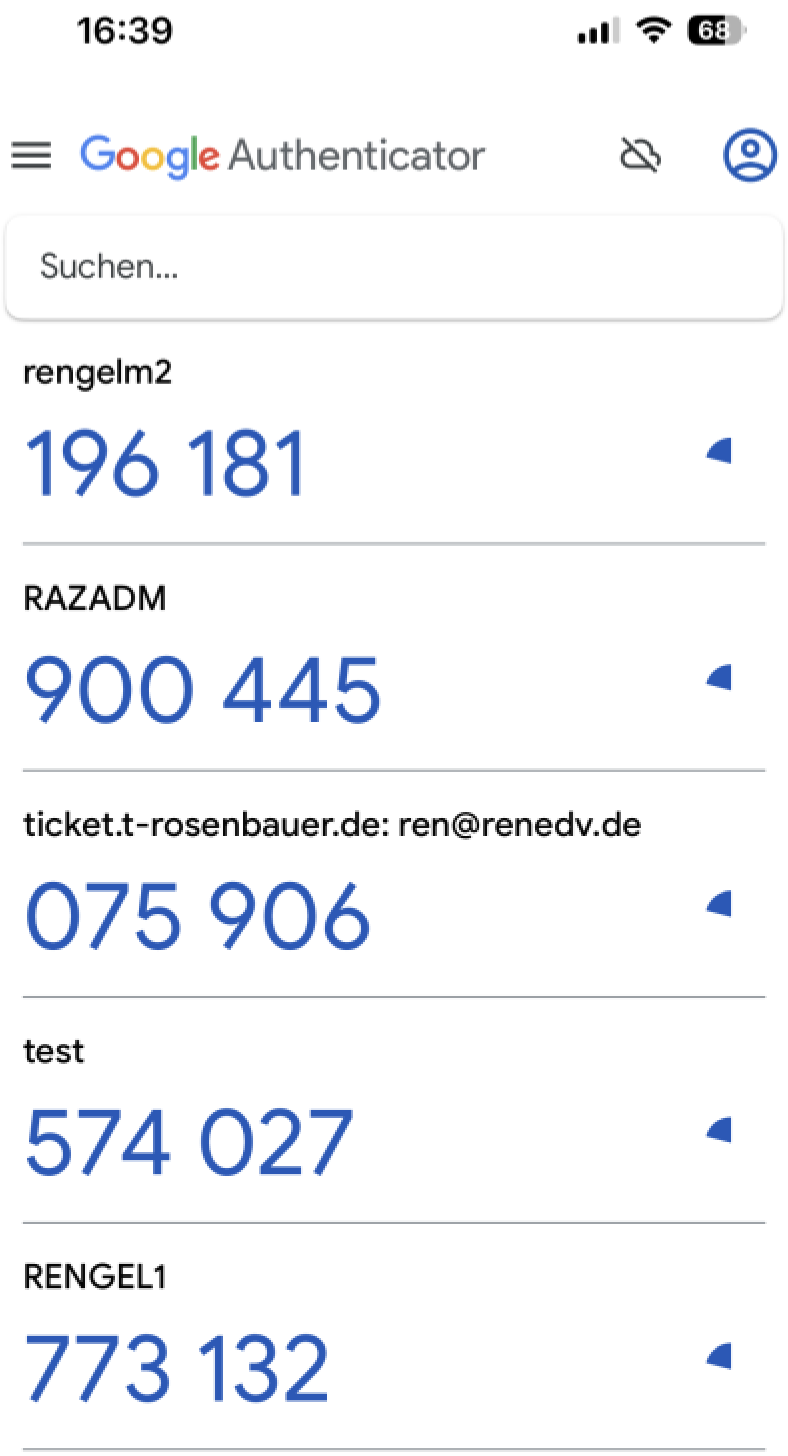
Edit the entry to give your account a meaningful name:



Konto bearbeiten

Konto
RENGEL1

You can now use the Authenticator app with this account:



16:39

Google Authenticator

Suchen...

rengelm2

196 181

RAZADM

900 445

ticket.t-rosenbauer.de: ren@renedv.de

075 906

test

574 027

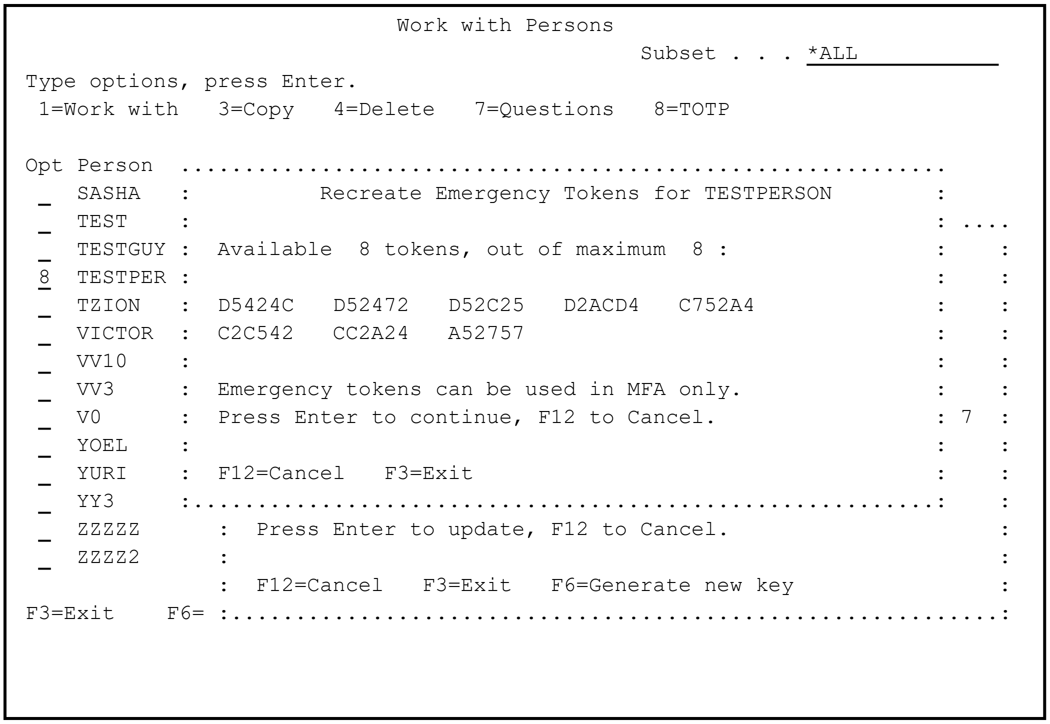
RENGEL1

773 132

To update the new key, press **`Enter`**.

Recreating Emergency Tokens for TOTP

To **recreate the emergency tokens** for the Person, enter **2** in the **`Selection`** field within the **Work with TOTP Secret Key** window (*STRMFA* **`> 1 > 1, 1`**), The **Recreate Emergency Tokens** window appears:



```
                              Work with Persons
                                                   Subset . . . *ALL
Type options, press Enter.
 1=Work with   3=Copy   4=Delete   7=Questions   8=TOTP

Opt Person  ...........................................................
 _  SASHA   :          Recreate Emergency Tokens for TESTPERSON       :
 _  TEST    :                                                         : ....
 _  TESTGUY :  Available  8 tokens, out of maximum  8 :               :    :
 8  TESTPER :                                                         :    :
 _  TZION   :  D5424C   D52472   D52C25   D2ACD4   C752A4             :    :
 _  VICTOR  :  C2C542   CC2A24   A52757                               :    :
 _  VV10    :                                                         :    :
 _  VV3     :  Emergency tokens can be used in MFA only.              :    :
 _  V0      :  Press Enter to continue, F12 to Cancel.                : 7  :
 _  YOEL    :                                                         :    :
 _  YURI    :  F12=Cancel   F3=Exit                                   :    :
 _  YY3     :.........................................................:    :
 _  ZZZZZ      :  Press Enter to update, F12 to Cancel.                    :
 _  ZZZZ2      :                                                           :
               :  F12=Cancel   F3=Exit   F6=Generate new key               :
F3=Exit    F6= :...........................................................:
```

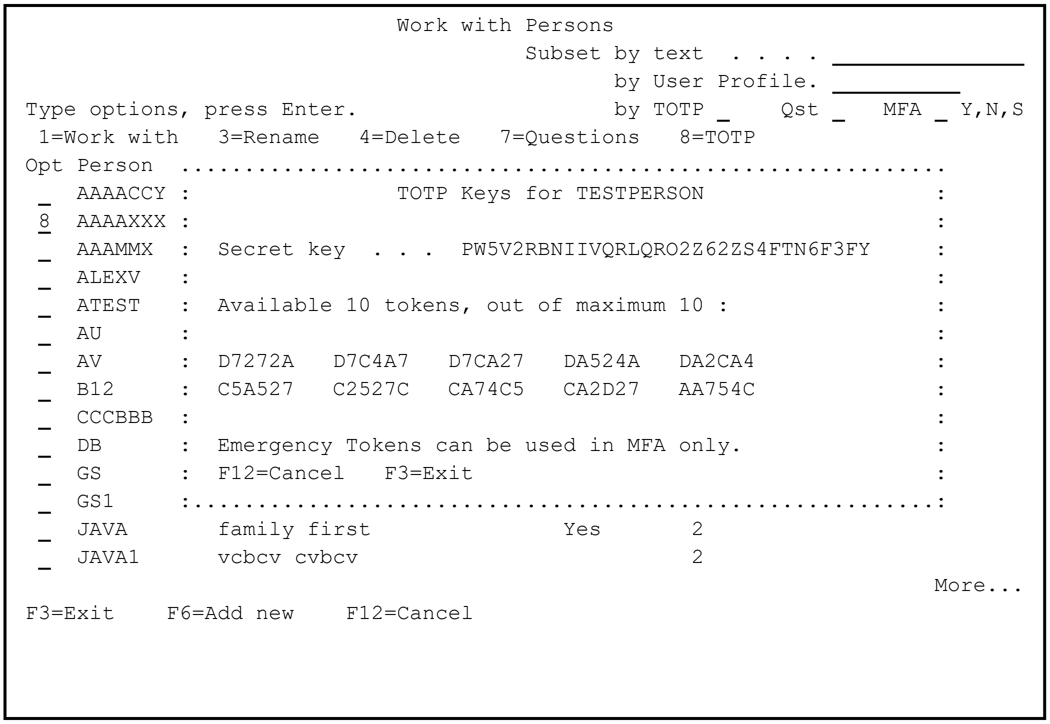
A set of emergency tokens appears. Make a copy of these codes. You can use these for MFA if you cannot access the usual TOTP authentication.

To **cancel the new tokens** and continue to use your current tokens, press **F12**.

To **accept the new tokens**, press **`Enter`**.

Displaying a TOTP Key and Emergency Tokens

To **display the TOTP key and emergency tokens** for the Person, enter **3** in the **`Selection`** field within the **Work with TOTP Secret Key** window (*STRMFA* **`> 1 > 1, 1`**), The **TOTP Keys** window appears:



```
                              Work with Persons
                                        Subset by text  . . . . _______________
                                               by User Profile. __________
Type options, press Enter.                     by TOTP _    Qst _    MFA _ Y,N,S
 1=Work with   3=Rename   4=Delete   7=Questions   8=TOTP
Opt Person  ............................................................
 _  AAAACCY :                TOTP Keys for TESTPERSON                  :
 8  AAAAXXX :                                                          :
 _  AAAMMX  :  Secret key  . . .  PW5V2RBNIIVQRLQRO2Z62ZS4FTN6F3FY     :
 _  ALEXV   :                                                          :
 _  ATEST   :  Available 10 tokens, out of maximum 10 :                :
 _  AU      :                                                          :
 _  AV      :  D7272A   D7C4A7   D7CA27   DA524A   DA2CA4              :
 _  B12     :  C5A527   C2527C   CA74C5   CA2D27   AA754C              :
 _  CCCBBB  :                                                          :
 _  DB      :  Emergency Tokens can be used in MFA only.               :
 _  GS      :  F12=Cancel   F3=Exit                                    :
 _  GS1     :..........................................................:
 _  JAVA       family first               Yes       2
 _  JAVA1      vcbcv cvbcv                          2
                                                                      More...
F3=Exit    F6=Add new    F12=Cancel
```

To return to the **Work with TOTP Secret Key** window, press **F12**.

To return to the **Work with Persons** screen, press **F3**.

