# iSecurity User Compliance, Native Object Compliance, IFS Compliance

## User Guide
## Version 15.04

www.razlee.com

# 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 User Compliance, Native Object Compliance, IFS ComplianceUser 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.

## Native IBM i (OS/400) User Interface

User Compliance, Native Object Compliance, IFS Compliance is designed to be a user-friendly product for auditors, managers, security personnel and system administrators. The user interface follows standard IBM i CUA conventions. All product features are available via the menus, so you are never required to memorize arcane commands.

Many features are also accessible via the command line, for the convenience of experienced users.

## 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 the previous page.

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

***COMMAND*** **> 81 > 32**

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

## Menus

Product menus allow easy access to all features with a minimum of keystrokes. Menu option numbering and terminology is consistent throughout this product and with other Raz-Lee products. *To* select a menu

option, simply type the option number and press **Enter**. The command line is available from nearly all product menus. If the command line does not appear (and your user profile allows use of the command line), press **F10** to display it.

## 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

(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.



Manual Revised: Thursday, August 29, 2024

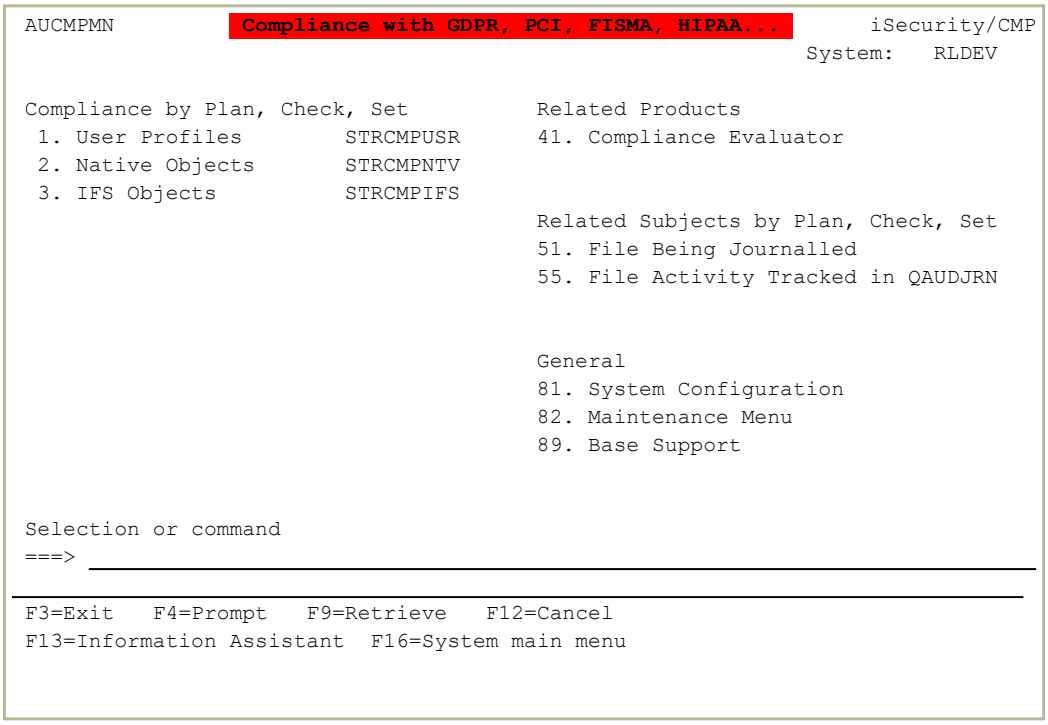
## Contacts

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)

# Working with Compliance

The purpose of this Chapter is to provide the means to access the menu that contains options for maintaining compliance with organizational standards.

To start **Compliance**, type *STRCMP* in the command line. The **Compliance with GDPR, PCI, FISMA, HIPAA** menu appears.




To **define User Compliance**, select **`1. User Profiles`**. The **User Compliance** menu appears, as shown in "Creating Template for User Profiles " on page 11.

To **define Native Objects Compliance**, select **`2. Native Objects`**. The **Native Object Compliance** menu appears, as shown in "Creating Native Object Security Planning" on page 29.

To **define IFS Objects Compliance**, select **`3. IFS Objects`**. The **IFS Object Compliance** menu appears, as shown in "Creating IFS Object Security Template" on page 53.

To **access other related products or subjects**, select what is needed: **`41. Compliance Evaluator`**, **`51. File Being Journalled`**, **`55. File Activity Tracked in QAUDJRN.`**

The following options also have their own chapters within this manual:

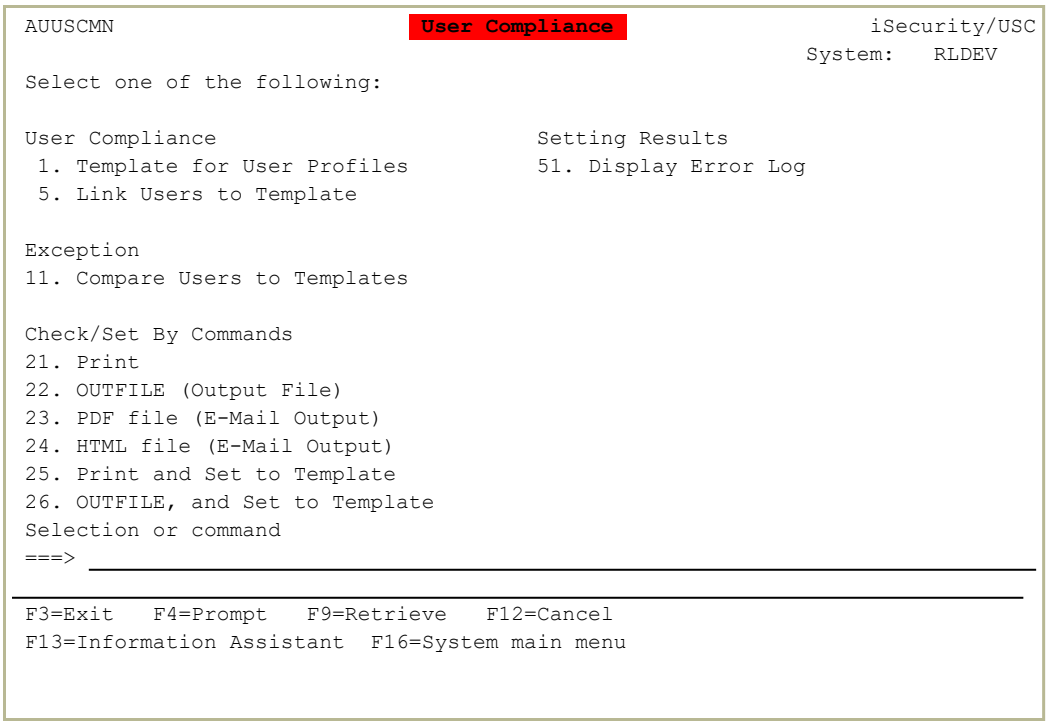
- "Working with User Profiles Compliance" on the next page
- "Working with Native Object Compliance" on page 28
- "Working with IFS Object Compliance" on page 52

# Working with User Profiles Compliance

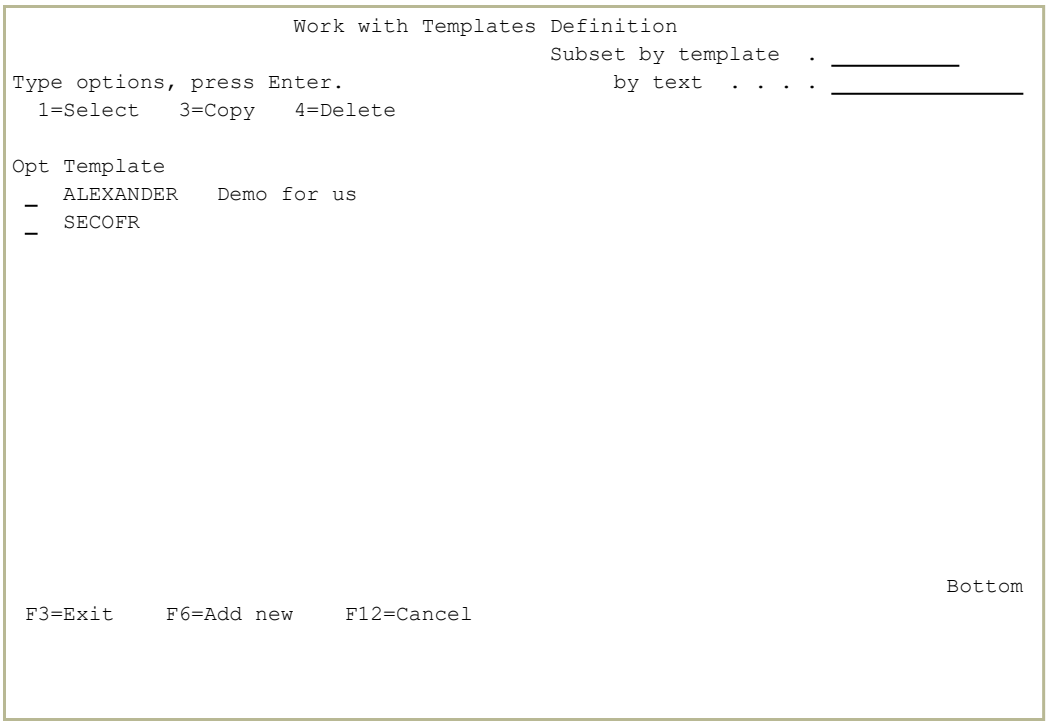
The purpose of this Chapter is to provide the means to create settings for User Profiles Compliance.

## Creating Template for User Profiles

1. To add a User Profile Template, select **`1. User Profiles`** in the **Compliance for PCI, SOX, HIPAA etc.** menu (*STRCMP*).
2. The **User Compliance** menu appears.

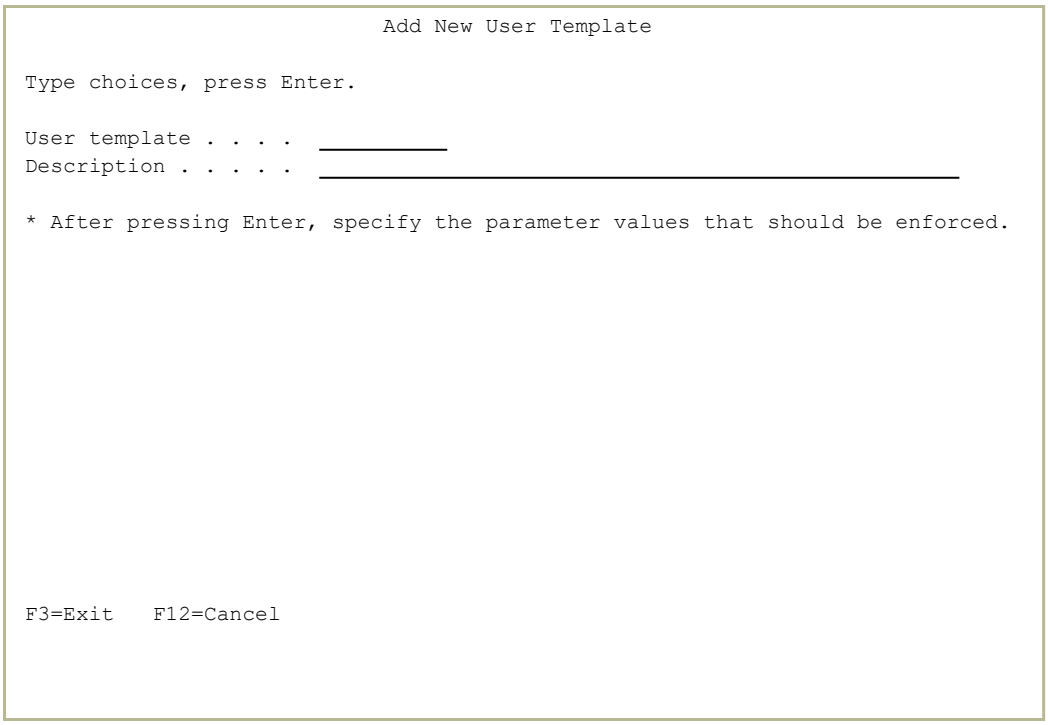



3. Select **`1. Template for User Profiles`**. The **Work with Templates Definition** screen appears.



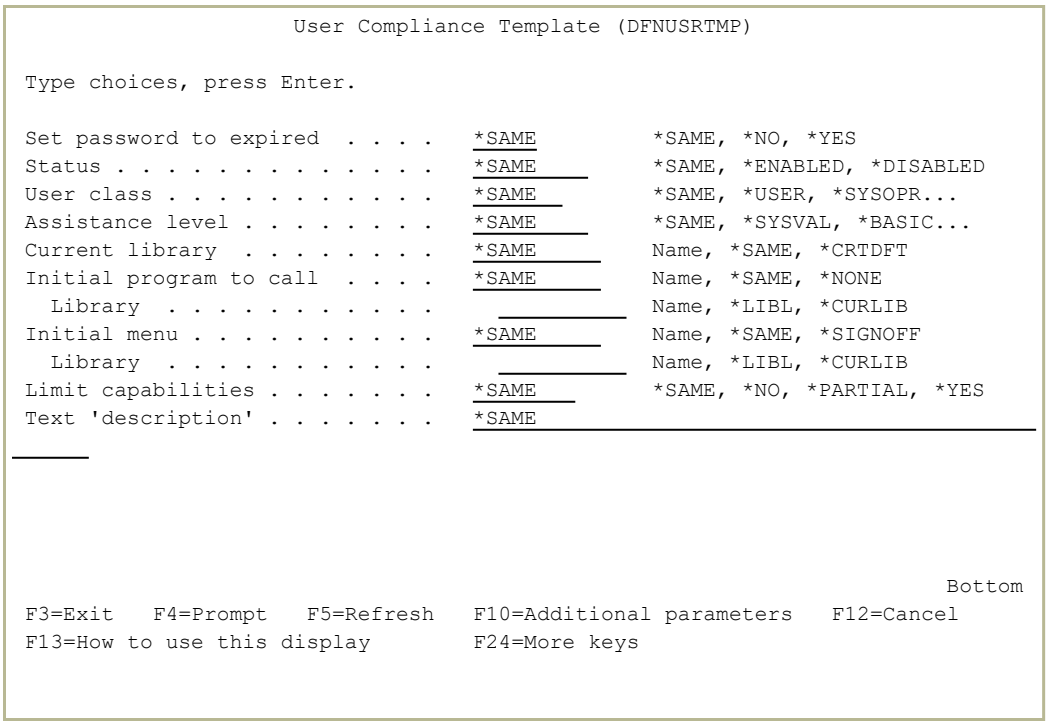

| Parameters | Description |
|---|---|
| 1=Select | Opens the **Modify User Template** screen. |
| 3=Copy | Opens the **Copy User Template** screen. |
| 4=Delete | Opens the **Delete User Template** screen. |
| Template | The Positions in your organization. |
| F6=Add new | Opens the **Add New User Template** screen. |

