NetIQ Security Solutions for IBM i
TGSecure 2.1
User Guide

Revised August 2019

Legal Notice

Table of Contents

TABLE OF CONTENTS ..... **III**

1. INTRODUCTION **15**

1.1. HISTORICAL PERSPECTIVE OF SECURITY 15
1.2. TGSECURE OVERVIEW 15
1.3. FEATURES 16
1.4. RULES DECISION ALGORITHM 17
1.5. RULES SUGGESTION ENGINE 18

2. GETTING STARTED **21**

2.1. LOG INTO TGSECURE 21
2.2. GETTING STARTING USING TGSECURE 21
2.2.1. Actions *21*
2.2.2. Process Flow *22*
2.2.3. Implementation Tasks *22*

3. NETWORK SECURITY **25**

3.1. NETWORK SECURITY DEFAULTS 26
3.1.1. Working with Network Security Default Settings *26*
3.1.2. Display Network Security Defaults *27*
3.1.3. Manage Network Security Defaults *29*
3.1.3.1. Enable Network Security Auditing 29
3.1.3.2. Enable Network Security Change Auditing 29
3.1.3.3. Enable Network Security Alerts 30
3.1.3.4. Enable Network Security Debug Log 30
3.1.3.5. Enable TELNET Auto Signon 30
3.1.3.6. Enable Group Profile Inheritance 32
3.1.4. Run Network Security Reports *32*
3.2. TRANSACTIONS 33
3.2.1. Working with Transactions *33*
3.2.2. Display List of Incoming Transactions *34*
3.2.2.1. Display List 34
3.2.2.2. Sort List 35
3.2.2.3. Move to Position in List 35
3.2.2.4. Filter List 35
3.2.3. Manage Incoming Transactions *36*
3.2.3.1. Display Incoming Transaction Details 36
3.2.3.2. Delete Incoming Transaction 37
3.2.3.3. Archive Incoming Transactions 37
3.2.3.4. Create a Rule Based on a Transaction 38
3.2.3.5. Accept a Rule Suggestion 38
*3.2.4. Run Transactions (*TRN) Report* *39*
3.2.4.1. Access the Network Reports Interface 40
3.2.4.2. Run Incoming Transaction Details 40
3.2.4.3. Run Transaction Summary by Server Report 40
3.2.4.4. Run Transaction Summary by User Report 41
3.2.4.5. Run Network Transaction Report 41

*3.2.5. Run Socket Transaction (*SOC) Reports* *42*
3.2.5.1. Access the Network Reports Interface 42
3.2.5.2. Run Socket Transaction Report 42
3.2.5.3. Run Socket Summary by Server Report 42
3.2.5.4. Run Transaction Summary by User Report 43
3.3. EXIT POINTS 43
3.3.1. Working with Exit Points *43*
3.3.2. Display List of Exit Points *45*
3.3.3. Manage Exit Points *46*
3.3.3.1. Display Exit Point Details 47
3.3.3.2. Enable Exit Point Auditing 49
3.3.3.3. Enable Exit Point Security 49
3.3.3.4. Enable Exit Point Alerts 49
3.3.3.5. Enable Exit Point Collection 50
3.3.3.6. Add Exit Program to Exit Point 50
3.3.3.7. Add Exit Programs to Exit Points (Mass Update) 50
3.3.3.8. Remove Exit Program from Exit Point 50
3.3.3.9. Remove Exit Programs from Exit Points (Mass Update) 51
3.3.3.10. Cycle Server 51
3.3.3.11. Cycle Servers (Mass Update) 51
3.3.3.12. Update all Exit Points (Mass Update) 52
3.3.4. Run Exit Points Report *53*
3.3.4.1. Access the Network Reports Interface 53
3.3.4.2. Run Exit Point Configuration Report 53
3.3.4.3. Run Exit Point Configuration Changes Report 54
3.4. SOCKET RULES 54
3.4.1. Working with Socket Rules *54*
3.4.2. Display List of Socket Rules *55*
3.4.2.1. Display List 55
3.4.2.2. Sort List 56
3.4.2.3. Move to Position in List 56
3.4.2.4. Filter List 57
3.4.3. Manage Socket Rules *57*
3.4.3.1. Add Socket Rule 58
3.4.3.2. Edit Socket Rule 58
3.4.3.3. Copy Socket Rule 58
3.4.3.4. Delete Socket Rule 59
3.4.3.5. Display List of Users in a Group 59
3.4.3.6. Display List of Clients in a Group 59
3.4.3.7. Display List of Servers in a Group 59
3.4.3.8. Display List of Operations in a Group 60
3.4.4. Run Socket Rule Reports *60*
3.4.4.1. Access the Network Reports Interface 60
3.4.4.2. Run Socket Rule Configuration Report 61
3.4.4.3. Run Socket Rule Configuration Changes Report 61
3.5. EXIT RULES 62
3.5.1. Working with Exit Rules *62*
3.5.2. Display List of Exit Rules *63*
3.5.2.1. Display List 63
3.5.2.2. Sort List 64
3.5.2.3. Move to Position in List 64
3.5.2.4. Filter List 64
3.5.3. Manage Exit Rules *65*

3.5.3.1. Add Exit Rule 65
3.5.3.2. Edit Exit Rule 66
3.5.3.3. Copy Exit Rule 67
3.5.3.4. Delete Exit Rule 67
3.5.3.5. Display List of Users 67
3.5.3.6. Display List of Clients 68
3.5.3.7. Display List of Servers 68
3.5.3.8. Display List of Operations 68
3.5.3.9. Display List of Objects 69
3.5.4. Run Exit Rule Reports 69
3.5.4.1. Access the Network Reports Interface 69
3.5.4.2. Run Exit Rule Configuration Report 70
3.5.4.3. Run Exit Rule Configuration Changes Report 70

4. ACCESS ESCALATION MANAGEMENT 73

4.1. ACCESS ESCALATION DEFAULTS 73
4.1.1. Working with Access Escalation Management Defaults 73
4.1.2. Display Access Escalation Defaults 74
4.1.3. Manage Access Escalation 75
4.1.3.1. Modify Access Escalation Defaults 76
4.1.3.2. Enable Access Escalation Change Auditing 76
4.1.4. Run Access Escalation Reports 76
4.2. ENTITLEMENTS 77
4.2.1. Working with Entitlements 77
4.2.2. Display List of Entitlements 78
4.2.2.1. Display List 78
4.2.2.2. Sort List 79
4.2.2.3. Move to Position in List 79
4.2.2.4. Filter List 80
4.2.3. Manage Entitlements 80
4.2.3.1. Add Entitlement 80
4.2.3.2. Edit Entitlement 81
4.2.3.3. Copy Entitlement 82
4.2.3.4. Delete Entitlement 82
4.2.4. Run Entitlement Reports 82
4.2.4.1. Access the Access Escalation Reports Interface 83
4.2.4.2. Run Entitlement Usage Report 83
4.2.4.3. Run Entitlement Configuration Report 83
4.2.4.4. Run Entitlement Configuration Changes Report 84
4.3. ACCESS CONTROL 84
4.3.1. Working with Access Control 84
4.3.2. Display Who Has Access to the AEM Interface 85
4.3.2.1. Display List 85
4.3.2.2. Sort List 86
4.3.2.3. Move to Position in List 86
4.3.2.4. Filter List 86
4.3.3. Manage Access Control 87
4.3.3.1. Add Access Control 87
4.3.3.2. Edit Access Control 88
4.3.3.3. Copy Access Control 88
4.3.3.4. Delete Access Control 88
4.3.4. Run Access Control Reports 88
4.3.4.1. Access the Escalation Reports interface 89

4.3.4.2. Run Access Control Configuration Report 89
4.3.4.3. Run Access Control Change Report 89
4.3.5. Execute an Entitlement Using the AEM Interface *90*
4.4. FILE EDITOR 91
4.4.1. Working with File Editor *91*
4.4.2. Display List of File Editors *91*
4.4.3. Manage File Editors *92*
4.4.3.1. Add File Editor 92
4.4.3.2. Edit File Editor 93
4.4.3.3. Copy File Editor 93
4.4.3.4. Delete File Editor 93
4.4.4. Run File Editor Reports *93*
4.4.4.1. Access the Access Escalation Reports Interface 94
4.4.4.2. Run File Editors Configuration Report 94
4.4.4.3. Run File Editor Change Report 94

5. INACTIVE SESSION LOCKDOWN 97

5.1. INACTIVE SESSION LOCKDOWN DEFAULTS 97
5.1.1. Working with Inactive Session Lockdown Defaults *97*
5.1.2. Display Inactive Session Lockdown Defaults *98*
5.1.3. Manage Inactive Session Lockdown Defaults *99*
5.1.3.1. Enable ISL Auditing 100
5.1.3.2. Enable ISL Change Auditing 100
5.1.3.3. Enable ISL Alerts 101
5.1.3.4. Set Check Interval 101
5.1.3.5. Set Warning Interval 101
5.1.3.6. Set Disconnect Message 101
5.1.3.7. Set Revoke Authority 102
5.1.3.8. Start Monitor 102
5.1.3.9. End Monitor 102
5.1.3.10. Check Monitor Status 103
5.1.4. Run Inactive Session Lockdown Reports *103*
5.1.4.1. Run Inactivity Disconnect Report 103
5.1.4.2. Run Inactivity Session Configuration Settings Report 104
5.1.4.3. Run Inactivity Session Configuration Changes Report 104
5.2. INACTIVE SESSION RULES 105
5.2.1. Working with Inactive Session Rules *105*
5.2.2. Display Inactive Session Rules *106*
5.2.2.1. Display List 106
5.2.2.2. Sort List 107
5.2.2.3. Move to Position in List 107
5.2.2.4. Filter List 107
5.2.3. Manage Inactive Session Rules *108*
5.2.3.1. Add Inactive Session Rule 108
5.2.3.2. Edit Inactive Session Rule 109
5.2.3.3. Copy Inactive Session Rule 109
5.2.3.4. Delete Inactive Session Rule 109
5.2.4. Run Inactive Session Rules Reports *110*
5.2.4.1. Run Inactivity Session Inclusion Exception Rules Report 110
5.2.4.2. Run Inactivity Session Rules Change Report 111
5.3. DISCONNECTION OPTIONS 111
5.3.1. Working with Disconnect Options *111*
5.3.2. Display Disconnect Options *112*

5.3.2.1. Display List 112
5.3.2.2. Sort List 113
5.3.2.3. Move to Position in List 113
5.3.2.4. Filter List 113
5.3.3. Manage Disconnect Options 114
5.3.3.1. Add Disconnect Option 114
5.3.3.2. Edit Disconnect Option 115
5.3.3.3. Copy Disconnect Option 115
5.3.3.4. Delete Disconnect Option 116
5.3.4. Run Disconnect Option Reports 116
5.3.4.1. Run Inactivity Session Disconnect Option Report 116
5.3.4.2. Run Inactivity Session Disconnect Option Change Report 117

6. RESOURCE MANAGER 119

6.1. RESOURCE MANAGER DEFAULTS 119
6.1.1. Working with Resource Manager Defaults 119
6.1.2. Display Resource Manager Defaults 120
6.1.3. Manage Resource Manager Defaults 121
6.1.3.1. Enable Resource Change Auditing 121
6.1.3.2. Enable Resource Change Alerts 122
6.1.4. Run Resource Manager Reports 122
6.1.4.1. Run Resource Manager Configuration Report 123
6.1.4.2. Run Resource Manager Configuration Change Report 123
6.1.4.3. Run Resource Manager Out of Compliance Data 124
6.1.4.4. Run Resource Manager Out of Compliance Data Changes Report 124
6.2. AUTHORITY SCHEMAS 125
6.2.1. Working with Authority Schemas 125
6.2.2. Display Authority Schemas 126
6.2.2.1. Display List of Schemas 126
6.2.2.2. Sort List of Schemas 127
6.2.2.3. Move to Position in List of Schemas 127
6.2.2.4. Filter List Schemas 127
6.2.2.5. Display List of Schemas Details 128
6.2.2.6. Sort List of Schemas Details 128
6.2.2.7. Move to Position in List of Schemas Details 129
6.2.2.8. Filter List Schemas Details 129
6.2.3. Manage Authority Schemas 129
6.2.3.1. Access the Work with Authority Schema Interface 130
6.2.3.2. Add Authority Schema 130
6.2.3.3. Edit Authority Schema 132
6.2.3.4. Copy Authority Schema 132
6.2.3.5. Delete Authority Schema 133
6.2.3.6. Enabling Authority Schema Alerting 133
6.2.3.7. Disable Authority Schema Alerting 133
6.2.3.8. Limit Scope of Authority Schema to System Libraries (SYS) 133
6.2.3.9. Limit Scope of Authority Schema to Integrated File System (IFS) 134
6.2.3.10. Change Scope of Authority Schema (Object or IFS) 134
6.2.3.11. Add Schema Details 135
6.2.3.12. Edit Schema Details 135
6.2.3.13. Copy Schema Detail 136
6.2.3.14. Delete Schema Detail 136
6.2.3.15. Display Authority Schema Compliance Issues 136
6.2.3.16. Enforce Authority Schema 137

6.2.4. Run Authority Schema Reports *138*
6.2.4.1. Run Resource Manager Schema Details Report 138
6.2.4.2. Run Resource Manager Schema Details Changes Report 139
6.2.4.3. Run Resource Manager Schema Header Report 139
6.2.4.4. Run Resource Manager Schema Header Changes Report 140
6.2.4.5. Run Authority Schema Compliance Report 140
6.3. AUTHORITY COLLECTION CONFIGURATION 141
6.3.1. Working with Authority Collections *141*
6.3.2. Display Authority Collection Configuration *142*
6.3.2.1. Display List of Authority Collections 142
6.3.2.2. Display Authority Collection Details 143
6.3.3. Manage Authority Collection Configuration *144*
6.3.3.1. Start Authority Collection 144
6.3.3.2. End Authority Collection 145
6.3.3.3. Delete Authority Collection 146
6.3.4. Run Authority Collection Configuration Reports *146*
6.3.4.1. Run Authority Compliance Report (Single Schema) 147
6.3.4.2. Run Authority Compliance Report (All Schemas) 147
6.3.4.3. Run Authority Collection Report (QSYS) 148
6.3.4.4. Run Authority Collection Report (IFS) 148

7. USER PROFILE MANAGEMENT 151

7.1. USER PROFILE MANAGEMENT DEFAULTS 151
7.1.1. Working with Profile Management Defaults *151*
7.1.2. Display User Profile Management Defaults *152*
7.1.3. Manage User Profile Management Defaults *153*
7.1.3.1. Enable Profile Auditing 154
7.1.3.2. Enable Profile Alerts 154
7.1.3.3. Enable Profile Archiving 155
7.1.3.4. Add Profile Exit Programs 155
7.1.3.5. Remove Profile Exit Programs 155
7.1.4. Run User Profile Management Default Reports *155*
7.1.4.1. Run User Profile Management Defaults Report 156
7.1.4.2. Run User Profile Management Defaults Changes Report 156
7.2. BLUEPRINTS 157
7.2.1. Working with Blueprints *157*
7.2.2. Display Blueprints *158*
7.2.2.1. Display List of Blueprints 158
7.2.2.2. Sort List of Blueprint 159
7.2.2.3. Move to Position in List of Blueprints 159
7.2.2.4. Filter List Blueprint 160
7.2.3. Manage Blueprints *160*
7.2.3.1. Add Blueprint 161
Step 1: Add Blueprint Details 161
Step 2: Add Profile Parameters to a Blueprint 162
Step 3: Add Object Authorities to a Blueprint 163
Step 4: Add Authority List Settings to a Blueprint 164
Step 5: Add 3rd Party Scripts to a Blueprint 164
Step 6: Add Permissions to a Blueprint 165
7.2.3.2. Copy Blueprint 165
7.2.3.3. Delete Blueprint 166
7.2.3.4. Display Blueprint Details 166
7.2.3.5. Display Inactivity Overrides 166

7.2.3.6. Edit Blueprint Details 167
7.2.3.7. Edit Blueprint Profile Parameters 167
7.2.3.8. Edit Blueprint Profile Authorities 167
7.2.3.9. Edit Blueprint Authority Lists 168
7.2.3.10. Edit Blueprint 3rd Party Scripts 168
7.2.3.11. Edit Blueprint Permissions 168
7.2.3.12. Add Blueprint User 169
7.2.3.13. Edit Blueprint User 169
7.2.3.14. Delete Blueprint User 169
7.2.3.15. Display Blueprint Compliance Issues 170
7.2.3.16. Display List of Non-Compliant Profiles 170
7.2.3.17. Enforce Blueprint 171
7.2.4. Run Blueprint Reports 172
7.2.4.1. Run Blueprint Compliance Report 172
7.2.4.2. Run Blueprint Master Report 173
7.2.4.3. Run Blueprint Permission File Report 174
7.2.4.4. Run Blueprint Parameter File Report 174
7.2.4.5. Run Blueprint Object Authority File Report 175
7.2.4.6. Run Blueprint Authority List Settings Report 175
7.2.4.7. Run Blueprint Non-Compliance User Profiles Report 176
7.2.4.8. Run Blueprint 3rd Party Integration File Report 176
7.2.4.9. Run Blueprint Master Change Report 176
7.2.4.10. Run Blueprint Permission File Change Report 177
7.2.4.11. Run Blueprint Parameter File Change Report 177
7.2.4.12. Run Blueprint Object Authority File Change Report 178
7.2.4.13. Run Blueprint Authority List Settings Change Report 178
7.2.4.14. Run Blueprint Non-Compliance User Profiles Change Report 179
7.2.4.15. Run Blueprint 3rd Party Integration File Change Report 179
7.3. USER EXCLUSIONS 180
7.3.1. Working with User Exclusions 180
7.3.2. Display User Exclusions 180
7.3.2.1. Display List of User Exclusions 181
7.3.2.2. Sort List of User Exclusions 181
7.3.2.3. Move to Position in List of User Exclusions 181
7.3.2.4. Filter List User Exclusions 182
7.3.3. Manage User Exclusions 182
7.3.3.1. Add Exclusion 183
7.3.3.2. Edit Exclusion 183
7.3.3.3. Copy Exclusion 183
7.3.3.4. Delete Exclusion 184
7.3.4. Run User Exclusion Reports 184
7.3.4.1. Run User Profile Exclusions Report 184
7.3.4.2. Run User Profile Exclusions Changes Report 185
7.4. ARCHIVED PROFILES 186
7.4.1. Working with Archived Profiles 186
7.4.2. Display Archived Profiles 186
7.4.2.1. Display List of Archived Profiles 186
7.4.2.2. Sort List of Archived Profiles 187
7.4.2.3. Move to Position in List of Archived Profiles 187
7.4.2.4. Filter List Archived Profiles 187
7.4.3. Manage Archived Profiles 188
7.4.3.1. Reactivate Profile 188
7.4.3.2. Delete Archived File 188

7.4.4. Run Archived Profile Reports *189*
7.4.4.1. Run User Profile Archive Report 189
7.4.4.2. Run User Profile Archive Changes Report 190
7.5. INACTIVE PROFILES 190
7.5.1. Working with Inactive Profiles *190*
7.5.2. Display Inactive Profile Settings *191*
7.5.3. Manage Inactive Profile *192*
7.5.3.1. Edit Inactive Profile Settings 192
7.5.3.2. Display the List of Inactive Profiles 193
7.5.3.3. Enforce Inactive Profile Rules 193
7.5.4. Run Inactive Profile Reports *194*
7.5.4.1. Run Inactivity Compliance Report 195
7.5.4.2. Run Profile Inactivity Settings Report 195
7.5.4.3. Run Profile Inactivity Settings Changes Report 195
7.6. USER PROFILES 196
7.6.1. Working with User Profiles *196*
7.6.2. Manage User Profiles *197*
7.6.2.1. Create User Profile Based on a Blueprint 197
7.6.2.2. Change User Profile Based on a Blueprint 198
7.6.3. Run User Profile Reports *198*
7.6.3.1. Run User Profile Create/Change via Blueprint 199
7.6.3.2. Run User Profile Activity Report 199
7.6.3.3. Run User Profile Changes Report 200
7.6.3.4. Run Invalid Sign-on Attempts Report 200
7.6.3.5. Run Authority Failures For User Report 200
7.7. PASSWORD RULES 201
7.7.1. Working with Password Rules *201*
7.7.2. Manage Password Rules *202*
7.7.2.1. Add Password Exit Program 202
7.7.2.2. Remove Password Exit Program 202
7.7.2.3. Edit Password Rules 203

8. REPORTS 205

8.1. WORKING WITH REPORTS 205
8.2. DISPLAY LIST OF REPORTS 205
8.2.1. Display list *205*
8.2.2. Sort List *205*
8.2.3. Move to Location in List *206*
8.2.4. Filter List *206*
8.3. RUN REPORTS 206
8.3.1. Run Reports with Start and End Time Requirements *207*
8.3.2. Run Reports without Start and End Time Requirements *208*
8.4. CREATE REPORTS 209
8.4.1. Add Report *209*
8.4.2. Select Data Source Collector *209*
8.4.3. Name the Report *210*
8.4.4. Select Report Fields *210*
8.4.5. Change Order of Fields *211*
8.4.6. Define Report Filter Criteria *211*
8.4.7. Define Run-time Collector Defaults *212*
8.4.8. Confirm Report Creation *212*
8.5. MANAGE REPORTS 213
8.5.1. Access the Work with Reports Interface *213*

8.5.2. Edit Report *213*
8.5.3. Copy Report *214*
8.5.4. Delete Report *214*
8.5.5. Enabling Report Alerting *214*

9. GROUPS 215

9.1. WORKING WITH GROUPS 215
9.2. USERS 215
9.2.1. Working with User Groups *215*
9.2.2. Display List of User Groups *216*
9.2.2.1. Display List 216
9.2.2.2. Sort List 217
9.2.2.3. Move to Position in List 217
9.2.2.4. Filter List 217
9.2.3. Display List of Users in a Group *218*
9.2.3.1. Display List 218
9.2.3.2. Sort List 218
9.2.3.3. Move to Position in List 218
9.2.4. Manage User Groups *219*
9.2.4.1. Add User Group 219
9.2.4.2. Edit User Group 219
9.2.4.3. Copy User Group 220
9.2.4.4. Delete User Group 220
9.2.5. Manage Users Within a Group *220*
9.2.5.1. Add a User 221
9.2.5.2. Edit a User 221
9.2.5.3. Delete a User 221
9.2.6. Run User Groups Report *222*
9.2.6.1. Run User Group Configuration Report 222
9.2.6.2. Run User Group Configuration Changes Report 222
9.3. NETWORKS 223
9.3.1. Working with Networks *223*
9.3.2. Display List of Network Groups *223*
9.3.2.1. Display List 224
9.3.2.2. Sort List 224
9.3.2.3. Move to Position in List 224
9.3.2.4. Filter List 224
9.3.3. Display List of Networks in a Group *225*
9.3.3.1. Display List 225
9.3.3.2. Sort List 225
9.3.3.3. Move to Position in List 226
9.3.4. Manage Network Groups *226*
9.3.4.1. Add Network Group 226
9.3.4.2. Edit Network Group 227
9.3.4.3. Copy Network Group 227
9.3.4.4. Delete Network Group 227
9.3.5. Manage Networks Within a Group *227*
9.3.5.1. Add Network 228
9.3.5.2. Edit Network 228
9.3.5.3. Delete Network 228
9.3.6. Run Network Groups Report *229*
9.3.6.1. Access the Network Reports Interface 229
9.3.6.2. Run Network Group Configuration Report 229

9.3.6.3. Run Network Group Configuration Changes Report 229
9.4. OPERATIONS 230
9.4.1. Working with Operations *230*
9.4.2. Display List of Operation Groups *231*
9.4.2.1. Display List 231
9.4.2.2. Sort List 231
9.4.2.3. Move to Position in List 231
9.4.2.4. Filter List 232
9.4.3. Display List of Operations in a Group *232*
9.4.3.1. Display List 232
9.4.3.2. Sort List 233
9.4.3.3. Move to Position in List 233
9.4.4. Manage Operation Groups *233*
9.4.4.1. Add Operation Group 234
9.4.4.2. Edit Operation Group 234
9.4.4.3. Copy Operation Group 234
9.4.4.4. Delete Operation Group 234
9.4.5. Manage Operations Within a Group *235*
9.4.5.1. Add Operation 235
9.4.5.2. Edit Operation 235
9.4.5.3. Delete Operation 236
9.4.6. Run Operation Groups Report *236*
9.4.6.1. Access the Network Reports Interface 236
9.4.6.2. Run Operation Groups Configuration Report 236
9.4.6.3. Run Operation Group Configuration Changes Report 237
9.5. OBJECTS 237
9.5.1. Working with Objects *237*
9.5.2. Display List of Object Groups *238*
9.5.2.1. Display List 238
9.5.2.2. Sort List 238
9.5.2.3. Move to a Position in the List 239
9.5.2.4. Filter List 239
9.5.3. Display a List of Object in a Group *239*
9.5.3.1. Display List 239
9.5.3.2. Sort List 240
9.5.3.3. Move to Position in List 240
9.5.4. Manage Object Groups *240*
9.5.4.1. Add Object Group 241
9.5.4.2. Edit Object Group 241
9.5.4.3. Copy Object Group 241
9.5.4.4. Delete Object Group 242
9.5.5. Manage Objects Within a Group *242*
9.5.5.1. Add Object 242
9.5.5.2. Edit Object 243
9.5.5.3. Delete Object 243
9.5.6. Run Object Groups Report *243*
9.5.6.1. Access the Network Reports Interface 243
9.5.6.2. Run Object Group Configuration Report 244
9.5.6.3. Run Object Group Configuration Changes Report 244

10. CALENDARS 245

10.1. WORKING WITH CALENDARS 245
10.2. DISPLAY LIST OF CALENDARS 246

10.2.1. Display List *246*
10.2.2. Sort List *246*
10.2.3. Move to a Position in the List *246*
10.2.4. Filter List *246*
10.3. MANAGE CALENDARS 247
10.3.1. Display Calendar Duration Details *247*
10.3.2. Display Calendar Day/Time Access Details *248*
10.3.3. Edit Calendar Duration Details *248*
10.3.4. Edit Calendar Day/Time Access Details *248*
10.3.5. Add Calendar *248*
10.3.6. Copy Calendar *249*
10.3.7. Delete Calendar *249*
10.4. MANAGE CALENDAR DAY/TIME ACCESS 250
10.4.1. Display Day/Time Details *250*
10.4.2. Add Day/Time Requirement *250*
10.4.3. Edit Day/Time Requirement *251*
10.4.4. Copy Day/Time Requirement *251*
10.4.5. Delete Day/Time Requirement *251*

11. SAVE AND RESTORE CONFIGURATION 253

11.1. MANAGE CONFIGURATION 253
11.1.1. Save Configuration *253*
11.1.2. Restore Configuration *255*
11.1.3. Copy Configuration *256*

12. TROUBLESHOOTING 257

12.1. FAQ 257
12.1.1. Why does my report have no data? *257*
12.2. ERROR MESSAGES 257
12.2.1. IBM Error Messages *257*
12.2.1.1. CPF4169 while accessing menu options 257
12.2.1.2. Exit program NTW[ID] could not be found in library 257
12.3. FIXES 258
12.3.1. Fix Files *258*
12.3.2. Save Fix to Agent Server *258*
12.3.3. Manage Fixes *259*
12.3.3.1. Apply Fix 259
12.3.3.2. Remove Fix 260
12.3.4. Display List of Fixes *260*

13. APPENDIX - COLLECTORS 262

What's New in Version 2.1

Groups

In the Network Security Default settings, you can now do the following:

- Enable group profile inheritance

Exit Program

The following exit program is now available for use:

- Showcase

Note: See Manage Exit Points for instruction on adding (installing) an exit program.

Report

The following report is now available:

- Network Transaction Showcase

Tip: See the **TGSecure Report Reference Guide** for information about individual reports.

1. Introduction

1.1. Historical Perspective of Security

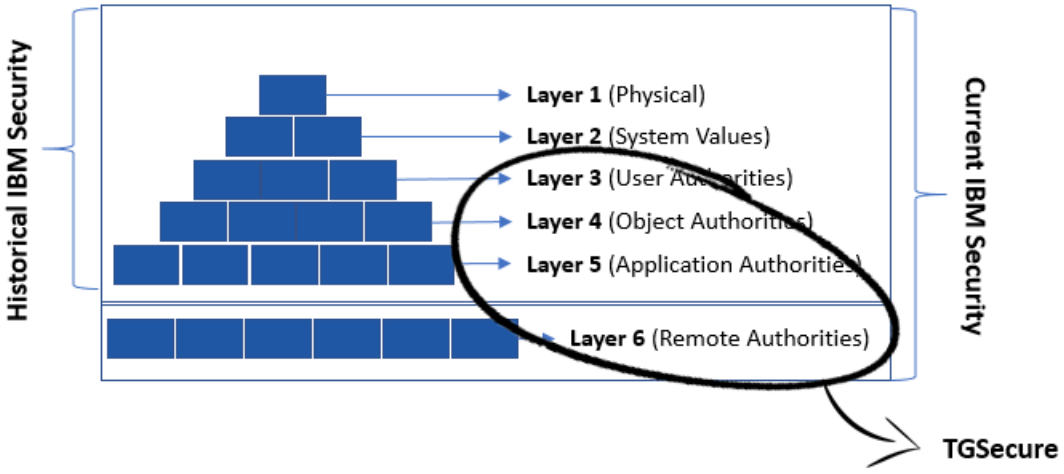
Before we talk about what TGSecure is or does, let's talk about where it fits. When the IBM® iSeries was introduced in 1988, client/server configurations and Internet-based networks were not widely used. At that time, iSeries servers were accessed through locally attached terminals. Security was controlled through the following structure:

- **Physical Security** - Restrict access by setting up the server in a secure computer room
- **System Values** - Use values that control system access (10: Physical Security, 20: Password Security, 30: Object Security, 40: System Integrity, 50: Resource Security)
- **User Authorities** - Restrict the user's ability to execute i5/OS or user-defined commands
- **Object Authorities** - Restrict the user's ability to execute commands on objects
- **Application Authorities** - Restrict the user's ability to access data or commands

Times have changed, and many iSeries servers are accessed via remote connections, which requires additional security structure:

- **Remote Authorities** - Restricting remote client access

TGSecure provides tools to help you manage user, object, application, and remote access.



See also

- Product Overview
- Product Features
- Decision Algorithm
- IBM System Values (external IBM Knowledge base topic)

1.2. TGSecure Overview

TGSecure allows you to manage security threats on IBM® iSeries systems from both external and internal sources. In addition, it provides reports for monitoring the security health of your system.

Note: While you can use TGSecure as a standalone product, it is also one component of a powerful security suite. For more information about the suite or other products in the suite, go to TrinityGuard.com.

See also

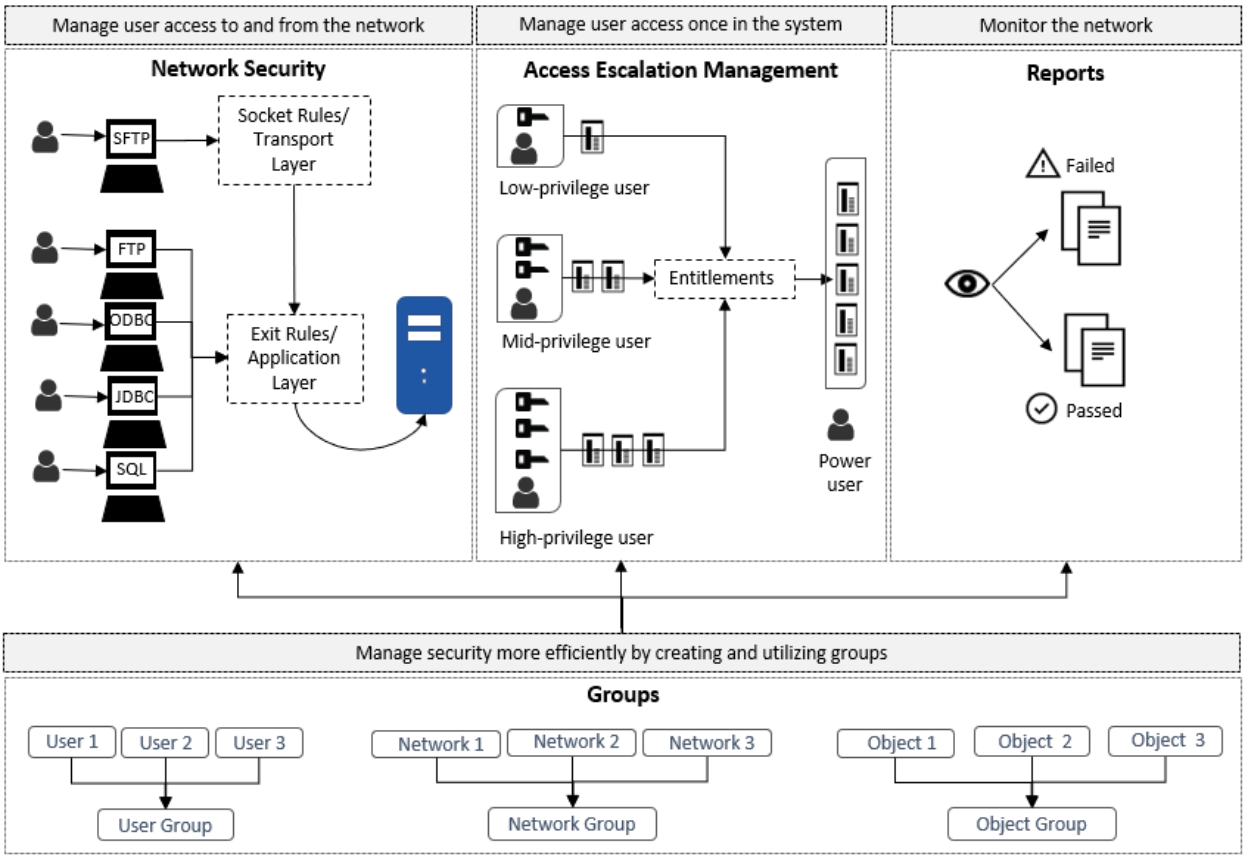
Features

Decision Algorithm

Getting Started Using TGSecure

1.3. Features

To help you design, manage, and maintain a secure system, TGSecure includes the following product features:



Network Security

This feature allows you to monitor remote requests (incoming transactions). The system performs this task by comparing incoming transactions with entry rules (i.e., socket and exit) and assigning each transaction a PASS or FAIL status based on those rules. The rules are evaluated using a decision algorithm.

- Manage Socket Rules
- Manage Exit Rules

Access Escalation Management

This feature allows you to manage privilege escalated access using user entitlements.

- Manage Entitlements
- Manage Access Control

Reports

This feature allows you to monitor activities that impact system security using built-in and custom reports.

Note: See Manage Reports for more information.

Groups

This feature enhances your ability to quickly manage security using user, network, operation, or object groups.

Note: Groups are used in conjunction with user entitlements to manage privilege escalated access.

- Manage User Groups
- Manage Network Groups
- Manage Operations Groups
- Manage Object Groups

See also

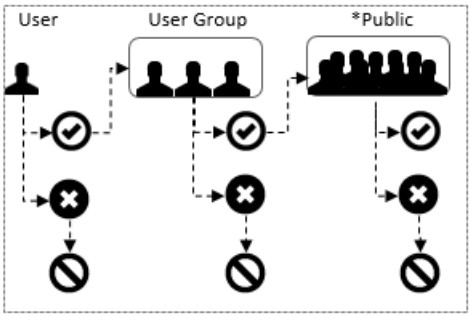
Rules Decision Algorithm
Rules Suggestion Engine
TGSecure Overview
Use TGSecure

1.4. Rules Decision Algorithm

The rules evaluation process used to manage network security is controlled through a decision-making algorithm, which coordinates a series of authority checks.

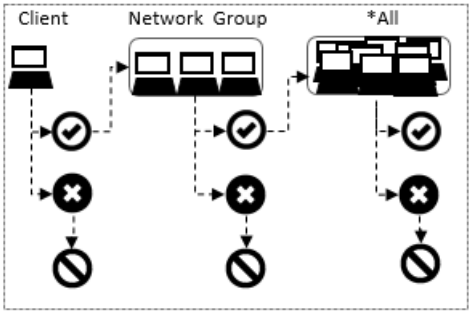
Check 1: Evaluate User

1) Apply rules for a specific user
2) Apply rules for a specific user group
3) Apply rules that apply to all users (*PUBLIC)



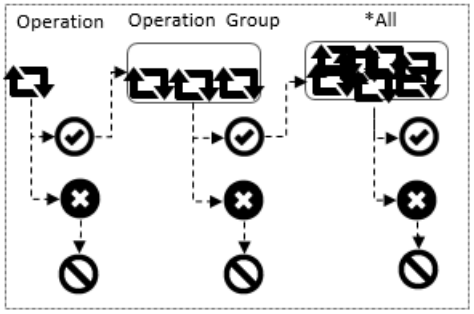
Check 2: Evaluate Network (Client Server)

1) Check rules for a specific client IP
2) Check rules for a generic IP (e.g., 11.111*)
3) Check rules for a network group
4) Check rules that apply to all networks (*ALL)



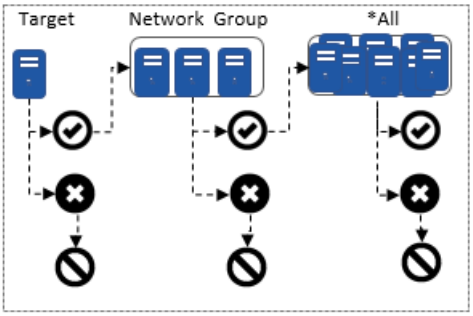
Check 3: Evaluate Operation

1) Check rules for a specific operation
2) Check rules for an operation group
3) Check rules that apply to all operations (*ALL)



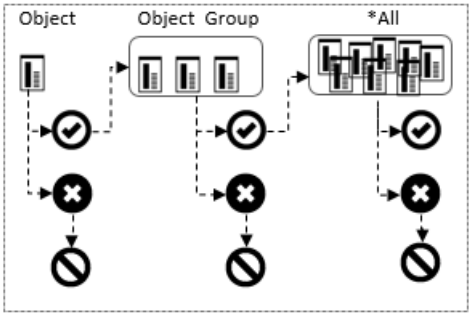
Check 4: Evaluate Network (Target Server)

1) Check rules for a specific target IP
2) Check rules for a generic IP (e.g., 11.111*)
3) Check rules for network group
4) Check rules that apply to all networks (*ALL)



Check 5: Evaluate Object

1) Check rules for a specific object
2) Check rules for a generic object (e.g., /home/etv/*...)
3) Check rules for an object group
4) Check rules that apply to all objects (*ALL)



See also

For information about how decisions are made regarding access escalation (the other main feature in the product), see Access Escalation Management.
For information about how to run reports, see Working with Reports.