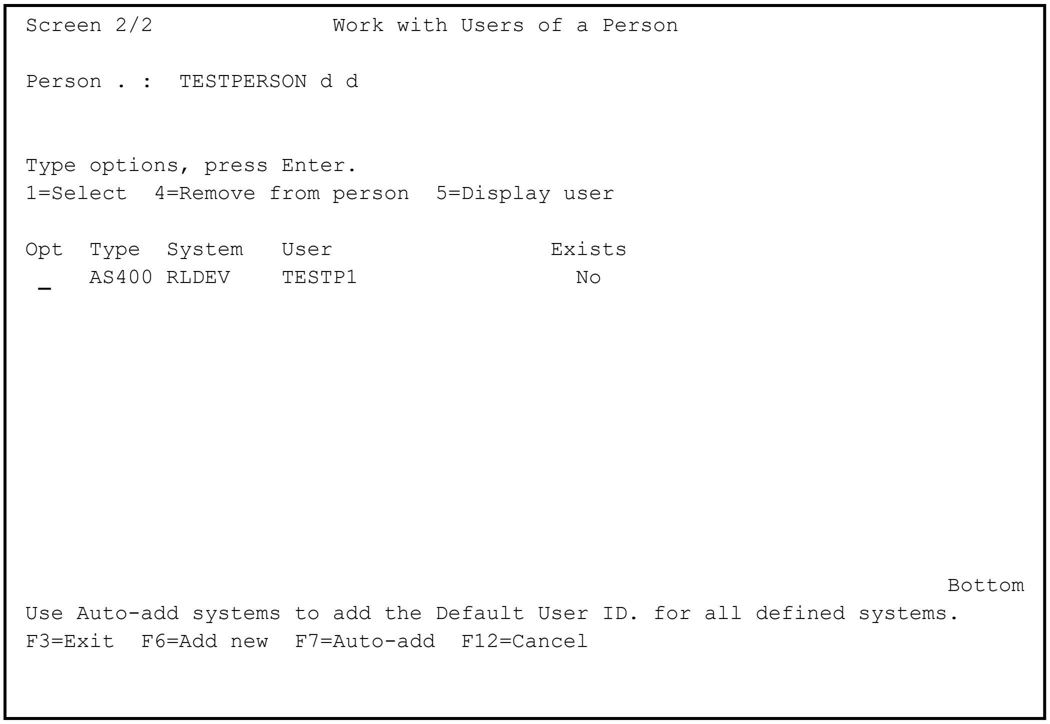
Setting Up Users for a Person

Each Person can correspond to users on multiple systems.

To **add or delete users from a defined Person**, open the **Work with Persons** menu (*STRMFA* **> `1` > `1`**).

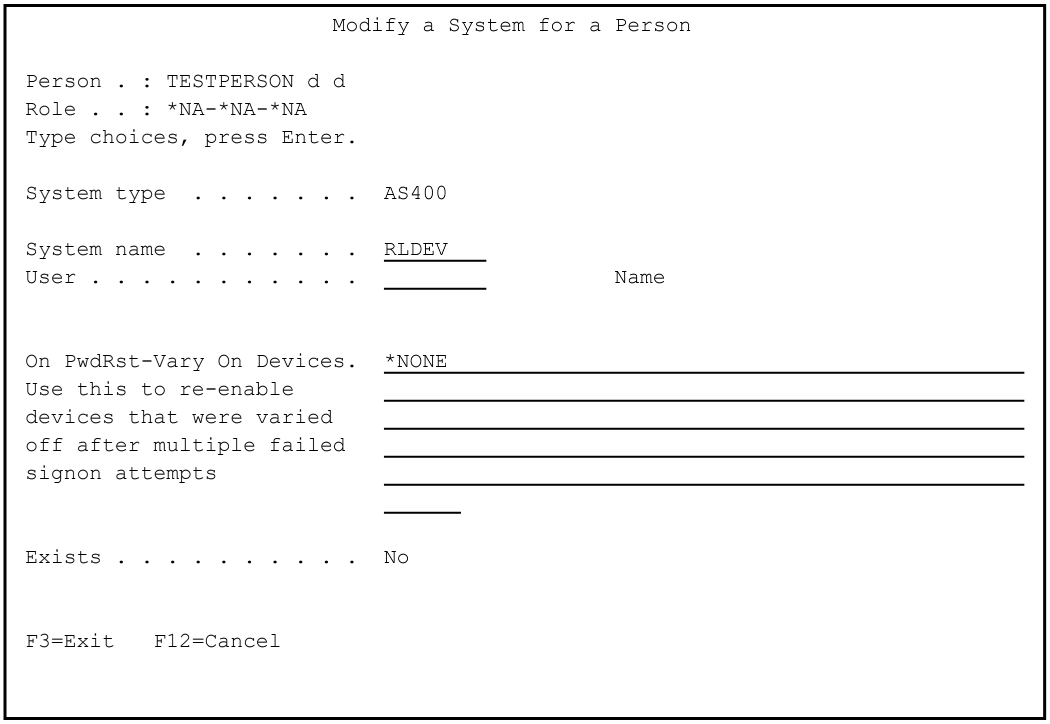
Enter **`1`** in the **`Opt`** field for the Person. The **Modify Person** screen appears.

Press **Enter** again. The **Work with Users of a Person** screen appears.



```
Screen 2/2              Work with Users of a Person

Person . :  TESTPERSON d d


Type options, press Enter.
1=Select  4=Remove from person  5=Display user

Opt  Type  System   User                 Exists
 _   AS400 RLDEV    TESTP1                 No












                                                                   Bottom
Use Auto-add systems to add the Default User ID. for all defined systems.
F3=Exit  F6=Add new  F7=Auto-add  F12=Cancel
```

To **add a user to a person**, press the **F6** key from the **Work with Users for a Person** screen (*STRMFA* **> `1` > `1, 1`**).. The **Modify a System for a Person** screen appears.



```
                         Modify a System for a Person

 Person . : TESTPERSON d d
 Role . . : *NA-*NA-*NA
 Type choices, press Enter.

 System type  . . . . . . .  AS400

 System name  . . . . . . .  RLDEV
 User . . . . . . . . . . .                    Name


 On PwdRst-Vary On Devices.  *NONE
 Use this to re-enable
 devices that were varied
 off after multiple failed
 signon attempts


 Exists . . . . . . . . . .  No


 F3=Exit   F12=Cancel
```

Enter the name of the system for the user in the **`System name`** field. By default, this is the system on which you are working,.

Enter the name of the user in the **`User`** field. Press the **F4** key to display a list of users on the system.

To **automatically add a user to a person**, press the **F7** key from the **Work with Users for a Person** screen (*STRMFA* **`> 1 > 1, 1`**). If a user with the same name of the Person exists on the system, that user is automatically added to the person.

To **modify information about an existing user for the person**, enter **`1`** in the **`Opt`** field for the user on the **Work with Users for a Person** screen (*STRMFA* **`> 1 > 1, 1`**). The **Modify a System for a Person** screen appears, as it does for adding a user, with the information for the current user.

To **delete an existing user from a person**, enter **4** in the **`Opt`** field for the user on the **Work with Users for a Person** screen (*STRMFA* **`> 1 > 1, 1`**). The **Delete a System for a Person** screen appears, with the same fields as the **Modify a System for a Person** screen. Press **Enter** to delete the user, or the **F12** key to cancel the deletion.

To **view detailed information on a user** in a convenient, read-only form, enter **`1`** in the **`Opt`** field for the user on the **Work with Persons by Users** screen (*STRMFA* **`> 1 > 3`**). The **Display User** screen appears, showing the information.

To **move a user to another person**, enter **`3`** in the **`Opt`** field for the user on the **Work with Persons by Users** screen (*STRMFA* **`> 1 > 3`**). The **Move User to another person** screen appears. Enter the name of the person to whom you are moving the user in the **`To person`** field.

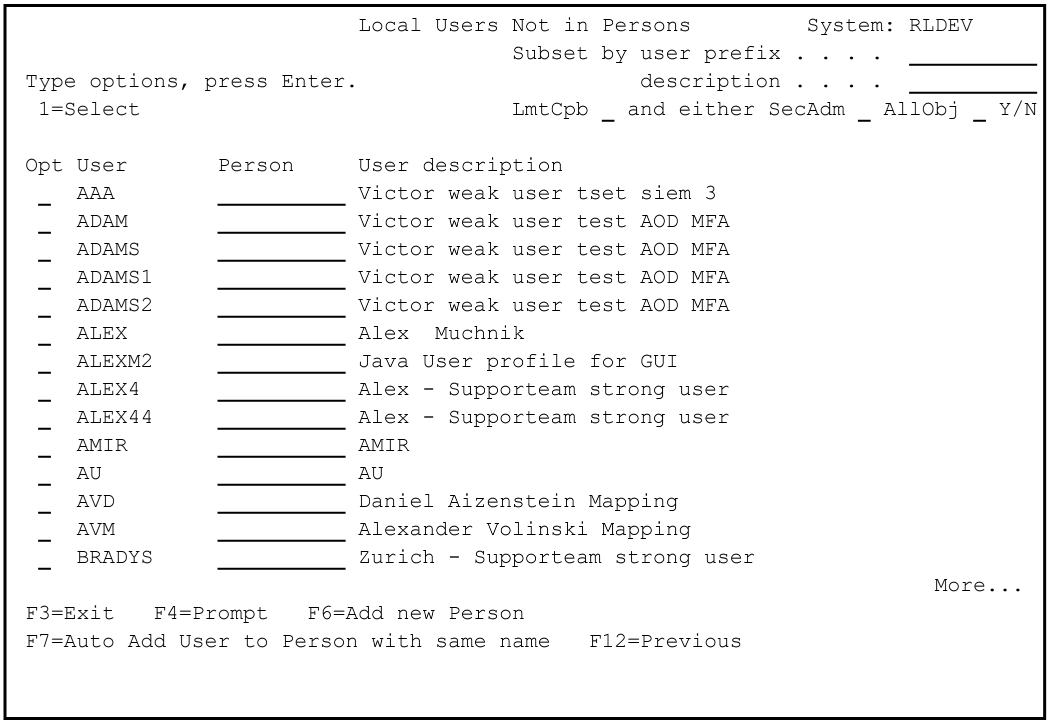
To **remove a user from a person**, enter **`4`** in the **`Opt`** field for the user on the **Work with Persons by Users** screen (*STRMFA* **`> 1 > 3`**). The **Remove Users from persons** screen appears, showing the name of the User and System and the Person from whom the user is to be removed. Press **Enter** to remove the user, or the **F12** key to cancel the removal.

To **view users who have not been assigned to persons**, select **`5. Local Users Not in Persons`** from the **Persons** menu (*STRMFA* **`> 1`**). The **Local Users Not in Persons** screen appears, as shown in "Assigning Users to Persons" on the facing page.

To **delete definitions for Persons** who should have been removed in other actions, select **`22. Delete Orphan Definitions`** from the **Persons** menu (*STRMFA* **`> 1`**). A **Call Program (CALL)** screen appears, which runs the *PRDLTOSR* command from the **`SMZO`** library.

Assigning Users to Persons

To **view users who have not been assigned to persons**, select **`5. Local Users Not in Persons`** from the **Persons** menu (*STRMFA* **`> 1`**). The **Local Users Not in Persons** screen appears.



```
                          Local Users Not in Persons        System: RLDEV
                                      Subset by user prefix . . . .  __________
Type options, press Enter.                      description . . . .  __________
 1=Select                             LmtCpb _ and either SecAdm _ AllObj _ Y/N

Opt User       Person     User description
 _  AAA        __________ Victor weak user tset siem 3
 _  ADAM       __________ Victor weak user test AOD MFA
 _  ADAMS      __________ Victor weak user test AOD MFA
 _  ADAMS1     __________ Victor weak user test AOD MFA
 _  ADAMS2     __________ Victor weak user test AOD MFA
 _  ALEX       __________ Alex  Muchnik
 _  ALEXM2     __________ Java User profile for GUI
 _  ALEX4      __________ Alex - Supporteam strong user
 _  ALEX44     __________ Alex - Supporteam strong user
 _  AMIR       __________ AMIR
 _  AU         __________ AU
 _  AVD        __________ Daniel Aizenstein Mapping
 _  AVM        __________ Alexander Volinski Mapping
 _  BRADYS     __________ Zurich - Supporteam strong user
                                                                       More...
F3=Exit   F4=Prompt   F6=Add new Person
F7=Auto Add User to Person with same name   F12=Previous
```

The body of the screen contains lines for each user on the current system that does not have a corresponding Person. Each line shows the **`User`** name, a free-text **`User description`**, and an empty **`Person`** field.

To **assign the user to an existing Person**, enter the Person's name in the **`Person`** field and press **Enter**.

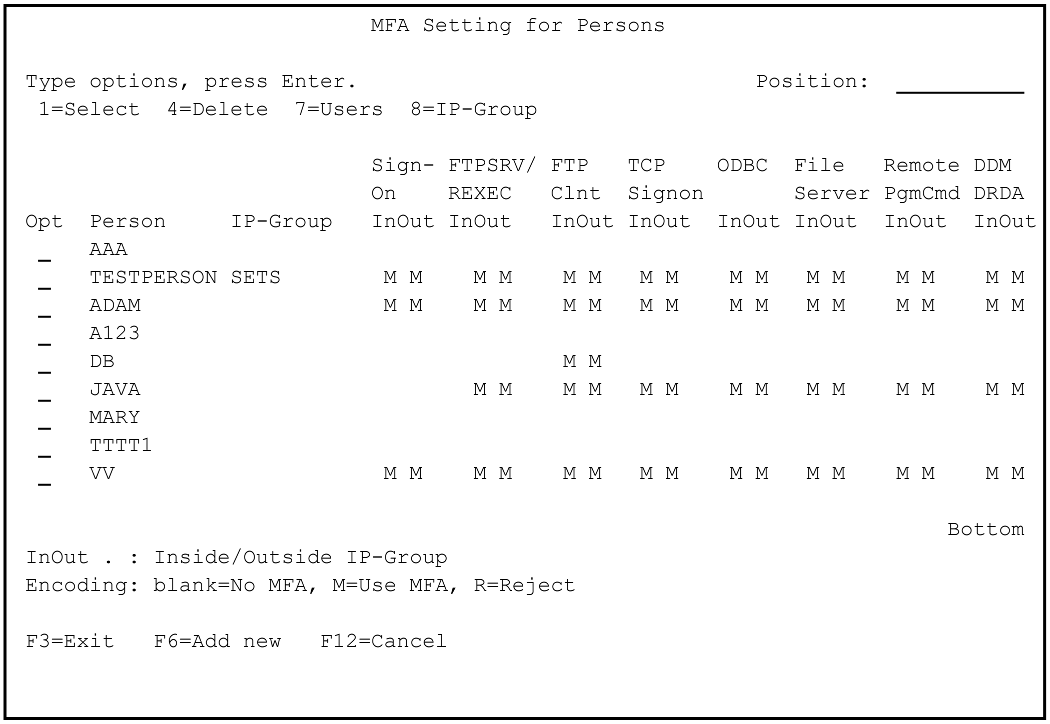
To **select from a list of existing persons**, press the **F4** key.