4. Press **F6** to create a new user template. The **Add New User Template** screen appears.




| Parameters | Description |
|---|---|
| User template | The name of the new User Template. |
| Description | A meaningful description of the template. |

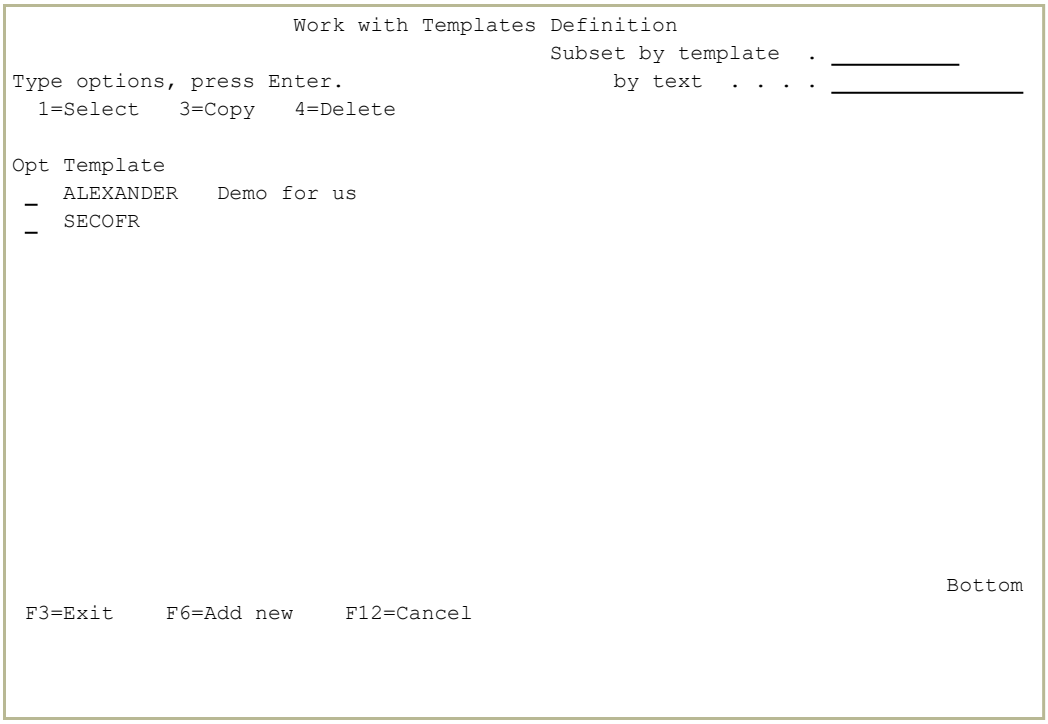
5. Enter relevant data for the **User template** and **Description** parameters and press **Enter**. The **User Compliance Template** screen appears.



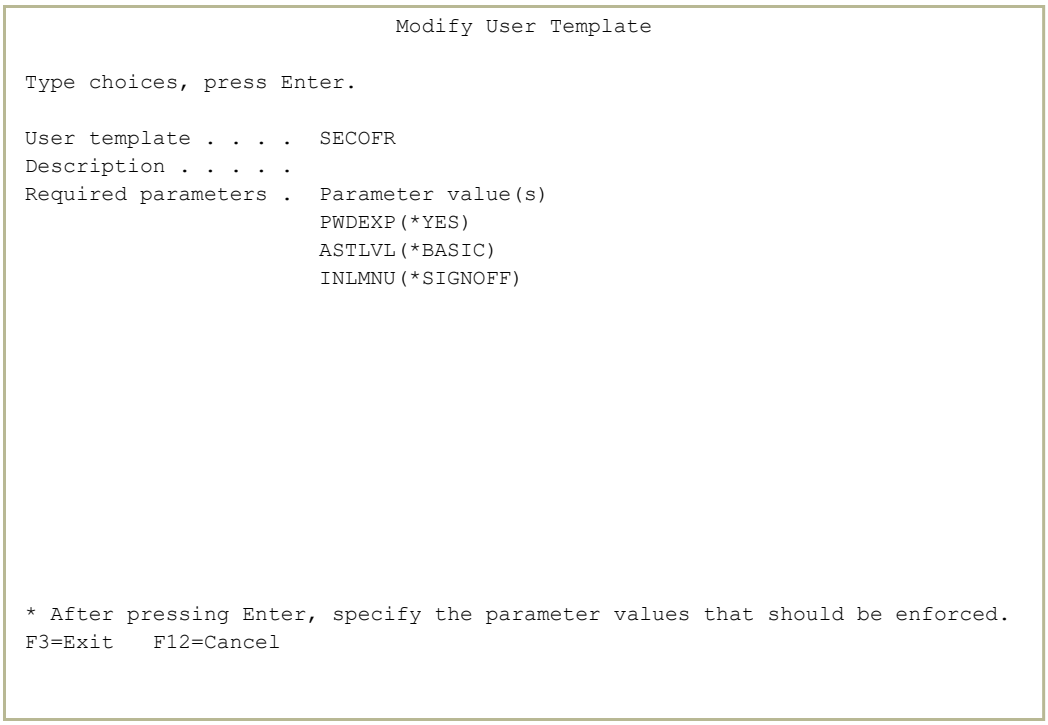

6. Enter required parameters for the template and press **Enter**. The new Template is added and now appears in the **Work with Templates Definition** screen.

## Modifying a Template for User Profiles

1. To modify a User Profile Template, select **`1. Template for User Profiles`** from the **User Compliance** menu (*STRCMP* **`> 1`** ). The **Work with Templates Definitions** screen appears.




2. Select the Template to be modified and press **1=Select**. The **Modify User Template** screen appears.

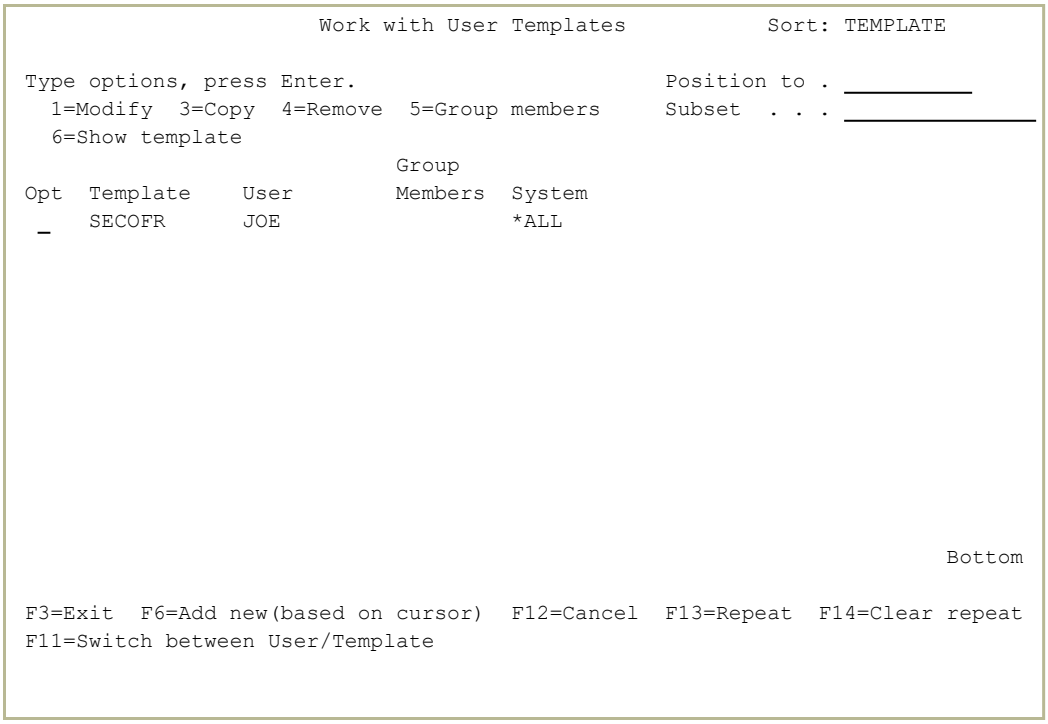



3. Press **Enter**. The **User Compliance Template** screen appears.
4. Enter required parameters for the template and press **Enter**. The Template is modified and now appears in the **Work with Templates Definition** screen.

To copy or delete the template, select the relevant option on the **Work with TemplatesDefinitions** screen.

## Linking Users to Template

1. To link users to templates, select **`5. Link Users to Template`** in the **User Compliance** menu (*STRCMP* **`> 1`**). The **Work with Users Templates** screen appears.




| Parameters | Description |
|---|---|
| 1=Modify | Opens the **`Modify User Template`** screen. |
| 3=Copy | Opens the **`Copy User Template`** screen. |
| 4=Remove | Opens the **`Remove User Template`** screen. |
| Template | The Positions in your organization. |
| F6=Add new | Opens the **`Add User Template`** screen. |

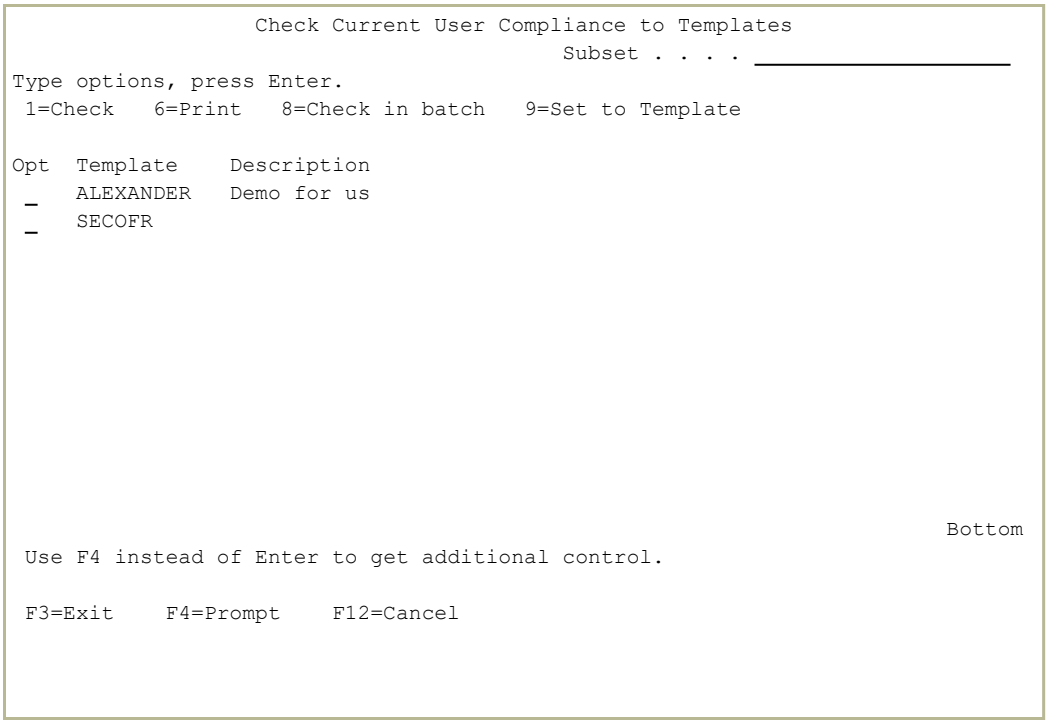
2. Select the relevant parameter to add, modify, copy, or remove.

# Compare Current User Compliance Settings

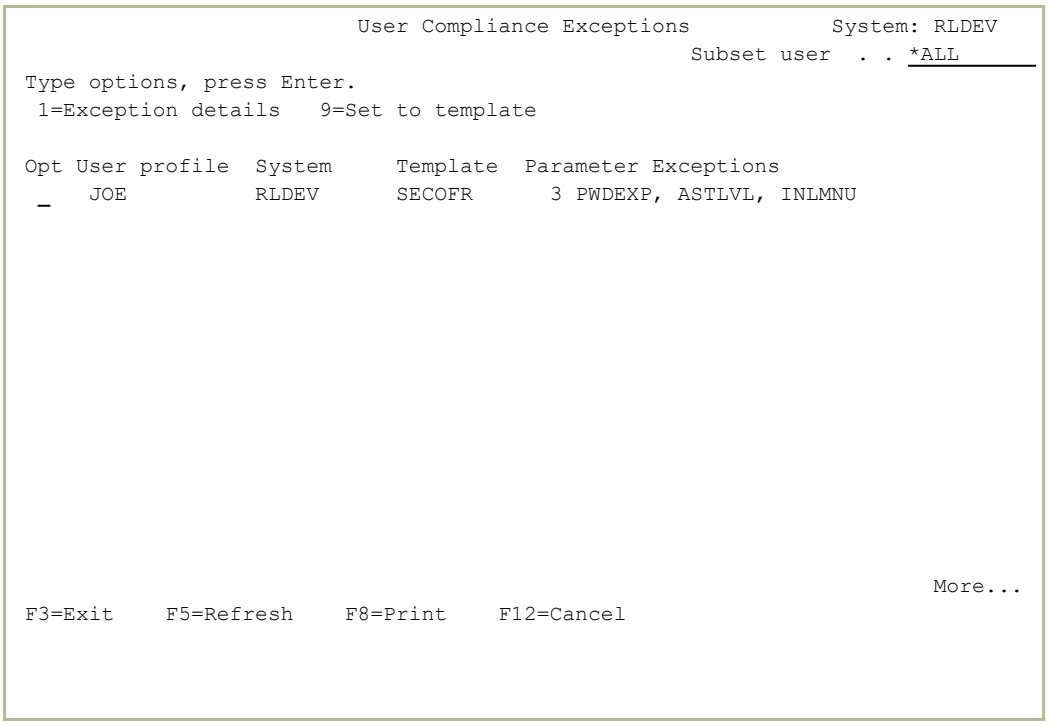
Because you sometimes change security settings due to changing circumstances, it is important to verify regularly that the current security settings match the planned security settings. You can view the settings online or print out a report.