1.5. Rules Suggestion Engine

Rules (i.e., exit rules or socket rules) are a power tool for managing network security, but to use rules efficiently, they must be used in conjunction with groups.

For example, if a new user is added to the system, and the security administrator determines that the user should have limited access, the administrator can easily create a rule defining the appropriate level of access for that individual, but that would be inefficient if the user was hired to fulfil a role shared by many. In that case, it would be more efficient to create a role-based rule that could be apply to a group of users.

Rule Example

Bob joins the company. Bob is provided with an IBM login. That morning, Bob logs into the system from a workstation set up in a training room for new hires. The administrator can see Bob's SIGNON transaction by viewing the list of incoming transactions. The administrator notices that in the evening Bob logs in again, but from

a different client IP address. At this point in Bob's onboarding, he should only access the system while under the supervision of his mentor or trainer. Bob is not doing anything wrong, but he has the potential because of his lack of experience to cause harm. Therefore, the administrator decides to create a rule that limits Bob's access while he is completing his training.

Rule Suggestion Example

The administrator creates a rule limiting Bob's access and tries to save the rule, but the suggestion (intelligence) engine notifies the administrator that a similar rule already exists, and instead of creating a rule specific to Bob, the administrator should instead add Bob to a user group titled: *Trainees* that was created six months earlier for a group of new hires in a similar situation.

Rule Suggestion Interface

There's no way to directly access the rules suggestion engine. The interface appears at the time you save a new rule and only if the suggestion (intelligence) engine identifies a situation in which updating an existing user group or network group would be more efficient than creating a new rule.

See also

Manage Incoming Transactions

Manage Exit Rules

Manage Socket Rules

Manage User Groups

TGSecure Overview

Use TGSecure

2. Getting Started

2.1. Log into TGSecure

Use this task to log into TGSecure.

To log into TGSecure

1) Sign into your IBM i server.
2) At the **Selection or command** prompt, enter **TGMENU**.
3) Press **Enter**.

Note: The **TG - Main** menu is displayed.

4) At the **Selection or command** prompt, enter **2** (TGSecure).

Note: The **TGSecure Main** menu is displayed.

See also

Use TGSecure

Features

2.2. Getting Starting Using TGSecure

This topic discusses the following:

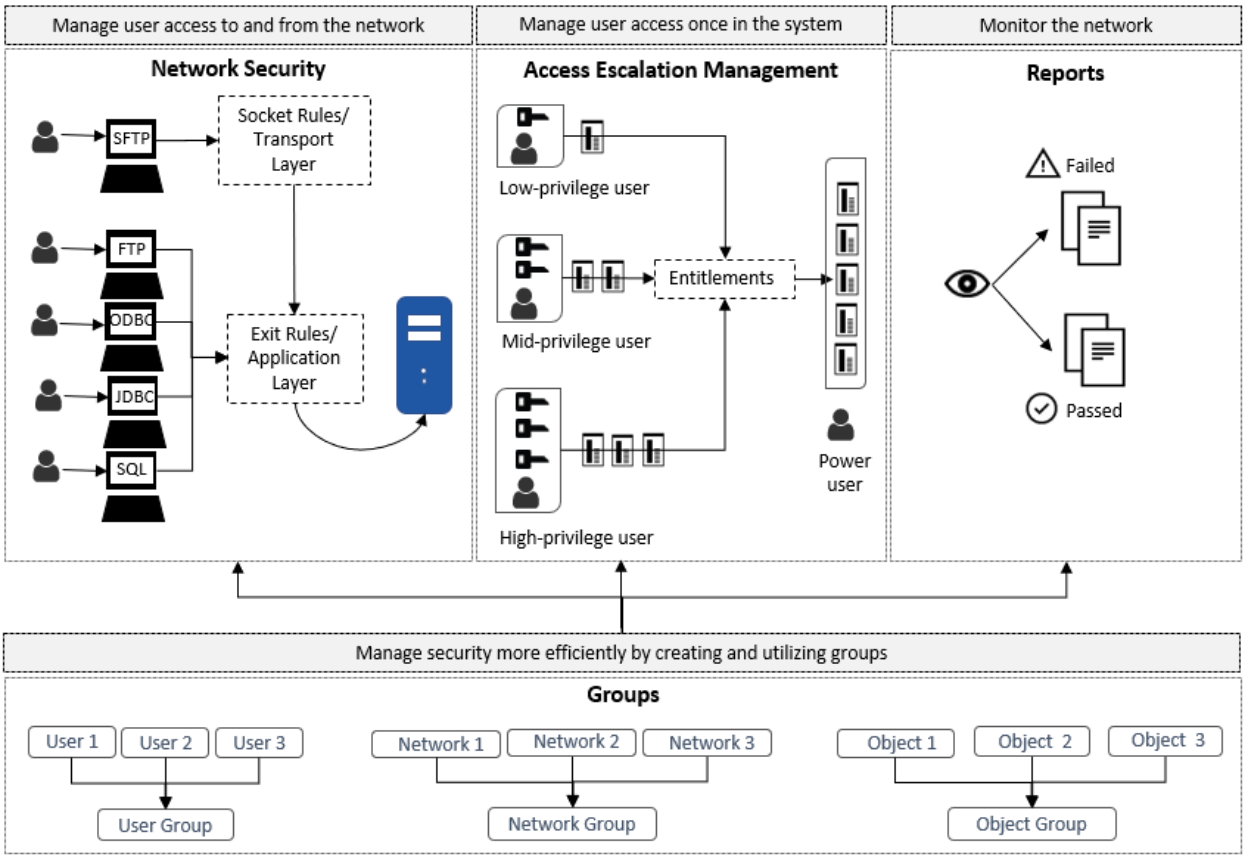
- Actions
- Process Flow
- Implementation Tasks

2.2.1. Actions

The following TGSecure features allow you to do the following:

- **Network Security** - Monitor incoming transactions and manage network security threats using rules (i.e., socket rules and exit rules)
- **Access Escalation Management** - Monitor and manage powerful-user activity and implement the least-privilege model using entitlements
- **Reports** - Generate reports to monitor network activity evaluate security health (i.e., pass/fail status)
- **Groups** - Create groups (i.e., user, network, operation, and object) to manage security more efficiently

2.2.2. Process Flow



2.2.3. Implementation Tasks

There is no single linear process for implementing TGSecure, but the following describes how a typical implementation might work. It's important to remember that security management is an iterative process.

Step 1 **Monitor Network Access**

To enhance security, you first need to understand who is accessing your network.

The Incoming Transactions module of TGSecure allows you to display the incoming transactions requesting access and executing commands on the server.

Step 2 **Create Groups**

With the vast number of elements that impact security, it might be necessary to group items together for efficiency.

For example, it might not be efficient to create an entitlement for each user. It would be more efficient to apply a single entitlement to a group of users. The same would hold true for a single rule being applied to a group of networks.

The Grouping module of TGSecure allows you to create groups for the following elements:

- Users
- Networks
- Operations
- Objects

Step 3	**Manage Network Access** Once you have a better awareness of who and how your system is accessed and you have created what you feel are logical and useful groupings, you can begin limiting network access. The Exit Point and Socket Rules modules of TGSecure allows you to apply rules to manage network access: • Application layer (exit rules) • Transport layer (socket rules)
Step 4	**Implement Least-privilege Model** Once the appropriate users have access to your system, you then want to ensure that these users have the appropriate level of authority to perform assigned tasks, but no more than that. The Access Escalation Management (AEM) module of TGSecure allows you to create entitlements to manage system access.
Step 5	**Run Reports** Ensuring your server and system remain secure involves continuous and proactive monitoring. The Reporting module of TGSecure allows you to run built-in reports and create custom reports to monitor security health of your server and system. **Note**: The built-in reports available to you are dependent on your license agreement.

See also

Log Into TGDetect

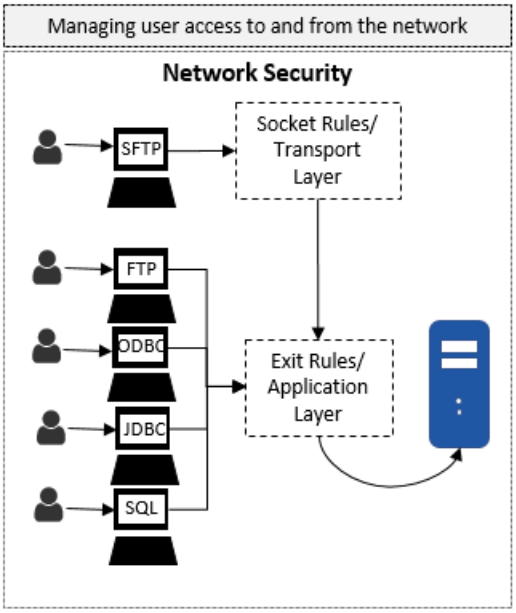
Benefits

Features

3. Network Security

In the past, the risk related to network security was limited to internal networks and required limited security measures. With the advancement of technology and availability of open networks, security risks increased. To bridge the security gap caused by open networks, IBM introduced remote exit points, which are hooks that allow you to attach custom exit programs that monitor network traffic (server transactions). You can customize these exit programs not only to monitor, but also limit access with the addition of exit rules, which allow you to establish pass/fail criteria for transactions. The introduction of exit points addressed the security risks associated with many traditional protocols (e.g., FTP, TELNET, and ODBC, etc.), but exit points did not close the security gap completely. Newer protocols (i.e., SSH and SFTP) were introduced to address weaknesses in older protocols in which data was transmitted in clear text. While the newer protocols reduced some security risks, they also opened the door to other risks because they bypassed the established remote exit points, which reside at the application level, and instead used socket communication at the transaction level.

The socket level risk was addressed by IBM with IBM i version 7.1. at which point you could begin monitoring socket communications and applying socket rules.



To access the Network Security interface

1) Log into to TGSecure.

Note: The **Main** menu appears.

2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.

Note: The **Network Security** interface is displayed.

See also

Log into TGSecure

Use TGSecure

Working with the Network Security

Managing Network Security

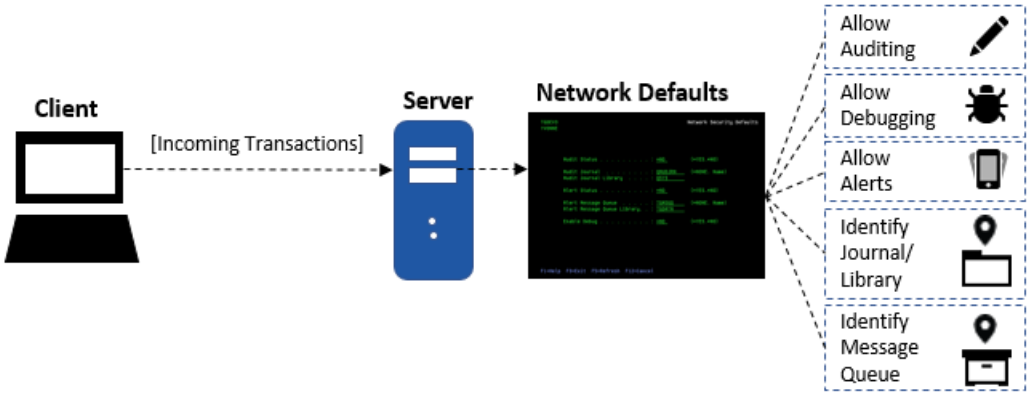
Run Network Security Reports

3.1. Network Security Defaults

3.1.1. Working with Network Security Default Settings

This section describes working with network security defaults. Network security defaults define the following:

- Journal in which the network transactions are stored
- Library in which the journal resides
- Message queue in which to store alert data
- Library in which message queue resides
- Whether debugging is enabled (log is created)
- Whether auditing (data collection) is enabled
- Whether to enable alerts
- Whether a user can inherit privileges from a group



In order to work with network security defaults, you must access the **Network Security Defaults** interface.

To access the Network Security Defaults interface

1) Log into to TGSecure.

Note: The **Main** menu appears.

2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **11** (Network Security Defaults).
5) Press **Enter**.

Note: The **Network Security Defaults** interface is displayed.

See also

Log into TGSecure

Display Network Security Defaults

Manage Network Security Defaults

Run Network Security Reports

3.1.2. Display Network Security Defaults

Use this task to display network security defaults.

To display the network security defaults

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.

Note: The **Network Security** interface is displayed.

4) At the **Selection or command** prompt, enter **11** (Network Security Defaults).
5) Press **Enter**.

Note: The **Network Security Defaults** interface is displayed.

Field	Description
Audit Status	Whether auditing is enabled globally (for all exit points). Auditing is required if you plan to run network security reports. ***YES** - Record incoming transaction data in the audit journal ***NO** - Do not record incoming transaction data in the audit journal **Tip**: If auditing is disabled at the network security (module) level, then auditing will not occur. The module level setting takes precedence. However, if auditing is enabled at the module level, you must also enable auditing at the secondary level (each exit point) if you want to record auditing data for a specific exit point. See Manage Exit Points for information about setting the audit status for an individual exit point.
Audit Journal	Journal in which to store network security audit data **Note**: The default audit journal for TG products is TGJRN. This journal resides in the TGDATA library.
Audit Journal Library	Library in which the journal resides
Audit Configuration Changes	Whether to collect data about network security changes **Y** - Enable tracking of changes **N** - Disable tracking of changes **Tip**: Set this flag to **Y** to if you plan to run network security change reports. **Note**: There are multiple product modules (e.g., network security, access escalation, inactive session lockdown, etc.) in which you can track configuration changes. Therefore, if you see ***NONE** in the comment field, this indicates that configuration changes are not being tracked in any module. This is common at the time the product is initially installed. If you see ***PARTIAL**, this indicates that configuration changes are being track in at least

	one module, but not all modules. If you see ***ALL**, this indicates that configuration changes are being tracked in all modules.
Alert Status	Whether alerting is enabled globally (for all exit points). Alerting is required if you plan to send alert notifications. ***YES** - Enable alerts for all (PASS and FAIL) connection attempts ***NO** - Disable alerts **Tip**: If alerts are disabled at the network security (module) level, then alerts are not stored in the message queue even if alerts are enabled at the exit point (secondary) level. The module level setting takes precedence. However, if alerts are enabled at the module level, you must also enable alerts at the secondary level if you want to record alerts for a specific exit point. See Manage Exit Points for information about setting the alert status for an individual exit point.
Alert Message Queue	Queue in which to store alerts
Alert Message Queue Library	Library in which to store the queue
TELNET AutoSignon Allowed	Whether auto signon is enabled ***YES** - Enabled auto signon ***NO** - Disable auto signon ***ENCPWD** - Enable auto sign and encrypt password ***PWDRQD** - Enable auto signon
Primary Group Inheritance	Whether to allow profile inheritance from the primary group ***YES** - Enable profile inheritance for the primary group ***NO** - Disable profile inheritance for the primary group **Note**: The primary group is the user ID entered in the **Group profile** field when using command CHGUSRPRF. The primary group is the first ID from which a user inherits privileges. See Manage Network Security Defaults for more information about enabling group profile inheritance.
Supplemental Group Inheritance	Whether to allow profile inheritance the supplemental groups ***YES** - Enable profile inheritance for supplemental groups ***NO** - Disable profile inheritance for supplemental groups **Note**: Supplemental groups are user IDs entered in the **Supplemental group** field when using command CHGUSRPRF. Each profile has the potential to be assigned up to 15 supplemental ID from which to inherit privileges. See Manage Network Security Defaults for more information about enabling group profile inheritance.
Enable Debug	Whether to collect data for a debug log ***YES** - Enable debug log ***NO** - Disable debug log **Note**: The debug log is not required but might help with troubleshoot issues.

See also

Working with Network Security Defaults

3.1.3. Manage Network Security Defaults

Use this task to do the following:

- Enable network security auditing
- Enable network security change auditing
- Enable network security alerts
- Enable network security debug log
- Enable TELNET auto sign on
- Enable group profile inheritance

To manage network defaults, access the **Network Security Defaults** interface.

To access the with Network Security Defaults interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.

Note: The **Network Security** interface is displayed.

4) At the **Selection or command** prompt, enter **11** (Network Security Defaults).
5) Press **Enter**.

Note: The **Network Security Defaults** interface is displayed.

3.1.3.1. Enable Network Security Auditing

Use this task to enable network security auditing.

Tip: Auditing is required if you plan to run network security reports.

Note: If auditing is disabled at the network security (module) level, then auditing will not occur. The module level setting takes precedence. However, if auditing is enabled at the module level, you must also enable it at the secondary level (each exit point) if you want to record auditing data for a specific exit point.

To enable network security auditing

1) Access the **Network Security Defaults** interface.
2) In the **Audit Status** field, enter ***YES**.
3) In the **Audit Journal** field, enter the name of the journal in which to store the auditing data.
4) In the **Audit Journal Library** field, enter the name of the library in which the journal resides.
5) Press **Enter**.

Note: The default audit journal for TG products is TGJRN. This journal resides in the TGDATA library.

3.1.3.2. Enable Network Security Change Auditing

Use this task to enable tracking of network security configuration changes.

Tip: Tracking is required if you plan to run network security change reports.

To enable network security configuration change tracking

1) Access the **Network Security Defaults** interface.
2) In the **Audit Configuration Changes** field, enter **Y**.
3) Press **Enter**.

Note: There are multiple product modules (e.g., network security, access escalation, inactive session lockdown, etc.) in which you can track configuration changes. Therefore, if you see ***NONE** in the comment field, this indicates that configuration changes are not being tracked in any module. This is common at the time the product is initially installed. If you see ***PARTIAL**, this indicates that configuration changes are being track in at least one module, but not all modules. If you see ***ALL**, this indicates that configuration changes are being tracked in all modules.

3.1.3.3. Enable Network Security Alerts

Use this task to enable network security alerts.

Tip: Alerting is required if you plan to send alert notifications.

Note: If alerts are disabled at the network security (module) level, then alerts are not stored in the message queue even if alerts are enabled at the exit point (secondary) level. The module level setting takes precedence. However, if alerts are enabled at the module level, you must also enable alerts at the secondary level if you want to record alerts for a specific exit point.

To enable network security alerts

1) Access the **Network Security Defaults** interface.
2) In the **Alert Status** field, enter ***YES**.
3) In the **Alert Message Queue** field, enter the name of the queue in which to store the alerts.
4) In the **Alert Message Queue Library** field, enter the name of the library in which the queue resides.
5) Press **Enter**.

3.1.3.4. Enable Network Security Debug Log

Use this task to enable the network security debugging log.

Note: The debug log is not required but might help with troubleshoot issues.

To enable network security debugging log

1) Access the **Network Security Defaults** interface.
2) In the **Enable Debug** field, enter ***YES**.
3) Press **Enter**.

3.1.3.5. Enable TELNET Auto Signon

Use this task to enable TELNET auto signon.

Warning: This feature must be maintained and monitored properly to avoid any security issues.

Enabling TELNET auto signon is a three-step process:

Step 1. Update the **QRMTSIGN** system value to enable TELNET auto signon

Step 2. Update the **Network Security Defaults** to enable TELNET auto signon

Step 3. Update the **Network Security Configuration** to include the TELNET exit program

Step 1: To update the QRMTSIGN system value for TELNET auto signon

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **WRKSYSVAL QRMTSIGN**.
3) Press **Enter**.

Note: The **Work with System Values** interface is displayed.

4) In the **Option** column beside the **QRMTSIGN** system value, enter **2** (Change).
5) Press **Enter**.

Note: The **Change System Value** interface is displayed.

6) In the **Remote sign-on control** field, enter ***VERIFY**.

7) Press **Enter** twice.

Step 2: Update the Network Security Defaults for TELNET auto signon

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.

Note: The **Network Security** interface is displayed.

4) At the **Selection or command** prompt, enter **11** (Network Security Defaults).
5) Press **Enter**.

Note: The **Network Security Defaults** interface is displayed.

6) In the **Telnet AutoSignon Allowed** field, enter ***YES**.
7) Press **Enter**.

Step 3: Update the Network Security Configuration for TELNET auto signon

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.

Note: The **Network Security** interface is displayed.

4) At the **Selection or command** prompt, enter **10** (Exit Point Configuration).
5) Press **Enter**.

Note: The **Network Security Configuration** interface is displayed.

2) In the **OPT** column beside the ***TELNET** network server, enter **11** (Add Exit Program).
3) Press **Enter**.

Note: Once an exit program is installed, you will see ***YES** in the **Exit Inst?** column for the exit point.

3.1.3.6. Enable Group Profile Inheritance

Use this task to enable users to inherit privileges as defined in their IBM profile. In other words, if an IBM user profile is a member of group (as defined by the **Group profile** and/or **Supplemental group** profile parameters), then you can use the following instruction to ensure that rules (socket rules, exit rules, etc.) created in TGSecure consider the privileges inherited by users when the system is enforcing rules.

Here is a usage example. There are two IBM users: User AAA (higher privilege user) and user BBB (lower privilege user). An IBM user administrator decides to allow user BBB to inherit the privileges from user AAA. To do this, the IBM user administrator uses the command CHGUSRPR, and then enters AAA in the **Group profile** or **Supplemental group** parameter. By taking this action, the user administrator is allowing user BBB to inherit the privileges as user AAA. Now if you want the inherited privileges granted by the IBM user administrator to be considered in TGSecure when evaluating rules, then you must enable group profile inheritance in TGSecure.

To enable group profile inheritance

1) Access the **Network Security Defaults** interface.
2) In the **Primary Group Inheritance** field, enter ***YES**.

Note: The primary group is the user ID entered in the **Group profile** field when using command CHGUSRPRF. The primary group is the first ID from which a user inherits privileges.

3) In some cases, a user might inherit privileges from multiple users. In such as case, enter ***YES** in **Supplemental Group Inheritance** field.

Note: Supplemental groups are user IDs entered in the **Supplemental group** field when using command CHGUSRPRF. Each profile has the potential to be assigned up to 15 supplemental ID from which to inherit privileges.

4) Press **Enter**.

See also

Manage Exit Points

Run Network Security Reports

Working with Network Security Defaults

3.1.4. Run Network Security Reports

Use this task to generate network security reports.

Note: Refer to the TGSecure Report Reference for a complete list of report definitions.

To run the Network Security Reports

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the category (e.g., **1**, **2**, **3**, **4**) of report type you want to run.
7) Press **Enter**.
8) Choose the desired report from the list.
9) Press **Enter**.

See also

Run Transaction Reports

Run Socket Reports

Run Exit Point Reports

Run Exit Rule Reports

Run Socket Rule Reports

Working with Network Security Defaults

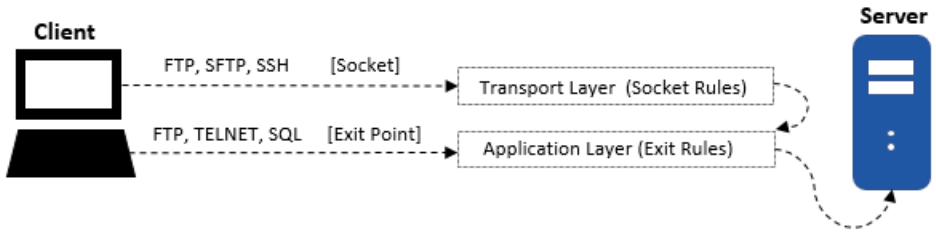
Working with Reports

3.2. Transactions

3.2.1. Working with Transactions

This section describes how to work with transactions. Remote transactions access the server through either a socket or exit point. The transaction can go directly from the client to the server through a socket unless an associated exit point has been defined. In which case, the system then checks for both socket and exit point rules before allowing access to the server.

For example, a user might attempt to access the system via the socket layer using FTP. If a socket rule exists for the FTP transactions, the system will validate that any socket rule criteria is met before allowing the FTP transaction. IBM has also established a standard exit point for FTP transactions, so any FTP transaction must also go through a second layer of security. The system will validate that any exit rules criteria is met before allowing the FTP transaction. Therefore, depending on the protocol used (e.g., FTP, SFTP, etc.), a transaction might go through both socket and exit point validation.



In order to work with incoming transactions, you must access the **Incoming Transactions** interface.

To access the Incoming Transactions interface

1) Log into to TGSecure.

Note: The **Main** menu appears.

2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.

Note: The **Network Security** interface is displayed.

4) At the **Selection or command** prompt, enter **1** (Incoming Transactions).
5) Press **Enter**.

Note: The **Incoming Transactions** interface is displayed.

See also

Log into TGSecure

Display List of Incoming Transactions

Manage Incoming Transactions

Run Transactions (*TRN) Reports

Run Socket (*SOC) Reports

3.2.2. Display List of Incoming Transactions

Use this task to do the following with transactions:

- Display list of transactions
- Sort transactions
- Move to a specific location within list of displayed transactions
- Filter transactions

3.2.2.1. Display List

Use this task to display the list of incoming transactions.

To display the list of incoming transactions

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.

Note: The **Network Security** interface is displayed.

4) At the **Selection or command** prompt, enter **1** (Incoming Transactions).
5) Press **Enter**.

Note: The **Incoming Transactions** interface is displayed.

Field	Description
Tran Type	There are two types of transactions: ***TRN** - Transaction coming through an exit point ***SOC** - Transaction coming through a socket
User	User who initiated the transaction
Server	Type of server
Function	Function being executed
SSL?	Whether SSL is enabled: ***YES** - SSL enabled ***NO** - SSL disabled ***N/A** - SSL Communication is not applicable
Client IP	IP address of the server initiating the transaction
Tran. Count	Total number of transactions attempted

	Note: The incoming transactions displayed in the interface are determined by the **Collector Status**. **Tip**: See Manage Exit Points for information about editing the **Collector Status**.
Object Details	Object effected by the transaction
Timestamp	Time at which the transaction was received

3.2.2.2. Sort List

Use this task to sort the list. The column on which the list is currently sorted appears in white text. For example, by default, the list is originally sorted by the **User** column so that column heading initially appears in white text.

To sort the list

1) Access the **Incoming Transactions** interface.
2) Place your cursor on the desired column heading.
3) Press the **F10** (Sort) function key.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

3.2.2.3. Move to Position in List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

To move to a specific position within the list

1) Access the **Incoming Transactions** interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.
4) Press **Enter**.

Note: The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

3.2.2.4. Filter List

Use this task to limit the objects displayed in the list by defining a subset for filtering purposes.

Tip: Use wildcard asterisk (*) to help define your subset.

-- Add an asterisk before text (e.g., *report) to find list items that end with specific text.

-- Add an asterisk after text (e.g., report*) to find list items that start with specific text.

-- Add asterisks around text (e.g., *report*) to find list items that contain specific text anywhere in the name.

To filter the list using a subset

1) Access the **Incoming Transactions** interface.
2) Press the **F8** (Subset) function key.
3) Enter the criteria you want to use to define the subset.

4) Press **Enter**.

Note: The system filters the results based on the criteria you defined for the subset.

See also

Working with Incoming Transactions

Manage Incoming Transactions

3.2.3. Manage Incoming Transactions

Use this task to do the following with incoming transactions:

- Display incoming transactions details
- Delete an incoming transaction
- Archive and then delete incoming transactions
- Create a security rule based on the transaction
- Accept rule suggestion

To manage incoming transactions, access the **Incoming Transactions** interface.

To access the Incoming Transactions interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **1** (Incoming Transactions).
5) Press **Enter**.

Note: The **Incoming Transactions** interface is displayed.

3.2.3.1. Display Incoming Transaction Details

Use this task to display the transaction details. There is limited space in the **Incoming Transactions** interface, so not all the details associated with an incoming transaction are displayed. Therefore, this task allows you to see the complete details for each incoming transaction.

To display the incoming transaction details

1) Access the **Incoming Transactions** interface.
2) In the **OPT** column for the desired transaction, enter **5** (Display).
3) Press **Enter**.

Field	Description
Transaction Type	There are two types of transactions: ***TRN** - Transaction coming through an exit point ***SOC** - Transaction coming through a socket
User Name	User who initiated the transaction
SSL Communication	Flag indicating whether SSL is enabled: ***YES** - SSL is enabled ***NO** - SSL is disabled

Field	Description
	***N/A** - SSL Communication is not applicable
Operation Server	Type of server
Function	Function being executed
Client IP	IP address of the server initiating the transaction
Server Name	Name of the server from which the user is initiating the transaction
Transaction Count	Total number of transactions attempted **Note**: The incoming transactions displayed in the interface are determined by the **Collector Status**. **Tip**: See Manage Exit Points for information about editing the **Collector Status**.
Action	Status of connection attempt (*PASS or *FAIL)
Reason	Reason for the transaction
Suggestion	Comments associated with the transaction
Object Details	Object effected by the transaction

3.2.3.2. Delete Incoming Transaction

Use this task to delete transactions.

Usage examples:

- You find that a specific transaction adds no value to your analysis
- You want to see what effect a new rule has on transactions from a specific client server
- You want to see what effect a new rule has on transactions for a specific user

To delete an incoming transaction

1) Access the **Incoming Transactions** interface.
2) In the **OPT** column for the desired transaction, enter **4** (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the correct transaction.
5) Press **Enter**.

3.2.3.3. Archive Incoming Transactions

Use this task to delete (cleanup) incoming transactions older than a specified date. You also have the option to create an archive before deleting the transactions. This is useful if you need to restore the list of transactions at a later point.

Usage examples:

- You want to delete older transactions to see what new transaction are coming in.
- You want to perform a transaction count.

For example, the customer might state that the product is running slowly. Therefore, you clear (delete) the transactions to get a better picture of what is occurring on the server. You discover that the customer is running hundreds of thousands of connections per second just to read one file. This is very inefficient and the transaction counts helps show this.

To archive incoming transactions

1) Access the **Incoming Transactions** interface.
2) Press the **F16** (Archive/Delete Transactions) function key.

Tip: For function keys higher than F12, you must use a combination of the **Shift** key and the appropriate function key. For example, to select F16, you must hold down the **Shift** key and F4.

3) Enter the age (in days) of the transactions you want to keep.

Note: For example, enter **1** to keep all transaction for today, but delete all transaction older than 1 day.

4) Enter ***YES** to create an archive before deleting the transactions.

3.2.3.4. Create a Rule Based on a Transaction

Use this task to create a security rule to address a security risk identified in your analysis of incoming transactions. For example, while you are reviewing the list of incoming transaction, you might identify suspicious activity coming from a server. You can quickly create a security rule (e.g., socket or exit rule) to block transactions from that server directly from the **Incoming Transactions** interface.

To create a security rule based on a transaction

1) Access the **Incoming Transactions** interface.
2) In the **OPT** column for the desired transaction, enter **1** (Create).

Note: The **Tran Type** field identifies the type of transaction: SOC = socket and TRN = exit point transaction. The screen the appears next is dependent on the type of transaction. The **Create Rule - Socket** screen appears when you are creating a socket rule and the **Create Rule - Exit** screen appears when you are creating an exit rule.

3) Press **Enter**.
4) Enter the necessary parameters to define your rule.
5) Press the **F23** (Accept Rule) function key.

Tip: For function keys higher than F12, you must use a combination of the **Shift** key and the appropriate function key. For example, to select F23, you must hold down the **Shift** key and F11.

6) Press **Enter**.

Note: At this point, you might receive suggestions from the Rules Suggestion Engine. For example, instead of creating a new rule for a specific user, it might be more efficient to add the user to an existing user group thereby reducing the total number of rules that must be managed. This same concept applies to network groups (client or server) as well.

Tip: If you decide to accept a suggestion, but then change your mind, in the **OPT** column for the desired rule, enter **6** (Undo Suggestion). **Note**: The opportunity the undo a suggestion is only available during the current session. Once you exit the session (press **F3** or **F12**), the option to undo the suggestion is lost. Any change after the point must be made manually by updating the group(s).

3.2.3.5. Accept a Rule Suggestion

Use this task to accept a suggestion made by the Rules Suggestion Engine. The intelligence engine provides suggestion when it might be more efficient to update a group versus create a new rule. In other words, a rule might already exist that utilizes a group, and instead of creating a new rule specific to an individual user, it might be more efficient to add the user to an existing user group that is reference by an existing rule. Therefore, a new rule is not created. Instead an existing user group is updated.

Note: You will only see the **Rule Suggestion** interface when the intelligence engine finds an opportunity to better utilize existing groups.

Tip: You can press **12** (Cancel) to reject any suggestions and exit the **Rule Suggestion** interface at any time.

To accept a rule suggestion

Obviously, the suggestions provided by the intelligence engine will vary depending on the situation, but expect to see one of the following variations:

Situation	If...	Then...
1	The intelligence engine provides one suggestion.	In the **Opt** column, enter **1** to acknowledge acceptance of the suggestion, and then press **Enter** to exit the **Rule Suggestion** interface.
2	The intelligence engine provides multiple suggestions from which you can select. For example, for socket rules, you could add the user to a user group, or you could add the client IP to a network group, or you could add the server name to a network group. In addition, for exit rules, operation can be added to operation groups, and object can be added to object groups.	In the **Opt** column, enter **1** beside the suggestion you feel is the most appropriate for your situation, and then press **Enter** to exit the **Rule Suggestion** interface.
3	Multiple groups must be modified in combination. In other words, to eliminate the need for the new rule, you must update a user group and a network group in combination. Therefore, in this situation, multiple groups are modified simultaneously.	Press **F23** (Confirm Adding to Group), and then press **Enter** to exit the **Rule Suggestion** interface.
4	You want to reject any and all suggestions.	Press **12** (Cancel) to exit the **Rule Suggestion** interface.

Tip: Use option **6** (Undo Suggestion) from the **Incoming Transactions** interface to undo your selection. Once you exit the session (press **F3** or **F12**), the ability to undo a suggestion is lost.

See also

Rules Suggestion Engine

Rules Decision Engine

Manage User Groups

Manage Socket Rules

Manage Exit Rules

Working with Transactions

3.2.4. Run Transactions (*TRN) Report

Use this task to generate reports that display the following for incoming transactions:

- Incoming transaction details
- Incoming transaction summary by server
- Incoming transaction summary by user
- Network transaction details

Note: Refer to the TGSecure Report Reference for a complete list of report definitions.

To work with exit point reports, access from the **Network Reports** interface.

3.2.4.1. Access the Network Reports Interface

To access the Access Escalation Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.

Note: The **Network Reports** interface is displayed.

3.2.4.2. Run Incoming Transaction Details

Use this report to display incoming transaction details.

To run the Incoming Transactions Details Report

1) Access the **Network Reports** interface.
2) At the **Selection or command** prompt, enter **1** (Transaction Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **1** (Incoming Transactions Report).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

3.2.4.3. Run Transaction Summary by Server Report

Use this report to display incoming transaction details by server.

To run the Transaction Summary by Server Report

1) Access the **Network Reports** interface.
2) At the **Selection or command** prompt, enter **2** (Summary Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **3** (Transaction Summary by Server).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

3.2.4.4. Run Transaction Summary by User Report

Use this report to display incoming transaction details by user.

To run the Transaction Summary by User Report

1) Access the **Network Reports** interface.
2) At the **Selection or command** prompt, enter **2** (Summary Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **4** (Transaction Summary by User).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

3.2.4.5. Run Network Transaction Report

Use this report to display network transaction.

To run the Network Transaction Report

1) Access the **Network Reports** interface.
2) At the **Selection or command** prompt, enter **1** (Transaction Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **3** (Network Transaction Report).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

See also:

Working with Transactions

Working with Reports

*3.2.5. Run Socket Transaction (*SOC) Reports*

Use this task to generate reports that display the following for socket rules.

- Socket transactions details
- Socket summary by server
- Socket summary by user

Note: Refer to the TGSecure Report Reference for a complete list of report definitions.

To work with socket transaction reports, access from the **Network Reports** interface.

3.2.5.1. Access the Network Reports Interface

To access the Access Escalation Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.

Note: The **Network Reports** interface is displayed.

3.2.5.2. Run Socket Transaction Report

Use this report to display the socket transaction details.

To run the Socket Transaction Report

1) Access the **Network Reports** interface.
2) At the **Selection or command** prompt, enter **1** (Transaction Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **2** (Socket Transactions Report).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

3.2.5.3. Run Socket Summary by Server Report

Use this report to display socket transaction details by server.

To run the Socket Summary by Server Report

1) Access the **Network Reports** interface.
2) At the **Selection or command** prompt, enter **2** (Summary Reports).

3) Press **Enter**.
4) At the **Selection or command** prompt, enter **1** (Socket Summary by Server).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

3.2.5.4. Run Transaction Summary by User Report

Use this report to display socket transaction details by user.

To run the Transaction Summary by User Report

1) Access the **Network Reports** interface.
2) At the **Selection or command** prompt, enter **2** (Summary Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **2** (Socket Summary by User).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

See also:

Working with Transactions

Working with Reports

3.3. Exit Points

3.3.1. Working with Exit Points

This section describes working with exit points. In the beginning of computing, the risk related to network security was limited to internal networks and required limited security measures. With the advancement of technology and with the increase in availability of open networks, security risks have increased. To bridge the security gap caused by open networks, IBM introduced remote exit points, which are hooks that allow you to attach custom exit programs that evaluate exit rules, which define the criteria used to determine whether a transaction should be allowed or rejected.

Analogy

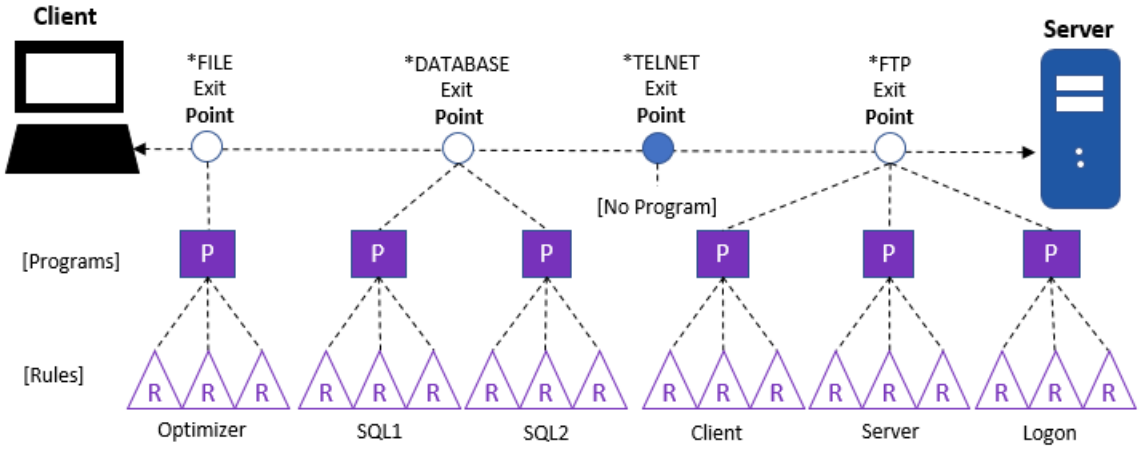
The prior paragraph uses a lot of jargon, so here is an analogy to help you conceptualize what an exit point represents. Say that your IBM server is a building. In the past, if someone wanted to access your building, they would just walk to it. Then, at some point, people started riding horses, and then bicycles, and then cars. To accommodate these newer forms of transportation, IBM built a parking lot. In the parking lot, they provided spots (points): a hitching rail for the horses, a bicycle rack for the bikes, and painted parking slots for the cars. You can image exit points as the elements in a parking lot that accommodate the different modes of transportation. So now image your exit program as a vehicle (a car) that you can park in an exit point (parking spot). Your vehicle (exit program) carries in it passengers (exit rules). Once an exit program is parked in an exit point, the rules (passengers) associated with that exit program become linked to the exit point.