To **automatically add the user to an existing Person with the same name**, press the **F7** key.

To **create a new Person**, press the **F6** key. The **Add New Person** screen appears, as shown in "Adding a New Person" on page 63.

MFA Settings for Persons

To specify which users require Multi Factor Authentication, select **3. MFA Setting for Persons** from the main Multi Factor Authentication (MFA) menu. The MFA Setting for Persons screen appears.



```
                           MFA Setting for Persons

Type options, press Enter.                               Position: __________
 1=Select  4=Delete  7=Users  8=IP-Group

                           Sign- FTPSRV/ FTP   TCP    ODBC  File   Remote DDM
                           On    REXEC   Clnt  Signon       Server PgmCmd DRDA
Opt  Person     IP-Group   InOut InOut   InOut InOut  InOut InOut  InOut  InOut
 _   AAA
 _   TESTPERSON SETS        M M    M M    M M   M M    M M   M M    M M    M M
 _   ADAM                   M M    M M    M M   M M    M M   M M    M M    M M
 _   A123
 _   DB                                   M M
 _   JAVA                          M M    M M   M M    M M   M M    M M    M M
 _   MARY
 _   TTTT1
 _   VV                     M M    M M    M M   M M    M M   M M    M M    M M

                                                                        Bottom
InOut . : Inside/Outside IP-Group
Encoding: blank=No MFA, M=Use MFA, R=Reject

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

The body of the screen only contains lines for persons for whom MFA settings have already been created. Person who have Password Reset settings but not MFA do not appear.

Each of these lines shows the **Person** name for that person, the **IP-Group** to which the person belongs, and the person's settings for each of several access services for the person. The settings for the services include two columns: an **In** column for accesses from within the persons's IP Group and an **Out** column for accesses from outside it.

The **In** and **Out** column for each service in each row indicates whether MFA allows access with or without authentication or rejects the access. Possible values are:

- **M**: Require authentication.
- **R**: Reject the access.
- **blank**: Allow access without authentication.

To **add a new person** to the list of users, press the **F6** key. The **Add MFA Setting for Person** screen appears, as shown in "Adding or Modifying MFA Settings for Persons" on the next page.

To **modify a person's MFA settings**, enter **`1`** in the **`Opt`** field for that person. The **Modify MFA Setting for Users** screen appears, as shown in "Adding or Modifying MFA Settings for Persons" on the next page.

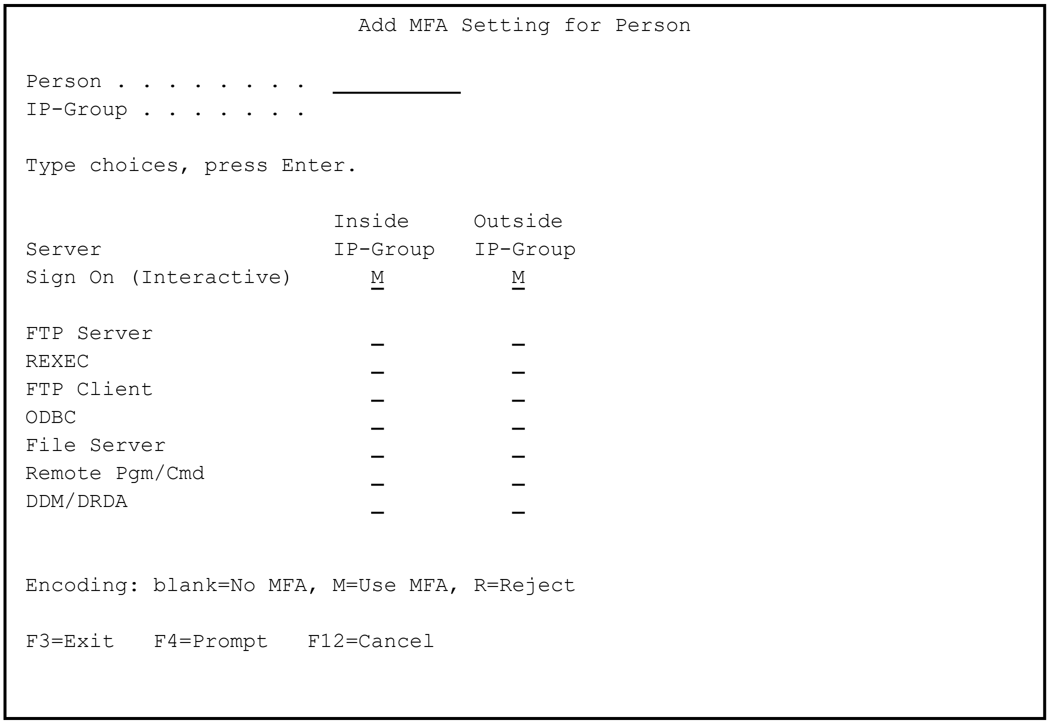
To **delete a person** from the list of users, enter **`4`** in the **`Opt`** field for that person. The **Delete MFA Setting for Persons** screen appears. Press **`Enter`** to delete the persons or the **`F12`** key to cancel.

To **display the users for a person**, enter **`7`** in the **`Opt`** field for the person. The **Users of a Person** window appears, showing, for each user, the **`System`** for the user, the **`User`** name, and whether the person **`Exists`** on that system.

To **display the definition of a person's IP Group**, if one is shown in the person's **`IP-Group`** field, enter 8 in the **`Opt`** field for the person. The **IP-Group** window appears, showing the IP Group definitions.

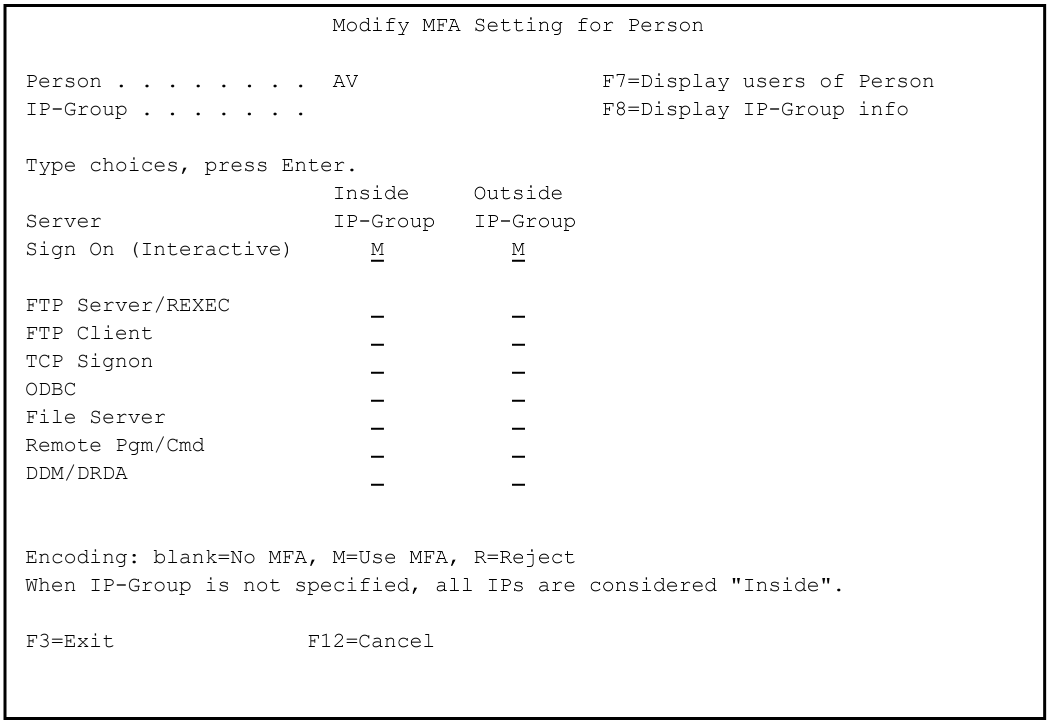
Adding or Modifying MFA Settings for Persons

To **add MFA settings for a person**, press the **F6** key on the **MFA Setting for Persons** screen (*STRMFA* **> 3**), The **Add MFA Setting for Person** screen appears.



```
                           Add MFA Setting for Person

Person . . . . . . . .   __________
IP-Group . . . . . . .

Type choices, press Enter.

                        Inside     Outside
Server                  IP-Group   IP-Group
Sign On (Interactive)      M          M

FTP Server                 _          _
REXEC                      _          _
FTP Client                 _          _
ODBC                       _          _
File Server                _          _
Remote Pgm/Cmd             _          _
DDM/DRDA                   _          _


Encoding: blank=No MFA, M=Use MFA, R=Reject

F3=Exit   F4=Prompt   F12=Cancel
```

To **modify MFA settings for a person**, enter **1** in the **Opt** field for that person on the **MFA Setting for Persons** screen (*STRMFA* **> 3**). The **Modify MFA Setting for Person** screen, which has the same fields as the **Add MFA Setting for Person** screen, appears.



```
                        Modify MFA Setting for Person

Person . . . . . . . .  AV                   F7=Display users of Person
IP-Group . . . . . . .                       F8=Display IP-Group info

Type choices, press Enter.
                        Inside     Outside
Server                  IP-Group   IP-Group
Sign On (Interactive)      M          M

FTP Server/REXEC           _          _
FTP Client                 _          _
TCP Signon                 _          _
ODBC                       _          _
File Server                _          _
Remote Pgm/Cmd             _          _
DDM/DRDA                   _          _


Encoding: blank=No MFA, M=Use MFA, R=Reject
When IP-Group is not specified, all IPs are considered "Inside".