## Display and Update Security Settings

1. Select **`11. Compare Users to Template`** in the User Compliance menu ***(STRCMP > 1)***. The Check Current User Compliance to Templates screen appears.




2. Type **1** to check the objects or **8** to check in batch. The User Compliance Exceptions screen appears.




3. Type **1** to view exception details settings. The new **User Compliance Exceptions** screen appears; the current values appears.

# Check/Set By Commands in User Compliance

The options in this section allow you to check the currents settings and, if necessary, to reset the settings to the template settings. The table below describes the parameters for all of the options in this section.

The options for the parameters shown below include all options for all fields, as this table is for all the Check/Set By Commands. Where the parameter appears with a > next to it, the parameter has been preset and should not be changed.

All the options in this sections are operated by the Work with User Compliance ***WRKUSC*** command.
The parameters of this command are:

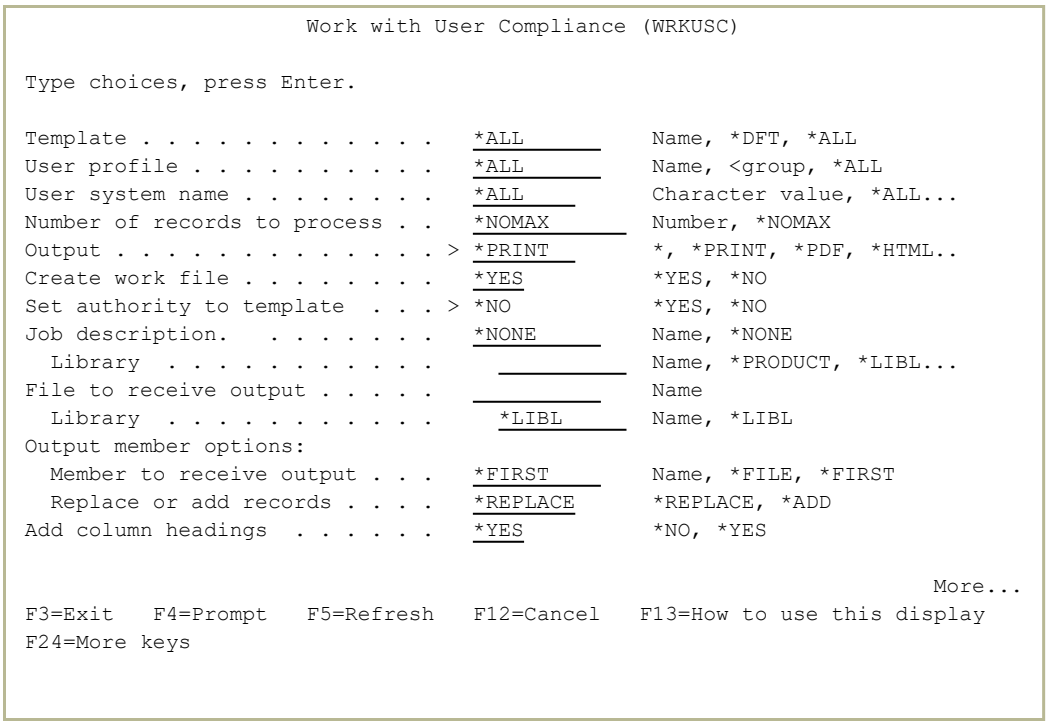
| Parameters | Description |
|---|---|
| Template | Name – Print or output the report for the specified template name.<br>*DFT – Print or output the report for the default template name.<br>*ALL – Print or output the report for all the templates. |
| User profile | Name – Print or output the report for the specified user profile.<br><group – Print or output the report for the specified user profile group .<br>*ALL – Print or output the report for all the user profiles. |
| User system name | *ALL – Print or output the report for all the user system name.<br>Character value - Print or output the report for the specified user system name. |
| Number of records to process | Number – the number of records to process from the input file<br>*NOMAX – process all records |
| Output | *<br>*NONE<br>*PDF<br>*HTML<br>*CSV<br>*OUTFILE<br>*PRINT<br>*PRINT1<br>*PRINT2<br>*PRINT3<br>*PRINT4<br>*PRINT5<br>*PRINT6<br>*PRINT7<br>*PRINT8<br>*PRINT9 |
| Create work file | *YES<br>*NO |

| Parameters | Description |
|---|---|
| Set authority to template | *YES<br>*NO |
| Job description / Library | Name<br>*NONE |
| File to receive output / Library | Name – Enter the name of the Outfile to receive the data in the given Library<br>*AUTO – to create a name for the Outfile in the given Library |
| Output member to receive output | The member to receive the Outfile<br>Name – Enter the name of the member in the Outfile<br>*FIRST – Use the first member of the Outfile<br>*FILE – Use the member with the same name as the Outfile itself |
| Replace or add records | *REPLACE – Replace records in an existing member with the records created now<br>*ADD – Add the records created now to the records that already exist in the member |
| Add column headings | *NO<br>*YES |
| Mail to | Enter the email addresses to receive the Compliance Report |
| Mail text | Enter a text for the mail. |
| Object size to allow attach | Enter the maximum size for the attachment to the email.<br>Number – Enter the maximum size of the attachment in megabytes<br>*NO – Do not allow an attachment<br>*NOMAX – There is no maximum size for the attachment |
| Delete if attached | *NO – Do not delete the original file if attaching it to an email<br>*YES – Delete the original file if attaching it to an email |
| Object | Name – Enter the name of the object<br>*AUTO – to create a name for the object |

| Parameters | Description |
| --- | --- |
| Directory | /iSecurity/report output/<br>*DATE – |

## Print and Send User Security Settings

1. To print User Security Settings, select **21. Print** in the User Compliance menu *(STRCMP > 1)*.. The **Work with User Compliance** screen appears. Enter the parameters for report you need and press Enter.



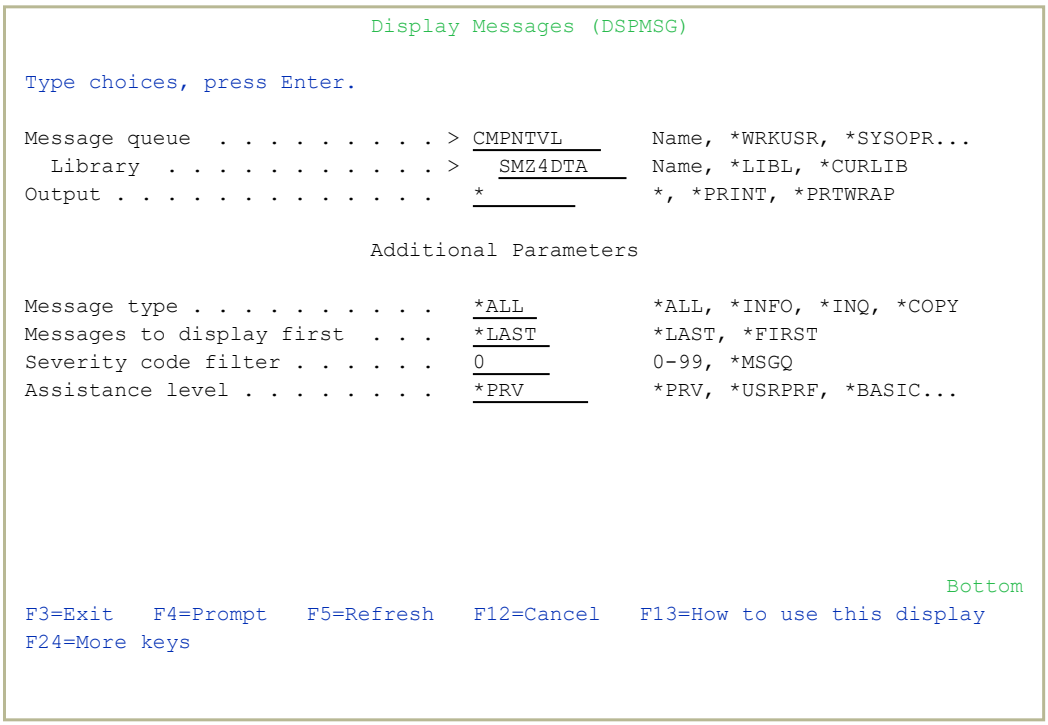
```
                    Work with User Compliance (WRKUSC)

Type choices, press Enter.

Template . . . . . .   *ALL          Name, *DFT, *ALL
User profile . . . . . .   *ALL      Name, <group, *ALL
User system name . . . . . .   *ALL   Character value, *ALL...
Number of records to process . .   *NOMAX      Number, *NOMAX
Output . . . . . . . . . . . . > *PRINT       *, *PRINT, *PDF, *HTML..
Create work file . . . . . .   *YES            *YES, *NO
Set authority to template  . . . > *NO        *YES, *NO
Job description.   . . . . . .   *NONE         Name, *NONE
  Library  . . . . . .              _____      Name, *PRODUCT, *LIBL...
File to receive output . . . . .    _____       Name
  Library  . . . . . .              *LIBL      Name, *LIBL
Output member options:
  Member to receive output . . .   *FIRST       Name, *FILE, *FIRST
  Replace or add records . . . .   *REPLACE     *REPLACE, *ADD
Add column headings  . . . . . .   *YES         *NO, *YES

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

2. To send User Security Settings to an outfile, *STRCMP* **> 1 > 22. OUTFILE (Output File)**. The **Work with User Compliance** screen appears. Enter the parameters for report you need and press Enter.
3. To send User Security Settings in an Email as a PDF or an HTML file, *STRCMP* **> 68 > 1 > 23. PDF file (E-Mail Output)** or *STRCMP* **> 1 > 24. HTML file (E-Mail Output)**. The **Work with User Compliance** screen appears. Enter the parameters for report you need and press Enter.

# Error Log in User Compliance

You can display an Error Log based on a dedicated compliance message queue.

1. Select **`51. Display Error Log`** in the **User Compliance** menu ***(STRCMP > 1).***. The **`Display Messages`** screen appears.



| Parameters | Description |
|---|---|
| Message queue | The message queue that contains the compliance error messages<br>CMPNTVL<br>*WRKUSR<br>*SYSOPR<br>*USRPRF<br>*WRKSTN |
| Library | The Library that contains the message queue<br>Name<br>*LIBL<br>*CURLIB |
| Output | The output format<br>* – Display the output on the screen<br>*PRINT – Send the output to the job's spool queue<br>*PRTWRAP – Send the output to the job's spool queue, where it will be printed without truncation on more than one line |
| Message type | *ALL – Show all messages from the message queue<br>*INFO – Show informational messages only<br>*INQ – Show inquiry messages only<br>*COPY – Show only copies of inquiry messages that were sent to other messages queues and are still waiting for replies |
| Messages to display first | Define the order in which to display the messages<br>*LAST – Show the last (newest) message at the beginning<br>*FIRST – Show the first (oldest) message at the beginning |
| Severity code filter | Only show messages of this severity or higher.<br>0-99 – Specify the value at which messages are shown. If you enter 00, all messages are shown<br>*MSGQ – All messages having a severity code greater than or equal to the severity code specified for the message queue are shown. |
| Assistance level | Define which user interface to display<br>*PRV – The previous user interface used appears<br>*USRPRF – The user interface stored in the current user profile is used<br>*BASIC – The Operational Assistant user interface is used<br>*INTERMED – The system user interface is used |

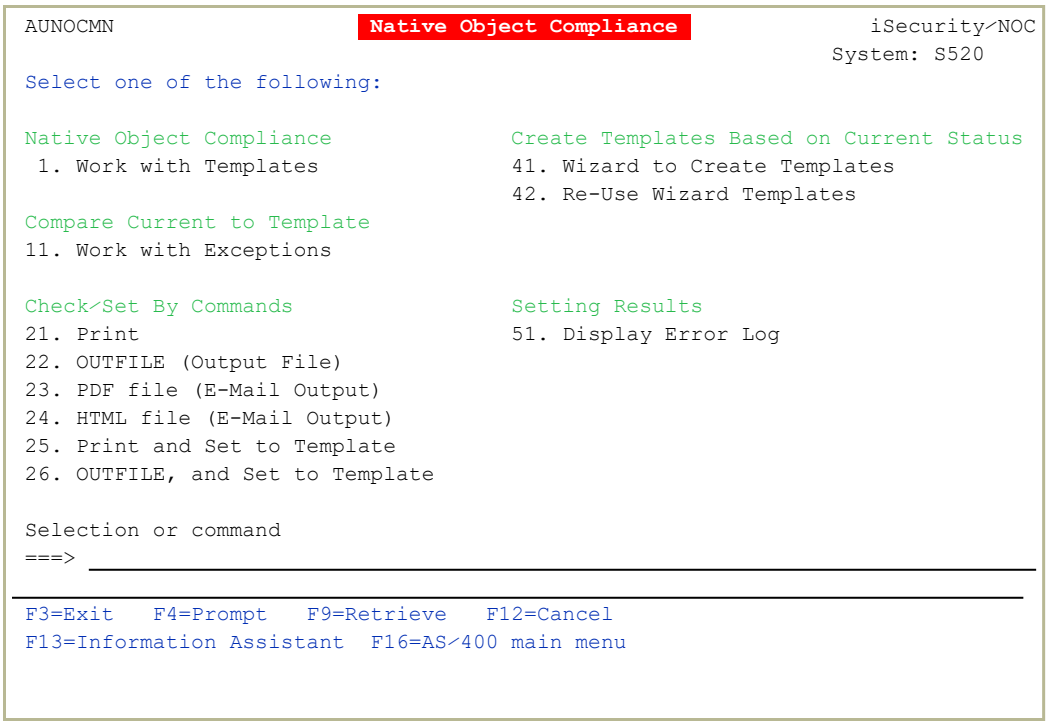
2. Enter the required parameters and press Enter.

# Working with Native Object Compliance

The purpose of this Chapter is to provide the means to create settings for Native Object Compliance.

## Creating Native Object Security Planning

1. To work with Native Object Security, select **`2. Native Objects`** in the **Compliance for PCI, SOX, HIPAA etc.** menu (*STRCMP*).
2. The **Native Object Compliance** menu appears.




3. Select **`1. Work with Templates`**. The **Work with Native Object Security Templates** window appears.