Client-Server Communication Process via transport layer:

(1) Exit Point (Parking Spot): An exit point is a point in the network communication process between a client and a server where control is turned over to an exit program if an exit program exists.

(2) Exit Program (Car): An exit programs can be created for each type of network communication (FTP, ODBC, JDBC, SQL, etc.). Exit programs control execution of transactions between a client and a server.

(3) Exit Rule (Passenger): An exit rule defines the criteria by which an exit program determines whether a transaction is allowed or rejected (forbidden).



Note: It's not necessary to manually associate an exit rule to an exit program. That happens programmatically, but it is necessary to associate an exit program to an exit point. In other words, you must install (add) a program to a point, and the program (once installed) searches through the list of available exit rules to determine which rules should be applied.

In order to work with exit points, you must access the **Network Security Configuration** interface.

To access the Network Security Configuration interface

1) Log into to TGSecure.

Note: The **TGSecure Main** menu appears.

2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.

Note: The **Network Security** interface is displayed.

4) At the **Selection or command** prompt, enter **10** (Exit Point Configuration).
5) Press **Enter**.

Note: The **Network Security Configuration** interface is displayed.

See also

Display List of Exit Points

Manage Exit Points

Run Exit Points Report

3.3.2. Display List of Exit Points

Use this task to display the list of exit points.

To display the list of exit points

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.

Note: The **Network Security** interface is displayed.

4) At the **Selection or command** prompt, enter **10** (Exit Point Configuration).
5) Press **Enter**.

Note: The **Network Security Configuration** interface is displayed.

Tip: Each row in the display represents an exit point. If ***YES** appears in the **Exit Inst?** column, that indicates that an exit program is installed at that exit point.

Field	Description
Network Server	Name of the server type
Audit Status	Whether auditing is enabled for a specific exit point. Auditing is required if you plan to run network security reports ***YES** - Record incoming transaction data in the audit journal ***NO** - Do not record incoming transaction data in the audit journal **Tip**: If auditing is disabled at the module level, then this setting is ignored. In other words, if auditing is disabled at the network security (module) level, then auditing will not occur even if auditing is enabled at the exit point (secondary) level. The module level setting takes precedence. However, if auditing is enabled at the module level, you must also enable alerting at the secondary level if you want to record auditing data for a specific exit point. **Note**: See Manage Network Security Defaults for information about enabling/disabling auditing globally.
Sec Status	Whether security is enabled for a specific exit point. Once you enable security, the exit rules associated with the exit point go in to effect. ***YES** - Apply exit rules (enable network security) ***NO** - Disable exit rules (disable network security)
Alert Status	Whether alerting is enabled for a specific exit point. Alerts are required if you plan to send alert notifications ***ALL** - Record an alert for all (PASS and FAIL) connection attempts

	***FAIL** - Record only FAIL connection attempts ***NONE** - Do not record alerts **Tip**: If alerts are disabled at the module level, then this setting is ignored. In other words, if alerts are disabled at the network security (module) level, then alerts are not stored in the message queue even if alerts are enabled at the exit point (secondary) level. The module level setting takes precedence. However, if alerts are enabled at the module level, you must also enable alerts at the secondary level if you want to record alerts for a specific exit point. See Manage Network Security Defaults for information about enabling/disabling alerting globally.
Smart Mode	Whether the smart mode (Rules Intelligence Engine) is enabled ***YES** - Enable the intelligence engine to create rules based on AI (artificial intelligence) analysis of incoming transactions ***NO** - Do not enable the intelligence engine to create rules **Note**: The system administrator can delete rules created by the Rules Intelligence Engine at any time.
Collector Status	Which incoming transactions you want to track (collect) in the **Incoming Transaction** interface ***ALL** - Collect and display all (PASS and FAIL) incoming transactions ***FAIL** - Collect and display only rejected (FAIL) incoming transactions ***NONE** - Do not collect or display any incoming transactions
Function Usage	Whether an IBM function usage rule is being applied at the exit point. This indicator is important because it helps to identify conflicts between exit rules and function usage rules. If there is a conflict (e.g., an exit rule states to do one thing, but a function usage rule states to do something different), then the system might produce an unexpected outcome. ***YES** - A function usage rule is applied at the exit point, so the potential for conflict with an exit rule exists ***NO** - No function usage rule is applied at the exit point ***NA** - Not applicable because IBM does not provide a function usage rule for this exit point
Exit Inst?	Whether the exit point is installed on the server ***YES** - Exit points are installed and ready for use ***NO** - Exit points are not installed **Note**: The exit rules associated with the exit point are not applied until the exit point is installed and the **Security Status** is set to ***YES**.
Network Description	A short description of the network

See also

Working with Exit Point

3.3.3. Manage Exit Points

Use this task to do the following with exit points.

- Display exit point details
- Enable exit point auditing
- Enable exit point security

- Enable exit point alerts
- Enable exit point incoming transaction collection
- Add an exit program to exit point
- Remove an exit program from an exit point
- Cycle (restart) a server
- Cycle multiple servers (mass update)
- Update all exit points (mass update)

To manage exit points, access the **Work with Network Security Configuration** interface.

To access the Work with Network Security Configuration

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.

Note: The **Network Security** interface is displayed.

4) At the **Selection or command** prompt, enter **10** (Exit Point Configuration).
5) Press **Enter**.

Note: The **Network Security Configuration** interface is displayed.

3.3.3.1. Display Exit Point Details

Use this task to display the details (definition) for a specific exit point. There is limited space in the **Network Security Configuration** interface, so not all the details associated with an exit point are displayed. Therefore, this task allows you to see the complete details for each exit point.

To display exit point details

1) Access the **Network Security Configuration** interface.
2) In the **OPT** column for the desired exit point, enter **5** (Display).
3) Press **Enter**.

Field	Description
Network Server	Name of the server type
Exit Point	Name assigned to the exit point
Exit Format	IBM format associated with the exit point
Exit Description	Description of the exit point
Exit Program Installed	Indicates whether the exit point is installed on the server ***YES** - Exit points are installed and ready for use ***NO** - Exit points are not installed **Note**: The exit rules associated with the exit point are not applied until the exit point is installed and the **Security Status** is set to ***YES**.
Function Usage Rule	Indicates whether an IBM function usage rule is being applied at the exit point. This indicator is important because it helps to identify conflicts between exit rules and function usage rules.

	If there is a conflict (e.g., an exit rule states to do one thing, but a function usage rule states to do something different), then the system might produce an unexpected outcome. ***YES** - A function usage rule is applied at the exit point, so the potential for conflict with an exit rule exists ***NO** - No function usage rule is applied at the exit point ***NA** - Not applicable because IBM does not provide a function usage rule for this exit point
Audit Status	Indicates whether auditing is enabled for a specific exit point. Auditing is required if you plan to run network security reports ***YES** - Record incoming transaction data in the audit journal ***NO** - Do not record incoming transaction data in the audit journal **Tip**: If auditing is disabled at the module level, then this setting is ignored. In other words, if auditing is disabled at the network security (module) level, then auditing will not occur even if auditing is enabled at the exit point (secondary) level. The module level setting takes precedence. However, if auditing is enabled at the module level, you must also enable alerting at the secondary level if you want to record auditing data for a specific exit point. **Note**: See Manage Network Security Defaults for information about enabling/disabling auditing globally.
Security Status	Indicates whether security is enabled for a specific exit point. Once you enable security, the exit rules associated with the exit point go in to effect. ***YES** - Apply exit rules (enable network security) ***NO** - Disable exit rules (disable network security)
Alert Status	Indicates whether alerts are enabled for a specific exit point. Alerts are required if you plan to send alert notifications ***ALL** - Record an alert for all (PASS and FAIL) connection attempts ***FAIL** - Record only FAIL connection attempts ***NONE** - Do not record alerts **Tip**: If alerts are disabled at the module level, then this setting is ignored. In other words, if alerts are disabled at the network security (module) level, then alerts are not stored in the message queue even if alerts are enabled at the exit point (secondary) level. The module level setting takes precedence. However, if alerts are enabled at the module level, you must also enable alerts at the secondary level if you want to record alerts for a specific exit point. See Manage Network Security Defaults for information about enabling/disabling alerting globally.
Smart Mode	Indicates whether the smart mode (Rules Intelligence Engine) is enabled ***YES** - Enable the intelligence engine to create rules based on AI (artificial intelligence) analysis of incoming transactions ***NO** - Do not enable the intelligence engine to create rules **Note**: The system administrator can delete rules created by the Rules Intelligence Engine at any time.
Collector Status	Indicates which incoming transactions you want to track (collect) in the **Incoming Transaction** interface ***ALL** - Collect and display all (PASS and FAIL) incoming transactions ***FAIL** - Collect and display only rejected (FAIL) incoming transactions ***NONE** - Do not collect or display any incoming transactions

3.3.3.2. Enable Exit Point Auditing

Use this task to enable auditing of incoming transactional data for a specific exit point. Auditing is required if you plan to run network security reports.

Prerequisite

Auditing must be enabled in the Network Security Module. See Manage Network Security Defaults.

To enable auditing for an exit point

1) Access the **Network Security Configuration** interface.
2) In the **OPT** column for the desired exit point, enter **2** (Edit).
3) Press **Enter**.
4) In the **Audit Status** field, enter ***YES**.
5) Press **Enter**.

3.3.3.3. Enable Exit Point Security

Use this task to enable security for a specific exit point. Once you enable security, the exit rules associated with the exit point go into effect.

Prerequisite

Create the exit rules you want to apply. See Manage Exit Rule.

Tip: Ensure that your rules provide the appropriate level of user access. If you fail to design your rules properly, you might block legitimate users from performing necessary work transactions.

To enable security for an exit point

1) Access the **Network Security Configuration** interface.
2) In the **OPT** column for the desired exit point, enter **2** (Edit).
3) Press **Enter**.
4) In the **Security Status** field, enter ***YES**.
5) Press **Enter**.

3.3.3.4. Enable Exit Point Alerts

Use this task to enable alerts for a specific exit point. Alerts are required if you plan to send alert notifications.

Prerequisite

Alerts must be enabled in the Network Security module, see Manage Network Security Defaults.

To enable alerts for an exit point

1) Access the **Network Security Configuration** interface.
2) In the **OPT** column for the desired exit point, enter **2** (Edit).
3) Press **Enter**.
4) In the **Alert Status** field, enter one of the following:

– ***ALL** - Record an alert for all (PASS and FAIL) connection attempts
– ***FAIL** - Record only FAIL connection attempts

5) Press **Enter**.

3.3.3.5. Enable Exit Point Collection

Use this task to enable the collection of incoming transactions for a specific exit point in the **Incoming Transaction** interface.

To enable incoming transaction collection for an exit point

1) Access the **Network Security Configuration** interface.
2) In the **OPT** column for the desired exit point, enter **2** (Edit).
3) Press **Enter**.
4) In the **Alert Status** field, enter one of the following:

– ***ALL** - Collect and display all (PASS and FAIL) incoming transactions
– ***FAIL** - Collect and display only rejected (FAIL) incoming transactions

5) Press **Enter**.

3.3.3.6. Add Exit Program to Exit Point

Use this task to add (install) an exit program to a single exit point. The system provides pre-built exit programs for each of the established IBM exit points. You have control of whether to add (install) a pre-built exit program to an exit point. The exit programs are what house the exit rules.

Note: It's not necessary to manually associate an exit rule to an exit program. That happens programmatically, but it is necessary to associate an exit program to an exit point. In other words, you must install (add) a program to a point, and the program (once installed) searches through the list of available exit rules to determine which rules should be applied.

To add exit program to exit point

1) Access the **Network Security Configuration** interface.
2) In the **OPT** column for the desired exit point, enter **11** (Add Exit Program).
3) Press **Enter**.

Note: Once an exit program is installed at an exit point, you will see ***YES** in the **Exit Inst?** column for the exit point.

3.3.3.7. Add Exit Programs to Exit Points (Mass Update)

Use this task to add (install) exit programs to multiple exit points.

Note: Once complete, you will see ***YES** in the **Exit Inst?** column for all modified exit points.

To add an exit programs to exit points

1) Access the **Network Security Configuration** interface.
2) Press the **F20** (Add Exit Programs) function key.

Tip: For function keys higher than F12, you must use a combination of the **Shift** key and the appropriate function key. For example, to select F20, you must hold down the **Shift** key and F8.

3) Enter ***All** to add all exit points to an exit program or enter a specific server type.
4) Press **Enter**.

3.3.3.8. Remove Exit Program from Exit Point

Use this task to remove exit program from single exit point.

Note: Once the exit program is uninstalled, you will see ***NO** in the **Exit Inst?** column for the modified exit point.

To remove an exit program from exit point

1) Access the **Network Security Configuration** interface.
2) In the **OPT** column for the desired exit point, enter **12** (Remove Exit Program).
3) Press **Enter**.

3.3.3.9. Remove Exit Programs from Exit Points (Mass Update)

Use this task to remove (uninstall) exit programs to multiple exit points.

Note: Once complete, you will see ***NO** in the **Exit Inst?** column for all modified exit points.

To remove an exit programs from exit points

1) Access the **Network Security Configuration** interface.
2) Press the **F21** (Remove Exit Programs) function key.

Tip: For function keys higher than F12, you must use a combination of the **Shift** key and the appropriate function key. For example, to select F21, you must hold down the **Shift** key and F9.

3) Enter ***All** to remove all exit programs or enter a specific server type.
4) Press **Enter**.

3.3.3.10. Cycle Server

Use this task to restart a single server. Cycling a server is useful when you add an exit program and you want to ensure that the exit rule(s) associated with that program are applied immediately (including to transactions currently running.) For example, there might be pre-start jobs that are running. In order for a new rule(s) to be applied to the pre-start jobs, the jobs must be stopped and restarted (cycled) for the new exit rule(s) to take effect.

To cycle a single server

1) Access the **Network Security Configuration** interface.
2) In the **OPT** column for the desired exit point, enter **13** (Cycle Server).
3) Press **Enter**.
4) Ensure that the correct server is selected.
5) Enter one of the following options:

– **Y** - Initiate cycling immediately (run in interactive mode)
– **N** - Place cycling request in queue (run as part of a job queue)

6) Press **Enter**.

3.3.3.11. Cycle Servers (Mass Update)

Use this task to restart multiple servers.

To cycle multiple servers

1) Access the **Network Security Configuration** interface.
2) Press the **F19** (Cycle Servers) function key.

Tip: For function keys higher than F12, you must use a combination of the **Shift** key and the appropriate function key. For example, to select F19, you must hold down the **Shift** key and F7.

3) Enter ***All** to cycle all servers or identify a specific server type.
4) Enter **Y** to execute the cycling immediately or **N** to add it a batch.
5) Press **Enter**.

3.3.3.12. Update all Exit Points (Mass Update)

Use this task to perform a mass update of all exit points.

To update all exit points

1) Access the **Network Security Configuration** interface.
2) Press the **F7** (Update all) function key.
3) Modify the setting as necessary.

Note: All editable settings are underlined.

Field	Description
Audit Status	Indicates whether auditing is enabled. Auditing is required if you plan to run network security reports. ***YES** - Record incoming transaction data in the audit journal for all installed exit points ***NO** - Do not record incoming transaction data in the audit journal for all installed exit points ***SAME** - Do not perform a mass update of the **Audit Status**. In other words, skip this setting. **Tip**: See Manage Network Security Defaults for information about enabling auditing globally. Global defaults take precedence over local settings.
Security Status	Indicates whether the exit rules associated with the exit point should be applied. ***YES** - Apply exit rules for all installed exit points ***NO** - Do not apply exit rules for all installed exit points ***SAME** - Do not perform a mass update of the **Security Status**. In other words, skip this setting during the mass update.
Alert Status	Indicates whether alerting is enabled. Alerting is required if you plan to send alert notifications. ***ALL** - Record an alert for all (PASS and FAIL) connection attempts ***FAIL** - Record only FAIL alerts for all installed exit points ***NONE** - Do not record alerts for all installed exit points ***SAME** - Do not perform a mass update of the **Alert Status**. In other words, skip this setting during the mass update. **Tip**: See Manage Network Security Defaults for information about enabling alerting globally. Global defaults take precedence over local settings.
Smart Mode	Indicates whether the smart mode (Rules Intelligence Engine) is enabled ***YES** - Enable the intelligence engine to create rules based on AI (artificial intelligence) analysis of incoming transactions ***NO** - Do not enable the intelligence engine to create rules ***SAME** - Do not perform a mass update of the **Smart Mode**. In other words, skip this setting during the mass update.

Collector Status	Indicates which incoming transactions are tracked (collect) in the **Incoming Transaction** interface. ***ALL** - Collect and display all (PASS and FAIL) connection attempts ***FAIL** - Collect and display only FAIL connection attempts ***NONE** - Do not collect or display any connection attempts ***SAME** - Do not perform a mass update of the **Collector Status**. In other words, skip this setting during the mass update.

4) Press **Enter**.

See also

Working with Exit Point

3.3.4. Run Exit Points Report

Use this task to generate reports that display the following for exit points:

- Exit point configuration details
- Exit point configuration changes

Note: Refer to the TGSecure Report Reference for a complete list of report definitions.

To work with exit point reports, access from the **Network Reports** interface.

3.3.4.1. Access the Network Reports Interface

To access the Access Escalation Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.

Note: The **Network Reports** interface is displayed.

3.3.4.2. Run Exit Point Configuration Report

Use this report to display exit point configuration details for exit points.

To run the Exit Point Configuration Report

1) Access the **Network Reports** interface.
2) At the **Selection or command** prompt, enter **3** (Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **3** (Exit Point Configuration Report).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

3.3.4.3. Run Exit Point Configuration Changes Report

Use this report to display the list of configuration changes made to exit points.

Tip: You must enable auditing to produce change reports. See Manage Network Security Defaults for additional information.

To run the Exit Point Configuration Change Report

1) Access the **Network Reports** interface.
2) At the **Selection or command** prompt, enter **4** (Configuration Changes).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **3** (Exit Point Configuration Changes).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

See also

Working with Exit Point

Working with Reports

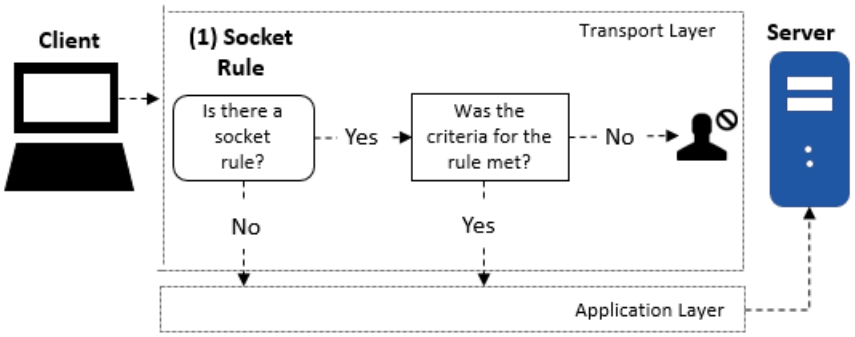
3.4. Socket Rules

3.4.1. Working with Socket Rules

This section describes working with socket rules. Socket rules allow you to address security risks associated with newer protocols (e.g., SFTP and SSH), which are not covered by exit rules at the application level. The newer protocols were designed to address weakness in older protocols (e.g., FTP, TELNET, ODBC, and SQL.) in which data was transmitted in clear text. While the newer protocols reduced some security risks, they opened the door to others. The newer protocols use socket communication at the transaction level, and in some cases might allow users to bypass security established using exit rules at the application level.

Example Usage:

A rule might be created to reject an incoming transaction (connection) to the server listening on a specific port or coming from a particular remote IP address after business hours (6pm - 6am).



In order to work with socket rules, you must access the **Work with Socket Rules** interface.

To access the Work with Socket Rules interface

1) Log into to TGSecure.

Note: The **Main** menu appears.

2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.

Note: The **Network Security** interface is displayed.

4) At the **Selection or command** prompt, enter **2** (Socket Rules).
5) Press **Enter**.

Note: The **Work with Socket Rules** interface is displayed.

See also

Log into TGSecure

Display List of Socket Rules

Manage Socket Rules

Run Socket Rules Report

3.4.2. Display List of Socket Rules

Use this task to do the following with socket rules:

- Display list of socket rules
- Sort socket rules
- Move to a specific location within list of socket rules
- Filter socket rules

3.4.2.1. Display List

Use this task to display the list of socket rules.

To display the list of socket rules

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).

3) Press **Enter**.

Note: The **Network Security** interface is displayed.

4) At the **Selection or command** prompt, enter **2** (Socket Rules).
5) Press **Enter**.

Note: The **Work with Socket Rules** interface is displayed.

Field	Description
User	User or user group that initiated the transaction
Operation Port	Port from which the transaction was initiated
Client IP	IP address from which the transaction was initiated
Calendar	Applicable calendar
Alert Status	Whether alerting is enabled: ***YES** - Alerts enabled ***NO** - Alerts disabled
Action	The level at which action was taken: ***EXITLVL** - Exit point level **Note**: If the action failed, you will see ***FAIL** in this column.

3.4.2.2. Sort List

Use this task to sort the list. The column on which the list is currently sorted appears in white text. For example, by default, the list is originally sorted by the **User** column so that column heading initially appears in white text.

To sort the list

1) Access the **Work with Socket Rules** interface.
2) Place your cursor on the desired column heading.
3) Press the **F10** (Sort) function key.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

3.4.2.3. Move to Position in List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down to locate a network.

To move to a specific position within the list

1) Access the **Work with Socket Rules** interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.
4) Press **Enter**.

Note: The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

3.4.2.4. Filter List

Use this task to limit the objects displayed in the list by defining a subset for filtering purposes.

Tip: Use wildcard asterisk (*) to help define your subset.

-- Add an asterisk before text (e.g., *report) to find list items that end with specific text.

-- Add an asterisk after text (e.g., report*) to find list items that start with specific text.

-- Add asterisks around text (e.g., *report*) to find list items that contain specific text anywhere in the name.

To filter the list using a subset

1) Access the **Work with Socket Rules** interface.
2) Press the **F8** (Subset) function key.
3) Enter the criteria you want to use to define the subset.
4) Press **Enter**.

Note: The system filters the results based on the criteria you defined for the subset.

See also

Working with Socket Rules

Manage Socket Rules

3.4.3. Manage Socket Rules

Use this task to do the following with socket rules:

- Add a socket rule
- Edit a socket rule
- Copy a socket rule
- Delete a socket rule
- Display list of users in a group
- Display list of client networks
- Display list of server networks
- Display list of operations

To manage socket rules, access the **Work with Socket Rules** interface.

To access the Work with Socket Rules interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.

Note: The **Network Security** interface is displayed.

4) At the **Selection or command** prompt, enter **2** (Socket Rules).
5) Press **Enter**.

Note: The **Work with Socket Rules** interface is displayed.

3.4.3.1. Add Socket Rule

Use this task to add a socket rule.

Tip: You can define a socket rule for an individual user, network, or operation, and you can define them for groups of users, networks, or operations.

To add a socket rule

1) Access the **Work with Socket Rules** interface.
2) Press the **F6** (Add) function key.
3) Define the rule using the fields provided.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

4) Press **Enter**.

Note: At this point, you might receive suggestions from the system. For example, instead of creating a new rule for a specific user, it might be more efficient to add the user to an existing user group thereby reducing the total number of rules that must be managed. This same concept applies to network groups (client or server) as well.

See also

Rules Suggestion Engine
Rules Decision Engine
Manage User Groups
Manage Socket Rules
Manage Exit Rules

3.4.3.2. Edit Socket Rule

Use this task to edit an existing socket rule.

To edit a socket rule

1) Access the **Work with Socket Rules** interface.
2) In the **OPT** column for the desired socket rule, enter **2** (Edit).
3) Press **Enter**.
4) Modify the parameters as necessary.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

5) Press **Enter** twice.

3.4.3.3. Copy Socket Rule

Use this task to create a new rule by copying a socket rule.

To copy a socket rule

1) Access the **Work with Socket Rules** interface.
2) In the **OPT** column for the desired socket rule, enter **3** (Copy).
3) Press **Enter**.
4) Modify the parameters as necessary.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

5) Press **Enter**.

3.4.3.4. Delete Socket Rule

Use this task to delete a socket rule.

To delete a socket rule

1) Access the **Work with Socket Rules** interface.
2) In the **OPT** column for the desired socket rule, enter **4** (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the correct rule.
5) Press **Enter**.

3.4.3.5. Display List of Users in a Group

Use this task when the **User Name** field contains a user group. You can access the user group at this point to display its details or modify the group.

Tip: Group names always begin with a colon.

To display the list of users

1) Access the **Work with Socket Rules** interface.
2) In the **OPT** column for the desired socket rule, enter **6** (User Grp).
3) Press **Enter**.
4) Review the list of users.

Tip: You can modify the user group at this point as well.

3.4.3.6. Display List of Clients in a Group

Use this task when **Client IP** field contains a network group. You can access the network group at this point to display its details or modify the group.

Tip: Group names always begin with a colon.

To display the list of clients

1) Access the **Work with Socket Rules** interface.
2) In the **OPT** column for the desired socket rule, enter **7** (Client Grp).
3) Press **Enter**.
4) Review the list of clients.

Tip: You can modify the network group at this point as well.

3.4.3.7. Display List of Servers in a Group

Use this task when the **Server Name** field contains a network group. You can access the network group at this point to display its details or modify the group.

Tip: Group names always begin with a colon.

To display the list of servers

1) Access the **Work with Socket Rules** interface.
2) In the **OPT** column for the desired socket rule, enter **8** (Server Grp).
3) Press **Enter**.
4) Review the list of servers.

Tip: You can modify the network group at this point as well.

3.4.3.8. Display List of Operations in a Group

Use this task when the **Operation/Port** field contains an operation group. You can access the operation group at this point to display its details or modify the group.

Tip: Group names always begin with a colon.

To display the list of operations

1) Access the **Work with Socket Rules** interface.
2) In the **OPT** column for the desired socket rule, enter **9** (Opr. Grp).
3) Press **Enter**.
4) Review the list of operations.

Tip: You can modify the operation group at this point as well.

See also

Working with Socket Rules

3.4.4. Run Socket Rule Reports

Use this task to generate reports that display the following for socket rules.

- Socket rule configuration details
- Socket rule configuration changes

Note: Refer to the TGSecure Report Reference for a complete list of report definitions.

To work with socket rule reports, access from the **Network Reports** interface.

3.4.4.1. Access the Network Reports Interface

To access the Access Escalation Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.

Note: The **Network Security** interface is displayed.

4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.

Note: The **Network Reports** interface is displayed.

3.4.4.2. Run Socket Rule Configuration Report

Use this report to display socket rule configuration details.

To run the Socket Rule Configuration Report

1) Access the **Network Reports** interface.
2) At the **Selection or command** prompt, enter **3** (Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **2** (Socket Rules Report).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

3.4.4.3. Run Socket Rule Configuration Changes Report

Use this report to display the list of configuration changes made to socket rules.

Tip: You must enable auditing to produce change reports. See Manage Network Security Defaults for additional information.

To run the Socket Rule Configuration Changes Report

1) Access the **Network Reports** interface.
2) At the **Selection or command** prompt, enter **4** (Configuration Changes).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **2** (Socket Rules Changes).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

See also

Working with Socket Rules

Working with Reports

3.5. Exit Rules

3.5.1. Working with Exit Rules

This section describes working with exit rules. Exit rules control network traffic associated with a specific application level communication protocol (i.e., FTP, TELNET, and ODB).

Example Usage:

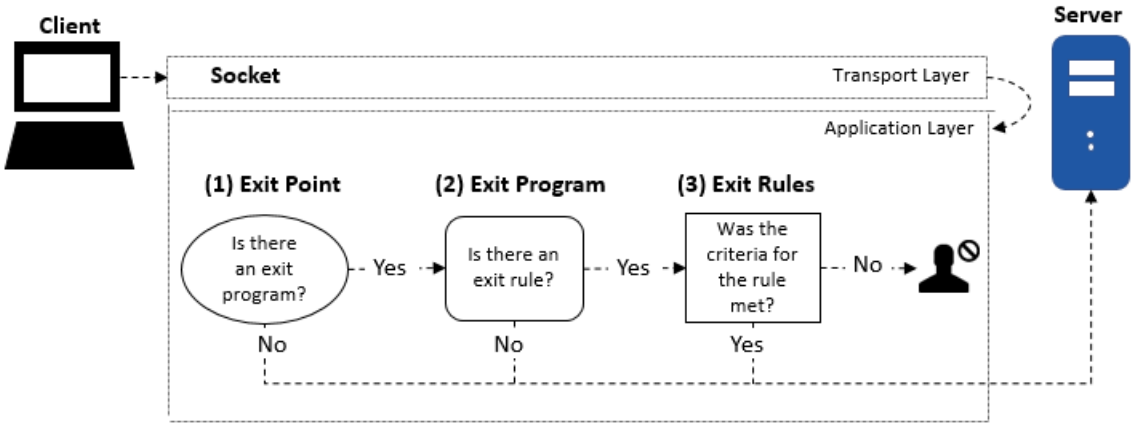
You might need a rule to reject all incoming transaction (connection) initiated by a specific user or member of a user group.

Client-Server Communication Process via transport layer:

(1) Exit Point: An exit point is a point in the network communication process between a client and a server where control is turned over to an exit program if an exit program exists.

(2) Exit Program: An exit programs can be created for each type of network communication (FTP, ODBC, JDBC, SQL, etc.). Exit programs control execution of transactions between a client and a server.

(3) Exit Rule: An exit rule defines the criteria by which an exit program determines whether a transaction is allowed or forbidden.



In order to work with exit rules, you must access the **Work with Exit Rules** interface.

To access the Work with Exit Rules interface

1) Log into to TGSecure.

Note: The **Main** menu appears.

2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.

Note: The **Network Security** interface is displayed.

4) At the **Selection or command** prompt, enter **3** (Remote Exit Rules).
5) Press **Enter**.

Note: The **Work with Exit Rules** interface is displayed.

See also

Log into TGSecure

Display List of Exit Rules

Manage Exit Rules

Run Exit Rule Reports

3.5.2. Display List of Exit Rules

Use this task to do the following with exit rule:

- Display list of exit rules
- Sort exit rules
- Move to a specific location within list of exit rules
- Filter exit rules

3.5.2.1. Display List

Use this task to display the list of exit rules.

To display the list of exit rules

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.

Note: The **Network Security** interface is displayed.

4) At the **Selection or command** prompt, enter **3** (Remote Exit Rules).
5) Press **Enter**.

Note: The **Work with Exit Rules** interface is displayed.

Field	Description
User	User or user group that initiated the transaction
Server	Server from which the transaction was initiated
Function	Function that was initiated
Client IP	IP address from which the transaction was initiated
Calendar	Applicable calendar
Alert Status	Whether alerting is enabled: ***YES** - Alerts enabled ***NO** - Alerts disabled
Action	The level at which action is taken: ***EXITLVL** - Exit point level **Note**: If the action failed, you will see ***FAIL** in this column.
Object Details	Short description of the object to which access was attempted

3.5.2.2. Sort List

Use this task to sort the list. The column on which the list is currently sorted appears in white text. For example, by default, the list is originally sorted by the **User** column so that column heading initially appears in white text.

To sort the list

1) Access the **Work with Exit Rules** interface.
2) Place your cursor on the desired column heading.
3) Press the **F10** (Sort) function key.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

3.5.2.3. Move to Position in List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down to locate a network.

To move to a specific position within the list

1) Access the **Work with Exit Rules** interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.
4) Press **Enter**.

Note: The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

3.5.2.4. Filter List

Use this task to limit the objects displayed in the list by defining a subset for filtering purposes.

Tip: Use wildcard asterisk (*) to help define your subset.

-- Add an asterisk before text (e.g., *report) to find list items that end with specific text.

-- Add an asterisk after text (e.g., report*) to find list items that start with specific text.

-- Add asterisks around text (e.g., *report*) to find list items that contain specific text anywhere in the name.

To filter the list using a subset

1) Access the **Work with Exit Rules** interface.
2) Press the **F8** (Subset) function key.
3) Enter the criteria you want to use to define the subset.
4) Press **Enter**.

Note: The system filters the results based on the criteria you defined for the subset.

See also

Working with Exit Rules

Manage Exit Rules

3.5.3. Manage Exit Rules

Use this task to do the following with exit rule:

- Add an exit rule
- Edit an exit rule
- Copy an exit rule
- Delete an exit rule
- Display list of users
- Display list of client networks
- Display list of server networks
- Display list of operations
- Display list of objects

To manage exit rules, access the **Work with Exit Rules** interface.

To access the Work with Exit Rules interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.

Note: The **Network Security** interface is displayed.

4) At the **Selection or command** prompt, enter **3** (Remote Exit Rules).
5) Press **Enter**.

Note: The **Work with Exit Rules** interface is displayed.

3.5.3.1. Add Exit Rule

Use this task to add an exit rule.

To add an exit rule

1) Access the **Work with Exit Rules** interface.
2) Press the **F6** (Add) function key.
3) Complete the following fields:

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

Field	Description
User Name	User or user group to which the rule applies
Client IP	IP address to which the rule applies
Operation Server	The server to which the rule applies
Function	Function to which the rule applies
Calendar	Applicable calendar
Alert Status	Whether alerting is enabled: ***YES** - Alerts enabled ***NO** - Alerts disabled

Action	The action that triggers a message: ***FAIL** - Send message if case of fail ***PASS** - Send message in case of pass
Rule Description	Short description of the rule
Type of Object	Object type to which the rule applies: ***QSYS** - limit the rule to QSYS objects ***IFS** - limit the rule to IFS objects ***NONE** - include both QSYS and IFS objects

4) Press **Enter**.

5) Complete the following additional fields based on your object type selection:

If	Then
you selected ***QSYS** as the object type	Complete the following additional fields: **Object Name** - Name of QSYS object to which the rule applies **Object Library** - Name of the QSYS library to which the rule applies **Object Type** - Type of QSYS object to which the rule applies **Tip**: You will receive a warning message if you enter a name/library/type combination that does not currently exist on the server. If this is your intention (e.g., you are creating a rule for future use or you are creating a generic rule that you plan to implement across multiple servers), then ignore the warning by clicking Enter. If it was not your intention to create a rule that cannot be applied on the current server, then make any necessary corrections at this time.
you selected ***IFS** as the object type	If you select ***IFS** as your object type, complete the following additional field: **IFS Object** - Enter the file path to the IFS object
you selected ***NONE**	No addition fields are required

6) Press **Enter**:

Note: At this point, you might receive suggestions from the system. For example, instead of creating a new rule for a specific user, it might be more efficient to add the user to an existing user group thereby reducing the total number of rules that must be managed. This same concept applies to network groups (client or server), object groups, and operations groups as well.

See also

Rules Suggestion Engine
Rules Decision Engine
Manage User Groups
Manage Socket Rules
Manage Exit Rules

3.5.3.2. Edit Exit Rule

Use this task to edit an existing exit rule.

To edit an exit rule

1) Access the **Work with Exit Rules** interface.
2) In the **OPT** column for the desired exit rule, enter **2** (Edit).
3) Press **Enter**.
4) Modify the parameters as necessary:
5) Press **Enter**.

3.5.3.3. Copy Exit Rule

Use this task to create a new rule by copying an existing rule.

To copy an exit rule

1) Access the **Work with Exit Rules** interface.
2) In the **OPT** column for the desired exit rule, enter **3** (Copy).
3) Press **Enter**.
4) Modify the parameters as necessary.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

5) Press **Enter**.

3.5.3.4. Delete Exit Rule

Use this task to delete an exit rule.

To delete an exit rule

1) Access the **Work with Exit Rules** interface.
2) In the **OPT** column for the desired exit rule, enter **4** (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the correct rule.
5) Press **Enter**.

3.5.3.5. Display List of Users

Use this task when the exit rule definition includes a user group in the **User Name** field. You can access the user group at this point to display its details or modify the group.

Tip: Group names always begin with a colon.

To display the list of users

1) Access the **Work with Exit Rules** interface.
2) In the **OPT** column for the desired exit rule, enter **6** (User Grp).
3) Press **Enter**.
4) Review the list of users.

See also

Manage Users

Manage User Groups

Working with Exit Rules

3.5.3.6. Display List of Clients

Use this task when the exit rule definition includes a network group in the **Client IP** field. You can access the network group at this point to display its details or modify the group.

Tip: Group names always begin with a colon.

To display the list of clients

1) Access the **Work with Exit Rules** interface.
2) In the **OPT** column for the desired exit rule, enter **7** (Client Grp).
3) Press **Enter**.
4) Review the list of clients.

See also

Manage Networks

Manage Network Groups

Working with Exit Rules

3.5.3.7. Display List of Servers

Use this task when the exit rule definition includes a network group in the **Server Name** field. You can access the network group at this point to display its details or modify the group.

Tip: Group names always begin with a colon.

To display the list of servers

1) Access the **Work with Exit Rules** interface.
2) In the **OPT** column for the desired exit rule, enter **8** (Server Grp).
3) Press **Enter**.
4) Review the list of servers.

See also

Manage Networks

Manage Network Groups

Working with Exit Rules

3.5.3.8. Display List of Operations

Use this task when the exit rule definition includes an operation group in the **Operation/Port** field. You can access the operation group at this point to display its details or modify the group.

Tip: Group names always begin with a colon.

To display the list of operations

1) Access the **Work with Exit Rules** interface.
2) In the **OPT** column for the desired exit rule, enter **9** (Opr. Grp).
3) Press **Enter**.
4) Review the list of operations.

See also

Manage Operations

Manage Operation Groups

Working with Exit Rules

3.5.3.9. Display List of Objects

Use this task when the exit rule definition includes an object group in the **Object Details** field. You can access the object group at this point to display its details or modify the group.

Tip: Group names always begin with a colon.