F3=Exit               F12=Cancel
```

The **`Person`** field contains the name of the person.

If the person is a member of an IP-Group, the group's name appears in the **`IP-Group`** field. You can assign the person to an IP-Group in the Modify Persons screen, as shown in "Modifying a Person" on page 66.

The body of the screen contains lines for each of the services that the Person might attempt to access. For each, fields indicate whether authentication is needed if the Person accesses the service from **`Inside`** or **`Outside`** their IP-Group. If no IP-Group is displayed for the Person, all accesses are considered to be **`Inside`**.

Possible values are:

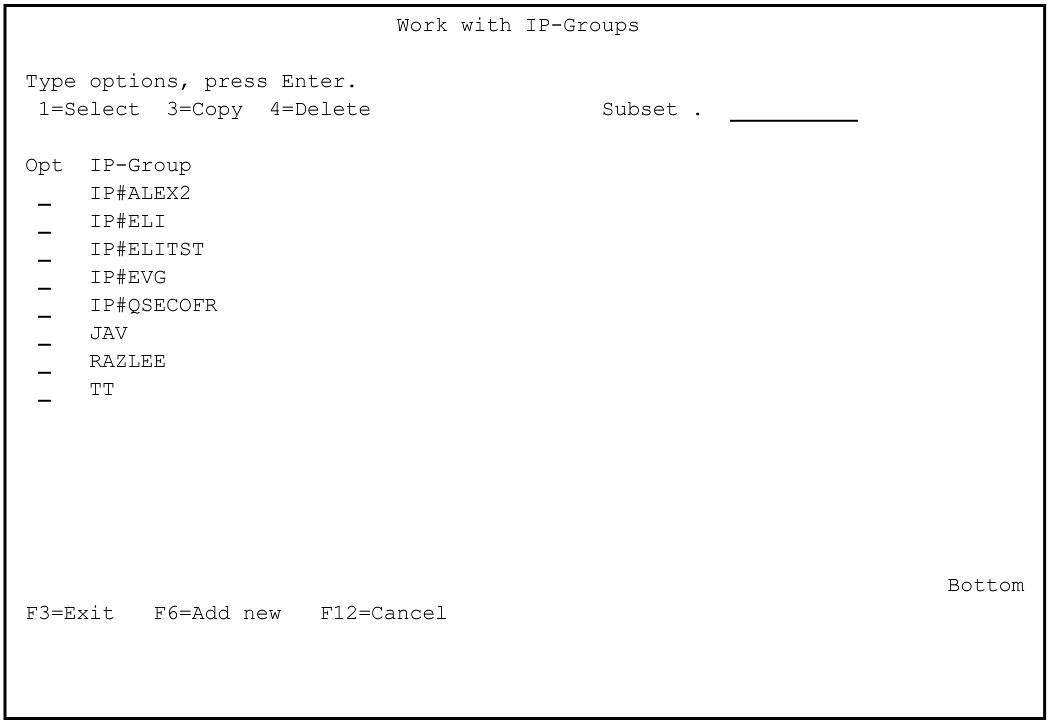
- **`M`**: Require authentication.
- **`R`**: Reject the access.
- **`blank`**: Allow access without authentication.

Defining IP Groups

Using IP Groups, you can define sets of IP addresses from which users might try to access your system. You can specify, for example, that users within a given IP group can connect to your systems without needing MFA, while the same users outside that set of addresses must use MFA for authentication or might be blocked entirely. A single IP Group can contain multiple IP address ranges.

For example, you might specify that workers at IP addresses within your Human Resources office could access HR systems freely. To reach those systems from off-site, the HR workers might need Multi-Factor Authentication, while workers from other departments might not be able to access those systems at all.

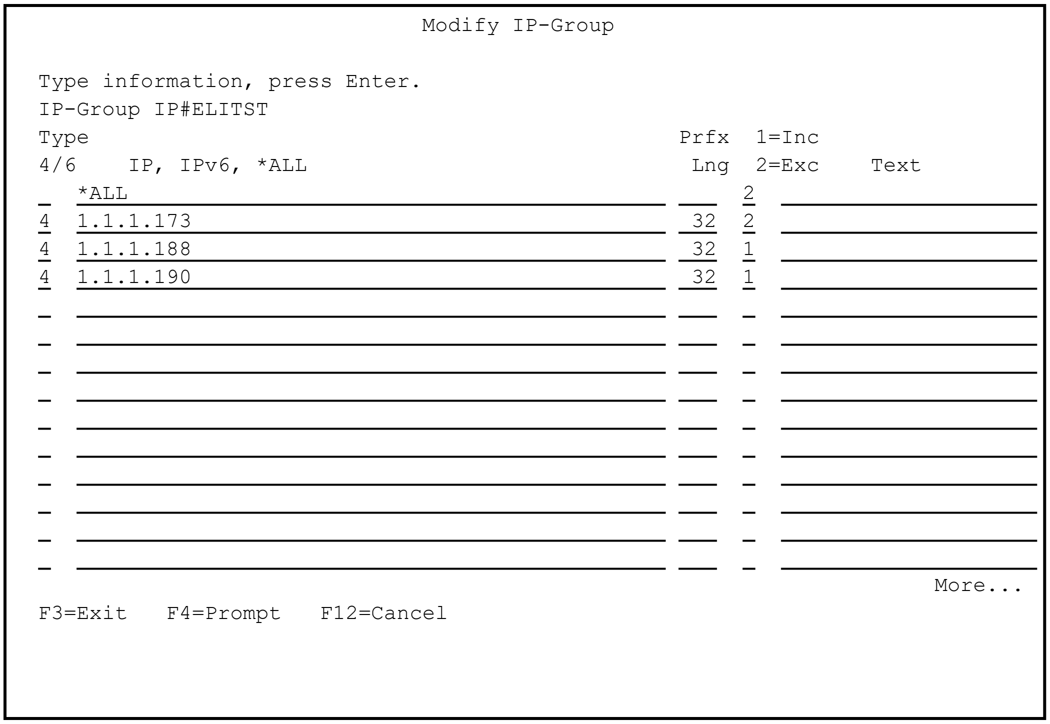
To **work with IP groups**, select **`8. IP-Groups`** from the main MFA screen (*STRMFA*). The **Work with IP-Groups** screen appears.



```
                             Work with IP-Groups

 Type options, press Enter.
  1=Select   3=Copy   4=Delete                  Subset .  __________

 Opt  IP-Group
  _   IP#ALEX2
  _   IP#ELI
  _   IP#ELITST
  _   IP#EVG
  _   IP#QSECOFR
  _   JAV
  _   RAZLEE
  _   TT







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

The **`IP-Group`** column shows the names of existing IP Groups.

To **view and modify** an IP Group, enter **`1`** in the **`Opt`** column for that group. The **Modify IP-Group** screen opens.



```
                              Modify IP-Group

Type information, press Enter.
IP-Group IP#ELITST
Type                                                  Prfx  1=Inc
4/6    IP, IPv6, *ALL                                  Lng  2=Exc    Text
_  *ALL______________________________________________  ___  2  ____________________
4  1.1.1.173_________________________________________   32  2  ____________________
4  1.1.1.188_________________________________________   32  1  ____________________
4  1.1.1.190_________________________________________   32  1  ____________________
_  __________________________________________________  ___  _  ____________________
_  __________________________________________________  ___  _  ____________________
_  __________________________________________________  ___  _  ____________________
_  __________________________________________________  ___  _  ____________________
_  __________________________________________________  ___  _  ____________________
_  __________________________________________________  ___  _  ____________________
_  __________________________________________________  ___  _  ____________________
_  __________________________________________________  ___  _  ____________________
_  __________________________________________________  ___  _  ____________________
_  __________________________________________________  ___  _  ____________________
                                                                          More...
F3=Exit   F4=Prompt   F12=Cancel
```

Each line on the body of the screen represents a single IP range. The line with the range **`*ALL`** represents all IP addresses not expressly included in the other ranges. The lines include these fields:

`4/6`

The IP version of the range; **`4`** for IPv4 and **`6`** for IPv6.

`IP, IPv6, *ALL`

The starting address of the address range, or **`*ALL`**

`Prfx Lng`

The prefix length for the range. Press the **F4** key in this field to display the ranges and their explanations, and to select from them.

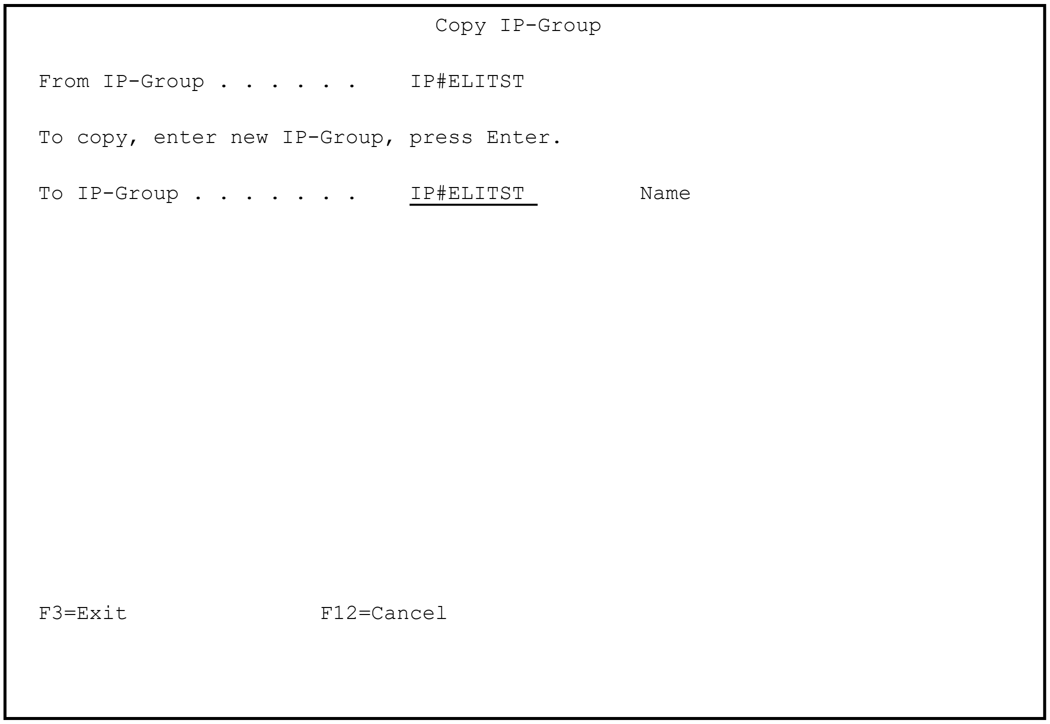
`1=Inc 2=Exc`

If "**`1`**", the rule refers to all addresses **within** the range. If "**`2`**", the rule refers to all addresses **outside** the range.

`Text`

A free-form text description of the address range.

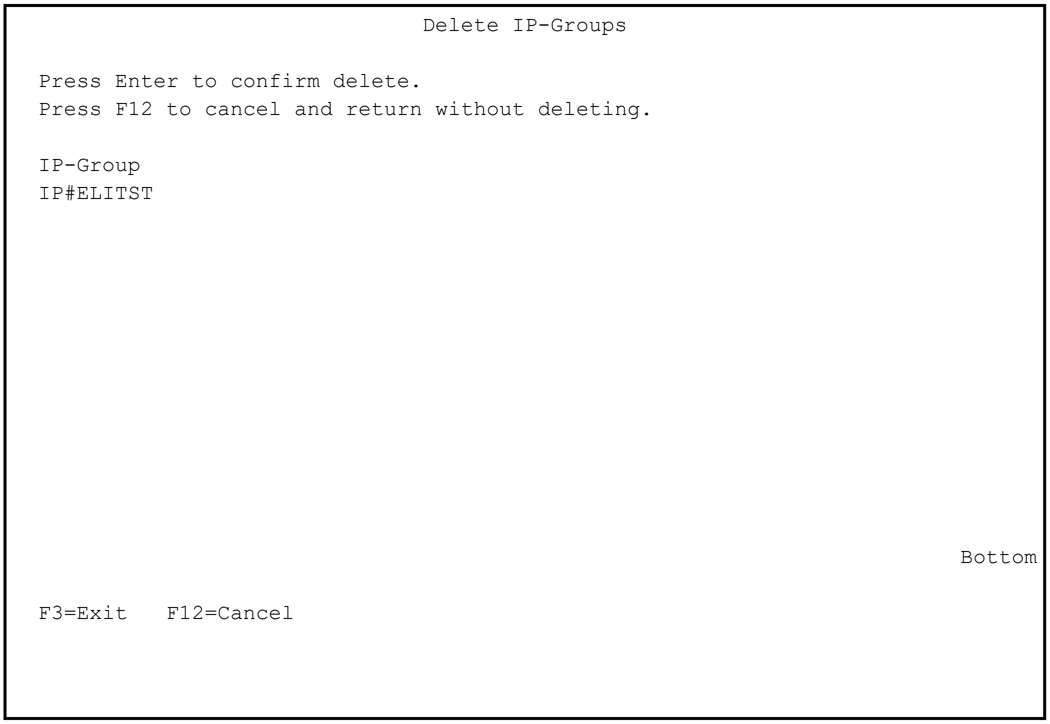
To **copy an IP-Group**, enter **`3`** in the **`Opt`** field for that group on the **Work with IP-Groups** screen. The **`Copy IP-Group`** screen opens.



```
                                Copy IP-Group

 From IP-Group . . . . . .    IP#ELITST

 To copy, enter new IP-Group, press Enter.

 To IP-Group . . . . . . .    IP#ELITST          Name















 F3=Exit               F12=Cancel
```

Enter the name of the new IP Group in the **`To IP-Group`** field. The new IP Group will be created, including all the settings of the original group.

To **delete an IP-Group**, enter **4** in the **`Opt`** field for that group on the **Work with IP-Groups** screen. The **`Delete IP-Group`** screen opens.



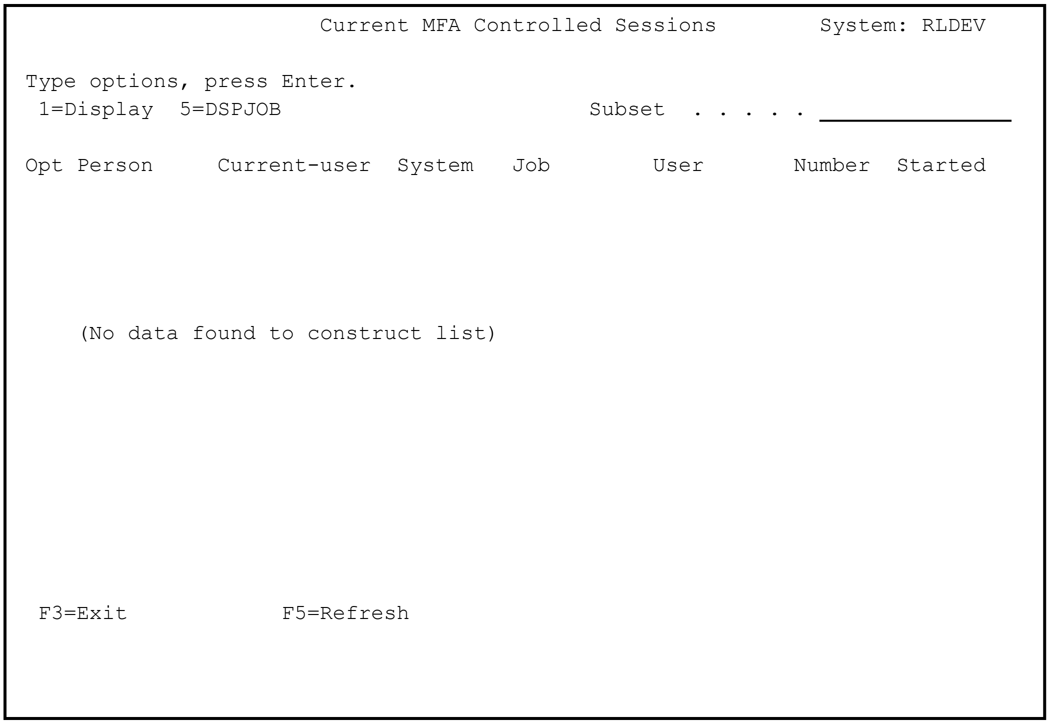
```
                               Delete IP-Groups

 Press Enter to confirm delete.
 Press F12 to cancel and return without deleting.

 IP-Group
 IP#ELITST

















                                                                       Bottom

 F3=Exit   F12=Cancel
```

Press **Enter** to confirm the deletion or **F12** to cancel it.