```
                  Work with Native Object Security Templates    System: S520
                                                 Subset Object  . . _________
Type options, press Enter.                         Library . . _________
 1=Select   3=Copy   4=Delete                    Type  . . . . _______
 6=Global template change   9=Explanation        Attribute . . _________
                                                 System  . . . *ALL
                                                                Audit
Opt Library    Type    Object     Attribute  System   Aut. List  Value
 _  QGPL       *ALL    *ALL       *ALL       *ALL                  *NONE
 _  SMZJ       *CMD    *ALL                  S520     *NONE
 _  SMZJ       *DTAARA JADUMP     *ALL       S520     *NONE
 _  SMZJ       *DTAARA JRREL      *ALL       S520     *NONE
 _  SMZJ       *FILE   *ALL       *ALL       S520     *NONE
 _  SMZJ       *MENU   GSLCKMNU   DSPF       S520     SECURITY4P
 _  SMZJ       *MENU   JDMAIN     DSPF       S520     SECURITY4P
 _  SMZJ       *MENU   JRBLJR     DSPF       S520     SECURITY4P
 _  SMZJ       *MENU   JRDAPP     DSPF       S520     SECURITY4P
 _  SMZJ       *MENU   JRDFILE    DSPF       S520     SECURITY4P
 _  SMZJ       *MENU   JRDSET     DSPF       S520     SECURITY4P
 _  SMZJ       *MENU   JRMAIN     DSPF       S520     *NONE
                                                                More...
 F3=Exit   F5=Refresh   F6=Add   F8=Print   F12=Cancel   F13=Repeat   F14=Clear Repeat
```

4. Press **F6** to create a new native object security planning. The **Add Native Object Security Template** screen appears.

```
                    Add Native Object Security Template        System: S520

 Type information, press Enter.

 Object  . . . .  *ALL          Name, generic*, *ALL
   Library . . .  _________     Name
 Type  . . . . .  *ALL         *ALL, *FILE, *PGM, *DTAARA...
 Attribute . . .  *ALL         *ALL, RPGLE, RPG, CLP, DSPF, PF-DTA...
 System  . . . .  *ALL         Name, *ALL


 Note: Type=*ALL is valid only for Object=*ALL.









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

| Parameters | Description |
|---|---|
| Object | Name = enter object name<br>generic* = type the first few letters of the object name and '*' to view a list of optional objects names.<br>*ALL = all the objects in the library |
| Library | Name = enter library name |
| Type | Enter object type.<br>Press **F4** for a full list of types.<br>*ALL is only valid if Object is also *ALL |
| Attribute | Enter object attribute.<br>Press **F4** for a full list of attribute. |
| System | Name = enter the system name<br>*ALL = all systems |

5. Enter the parameters for the object you want to define and press **Enter**. The second **Add Native Object Security Template** appears.

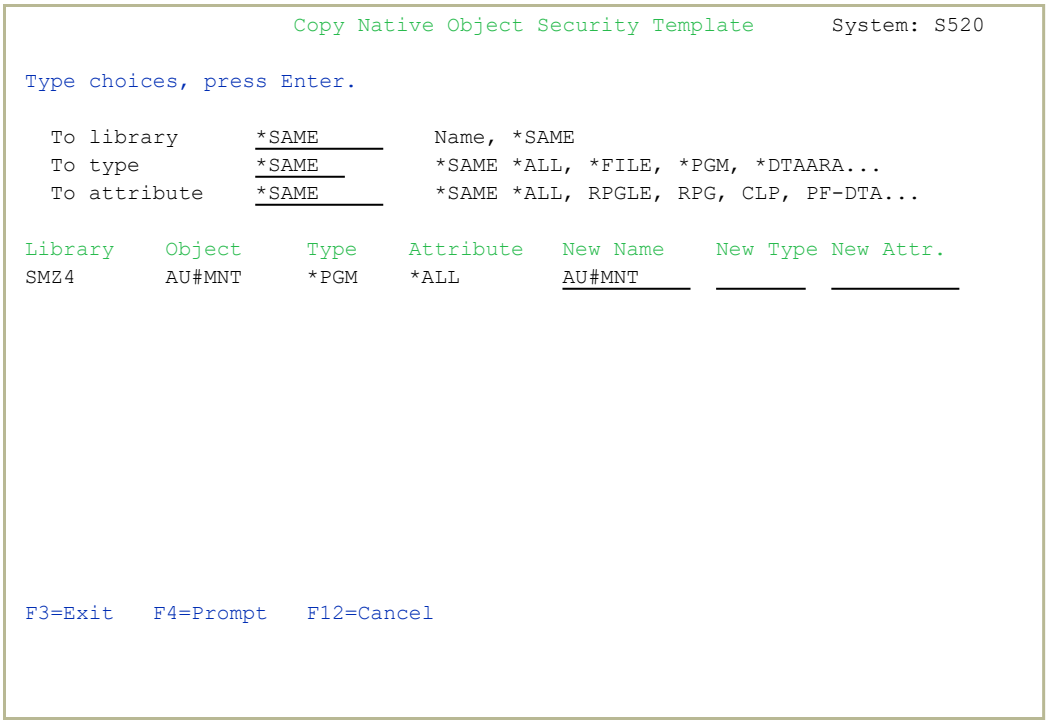
```
                    Add Native Object Security Template       System: S520
Object  . . :  AU#MNT               Type  . . . :  *PGM
  Library . :  SMZ4                 Attribute . :  *ALL
                                    System  . . :  S520
Type information to verify, press Enter. (Blank fields are not verified)
Authorization list  .  __________     Name, *NONE
Owner . . . . . . . .  __________     Name
Primary group . . . .  __________     Name, *NONE
Audit value . . . . .  _______        *USRPRF, *ALL, *CHANGE, *NONE

Replace specific aut.  N              Y=Yes, A=Add, N=No change
           Object   ----------Object-----------  ------------Data------------
User       Authority Opr  Mgt  Exist  Alter  Ref  Read  Add  Upd  Dlt  Execute
__________ _________  _    _     _      _     _     _    _    _    _      _
__________ _________  _    _     _      _     _     _    _    _    _      _
__________ _________  _    _     _      _     _     _    _    _    _      _
__________ _________  _    _     _      _     _     _    _    _    _      _
__________ _________  _    _     _      _     _     _    _    _    _      _
__________ _________  _    _     _      _     _     _    _    _    _      _
__________ _________  _    _     _      _     _     _    _    _    _      _
                                                                      More...
F3=Exit    F4=Prompt    F10=Insert current object authority    F12=Cancel
```

| Parameters | Description |
|---|---|
| Authorization list | Name = enter authorization list name<br>*NONE<br>Press **F4** to view a list of the authorization list |
| Owner | Name = enter object name |
| Primary Group | Another owner of the object<br>Name = enter primary group name<br>*NONE<br>Press **F4** to view a list of groups |
| Audit Value | When to record object access<br>*USRPRF = Every access to the object done by a specific user profile will be recorded<br>*ALL = Every access to the object will be recorded<br>*CHANGE = only changes in the object are recorded<br>*NONE = |
| Replace specific aut. | Y=Yes, replace current authorization<br>A=Add to the current authorizations<br>N=No change |
| User/Object Authority | User = Type a specific User Name or press **F4** to view a list of Users<br>Object Authority =Type one of the following options<br>*ALL<br>*USE<br>*EXCLUDE<br>*CHANGE<br>*AUTL (Only available for User *PUBLIC)<br>Define the actions a user can perform on a specific object within the library:<br>■ Opr = Object operational authority<br>■ Mgt = Object management authority<br>■ Exist = authority to control the object's existence and ownership<br>■ Alter = authority to change the attributes of an object<br>■ Ref = specify the object as the first level in a referential constraint.<br>■ Read = access the object contents<br>■ Add = add entries to the object.<br>■ Upd = change the content of existing entries in the object.<br>■ Dtl = remove entries from the object<br>■ Execute = authority to run a program or search a library or directory. |

6. Enter the parameters for the object you want to define and press **Enter**.

## Copying Native Object Security Template

1. Select **1. Work with Templates** in the Native Object Compliance menu (*STRCMP* **> 2**). The Work with Native Object Security Templates window appears.
2. Enter **3** on each row you want to copy and press **Enter**. The **Copy Native Object Security Template** screen appears.

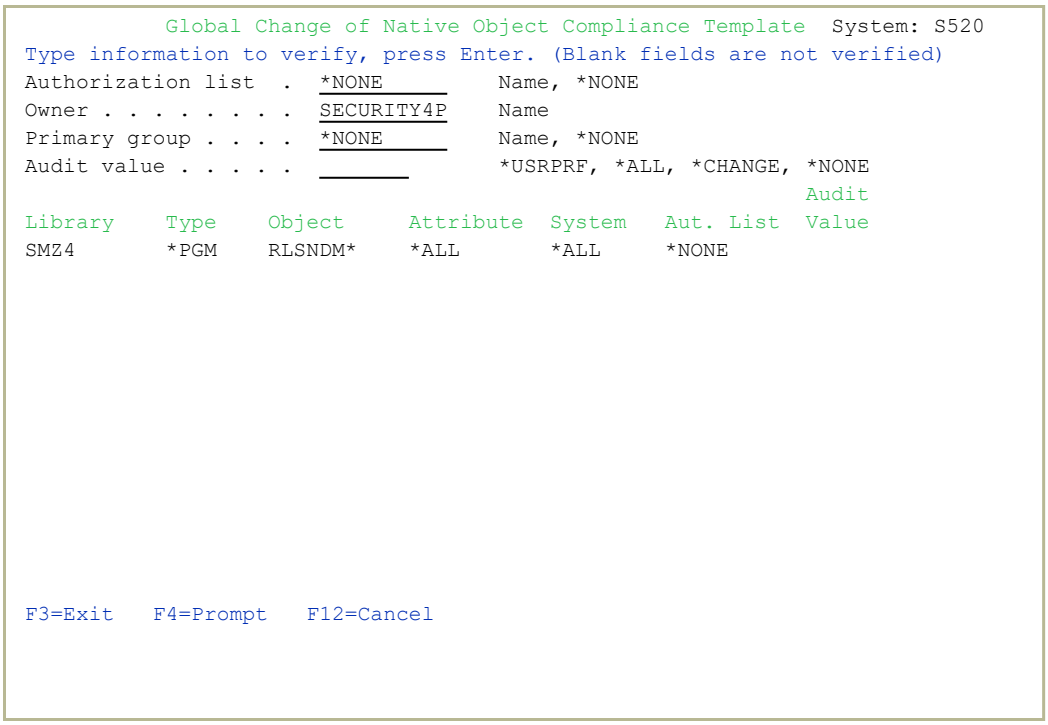



3. Enter the library to which to copy the Native Object Security Planning. In the **Type** field, enter the type or *SAME to leave it unchanged. In the **Attribute** field, enter the attribute or *SAME to leave it unchanged. Press **Enter**.

The data is copied and displayed in the table below, as well as in the updated **Work with Native Object Security Templates** screen.

## Changing Native Object Security Templates

1. Select **`1. Work with Templates`** in the Native Object Compliance menu (*STRCMP* **> 2**). The Work with Native Object Security Templates window appears.
2. To change batches of native object security planning, enter option 6 for each row you want to change and press Enter. The Global Change of Native Object Compliance Template screen appears.




3. For the **`Authorization list`**, **`Owner`**, **`Primary group`** and **`Audit value`**, enter the specific changes to make and press Enter.

The data is changed and displayed in the screen, as well as in the updated Work with Native Object Security Templates screen.

## Compare Current Security to Planned

Because you sometimes change security settings due to changing circumstances, it is important to verify regularly that the current security settings match the planned security settings. You can view the settings online, print out a report, or send them to an OUTFILE which you can analyze later.