To display the list of objects

1) Access the **Work with Exit Rules** interface.
2) In the **OPT** column for the desired exit rule, enter **10** (Obj. Grp).
3) Press **Enter**.
4) Review the list of operations.

See also

Manage Objects

Manage Object Groups

Working with Exit Rules

3.5.4. Run Exit Rule Reports

Use this task to generate reports that display the following for exit rules:

- Exit rule configuration details
- Exit rule configuration changes

Note: Refer to the TGSecure Report Reference for a complete list of report definitions.

To work with socket rule reports, access from the **Network Reports** interface.

3.5.4.1. Access the Network Reports Interface

To access the Access Escalation Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.

Note: The **Network Security** interface is displayed.

4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.

Note: The **Network Reports** interface is displayed.

3.5.4.2. Run Exit Rule Configuration Report

Use this report to display exit rule configuration details.

To run the Exit Rule Configuration Report

1) Access the **Network Reports** interface.
2) At the **Selection or command** prompt, enter **3** (Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **1** (Remote Exit Rules Report).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

3.5.4.3. Run Exit Rule Configuration Changes Report

Use this report to display the list of configuration changes made to exit rules.

Tip: You must enable auditing to produce change reports. See Manage Network Security Defaults for additional information.

To run the Exit Point Configuration Changes Report

1) Access the **Network Reports** interface.
2) At the **Selection or command** prompt, enter **4** (Configuration Changes).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **1** (Remote Exit Rules Changes).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

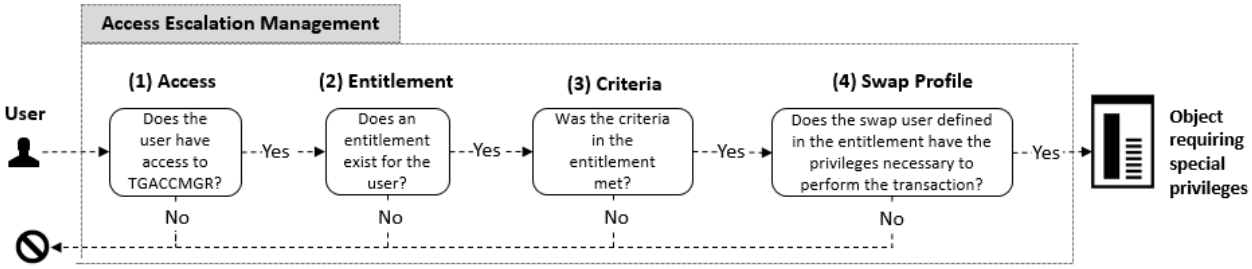
See also

Working with Exit Rules

Working with Reports

4. Access Escalation Management

Security threats are not exclusive to rogue users attempting to access your network from outside sources. Threats can also arise from within (unintentional or intentional). For example, you might have a user who is granted more access than necessary and that user might unintentionally perform a transaction that has negative system-wide implications. One way to reduce internal threats is to ensure that your users have appropriate, role-based access, but situations might arise that require a user to perform a task that is outside of his/her access authority. To address such cases, you can create an entitlement, which the user can execute within the Access Escalation Management (AEM) interface. An entitlement allows a user to perform a specific task (as defined by the entitlement) using the privileges of a swap user (as defined by the entitlement).



To access the Access Escalation Management interface

1) Log into to TGSecure.

Note: The **Main** menu appears.

2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
3) Press **Enter**.

Note: The **Access Escalation Management** interface is displayed.

See also

Log into TGSecure

Use TGSecure

Working with Access Escalation Management

Manage Access Escalation

Run Access Escalation Reports

4.1. Access Escalation Defaults

4.1.1. Working with Access Escalation Management Defaults

This section describes working with Access Escalation Management (AEM) defaults. These defaults apply to all entitlements unless otherwise defined.

Access escalation defaults allow you to define the following:

- Default swap user
- How long an AEM session will last before requiring the user to reenter a password
- Journal in which to store AEM changes
- Library in which to store AEM changes
- Whether to enable auditing of AEM changes
- Queue in which to store AEM user alerts
- Queue library in which to store AEM user alerts

In order to use the access escalation manager, you must access the **Work with Access Escalation** interface.

To access the Work with Access Escalation interface

1) Log into to TGSecure.

Note: The **Main** menu appears.

2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
3) Press **Enter**.

Note: The **Access Escalation Management** interface is displayed.

4) At the **Selection or command** prompt, enter **10** (Access Escalation Defaults).
5) Press **Enter**.

Note: The **Work with Access Escalation** interface is displayed.

See also

Log into TGSecure

Display Access Escalation Defaults

Manage Access Escalation

Run Access Escalation Reports

4.1.2. Display Access Escalation Defaults

Use this task to see the default parameters set for access escalation. These defaults apply to all entitlements unless otherwise define.

To display access escalation defaults

1) Access the TGSecure **Main** menu.

2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
3) Press **Enter**.

Note: The **Access Escalation Management** interface is displayed.

4) At the **Selection or command** prompt, enter **10** (Access Escalation Defaults).
5) Press **Enter**.

Note: The **Work with Access Escalation** interface is displayed.

Field	Description
Default Swap User	The default swap user (if one is not identified)
Authentication Timeout	Number of minutes the AEM session will remain enabled before requiring the user to reenter a password
Transaction Journal	Journal in which to store journal data
Transaction Journal Library	Library in which the journal resides
Audit Configuration Changes	Whether to collect data about AEM changes **Y** - Enable tracking of changes **N** - Disable tracking of changes **Tip**: This flag must be set to **Y** to if you plan to run access escalation change reports. **Note**: There are multiple product modules (e.g., network security, access escalation, etc.) in which you can track configuration changes. Therefore, if you see ***NONE** in the comment field, this indicates that configuration changes are not being tracked in any module. This is common at the time the product is initially installed. If you see ***PARTIAL**, this indicates that configuration changes are being track in at least one module, but not all modules. If you see ***ALL**, this indicates that configuration changes are being tracked in all modules.
Alert Message Queue	Queue in which to store alerts
Alert Message Queue Library	Library in which to store the queue

See also

Working with Access Escalation

4.1.3. Manage Access Escalation

Use this task to do the following:

- Modify access escalation defaults
- Enable access escalation change auditing

To manage access escalation, access the **Work with Access Escalation** interface.

To access the Work with Access Escalation interface

1) Access the TGSecure **Main** menu.

2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
3) Press **Enter**.

Note: The **Access Escalation Management** interface is displayed.

4) At the **Selection or command** prompt, enter **10** (Access Escalation Defaults).
5) Press **Enter**.

Note: The **Work with Access Escalation** interface is displayed.

4.1.3.1. Modify Access Escalation Defaults

Use this task to modify the exiting access escalation defaults. These defaults determine the following:

- Which journal to monitor
- Where to store the alerts
- Whether to collect data about access escalation changes (This flag must be set to **Y** to if you plan to run change reports.)

To modify access escalation defaults

1) Access the **Work with Access Escalation** interface.
2) Modify the parameters as necessary.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description or press **F4** (Prompt) for a list of valid options.

3) Press **Enter** twice.

4.1.3.2. Enable Access Escalation Change Auditing

Use this task to enable tracking of access escalation configuration changes.

Tip: Tracking is required if you plan to run access escalation change reports.

To enable access escalation configuration change tracking

1) Access the **Work with Access Escalation** interface.
2) In the **Audit Configuration Changes** field, ensure the flag is set to **Y** (Yes).
3) Press **Enter** twice.

Note: There are multiple product modules (e.g., network security, access escalation, inactive session lockdown, etc.) in which you can track configuration changes. Therefore, if you see ***NONE** in the comment field, this indicates that configuration changes are not being tracked in any module. This is common at the time the product is initially installed. If you see ***PARTIAL**, this indicates that configuration changes are being track in at least one module, but not all modules. If you see ***ALL**, this indicates that configuration changes are being tracked in all modules.

See also

Run Access Escalation Reports

Working with Access Escalation

4.1.4. Run Access Escalation Reports

Use this task to generate access escalation reports.

Note: Refer to the TGSecure Report Reference for a complete list of report definitions.

To run the Access Escalation Reports

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Access Escalation Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter the category (e.g., **1**, **2**, **3**) of report type you want to run.
7) Press **Enter**.
8) Choose the desired report from the list.
9) Press **Enter**.

See also:

Working with Access Escalation

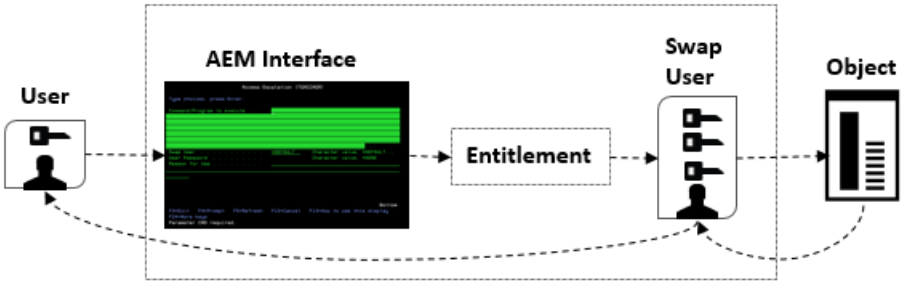
Working with Reports

4.2. Entitlements

4.2.1. Working with Entitlements

This section describes working with entitlements. Entitlements allow a user to borrow the access rights of a higher-privileged user (swap user) temporarily to execute an activity on an object.

Tip: A user can execute entitlements only from within the Access Escalation Management (AEM) interface. The system administrator can limit who has access to the AEM interface, which provides an additional layer of security.



Usage Example: Say your company has a day-shift and a night-shift administrator. In this scenario, the night administrator's only high-level task is creating a daily system backup. Instead of granting the night-shift administrator the same privileges as the day-shift administrator, you could create an entitlement that allows the night-shift administrator to perform the evening backup. In other words, this entitlement allows you to implement a privilege model that reduces your security exposure.

In order to work with entitlements, you must access the **Work with Entitlements** interface.

To access the Work with Entitlements interface

1) Log into to TGSecure.

Note: The **Main** menu appears.

2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).

3) Press **Enter**.

Note: The **Access Escalation Management** interface is displayed.

4) At the **Selection or command** prompt, enter **1** (Work with Entitlements).
5) Press **Enter**.

Note: The **Work with Entitlements** interface is displayed.

To access the AEM interface

1) At the **Selection or command** prompt, enter **TGACCMGR**.
2) Press **Enter**.

Note: The **AEM** interface is displayed.

See also

Log into TGSecure

Display List of Entitlements

Manage Entitlements

Run Entitlement Reports

Executing a Task using an Entitlements

4.2.2. Display List of Entitlements

Use this task to do the following with entitlements:

- Display list of entitlements
- Sort entitlements
- Move to a specific location within list of entitlements
- Filter entitlements

4.2.2.1. Display List

Use this task to display the list of incoming transactions.

To display the list of incoming transactions

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
3) Press **Enter**.

Note: The **Access Escalation Management** interface is displayed.

4) At the **Selection or command** prompt, enter **1** (Work with Entitlements).
5) Press **Enter**.

Note: The **Work with Entitlements** interface is displayed.

Field	Description
Enable Status	Whether the entitlement is enabled: **Y** - Enabled

	N - Disabled
User	User or user group to which the entitlement applies
Object	Object or object group to which the entitlement applies
Library	Library in which the object resides
Type	Type of object ***PMG** - Program ***CMD** - Command ***File** - Database file
Swap User	Swap profile whose privileges will be used to execute the entitlement
Aut Req?	Whether user must enter a password (authenticate) in order to use the entitlement **Y** - Password required **N** - No password required
Alr Req?	Whether an alert is sent to the alert queue when an attempt is made to use the entitlement **Y** - Alert enabled **N** - Alert Disabled
Entitlement Description	Short description identifying the purpose of the entitlement

4.2.2.2. Sort List

Use this task to sort the list. The column on which the list is currently sorted appears in white text. For example, by default, the list is originally sorted by the **User** column so that column heading initially appears in white text.

To sort the list

1) Access the **Work with Entitlements** interface.
2) Place your cursor on the desired column heading.
3) Press the **F10** (Sort) function key.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

4.2.2.3. Move to Position in List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

To move to a specific position within the list

1) Access the **Work with Entitlements** interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.
4) Press **Enter**.

Note: The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

4.2.2.4. Filter List

Use this task to limit the entitlement displayed in the list by defining a subset for filtering purposes.

Tip: Use wildcard asterisk (*) to help define your subset.

-- Add an asterisk before text (e.g., *report) to find list items that end with specific text.

-- Add an asterisk after text (e.g., report*) to find list items that start with specific text.

-- Add asterisks around text (e.g., *report*) to find list items that contain specific text anywhere in the name.

To filter the list using a subset

1) Access the **Work with Entitlements** interface.
2) Press the **F8** (Subset) function key.
3) Enter the criteria you want to use to define the subset.
4) Press **Enter**.

Note: The system filters the results based on the criteria you defined for the subset.

See also

Working with Entitlements

Manage Entitlements

4.2.3. Manage Entitlements

Use this task to do the following with entitlements:

- Add entitlements
- Edit entitlements
- Copy entitlements
- Delete entitlements

To manage entitlements, access the **Work with Entitlements** interface.

To access the Work with Entitlements interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.

Note: The **Access Escalation Management** interface is displayed.

4) At the **Selection or command** prompt, enter **1** (Work with Entitlements).
5) Press **Enter**.

Note: The **Work with Entitlements** interface is displayed.

4.2.3.1. Add Entitlement

Use this task to add an entitlement. The entitlement parameters (e.g., object, library, server, etc.) you define allow you to control the access-level for a user or a use group at a granular level.

To add entitlement

1) Access the **Work with Entitlement** interface.
2) Press the **F6** (Add) function key.
3) Enter the parameters necessary to define the entitlement.

Note: Most parameters require a name. If you see a + sign next to the field, you may enter a group. Press **F4** (Prompt) for a list available groups.

Tip: Press **F1** (Help) to access field descriptions.

Field	Description
User Name	User or user group to which the entitlement applies
Object Name	Object or object group to which the entitlement applies
Object Library	Library in which the object resides
Object Type	Type of object ***PMG** - Program ***CMD** - Command ***File** - Database file
Swap User	Swap profile whose privileges will be used to execute the entitlement
Server Name	Server or server group from which the user must be accessing the system
Calendar	Calendar to be applied
Enable Status	Whether the entitlement is enabled: **Y** - Enabled **N** - Disabled
Authentication?	Whether user must enter a password (authenticate) in order to use the entitlement **Y** - Password required **N** - No password required
Alerting?	Whether an alert is sent to the alert queue when an attempt is made to use the entitlement **Y** - Alert enabled **N** - Alert Disabled
Entitlement Description	Short description identifying the purpose of the entitlement

4) Press **Enter** twice.

4.2.3.2. Edit Entitlement

Use this task to edit an entitlement.

To edit entitlement

1) Access the **Work with Entitlement** interface.
2) In the **OPT** column for the desired entitlement, enter **2** (Edit).
3) Press **Enter**.

4) Modify the parameters as necessary.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description or press **F4** (Prompt) for a list of available groups.

5) Press **Enter** twice.

4.2.3.3. Copy Entitlement

Use this task to copy an entitlement. This is a fast way to create a new entitlement based on an existing entitlement.

To copy entitlement

1) Access the **Work with Entitlement** interface.
2) In the **OPT** column for the desired entitlement, enter **3** (Copy).
3) Press **Enter**.
4) Modify the parameters as necessary.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description or press **F4** (Prompt) for a list of available groups.

5) Press **Enter**.

4.2.3.4. Delete Entitlement

Use this task to delete an entitlement.

To delete entitlement

1) Access the **Work with Entitlement** interface.
2) In the **OPT** column for the desired group, enter **4** (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the correct entitlement.
5) Press **Enter**.

See also

Working with Entitlements

4.2.4. Run Entitlement Reports

Use this task to generate reports that display the following for entitlements:

- Entitlement usage details
- Entitlement configuration details
- Entitlement configuration changes

Note: Refer to the TGSecure Report Reference for a complete list of report definitions.

To work with entitlement reports, access from the **Access Escalation Reports** interface.

4.2.4.1. Access the Access Escalation Reports Interface

To access the Access Escalation Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
3) Press **Enter**.

Note: The **Access Escalation Management** interface is displayed.

4) At the **Selection or command** prompt, enter **20** (Access Escalation Reports).
5) Press **Enter**.

Note: The **Access Escalation Reports** interface is displayed.

4.2.4.2. Run Entitlement Usage Report

Use this report to display entitlement usages details.

To run the Entitlement Usage Report

1) Access the **Access Escalation Report** interface.
2) At the **Selection or command** prompt, enter **1** (Access Escalation Usage Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **5** (Entitlement Usage).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

4.2.4.3. Run Entitlement Configuration Report

Use this report to display entitlement configuration details.

To run the Entitlement Configuration Report

1) Access the **Access Escalation Report** interface.
2) At the **Selection or command** prompt, enter **2** (Access Escalation Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **3** (Entitlements).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

4.2.4.4. Run Entitlement Configuration Changes Report

Use this report to display the list of configuration changes made to entitlements.

Tip: You must enable auditing to produce change reports. See Enable AEM Change Auditing for additional information.

To run the Entitlement Configuration Changes Report

1) Access the **Access Escalation Report** interface.
2) At the **Selection or command** prompt, enter **3** (Access Escalation Change Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **3** (Entitlements Changes).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

See also

Working with Entitlements

Working with Reports

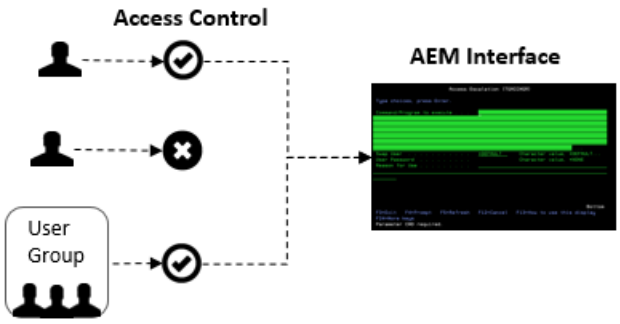
4.3. Access Control

4.3.1. Working with Access Control

This section describes how to grant or revoke access to the Access Escalation Management (AEM) interface. The AEM interface is the tool from which a user can execute an entitlement.

The tasks described in this section apply to both users and user groups.

Tip: Until the administrator adds the first user (or user group), all users have access to the AEM interface. Once the first user is explicitly granted access, then only the administrator and the user(s) who have been granted access control can access the AEM interface.



In order to work with access controls, you must access the **Work with Access Control** interface.

To access the Work with Access Control interface

1) Log into to TGSecure.

Note: The **Main** menu appears.

2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
3) Press **Enter**.

Note: The **Access Escalation Management** interface is displayed.

4) At the **Selection or command** prompt, enter **3** (Work with Access Control).
5) Press **Enter**.

Note: The **Work with Access Control** interface is displayed.

See also

Log into TGSecure

Display Who Has Access Control

Manage Access Control

Run Access Control Reports

Execute and Entitlement Using the AEM Interface

4.3.2. Display Who Has Access to the AEM Interface

Use this task to do the following with the Access Escalation Management (AEM) interface:

- Display list of users who have authority to use the AEM interface
- Sort users
- Move to a specific position within list of users
- Filter users

4.3.2.1. Display List

Use this task to display the list of users (including user groups).

To display the list of users who have access control

1) Access the TGSecure **Main** menu.

2) At the **Selection or command** prompt, enter **4** (Access Escalation Management).
3) Press **Enter**.

Note: The **Access Escalation Management** interface is displayed.

4) At the **Selection or command** prompt, enter **3** (Work with Access Control).
5) Press **Enter**.

Note: The **Work with Access Control** interface is displayed.

Field	Description
User	User or user group to which the entitlement applies
Client IP	IP address from which the transaction was initiated

4.3.2.2. Sort List

Use this task to sort the list. The column on which the list is currently sorted appears in white text. For example, by default, the list is originally sorted by the **User** column so that column heading initially appears in white text.

To sort the list

1) Access the **Work with Access Control** interface.
2) Place your cursor on the desired column heading.
3) Press the **F10** (Sort) function key.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

4.3.2.3. Move to Position in List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

To move to a specific position within the list

1) Access the **Work with Access Control** interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.
4) Press **Enter**.

Note: The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

4.3.2.4. Filter List

Use this task to limit the entitlement displayed in the list by defining a subset for filtering purposes.

Tip: Use wildcard asterisk (*) to help define your subset.

-- Add an asterisk before text (e.g., *report) to find list items that end with specific text.

-- Add an asterisk after text (e.g., report*) to find list items that start with specific text.

-- Add asterisks around text (e.g., *report*) to find list items that contain specific text anywhere in the name.

To filter the list using a subset

1) Access the **Work with Access Control** interface.
2) Press the **F8** (Subset) function key.
3) Enter the criteria you want to use to define the subset.
4) Press **Enter**.

Note: The system filters the results based on the criteria you defined for the subset. Type topic text here.

See also

Working with Access Control

4.3.3. Manage Access Control

Use this task to do the following:

- Add access control
- Edit access control
- Copy access control
- Delete access control

To manage access control, access the **Work with Access Control** interface.

To access the Work with Access Control interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **4** (Access Escalation Management).
3) Press **Enter**.

Note: The **Access Escalation Management** interface is displayed.

4) At the **Selection or command** prompt, enter **3** (Work with Access Control).
5) Press **Enter**.

Note: The **Work with Access Control** interface is displayed.

4.3.3.1. Add Access Control

Use this task to add access control for a user/user group. Once added, they are granted access to the AEM interface.

Tip: Until the first user is added, all users can access the AEM interface. Once the first user is added, only an administrator and the user(s) who have been granted access control (added) can access the AEM interface.

1) Access the **Work with Access Control** interface.
2) Press the **F6** (Add) function key on your keyboard.
3) Enter the parameters necessary to define the control.

Field	Description
User Name	User or user group to which the entitlement applies
Client IP	IP address from which the transaction was initiated

Note: Most parameters require a name. If you see a + sign next to the field, you may enter a group. Press **F4** (Prompt) for a list available groups.

Tip: Press **F1** (Help) to access field descriptions.

4) Press **Enter** twice.

4.3.3.2. Edit Access Control

Use this task to modify an exiting access control record.

To edit entitlement

1) Access the **Work with Access Control** interface.
2) In the **OPT** column for the desired access control record, enter **2** (Edit).
3) Press **Enter**.
4) Modify the parameters as necessary.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description or press **F4** (Prompt) for a list of valid entries.

5) Press **Enter** twice.

4.3.3.3. Copy Access Control

Use this task to create a new access control record based on an existing access control record.

To copy access control

1) Access the **Work with Access Control** interface.
2) In the **OPT** column for the user control record you want to copy, enter **3** (Copy).
3) Press **Enter**.
4) Modify the parameters as necessary.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description or press **F4** (Prompt) for a list of valid entries.

5) Press **Enter**.

4.3.3.4. Delete Access Control

Use this task to delete an access control record.

To delete entitlement

1) Access the **Work with Entitlement** interface.
2) In the **OPT** column for the desired group, enter **4** (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the right user.
5) Press **Enter**.

See also

Working with Access Control

4.3.4. Run Access Control Reports

Use this task to generate the following reports:

- Access control configuration details

- Access control configuration changes

Note: Refer to the TGSecure Report Reference for a complete list of report definitions.

To work with access control reports, access from the **Access Escalation Reports** interface.

4.3.4.1. Access the Escalation Reports interface

To access the Access Escalation Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
3) Press **Enter**.

Note: The **Access Escalation Management** interface is displayed.

4) At the **Selection or command** prompt, enter **20** (Access Escalation Reports).
5) Press **Enter**.

Note: The **Access Escalation Reports** interface is displayed.

4.3.4.2. Run Access Control Configuration Report

Use this report to display the users who have access to the AEM interface.

To run the Access Control Configuration Report

1) Access the **Access Escalation Report** interface.
2) At the **Selection or command** prompt, enter **2** (Access Escalation Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **4** (Access Controls).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.

8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

4.3.4.3. Run Access Control Change Report

Use this report to display the list of configuration changes made to access control. In other words, which users have been added or delete.

Tip: You must enable auditing to produce change reports. See Enable AEM Change Auditing for additional information.

To run the Access Control Change Report

1) Access the **Access Escalation Report** interface.

2) At the **Selection or command** prompt, enter **3** (Access Escalation Change Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **4** (Access Control Changes).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

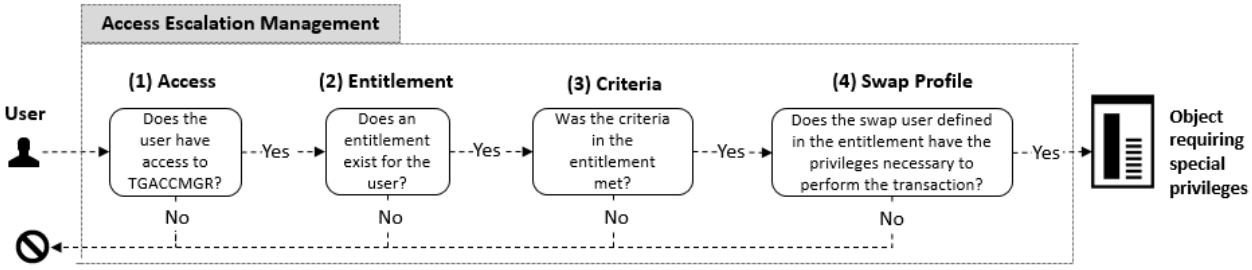
See also

Working with Access Control

Working with Reports

4.3.5. Execute an Entitlement Using the AEM Interface

Use this task to access the Access Escalation Management (AEM) interface and execute an entitlement (which allows the users to borrow the privileges of a swap profile).
The following requirements must be met for a user to access the AEM interface and execute a task (e.g., download a highly sensitive HR document) using a swap profile:
Requirement 1: The user must have access to the AEM interface.
Requirement 2: An entitlement must be defined for the user.
Requirement 3: The criteria in the entitlement must be met.
Requirement 4: A user with appropriate privileges to perform the task must be identified as the swap user within the entitlement.



Tip: If you are unable to access the AEM interface, contact your system administrator and request that an access control record be added for your user profile.

To access the AEM interface

1) At the **Selection or command** prompt, enter **TGACCMGR**.
2) Press **Enter**.
3) Enter the program/command you want to execute.
4) Enter the appropriate swap profile.

Note: This is the user who has the privilege to perform the command/program you are attempting to execute.

5) Enter your user password (for some entitlements this is optional).
6) Enter a description for why you are performing this task.
7) Press **Enter**.

See also

Working with Access Control

4.4. File Editor

4.4.1. Working with File Editor

This section describes working with the File Editor tool. The file editors are third-party commands used to modify files (objects). These commands might be used in conjunction with the standard IBM iSeries commands or they might be used as replacement commands. In any case, the third-party commands you plan to use must be registered using the File Editor tool in order for TG products to recognize those commands.

Usage Example: Your company might have purchased a third-party DFU (data file utility). Most, but not all, IBM clients use the standard IBM DFU. TG products recognize all standards IBM i Series commands. If your company plans to use third-party commands, you must use the File Editor tool to register those third-party commands so that they are recognized and executed properly by TG products.

In order to work with the file editor, you must access the **Work with File Editor** interface.

To access the Work with File Editors interface

1) Log into to TGSecure.
Note: The **Main** menu appears.
2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **11** (Work with File Editors).
5) Press **Enter**.

Note: The **Work with File Editors** interface is displayed.

See also

Log into TGSecure

Display List of File Editors

Manage File Editors

Run File Editor Reports

4.4.2. Display List of File Editors

Use this task to display a list of third-party file editors.

To display the list of File Editors

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).

3) Press **Enter**.
4) At the **Selection or command** prompt, enter **11** (Work with File Editors).
5) Press **Enter**.

Note: The **Work with File Editors** interface is displayed.

Field	Description
Editor Command	Command to be executed
Editor Library	Library in which to execute the command
Editor Parameter	Parameter to be executed

See also

Working with File Editor

Manage File Editors

4.4.3. Manage File Editors

Use these tasks to do the following with file editors:

- Add file editor
- Edit file editor
- Copy file editor
- Delete file editor

To access the Work with File Editors interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **11** (Work with File Editors).
5) Press **Enter**.

Note: The **Work with File Editors** interface is displayed.

4.4.3.1. Add File Editor

Use this task to add a file editor.

To add file editor

1) Access the **Work with File Editors** interface.
2) Press the **F6** (Add) function key on your keyboard.
3) Enter the parameters necessary to define the file editor.

Tip: Press **F1** (Help) to access field descriptions.

4) Enter a description for the file editor.
5) Press **Enter** twice.

4.4.3.2. Edit File Editor

Use this task to edit a file editor.

To edit file editor

1) Access the **Work with File Editor** interface.
2) In the **OPT** column for the desired file editor, enter **2** (Edit).
3) Press **Enter**.
4) Modify the parameters as necessary.
5) Press **Enter** twice.

4.4.3.3. Copy File Editor

Use this task to copy a file editor. This is a fast way to reference a new file editor based on an existing file editor record.

To copy file editor

1) Access the **Work with File Editor** interface.
2) In the **OPT** column for the desired file editor, enter **3** (Copy).
3) Press **Enter**.
4) Modify the parameters as necessary.
5) Press **Enter**.

4.4.3.4. Delete File Editor

Use this task to delete a file editor.

To delete file editor

1) Access the **Work with File Editor** interface.
2) In the **OPT** column for the desired file editor, enter **4** (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the correct file editor.
5) Press **Enter**.

See also

Working with File Editor

4.4.4. Run File Editor Reports

Use these tasks to generate reports that display the following for file editors.

- File editor configuration details
- File editor configuration changes

Note: Refer to the TGSecure Report Reference for a complete list of report definitions.

To work with file editor reports, access from the **Access Escalation Reports** interface.

4.4.4.1. Access the Access Escalation Reports Interface

To access the Access Escalation Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **2** (Access Escalation Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Access Escalation Reports).
5) Press **Enter**.

Note: The **Access Escalation Reports** interface is displayed.

4.4.4.2. Run File Editors Configuration Report

Use this task to display file editor configuration details.

To run File Editor Report

1) Access the **Access Escalation Reports** interface
2) At the **Selection or command** prompt, enter **2** (Access Escalation Configuration Reports).
3) Press **Enter**.

Note: The **Access Escalation Configuration Reports** interface is displayed

4) At the **Selection or command** prompt, enter **2** (File Editors).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

4.4.4.3. Run File Editor Change Report

Use this task to display the list of configuration changes made to file editors.

Tip: You must enable auditing to produce change reports. See Enable AEM Change Auditing for additional information.

To run File Editor Change Report

1) Access the **Access Escalation Reports** interface.
2) At the **Selection or command** prompt, enter **3** (Access Escalation Change Reports).
3) Press **Enter**.

Note: The **Access Escalation Change Reports** interface is displayed

4) At the **Selection or command** prompt, enter **2** (File Editors Changes).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

See also

Working with File Editor

Working with Reports

5. Inactive Session Lockdown

The Inactive Session Lockdown (ISL) feature allows you to customize how and when to end a user's session or lock a user's session when the system detects user inactivity for a specified duration (which is defined by an ISL rule). For security purposes, an inactive session has the potential to expose the system to unauthorized access and abuse.

Note: An inactive session is a session in which the user has not interacted with their keyboard or mouse and/or when the system is not pulling resources. For example, if a job or report is running in the background, the system is consuming resource, so even though the user might not interact with their keyboard or mouse (i.e., user inactivity), the session is considered active because of the consumption of resources.

In addition, the Inactive Session Lockdown feature allows you to do the following:

- Work with inactive session lockdown defaults
- Work with inactive session rules
- Work with disconnect options

To access the Inactive Session Lockdown interface

1) Log into to TGSecure.

Note: The **Main** menu appears.

2) At the **Selection or command** prompt, enter **3** (Inactive Session Lockdown).
3) Press **Enter**.

Note: The **Inactive Session Lockdown** interface is displayed.

See also

Log into TGSecure

Use TGSecure

Working with Inactive Session Lockdown

Manage Inactive Session Lockdown

Run Inactive Session Lockdown Reports

5.1. Inactive Session Lockdown Defaults

5.1.1. Working with Inactive Session Lockdown Defaults

This section describes working with Inactivity Session Lockdown (ISL) defaults. These defaults apply to all ISL rules unless otherwise defined.

Inactive session lockdown defaults allow you to define the following:

- How often the system checks for inactive sessions (e.g., every 30 seconds)
- Whether to track data about sessions disconnected by ISL

- Journal in which to store the data about sessions disconnected by ISL
- Library in which to store the data about sessions disconnected by ISL
- Whether to store changes to ISL rules or defaults
- Queue in which to store ISL admin alerts
- Queue library in which to store ISL admin alerts
- Warning message to share with user before session disconnect
- How often to share warning messages before session disconnect
- Whether to revoke user privileges when at least one of their sessions is in lockdown

See also

Log into TGSecure

Display Inactive Session Lockdown Defaults

Manage Inactive Session Lockdown

Run Inactive Session Lockdown Reports

5.1.2. Display Inactive Session Lockdown Defaults

Use this task to display inactive session lockdown (ISL) defaults.

To display the Interactive Session Lockdown defaults

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **3** (Inactive Session Lockdown).
3) Press **Enter**.

Note: The **Inactive Session Lockdown** interface is displayed.

4) At the **Selection or command** prompt, enter **10** (ISL Defaults).
5) Press **Enter**.

Note: The **Work with Inactive Session Lockdown Settings** interface is displayed.

Field	Description
Check Interval	How often the system checks for inactive sessions
Audit Status	Whether the system should track (audit) inactive sessions data ***YES** - Enable auditing ***NO** - Disable auditing **Tip**: Set this flag to ***YES** if you plan to run ISL usage reports.
Audit Journal	Journal in which to store ISL usage data **Note**: The default audit journal for TG products is TGJRN. This journal resides in the TGDATA library.
Audit Journal Library	Library in which the journal resides
Audit Configuration Changes	Whether to collect data about ISL configuration changes **Y** - Enable tracking of changes **N** - Disable tracking of changes **Tip**: Set this flag to **Y** to if you plan to run ISL change reports.

	Note: There are multiple product modules (e.g., network security, access escalation, inactive session lockdown, etc.) in which you can track configuration changes. Therefore, if you see ***NONE** in the comment field, this indicates that configuration changes are not being tracked in any module. This is common at the time the product is initially installed. If you see ***PARTIAL**, this indicates that configuration changes are being track in at least one module, but not all modules. If you see ***ALL**, this indicates that configuration changes are being tracked in all modules.
Alert Status	Whether alerts are enabled (stored in alert queue): ***YES** - Enable alerts (create admin alert) ***NO** - Disable alerts
Alert Message Queue	Queue in which to store alerts
Alert Message Queue Library	Library in which to store the queue
Temporary Disconnect Message	Custom message defined by the administrator and used to inform the user that their session is about to be locked or ended
Temporary Sign on Screen Header	The title assigned to the message screen that notifies the user of an impending disconnect (e.g., company name)
Send Warning	Whether alerts are sent to warn the user of an impending disconnect ***YES** - Warning alert enabled ***NO** - Warning alert disabled
Warning Interval	When to send the user a warning message (seconds before disconnect)
Revoke Authority	Whether to revoke a user's authority when they are locked or their session is ended ***YES** - The user's session is locked or ended, and the user's authority is revoked ***NO** - The user's session is locked or ended, but the user's authority is maintained **Note**: When a user's authority is revoked, the user is prohibited from performing tasks in any concurrent sessions. In other words, the lockdown is not limited to one session; it impacts all sessions associated with a specific user ID. **Warning**: Consider the workflow consequences thoroughly before enabling this feature.

See also

Working with Inactive Session Lockdown

5.1.3. Manage Inactive Session Lockdown Defaults

Use this task to do the following:

- Enable ISL auditing
- Enable ISL change auditing
- Enable ISL alerts
- Set check interval
- Set warning interval

- Set disconnect message
- Set revoke authority
- Start monitor
- End monitor
- Check monitor status

To manage Interactive Session Lockdown (ISL) defaults, access from the **Work with Inactive Session Lockdown Settings** interface.

To access the Work with Interactive Session Lockdown Settings interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **3** (Inactive Session Lockdown).
3) Press **Enter**.

Note: The **Inactive Session Lockdown** interface is displayed.

4) At the **Selection or command** prompt, enter **10** (ISL Defaults).
5) Press **Enter**.

Note: The **Work with Inactive Session Lockdown Settings** interface is displayed.

5.1.3.1. Enable ISL Auditing

Use this task to enable inactive session auditing.

Tip: Auditing is required if you plan to run ISL usage reports.

To enable the ISL auditing

1) Access the **Work with Inactive Session Lockdown Settings** interface.
2) In the **Audit Status** field, enter ***YES**.
3) In the **Audit Journal** field, enter the name of the journal in which to store the auditing data.
4) In the **Audit Journal Library** field, enter the name of the library in which the journal resides.
5) Press **Enter** twice.

Note: The default audit journal for TG products is TGJRN. This journal resides in the TGDATA library.

5.1.3.2. Enable ISL Change Auditing

Use this task to enable tracking of configuration changes to inactive session defaults.

Tip: Auditing is required if you plan to run ISL change reports.

To enable tracking of configuration changes in the ISL module

1) Access the **Work with Inactive Session Lockdown Settings** interface.
2) In the **Audit Configuration Changes** field, enter **Y**.
3) Press **Enter** twice.

Note: There are multiple product modules (e.g., network security, access escalation, inactive session lockdown, etc.) in which you can track configuration changes. Therefore, if you see ***NONE** in the comment field, this indicates that configuration changes are not being tracked in any module. This is common at the time the product is initially installed. If you see ***PARTIAL**, this indicates that configuration changes are being track in at least one

module, but not all modules. If you see ***ALL**, this indicates that configuration changes are being tracked in all modules.

5.1.3.3. Enable ISL Alerts

Use this task to enable ISL alerts.

Tip: Alerting is required if you plan to send alert notifications.

To enable ISL alerts

1) Access the **Work with Inactive Session Lockdown Settings** interface.
2) In the **Alert Status** field, enter ***YES**.
3) In the **Alert Message Queue** field, enter the name of the queue in which to store the alerts.
4) In the **Alert Message Queue Library** field, enter the name of the library in which the queue resides.
5) Press **Enter** twice.

5.1.3.4. Set Check Interval

Use this task to determine how often the system checks for inactive sessions.

To set the check interval

1) Access the **Work with Inactive Session Lockdown Settings** interface.
2) In the **Check Interval** field, enter the desired time interval in seconds.

Note: This value must be less than or equal to the warning interval.

3) Press **Enter** twice.