Specifying IP-Groups

You can specify (on the **Users Requiring MFA** screen, shown in "MFA Settings for Persons" on page 82) 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:



```
                        Current MFA Controlled Sessions        System: RLDEV

 Type options, press Enter.
  1=Display   5=DSPJOB                        Subset  . . . . .  _______________

 Opt  Person     Current-user  System   Job         User       Number  Started



     (No data found to construct list)








  F3=Exit             F5=Refresh
```

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`

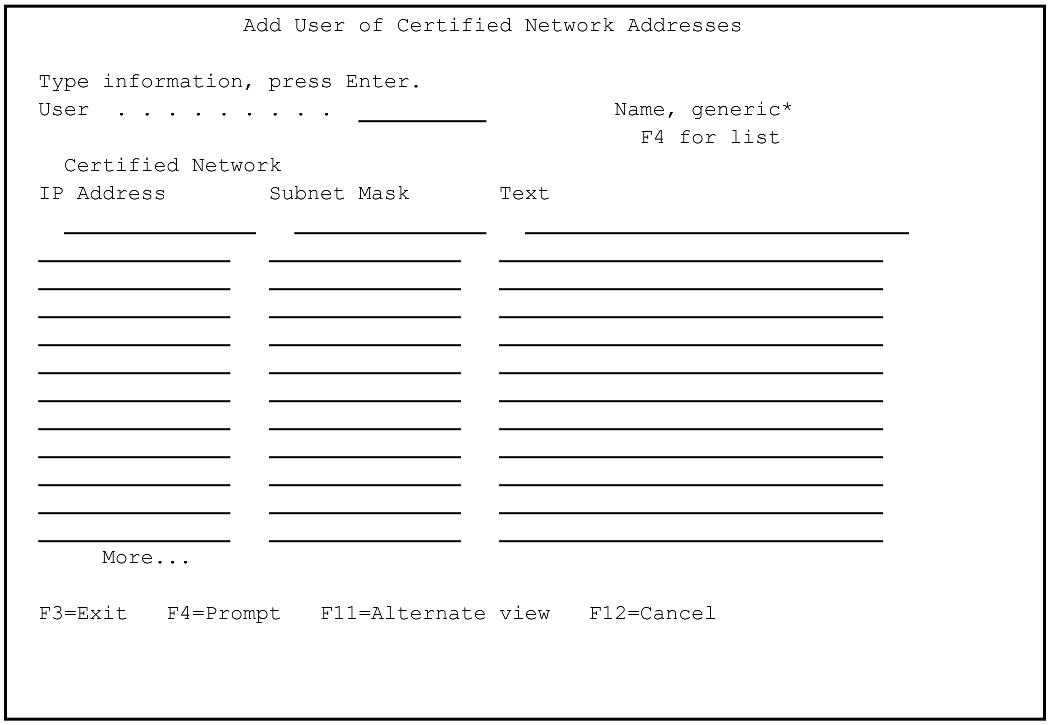
Certified IP addresses for the user. If they connect from these IP Addresses, and the user is set not to require MFA when connecting via that protocol via certified addresses (by setting the field for that user and protocol to the letter **O** on the **Users Requiring MFA** screen), MFA is not required.

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 93.

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 IP-Groups" on page 90). 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

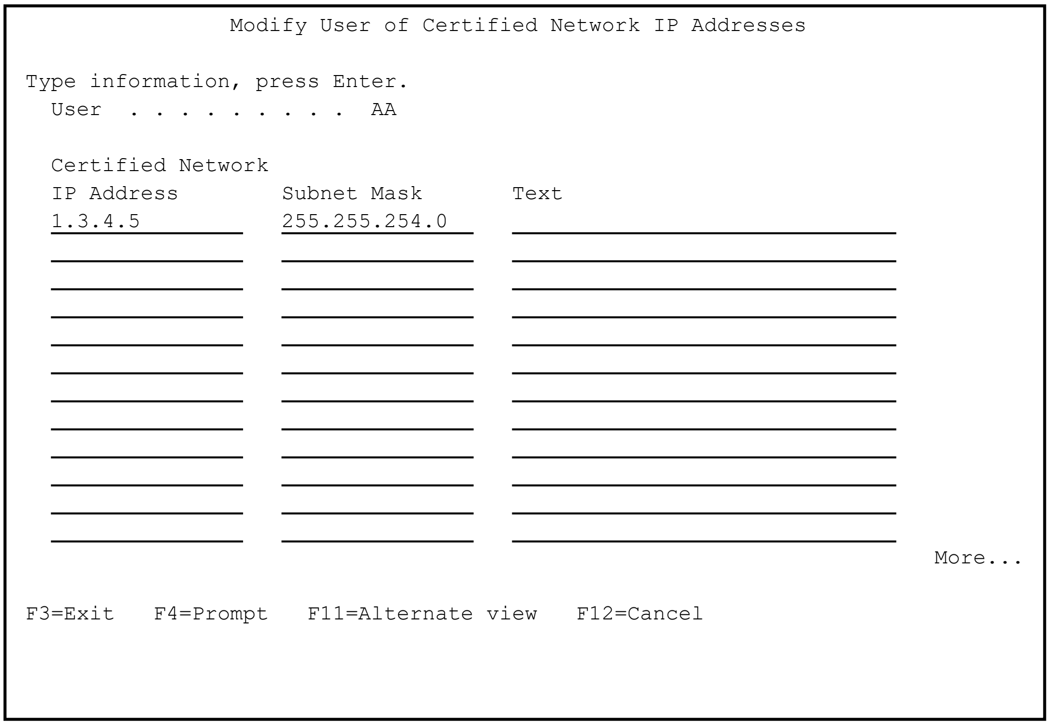
A subnet mask indicating the range of addresses including that address.

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 IP-Groups" on page 90). The **Modify User of Certified Network IP Addresses** screen appears:



```
                 Modify User of Certified Network IP Addresses

Type information, press Enter.
  User  . . . . . . . . .   AA

  Certified Network
  IP Address         Subnet Mask        Text
  1.3.4.5            255.255.254.0
                                                                         More...

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

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`

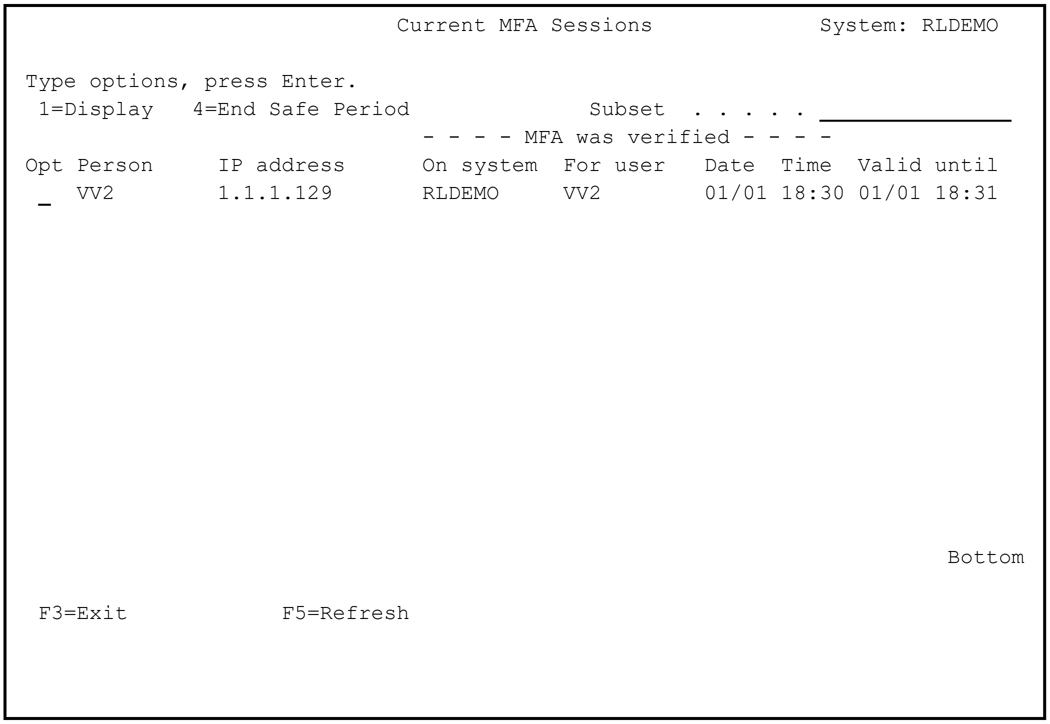
A subnet mask indicating the range of addresses including that address.

`Text`

A text description of the range.

Displaying Sessions Controlled by MFA

To **display sessions 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 17). The **Current MFA Sessions** screen appears:



```
                              Current MFA Sessions             System: RLDEMO

Type options, press Enter.
 1=Display   4=End Safe Period              Subset  . . . . .  _______________
                                - - - - MFA was verified - - - -
Opt Person      IP address       On system  For user    Date  Time  Valid until
 _  VV2         1.1.1.129        RLDEMO     VV2         01/01 18:30 01/01 18:31









                                                                          Bottom

 F3=Exit             F5=Refresh
```

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

`Person`

The name of the person

`IP address`

The IP address of client where the job was initiated

`MFA was verified:`

`On system`

The system on which the user is authenticated using MFA

`For User`

The user id of the user who started the job

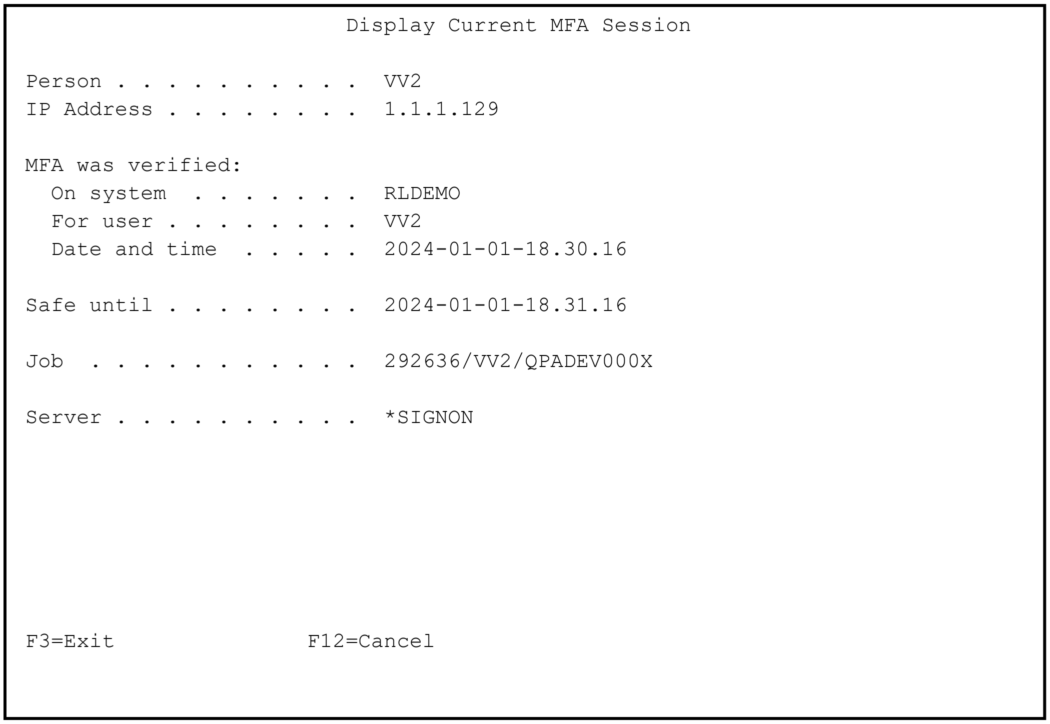
Date/Time

The starting date/time of the session

Valid until

Date and time at which the session will expire. The user will have to authenticate again if he signs on after this time.

To **display further information about a job**, enter 1 in the **Opt** field for that job. The **Display Current MFA Session** screen appears.