## Display and Update Security Settings

1. Select **`11. Work with Exceptions`** in the **Native Object Compliance** menu (*STRCMP* **> 2**). The **Check Current Object Security to Templates** screen appears.

```
                Check Current Object Security to Templates
                                              Subset . . . . _____________________
Type options, press Enter.
 1=Check   6=Print   8=Check in batch   9=Set to Template

Opt  Library
 _   QGPL       General Purpose Library
 _   SMZJ       Security Part 3
 _   SMZO
 _   SMZV       AV Regular
 _   SMZ1
 _   SMZ2
 _   SMZ4       Audit (Security part 2)









                                                                        Bottom
 Use F4 instead of Enter to get additional control.

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

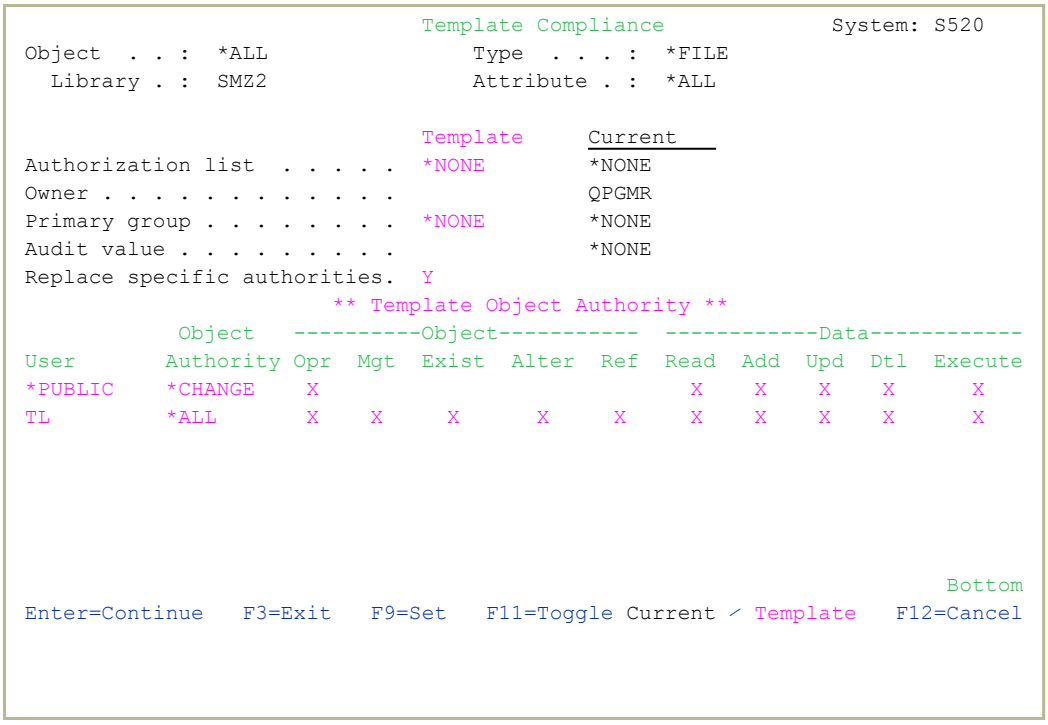
2. Type **1** to check the objects or **8** to check in batch. The **Native Object Security Exceptions** screen appears.

```
                    Native Object Security Exceptions          System: S520
                                                 Subset Object  . . . _________
Type options, press Enter.                                 Library . . _________
 1=Current security    5=Template security                 Type  . . . . _______
 7=Add new template    8=Modify template                   Attribute . . _________
 9=Set to template
Opt Library    Object     Type    Attribute  Exception
 _  SMZ2       CPYFRMPCFM *FILE   DSPF       Owner mismatch.
 _  SMZ2       DEMODTAQ   *FILE   PF-DTA     Owner mismatch.
 _  SMZ2       FSDDSSRC   *FILE   PF-SRC     Missing or mismatch object authori
 _  SMZ2       FSLDTAFM   *FILE   DSPF       Missing or mismatch object authori
 _  SMZ2       FSTMENU    *FILE   DSPF       Missing or mismatch object authori
 _  SMZ2       PRDSTEMP   *FILE   PF-DTA     Missing or mismatch object authori
 _  SMZ2       PSPMSGFM   *FILE   DSPF       Missing or mismatch object authori
 _  SMZ2       PSRDRIFM   *FILE   DSPF       Missing or mismatch object authori
 _  SMZ2       PSRDRRRN   *FILE   PF-DTA     Missing or mismatch object authori
 _  SMZ2       PSRDRUFM   *FILE   DSPF       Missing or mismatch object authori
 _  SMZ2       RMVFM      *FILE   DSPF       Missing or mismatch object authori
 _  SMZ2       SMZPLGFM   *FILE   DSPF       Missing or mismatch object authori
 _  SMZ2       TLDTQF     *FILE   PF-DTA     Missing or mismatch object authori
                                                                        More...
F3=Exit    F8=Print    F12=Cancel
```

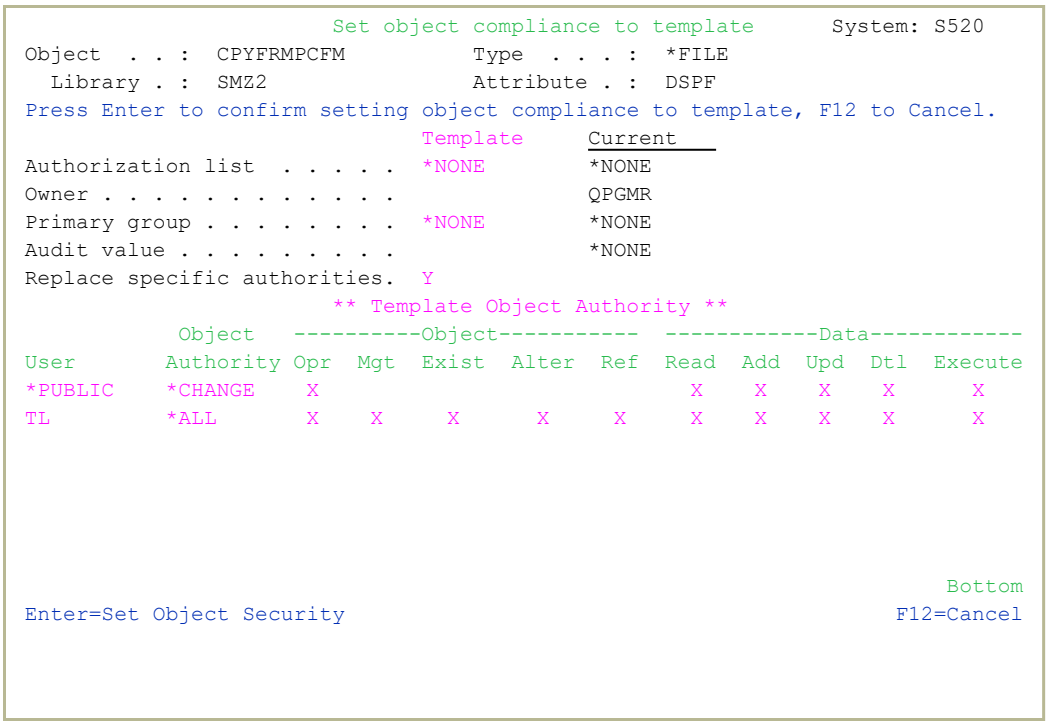
3. Type **1** to view the current security settings. The **Current Object Compliance** screen appears; the mismatch fields appear on a black background. The screen details the current object authority at the bottom of the screen.

```
                          Current Object Compliance            System: S520
Object  . . :  CPYFRMPCFM          Type  . . . :  *FILE
  Library . :  SMZ2                Attribute . :  DSPF

                                Template     Current
Authorization list  . . . . .   *NONE        *NONE
Owner . . . . . . . . . . . .                QPGMR
Primary group . . . . . . . .   *NONE        *NONE
Audit value . . . . . . . . .                *NONE
Replace specific authorities.  Y
                         ** Current Object Authority **
            Object   ----------Object-----------  ------------Data------------
User        Authority Opr  Mgt  Exist  Alter  Ref  Read  Add  Upd  Dtl  Execute
*PUBLIC     *CHANGE    X                              X    X    X    X       X
QPGMR       *ALL       X    X     X      X     X     X    X    X    X       X
                                                                        Bottom
Enter=Continue   F3=Exit   F9=Set   F11=Toggle Current / Template   F12=Cancel
```

4. Type **5** in the **Native Object Security Exceptions** (*STRCMP > 2 > 11 > 1*) screen to view the planned security settings. The **Template Compliance** screen appears; the mismatch fields will appear on a black background. The screen details the template object authority at the bottom of the screen.




5. Type **8** in the **Native Object Security Exceptions** (*STRCMP > 2 > 11 > 1*) screen to modify the object security plan.
6. To adjust the object authorization settings to the plan, type **9** in the **Native Object Security Exceptions (*STRCMP > 2 > 11 > 1*)** screen, and the **Set object compliance to template** screen will appear displaying the planned authorization settings.




7. Press **Enter** to confirm and change single object authority. If there is an error, the following message appears:

"Some settings were NOT set for object <ObjectName> type <ObjectType> in library <LibraryName>"

# Check/Set By Commands

The options in this section allow you to check the currents settings and, if necessary, to reset the settings to the template settings. The table below describes the parameters for all of the options in this section.

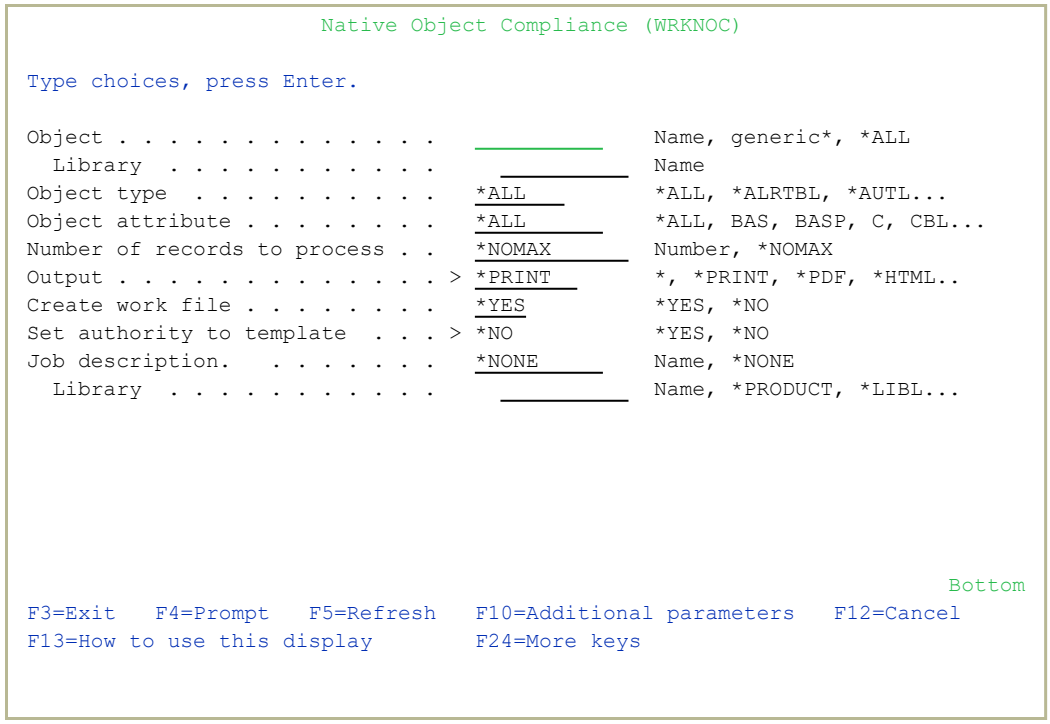
The options for the parameters shown below include all options for all fields, as this table is for all the Check/Set By Commands. Where the parameter appears with a > next to it, the parameter has been preset and should not be changed.

| Parameters | Description |
|---|---|
| Object / Library | Name – Print the report for a specific object only.<br>Generic* – Print the report with all objects whose name starts with the given string in the given library.<br>*ALL – Print the report for all the objects in the library. |
| Object type | *ALL – Print the report for all object types.<br>Name – Print the report for a specific object type only. |
| Object attribute | *ALL – Print the report for all object attributes.<br>Name – Print the report for a specific object attribute only. |
| Number of records to process | Number – the number of records to process from the input file<br>*NOMAX – process all records |
| Output | *<br>*NONE<br>*PDF<br>*HTML<br>*CSV<br>*OUTFILE<br>*PRINT<br>*PRINT1<br>*PRINT2<br>*PRINT3<br>*PRINT4<br>*PRINT5<br>*PRINT6<br>*PRINT7<br>*PRINT8<br>*PRINT9 |
| Create work file | *YES<br>*NO |
| Set authority to template | *YES<br>*NO |
| Job description | Name<br>*NONE |

| Parameters | Description |
|---|---|
| / Library | |
| File to receive output / Library | Name – Enter the name of the Outfile to receive the data in the given Library<br>*AUTO – to create a name for the Outfile in the given Library |
| Output member to receive output | The member to receive the Outfile<br>Name – Enter the name of the member in the Outfile<br>*FIRST – Use the first member of the Outfile<br>*FILE – Use the member with the same name as the Outfile itself |
| Replace or add records | *REPLACE – Replace records in an existing member with the records created now<br>*ADD – Add the records created now to the records that already exist in the member |
| Add column headings | *NO<br>*YES |
| Mail to | Enter the email addresses to receive the Compliance Report |
| Mail text | Enter a text for the mail. |
| Object size to allow attach | Enter the maximum size for the attachment to the email.<br>Number – Enter the maximum size of the attachment in megabytes<br>*NO – Do not allow an attachment<br>*NOMAX – There is no maximum size for the attachment |
| Delete if attached | *NO – Do not delete the original file if attaching it to an email<br>*YES – Delete the original file if attaching it to an email |
| Object | Name – Enter the name of the object<br>*AUTO – to create a name for the object |
| Directory | /iSecurity/NOC –<br>*DATE – |
| User defined data | Internal use only |

## Print Security Settings

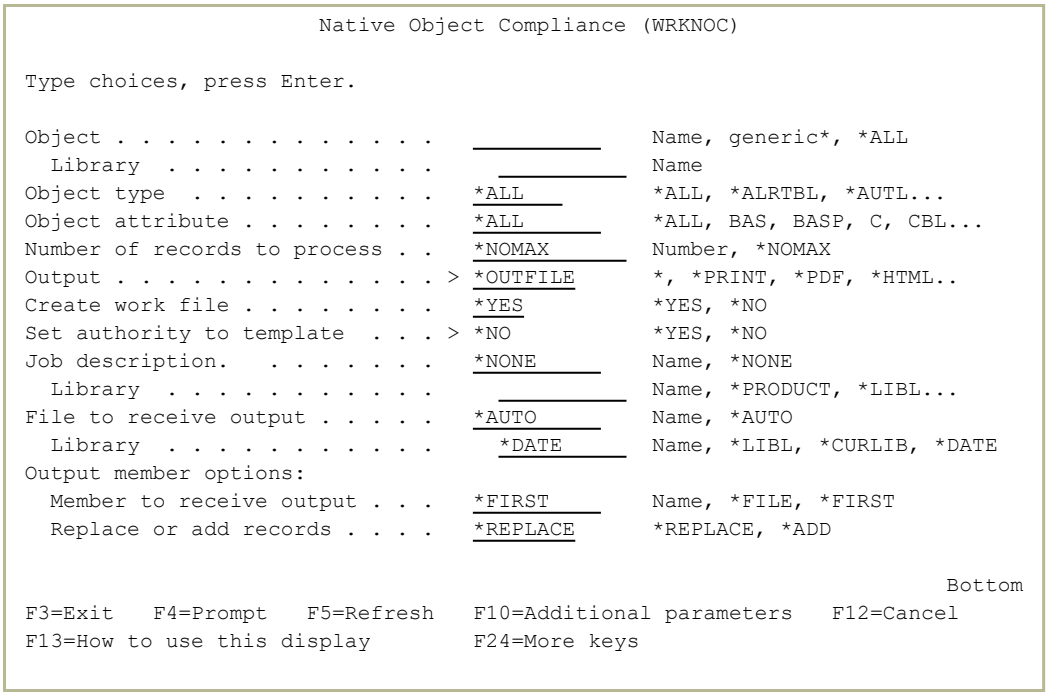
1. Select **21. Print** in the **Native Object Compliance** menu (*STRCMP* **> 2**). The **Native Object Compliance** screen appears.




2. Enter the parameters for report you need and press Enter.

## Send Security Settings to an Outfile

1. Select **`22. OUTFILE (Output File)`** in the Native Object Compliance menu (*STRCMP* **`> 2`**). The **`Native Object Compliance`** screen appears.

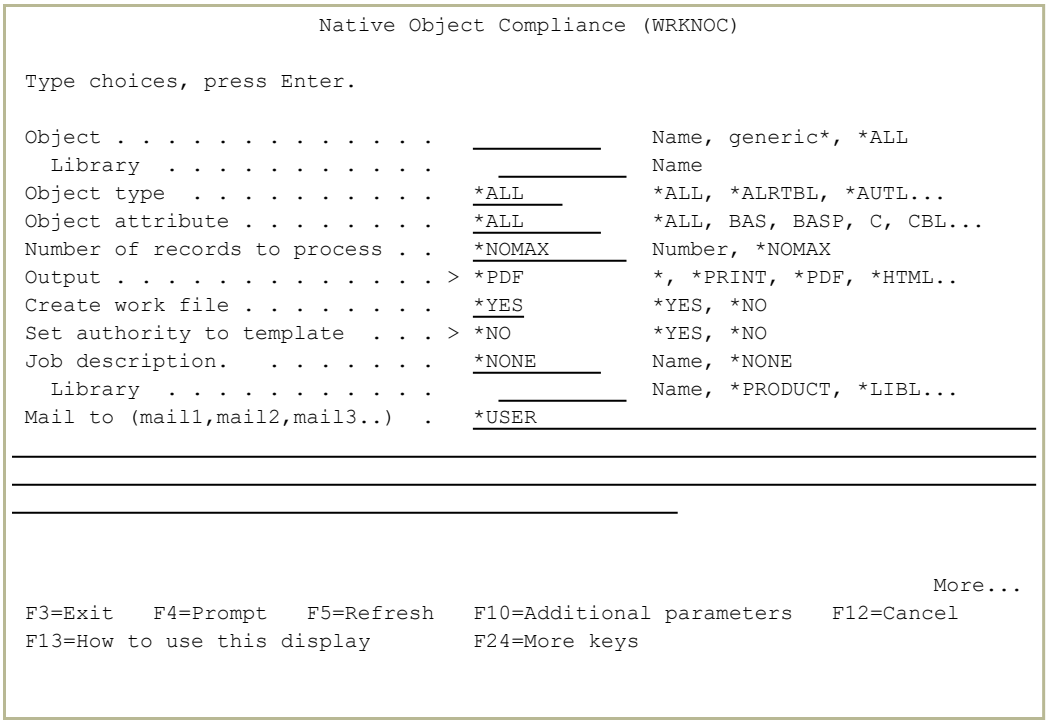