5.1.3.5. Set Warning Interval

Use this task to enable ISL warnings and to determine when the system sends out a warning to the user that their inactive session is about to be terminated.

To set the warning interval

1) Access the **Work with Inactive Session Lockdown Settings** interface.
2) In the **Send Warning** field, enter one of the following:
– ***YES** - Enable the warning feature
– ***NO** - Disable the warning feature
3) In the **Warning Interval** field, enter the desired time interval in seconds.

Note: This indicates how much time the user has to perform an action before the inactive session is terminated. This value must be greater or equal to the check interval.

4) Press **Enter** twice.

5.1.3.6. Set Disconnect Message

Use this task to define the message you want to send to the user warning them that their inactive session is about to be terminated.

To set the disconnect message

1) Access the **Work with Inactive Session Lockdown Settings** interface.

2) In the **Temporary Disconnect Message** field, enter the desired message.
3) In the **Temporary Sign on Screen Header** field, enter the desired disconnect dialog box heading.
4) Press **Enter** twice.

5.1.3.7. Set Revoke Authority

Use this task to revoke a user's authority to perform system tasks when inactivity triggers a session lockdown.

Warning: When a user's authority is revoked, the user is prohibited from performing tasks in any concurrent sessions. In other words, the lockdown is not limited to one session; it impacts all sessions associated with a specific user ID.

Tip: Revoking a user's authority can have a serious impact on workflow, depending on the user's level of responsibility and access, so consider the downstream consequences of enabling this feature.

To set the revoke authority

1) Access the **Work with Inactive Session Lockdown Settings** interface.
2) In the **Revoke Authority** field, enter on of the following:
– ***YES** - Enable the revoke feature
– ***NO** - Disable the revoke feature
3) Press **Enter** twice.

5.1.3.8. Start Monitor

Use this task to start ISL monitoring.

Note: Once started, the monitor status (which appears in the upper right corner of the screen) should display a status of ***ACTIVE**.

To monitor status

1) Access the **Work with Inactive Session Lockdown Settings** interface.
2) Press F22 (**Start monitor**) function key on your keyboard.

Tip: For function keys higher than F12, you must use a combination of the **Shift** key and the appropriate function key. For example, to select F22, you must hold down the **Shift** key and F10.

3) Press **Enter**.

5.1.3.9. End Monitor

Use this task to end ISL monitoring.

Note: Once ended, the monitor status (which appears in the upper right corner of the screen) should show status of ***INACTIVE**.

To monitor status

1) Access the **Work with Inactive Session Lockdown Settings** interface.
2) Press F23 (**Stop monitor**) function key on your keyboard.

Tip: For function keys higher than F12, you must use a combination of the Shift key and the appropriate function key. For example, to select F23, you must hold down the Shift key and F11.

3) Press **Enter**.

5.1.3.10. Check Monitor Status

Use this task to check the status of the monitor. This might be useful during troubleshooting.

To monitor status

1) Access the **Work with Inactive Session Lockdown Settings** interface.
2) Press F21 (**Monitor status**) function key on your keyboard.

Tip: For function keys higher than F12, you must use a combination of the **Shift** key and the appropriate function key. For example, to select F21, you must hold down the **Shift** key and F9.

3) Press **Enter**.

See also

Run Inactive Session Lockkdown Reports

Working with Inactive Session Lockdown

5.1.4. Run Inactive Session Lockdown Reports

Use this task to generate the following reports:

Usage Report

- Inactivity Disconnect Report

Configuration Report

- Inactivity Session Configuration Settings Report

Change Report

- Inactivity Session Configuration Changes Report

To work with ISL reports, access from the **Inactivity Session Reports** interface.

To access the Inactivity Session Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **3** (Inactive Session Lockdown).
3) Press **Enter**.

Note: The **Inactive Session Lockdown** interface is displayed.

4) At the **Selection or command** prompt, enter **20** (Inactive Session Reports).
5) Press **Enter**.

Note: The **Inactivity Session Reports** interface is displayed.

5.1.4.1. Run Inactivity Disconnect Report

Use this report to display the list of instances that triggered a disconnection due to user inactivity.

Tip: ISL monitoring must be started for data to be present in this report. See Start Monitor for additional information.

To run the Inactivity Disconnect report

1) Access the **Inactivity Session Reports** interface.
2) At the **Selection or command** prompt, enter **1** (Inactivity Session Usage Reports).
3) Press **Enter**.

Note: The **Inactivity Session Usage Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **1** (Inactivity Disconnect Report).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

5.1.4.2. Run Inactivity Session Configuration Settings Report

Use this report to view the ISL configuration settings.

Tip: You must enable auditing to produce change reports. See Enable ISL Auditing for additional information.

To run the Inactivity Session Configuration Settings report

1) Access the **Inactivity Session Reports** interface.
2) At the **Selection or command** prompt, enter **2** (Inactivity Session Configuration Reports).
3) Press **Enter**.

Note: The **Inactivity Session Configuration Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **1** (Inactivity Session Configuration Settings).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

5.1.4.3. Run Inactivity Session Configuration Changes Report

Use this report to view the changes made to the ISL configuration settings.

Tip: ISL Change auditing must be enabled for data to be present in this report. See Enable ISL Change Auditing for additional information.

To run the Inactivity Session Configuration Changes report

1) Access the **Inactivity Session Reports** interface.
2) At the **Selection or command** prompt, enter **3** (Inactivity Session Changes Reports).
3) Press **Enter**.

Note: The **Inactivity Session Changes Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **1** (Inactivity Session Configuration Changes).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

See also

Working with Inactive Session Lockdown Defaults

Working with Reports

Run Inactive Session Rules Reports

Run Disconnect Reports

5.2. Inactive Session Rules

5.2.1. Working with Inactive Session Rules

This section describes working with inactive session rules. Inactive session rules allow you to define when a user is automatically logged out of the system after a period of inactivity. For example, if a user forgets to log out of the system before leaving for lunch, a meeting, or at the end of the day, you can establish an inactivity session rule that will log the user out.

Tip: Any unattended workstations present a security vulnerability. User should never leave active sessions unattended.

In order to work with inactive session rules, you must access the **Working with Inactive Session Rules** interface.

To access the Work with Inactive Session Rules interface

1) Log into to TGSecure.

Note: The **Main** menu appears.

2) At the **Selection or command** prompt, enter **3** (Inactive Session Lockdown).
3) Press **Enter**.

Note: The **Inactive Session Lockdown** interface is displayed.

4) At the **Selection or command** prompt, enter **1** (Work with Inactive Session Rules).
5) Press **Enter**.

Note: The **Work with Inactive Session Rules** interface is displayed.

See also

Log into TGSecure

Display Inactive Session Rules

Manage Inactive Session Rules

Run Inactive Session Rules Reports

5.2.2. Display Inactive Session Rules

Use this task to do the following with inactive session rules:

- Display list
- Sort list
- Move to position in list
- Filter list

5.2.2.1. Display List

Use this task to display the list of inactive session rules.

To display the list of inactive session rules

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **3** (Inactive Session Lockdown).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **1** (Work with Inactive Session Rules).
5) Press **Enter**.

Note: The **Work with Inactive Session Rules** interface is displayed.

Field	Description
Rule Type	The type of rule: ***PGM** - Rule that affects a program ***WRKSTN** - Rule that affects a workstation ***SBSD** - Rule that affects a subsystem (e.g., country, region, department, etc.) ***CTL** - Rule that affects a controller ***USER** - Rule that affects a user **Note**: If ***USER** is specified, then the user name or user group should appear in the **Object** field.
Object	The object name or object group to which the rule applies
Library	The name of the library in which the rule applies
Calendar	The name of the calendar that defines when the rule is enabled

Disconnect Option	The disconnect option used when the rule is applicable
Rule Action	Whether the rule should be used to include or exclude ***INCLUDE** - Who and what is affected by a rule ***EXCLUDE** - Who and what is not affected by a rule
Rule Description	A short description of the rule

5.2.2.2. Sort List

Use this task to sort the list. The column on which the list is currently sorted appears in white text.

To sort the list

1) Access the **Work with Inactive Session Rules** interface.
2) Place your cursor on the desired column heading.
3) Press the **F10** (Sort) function key.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

5.2.2.3. Move to Position in List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

To move to a specific position within the list

1) Access the **Work with Inactive Session Rules** interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.
4) Press **Enter**.

Note: The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

5.2.2.4. Filter List

Use this task to limit the objects displayed in the list by defining a subset for filtering purposes.

Tip: Use wildcard asterisk (*) to help define your subset.

-- Add an asterisk before text (e.g., *report) to find list items that end with specific text.

-- Add an asterisk after text (e.g., report*) to find list items that start with specific text.

-- Add asterisks around text (e.g., *report*) to find list items that contain specific text anywhere in the name.

To filter the list using a subset

1) Access the **Work with Inactive Session Rules** interface.
2) Press the **F8** (Subset) function key.
3) Enter the criteria you want to use to define the subset.
4) Press **Enter**.

Note: The system filters the results based on the criteria you defined for the subset.

See also

Working with Inactive Session Rules

5.2.3. Manage Inactive Session Rules

Use this task to do the following with inactive session rules:

- Add inactive session rule
- Edit inactive session rule
- Copy inactive session rule
- Delete inactive session rule

To manage ISL rules, access the **Work with Inactive Session Rules** interface.

To access the Work with Inactive Session interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **3** (Inactive Session Lockdown).
3) Press **Enter**.

Note: The **Inactive Session Lockdown** interface is displayed.

4) At the **Selection or command** prompt, enter **1** (Work with Inactive Session Rules).
5) Press **Enter**.

Note: The **Work with Inactive Session Rules** interface is displayed.

5.2.3.1. Add Inactive Session Rule

Use this task to add an inactive session rule.

To add an inactive session rule

1) Access the **Work with Inactive Session Rules** interface.
2) Press the **F6** (Add) function key.
3) Define the rule using the fields provided.

Field	Description
Rule Type	Enter the type of rule: ***PGM** - Rule that affects a program ***WRKSTN** - Rule that affects a workstation ***SBSD** - Rule that affects a subsystem (e.g., country, region, department) ***CTL** - Rule that affects a controller ***USER** - Rule that affects a user **Note**: If ***USER** is specified, then enter user name or user group the **Object** field.
Object	Enter the object name or object group to which the rule is applicable **Tip**: Enter ***ALL** to apply the rule to all objects, except when **Rule Type** is defined as ***USER**.

Library	Enter the name of the library to which the rule is applicable **Tip**: Leave the field blank to apply to all libraries.
Calendar	Enter the name of the calendar that defines when the rule is applicable **Tip**: Enter ***NONE** if no calendar is applicable.
Disconnect Option	Enter the disconnect option to use when the rule is applicable
Rule Action	Identify whether the rule includes or excludes ***INCLUDE** - Who and what is affected by a rule ***EXCLUDE** - Who and what is not affected by a rule
Rule Description	Enter a description of the rule

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

4) Press **Enter** twice.

5.2.3.2. Edit Inactive Session Rule

Use this task to edit an existing ISL rule.

To edit an inactive session rule

1) Access the **Work with Inactive Session Rules** interface.
2) In the **OPT** column for the desired rule, enter **2** (Edit).
3) Press **Enter**.
4) Modify the parameters as necessary.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

5) Press **Enter** twice.

5.2.3.3. Copy Inactive Session Rule

Use this task to create a new ISL rule by copying an existing rule.

To copy an inactive session rule

1) Access the **Work with Inactive Session Rules** interface.
2) In the **OPT** column for the desired rule, enter **3** (Copy).
3) Press **Enter**.
4) Modify the parameters as necessary.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

5) Press **Enter** twice.

5.2.3.4. Delete Inactive Session Rule

Use this task to delete an ISL k rule.

To delete an inactive session rule

1) Access the **Work with Inactive Session Rules** interface.
2) In the **OPT** column for the desired transaction, enter **4** (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the correct rule.
5) Press **Enter** twice.

See also

Working with Inactive Session Rules

5.2.4. Run Inactive Session Rules Reports

Use this task to generate the following reports:

- Run inactivity session inclusion exception rules report
- Run inactivity session rules change report

To work with ISL reports, access from the **Inactive Session Reports** interface.

To access the Inactive Sessions Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **3** (Inactive Session Lockdown).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Inactive Session Reports).
5) Press **Enter**.

Note: The **Inactivity Session Reports** interface is displayed.

5.2.4.1. Run Inactivity Session Inclusion Exception Rules Report

Use this report to view the list of inclusion exception rules.

Tip: ISL auditing must be enabled to run ISL reports. See Enable ISL Auditing for additional information.

To run the Inactivity Session Inclusion Exception Rules report

1) Access the **Inactivity Session Reports** interface.
2) At the **Selection or command** prompt, enter **2** (Inactivity Session Configuration Reports).
3) Press **Enter**.

Note: The **Inactivity Session Configuration Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **3** (Inactivity Session Inclusion Exception Rules).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.

8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

5.2.4.2. Run Inactivity Session Rules Change Report

Use this report to view the changes made to ISL rules.

Tip: You must enable auditing to produce change report. See Enable ISL Change Auditing for additional information.

To run the Inactivity Session Rules Change report

1) Access the **Inactivity Session Reports** interface.
2) At the **Selection or command** prompt, enter **3** (Inactivity Session Changes Reports).
3) Press **Enter**.

Note: The **Inactivity Session Change Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **3** (Inactivity Session Rule Changes).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

See also:

Working with Inactive Session Rules

Working with Reports

Run Inactive Session Lockdown Reports

Run Disconnect Reports

5.3. Disconnection Options

5.3.1. Working with Disconnect Options

This section describes working with the methods used to disconnect a user when the user's session is deemed inactive and therefore, vulnerable to attach.

You have choices (and therefore decisions to make) regarding how to disconnect a user when the user's session is deemed to be inactive:

- Disconnect (pause) the job
- Hold (freeze) the job (only an admin can unfreeze a job)
- End the job (user remains logged into the server, but the user must restart the job)
- End the session (user is logged off the server, and the user must restart the session and job)

In order to work with disconnect options, you must access the **Working with Disconnect Options** interface.

To access the Work with Disconnect Option interface

1) Log into to TGSecure.

Note: The **Main** menu appears.

2) At the **Selection or command** prompt, enter **3** (Interactive Session Lockdown).
3) Press **Enter**.

Note: The **Inactive Session Lockdown** interface is displayed.

4) At the **Selection or command** prompt, enter **11** (Work with Disconnect Options).
5) Press **Enter**.

Note: The **Work with Disconnect Options** interface is displayed.

See also

Log into TGSecure

Display Disconnect Options

Manage Disconnect Options

Run Disconnect Option Reports

5.3.2. Display Disconnect Options

Use this task to do the following with disconnect options:

- Display list
- Sort list
- Move to position in list
- Filter list

5.3.2.1. Display List

Use this task to display the list of disconnect options.

To display the list of disconnect options

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **3** (Inactive Session Lockdown).
3) Press **Enter**.

Note: The **Inactive Session Lockdown** interface is displayed.

4) At the **Selection or command** prompt, enter **11** (Work with Disconnect Options).
5) Press **Enter**.

Note: The **Work with Disconnect Options** interface is displayed.

Field	Description
Disconnect Option	Name assigned to the disconnect option

Time Limit	Time the system must remain inactive to trigger the disconnect
Disconnect Type	The type of disconnect: **ENDJOB** - End the job (user must restart their job) **DSCJOB** - Disconnect (pause) the job and show the IBM standard disconnect message **TGDSCJOB** - Disconnect (pause) the job and show a custom disconnect message **HLDJOB** - Hold (freeze) the job (only an admin can unfreeze a job) **SIGNOFF** - End the session (user must restart their session and job) **Tip**: If **TGDSCJOB** is defined as the disconnect type, ensure that program **ISL80001P** in library **TGPROD** is defined as the user's initial. To see which program is defined as the initial program for the user, at the **Selection or command** prompt, enter **DSPUSRPRF**. Enter the desired user in the **User Profile** field. Press **Enter**. Page down until you see **Initial Program** and **Library** entries. if ISL80001P is not defined as the initial program, you must either use a different disconnect type, or change the user's initial program.

5.3.2.2. Sort List

Use this task to sort the list. The column on which the list is currently sorted appears in white text.

To sort the list

1) Access the **Work with Disconnect Options** interface.
2) Place your cursor on the desired column heading.
3) Press the **F10** (Sort) function key.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

5.3.2.3. Move to Position in List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

To move to a specific position within the list

1) Access the **Work with Disconnect Options** interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.
4) Press **Enter**.

Note: The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

5.3.2.4. Filter List

Use this task to limit the objects displayed in the list by defining a subset for filtering purposes.

Tip: Use wildcard asterisk (*) to help define your subset.

-- Add an asterisk before text (e.g., *report) to find list items that end with specific text.

-- Add an asterisk after text (e.g., report*) to find list items that start with specific text.

-- Add asterisks around text (e.g., *report*) to find list items that contain specific text anywhere in the name.

To filter the list using a subset

1) Access the **Work with Disconnect Options** interface.
2) Press the **F8** (Subset) function key.
3) Enter the criteria you want to use to define the subset.
4) Press **Enter**.

Note: The system filters the results based on the criteria you defined for the subset.

See also

Working with Disconnect Options

5.3.3. Manage Disconnect Options

Use this task to do the following with disconnect options:

- Add disconnect option
- Edit disconnect option
- Copy disconnect option
- Delete disconnect option

To manage disconnect options, access the **Work with Disconnect Options** interface.

To access the Work with Disconnect Options interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **3** (Inactive Session Lockdown).
3) Press **Enter**.

Note: The **Inactive Session Lockdown** interface is displayed.

4) At the **Selection or command** prompt, enter **11** (Work with Disconnect Options).
5) Press **Enter**.

Note: The **Work with Disconnect Options** interface is displayed.

5.3.3.1. Add Disconnect Option

Use this task to add a disconnect option.

To add a disconnect option

1) Access the **Work with Disconnect Options** interface.
2) Press the **F6** (Add) function key on your keyboard.
3) Define the disconnect option using the fields provided.

Field	Description
Disconnect Option	Enter the name you want to assign the disconnect option

Time Limit	Enter the time the system must remain inactive to trigger the disconnect option
Disconnect Type	Enter one of the following: **ENDJOB** - End the job (user must start the job over) **DSCJOB** - Disconnect (pause) the job and show the IBM standard disconnect message **TGDSCJOB** - Disconnect (pause) the job and show a custom disconnect message **HLDJOB** - Hold (freeze) the job (only an admin can unfreeze a job) **SIGNOFF** - Signoff from the server **Warnings**: Do not select **HLDJOB** if a trained admin will not be available to unfreeze the job. **Tip**: If you select **TGDSCJOB**, ensure that program **ISL80001P** in library **TGPROD** is defined as the as the user's initial program. To see which program is defined as the initial program for the user, at the **Selection or command** prompt, enter **DSPUSRPRF**. Enter the desired user in the **User Profile** field. Press **Enter**. Page down until you see **Initial Program** and **Library** entries. if ISL80001P is not defined as the initial program, you must either use a different disconnect type, or change the user's initial program.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

4) Press **Enter** twice.

5.3.3.2. Edit Disconnect Option

Use this task to edit an existing disconnect option.

To edit a disconnect option

1) Access the **Work with Disconnect Options** interface.
2) In the **OPT** column for the desired rule, enter **2** (Edit).
3) Press **Enter**.
4) Modify the parameters as necessary.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

5) Press **Enter** twice.

5.3.3.3. Copy Disconnect Option

Use this task to create a new disconnect option by copying an existing disconnect option.

To copy a disconnect option

1) Access the **Work with Disconnect Options** interface.
2) In the **OPT** column for the desired rule, enter **3** (Copy).
3) Press **Enter**.
4) Modify the parameters as necessary.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

5) Press **Enter** twice.

5.3.3.4. Delete Disconnect Option

Use this task to delete a disconnect option.

To delete a disconnect option

1) Access the **Work with Disconnect Options** interface.
2) In the **OPT** column for the desired rule, enter **4** (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the correct rule.
5) Press **Enter** twice.

See also

Working with Disconnect Options

5.3.4. Run Disconnect Option Reports

Use this task to generate the following reports:

- Inactivity Session Disconnect Options Report
- Inactivity Session Disconnect Option Change Report

To work with ISL reports, access from the **Inactive Session Reports** interface.

To access the Inactive Sessions Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **3** (Inactive Session Lockdown).
3) Press **Enter**.

Note: The **Inactive Session Lockdown** interface is displayed.

4) At the **Selection or command** prompt, enter **20** (Inactive Session Reports).
5) Press **Enter**.

Note: The **Inactivity Session Reports** interface is displayed.

5.3.4.1. Run Inactivity Session Disconnect Option Report

Use this report to view the list of disconnect options.

Tip: ISL auditing must be enabled to run ISL reports. See Enable ISL Auditing for additional information.

To run the Inactivity Session Disconnect Option report

1) Access the **Inactivity Session Reports** interface.
2) At the **Selection or command** prompt, enter **2** (Inactivity Session Configuration Reports).
3) Press **Enter**.

Note: The **Inactivity Session Configuration Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **2** (Inactivity Session Disconnect Options).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

5.3.4.2. Run Inactivity Session Disconnect Option Change Report

Use this report to view changes made to ISL disconnection options.

Tip: You must enable auditing to produce change reports. See Enable ISL Change Auditing for additional information.

To run the Inactivity Session Disconnect Option Change report

1) Access the **Inactivity Session Reports** interface.
2) At the **Selection or command** prompt, enter **3** (Inactivity Session Changes Reports).
3) Press **Enter**.

Note: The **Inactivity Session Change Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **2** (Inactivity Session Disconnect Option Changes).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

See also

Working with Disconnect Options

Working with Reports

Run Inactive Session Rules Reports

Run Inactive Session Rules Reports

6. Resource Manager

The Resource Manager allows you to manage object-level security using authority schemas. Think of an authority schema as a template that defines authority best practices. Once you create an authority schema, you can use it to evaluate and modify the authority levels of multiple users.

In addition, the Resource Manager allows you to do the following:

- Work with Resource Manager Defaults
- Work with Authority Schemas
- Work with Authority Collections

To access the Resource Manager interface

1) Log into to TGSecure.

Note: The **Main** menu appears.

2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**.

See also

Log into TGSecure

Use TGSecure

Working with Resource Manager Defaults

Display Resource Manager Defaults

Manage Resource Manager Defaults

Run Resource Manager Reports

6.1. Resource Manager Defaults

6.1.1. Working with Resource Manager Defaults

This section describes working with Resource Manager defaults.

Resource Manager defaults allow you to define the following:

- Whether to send resource change alerts
- Whether to track resource changes (required if you plan to run reports)
- Journal in which to store resource changes
- Library in which to store resource changes
- Queue in which to store resource alerts
- Queue library in which to store resource alerts

In order to work with the resource manager, you must access the **Resource Manager Defaults** interface.

To access the Resource Manager interface

1) Log into to TGSecure.

Note: The **Main** menu appears.

2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**.

Note: The **Resource Manager** interface is displayed.

4) At the **Selection or command** prompt, enter **4** (Resource Manager Defaults).
5) Press **Enter**.

Note: The **Resource Manager Defaults** interface is displayed.

See also

Log into TGSecure

Display Resource Manager Defaults

Manage Resource Manager Defaults

Run Resource Manager Reports

6.1.2. Display Resource Manager Defaults

Use this task to display the Resource Manager defaults.

To display the Resource Manager defaults

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**.

Note: The **Resource Manager** interface is displayed.

4) At the **Selection or command** prompt, enter **4** (Resource Manager Defaults).
5) Press **Enter**.

Note: The **Resource Manager Defaults** interface is displayed.

Field	Description
Audit Journal	Journal in which to store resource manager usage data **Note**: The default audit journal for TG products is TGJRN. This journal resides in the TGDATA library. **Tip**: The Audit Journal and Library fields must be filled with a valid values if you plan to run Resource Manager usage reports.
Audit Journal Library	Library in which the audit journal resides

Audit Configuration Changes	Whether to collect data about resource changes: **Y** - Enable tracking of changes **N** - Disable tracking of changes **Tip**: Set this flag to **Y** if you plan to run the resource manager change reports. **Note**: There are multiple product modules (e.g., network security, access escalation, inactive session lockdown, etc.) in which you can track configuration changes. Therefore, if you see ***NONE** in the comment field, this indicates that configuration changes are not being tracked in any module. This is common at the time the product is initially installed. If you see ***PARTIAL**, this indicates that configuration changes are being track in at least one module, but not all modules. If you see ***ALL**, this indicates that configuration changes are being tracked in all modules
Alert Status	Whether alerts are enabled: ***YES** - Enable alerts (create admin alert) ***NO** - Disable alerts
Alert Message Queue	Queue in which to store alerts
Alert Message Queue Library	Library in which to store the queue

See also

Working with Resource Manager Defaults

6.1.3. Manage Resource Manager Defaults

Use this task to do the following:

- Enable resource change auditing
- Enable resource change alerts

To manage Resource Manager defaults, access the **Resource Manager Defaults** interface.

To access the Resource Manager Defaults interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**.

Note: The **Resource Manager** interface is displayed.

4) At the **Selection or command** prompt, enter **4** (Resource Manager Defaults).
5) Press **Enter**.

Note: The **Resource Manager Defaults** interface is displayed.

6.1.3.1. Enable Resource Change Auditing

Use this task to enable resource change auditing.

Tip: Auditing is required if you plan to run resource manager change reports.

To enable the resource auditing

1) Access the **Resource Manager Defaults** interface.
2) In the **Audit Configuration Change** field, enter **Y**.
3) In the **Audit Journal** field, enter the name of the journal in which to store changes.
4) In the **Audit Journal Library** field, enter the name of the library in which the journal resides.
5) Press **Enter**.

Note: There are multiple product modules (e.g., network security, access escalation, inactive session lockdown, etc.) in which you can track configuration changes. Therefore, if you see ***NONE** in the comment field, this indicates that configuration changes are not being tracked in any module. This is common at the time the product is initially installed. If you see ***PARTIAL**, this indicates that configuration changes are being track in at least one module, but not all modules. If you see ***ALL**, this indicates that configuration changes are being tracked in all modules

6.1.3.2. Enable Resource Change Alerts

Use this task to enable inactive session alerts.

Tip: Alerting is required if you plan to send alert notifications.

To enable resource alerts

1) Access the **Resource Manager Defaults** interface.
2) In the **Alert Status** field, enter ***YES**.
3) In the **Alert Message Queue** field, enter the name of the queue in which to store the alerts.
4) In the **Alert Message Queue Library** field, enter the name of the library in which the queue resides.
5) Press **Enter**.

See also

Working with Resource Manager Defaults

Run Resource Manager Reports

6.1.4. Run Resource Manager Reports

Use this task to generate the following reports:

Usage Report

- Resource Manager Out of Compliance Data

Configuration Report

- Resource Manager Configuration

Change Reports

- Resource Manager Configuration Change
- Resource Manager Out of Compliance Data Changes

To work with Resource Manager reports, access from the **Resource Manger Reports** interface.

To access the Resource Manager Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**.

Note: The **Resource Manager** interface is displayed.

4) At the **Selection or command** prompt, enter **20** (Resource Manager Reports).
5) Press **Enter**.

Note: The **Resource Manger Reports** interface is displayed.

6.1.4.1. Run Resource Manager Configuration Report

Use this report to view the Resource Manager configuration details.

To run the Resource Manager Configuration Report

1) Access the **Resource Manager Reports** interface.
2) At the **Selection or command** prompt, enter **2** (Resource Manager Configuration Reports).
3) Press **Enter**.

Note: The **Resource Manager Configuration Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **1** (Resource Manager Configuration).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

6.1.4.2. Run Resource Manager Configuration Change Report

Use this report to view changes made to the Resource Manager configuration details.

Tip: You must enable auditing to produce change reports. See Enable Resource Change Auditing for additional information.

To run the Resource Manager Configuration Change Report

1) Access the **Resource Manager Reports** interface.
2) At the **Selection or command** prompt, enter **3** (Resource Manager Change Reports).
3) Press **Enter**.

Note: The **Resource Manager Change Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **1** (Resource Manager Configuration Changes).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

6.1.4.3. Run Resource Manager Out of Compliance Data

Use this report to view user authorities that are deemed out of compliance based on a defined authority schema.

To run the Resource Manager Out of Compliance Report

1) Access the **Resource Manager Reports** interface.
2) At the **Selection or command** prompt, enter **2** (Resource Manager Configuration Reports).
3) Press **Enter**.

Note: The **Resource Manager Configuration Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **4** (Resource Manager Out of Compliance Data).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

6.1.4.4. Run Resource Manager Out of Compliance Data Changes Report

Use this report to view changes made to user authorities that are deemed out of compliance based on a defined authority schema.

To run the Resource Manager Out of Compliance Data Changes Report

1) Access the **Resource Manager Reports** interface.
2) At the **Selection or command** prompt, enter **3** (Resource Manager Change Reports).
3) Press **Enter**.

Note: The **Resource Manager Configuration Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **4** (Resource Manager Out of Compliance Data Changes).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

See also:

Working with Resource Manager Defaults

Working with Reports

Run Authority Schema Report

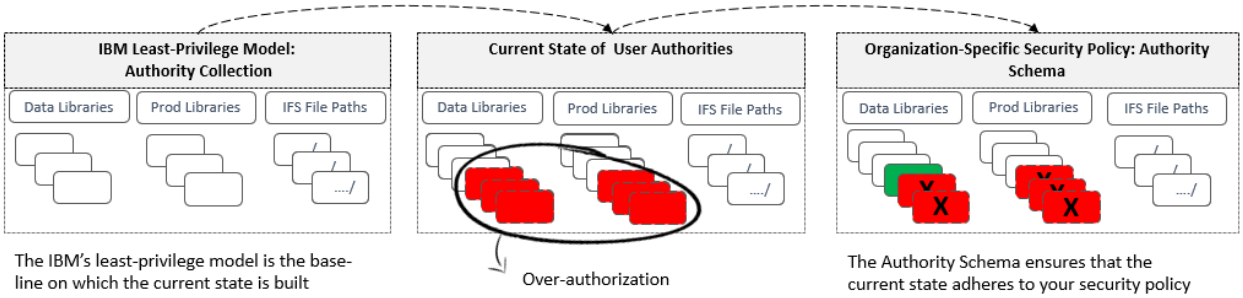
Run Authority Collection Configuration Reports

6.2. Authority Schemas

6.2.1. Working with Authority Schemas

This section describes working with authority schemas. Authority schemas allow you to define an architecture (template) for granting user authorities. Each authority scheme is the ideal model of how your organization should implemented user authorities. Therefore, each authority schema should be unique to an organization and be based on a well-defined security policy.

The following is the process used to define and implement authorities schemas:



In order to work with authority schemas, you must access the **Working with Authority Schemas** interface.

To access the authority schemas interface

1) Log into to TGSecure.

Note: The **Main** menu appears.

2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**.

Note: The **Resource Manager** interface is displayed.

4) At the **Selection or command** prompt, enter **1** (**Authority Schema Configuration**).
5) Press **Enter**.

Note: The **Work with Authority Schemas** interface is displayed.

See also

Log into TGSecure

Display Authority Schemas

Manage Authority Schemas

Run Authority Schema Reports

6.2.2. Display Authority Schemas

Use this task to do the following with inactive session rules:

Schemas

- Display list of schemas
- Sort list of schemas
- Move to position in list of schemas
- Filter list of schemas

Schema Details (exceptions)

- Display list of schemas details
- Sort list of schemas details
- Move to position in list of schemas details
- Filter list schemas details

6.2.2.1. Display List of Schemas

Use this task to display the list of available authority schemas.

To display the list of authority schemas

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**.

Note: The **Resource Manager** interface is displayed.

4) At the **Selection or command** prompt, enter **1** (Authority Schema Configuration).
5) Press **Enter**.

Note: The **Work with Authority Schemas** interface is displayed.

Field	Description
Schema ID	ID assigned to the schema
Compliances	Date and time at which the last check for authority schema compliance was performed
Enforcement	Date and time at which user authorities where compared to the authority schema and compliance with the schema was enforced
Alert Status	Whether alerts are enabled: ***YES** - Enable alerts (create admin alerts)

	***NO** - Disable alerts
Schema Description	Description of the authority schema
Compliance Status	Whether the current authority levels comply with the schema ***PASS** - User authorities comply with the current authority scheme ***FAIL** - User authorities do not comply with the current authority scheme **Note**: See Manage Authority Scheme for instruction on enforcing an authority schema.

6.2.2.2. Sort List of Schemas

Use this task to sort the list. The column on which the list is currently sorted appears in white text.

To sort the list

1) Access the **Work with Authority Schemas** interface.
2) Place your cursor on the desired column heading.
3) Press the **F10** (Sort) function key on your keyboard.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

6.2.2.3. Move to Position in List of Schemas

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

To move to a specific position within the list

1) Access the **Work with Authority Schemas** interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.
4) Press **Enter**.

Note: The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

6.2.2.4. Filter List Schemas

Use this task to limit the objects displayed in the list by defining a subset for filtering purposes.

Tip: Use wildcard asterisk (*) to help define your subset.

-- Add an asterisk before text (e.g., *report) to find list items that end with specific text.

-- Add an asterisk after text (e.g., report*) to find list items that start with specific text.

-- Add asterisks around text (e.g., *report*) to find list items that contain specific text anywhere in the name.

To filter the list using a subset

1) Access the **Work with Authority Schemas** interface.
2) Press the **F8** (Subset) function key on your keyboard.
3) Enter the criteria you want to use to define the subset.

4) Press **Enter**.

Note: The system filters the results based on the criteria you defined for the subset.

6.2.2.5. Display List of Schemas Details

Use this task to display the list of available schema details and exceptions.

To display the list of authority schema details

1) Access the **Work with Authority Schemas** interface.
2) In the **OPT** column for the desired schema, enter **10** (Work with Authority Schema Details).
3) Press **Enter**.

Note: The **Work with Authority Schema Details** interface is displayed.

Field	Description
File Sys	File system to monitor
Path or ASP	File path or ASP to monitor
Library	Library to monitor
Object Name	Object name to monitor
Object Type	Object type to monitor
Object Owner	Name of the object owner
Auth List	Name of the authority list **Note**: An authority list displays the users who have authority to specific objects.
User Object	Name of the user (or group) that has access to the object
Auth	User or group authority level: ***ALL** - All authorities (i.e., change, exclude, use, etc.) ***CHANGE** - Change authority ***EXCLUDE** - Prohibit the user from performing operations on the object ***USE** - Allow the user to use the object (but not change it) ***AUTL** - Default level of authority defined for public users (*PUBLIC)
Exception	Whether excepts are defined ***YES** - This entry is an exception to the default rules for this schema ***NO** - This entry is a default rule for this schema **Note**: Exceptions are defined as schema details.

6.2.2.6. Sort List of Schemas Details

Use this task to sort the list. The column on which the list is currently sorted appears in white text.

To sort the list

1) Access the **Work with Authority Schemas** interface.
2) Place your cursor on the desired column heading.

3) Press the **F10** (Sort) function key on your keyboard.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

6.2.2.7. Move to Position in List of Schemas Details

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

To move to a specific position within the list

1) Access the **Work with Authority Schemas** interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.
4) Press **Enter**.

Note: The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

6.2.2.8. Filter List Schemas Details

Use this task to limit the objects displayed in the list by defining a subset for filtering purposes.

To filter the list using a subset

1) Access the **Work with Authority Schemas** interface.
2) Press the **F8** (Subset) function key on your keyboard.
3) Enter the criteria you want to use to define the subset.
4) Press **Enter**.

Note: The system filters the results based on the criteria you defined for the subset.

See also

Working with Authority Schemas

6.2.3. Manage Authority Schemas

Use this task to do the following with authority schemas:

Authority Schema: (part I)

- Add authority schema
- Edit authority schema
- Copy authority schema
- Delete authority schema
- Enabling authority schema alerting
- Disable authority schema alerting
- Limit scope of authority schema to integrated file system (IFS)
- Limit scope of authority schema to system libraries (SYS)

Authority Schema Details (part II)

- Add schema details
- Edit schema details
- Copy schema detail
- Delete schema detail

Authority Schema Enforcement (part III)

- Display authority schema compliance issues
- Enforce authority schema

To manage authority schemas, access the **Work with Authority Schemas** interface.

6.2.3.1. Access the Work with Authority Schema Interface

To access the Work with Authority Schemas interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**.

Note: The **Resource Manager** interface is displayed.

4) At the **Selection or command** prompt, enter **1** (Authority Schema Configuration).
5) Press **Enter**.

Note: The **Work with Authority Schemas** interface is displayed.

Authority Schema

6.2.3.2. Add Authority Schema

Use this task to add an authority schema.

To add an authority schema

1) Access the **Work with Authority Schemas** interface.
2) Press the **F6** (Create) function key on your keyboard.
3) Complete the following fields.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

Field	Description
Schema ID	ID you want to assign to the schema
Schema Description	Text describing the purpose of the schema
Alert Status	Whether alerts are enabled: ***YES** - Enable alerts (create admin alerts) ***NO** - Disable alerts
Include IFS or Library Object	Which structures to check: ***SYS** - Enable check only in system libraries

	***IFS** - Enable check only in Integrated File System (IFS). **Note**: IFS a newer file management structure that supports stream input/output and is similar to the structure used by personal computers and UNIX operating systems. For more information about IBM file systems, refer to the IBM Knowledge Center. ***ALL** - Enable check in both SYS and IFS ***NO** - Disable check

4) Define the object scope for library (SYS) objects.

Note: The values you enter in the following fields limit the scope of the schema to a single object or an object group.

Field	Description
Object Name	Enter a specific object name or object group to which this schema applies You can also choose one of the following options: ***NONE** - No objects ***ALL** - All objects **Tip:** You can skip this field for IFS files.
Object Library	Enter the name of the library to which this authority schema applies, or enter ***ALL** to include all libraries **Tip:** You can skip this field for IFS files.
Object Type	Enter the object type to which this authority schema applies, or enter ***ALL** to include all object types **Tip:** You can skip this field for IFS files.
Path or ASP Name	Do one of the following: -- Enter the file path for the IFS or -- Enter the ASP (Auxiliary Storage Pool) for system libraries **Note**: If you enter ***SYSBAS**, the system ASP and all basic user ASPs are included.

5) Define the authorities.

Note: The values you enter in the following fields define the recommended object authority settings for the object or object group associated with the schema.

Field	Description
Object Owner	Enter the name of the object owner
Authorization List	Enter the name of the authority list to which this authority schema applies, or enter ***NONE** if not applicable **Note**: An authority list displays the users who have authority to access a specific object.
Object Primary Group	Enter the name of the primary group to which the object belongs or enter ***NONE** if not applicable
Adopt User Profile	Enter the name of the user profile to adopt when the schema is enforced
Adopt Authority	Whether to allow the ability to adopt authority: ***YES** - Enable the program to adopt the authorities from the previous program

	***NO** - Disable the program from adopting the authorities from the previous program

6) Define the user authorities.