```
                         Display Current MFA Session

Person . . . . . . . . . .  VV2
IP Address . . . . . . . .  1.1.1.129

MFA was verified:
  On system  . . . . . . .  RLDEMO
  For user . . . . . . . .  VV2
  Date and time  . . . . .  2024-01-01-18.30.16

Safe until . . . . . . . .  2024-01-01-18.31.16

Job  . . . . . . . . . . .  292636/VV2/QPADEV000X

Server . . . . . . . . . .  *SIGNON






F3=Exit               F12=Cancel
```

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

- the **Job** from which the connection was made
- the **Server** through which the connection was made

Configuring the Password Reset and MFA Webserver

iSecurity Password Reset and Multi Factor Authentication use the same web server.

MFA for TCP services other than 5250 signon works differently:

- The user tries to sign on using one of the activated servers (***STRMFA* > 81 > 52**). This starts the signon process.
- If MFA is required, the user receives an email containing a link to the MFA website.
- The user clicks on the link and the Browser asking for identification starts on his device.
- The user identifies himself using a TOTP Token (from Microsoft Authenticator, Google authenticator or any other) or against Oauth 2 method
- If the authentication is completed, the user continues using the chosen service.
- If the authentication cannot be completed within the specified time, the service is rejected.

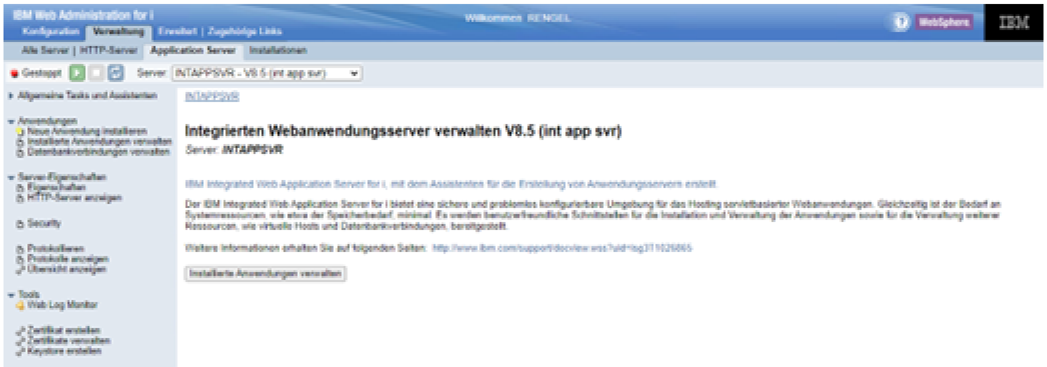
The web server can run either on a Tomcat 10 web server on any PC or server in the company, or on the integrated Application Server for IBM I, which is available, free of charge, on any IBM i server.

Configuring the Application Server on IBM i

In your web browser, open URL: **`http://`*ipaddressofibmi*`:2001/HTTPAdmin`** where *ipaddressofibmi* is the IP address of your IBM i.

Sign on with **`QSECOFR`** or similar profile with enough special authorities.

The configuration screen appears



Integrierten Webanwendungsserver verwalten V8.5 (int app svr)

Server: INTAPPSVR

IBM Integrated Web Application Server for i, mit dem Assistenten für die Erstellung von Anwendungsservern erstellt.

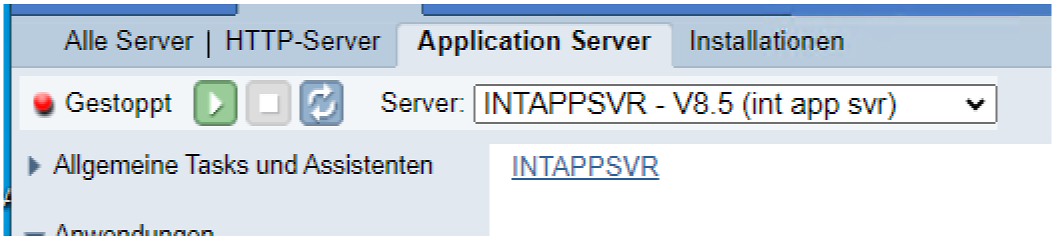
Der IBM Integrated Web Application Server for i bietet eine sichere und problemlos konfigurierbare Umgebung für das Hosting servletbasierter Webanwendungen. Gleichzeitig ist der Bedarf an Systemressourcen, wie etwa der Speicherbedarf, minimal. Es werden benutzerfreundliche Schnittstellen für die Installation und Verwaltung der Anwendungen sowie für die Verwaltung weiterer Ressourcen, wie virtuelle Hosts und Datenbankverbindungen, bereitgestellt.

Weitere Informationen erhalten Sie auf folgenden Seiten: http://www.ibm.com/support/docview.wss?uid=isg3T1025865

Use the Configuration tab to configure a new application server or use your existing application server.

To configure a new application server, click on **Create new application server** and proceed through all the screens up to the end.

Ensure that your application server has been started. If it has not, click on the green **start** button


Alle Server | HTTP-Server
Application Server
Installationen
Gestoppt
Server: INTAPPSVR - V8.5 (int app svr)
Allgemeine Tasks und Assistenten
INTAPPSVR
Anwendungen

Once your application server is started, you have to rename the **`tomcat9-pr.war`** file to **`pr.war`**. The **`war`** file is located in the IFS directory **`/iSecurits/PRWEB`**.

Configuring the Application Server on Tomcat10

1. Download current version of the Apache Tomcat server (in this case 10.0.20) and install it on your PC/Server in drive **`C:`**
2. In the installation directory: **`C:\apache-tomcat-10.0.20\bin`**, edit the files **`startup.bat`** and **`shutdown.bat`** to set the JAVA_ HOME or JRE_HOME directory:

   ```
   setlocal
   set "JRE_HOME=C:\Program Files\Java\jdk-15.0.2"
   ```

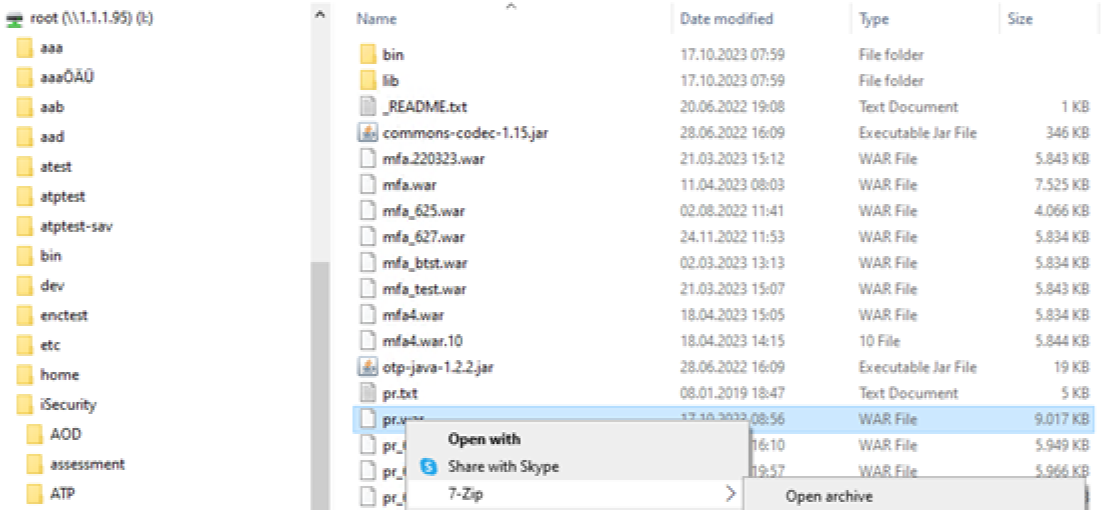
3. In the **`C:\apache-tomcat-10.0.20\conf directory`**, enter the appropriate port number in the **`server.xml`** file. In this example, it is "**8081**":

   ```
   <Connector port="8081" protocol="HTTP/1.1"
   connectionTimeout="20000"
   redirectPort="8443" />
   ```