```
                    Native Object Compliance (WRKNOC)

Type choices, press Enter.

Object . . . . . .              __________    Name, generic*, *ALL
  Library  . . . . . .            __________  Name
Object type  . . . . . .        *ALL          *ALL, *ALRTBL, *AUTL...
Object attribute . . . . . .    *ALL          *ALL, BAS, BASP, C, CBL...
Number of records to process .  *NOMAX        Number, *NOMAX
Output . . . . . .            > *OUTFILE      *, *PRINT, *PDF, *HTML..
Create work file . . . . . .    *YES          *YES, *NO
Set authority to template  . . > *NO          *YES, *NO
Job description.   . . . . . .  *NONE        Name, *NONE
  Library  . . . . . .            __________  Name, *PRODUCT, *LIBL...
File to receive output . . . . .  *AUTO       Name, *AUTO
  Library  . . . . . .              *DATE     Name, *LIBL, *CURLIB, *DATE
Output member options:
  Member to receive output . . .  *FIRST       Name, *FILE, *FIRST
  Replace or add records . . . .  *REPLACE     *REPLACE, *ADD

                                                                    Bottom
F3=Exit   F4=Prompt   F5=Refresh   F10=Additional parameters   F12=Cancel
F13=How to use this display        F24=More keys
```

2. Enter the parameters for the report you need and press Enter.

## Send Security Settings in an Email as a PDF or an HTML file

1. Select **`23. PDF file (E-Mail Output)`** or **`24. HTML file (E-Mail Output)`** in the Native Object Compliance menu (*STRCMP* **`> 2`**). The **`Native Object Compliance`** screen appears.




2. Enter the parameters for the report you need and press Enter.

## Enforce Security

1. Select **25. Print and Set to Template** or **26. OUTFILE, and Set to Template** in the **Native Object Compliance** menu (*STRCMP* **> 2**). The **Native Object Compliance** screen appears.

```
                    Native Object Compliance (WRKNOC)

Type choices, press Enter.

Object . . . . . .              _____       Name, generic*, *ALL
  Library  . . . . . .            _____     Name
Object type  . . . . . .        *ALL        *ALL, *ALRTBL, *AUTL...
Object attribute . . . . . .    *ALL        *ALL, BAS, BASP, C, CBL...
Number of records to process . . *NOMAX     Number, *NOMAX
Output . . . . . .           > *PRINT       *, *PRINT, *PDF, *HTML..
Create work file . . . . . .    *YES        *YES, *NO
Set authority to template  . . . > *NO      *YES, *NO
Job description.   . . . . . .  *NONE      Name, *NONE
  Library  . . . . . .            _____     Name, *PRODUCT, *LIBL...

                                                                  Bottom
F3=Exit   F4=Prompt   F5=Refresh   F10=Additional parameters   F12=Cancel
F13=How to use this display        F24=More keys
```

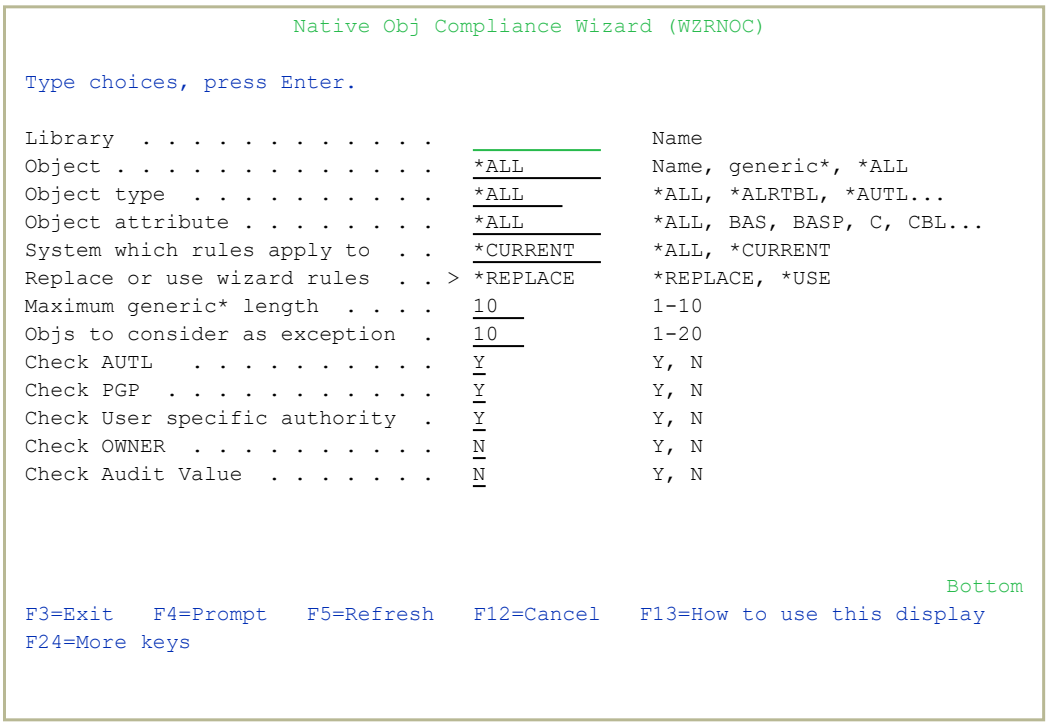
```
                    Native Object Compliance (WRKNOC)

Type choices, press Enter.

Object . . . . . .              _____       Name, generic*, *ALL
  Library  . . . . . .            _____     Name
Object type  . . . . . .        *ALL        *ALL, *ALRTBL, *AUTL...
Object attribute . . . . . .    *ALL        *ALL, BAS, BASP, C, CBL...
Number of records to process . . *NOMAX     Number, *NOMAX
Output . . . . . .           > *OUTFILE     *, *PRINT, *PDF, *HTML..
Create work file . . . . . .    *YES        *YES, *NO
Set authority to template  . . . > *NO      *YES, *NO
Job description.   . . . . . .  *NONE      Name, *NONE
  Library  . . . . . .            _____     Name, *PRODUCT, *LIBL...
File to receive output . . . . .  *AUTO      Name, *AUTO
  Library  . . . . . .            *DATE     Name, *LIBL, *CURLIB, *DATE
Output member options:
  Member to receive output . . .  *FIRST     Name, *FILE, *FIRST
  Replace or add records . . . .  *REPLACE   *REPLACE, *ADD

                                                                  Bottom
F3=Exit   F4=Prompt   F5=Refresh   F10=Additional parameters   F12=Cancel
F13=How to use this display        F24=More keys
```

Since this option is based on the WRKNOC command, it can be scheduled to run when needed to prevent system overload.

# Rules Wizard

Use the Rules Wizard to define rule settings quickly.

1. Select **41. Wizard to Create Rules** in the Native Object Compliance menu (*STRCMP* **> 2**). The **Native Obj Sec Rules Wizard** screen appears.



```
                    Native Obj Compliance Wizard (WZRNOC)

Type choices, press Enter.

Library  . . . . . .                 Name
Object . . . . . .   *ALL            Name, generic*, *ALL
Object type  . . . . . .   *ALL      *ALL, *ALRTBL, *AUTL...
Object attribute . . . . . .   *ALL   *ALL, BAS, BASP, C, CBL...
System which rules apply to  . .   *CURRENT   *ALL, *CURRENT
Replace or use wizard rules  . . > *REPLACE   *REPLACE, *USE
Maximum generic* length  . . . .   10        1-10
Objs to consider as exception  .   10        1-20
Check AUTL  . . . . . .   Y                  Y, N
Check PGP  . . . . . .   Y                   Y, N
Check User specific authority  .   Y         Y, N
Check OWNER  . . . . . .   N                 Y, N
Check Audit Value  . . . . . .   N           Y, N




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

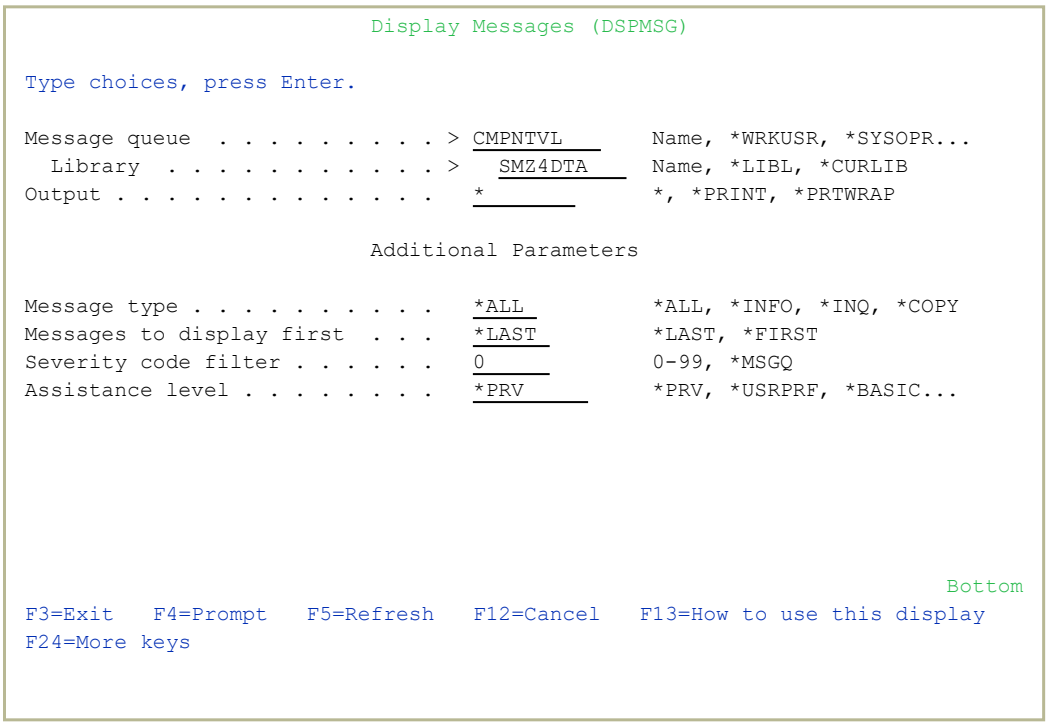
| Parameters | Description |
|---|---|
| Library | The Library that contains the objects on which the rules will apply |
| Object | The object for which the rules will apply.<br>Name – a specific object<br>Generic* - all objects that start with the entry<br>*ALL – all objects |
| Object type | The Object type on which the rules will apply.<br>Enter *ALL or press F4 for a list of object types. |
| Object attribute | The Object attribute on which the rules will apply.<br>Enter *ALL or press F4 for a list of object attributes. |
| System which rules apply to | *CURRENT = The rules will apply only on the current system<br>*ALL = The rules will apply on all systems |
| Replace or use wizard rules | *REPLACE = replace existing rules |
| Maximum generic* length | 1-10 |
| Objs to consider as exception | 1-20 |
| Check AUTL | Y = Yes<br>N = No<br>The default value is Y. |
| Check PGP | Y = Yes<br>N = No<br>The default value is Y. |
| Check User specific authority | Y = Yes<br>N = No<br>The default value is Y. |
| Check OWNER | Y = Yes<br>N = No<br>The default value is N. |
| Check Audit Value | Y = Yes<br>N = No<br>The default value is N. |

2. Enter the required parameters and press Enter.

# Error Log

You can display an Error Log based on a dedicated compliance message queue.