Note: The values you enter in the following fields define the recommended user authority settings for the user or user group associated with the schema.

Field	Description
User Name	Enter the user's name
*Public Authority	Enter the authority level you want to assign to public users (*Public): **Note:** Public users do not have the following: -- They do not have specific authority to use the function -- They do not appear on the authorization list -- They are not members of a user group that has specific authority to the object Select the level of authority you want to grant public users: ***ALL** - Grant public users all authorities (i.e., change, exclude, use, etc.) ***CHANGE** - Grant public users change authority ***EXCLUDE** - Prohibit public users from performing operations on the object ***USE** - Grant access to the object attributes and allow public users to use of the object (but not change the object) ***AUTL** - Grant public users the default level of authority specified for the authority list

7) Press **Enter** twice.

6.2.3.3. Edit Authority Schema

Use this task to edit an existing authority schema.

To edit an authority schema

1) Access the **Work with Authority Schemas** interface.
2) In the **OPT** column for the desired schema, enter **2** (Edit).
3) Press **Enter**.
4) Modify the parameters as necessary.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

5) Press **Enter** twice.

6.2.3.4. Copy Authority Schema

Use this task to create a new authority schema by copying an existing authority schema.

To copy an authority schema

1) Access the **Work with Authority Schemas** interface.
2) In the **OPT** column for the desired schema, enter **3** (Copy).
3) Press **Enter**.
4) Modify the parameters as necessary.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

5) Press **Enter**.

6.2.3.5. Delete Authority Schema

Use this task to delete an authority schema.

To delete an authority schema

1) Access the **Work with Authority Schemas** interface.
2) In the **OPT** column for the desired schema, enter **4** (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the correct schema.
5) Press **Enter** twice.

6.2.3.6. Enabling Authority Schema Alerting

Use this task to enable alerting.

To enable/disable authority schema alerting

1) Access the **Work with Authority Schemas** interface.
2) In the **OPT** column for the desired schema, enter **2** (Edit).
3) Press **Enter**.
4) In the **Alert Status** field, enter ***YES** to enable alerting.

6.2.3.7. Disable Authority Schema Alerting

Use this task to disable alerting.

To enable/disable authority schema alerting

1) Access the **Work with Authority Schemas** interface.
2) In the **OPT** column for the desired schema, enter **2** (Edit).
3) Press **Enter**.
4) In the **Alert Status** field, enter ***NO** to disable alerting.

6.2.3.8. Limit Scope of Authority Schema to System Libraries (SYS)

Use this task to limit the scope of an authority schema to only address system libraries (SYS).

To limit the scope of the schema

1) Access the **Work with Authority Schemas** interface.
2) In the **OPT** column for the desired schema, enter **2** (Edit).
3) Press **Enter**.
4) In the **Include IFS or Library Object** field, enter ***SYS**.

6.2.3.9. Limit Scope of Authority Schema to Integrated File System (IFS)

Use this task to limit the scope of an authority schema to only address the Integrated File System (IFS).

To limit the scope of the schema

1) Access the **Work with Authority Schemas** interface.
2) In the **OPT** column for the desired schema, enter **2** (Edit).
3) Press **Enter**.
4) In the **Include IFS or Library Object** field, enter ***IFS**.

6.2.3.10. Change Scope of Authority Schema (Object or IFS)

Use this task to change the scope of an authority schema.

To change the scope of the schema

1) Access the **Work with Authority Schemas** interface.
2) In the **OPT** column for the desired schema, enter **12** (Edit).
3) Press **Enter**.

Note: The **Change Scope (Object or IFS)** interface is displayed.

4) Updated the following fields as necessary:

Field	Description
File Type	Enter the appropriate file type: ***SYS** - QSYS.Lib (tradition) file types ***IFS** - IFS (Integrated File System) file types **Note**: For more information about IBM file systems, refer to the IBM Knowledge Center.
Object Name	Enter a specific object name or object group to which this schema applies You can also choose one of the following options: ***NONE** - No objects ***ALL** - All objects **Tip:** You can skip this field for IFS files.
Object Type	Enter the object type to which this authority schema applies, or enter ***ALL** to include all object types **Tip:** You can skip this field for IFS files.
Object Library	Enter the name of the library to which this authority schema applies, or enter ***ALL** to include all libraries **Tip:** You can skip this field for IFS files.
ASP Name	Do one of the following: -- Enter the file path for the IFS or -- Enter the ASP (Auxiliary Storage Pool) for system libraries

Note: If you enter ***SYSBAS**, the system ASP and all basic user ASPs are included.

6.2.3.11. Add Schema Details

Use this task to add an authority schema details. The details are the exceptions that are allowed.

To add an authority schema details

1) Access the **Work with Authority Schemas** interface.
2) In the **OPT** column for the desired schema, enter **10** (Work with Authority Schema Details).
3) Press **Enter**.

Note: The **Work with Authority Schema Details** interface is displayed.

4) Press the **F6** (Create) function key on your keyboard.
5) Complete the following fields.

Field	Description
Schema ID	ID assigned to the schema (not editable)
Schema Description	Text describing the purpose of the schema (not editable)
File Type	Enter the appropriate file type: ***SYS** - QSYS.Lib (tradition) file types ***IFS** - IFS (Integrated File System) file types **Note**: For more information about IBM file systems, refer to the IBM Knowledge Center.
Object Owner	Enter the name of the object owner
Authorization List	Enter the name of the authority list to which this authority schema applies, or enter ***NONE** if not applicable
Object Primary Group	Enter the name of the object primary group to which this authority schema applies or enter ***NONE** if not applicable
User Name	Enter the name of the user (or group) to which the exception applies or enter ***PUBLIC** to apply to all users.
Object Authority	Enter the authority level: ***ALL** - Grant public users all authorities (i.e., change, exclude, use, etc.) ***CHANGE** - Grant public users change authority ***EXCLUDE** - Prohibit public users from performing operations on the object ***USE** - Grant access to the object attributes and allow public users to use of the object (changes to object not allowed) ***AUTL** - Grant public users the public authority specified in the authority list

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

6) Press **Enter** twice.

6.2.3.12. Edit Schema Details

Use this task to edit schema details.

To edit schema details

1) Access the **Work with Authority Schemas** interface.
2) In the **OPT** column for the desired schema, enter **10** (Work with Authority Schema Details).
3) Press **Enter**.

Note: The **Work with Authority Schema Details** interface is displayed.

4) In the **OPT** column for the desired schema, enter **2** (Edit).
5) Press **Enter**.
6) Modify the parameters as necessary.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter** twice.

6.2.3.13. Copy Schema Detail

Use this task to create a new schema detail by copying an existing schema detail.

To copy schema details

1) Access the **Work with Authority Schemas** interface.
2) In the **OPT** column for the desired schema, enter **10** (Work with Authority Schema Details).
3) Press **Enter**.

Note: The **Work with Authority Schema Details** interface is displayed.

4) In the **OPT** column for the desired schema, enter **3** (Copy).
5) Press **Enter**.
6) Modify the parameters as necessary.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**.

6.2.3.14. Delete Schema Detail

Use this task to delete a schema detail.

To delete a schema detail

1) Access the **Work with Authority Schemas** interface.
2) In the **OPT** column for the desired schema, enter **10** (Work with Authority Schema Details).
3) Press **Enter**.

Note: The **Work with Authority Schema Details** interface is displayed.

4) In the **OPT** column for the desired schema, enter **4** (Delete).
5) Press **Enter**.
6) Review the record to ensure you are deleting the correct schema.
7) Press **Enter** twice.

6.2.3.15. Display Authority Schema Compliance Issues

Use this task to display authority schema compliance issues.

Tip: Run this task before you attempt to enforce authority schema to determine if exceptions (details) are required (see Add Schema Details).

To display authority schema compliance issues

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **10** (Enforcement based on Authority Schema).
5) Press **Enter**.
6) Complete the following fields.

Field	Description
Scheme ID	ID assigned to the scheme you want to analyze for compliance
Audit report	Enter ***YES** to enable auditing (tracking)
Report output type	Enter the desired report output format (*HTML, *PRINT, etc.)
Enforcement	Enter ***NO** to display only (not enforce) compliance issues. **Tip**: Always display and investigate before enforcing.
Run interactively	Whether to run interactively or add to batch: ***YES** - Run the report immediately ***NO** - Add the report to a batch job to be run when most efficient for the system

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**.

6.2.3.16. Enforce Authority Schema

Use this task to enforce an authority schema.

Tip: Before enforcing an authority schema, first identify where non-compliance is occurring (see Display Authority Schema Compliance Issues). In some cases, an issue of non-compliance might identify an exception (authority detail) that must be added. In other words, you might need to update the scheme.

To enforce authority schemas

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **10** (Enforcement based on Authority Schema).
5) Press **Enter**.
6) Complete the following fields.

Field	Description
Scheme ID	ID assigned to the scheme you want to analyze for compliance
Audit report	Enter ***YES** to enable auditing (tracking)
Enforcement	Enter ***YES** to enforce the schema

Run interactively	Whether to run interactively or add to batch: ***YES** - Run the report immediately ***NO** - Add the report to a batch job to be run when most efficient for the system

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**.

See also

Working with Authority Schemas

Run Authority Schema Reports

6.2.4. Run Authority Schema Reports

Use this task to generate the following reports:

Usage Report

- Run Authority Schema Compliance Report

Configuration Reports

- Resource Manager Schema Details
- Resource Manager Schema Header

Change Reports

- Resource Manager Schema Details Changes
- Resource Manager Schema Header Changes

To work with Resource Manager reports, access from the **Resource Manger Reports** interface.

To access the Inactive Sessions Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Resource Manager Reports).
5) Press **Enter**.

Note: The **Resource Manger Reports** interface is displayed.

6.2.4.1. Run Resource Manager Schema Details Report

Use this report to view the list of details (exceptions) associated with each authority schema.

To run the Resource Manager Schema Details Report

1) Access the **Resource Manager Reports** interface.
2) At the **Selection or command** prompt, enter **2** (Resource Manager Configuration Reports).

3) Press **Enter**.

Note: The **Resource Manager Configuration Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **2** (Resource Manager Schema Details).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

6.2.4.2. Run Resource Manager Schema Details Changes Report

Use this report to view the list of changes made to the details (exceptions) associated with each authority schema.

Tip: You must enable auditing to produce change reports. See Enable Resource Change Auditing for additional information.

To run the Resource Manager Schema Details Changes Report

1) Access the **Resource Manager Reports** interface.
2) At the **Selection or command** prompt, enter **3** (Resource Manager Change Reports).
3) Press **Enter**.

Note: The **Resource Manager Configuration Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **2** (Resource Manager Schema Details Changes).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

6.2.4.3. Run Resource Manager Schema Header Report

Use this report to display the list of schema headers.

To run the Resource Manager Schema Header Report

1) Access the **Resource Manager Reports** interface.
2) At the **Selection or command** prompt, enter **2** (Resource Manager Configuration Reports).

3) Press **Enter**.

Note: The **Resource Manager Configuration Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **3** (Resource Manager Schema Header).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

6.2.4.4. Run Resource Manager Schema Header Changes Report

Use this report to display the list of changes to schema headers.

To run the Resource Manager Schema Header Changes Report

1) Access the **Resource Manager Reports** interface.
2) At the **Selection or command** prompt, enter **3** (Resource Manager Change Reports).
3) Press **Enter**.

Note: The **Resource Manager Configuration Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **3** (Resource Manager Schema Header Changes).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

6.2.4.5. Run Authority Schema Compliance Report

Use this task to display authority schema compliance issues.

Tip: Run this task before you attempt to enforce an authority schema to determine if exceptions (details) are required (see Add Schema Details).

To run the authority schema compliance report

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).

3) Press **Enter**.
4) At the **Selection or command** prompt, enter **10** (Enforcement based on Authority Schema).
5) Press **Enter**.
6) Complete the following fields.

Field	Description
Scheme ID	ID assigned to the scheme you want to analyze for compliance
Audit report	Enter ***YES** to enable auditing (tracking)
Report output type	Enter the desired report output format (*HTML, *PRINT, etc.)
Enforcement	Enter ***NO** to display (not enforce) compliance issues. **Tip**: Always display and investigate before enforcing.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**.

See also

Working with Authority Schemas

Working with Reports

Run Resource Manager Reports

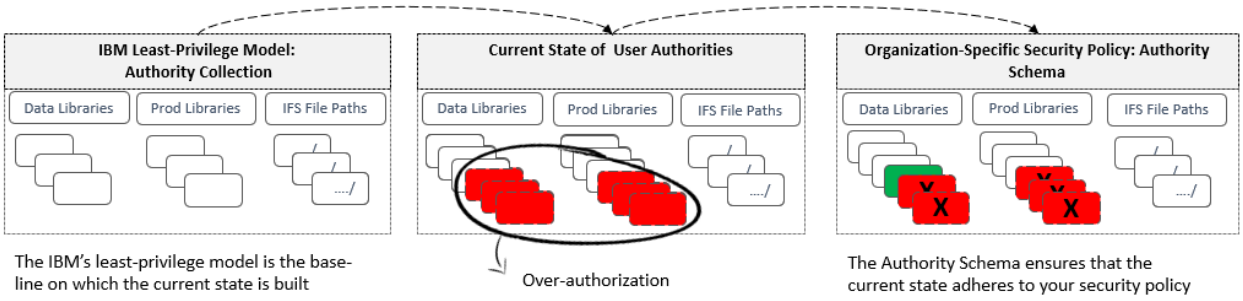
Run Authority Collection Configuration Reports

6.3. Authority Collection Configuration

6.3.1. Working with Authority Collections

This section describes working with the authority collections to compare IBM's least-privileges model with your current authority state in order to help define an authority schema that best meets the security needs of your organization.

Tip: It's good practice is to compare IBM's least privilege model with your current authority state to determine if a user has been granted more authority than necessary. This helps you to eliminate unnecessary over-authorization.



In order to work with authority collections, you must access the **Work with Authority Collection Configuration Users** interface.

To access the Work with Authority Collection Configuration Users interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**.

Note: The **Resource Manager** interface is displayed.

4) At the **Selection or command** prompt, enter **2** (Authority Collection Configuration).
5) Press **Enter**.

Note: The **Work with Authority Collection Configuration Users** interface is displayed.

See also

Log into TGSecure

Display Authority Collection Configuration

Run Authority Collection Reports

6.3.2. Display Authority Collection Configuration

Use this task to do the following:

- Display list of authority collections
- Display authority collection details

6.3.2.1. Display List of Authority Collections

Use this task to display the list of authority collections.

Important: Authority collection is only available with OS IBM i 7.3. or higher.

To display the list of authority collections

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**.

Note: The **Resource Manager** interface is displayed.

4) At the **Selection or command** prompt, enter **2** (Authority Collection Configuration).
5) Press **Enter**.

Note: The **Work with Authority Collection Configuration Users** interface is displayed.

Field	Description
User	Name of the user
Collection Active	Whether user authority data is collected: **YES** - Collection enabled (started) **NO** - Collection disabled (ended)
Repository Exists	Whether a repository exists for the storage of authority data: **YES** - Repository exists **NO** - Repository does not exist

6.3.2.2. Display Authority Collection Details

To display the authority collection configuration details

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **1** (Authority Collection Configuration).
5) Press **Enter**.

Note: The **Work with Authority Collection Configuration** interface is displayed.

6) In the **OPT** column for the desired authority collection, enter **5** (Display Collection Details).
7) Press **Enter**.

Note: The **Display Collection Details** interface is displayed.

Field	Description
User profile	Name of the user for which authority data is being collected
Library	Name of the library monitored, or one of the following: ***NONE** - Exclude libraries ***ALL** - Include all libraries
ASP Device	Name of the ASP device or ***SYSBAS**
Object	Name of the object or one of the following: generic* - First few letters of an object name followed by an asterisk (wildcard) This indicates that all object that begin with the letters identified are to be included. ***ALL** - Include all objects
Object type	Name of the object type or one of the following: ***ALL** - Include all object types
Include DLO	Identifies the document libraries to include: ***NONE** - Exclude document library objects ***ALL** - Include all document library objects (*DOC and *FLR) ***DOC** - include only documents ***FLR** - Include only folders
Include file system objects	Identifies the file system objects to include: ***NONE** - Exclude file system objects ***ALL** - Include all file system objects ***BLKSF** - Include only block files ***CHRSF** - Include only character files ***DIR** - Include only directories ***FIFO** - Include only first-in-first-out special files ***SOCKET** - Include only socket files ***STMF** - Include only steam files ***SYMLNK** - Include only symbolic links

Delete collection	Whether to store or dispose of the collection ***NO** - Dispose ***YES** - Store
Detail	What level of detail should be collected ***OBJINF** - Collect authority details for each unique instance of the object level information ***OBJJOB** - Collect authority details for each unique instance of the object level information and each unique instance of the job

See also

Working with Authority Collection

6.3.3. Manage Authority Collection Configuration

Use this task to do the following with:

- Start authority collection
- End authority collection
- Delete authority collection

To manage authority collections, access the **Work with Authority Collection Users** interface.

To access the Work with Authority Collections Users interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**.

Note: The **Resource Manager** interface is displayed.

4) At the **Selection or command** prompt, enter **2** (Authority Collection Configuration).
5) Press **Enter**.

Note: The **Work with Authority Collection Users** interface is displayed.

6.3.3.1. Start Authority Collection

Use this task to add an authority collection.

To add an authority collection

1) Access the **Work with Authority Collections Users** interface.
2) Press the **F6** (Start Collection) function key on your keyboard.
3) Complete the following fields.

Field	Description
User profile	Name of the user for which you want to begin collecting authority data
Library	Name of the library you want to monitor, or enter one of the following: ***ALL** - Include all libraries ***NONE** - Exclude libraries

ASP Device	Name of the ASP device or ***SYBAS**
Object	Name of the object or one of the following: generic* - First few letters of an object name followed by an asterisk (wildcard). This indicates that all object that begin with the letters identified are to be included. ***ALL** - Include all objects
Object type	Name of the object type or one of the following: ***ALL** - Include all object types
Include DLO	Identifies the document libraries to include: ***ALL** - Include all document library objects (*DOC and *FLR) ***DOC** - include only documents ***FLR** - Include only folders ***NONE** - Exclude document library objects
Include file system objects	Identifies the file system objects monitored: ***ALL** - Include all file system objects ***BLKSF** - Include only block files ***CHRSF** - Include only character files ***DIR** - Include only directories ***FIFO** - Include only first-in-first-out special files ***SOCKET** - Include only socket files ***STMF** - Include only steam files ***SYMLNK** - Include only symbolic links ***NONE** - Exclude file system objects
Delete collection	Whether to store or dispose of the collection ***NO** - Dispose ***YES** - Store
Detail	What level of detail should be collected ***OBJINF** - Collect authority details for each unique instance of the object level information ***OBJJOB** - Collect authority details for each unique instance of the object level information and each unique instance of the job

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

4) Press **Enter** twice.

6.3.3.2. End Authority Collection

Use this task to end an authority collection.

To edit an authority collection

1) Access the **Work with Authority Collections Users** interface.

2) In the **OPT** column for the desired schema, enter **3** (End Collection).
3) Press **Enter**.
4) Review the record to ensure you are ending the correct collection.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

5) Press **Enter** twice.

6.3.3.3. Delete Authority Collection

Use this task to delete an authority collection.

To delete an authority collection

1) Access the **Work with Authority Collections Users** interface.
2) In the **OPT** column for the desired schema, enter **4** (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the correct collection.
5) Press **Enter** twice.

See also:

Working with Authority Collections

Run Authority Collection Reports

6.3.4. Run Authority Collection Configuration Reports

Use this task to generate the following reports:

Usage Reports

- Authority Collection Report (QSYS)
- Authority Collection Report (IFS)
- Authority Compliance Report (Single Schema)
- Authority Compliance Report (All Schemas)

To work with authority collection reports, access from the **Resource Manger Reports** interface.

To access the Resource Manager Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**.

Note: The **Resource Manager** interface is displayed.

4) At the **Selection or command** prompt, enter **20** (Resource Manager Reports).
5) Press **Enter**.

Note: The **Resource Manger Reports** interface is displayed.

6.3.4.1. Run Authority Compliance Report (Single Schema)

Use this report to identify compliance issues with your authority schema(s). You can use this report to identify two states:

- Instances in which your authority scheme is being enforced (i.e., in compliance with your schema)
- Instances in which your authority scheme is not being enforced (i.e., out of compliance with your schema)

To run the Authority Compliance report for all schemas

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **4** (Resource Manager).
3) Press **Enter**.

Note: The **Resource Manager** interface is displayed.

4) At the **Selection or command** prompt, enter **1** (Authority Schema Configuration).
5) Press **Enter**.

Note: The **Work with Authority Schemas** interface is displayed.

6) In the **OPT** column for the desired schema, enter **22** (Run Compliance Report).
7) Press **Enter**.
8) In the **Audit report** field, enter ***YES**.
9) Enter the desired output format in the **Report output type** field.
10) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

6.3.4.2. Run Authority Compliance Report (All Schemas)

Note: Running authority compliance for all reports might take a lot time and system resources.

Use this report to identify compliance issues with your authority schema(s). You can use this report to identify two states:

- Instances in which your authority scheme is being enforced (i.e., in compliance with your schema)
- Instances in which your authority scheme is not being enforced (i.e., out of compliance with your schema)

To run the Authority Compliance report for all schemas

1) Access the **Resource Manager Reports** interface.
2) At the **Selection or command** prompt, enter **1** (Resource Manager Usage Reports).
3) Press **Enter**.

Note: The **Resource Manager Usage Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **1** (Authority Compliance Report).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

6.3.4.3. Run Authority Collection Report (QSYS)

Use this task to generate the authority collection report for QSYS.

Note: QSYS is the traditional file management structure used to control the storing and accessing of traditional file objects (*FILE objects in the QSYS.LIB library). For more information about IBM file systems, refer to the IBM Knowledge Center.

To run the Authority Collection report (QSYS)

1) Access the **Resource Manager Reports** interface.
2) At the **Selection or command** prompt, enter **1** (Resource Manager Usage Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **3** (Authority Collection Report - QSYS).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

6.3.4.4. Run Authority Collection Report (IFS)

Use this task to generate the authority collection report for Integrated File System (IFS).

Note: IFS a newer file management structure that supports stream input/output and is similar to the structure used by personal computers and UNIX operating systems. For more information about IBM file systems, refer to the IBM Knowledge Center.

To run the Authority Collection report (IFS)

1) Access the **Resource Manager Reports** interface.
2) At the **Selection or command** prompt, enter **1** (Resource Manager Usage Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **2** (Authority Collection Report - IFS).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

See also

Working with Authority Collection

Working with Reports

7. User Profile Management

The User Profile Management feature allows you to manage user profiles using blueprints. Think of a blueprint as template that defines user profile best practices. Once you create a blueprint, you can use it to evaluate, create, or modify user profiles.

In addition, the Profile Manager allows you to do the following:

- Work with profile manager defaults
- Work with blueprints
- Work with user exclusions
- Work with archived profiles
- Work with inactive profiles
- Work with user profiles
- Work with password rules

To access the Profile Manager interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Manager).
3) Press **Enter**.

See also

Log into TGSecure

Use TGSecure

Working with Profile Manager Defaults

Display Profile Manager Defaults

Manage Profile Manager Defaults

Run Profile Manager Reports

7.1. User Profile Management Defaults

7.1.1. Working with Profile Management Defaults

This section describes working with User Profile Management defaults.

User Profile Manager defaults allow you to define the following:

- Whether to send profile change alerts
- Whether to track profile changes (required if you plan to run reports)
- Journal in which to store profile changes
- Library in which to store profile changes
- Queue in which to store profile alerts
- Queue library in which to profile alerts

In order to work with profile manager defaults, you must access the **User Profile Management Defaults** interface.

To access the User Profile Management Defaults interface

1) Log into to TGSecure.

Note: The **Main** menu appears.

2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.

Note: The **User Profile Management** interface is displayed.

4) At the **Selection or command** prompt, enter **7** (User Profile Management Defaults).
5) Press **Enter**.

Note: The **Profile Manager Defaults** interface is displayed.

See also

Log into TGSecure

Display User Profile Management Defaults

Manage User Profile Management Defaults

Run User Profile Management Reports

7.1.2. Display User Profile Management Defaults

Use this task to display the User Profile Management defaults.

To display the Profile Manager defaults

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.

Note: The **User Profile Management** interface is displayed.

4) At the **Selection or command** prompt, enter **7** (Profile Manager Defaults).
5) Press **Enter**.

Note: The **User Profile Management Defaults** interface is displayed.

Field	Description
Audit Journal	Journal in which to store resource manager usage data **Note**: The default audit journal for TG products is TGJRN. This journal resides in the TGDATA library.
Audit Journal Library	Library in which the journal resides
Audit Configuration Changes	Whether to track profile changes: **Y** - Enable tracking of changes **N** - Disable tracking of changes **Tip**: Set this flag to **Y** if you plan to run usage reports. **Note**: There are multiple product modules (e.g., network security, access escalation, inactive session lockdown, etc.) in which you can track configuration changes. Therefore, if you see ***NONE** in the comment field, this indicates that

	configuration changes are not being tracked in any module. This is common at the time the product is initially installed. If you see ***PARTIAL**, this indicates that configuration changes are being track in at least one module, but not all modules. If you see ***ALL**, this indicates that configuration changes are being tracked in all modules
Alerting Status	Whether alerts are enabled: ***YES** - Enable alerts (create admin alert) ***NO** - Disable alerts
Alert Message Queue	Queue in which to store alerts
Alert Message Queue Library	Library in which to store the queue
Archive User Profile	Whether to archive inactive profiles: ***YES** - Create an archive ***NO** - Do not create an archive **Tip**: For the system to archive user profiles, you must install the necessary exit programs, and the following conditions must be met: a. The user profile is deleted via the OS (i.e., DLTUSRPRF, etc.) b. The user profile is associated with a blueprint c. The user profile is inactive for greater than the number of days defined for profiles that qualify for deletion
Archive Profiles Retention (Days)	Number of days an archived profile is retained by the system
Exit Programs Installed	Whether the exit programs necessary for profile management (including archiving) are installed: ***YES** - The exit programs that support user profile management are installed ***NO** - The exit programs that support user profile management are uninstalled **Note**: See Manage Profile Manager Defaults for instruction on adding exit programs.

See also

Working with User Profile Management Defaults

Run User Profile Management Reports

Run Blueprint Reports

Run User Exclusion Reports

Run Archived Profile Reports

Run Inactive Profile Reports

Run User Profile Reports

7.1.3. Manage User Profile Management Defaults

Use this task to do the following:

- Enable profile auditing
- Enable profile alerts
- Enable profile archiving
- Add profile exit programs
- Remove profile exit programs

To manage Profile Manager defaults, access the **User Profile Management Defaults** interface.

To access the User Profile Management Defaults interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.

Note: The **User Profile Management** interface is displayed.

4) At the **Selection or command** prompt, enter **7** (User Profile Management Defaults).
5) Press **Enter**.

Note: The **User Profile Management Defaults** interface is displayed.

7.1.3.1. Enable Profile Auditing

Use this task to enable profile change auditing.

Tip: Auditing is required if you plan to run profile change reports.

To enable profile auditing

1) Access the **User Profile Management Defaults** interface.
2) In the **Audit Journal** field, enter the name of the journal in which to store changes.
3) In the **Audit Journal Library** field, enter the name of the library in which the journal resides.
4) In the **Audit Configuration Change** field, enter **Y**.
5) Press **Enter**.

Note: There are multiple product modules (e.g., network security, access escalation, inactive session lockdown, etc.) in which you can track configuration changes. Therefore, if you see ***NONE** in the comment field, this indicates that configuration changes are not being tracked in any module. This is common at the time the product is initially installed. If you see ***PARTIAL**, this indicates that configuration changes are being track in at least one module, but not all modules. If you see ***ALL**, this indicates that configuration changes are being tracked in all modules

7.1.3.2. Enable Profile Alerts

Use this task to enable profile change alerts.

Tip: Alerting is required if you plan to send alert notifications.

To enable profile alerts

1) Access the **User Profile Management Defaults** interface.
2) In the **Alerting Status** field, enter ***YES**.
3) In the **Alert Message Queue** field, enter the name of the queue in which to store the alerts.
4) In the **Alert Message Queue Library** field, enter the name of the library in which the queue resides.
5) Press **Enter**.

7.1.3.3. Enable Profile Archiving

Use this task to enable archiving of inactive user profiles.

Tip: The exit programs are required (must be installed) if you plan to use the Program Manager feature.

To enable profile archiving

1) Access the **User Profile Management Defaults** interface.
2) In the **Archive User Profile** field, enter ***YES**.
3) In the **Archive Profiles Retention** field, enter the number of days the archived should be retained.
4) Press **Enter**.

7.1.3.4. Add Profile Exit Programs

Use this task to add (install) the User Profile Management exit program.

Tip: This exit program is required to enable Program Manager features.

To add Profile Manager exit programs

1) Access the **User Profile Management Defaults** interface.
2) Press the **F20** (Add Exit Program) function key on your keyboard.

7.1.3.5. Remove Profile Exit Programs

Use this task to remove (uninstall) the User Profile Management exit program.

Tip: The exit program is required to enable Program Manager features.

To remove profile exit programs

1) Access the **User Profile Management Defaults** interface.
2) Press the **F21** (Remove Exit Program) function key on your keyboard.

See also

Working with User Profile Management Defaults

Run User Profile Management Reports

7.1.4. Run User Profile Management Default Reports

The following Profile Manager reports are available:

Configuration Report

- User Profile Management Defaults

Change Report

- User Profile Management Defaults Changes

Tip: You can schedule the Profile Manager Default reports (like all other reports) to run when most convenient.

To work with Profile Manager Default reports, access from the **User Profile Reports** interface.

To access the User Profile Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (User Profile Reports).
5) Press **Enter**.

Note: The **User Profile Reports** interface is displayed.

7.1.4.1. Run User Profile Management Defaults Report

To run the User Profile Manager Default Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **2** (User Profile Configuration Reports).
3) Press **Enter**.

Note: The **User Profile Configuration Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **11** (Profile Manager Defaults).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

7.1.4.2. Run User Profile Management Defaults Changes Report

Tip: You must enable auditing to produce change reports. See Enable Profile Auditing for additional information.

To run the Profile Manager Default Changes Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **3** (User Profile Change Reports).
3) Press **Enter**.

Note: The **User Profile Change Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **11** (Profile Manager Defaults Changes).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

See also:

Working with User Profile Management Defaults

Working with Reports

Run Blueprint Reports

Run User Exclusion Reports

Run Archived Profile Reports

Run Inactive Profile Reports

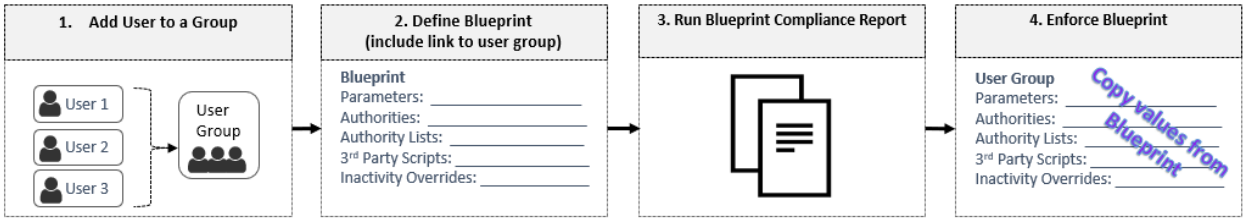
Run User Profile Reports

7.2. Blueprints

7.2.1. Working with Blueprints

This section describes working with blueprints. Blueprints allow you to design a 'template' by which to create new user profiles. In addition, you can use a blueprint to perform a mass update to all profiles assigned to a specific user group. To determine if the profiles within a user group conform to a blueprint, run the blueprint compliance report. The report identifies any discrepancies. You can then enforce a blueprint to eliminate the discrepancies (modify the user profiles within a group to 'match' the blueprint.

The following is the process used to define and implement blueprints:



In order to work with blueprints, you must access the **Work with Blueprints** interface.

To access the Work with Blueprint interface

1) Log into to TGSecure.

Note: The **Main** menu appears.

2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.

Note: The **User Profile Management** interface is displayed.

4) At the **Selection or command** prompt, enter **1** (Work with Blueprints).
5) Press **Enter**.

Note: The **Work with Blueprints** interface is displayed.

See also

Log into TGSecure

Display Blueprints

Manage Blueprints

Run Blueprint Reports

7.2.2. Display Blueprints

Use this task to do the following with blueprints:

- Display list of blueprints
- Sort list of blueprints
- Move to position in list of blueprints
- Filter list blueprint

7.2.2.1. Display List of Blueprints

Use this task to display the list of available blueprints.

To display the list of blueprints

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.

Note: The **User Profile Management** interface is displayed.

4) At the **Selection or command** prompt, enter **1** (Work with Blueprints).
5) Press **Enter**.

Note: The **Work with Blueprints** interface is displayed.

Field	Description
Blueprint ID	ID assigned to the blueprint
User Group	Name of user group to which the blueprint applies
Prf Parm	Whether parameters are defined: ***YES** - One or more profile parameters are defined for the blueprint ***NO** - No profile parameters are defined
Prf Auth	Whether object authorities are defined: ***YES** - One or more object authorities are defined for the blueprint ***NO** - No object authorities are defined
Auth List	Whether authority lists are defined: ***YES** - One or more authority lists are defined for the blueprint ***NO** - No object authorities are defined
3rd Party	Whether 3rd party scripts are defined: ***YES** - One or more 3rd party scripts are defined for the blueprint

	***NO** - No 3rd party scripts are defined
Alt Sts	Whether alerts are enabled: ***YES** - Alerts enabled (create admin alerts) ***NO** - Alerts disabled
Compliance Date	Date on which blueprint compliance and profile inactivity check was last performed
Compliance Time	Time at which blueprint compliance and profile inactivity check was last performed
Inact Ovr	Whether inactivity overrides are enabled: ***YES** - Overrides are enabled ***NO** - Overrides disabled
Inact Prf?	Whether inactive profiles exist (according to last report run): **Y** - Inactive profile were found (consider running enforcement) **N** - Inactive profiles were not found
Comp Status	Whether the current authority levels comply with the blueprint **PASS** - User authorities comply with the current blueprint **FAIL** - User authorities do not comply with the current blueprint
Blueprint Description	Description of the blueprint

7.2.2.2. Sort List of Blueprint

Use this task to sort the list. The column on which the list is currently sorted appears in white text.

To sort the list

1) Access the **Work with Blueprint** interface.
2) Place your cursor on the desired column heading.
3) Press the **F10** (Sort) function key.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

7.2.2.3. Move to Position in List of Blueprints

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

To move to a specific position within the list

1) Access the **Work with Blueprint** interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.
4) Press **Enter**.

Note: The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

7.2.2.4. Filter List Blueprint

Use this task to limit the objects displayed in the list by defining a subset for filtering purposes.

Tip: Use wildcard asterisk (*) to help define your subset.

-- Add an asterisk before text (e.g., *report) to find list items that end with specific text.

-- Add an asterisk after text (e.g., report*) to find list items that start with specific text.

-- Add asterisks around text (e.g., *report*) to find list items that contain specific text anywhere in the name.

To filter the list using a subset

1) Access the **Work with Blueprint** interface.
2) Press the **F8** (Subset) function key.
3) Enter the criteria you want to use to define the subset.
4) Press **Enter**.

Note: The system filters the results based on the criteria you defined for the subset.

See also

Working with Blueprints

Manage Blueprints

Run Blueprint Reports

7.2.3. Manage Blueprints

Use this task to do the following with blueprints:

Blueprints

- Add blueprint
- Copy blueprint
- Delete blueprint
- Display blueprint details
- Display inactivity overrides
- Edit blueprint details
- Edit blueprint profile parameters
- Edit blueprint profile authorities
- Edit blueprint authority lists
- Edit blueprint 3rd party scripts
- Edit blueprint permissions

Blueprint Users

- Add blueprint user
- Edit blueprint user
- Delete blueprint user

Blueprint Enforcement

- Display blueprint compliance issues
- Display list of non-compliant profiles
- Enforce blueprint

To manage blueprints, access the **Work with Blueprints** interface.

To access the Work with Blueprints interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.

Note: The **User Profile Management** interface is displayed.

4) At the **Selection or command** prompt, enter **1** (Work with Blueprints).
5) Press **Enter**.

Note: The **Work with Blueprints** interface is displayed.

7.2.3.1. Add Blueprint

Use this task to add a blueprint. There a number of details that need to be included in each blueprint, so a wizard has been designed to help you complete this multi-step process.

- Step 1: Add blueprint details
- Step 2: Add profile parameters to a blueprint
- Step 3: Add object authorities to a blueprint
- Step 4: Add authority list settings to a blueprint
- Step 5: Add 3rd party scripts to a blueprint
- Step 6: Add permissions to a blueprint

Tip: Press the **F12** (Cancel) function key if you make a mistake in the wizard and you want to return to a previous step to make modifications.

Step 1: Add Blueprint Details

To add blueprint details

1) Access the **Work with Blueprints** interface.
2) Press the **F6** (Add Wizard) function key on your keyboard.

Note: The **Blueprint - Add** interface is displayed.

3) Complete the following fields.

Field	Description
Blueprint ID	ID you want to assign to the blueprint
Blueprint Description	Text describing the purpose of the blueprint
Alert Status	Whether alerts are enabled: ***YES** - Enable alerts (create admin alerts) ***NO** - Disable alerts
User Scope	Enter the user group you want to associate with the blueprint.

	Note: If you create a new profile based on this blueprint, the group you enter in this field will be the user group to which you can add new profiles. This is also the user group whose member are updated when a blueprint is enforced. (See Manager User Profiles, for information about adding a user profile based on an exiting blueprint.)
Inactivity until User Profile is disabled (days)	Number of days a profile must remain inactive profile before it is **disabled** **Note**: *DFT (Default) indicates that the standard number of days defined by IBM should be applied
Inactivity until User Profile is deleted (days)	Number of days a profile must remain inactive profile before it is **deleted** **Note**: *DFT (Default) indicates that the standard number of days defined by IBM should be applied
Object owner for objects owned by deleted profiles	Name of the user whom should take over ownership of objects when/if a profile is disabled or deleted **Note**: *DFT (Default) indicates that the standard owner defined by IBM should be applied

4) Press **Enter**.

Note: The **User Profile Parameter Settings** interface is displayed.

Tip: Press the **F12** (Cancel) function key if you make a mistake in the wizard and you want to return to a previous step to make modifications.