4. Deploy the application directories within the **`C:\apache-tomcat-10.0.20\webapps`** directory.
5. Copy the HTML with your links to the **`LPARs/Applications`** file in the **`C:\apache-tomcat-10.0.20\webapps\ROOT`** directory:
   `http://ipaddress:8081/RAZLEE-L.HTML`
6. Clean old logs in the **`C:\apache-tomcat-10\logs directory`**.
7. Clean directories in the **`C:\apache-tomcat-10.0.20\work\Catalina\localhost`** directory.

Configuring the pr.war File

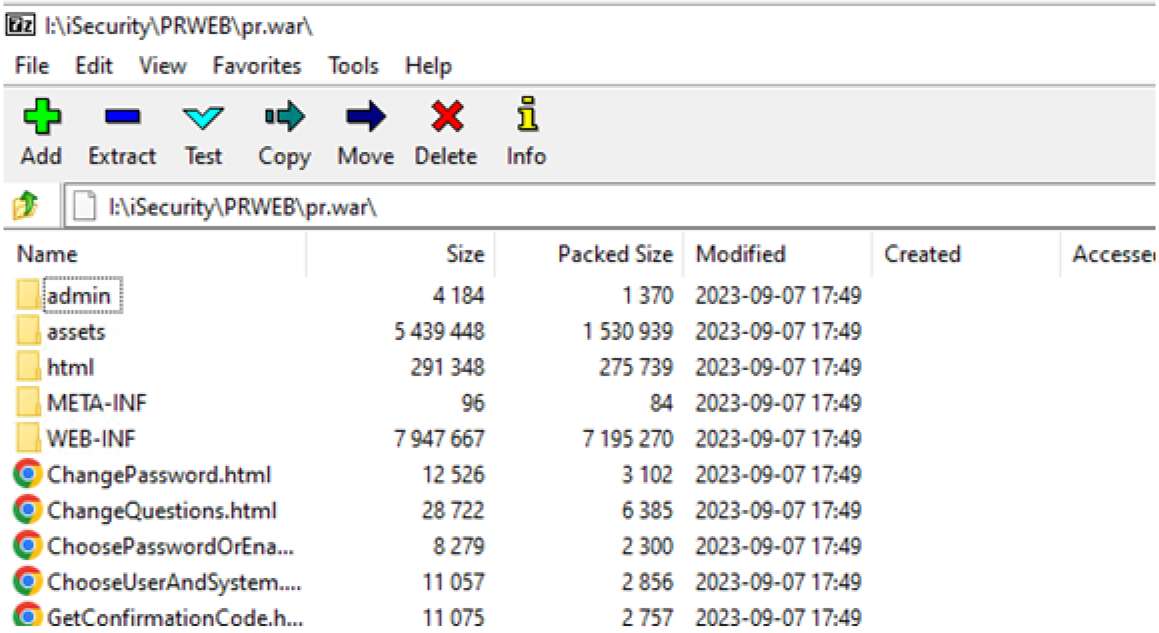
Open the pr.war file using a zip program such as 7-zip:



root (\\1.1.1.95) (I:)
aaa
aaaÖÄÜ
aab
aad
atest
atptest
atptest-sav
bin
dev
enctest
etc
home
iSecurity
AOD
assessment
ATP

Name	Date modified	Type	Size
bin	17.10.2023 07:59	File folder	
lib	17.10.2023 07:59	File folder	
_README.txt	20.06.2022 19:08	Text Document	1 KB
commons-codec-1.15.jar	28.06.2022 16:09	Executable Jar File	346 KB
mfa.220323.war	21.03.2023 15:12	WAR File	5.843 KB
mfa.war	11.04.2023 08:03	WAR File	7.525 KB
mfa_625.war	02.08.2022 11:41	WAR File	4.066 KB
mfa_627.war	24.11.2022 11:53	WAR File	5.834 KB
mfa_btst.war	02.03.2023 13:13	WAR File	5.834 KB
mfa_test.war	21.03.2023 15:07	WAR File	5.843 KB
mfa4.war	18.04.2023 15:05	WAR File	5.834 KB
mfa4.war.10	18.04.2023 14:15	10 File	5.844 KB
otp-java-1.2.2.jar	28.06.2022 16:09	Executable Jar File	19 KB
pr.txt	08.01.2019 18:47	Text Document	5 KB
pr.war	17.10.2023 08:56	WAR File	9.017 KB
pr_	16:10	WAR File	5.949 KB
pr_	19:57	WAR File	5.966 KB
pr_			

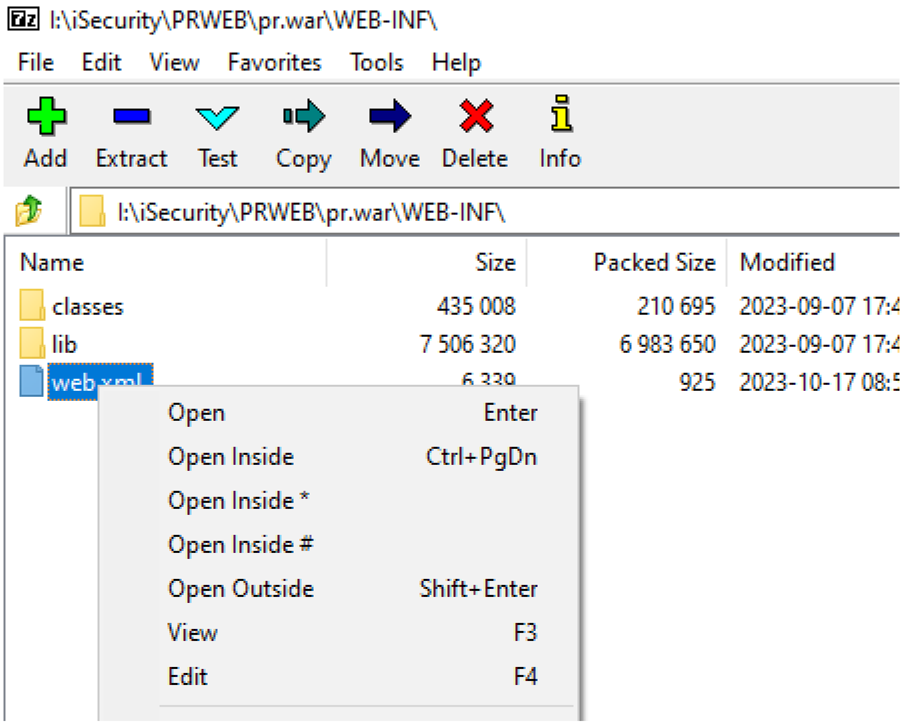
Click the right mouse button and choose **7-zip**. The **`.war`** file opens in 7-zip.



I:\iSecurity\PRWEB\pr.war\

Name	Size	Packed Size	Modified	Created	Accesse
admin	4 184	1 370	2023-09-07 17:49		
assets	5 439 448	1 530 939	2023-09-07 17:49		
html	291 348	275 739	2023-09-07 17:49		
META-INF	96	84	2023-09-07 17:49		
WEB-INF	7 947 667	7 195 270	2023-09-07 17:49		
ChangePassword.html	12 526	3 102	2023-09-07 17:49		
ChangeQuestions.html	28 722	6 385	2023-09-07 17:49		
ChoosePasswordOrEna...	8 279	2 300	2023-09-07 17:49		
ChooseUserAndSystem....	11 057	2 856	2023-09-07 17:49		
GetConfirmationCode.h...	11 075	2 757	2023-09-07 17:49		

Double click on the **`WEB-INF`** directory



RIght click on **`web.xml`** and choose **Edit** .

In the **`pr.war`** file you find three occurrences of this starting with **`<init-param>`**:

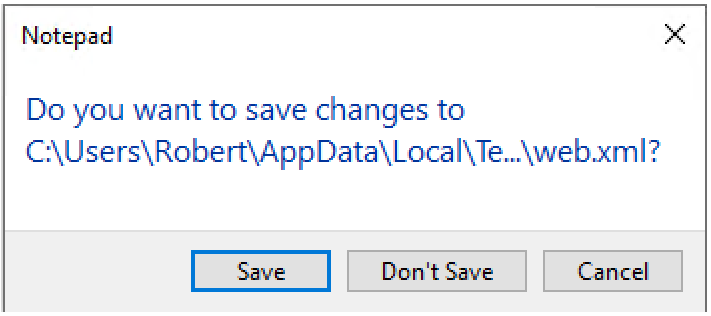
```
<init-param>
    <description>IBMi-Name/ip</description>
    <param-name>host</param-name>
    <param-value>localhost</param-value>
</init-param>
<init-param>
    <description>IBMi-User</description>
    <param-name>user</param-name>
    <param-value>*CURRENT</param-value>
</init-param>
<init-param>
    <description>IBMi-password</description>
    <param-name>password</param-name>
    <param-value>*CURRENT</param-value>
</init-param>
```

Now replace all instances of **localhost** with the IP address of your IBM i

Then replace all instances of ***CURRENT** in the line below **user** with the user profile that you want to use for authentication. We recommend that you copy the user profile **SECURITY8** to **SECURITY8W** and assign this new profile a proper password.

Then replace all instances of ***CURRENT** in the line below **password** with the password of the user profile.

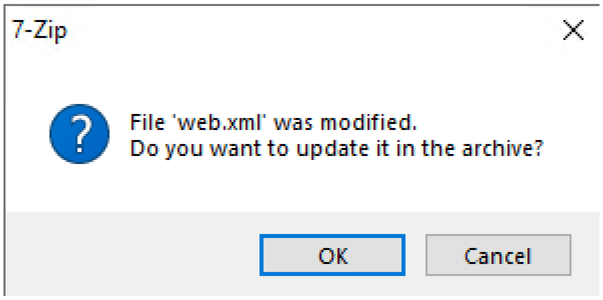
Now close the editor and save the changes by clicking on Save:



Notepad

Do you want to save changes to C:\Users\Robert\AppData\Local\Te...\web.xml?

Also save the modified **web.xml** into the **war** file by clicking on OK:



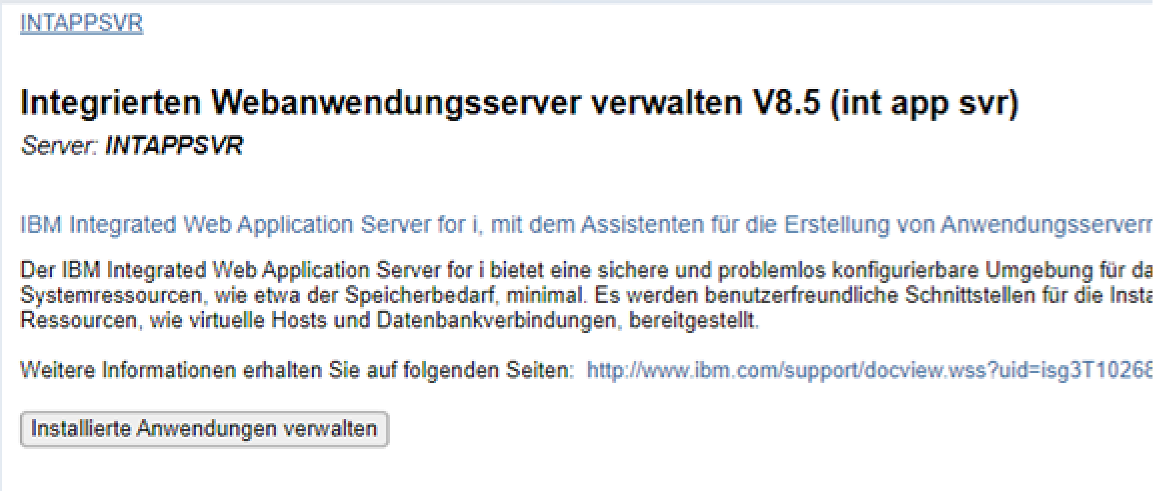
7-Zip

File 'web.xml' was modified.
Do you want to update it in the archive?

Close the **`.war`** file

Completing Configuration on Integrated Application Server on IBM I

Click on the **Application Server** tab and choose **Maintain installed applications**:



INTAPPSVR

Integrierten Webanwendungsserver verwalten V8.5 (int app svr)

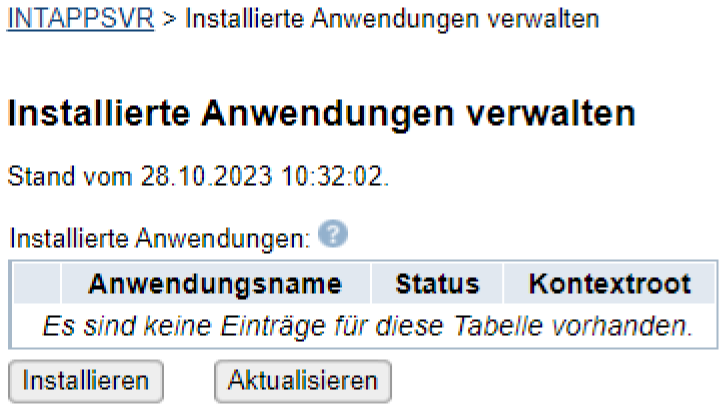
*Server: **INTAPPSVR***

IBM Integrated Web Application Server for i, mit dem Assistenten für die Erstellung von Anwendungsserverr