1. Select **`51. Display Error Log`** in the **Native Object Compliance** menu (*STRCMP* **`> 2`**). The **`Display Messages`** screen appears.



| Parameters | Description |
|---|---|
| Message queue | The message queue that contains the compliance error messages<br>CMPNTVL<br>*WRKUSR<br>*SYSOPR<br>*USRPRF<br>*WRKSTN |
| Library | The Library that contains the message queue<br>Name<br>*LIBL<br>*CURLIB |
| Output | The output format<br>* – Display the output on the screen<br>*PRINT – Send the output to the job's spool queue<br>*PRTWRAP – Send the output to the job's spool queue, where it will be printed without truncation on more than one line |
| Message type | *ALL – Show all messages from the message queue<br>*INFO – Show informational messages only<br>*INQ – Show inquiry messages only<br>*COPY – Show only copies of inquiry messages that were sent to other messages queues and are still waiting for replies |
| Messages to display first | Define the order in which to display the messages<br>*LAST – Show the last (newest) message at the beginning<br>*FIRST – Show the first (oldest) message at the beginning |
| Severity code filter | Only show messages of this severity or higher.<br>0-99 – Specify the value at which messages are shown. If you enter 00, all messages are shown<br>*MSGQ – All messages having a severity code greater than or equal to the severity code specified for the message queue are shown. |
| Assistance level | Define which user interface to display<br>*PRV – The previous user interface used appears<br>*USRPRF – The user interface stored in the current user profile is used<br>*BASIC – The Operational Assistant user interface is used<br>*INTERMED – The system user interface is used |

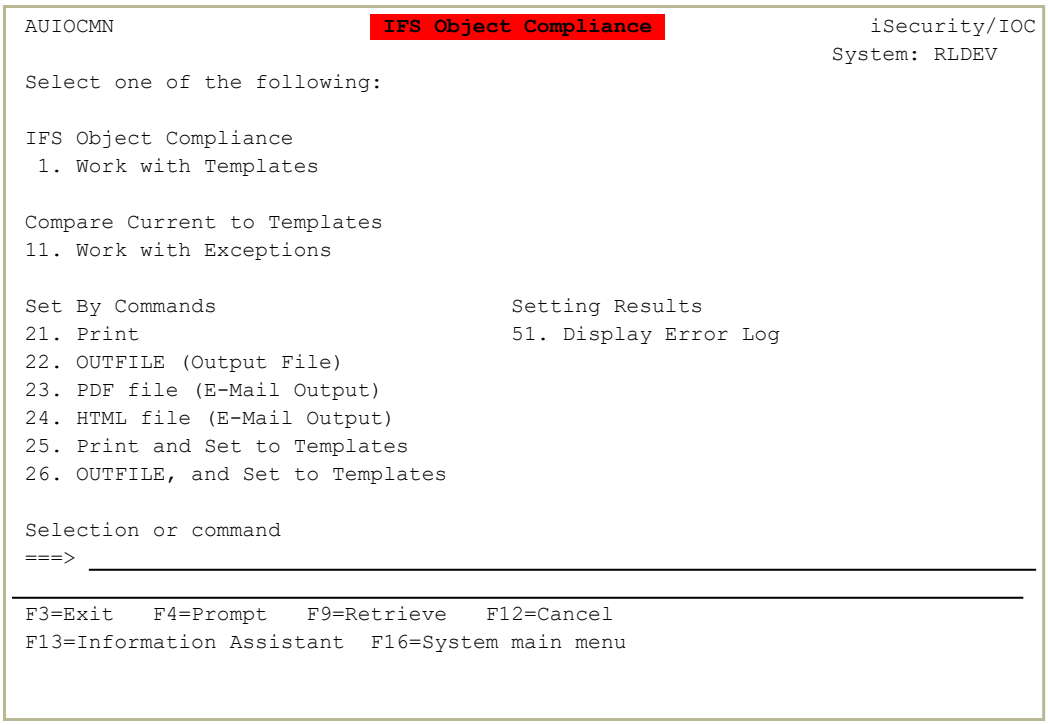
2. Enter the required parameters and press Enter.

# Working with IFS Object Compliance

The purpose of this Chapter is to provide the means to create settings for IFS Object Compliance.

## Creating IFS Object Security Template

1. To work with IFS Object Security Templates, select **`3. IFS Objects`** in the **Compliance for PCI, SOX, HIPAA etc.** menu (*STRCMP*).
2. The **IFS Object Compliance** menu appears.




3. Select **`1. Work with Templates`**. The **Work with IFS Object Security Templates** screen appears.

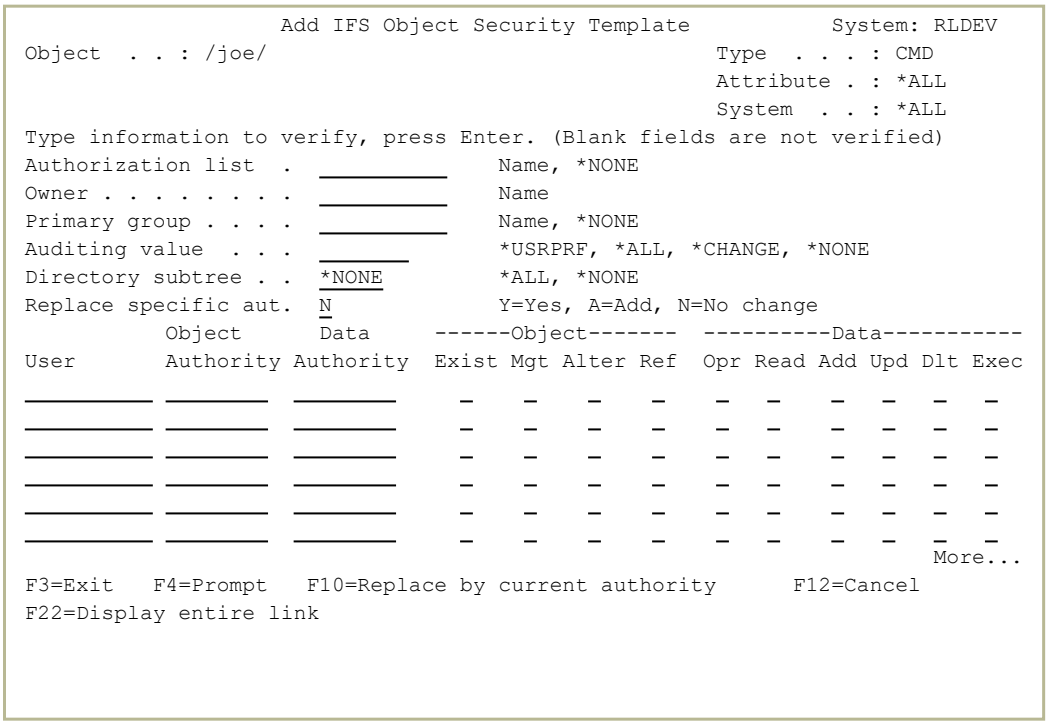
```
                  Work with IFS Object Security Templates      System: RLDEV
                                              Subset Object  . . . _______________
Type options, press Enter.                      Type  . . . . _______
 1=Select 3=Copy 4=Delete 6=Global template chg.  Attribute . . _________
 7=Display Authority      9=Compliance           System  . . . *ALL____

                                                                      Directory
   Object Link                                  Type/Attr. System   Subtree
_  *ALL                                         *ALL       *ALL     *NONE
_  /alex/                                       STMF       *ALL     *NONE
_  /tmp/                                        STMF       *ALL     *NONE

                                                                          Bottom
 F3=Exit F5=Refresh F6=Add new F8=Print F12=Cancel F13=Repeat F14=Clear Repeat
 F22=Display entire link
```

4. Press **F6** to create a new IFS object security planning. The **Add IFS Object Security Template** screen appears.

```
                      Add IFS Object Security Template         System: RLDEV

 Type information, press Enter.

 Object  . . . . .   *ALL_____________________________
                     _____________________________
                     _____________________________
                     _____________________________
                     _____________________________
                     _____________________________
                     _____________________________

 Type  . . . . . .   *ALL____                      *ALL, DIR, STMF, FILE...
 Attribute . . . .   *ALL_____                     *ALL, DOC, ZIP, PF-DTA...
 System  . . . . .   *ALL____                      *ALL, Name
 Directory subtree   *NONE                         *ALL, *NONE


 Type=*ALL is valid only for Object=*ALL.
 It is not recommended to mix Directory subtree *ALL and *NONE for same tree.

 F3=Exit   F4=Prompt   F12=Cancel   F22=Display entire object
```

| Parameters | Description |
|---|---|
| Object | *ALL = all the objects in the library |
| Type | Enter object type.<br>Press **F4** for a full list of types.<br>*ALL is only valid if Object is also *ALL |
| Attribute | Enter object attribute.<br>Press **F4** for a full list of attribute. |
| System | Name = enter the system name<br>*ALL = all systems |

5. Enter the parameters for the object you want to define and press **Enter**. The second **Add IFS Object Security Template** appears.



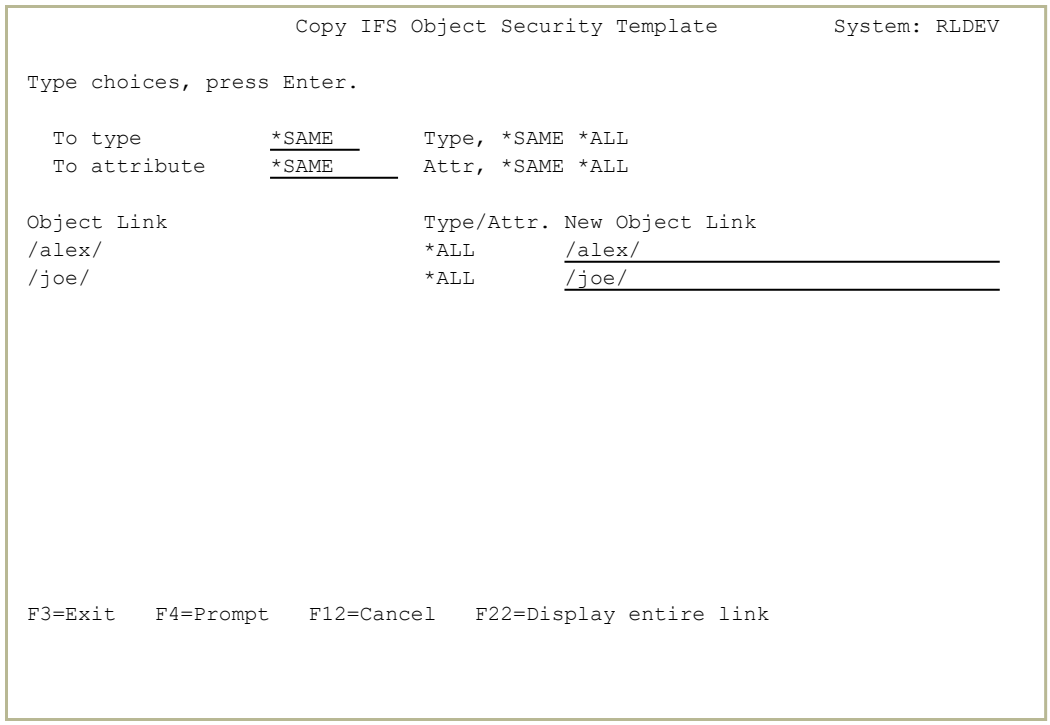
```
                    Add IFS Object Security Template           System: RLDEV
Object  . . : /joe/                                  Type  . . . : CMD
                                                     Attribute . : *ALL
                                                     System  . . : *ALL
Type information to verify, press Enter. (Blank fields are not verified)
Authorization list  .  __________    Name, *NONE
Owner . . . . . . . .  __________    Name
Primary group . . . .  __________    Name, *NONE
Auditing value  . . .  _______       *USRPRF, *ALL, *CHANGE, *NONE
Directory subtree . .  *NONE         *ALL, *NONE
Replace specific aut.  N             Y=Yes, A=Add, N=No change
           Object      Data     ------Object-------  ----------Data-----------
User       Authority Authority  Exist Mgt Alter Ref  Opr Read Add Upd Dlt Exec
__________ _________ _________    _    _    _    _    _   _    _   _   _   _
__________ _________ _________    _    _    _    _    _   _    _   _   _   _
__________ _________ _________    _    _    _    _    _   _    _   _   _   _
__________ _________ _________    _    _    _    _    _   _    _   _   _   _
__________ _________ _________    _    _    _    _    _   _    _   _   _   _
__________ _________ _________    _    _    _    _    _   _    _   _   _   _
                                                                        More...
F3=Exit   F4=Prompt   F10=Replace by current authority      F12=Cancel
F22=Display entire link
```