Step 2: Add Profile Parameters to a Blueprint

Tip: You can skip this step by pressing **Enter**.

To add profile parameters to your blueprint

1) Do one of the following:

If	Then
If you want to see only the system-suggested parameters	Press the **F7** (Add Suggested) function key **Note**: This option adds only the profile parameters suggested by the intelligence engine.
If you want to see all available parameters	Press the **F6** (Add All) function key **Note**: This option adds all available profile parameters (and their associated default values). You can edit the default value if necessary. **Tip**: ***ANY** is not a valid parameter value. If ***ANY** is the default value, you will be required to enter a specific value before you can save the blueprint.

Note: The **Parameter Selection** dialog appears.

2) In the **Sel** column, enter **1** beside the parameter(s) you want to add.

Tip: To make no selections, press the **F12** (Cancel) function key to return to the previous screen.

3) Press **Enter** to add the selected parameters and return to the **User Profile Parameter Settings** interface.
4) Press **Enter**.

Note: The **User Profile Object Authority** interface is displayed.

Tip: Press the **F12** (Cancel) function key if you make a mistake in the wizard and you want to return to a previous step to make modifications.

Step 3: Add Object Authorities to a Blueprint

Tip: You can skip this step by pressing **Enter**.

To add object authorities to your blueprint

1) In the ***USRPRF Object** area, complete the following fields:

Field	Description
Object Owner	Enter one the following: [Name] - Enter the user name you want to assign as the owner of user profile objects ***DFT** - Assign user profile object ownership to the default (IBM) user ***USRPRF** - Assign user profile object ownership to the user running the program **Note**: If *DFT appears in this column, the two fields below should be left blank.
Owner Authority	Enter the authority level you want to assign the object owner: ***ALL** - Grant owner all authorities (i.e., change, exclude, use, etc.) ***CHANGE** - Grant owner change authority ***EXCLUDE** - Prohibit owner from performing operations on the object ***USE** - Grant access to the object attributes and allow owner to use of the object (but not change the object)
*PUBLIC Authority	Enter the authority level you want to assign to public users (*Public): ***ALL** - Grant public users all authorities (i.e., change, exclude, use, etc.) ***AUTL** - Grant public users the default level of authority specified by the authority list ***CHANGE** - Grant public users change authority ***EXCLUDE** - Prohibit pubic users from performing operations on the object ***USE** - Grant access to the object attributes and allow public users to use of the object (but not change the object)

2) In the ***MSGQ Object** area, complete the following fields:

Field	Description
Object Owner	Enter one the following: [Name] - Enter the user name you want to assign as the owner of message queue objects ***DFT** - Assign message queue object ownership to the default (IBM) user ***USRPRF** - Assign message queue object ownership to the user running the program **Note**: If *DFT appears in this column, the two fields below should be left blank.
Owner Authority	Enter the authority level you want to assign the object owner: ***ALL** - Grant owner all authorities (i.e., change, exclude, use, etc.) ***CHANGE** - Grant owner change authority ***EXCLUDE** - Prohibit owner from performing operations on the object ***USE** - Grant access to the object attributes and allow owner to use of the object (but not change the object)

*PUBLIC Authority	Enter the authority level you want to assign to public users (*Public): ***ALL** - Grant public users all authorities (i.e., change, exclude, use, etc.) ***AUTL** - Grant public users the default level of authority specified by the authority list ***CHANGE** - Grant public users change authority ***USE** - Grant access to the object attributes and allow public users to use of the object (but not change the object)

3) Press **Enter**.

Note: The **Authority List Settings** interface is displayed.

Tip: Press the **F12** (Cancel) function key if you make a mistake in the wizard and you want to return to a previous step to make modifications.

Step 4: Add Authority List Settings to a Blueprint

Tip: You can skip this step by pressing **Enter**.

To add authority list settings to your blueprint

1) Press the **F6** (Add) function key on your keyboard.

Note: The **Authority List Settings** interface is displayed.

2) Complete the following fields:

Field	Description
Authority List	Enter the name of the authority list to which this blueprint applies **Note**: An authority list displays the users who have authority to access a specific object.
Authority Value	Enter the authority level you want to assign users who are members of the authority list: ***ALL** - Grant users all authorities (i.e., change, exclude, use, etc.) ***CHANGE** - Grant users change authority ***EXCLUDE** - Prohibit uses from performing operations on the object ***USE** - Grant access to the object attributes and allow users to use of the object (but not change the object)

3) Press **Enter** to add the authority list and return to the User **Authority List Settings** interface.
4) Press **Enter**.

Note: The **3rd Party Integration** interface is displayed.

Tip: Press the **F12** (Cancel) function key if you make a mistake in the wizard and you want to return to a previous step to make modifications.

Step 5: Add 3rd Party Scripts to a Blueprint

Tip: You can skip this step by pressing **Enter**.

To add 3rd party scripts to your blueprint

1) Press the **F6** (Add) function key on your keyboard.

Note: The **3rd Party Integration** interface is displayed.

2) Complete the following fields:

Field	Description
Script Type	Type of third-party script
Script Statement	3rd party script text

4) Press **Enter**.

Tip: Press the **F12** (Cancel) function key if you make a mistake in the wizard and you want to return to a previous step to make modifications.

Step 6: Add Permissions to a Blueprint

Tip: You can skip this step by pressing **Enter**.

To add permissions to a blueprint

1) Press the **F6** (Add) function key on your keyboard.

Note: The **Blueprint Permissions** interface is displayed.

2) Complete the following fields:

Field	Description
User/Group	User or user group that has permission to use the blueprint to create and change user profiles **Tip**: Press the F4 (List) function key to see of list of available options.
Create Permission	Whether the user/user group has permission to create new user profiles based on blueprint ***YES** - Enable create ***NO** - Disable create
Change Permission	Whether the user/user group has permission to change user profiles based on blueprint ***YES** - Enable change ***NO** - Disable change

3) Press **Enter**.

Tip: Press the **F12** (Cancel) function key if you make a mistake in the wizard and you want to return to a previous step to make modifications.

7.2.3.2. Copy Blueprint

Use this task to create a new blueprint by copying an existing blueprint.

To copy a blueprint

1) Access the **Work with Blueprint** interface.
2) In the **OPT** column for the desired blueprint, enter **3** (Copy).
3) Press **Enter**.
4) Modify the parameters as necessary.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

5) Press **Enter** twice.

7.2.3.3. Delete Blueprint

Use this task to delete a blueprint.

To delete a blueprint

1) Access the **Work with Blueprint** interface.
2) In the **OPT** column for the desired blueprint, enter **4** (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the correct blueprint.
5) Press **Enter** twice.

7.2.3.4. Display Blueprint Details

Use this task to display blueprint details.

To display blueprint details

1) Access the **Work with Blueprints** interface.
2) In the **OPT** column for the desired blueprint, enter **5** (Display).
3) Press **Enter**.

Field	Description
Blueprint ID	ID assign to the blueprint
Blueprint Description	Text describing the purpose of the blueprint
Alert Status	Whether alerts are enabled ***YES** - Enable alerts (create admin alerts) ***NO** - Disable alerts
User Scope	User group to which the blueprint applies
Inactivity until User Profile is disabled (days)	Number of days a profile must remain inactive before it is disabled **Note**: *DFT (Default) indicates that the standard number of days defined by IBM should be applied
Inactivity until User Profile is deleted (days)	Number of days a profile must remain inactive before it is deleted **Note**: *DFT (Default) indicates that the standard number of days defined by IBM should be applied
Object owner for objects owned by deleted profiles	Name of the user whom should take over ownership of objects when a profile is disabled or deleted **Note**: All objects must be assigned an owner.

7.2.3.5. Display Inactivity Overrides

Use this task to display inactivity overrides. When you create a blueprint, you have the option to use the default (*DFT) IBM policy to determine when an inactive user profile is disabled or deleted (and to whom object ownership should be transferred in such a case).

To display inactive overrides

1) Access the **Work with Blueprints** interface.
2) In the **OPT** column for the desired blueprint, enter **14** (Inactivity Overrides).
3) Press **Enter**.

Field	Description
Inactivity until User Profile is disabled (days)	Number of days a profile must remain inactive profile before it is **disabled** **Note**: *DFT (Default) indicates that the standard number of days defined by IBM should be applied
Inactivity until User Profile is deleted (days)	Number of days a profile must remain inactive profile before it is **deleted** **Note**: *DFT (Default) indicates that the standard number of days defined by IBM should be applied
Object owner for objects owned by deleted profiles	Name of the user whom should take over ownership of objects when a profile is disabled or deleted

7.2.3.6. Edit Blueprint Details

Use this task to edit the details of an existing blueprint.

To edit blueprint details

1) Access the **Work with Blueprints** interface.
2) In the **OPT** column for the desired blueprint, enter **2** (Edit).
3) Press **Enter**.
4) Modify the parameters as necessary.
5) Press **Enter** twice.

7.2.3.7. Edit Blueprint Profile Parameters

Use this task to edit the profile parameters for an existing blueprint.

To edit blueprint profile parameters

1) Access the **Work with Blueprints** interface.
2) In the **OPT** column for the desired blueprint, enter **10** (Profile Parameters).
3) Press **Enter**.
4) Modify the parameters as necessary.

Note: You also have the ability to add and delete parameters.

5) Press **Enter** twice.

7.2.3.8. Edit Blueprint Profile Authorities

Use this task to edit the profile authorities for an existing blueprint.

To edit blueprint profile authorities

1) Access the **Work with Blueprints** interface.
2) In the **OPT** column for the desired blueprint, enter **11** (Profile Authorities).

3) Press **Enter**.
4) Modify the parameters as necessary.

Note: You also have the ability to add and delete profile authorities.

5) Press **Enter** twice.

7.2.3.9. Edit Blueprint Authority Lists

Use this task to edit the authority list for an existing blueprint.

To edit blueprint authority list

1) Access the **Work with Blueprints** interface.
2) In the **OPT** column for the desired blueprint, enter **12** (Authority Lists).
3) Press **Enter**.
4) Modify the parameters as necessary.

Note: You also have the ability to add and delete authority lists.

5) Press **Enter** twice.

7.2.3.10. Edit Blueprint 3rd Party Scripts

Use this task to edit 3rd party scripts associated with an existing blueprint.

To edit blueprint 3rd party scripts

1) Access the **Work with Blueprints** interface.
2) In the **OPT** column for the desired blueprint, enter **13** (3rd Party).
3) Press **Enter**.
4) Modify the parameters as necessary.

Note: You also have the ability to add and delete 3rd party scripts.

5) Press **Enter** twice.

7.2.3.11. Edit Blueprint Permissions

Use this task to manage who can use a blueprint (as a template) to create and change user profiles.

To edit blueprint permissions

1) Access the **Work with Blueprints** interface.
2) In the **OPT** column for the desired blueprint, enter **30** (Blueprint Permissions).
3) Press **Enter**.
4) Modify the following fields as necessary.

Field	Description
User/Group	User or user group who has permission to use the blueprint to create and change user profile **Tip**: Press the F4 (List) function key to see of list of available options.
Create Permission	Whether the user/user group has create permission ***YES** - Enable create

	***NO** - Disable create
Change Permission	Whether the user/user group has change permission ***YES** - Enable change ***NO** - Disable change

5) Press **Enter** twice.

7.2.3.12. Add Blueprint User

Use this task to add a user (member) to a blueprint user group.

To add blueprint user

1) Access the **Work with Blueprints** interface.
2) In the **OPT** column for the desired blueprint, enter **15** (Work with Users).
3) Press **Enter**.

Note: The **Work with Users** interface is displayed.

4) Press the **F6** (Add) function key on your keyboard.

Note: The **Work with Users - Add Record** interface is displayed.

5) Complete the following fields.

Field	Description
User Name	Name of user
User Description	Description of user

6) Press **Enter**.

Note: If the system locates the user on the server, then a ***YES** appears in the **Exists on Server** field.

7.2.3.13. Edit Blueprint User

Use this task to edit the user details of a user (member) assigned to a blueprint group.

To edit a blueprint user

1) Access the **Work with Blueprints** interface.
2) In the **OPT** column for the desired blueprint, enter **15** (Work with Users).
3) Press **Enter**.

Note: The **Work with Users** interface is displayed.

4) In the **OPT** column for the desired user, enter **2** (Edit).
5) Press **Enter**.
6) Modify the parameters as necessary.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter** twice.

7.2.3.14. Delete Blueprint User

Use this task to delete a user (member) from a blueprint group.

To delete a blueprint user

1) Access the **Work with Blueprints** interface.
2) In the **OPT** column for the desired blueprint, enter **15** (Work with Users).
3) Press **Enter**.

Note: The **Work with Users** interface is displayed.

4) In the **OPT** column for the desired user, enter **4** (Delete).
5) Press **Enter**.
6) Review the record to ensure you are deleting the correct blueprint.
7) Press **Enter** twice

7.2.3.15. Display Blueprint Compliance Issues

Use this task to display blueprint compliance issues. This is another way of running the blueprint compliance report.

To display blueprint compliance issues

1) Access the **Work with Blueprints** interface.
2) In the **OPT** column for the desired blueprint, enter **22** (Run Compliance Report).
3) Press **Enter**.
4) Complete the following fields.

Field	Description
Component	Name of blueprint
Audit report	Enter ***YES** to enable auditing (tracking)
Report output type	Enter the desired report output format (*HTML, *PRINT, etc.)
Enforcement	Enter ***NO** to display only (not enforce them) compliance issues **Tip**: Always display and investigate before enforcing.
Run interactively	Whether to run interactively or add to batch: ***YES** - Run the report immediately ***NO** - Add the report to a batch job to be run when most efficient for the system.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

5) Press **Enter**.

7.2.3.16. Display List of Non-Compliant Profiles

Use this task to display blueprint compliance issues identified when the blueprint compliance report was last run.

Tip: Before you can display compliance issues you must run the blueprint compliance report.

To display blueprint compliance issues

1) Access the **Work with Blueprints** interface.
2) In the **OPT** column for the desired blueprint, enter **20** (Non-Compliant).
3) Press **Enter**.

Field	Description
User Name	Name of the user
Violation	How the user's profile is in violation of the blueprint: **Category** - Category of violation **Keyword** - Parameter that is in violation **Description** - Description of object in violation
Blueprint Value	Parameter value defined in the blueprint
Actual Value	Parameter value defined in the user profile

7.2.3.17. Enforce Blueprint

Use this task to enforce a blueprint.

Tip: Before enforcing a blueprint, first display the blueprint compliance issues to identify where non-compliance is occurring. In some cases, an issue of non-compliance might identify the need for an exclusion to be added. In other words, you might need to update the blueprint.

To enforce authority blueprint

1) Access the **Work with Blueprints** interface.
2) In the **OPT** column for the desired blueprint, enter **24** (Run Enforcement).
3) Press **Enter**.
4) Complete the following fields.

Field	Description
Component	Name of blueprint
Audit report	Enter ***YES** to enable auditing (tracking)
Report output type	Enter the desired report output format (*HTML, *PRINT, etc.)
Enforcement	Enter ***YES** to enforce the blueprint **Tip**: Always display and investigate before enforcing.
Run interactively	Whether to run interactively or add to batch: ***YES** - Run the report immediately ***NO** - Add the report to a batch job to be run when most efficient for the system.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

5) Press **Enter**.

See also

Working with Blueprints

Run Blueprint Reports

Manage User Profiles

7.2.4. Run Blueprint Reports

Use this task to generate the following blueprint reports:

Usage Report

- Run Blueprint Compliance Report

Configuration Reports

- Blueprint Master
- Blueprint Permission File
- Blueprint Parameter File
- Blueprint Object Authority File
- Blueprint Authority List Settings File
- Blueprint Non-Compliance User Profiles
- Blueprint 3rd Party Integration File

Change Reports

- Blueprint Master Changes
- Blueprint Permission File Changes
- Blueprint Parameter File Changes
- Blueprint Object Authority File Changes
- Blueprint Authority List Settings File Changes
- Blueprint Non-Compliance User Profiles Changes
- Blueprint 3rd Party Integration File Changes

Tip: You can schedule the blueprint reports (like all other reports) to run when most convenient.

To work with blueprint reports, access from the **User Profile Reports** interface.

To access the User Profile Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (User Profile Reports).
5) Press **Enter**.

Note: The **User Profile Reports** interface is displayed.

7.2.4.1. Run Blueprint Compliance Report

Use this task to run the blueprint compliance issues report. This report lists the users whose profile authorities do not meet blueprint requirements.

Tip: Run this task before you attempt to enforce a blueprint to determine if exclusions are required (see Add Exclusions).

To run the Blueprint Compliance Report

1) Access the **User Profile Reports** interface.

2) At the **Selection or command** prompt, enter **1** (User Profile Usage Reports).
3) Press **Enter**.

Note: The **User Profile Usage Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **1** (Blueprint Compliance Report).
5) Press **Enter**.
6) Complete the following fields.

Tip: To see the complete list of available parameters, press the **F9** function key.

Field	Description
Component	Enter ***BLUEPRINT**
Audit report	Enter ***YES** to enable auditing (tracking)
Users	User profile to include in the report
Days for disable user profile	Number of days a profile must remain inactive profile before it is **disabled** **Note**: *DFT (Default) indicates that the standard number of days defined by IBM should be applied
Days for delete user profile	Number of days a profile must remain inactive profile before it is **deleted** **Note**: *DFT (Default) indicates that the standard number of days defined by IBM should be applied
Report output type	Enter the desired report output format (*HTML, *PRINT, etc.)
File to receive output	Name of file to receive report output
Library	Library in which the file resides
Replace or add records	Whether to replace or append records to the file
Enforcement	Enter ***NO** to display only (not enforce) compliance issues **Tip**: Always display and investigate before enforcing.
Run interactively	Whether to run interactively or add to batch: ***YES** - Run the report immediately ***NO** - Add the report to a batch job to run when most efficient for the system.
Job queue	If you want to include report in batch, enter job queue
Library	Library in which job queue resides
Schedule?	Whether report is scheduled

7) Press **Enter**.

7.2.4.2. Run Blueprint Master Report

Use this task to display the list of blueprints.

To run the Blueprint Master Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **2** (User Profile Configuration Reports).
3) Press **Enter**.

Note: The **User Profile Configuration Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **1** (Blueprint Master).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

7.2.4.3. Run Blueprint Permission File Report

Use this task to display permissions associated with blueprints. Permissions determine who can use a blueprint to create or modify user profiles.

To run the Blueprint Permission File Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **2** (User Profile Configuration Reports).
3) Press **Enter**.

Note: The **User Profile Configuration Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **2** (Blueprint Permission File).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

7.2.4.4. Run Blueprint Parameter File Report

Use this task to display parameters associated with blueprints. For a user profile to be in compliance with a blueprint, the parameter values in the blueprint must match the parameter values in the associated user profile.

To run the Blueprint Parameter File Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **2** (User Profile Configuration Reports).
3) Press **Enter**.

Note: The **User Profile Configuration Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **3** (Blueprint Parameter File).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

7.2.4.5. Run Blueprint Object Authority File Report

Use this task to display object authorities associated with blueprints.

To run the Blueprint Object Authority File Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **2** (User Profile Configuration Reports).
3) Press **Enter**.

Note: The **User Profile Configuration Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **4** (Blueprint Object Authority File).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

7.2.4.6. Run Blueprint Authority List Settings Report

Use this task to display authority list associated with blueprints.

To run the Blueprint Authority List Settings Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **2** (User Profile Configuration Reports).
3) Press **Enter**.

Note: The **User Profile Configuration Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **5** (Blueprint Authority List Settings).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

7.2.4.7. Run Blueprint Non-Compliance User Profiles Report

Use this task to display list of user profiles that are not compliant with blueprints.

To run the Blueprint Non-Compliance User Profiles Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **2** (User Profile Configuration Reports).
3) Press **Enter**.

Note: The **User Profile Configuration Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **6** (Blueprint Non-Compliance User Profiles).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

7.2.4.8. Run Blueprint 3rd Party Integration File Report

Use this task to display 3rd party scripts associated with blueprints.

To run the Blueprint 3rd Party Integration File Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **2** (User Profile Configuration Reports).
3) Press **Enter**.

Note: The **User Profile Configuration Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **7** (Blueprint 3rd Party Integration File).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

7.2.4.9. Run Blueprint Master Change Report

Use this task to display changes made to the blueprint master.

Tip: You must enable auditing to produce change reports. See Enable Profile Auditing for additional information.

To run the Blueprint Master Change Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **3** (User Profile Change Reports).
3) Press **Enter**.

Note: The **User Profile Change Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **1** (Blueprint Master Changes).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

7.2.4.10. Run Blueprint Permission File Change Report

Use this task to display changes made to blueprint permissions. Permissions determine who can use a blueprint to create or modify user profiles.

To run the Blueprint Permission File Change Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **3** (User Profile Change Reports).
3) Press **Enter**.

Note: The **User Profile Change Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **2** (Blueprint Permission File Changes).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

7.2.4.11. Run Blueprint Parameter File Change Report

Use this task to display changes made to blueprint parameters.

To run the Blueprint Parameter File Change Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **3** (User Profile Change Reports).
3) Press **Enter**.

Note: The **User Profile Change Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **3** (Blueprint Parameter File Changes).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

7.2.4.12. Run Blueprint Object Authority File Change Report

Use this task to display changes made to blueprint object authorities.

To run the Blueprint Object Authority File Change Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **3** (User Profile Change Reports).
3) Press **Enter**.

Note: The **User Profile Change Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **4** (Blueprint Object Authority File Changes).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

7.2.4.13. Run Blueprint Authority List Settings Change Report

Use this task to display changes made to blueprint authority lists.

To run the Blueprint Authority List Settings Change Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **3** (User Profile Change Reports).
3) Press **Enter**.

Note: The **User Profile Change Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **5** (Blueprint Authority List Settings Changes).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

7.2.4.14. Run Blueprint Non-Compliance User Profiles Change Report

Use this task to display changes made to non-compliant user profiles.

To run the Blueprint Non-Compliance User Profiles Change Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **3** (User Profile Change Reports).
3) Press **Enter**.

Note: The **User Profile Change Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **6** (Blueprint Non-Compliance User Profiles Changes).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

7.2.4.15. Run Blueprint 3rd Party Integration File Change Report

Use this task to display changes made to 3rd party scripts.

To run the 3rd Party Integration File Change Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **3** (User Profile Change Reports).
3) Press **Enter**.

Note: The **User Profile Change Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **7** (Blueprint 3rd Party Integration File Changes).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

See also

Working with Blueprints

Working with Reports

Run User Profile Management Default Reports

Run User Exclusion Reports

Run Archived Profile Reports

Run Inactive Profile Reports

Run User Profile Reports

7.3. User Exclusions

7.3.1. Working with User Exclusions

This section describes working with user exclusions.

In order to work with user exclusions, you must access the **Work with User Exclusions** interface.

To access the Work with User Exclusions interface

1) Log into to TGSecure.

Note: The **Main** menu appears.

2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.

Note: The **User Profile Management** interface is displayed.

4) At the **Selection or command** prompt, enter **2** (Work with User Exclusions).
5) Press **Enter**.

Note: The **Work with User Exclusions** interface is displayed.

See also

Log into TGSecure

Display User Exclusions

Manage User Exclusions

Run User Exclusion Reports

7.3.2. Display User Exclusions

Use this task to do the following with user exclusions:

- Display list of user exclusions
- Sort list of user exclusions
- Move to position in list of user exclusions
- Filter list of user exclusions

7.3.2.1. Display List of User Exclusions

Use this task to display the list of available user exclusions.

To display the list of user exclusions

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.

Note: The **User Profile Management** interface is displayed.

4) At the **Selection or command** prompt, enter **2** (Work with User Exclusions).
5) Press **Enter**.

Note: The **Work with User Exclusions** interface is displayed.

Field	Description
User Group	Name of the user group to which exclusions apply
Exclusion Type	Type of exclusion ***ALL** - All types ***ACTIVITY** - Exclude the user group from being checked for inactivity ***SYNC** - Exclude the user group from being synchronized with other iseries systems

7.3.2.2. Sort List of User Exclusions

Use this task to sort the list. The column on which the list is currently sorted appears in white text.

To sort the list

1) Access the **Work with User Exclusion** interface.
2) Place your cursor on the desired column heading.
3) Press the **F10** (Sort) function key.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

7.3.2.3. Move to Position in List of User Exclusions

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

To move to a specific position within the list

1) Access the **Work with User Exclusion** interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.

4) Press **Enter**.

Note: The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

7.3.2.4. Filter List User Exclusions

Use this task to limit the objects displayed in the list by defining a subset for filtering purposes.

Tip: Use wildcard asterisk (*) to help define your subset.

-- Add an asterisk before text (e.g., *report) to find list items that end with specific text.

-- Add an asterisk after text (e.g., report*) to find list items that start with specific text.

-- Add asterisks around text (e.g., *report*) to find list items that contain specific text anywhere in the name.

To filter the list using a subset

1) Access the **Work with User Exclusion** interface.
2) Press the **F8** (Subset) function key.
3) Enter the criteria you want to use to define the subset.
4) Press **Enter**.

Note: The system filters the results based on the criteria you defined for the subset.

See also

Working with User Exclusions

Run User Exclusion Reports

7.3.3. Manage User Exclusions

Use this task to do the following:

- Add exclusion
- Edit exclusion
- Copy exclusion
- Delete exclusion

To manage user exclusions, access the **Work with User Exclusions** interface.

To access the Work with User Exclusions interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.

Note: The **User Profile Management** interface is displayed.

4) At the **Selection or command** prompt, enter **2** (Work with User Exclusions).
5) Press **Enter**.

Note: The **Work with User Exclusions** interface is displayed

7.3.3.1. Add Exclusion

Use this task to create a new user exclusion.

To copy an exclusion

1) Access the **Work with User Exclusions** interface.
2) Press the **F6** (Add) function key on your keyboard.
3) Press **Enter**.

Note: The **Work with User Exclusion - Add** interface is displayed.

3) Complete the following fields.

Field	Description
User Group	Name of the user group to which exclusions apply
Exclusion Type	Type of exclusion ***ALL** - All types ***ACTIVITY** - Exclude the user group from being checked for inactivity ***SYNC** - exclude the user group from being synchronized with other systems (e.g., TGCentral)

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

5) Press **Enter** twice.

7.3.3.2. Edit Exclusion

Use this task to edit an existing user exclusion.

To edit an exclusion

1) Access the **Work with User Exclusions** interface.
2) In the **OPT** column for the desired exclusion, enter **2** (Edit).
3) Press **Enter**.
4) Modify the parameters as necessary.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

5) Press **Enter** twice.

7.3.3.3. Copy Exclusion

Use this task to create a new user exclusion by copying an existing user exclusion.

To copy an exclusion

1) Access the **Work with User Exclusions** interface.
2) In the **OPT** column for the desired exclusion, enter **3** (Copy).
3) Press **Enter**.
4) Modify the parameters as necessary.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

5) Press **Enter** twice.

7.3.3.4. Delete Exclusion

Use this task to delete an exclusion.

To delete an exclusion

1) Access the **Work with User Exclusions** interface.
2) In the **OPT** column for the desired exclusion, enter **4** (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the correct exclusion.
5) Press **Enter** twice.

See also

Working with User Exclusions

Run User Exclusion Reports

7.3.4. Run User Exclusion Reports

Use this task to generate the following user exclusion reports:

Configuration Report

- User Profile Exclusions

Change Report

- User Profile Exclusions Changes

Tip: You can schedule the user exclusion reports (like all other reports) to run when most convenient.

To work with user exclusion reports, access from the **User Profile Reports** interface.

To access the User Profile Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (User Profile Reports).
5) Press **Enter**.

Note: The **User Profile Reports** interface is displayed.

7.3.4.1. Run User Profile Exclusions Report

Use this report to view the list of user profile exclusions.

To run the User Profile Exclusions Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **2** (User Profile Configuration Reports).
3) Press **Enter**.

Note: The **User Profile Configuration Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **8** (User Profile Exclusions).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

7.3.4.2. Run User Profile Exclusions Changes Report

Use this report to view the changes made to user profile exclusions.
Tip: You must enable auditing to produce change reports. See Enable Profile Auditing for additional information.

To run the User Profile Exclusions Changes Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **3** (User Profile Change Reports).
3) Press **Enter**.

Note: The **User Profile Change Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **8** (User Profile Exclusions Changes).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

See also:

Working with User Profile Manager Defaults

Working with Reports

Run User Profile Management Default Reports

Run Blueprint Reports

Run Archived Profile Reports

Run Inactive Profile Reports

Run User Profile Reports

7.4. Archived Profiles

7.4.1. Working with Archived Profiles

This section describes working with archived profiles.

In order to work with archived profiles, you must access the **Work with Archived Profiles** interface.

To access the Work with Archived Profiles interface

1) Log into to TGSecure.

Note: The **Main** menu appears.

2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.

Note: The **User Profile Management** interface is displayed.

4) At the **Selection or command** prompt, enter **3** (Work with Archived Profiles).
5) Press **Enter**.

Note: The **Work User Archived Profiles** is displayed.

See also

Log into TGSecure

Display Archived Profiles

Manage Archived Profiles

Run Archived Profile Reports

7.4.2. Display Archived Profiles

Use this task to do the following with archived profiles:

- Display list of archived profiles
- Sort list of archived profiles
- Move to position in list of archived profiles
- Filter list of archived profiles

7.4.2.1. Display List of Archived Profiles

Use this task to display the list of available archived profiles.

To display the list of archived profiles

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.

Note: The **User Profile Management** interface is displayed.

4) At the **Selection or command** prompt, enter **3** (Work with Archived Profiles).
5) Press **Enter**.

Note: The **Work with Archived Profiles** is displayed.

Field	Description
User Name	Name of user whose profile has met inactivity limits and should therefore be disabled or deleted
Archived Date	Date on which the user profile was archived
User Description	Description of the user
Arch Available	Where archive is available
Archived Library	Name of the archive library
Archived File	Name of the archive file

7.4.2.2. Sort List of Archived Profiles

Use this task to sort the list. The column on which the list is currently sorted appears in white text.

To sort the list

1) Access the **Work with Archived Profiles** interface.
2) Place your cursor on the desired column heading.
3) Press the **F10** (Sort) function key on your keyboard.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

7.4.2.3. Move to Position in List of Archived Profiles

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

To move to a specific position within the list

1) Access the **Work with Archived Profiles** interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.
4) Press **Enter**.

Note: The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

7.4.2.4. Filter List Archived Profiles

Use this task to limit the objects displayed in the list by defining a subset for filtering purposes.

Tip: Use wildcard asterisk (*) to help define your subset.

-- Add an asterisk before text (e.g., *report) to find list items that end with specific text.

-- Add an asterisk after text (e.g., report*) to find list items that start with specific text.

-- Add asterisks around text (e.g., *report*) to find list items that contain specific text anywhere in the name.

To filter the list using a subset

1) Access the **Work with Archived Profiles** interface.
2) Press the **F8** (Subset) function key on your keyboard.
3) Enter the criteria you want to use to define the subset.
4) Press **Enter**.

Note: The system filters the results based on the criteria you defined for the subset.

See also

Working with Archived Profiles

Run Archived Profile Reports

7.4.3. Manage Archived Profiles

Use this task to do the following:

- Reactivate profile
- Delete archived file

To manage archived profiles, access the **Work with Archived Profiles** interface.

To access the Work with Archived Profiles interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.

Note: The **User Profile Management** interface is displayed.

4) At the **Selection or command** prompt, enter **3** (Work with Archived Profiles).
5) Press **Enter**.

Note: The **Work with Archived Profiles** is displayed.

7.4.3.1. Reactivate Profile

Use this task to reactivate a profile.

Note: Profiles are archived (retired from the system and stored in an archive file) once they meet inactivity requirements that are set in the profile settings.

To reactivate a profile

1) Access the **Work with Archived Profiles** interface.
2) In the **OPT** column for the desired profile, enter **6** (Reactivate Profile).
3) Press **Enter**.

7.4.3.2. Delete Archived File

Warning: Before deleting an archive file, ensure you have a back-up of the file.

Use this task to delete an archive file, which contains multiple archived user profiles.

To delete an archive file

1) Access the **Work with Archived Profiles** interface.
2) In the **OPT** column for the desired archive file, enter **9** (Delete Archive File).
3) Press **Enter** twice.

See also

Working with Archived Profiles

7.4.4. Run Archived Profile Reports

Use this task to generate the following archived profile reports:

Configuration Report

- User Profile Archive

Change Report

- User Profile Archive Changes

Tip: You can schedule the archived profile reports (like all other reports) to run when most convenient.

To work with archived profile reports, access from the **User Profile Reports** interface.

To access the User Profile Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (User Profile Reports).
5) Press **Enter**.

Note: The **User Profile Reports** interface is displayed.

7.4.4.1. Run User Profile Archive Report

Use this report to view the list of archived profiles.

To run the User Profile Archive Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **2** (User Profile Configuration Reports).
3) Press **Enter**.

Note: The **User Profile Configuration Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **9** (User Profile Archive).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

7.4.4.2. Run User Profile Archive Changes Report

Use this report to view the list of changes made to archived profiles.
Tip: You must enable auditing to produce change reports. See Enable Profile Auditing for additional information.

To run the User Profile Archive Changes Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **3** (User Profile Change Reports).
3) Press **Enter**.

Note: The **User Profile Change Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **9** (User Profile Archive Changes).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

See also:

Working with Archived Profiles

Working with Reports

Run User Profile Management Default Reports

Run Blueprint Reports

Run User Exclusion Reports

Run Inactive Profile Reports

Run User Profile Reports

7.5. Inactive Profiles

7.5.1. Working with Inactive Profiles

This section describes working inactive profiles.

In order to work with inactive profiles, you must access the **Profile Inactivity Settings** interface.

To access the Profile Inactivity Settings interface

1) Log into to TGSecure.

Note: The **Main** menu appears.

2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.

Note: The **User Profile Management** interface is displayed.

4) At the **Selection or command** prompt, enter **5** (Profile Inactivity Settings).
5) Press **Enter**.

Note: The **Profile Inactivity Settings** interface is displayed.

See also

Log into TGSecure

Display Inactive Profile Settings

Manage Inactive Profiles

Run Inactive Profile Reports

7.5.2. Display Inactive Profile Settings

Use this task to display the inactive profile settings.

To display Inactive profile settings

1) From the TGSecure **Main** menu appears.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.

Note: The **User Profile Management** interface is displayed.

4) At the **Selection or command** prompt, enter **5** (Profile Inactivity Settings).
5) Press **Enter**.

Note: The **Profile Inactivity Settings** interface is displayed.

Field	Description
Inactivity until user profile is disabled	Number of days before an inactive user profile is disabled
Inactivity until user profile is deleted	Number of days before an inactive user profile is deleted
Delete profiles with password of *NONE	Whether to delete profiles that do not have an assigned password ***YES** - Delete the profiles ***NO** - Keep the profiles
Object owner for objects owned by deleted profiles	The name of the user who will inherit ownership of objects for deleted user profiles
Remove deleted profiles from TG user group	Whether to remove deleted profiles from TG user groups ***YES** - Delete the user profile from TG groups ***NO** - Keep the user profile as member of TG groups

Remove deleted profiles from TG rules	Whether to remove deleted profiles from TG rules. ***YES** - Delete the user profile from rule definition ***NO** - Keep the user profile as part of rule definition
Alert when inactivity found	Whether to send an alert to the admin when inactive profiles are detected ***YES** - Enable alerts ***NO** - Disable alerts

See also

Working with Inactive Profiles

Run Inactive Profile Reports

7.5.3. Manage Inactive Profile

Use this task to do the following:

- Edit Inactive Profile Settings
- Display a list of inactive profiles
- Enforce inactive profile rules

To manage Profile Manager defaults, access the **Profile Inactivity Settings** interface.

To access the Profile Inactivity Settings interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.

Note: The **User Profile Management** interface is displayed.

4) At the **Selection or command** prompt, enter **5** (Profile Inactivity Settings).
5) Press **Enter**.

Note: The **Profile Inactivity Settings** interface is displayed.

7.5.3.1. Edit Inactive Profile Settings

To display Inactive profile settings

1) Access the **Profile Inactivity Settings** interface.
2) Modify the necessary parameters:

Field	Description
Inactivity until user profile is disabled	Number of days before an inactive user profile is flagged as needing to be disabled
Inactivity until user profile is deleted	Number of days before an inactive user profile is flagged as needing to be deleted
Delete profiles with password of *NONE	Whether to delete profiles with the password value of *NONE

	***YES** - Delete the profiles ***NO** - Keep the profiles
Object owner for objects owned by deleted profiles	The name of the user who will inherit ownership of objects from deleted or disabled user profiles **Note**: All objects must be assigned an owner.
Remove deleted profiles from TG user group	Whether to remove deleted profiles from TG user groups ***YES** - Delete the user profile from TG groups ***NO** - Keep the user profile as member of TG groups
Remove deleted profiles from TG rules	Whether to remove rules that are no longer associated with a user because the user profile for which the rule was defined is no longer present in the system ***YES** - Delete the rule ***NO** - Keep the rule
Alert when inactivity found	Whether to send an alert to the admin when inactive profiles are detected ***YES** - Enable alerts ***NO** - Disable alerts

3) Press **Enter** twice.

7.5.3.2. Display the List of Inactive Profiles

Use this task display the list of user profiles that the system (based on the inactive profile settings) has deemed as inactive.

To display the list of inactive user profiles

1) Access the **Profile Inactivity Settings** interface.

2) Press the **F22** (Run Inactive Report) function key on your keyboard.

Tip: For function keys higher than **F12**, you must use a combination of the **Shift** key and the appropriate function key. For example, to select **F24**, you must hold down the **Shift** key and **F12**.

3) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

4) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

7.5.3.3. Enforce Inactive Profile Rules

Use this task to enforce the inactive profile rules.

Note: Whether a profile is disabled or deleted during enforcement is based on the inactive profile settings.

To enforce profile inactivity rules

1) Access the **Profile Inactivity Settings** interface.

2) Press the **F23** (Run Inactivity Enforcement) function key on your keyboard.

Tip: For function keys higher than **F12**, you must use a combination of the **Shift** key and the appropriate function key. For example, to select **F23**, you must hold down the **Shift** key and **F11**.

3) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

4) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

See also

Working with Inactive Profiles

Display Inactive Profiles Settings

Run Inactive Profile Reports

Run Reports

7.5.4. Run Inactive Profile Reports

Use this task to generate the following inactive profile report.

Usage Report

- Inactivity Compliance Report

Configuration Report

- Profile Inactivity Settings

Change Report

- Profile Inactivity Settings Changes

Tip: You can schedule the Archived Profile reports (like all other reports) to run when most convenient.

To work with Archived Profile reports, access from the **User Profile Reports** interface.

To access the User Profile Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (User Profile Reports).
5) Press **Enter**.

Note: The **User Profile Reports** interface is displayed.