Der IBM Integrated Web Application Server for i bietet eine sichere und problemlos konfigurierbare Umgebung für da Systemressourcen, wie etwa der Speicherbedarf, minimal. Es werden benutzerfreundliche Schnittstellen für die Insta Ressourcen, wie virtuelle Hosts und Datenbankverbindungen, bereitgestellt.

Weitere Informationen erhalten Sie auf folgenden Seiten: http://www.ibm.com/support/docview.wss?uid=isg3T1026

If no application is installed, you will see this screen. If there an old application is installed already, uninstall it first.



INTAPPSVR > Installierte Anwendungen verwalten

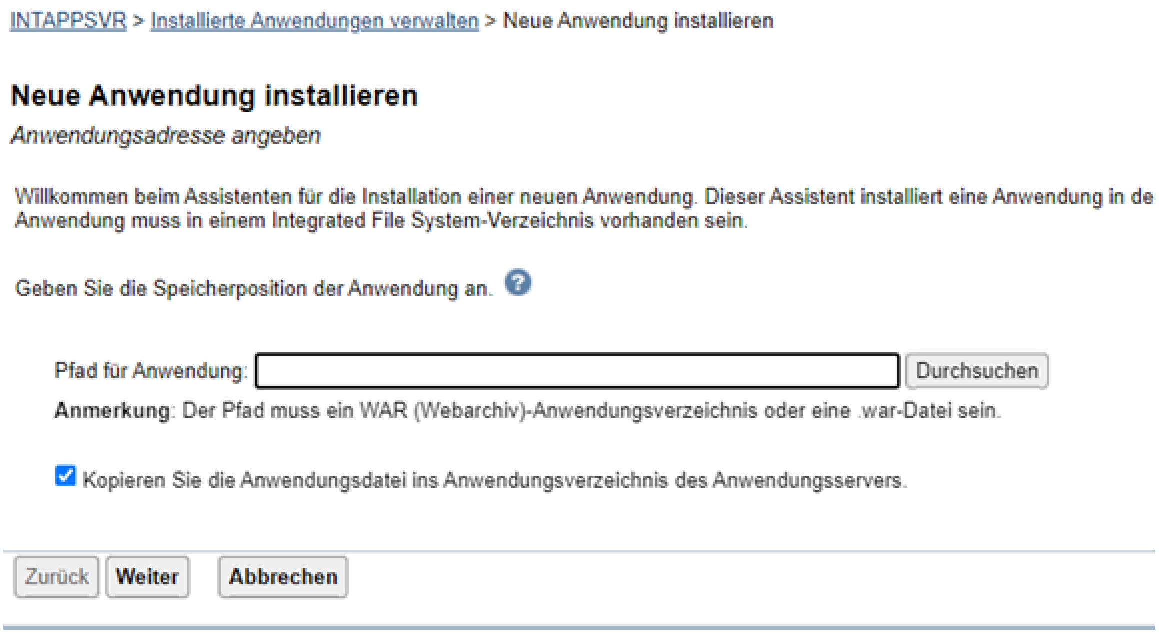
Installierte Anwendungen verwalten

Stand vom 28.10.2023 10:32:02.

Installierte Anwendungen:

	Anwendungsname	Status	Kontextroot
Es sind keine Einträge für diese Tabelle vorhanden.			

Click on **Install**



INTAPPSVR > Installierte Anwendungen verwalten > Neue Anwendung installieren

Neue Anwendung installieren

Anwendungsadresse angeben

Willkommen beim Assistenten für die Installation einer neuen Anwendung. Dieser Assistent installiert eine Anwendung in de
Anwendung muss in einem Integrated File System-Verzeichnis vorhanden sein.

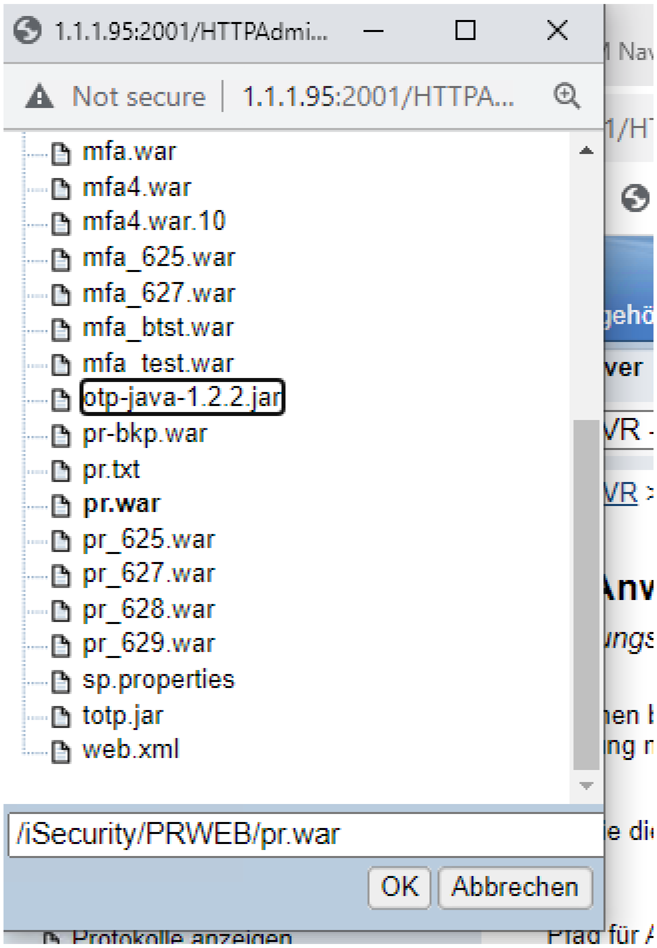
Geben Sie die Speicherposition der Anwendung an.

Pfad für Anwendung: [ ] Durchsuchen

Anmerkung: Der Pfad muss ein WAR (Webarchiv)-Anwendungsverzeichnis oder eine .war-Datei sein.

☑ Kopieren Sie die Anwendungsdatei ins Anwendungsverzeichnis des Anwendungsservers.

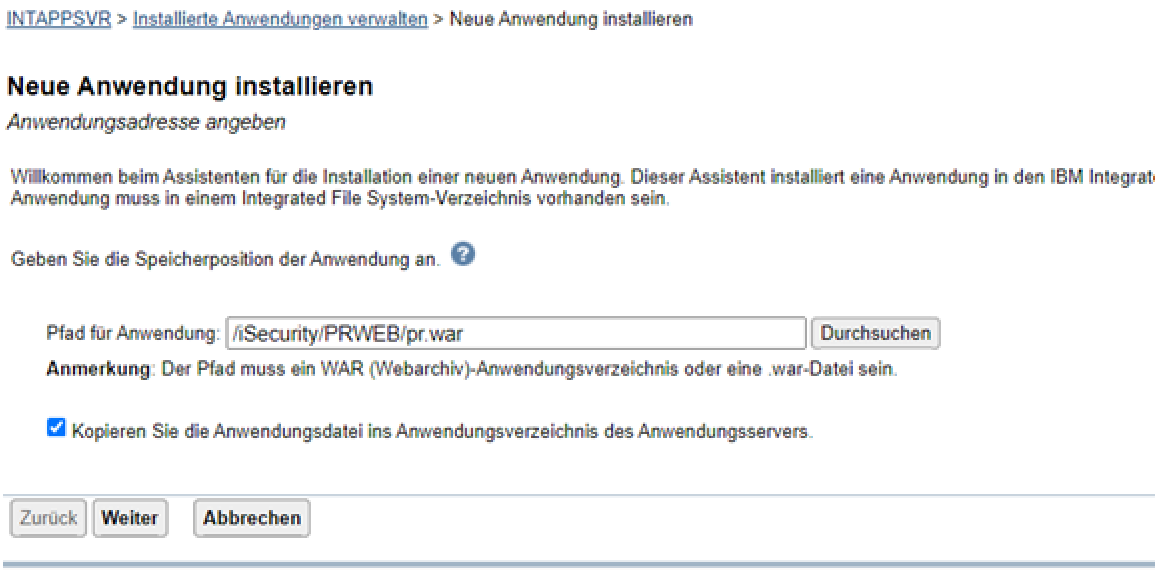
Click on **Browse** and navigate to the **`/iSecurity/PRWEB`** directory



- mfa.war
- mfa4.war
- mfa4.war.10
- mfa_625.war
- mfa_627.war
- mfa_btst.war
- mfa_test.war
- otp-java-1.2.2.jar
- pr-bkp.war
- pr.txt
- **pr.war**
- pr_625.war
- pr_627.war
- pr_628.war
- pr_629.war
- sp.properties
- totp.jar
- web.xml

/iSecurity/PRWEB/pr.war

Click on **OK**


INTAPPSVR > Installierte Anwendungen verwalten > Neue Anwendung installieren

Neue Anwendung installieren

Anwendungsadresse angeben

Willkommen beim Assistenten für die Installation einer neuen Anwendung. Dieser Assistent installiert eine Anwendung in den IBM Integrat
Anwendung muss in einem Integrated File System-Verzeichnis vorhanden sein.

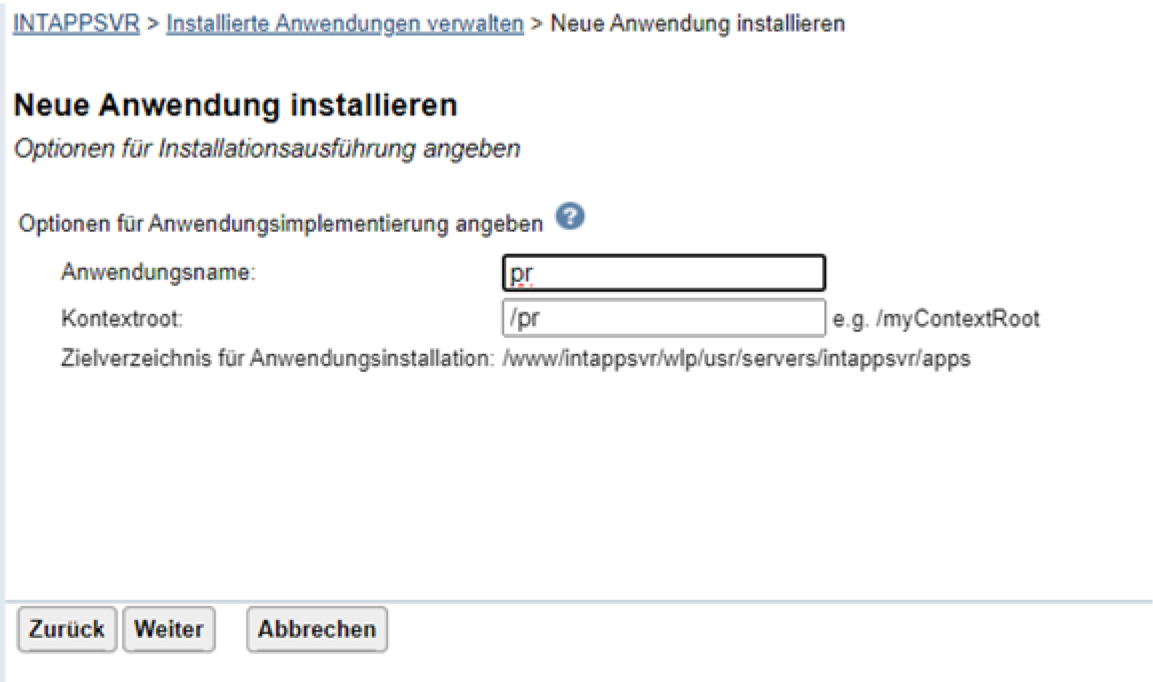
Geben Sie die Speicherposition der Anwendung an.

Pfad für Anwendung: /iSecurity/PRWEB/pr.war

Anmerkung: Der Pfad muss ein WAR (Webarchiv)-Anwendungsverzeichnis oder eine .war-Datei sein.

☑ Kopieren Sie die Anwendungsdatei ins Anwendungsverzeichnis des Anwendungsservers.

Click on **Continue**


INTAPPSVR > Installierte Anwendungen verwalten > Neue Anwendung installieren

Neue Anwendung installieren

Optionen für Installationsausführung angeben

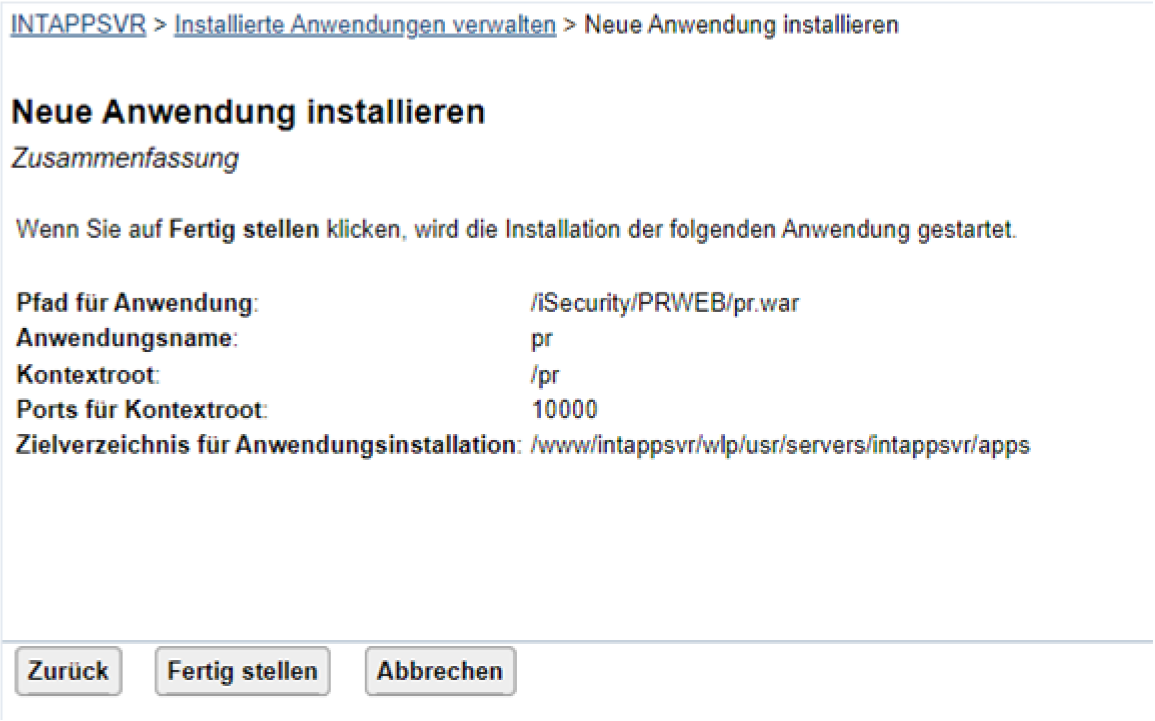
Optionen für Anwendungsimplementierung angeben

Anwendungsname: pr

Kontextroot: /pr e.g. /myContextRoot

Zielverzeichnis für Anwendungsinstallation: /www/intappsvr/wlp/usr/servers/intappsvr/apps

The screen shows your application. Click on **Continue.**



INTAPPSVR > Installierte Anwendungen verwalten > Neue Anwendung installieren

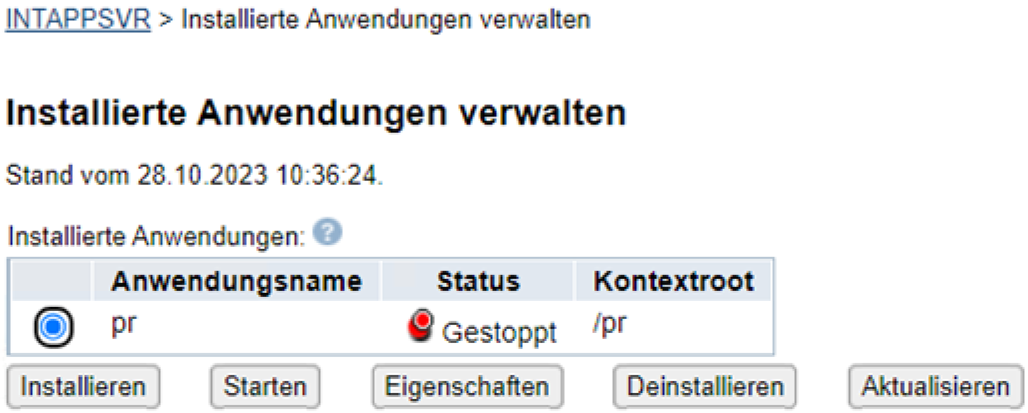
Neue Anwendung installieren

Zusammenfassung

Wenn Sie auf **Fertig stellen** klicken, wird die Installation der folgenden Anwendung gestartet.

Pfad für Anwendung:	/iSecurity/PRWEB/pr.war
Anwendungsname:	pr
Kontextroot:	/pr
Ports für Kontextroot:	10000
Zielverzeichnis für Anwendungsinstallation:	/www/intappsvr/wlp/usr/servers/intappsvr/apps

The screen displays the port that is used for your application. Click on **Complete**



INTAPPSVR > Installierte Anwendungen verwalten

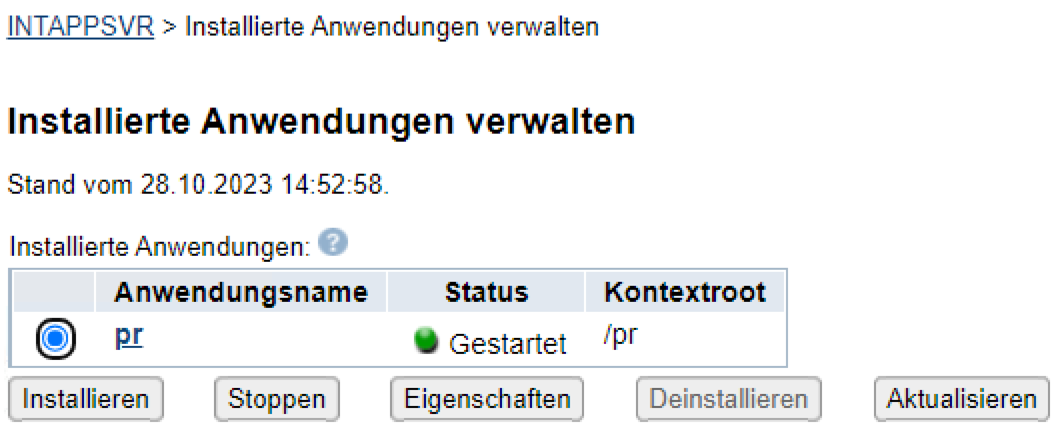
Installierte Anwendungen verwalten

Stand vom 28.10.2023 10:36:24.

Installierte Anwendungen:

	Anwendungsname	Status	Kontextroot
●	pr	● Gestoppt	/pr

The screen shows the application, which is notyet active. To start it, click on **Start**.



INTAPPSVR > Installierte Anwendungen verwalten

Installierte Anwendungen verwalten

Stand vom 28.10.2023 14:52:58.

Installierte Anwendungen:

	Anwendungsname	Status	Kontextroot
◉	pr	● Gestartet	/pr

The screen shows that the application is now active.

Completing Configuration on Tomcat10

Copy the **`pr.war`** file into the **`\apps`** directory and restart the Tomcat webserver.