| Parameters | Description |
|---|---|
| Authorization list | Name = enter authorization list name<br>*NONE<br>Press **F4** to view a list of the authorization list |
| Owner | Name = enter User's name |
| Primary Group | Another owner of the object<br>Name = enter primary group name<br>*NONE<br>Press **F4** to view a list of groups |
| Auditing Value | When to record object access<br>*USRPRF = Every access to the object done by a specific user profile will be recorded<br>*ALL = Every access to the object will be recorded<br>*CHANGE = only changes in the object are recorded<br>*NONE = |
| Replace specific aut. | Y=Yes, replace current authorization<br>A=Add to the current authorizations<br>N=No change |
| User/Object Authority | User = Type a specific User Name or press **F4** to view a list of Users<br>Object Authority =Type one of the following options<br>*ALL<br>*NONE<br>Data Authority =Type one of the following options<br>*RWX<br>*RX<br>*RW<br>*WX<br>*R<br>*W<br>*X<br>*EXCLUDE<br>*NONE<br>*AUTL (for *PUBLIC only)<br>Define the actions a user can perform on a specific object within the library:<br>■ Exist = authority to control the object's existence and ownership<br>■ Mgt = Object management authorit<br>■ Alter = authority to change the attributes of an object<br>■ Ref = specify the object as the first level in a referential constraint.<br>■ Opr = Object operational authority<br>■ Read = access the object contents<br>■ Add = add entries to the object.<br>■ Upd = change the content of existing entries in the object.<br>■ Dtl = remove entries from the object<br>■ Execute = authority to run a program or search a library or directory. |

6. Enter the parameters for the object you want to define and press **Enter**.

## Copying IFS Object Security Template

1. Select **`1. Work with Templates`** in the **IFS Object Security** menu *(STRCMP* **`> 3`**). The **Work with IFS Object Security Templates** window appears.
2. Enter **3** on each row you want to copy and press **Enter**. The **Copy IFS Object Security Template** screen appears.

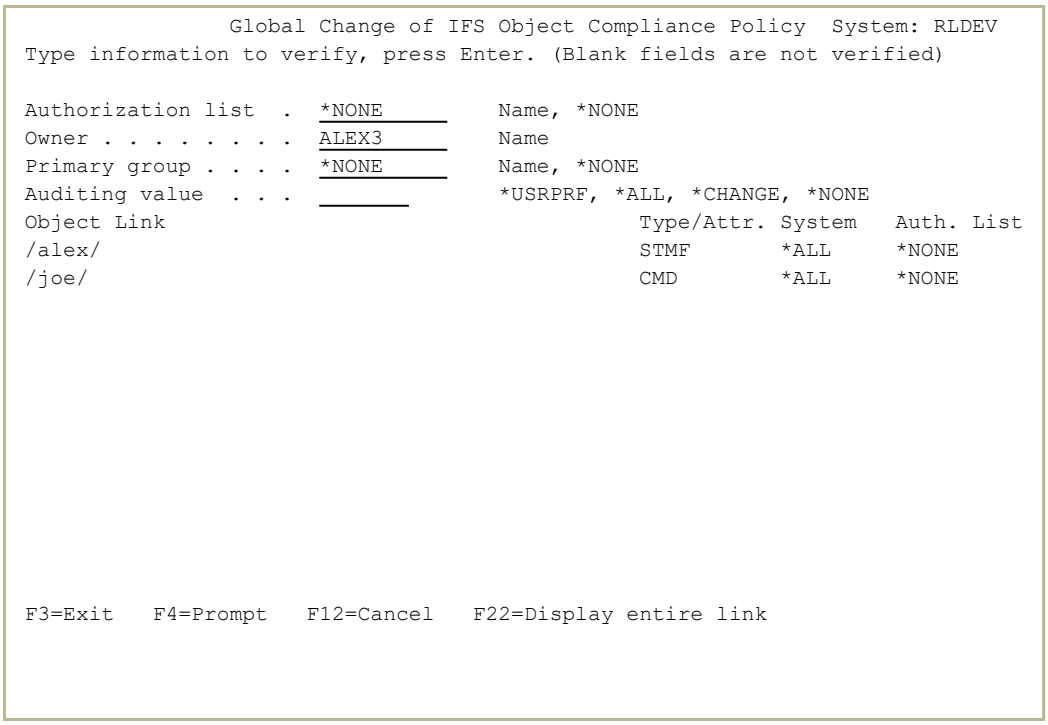



3. In the **`Type`** field, enter the type or `*SAME` to leave it unchanged. In the **`Attribute`** field, enter the attribute or `*SAME` to leave it unchanged. Press **Enter**.

The data is copied and displayed in the table below, as well as in the updated **Work with IFS Object Security Templates** screen.

## Changing IFS Object Security Templates

1. Select **`1. Work with Templates`** in the IFS Object Security menu *(STRCMP* **`>`** **`3`**). The Work with IFS Object Security Templates screen appears.
2. To change batches of IFS object security planning, enter option **6** for each row you want to change and press Enter. The Global Change of IFS Object Compliance Policy screen appears.

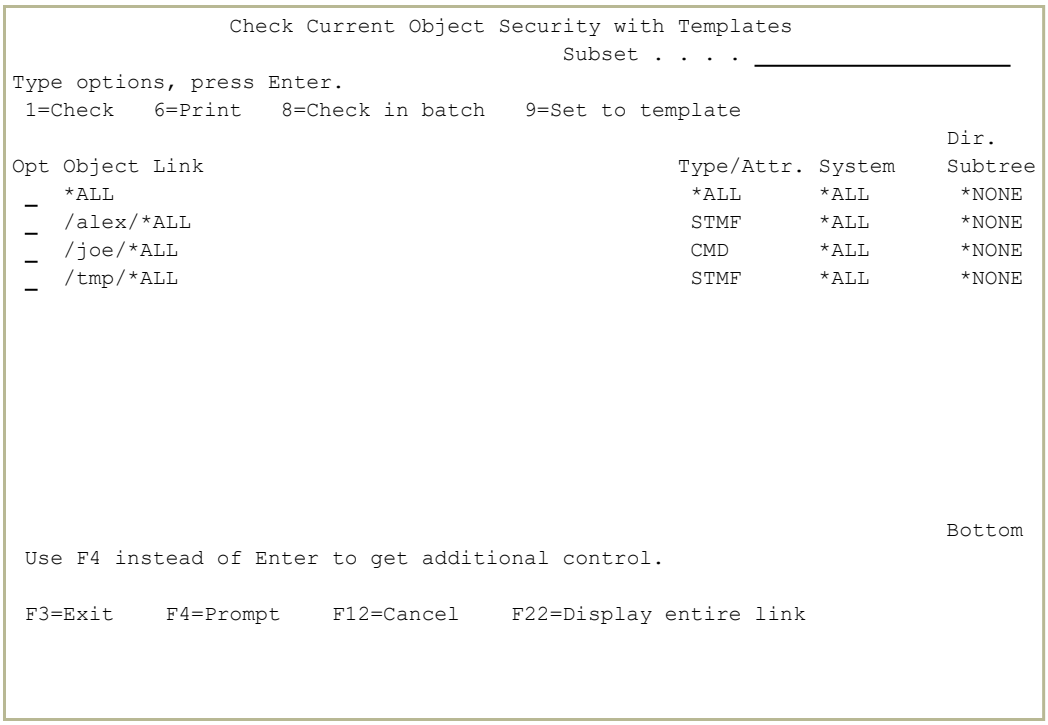



3. For the **`Authorization list`**, **`Owner`**, **`Primary group`** and **`Aduititing value`**, enter the specific changes to make and press Enter.

The data is changed and displayed in the screen, as well as in the updated Work with IFS Object Security Templates screen.

## Display and Update IFS Object Security Settings

1. Select **`11. Work with Exceptions`** in the IFS Object Security menu *(STRCMP > 3)*. The Check Current Object Security with Templates screen appears.



```
                Check Current Object Security with Templates
                                          Subset . . . . _____________________
Type options, press Enter.
 1=Check   6=Print   8=Check in batch   9=Set to template
                                                                        Dir.
Opt Object Link                                    Type/Attr. System    Subtree
 _  *ALL                                            *ALL      *ALL       *NONE
 _  /alex/*ALL                                      STMF      *ALL       *NONE
 _  /joe/*ALL                                       CMD       *ALL       *NONE
 _  /tmp/*ALL                                       STMF      *ALL       *NONE
                                                                        Bottom
 Use F4 instead of Enter to get additional control.

 F3=Exit    F4=Prompt    F12=Cancel    F22=Display entire link
```

2. Type **1** to check the objects or **8** to check in batch. The IFS Object Security Exceptions screen appears.
3. Type **1** to view the current security settings. The Current Object Compliance screen appears; the mismatch fields appear on a black background. The screen details the current object authority at the bottom of the screen.
4. Type **5** in the IFS Object Security Exceptions screen to view the planned security settings. The Template Compliance screen appears; the mismatch fields will appear on a black background. The screen details the template object authority at the bottom of the screen.
5. Type **8** in the IFS Object Security Exceptions screen to modify the object security plan.

6. To adjust the object authorization settings to the plan, type **9** in the **IFS Object Security Exceptions** screen, and the **Set object compliance to template** screen will appear displaying the planned authorization settings.
7. Press **Enter** to confirm and change single object authority.

# Set By Commands

The options in this section allow you to check the currents settings and, if necessary, to reset the settings to the template settings. The table below describes the parameters for all of the options in this section.

The options for the parameters shown below include all options for all fields, as this table is for all the Set By Commands. Where the parameter appears with a > next to it, the parameter has been preset and should not be changed.

| Parameters | Description |
|---|---|
| IFS Object Directory | Print the report for a specified IFS Object Directory. |
| Object type | *ALL – Print the report for all object types.<br>Name – Print the report for a specific object type only.<br>Press F4 for a list of object types. |
| Object attribute | *ALL – Print the report for all object attributes.<br>Name – Print the report for a specific object attribute only.<br>Press F4 for a list of object types. |
| Number of records to process | Number – the number of records to process from the input file<br>*NOMAX – process all records |
| Output | *<br>*NONE<br>*PDF<br>*HTML<br>*CSV<br>*OUTFILE<br>*PRINT<br>*PRINT1<br>*PRINT2<br>*PRINT3<br>*PRINT4<br>*PRINT5<br>*PRINT6<br>*PRINT7<br>*PRINT8<br>*PRINT9 |
| Create work file | *YES<br>*NO |
| Set authority to template | *YES<br>*NO |
| Job description | Name<br>*NONE |

| Parameters | Description |
|---|---|
| / Library | |
| File to receive output / Library | Name – Enter the name of the Outfile to receive the data in the given Library<br>*AUTO – to create a name for the Outfile in the given Library |
| Output member options | The member to receive the Outfile<br>Name – Enter the name of the member in the Outfile<br>*FIRST – Use the first member of the Outfile<br>*FILE – Use the member with the same name as the Outfile itself |
| Replace or add records | *REPLACE – Replace records in an existing member with the records created now<br>*ADD – Add the records created now to the records that already exist in the member |
| Mail to | Enter the email addresses to receive the Compliance Report |
| Mail text | Enter a text for the mail. |
| Object size to allow attach | Enter the maximum size for the attachment to the email.<br>Number – Enter the maximum size of the attachment in megabytes<br>*NO – Do not allow an attachment<br>*NOMAX – There is no maximum size for the attachment |
| Delete if attached | *NO – Do not delete the original file if attaching it to an email<br>*YES – Delete the original file if attaching it to an email |
| Object | Name – Enter the name of the object<br>*AUTO – to create a name for the object |
| Directory | /iSecurity/report output/<br>*DATE |

## Print and Send Security Settings

1. To print IFS Object Compliance settings, select **21. Print** in the IFS Object Security menu *(STRCMP* **> 3**). The **IFS Object Compliance** screen appears. Enter the parameters for report you need and press Enter.

```
                        IFS Object Compliance (WRKIOC)

Type choices, press Enter.

IFS Object Directory . . . . . _____________________________________________
_____________________________________________________________________________
_______
Object type  . . . . . .  *ALL___       *ALL, AUTL, BLKSF, CFGL...
Object attribute . . . . . *ALL_____    *ALL, BAS, BASP, C, CBL...
Number of records to process . . *NOMAX_____  Number, *NOMAX
Output . . . . . > *PRINT       *, *PRINT, *PDF, *HTML..
Directory subtree  . . . . . *NONE      *ALL, *NONE
Create work file . . . . . *YES         *YES, *NO
Set authority to template  . . . > *NO  *YES, *NO
Job description.   . . . . . *NONE_____ Name, *NONE
  Library  . . . . . _____      Name, *PRODUCT, *LIBL...




                                                                      Bottom
F3=Exit   F4=Prompt   F5=Refresh   F10=Additional parameters   F12=Cancel
F13=How to use this display        F24=More keys
```

2. To send IFS Object Compliance settings to an outfile, *STRCMP* **> 3 > 22. OUTFILE (Output File)**. The **IFS Object Compliance** screen appears. Enter the parameters for report you need and press Enter.
3. To send IFS Object Compliance settings in an Email as a PDF or an HTML file, *STRCMP* **> 3 23. PDF file (E-Mail Output)** or *STRCMP* **> 68 > 3 > 24. HTML file (E-Mail Output)**. The **IFS Object Compliance** screen appears. Enter the parameters for report you need and press Enter.