7.5.4.1. Run Inactivity Compliance Report

Use this report to display the list of inactive profiles.

To run the Inactivity Compliance Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **1** (User Profile Usage Reports).
3) Press **Enter**.

Note: The **User Profile Usage Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **2** (Inactivity Compliance Report).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

7.5.4.2. Run Profile Inactivity Settings Report

Use this report to view the list of profile inactivity settings.

To run the Profile Inactivity Settings Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **2** (User Profile Configuration Reports).
3) Press **Enter**.

Note: The **User Profile Configuration Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **10** (Profile Inactivity Settings).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

7.5.4.3. Run Profile Inactivity Settings Changes Report

Use this report to view the list of changes made to the profile inactivity settings.
Tip: You must enable auditing to produce change reports. See Enable Profile Auditing for additional information.

To run the Profile Inactivity Settings Changes Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **3** (User Profile Change Reports).
3) Press **Enter**.

Note: The **User Profile Change Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **10** (Profile Inactivity Settings Changes).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

See also:

Working with User Profile Manager Defaults

Working with Reports

Run User Profile Management Default Reports

Run Blueprint Reports

Run User Exclusion Reports

Run Archived Profile Reports

Run User Profile Reports

7.6. User Profiles

7.6.1. Working with User Profiles

This section describes working with user profiles.

In order to work with user profiles, you must access the **TG User Profile Manager** interface.

To access the TG User Profile Manager interface

1) Log into to TGSecure.

Note: The **Main** menu appears.

2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.

Note: The **User Profile Management** interface is displayed.

4) At the **Selection or command** prompt, enter **4** (Create/Change User Profile - TGUSRMGR).
5) Press **Enter**.

Note: The **TG User Profile Manager** interface is displayed.

See also

Log into TGSecure

Manage User Profiles

Run User Profile Reports

7.6.2. Manage User Profiles

Use this task to do the following:

- Create user profile based on a blueprint
- Change user profile based on a blueprint

To manage user profiles using blueprints, access the **TG User Profile Manager** interface.

To access the TG User Profile Manager interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.

Note: The **User Profile Management** interface is displayed.

4) At the **Selection or command** prompt, enter **4** (Create/Change User Profile - Blueprint).
5) Press **Enter**.

Note: The **TG User Profile Manager** interface is displayed.

7.6.2.1. Create User Profile Based on a Blueprint

Use this task to create a user profile based on a blueprint.
Tip: Ensure you have permission to use the blueprint to create profiles before attempting this task.

To create a user profile based on a blueprint

1) Access the **TG User Profile Manager** interface.
2) In the **Action type** field, enter ***CRT**.
3) Press Enter.
4) Complete the following fields:

Field	Description
Blueprint ID	Name of the blueprint on which to base the user profile
User Name	Name of the user
User Description	Description of the user
Add to Blueprint user group	Whether to add the user to the user group associated with the named blueprint ***YES** - Add the user to the blueprint user group ***NO** - Based the user profile on the blueprint only, but do not add the user to the blueprint user group

5) Press **Enter**.

7.6.2.2. Change User Profile Based on a Blueprint

Use this task to change a user profile based on a blueprint.
Tip: Ensure you have permission to use the blueprint to change profiles before attempting this task.

To change a user profile based on a blueprint

1) Access the **TG User Profile Manager** interface.
2) In the **Action type** field, enter ***CHG**.
3) Press **Enter**.
4) Complete the following fields:

Field	Description
Blueprint ID	Name of the blueprint on which to base the user profile
User Name	Name of the user
User Description	Description of the user
Add to Blueprint user group	Whether to add the user to the user group associated with the named blueprint ***YES** - Add the user to the blueprint user group ***NO** - Based the user profile on the blueprint only, but do not add the user to the blueprint user group

5) Press **Enter**.

See also

Working with User Profiles

Working with Blueprints

7.6.3. Run User Profile Reports

Use this task to run the following reports:

Usage Reports

- User Profile Create/Change via Blueprint
- User Profile Activity
- User Profile Changes
- Invalid Sign-on Attempts
- Run Authority Failures For User

Tip: You can schedule the user profile reports (like all other reports) to run when most convenient.

To work with user profile reports, access from the **User Profile Reports** interface.

To access the User Profile Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (User Profile Reports).
5) Press **Enter**.

Note: The **User Profile Reports** interface is displayed.

7.6.3.1. Run User Profile Create/Change via Blueprint

Use this report to view the profiles either created or changed using the profile manager feature.

To run the User Profile Create/Change via Blueprint Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **1** (User Profile Usage Reports).
3) Press **Enter**.

Note: The **User Profile Usage Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **3** (User Profile Create/Change via Blueprint).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

7.6.3.2. Run User Profile Activity Report

Use this report to view modifications made to user profiles. The information is presented in two-row partners. The first row shows the previous state and the second row shows the change state.

Tip: This report has numerous columns. If you are interested in only a subset of user profile parameters, consider creating a custom report based on this built in report.

To run the User Profile Activity Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **1** (User Profile Usage Reports).
3) Press **Enter**.

Note: The **User Profile Usage Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **4** (User Profile Activity).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

7.6.3.3. Run User Profile Changes Report

Use this report to view who has modified user profiles and what they have changed.

Tip: You must enable auditing to produce change reports. See Enable Profile Auditing for additional information.

To run the User Profile Change Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **1** (User Profile Usage Reports).
3) Press **Enter**.

Note: The **User Profile Usage Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **6** (User Profile Changes).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

7.6.3.4. Run Invalid Sign-on Attempts Report

Use this report to view the list of unsuccessful sign-on attempts.

To run the Invalid Sign-on Attempts Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **1** (User Profile Usage Reports).
3) Press **Enter**.

Note: The **User Profile Usage Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **5** (Invalid Sign-on Attempts).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

7.6.3.5. Run Authority Failures For User Report

Use this report to view job failures due to inadequate user authorities.

To run the Invalid Sign-on Attempts Report

1) Access the **User Profile Reports** interface.
2) At the **Selection or command** prompt, enter **1** (User Profile Usage Reports).
3) Press **Enter**.

Note: The **User Profile Usage Reports** interface is displayed.

4) At the **Selection or command** prompt, enter **7** (Authority Failures For User).
5) Press **Enter**.
6) Modify the report run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

See also:

Working with User Profiles

Working with Reports

Run User Profile Management Default Reports

Run Blueprint Reports

Run User Exclusion Reports

Run Archived Profile Reports

Run Inactive Profile Reports

7.7. Password Rules

7.7.1. Working with Password Rules

This section describes working password rules.

In order to work with inactive profiles, you must access the **Password Rule Settings** interface.

To access the Password Rules Settings interface

1) Log into to TGSecure.

Note: The **Main** menu appears.

2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.

Note: The **User Profile Management** interface is displayed.

4) At the **Selection or command** prompt, enter **6** (Password Rule Settings).
5) Press **Enter**.

Note: The **Password Rules Settings** interface is displayed.

See also

Log into TGSecure

Manage Password Rules

7.7.2. Manage Password Rules

Use this task to do the following:

- Add password exit program
- Remove password exit program
- Edit password rules

To manage password rules, access the **Password Rules Setting** interface.

To access the Work with Archived Profiles interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **5** (User Profile Management).
3) Press **Enter**.

Note: The **User Profile Management** interface is displayed.

4) At the **Selection or command** prompt, enter **6** (Password Rules Settings).
5) Press **Enter**.

Note: The **Password Rules Setting** is displayed.

7.7.2.1. Add Password Exit Program

Use this task to add (install) the password exit program.

Note: Before using the Profile Manager to modify password rules, you must install the password exit program.

To add password exit programs

1) Access the **Password Rule Settings** interface.

2) Press the **F20** (Add Password Exits) function key on your keyboard.

Tip: For function keys higher than **F12**, you must use a combination of the **Shift** key and the appropriate function key. For example, to select **F20**, you must hold down the **Shift** key and **F8**.

7.7.2.2. Remove Password Exit Program

Use this task to remove the password exit program.

To remove password exit programs

1) Access the **Password Rule Settings** interface.

2) Press the **F21** (Remove Password Exits) function key on your keyboard.

Tip: For function keys higher than **F12**, you must use a combination of the **Shift** key and the appropriate function key. For example, to select **F21**, you must hold down the **Shift** key and **F9**.

7.7.2.3. Edit Password Rules

Use this task to edit password rules.

Tip: Changes made in this interface will not impact password rules unless the password exit program is installed.

Note: IBM provides documentation for all password rule parameters. To access the IBM documentation, enter the following at the **Selection or command** prompt:

WRKSYSVAL SYSVAL(QPWDRULES) and then press F1 (Help).

To edit password rules

1) Access the **Password Rules Setting** interface.
2) Complete the following fields:

Field	Description
Current password level (QPWDLVL)	Enter the desired password level
Password rule value set to *PWDSYSVAL	Whether to use default system values or custom rules ***YES** - Use default password system values ***NO** - Allow the admin to customize password rules **Tip**: This value must be set to ***NO** if you want to use the profile manager feature to update password rules.
Number of Mixed case letters (*MIXCASEn)	[**0-9**] - Number of mix-case letters required in the password
Limit Repeat Characters (*CHRLMTREP)	Whether a password to contain characters that repeat (appears next to each other) **Y** - Disallow consecutive use of characters **N** - Allow consecutive use of characters
Limit Same Character (*LMTSAMPOS)	Whether characters can be used in the same position as the previous password **Y** - Disallow characters in same position **N** - Allow characters in the same position
Require Upper/Lower/Digits/Special Char (*REQANY3)	Whether a password is required to contain the following types of characters: uppercase, lowercase, special characters or digits **Y** - Require character variation **N** - Do not require character variation
Limit Profile Name (*LMTPRFNAME)	Whether password can contain the user's profile name. **Y** - Disallow user's profile name in password **N** - Allow user's profile name in password
Password cannot be same as last	[**0-32**] - Number of times before a password can be repeated
Block password change (Hours)	[**1-99**] - Number of hours allowed between password changes **Note**: Enter ***NONE** to ignore this rule.
Password expiration interval (Days)	[**1-366**] - Number of days a password is valid **Note**: Enter ***NOMAX** to ignore this rule.

Password expiration warning (Days)	[**1-99**] - Number of days before a password expiration warning is issued to user
Limit Adjacent	Whether to allow adjacent elements: **Y** - Disallow adjacent characters, digits, or special Characters **N** - Allow adjacent characters, digits, or special Characters
Limit First Char	Whether to place limits on the first character **Y** - Disallow password to start with a character, digit, or special character **N** - Allow password to start with a character, digit, or special character
Limit Last Char	Whether to place limits on the last character **Y** - Disallow password to end with a character, digit, or special character **N** - Allow password to end with a character, digit, or special character
Maximum	[**0-9**] - Maximum number of characters, digits, or special characters allowed in the password
Minimum	[**0-9**] - Minimum number of characters, digits, or special characters allowed in the password (0-9)

3) Press the **F8** (Save Settings) function key on your keyboard.

See also

Working with Password Rules

8. Reports

8.1. Working with Reports

This section describes working with built-in reports:

- Display list of reports
- Run reports

Note: See the Report Reference Guide for details about a specific report.

To work with built-in reports, access the **Work with Reports** interface.

To access the Work with Reports interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**.

See also

Reports

8.2. Display List of Reports

Use this task to do the following:

- Display the list
- Sort the list
- Move to a specific location within the list
- Filter the list

8.2.1. Display list

Use this task to display the list of available reports.

To display the list of reports

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**.

Note: The **Work with Reports** interface is displayed.

8.2.2. Sort List

Use this task to sort the list of available reports. The column on which the list is currently sorted appears in white text. For example, by default, the list is originally sorted by the **Collector ID** column so that column heading initially appears in white text.

To sort the list

1) Access the **Work with Reports** interface.
2) Place your cursor on a column heading (e.g., Collector ID, Report Name, or Category).
3) Press the **F10** (Sort) function key.

Tip: The system sorts the list of reports in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

8.2.3. Move to Location in List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down to locate a report.

To move to a specific position within the list

1) Access the **Work with Reports** interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.
4) Press **Enter**.

Note: The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

8.2.4. Filter List

Use this task to limit the reports displayed in the list by defining a subset for filtering purposes.

To filter the list using a subset

1) Access the **Work with Reports** interface.
2) Press the **F8** (Subset) function key.
3) Enter the criteria you want to use to define the subset.
4) Press **Enter**.

Note: The system filters the results based on the criteria you defined for the subset.

See also

Working with Reports

Working with Report Outputs

8.3. Run Reports

Use this task to run a built-in or custom report using the **Work with Reports** interface:

Note: See the **TG Audit Report Reference Guide** for information about individual reports.

- Run reports with start and end time requirements
- Run reports without start and end timer requirements

Tip: You can schedule reports to run when most convenient.

8.3.1. Run Reports with Start and End Time Requirements

Use these instructions when the report requires a start and end time entries.

Identifying a start and end time helps you filter the data reported and is required for some types of reports that have the potential to contain a huge amount of data.

To run a report with start and end time requirements

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**.
4) Enter **7** in the **Opt** column for the report you want to run.
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

Field	Description
Collector ID	ID identifying the collector from which report data is obtained (not an editable field)
Collector Name	Name assigned to the collector (not an editable field)
Report ID	ID assigned to the report you want to run (not an editable field)
User profile	Name of the user or group for which you want to report data **Tip**: Enter ***ALL** to include all users
Starting date	Select from the options available: ***CUR** - Use the current date ***CMS** - Use the current month's start date ***LMS** - Use the last month's start date ***LME** - Use the last month end date ***LYS** - Use the last year's start date ***LYE** - Use the last year's end date ***LWS** - Use the last week's start date (last 7 days) ***LDS** - Use the last day's start date
Starting time	Enter time in the format (hhmmss): hour, minute, second
Ending date	Select from the options available
Ending time	Enter time in the format (hhmmss): hour, minute, second
Override report defaults?	Whether to override report defaults: ***YES** - Ignore run-time collector defaults ***NO** - Apply Run-time collector defaults
Reload collector data	Whether to reload the collector data: ***AI** - Allow the artificial intelligence engine to determine if data source collection should be re-run ***YES** - Re-run data source collection before producing the report output

	***NO** - Used cached version of data source collection
Report output type	Enter the desired report output format (*HTML, *PRINT, etc.)
Run interactively?	Whether to run interactively or add to batch: ***YES** - Run the report immediately ***NO** - Add the report to a batch job to be run when most efficient for the system.

8.3.2. Run Reports without Start and End Time Requirements

Use these instructions when the report does not require a start and end time.

To run a report without start and end time requirements

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**.
4) Enter **7** in the **Opt** column for the report you want to run.
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

Field	Description
Collector ID	ID identifying the collector (not an editable field)
Collector	Name assigned to the collector (not an editable field)
Report ID	ID assigned to the report you want to run (must be a report associated with the collector) **Note**: Multiple reports can be produced from a single collector, so at this point you could change the report ID to any of the reports linked to the identified collector.
Override report defaults	Whether to override report defaults: ***YES** - Ignore run-time collector defaults ***NO** - Apply Run-time collector defaults **Tip**: Run-time collector defaults maximize report efficiency. Collector defaults allow you to filter collector data before attempting to generate your report. See Create Reports for additional information about setting up run-time collector defaults.
Reload collector data	Whether to reload the collector data: ***AI** - Allow the artificial intelligence engine to determine if data source collection should be re-run ***YES** - Re-run data source collection before producing the report output ***NO** - Used cached version of data source collection
Report output type	Enter the desired report output format (*HTML, *PRINT, etc.)
Run interactively?	Whether to run interactively or add to batch: ***YES** - Run the report immediately

	***NO** - Add the report to a batch job to be run when most efficient for the system.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

See also

Working with Reports

Working with Report Outputs

8.4. Create Reports

Use this task to create a custom report. Creating a report is a multi-step process:

Step 1 - Add report

Step 1 - Select source from which to collect report data

Step 2 - Name the report

Step 3 - Select the columns you want to include in the report

Step 4 - Define the filter criteria

Step 5 - Define the run-time collector defaults

Step 6 - Confirm the report details

To create reports, access the **Work with Reports** interface.

To access the Work with Reports interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**.

8.4.1. Add Report

To add a Report

1) Access the **Work with Reports** interface.
2) Press the **F6** (Add Report) function key on your keyboard.
3) Follow the steps in the report wizard.

8.4.2. Select Data Source Collector

Use this task to select the data source collector for your custom report. Each report must have a least one source (collector) from which to pull data.

To select the data source collector

1) In the **Opt** column for the collector that you want to use as the data source for your report, enter **1** (Select).
2) Press **Enter**.

8.4.3. Name the Report

Use this task to assign a name, ID, and category to your custom report.

To identify the report

1) Complete the following fields:

Field	Description
Report ID	ID you want to assign to the report **Tip**: The name cannot contain spaces.
Report Name	Name you want to assign the report **Tip**: Use a name that describes the data that will appear in the report.
Category	The report category under which you want to group the report **Tip**: There are four standard categories: Configuration, Resources, Profiles, Network.

2) Press **Enter**.

Note: The report should now be linked to the collector and appear in your list of available reports under the identified category.

8.4.4. Select Report Fields

Use this task to select the collector fields that you want to appear as columns in your report.

Note: By default, all collector fields are selected when you create a custom report.

Tip: To customize which collector fields to include, press the **F4** (Select Fields) function key on your keyboard.

To select report fields

1) Press the **F4** (Select Fields) function key on your keyboard.
2) Enter **1** in the **Sel** column for each field you want to include as a column in your custom report.
3) Press **Enter**.

Figure: Select Report Fields

8.4.5. Change Order of Fields

To change the order of the selected fields

Use this task to define the order in which fields should appear in the report.

Tip: The column with the lowest sequence number appears as the first column. The column with the highest sequence number appears as the last column.

1) Adjust the sequence numbers in the **Seq** column.
2) Press **Enter**.

8.4.6. Define Report Filter Criteria

Use this task to define the filter criteria for your custom report.

Note: Filters are not necessary but might improve the performance of your report.

To build report filter criteria

1) Press the **F4** (Select Fields) function key on your keyboard.
2) Enter **1** in the **Sel** column for each field to which you want to apply a filter.
3) Press **Enter**.

To add filter criteria

1) Add operators and comparison values as necessary.
2) Press **Enter**.

Tip: An SQL-like format is used to create report filters. For a list of supported operators, press **F10**.

Note: You can use up to five levels of nesting. To begin a nested condition, enter an open parenthesis "(" in the **Nest Str** column. Likewise, to end a nested condition, enter a closing parenthesis ")" in the **Nest End** column.

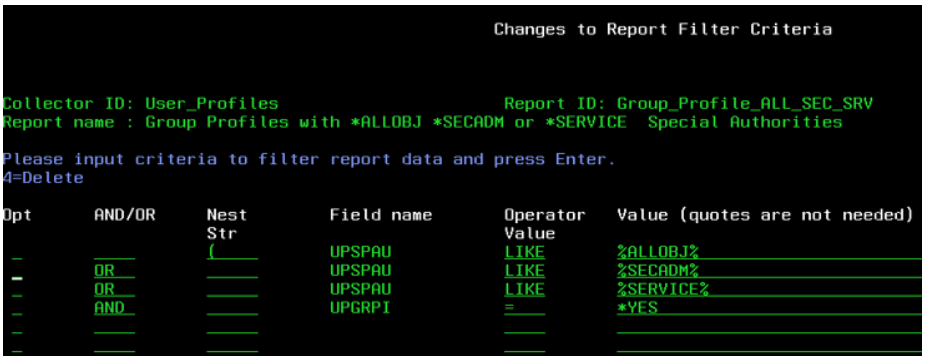


Figure: Build Report Filter Criteria

To delete filter criteria

1) Enter **4** (Delete) in the **Opt** column for the filter criteria you want to delete.
2) Press **Enter**.

8.4.7. Define Run-time Collector Defaults

Use this task to customize the defaults for the data source collection. This enables you to maximize how efficiently the report runs. Report defaults provide options specific to the data source collector on which the report is based, so you can filter the actual data source before the report filter is even applied.

An example of when report defaults are very useful is in the case of reports based on QAUDJRN journal data or database file journal data, where very large amounts of data can potentially accumulate and take a long time to process in a typical reporting scheme. With report defaults, you can specify particular date ranges so that any report filters are only run across a subset of data instead of the entire range of available data.

Report defaults are processed before any report run-time options, except when a user selects ***YES** in the **Override report defaults** field at the time they run a report.

(See Run Reports for additional information about the **Override report defaults** field.)

Tip: Collector defaults are highly recommended, but they are not required. Click the **F2** function key to skip this step.

To define report defaults

1) Enter the desired run-time collector default values.
2) Press **Enter**.

8.4.8. Confirm Report Creation

Use this task to confirm that you want to create the report that you have just defined.

Tip: Click the **F12** function key to go back one step at a time if you want to make changes or verify that you entered the correct information.

To confirm report creation

1) Review the information.
2) Press **Enter**.

See also

Working with Custom Reports

8.5. Manage Reports

Use this task to do the following:

- Edit reports
- Copy reports
- Delete reports
- Enabling report alerting

To manage reports, access the **Work with Reports** interface.

8.5.1. Access the Work with Reports Interface

To access the Work with Reports interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**.

Note: The **Work with Reports Interface** is displayed.

Alternatively, at the IBM i command line, enter **TGWRKRPT**, and press **Enter**.

8.5.2. Edit Report

Use this task to edit a custom report.

Tip: You cannot edit built-in reports, but you can create a copy of a built-in report and then edit the copy.

Important: The **Report ID** cannot be edited after the report is created.

To edit a report

1) Access the **Work with Reports** interface.
2) Enter the appropriate option in the **Opt** column for the report you want to modify:

Option	Description
2 (Edit)	Modify the report name, category, and regulation details **Note**: Only available for custom reports, not built-in reports (those shipped with the product)
5 (Alerts)	Modify the condition (number of rows returned) that trigger the generation of an alert
6 (Defaults)	Modify the run-time collector defaults, which help to filter collector data **Note**: See Create Reports for additional information about run-time collector defaults.
8 (Field List)	Modify which collector fields you want to display in your report **Note**: Modifications cannot be made to built-in reports
9 (Filter)	Modify the filters you want applied to the data obtained from the collector **Note**: Modifications cannot be made to built-in reports

8.5.3. Copy Report

Use this task to copy a report. This is useful when an existing report provides results that are close to what you need, but still do not quite meet your requirements. You can save time by copying the report and customizing it instead of beginning from scratch.

To copy a report

1) Access the **Work with Reports** interface.
2) In the **Opt** column for the report you want to copy, enter **3** (Copy).
3) Enter a unique Report ID and continue customization as desired. Please refer to "Creating Reports" for details.

8.5.4. Delete Report

Use this task to delete a report.

Note: You can delete only customer reports, not built-in reports.

To delete a report

1) Access the **Work with Reports** interface.
2) In the **Opt** column for the report you want to delete, enter **4** (Delete).

8.5.5. Enabling Report Alerting

Use this task to enable alerting based on the results (number of rows) produced in a given report. This is useful if you want the system to send a notification when the number of rows in a report exceeds a threshold.

Tip: You can set up alerts for both built-in and custom reports.

To enable report alerting

1) Access the **Work with Reports** interface.
2) In the **Opt** column for the desired report, enter **5** (Alerts).
3) Complete the following fields:

Field	Description
Alert Status	Enter ***YES** to enable alerts for this specific report (local setting)
Alert Criteria (Condition)	Enter the desired mathematical symbol (<, >, =, etc.)
Alert Criteria (No. of Rows)	Enter the number of rows used in conjunction with mathematical symbol to determine the threshold used to trigger an alert (e.g., if the number of rows is > 10, then trigger an alert). **Note**: See Set Up Alert Defaults for instructions on defining the action taken when a report triggers an alert.

See also

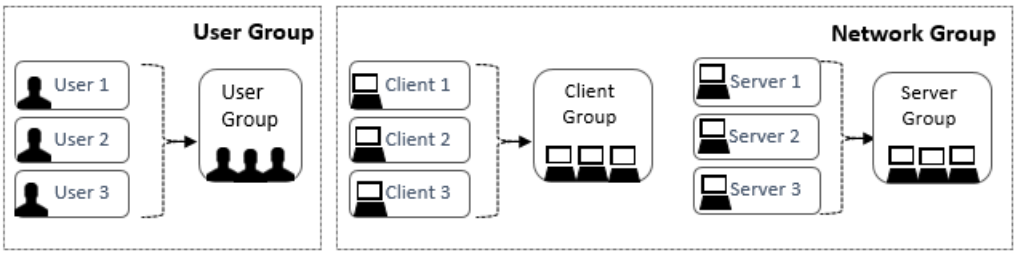
Working with Custom Reports

9. Groups

9.1. Working with Groups

There are several types of groups that you can create.

- User
- Network
- Operation
- Object



To access the Work with Groups interface

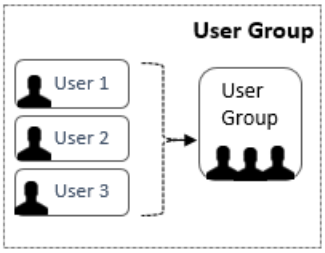
1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**.

Note: The **Work with Groups** interface is displayed.

9.2. Users

9.2.1. Working with User Groups

This section describes what you need to know about user groups.



To work with user groups, you must access the **Work with User Groups** interface.

To access the Work with User Groups interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).

3) Press **Enter**.
4) At the **Selection or command** prompt, enter **1** (Work with User Groups).
5) Press **Enter**.

Note: The **Work with User Groups** interface is displayed.

To access the Work with User Groups interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **10** (Work with User Groups).
3) Press **Enter**.

Note: The **Work with User Groups** interface is displayed.

See also

Display List of User Groups

Display List of Users

Manage User Groups

Manage Users

Run User Groups Report

9.2.2. Display List of User Groups

Use this task to do the following with user groups:

- Display the list of user groups
- Sort the list of user groups
- Move to a specific location within the list of user groups
- Filter the list user groups

9.2.2.1. Display List

Use this task to display the list of user groups.

To display the list of user groups

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **1** (Work with User Groups).
5) Press **Enter**.

Note: The **Work with User Groups** interface is displayed.

To display the list of user groups

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **10** (Work with User Groups).
3) Press **Enter**.

Note: The **Work with User Groups** interface is displayed.

9.2.2.2. Sort List

Use this task to sort the list of available networks. The column on which the list is currently sorted appears in white text. For example, by default, the list is originally sorted by the **Group Name** column so that column heading initially appears in white text.

To sort the list

1) Access the **Work with User Groups** interface.
2) Place your cursor on the desired column heading.
3) Press the **F10** (Sort) function key.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

9.2.2.3. Move to Position in List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

To move to a specific position within the list

1) Access the **Work with User Groups** interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.
4) Press **Enter**.

Note: The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

9.2.2.4. Filter List

Use this task to limit the user groups displayed in the list by defining a subset for filtering purposes.

Tip: Use wildcard asterisk (*) to help define your subset.

-- Add an asterisk before text (e.g., *report) to find list items that end with specific text.

-- Add an asterisk after text (e.g., report*) to find list items that start with specific text.

-- Add asterisks around text (e.g., *report*) to find list items that contain specific text anywhere in the name.

To filter the list using a subset

1) Access the **Work with User Groups** interface.
2) Press the **F8** (Subset) function key.
3) Enter the criteria you want to use to define the subset.
4) Press **Enter**.

Note: The system filters the results based on the criteria you defined for the subset.

See also

Working with User Groups

9.2.3. Display List of Users in a Group

Use this task to do the following with user groups:

- Display the list of users within a group
- Sort the list of users within a group
- Move to a specific location within the list of users

9.2.3.1. Display List

Use this task to display the list of users assigned to a user group.

To display the list of users assigned to a group

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **1** (Work with User Groups).
5) Press **Enter**.
6) In the **OPT** column, enter **10** (Work with Users).
7) Press **Enter**.

Note: The **Work with Users** interface is displayed.

To display the list of users assigned to a group

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **10** (Work with User Groups).
3) Press **Enter**.
4) In the **OPT** column, enter **10** (Work with Users).
5) Press **Enter**.

Note: The **Work with Users** interface is displayed.

9.2.3.2. Sort List

Use this task to sort the list of available users.

To sort the list

1) Access the **Work with Users** interface.
2) Place your cursor on the desired column heading.
3) Press the **F10** (Sort) function key.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

9.2.3.3. Move to Position in List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

To move to a specific position within the list

1) Access the **Work with Users** interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.
4) Press **Enter**.

Note: The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

See also

Working with User Groups

9.2.4. Manage User Groups

Use this task to do the following with user groups:

- Add user groups
- Edit user groups
- Copy user group
- Delete user groups

To manage user groups, access the **Work with User Groups** interface.

To access the Work with User Groups interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **1** (Work with User Groups).
5) Press **Enter**.

Note: The **Work with User Groups** interface is displayed.

9.2.4.1. Add User Group

Use this task to add a user group.

To add user group

1) Access the **Work with User Groups** interface.
2) Press the **F6** (Add) function key.
3) Enter the name (ID) you want to assign to the group.

Tip: Group names must begin with a colon (:) and cannot contain spaces.

4) Enter a description for the group.
5) Press **Enter** twice.

9.2.4.2. Edit User Group

Use this task to edit a user group.

To edit user group

1) Access the **Work with User Groups** interface.

2) In the **OPT** column for the desired group, enter **2** (Edit).
3) Press **Enter**.
4) Modify the description as necessary.

Note: You cannot edit the name.

5) Press **Enter** twice.

9.2.4.3. Copy User Group

Use this task to copy a user group.

To copy user group

1) Access the **Work with User Groups** interface.
2) In the **OPT** column for the desired group, enter **3** (Copy).
3) Press **Enter**.
4) Modify the description as necessary.
5) Press **Enter** twice.

9.2.4.4. Delete User Group

Use this task to delete a user group

To delete user group

1) Access the **Work with User Groups** interface.
2) In the **OPT** column for the desired group, enter **4** (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the correct group.
5) Press **Enter** twice.

See also

Working with User Groups

9.2.5. Manage Users Within a Group

Use this task to do the following with user groups:

- Add users
- Edit users
- Delete users

To manage users, access the **Work with Users** interface.

To access the Work with Users interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **1** (Work with User Groups).
5) Press **Enter**.
6) In the **OPT** column of the user group you want to manage, enter **10** (Work with Users).

7) Press **Enter**.

Note: The **Work with Users** interface is displayed.

9.2.5.1. Add a User

Use this task to add a user.

To add user

1) Access the **Work with Users** interface.
2) Press the **F6** (Add) function key.
3) Enter the name (ID) you want to assign to the user.

Tip: Names cannot contain spaces.

4) Enter a description for the user.
5) Press **Enter** twice.

Note: If the user already exists, you will see a ***YES** in the **Exists on Server** field the first time you press **Enter**. If the user does not exist, you will see ***No** in the **Exists on Server** field the first time you press **Enter**.

9.2.5.2. Edit a User

Use this task to edit a user.

Note: You can only edit the user description, not the user name.

To edit user

1) Access the **Work with Users** interface.
2) In the **OPT** column for the desired user, enter **2** (Edit).
3) Press **Enter**.
4) Modify the user description as necessary.

Note: You cannot edit the user name.

5) Press **Enter** twice.

9.2.5.3. Delete a User

Use this task to delete a user.

To delete user

1) Access the **Work with Users** interface.
2) In the **OPT** column for the desired user, enter **4** (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the correct user.
5) Press **Enter** twice.

See also

Working with User Groups

9.2.6. Run User Groups Report

Use this task to generate reports that display the following for user groups.

- User group configuration details
- User group configuration changes

9.2.6.1. Run User Group Configuration Report

Use this task to display user group configuration details.

To run User Group Configuration Report

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **3** (Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **4** (User Groups Report).
9) Press **Enter**.
10) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

11) Enter the desired output format in the **Report output type** field.
12) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

9.2.6.2. Run User Group Configuration Changes Report

Use this task to display the list of configuration changes made to user groups.

Tip: You must enable auditing to produce change reports. See Enable Access Escalation Change Auditing for additional information.

To run User Group Configuration Changes Report

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **4** (Configuration Changes).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **4** (User Groups Changes Report).
9) Press **Enter**.
10) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

11) Enter the desired output format in the **Report output type** field.
12) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

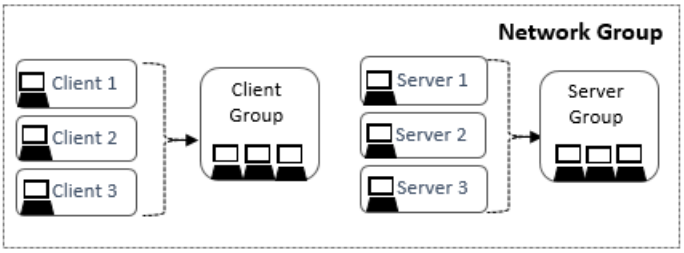
See also

Working with User Groups

9.3. Networks

9.3.1. Working with Networks

This section describes how to work with networks and network groups.



To work with network groups, you must access the **Work with Network/Server Groups** interface.

To access the Work with Network/Server Groups interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **2** (Work with Network/Server Groups).
5) Press **Enter**.

Note: The **Work with Network/Server Groups** interface displays.

See also

Display List of Network/Server Groups

Display List of Networks

Manage Network Groups

Manage Networks

Run Network Groups Report

9.3.2. Display List of Network Groups

Use this task to do the following with network groups:

- Display the list of network groups

- Sort the list of network groups
- Move to a specific location within the list of network groups
- Filter the list of network groups

9.3.2.1. Display List

Use this task to display the list of network groups.

To display the list of network groups

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **2** (Work with Network/Server Groups).
5) Press **Enter**.

Note: The **Work with Network/Server Groups** interface displays.

9.3.2.2. Sort List

Use this task to sort the list. The column on which the list is currently sorted appears in white text. For example, by default, the list is originally sorted by the **Group Name** column so that column heading initially appears in white text.

To sort the list

1) Access the **Work with Network Groups** interface.
2) Place your cursor on the desired column heading.
3) Press the **F10** (Sort) function key.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

9.3.2.3. Move to Position in List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

To move to a specific position within the list

1) Access the **Work with Network Groups** interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.
4) Press **Enter**.

Note: The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

9.3.2.4. Filter List

Use this task to limit the network groups displayed in the list by defining a subset for filtering purposes.

Tip: Use wildcard asterisk (*) to help define your subset.

-- Add an asterisk before text (e.g., *report) to find list items that end with specific text.

-- Add an asterisk after text (e.g., report*) to find list items that start with specific text.

-- Add asterisks around text (e.g., *report*) to find list items that contain specific text anywhere in the name.

To filter the list using a subset

1) Access the **Work with Network Groups** interface.
2) Press the **F8** (Subset) function key.
3) Enter the criteria you want to use to define the subset.
4) Press **Enter**.

Note: The system filters the results based on the criteria you defined for the subset.

See also

Working with Networks

Manage Network Groups

9.3.3. Display List of Networks in a Group

Use this task to do the following with network groups:

- Display the list of networks within a group
- Sort the list of networks within a group
- Move to a specific location within the list of networks

9.3.3.1. Display List

Use this task to display the list of networks assigned to a network group.

To display the list of networks assigned to a group

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **2** (Work with Network/Server Groups).
5) Press **Enter**.
6) In the **OPT** column, enter **10** (Work with Networks).
7) Press **Enter**.

Note: The **Work with Networks** interface is displayed.

9.3.3.2. Sort List

Use this task to sort the list of available networks.

To sort the list

1) Access the **Work with Networks** interface.
2) Place your cursor on the desired column heading.
3) Press the **F10** (Sort) function key.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

9.3.3.3. Move to Position in List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

To move to a specific position within the list

1) Access the **Work with Networks** interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.
4) Press **Enter**.

Note: The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

See also

Working with Networks

Manage Networks within a Group

9.3.4. Manage Network Groups

Use this task to do the following with network groups:

- Add network groups
- Edit networks groups
- Copy network groups
- Delete network groups

To manage network groups, access the **Work with Network Groups** interface.

To access the Work with Network Groups interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **4** (Work with Groups).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **2** (Work with Network/Server Groups).
7) Press **Enter**.

Note: The **Work with Network Groups** interface is displayed.

9.3.4.1. Add Network Group

Use this task to add a network group.

To add network group

1) Access the **Work with Network Groups** interface.
2) Press the **F6** (Add) function key.
3) Enter the name (ID) you want to assign the network group.

Tip: Group names must begin with a colon (:) and cannot contain spaces.

4) Enter a description for the network group.
5) Press **Enter** twice.

9.3.4.2. Edit Network Group

Use this task to edit a network group.

To edit network group

1) Access the **Work with Network Groups** interface.
2) In the **OPT** column for the desired group, enter **2** (Edit).
3) Press **Enter**.
4) Modify the description as necessary.
5) Press **Enter** twice.

9.3.4.3. Copy Network Group

Use this task to copy a network group. This is a fast way to create a new group based on an existing group.

To copy network group

1) Access the **Work with User Groups** interface.
2) In the **OPT** column for the desired group, enter **3** (Copy).
3) Press **Enter**.
4) Enter the name (ID) you want to assign the group.

Tip: Group names must begin with a colon (:) and cannot contain spaces.

5) Enter a description for the group.
6) Press **Enter**.

9.3.4.4. Delete Network Group

Use this task to delete a network group

To delete network group

1) Access the **Work with Network Group** interface.
2) In the **OPT** column for the desired group, enter **4** (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the correct group.
5) Press **Enter** twice.

See also

Working with Networks

9.3.5. Manage Networks Within a Group

Use this task to do the following with network groups:

- Add networks
- Edit networks

- Delete networks

To manage networks, access the **Work with Networks** interface.

To access the Work with Networks interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **2** (Work with Network/Server Groups).
5) Press **Enter**.
6) In the **OPT** column of the network group you want to manage, enter **10** (Work with Networks)
7) Press **Enter**.

Note: The **Work with Networks** interface is displayed.

9.3.5.1. Add Network

Use this task to add a network.

To add network

1) Access the **Work with Networks** interface.
2) Press the **F6** (Add) function key.
3) Enter the name (ID) you want to assign to the network.

Tip: Names cannot contain spaces.

4) Enter a description for the network.
5) Press **Enter** twice.

9.3.5.2. Edit Network

Use this task to edit a network.

To edit network

1) Access the **Work with Networks** interface.
2) In the **OPT** column for the desired network, enter **2** (Edit).
3) Press **Enter**.
4) Modify the network parameters as necessary.

Note: You cannot edit the network name.

5) Press **Enter** twice.

9.3.5.3. Delete Network

Use this task to delete a network.

To delete network

1) Access the **Work with Networks** interface.
2) In the **OPT** column for the desired network, enter **4** (Delete).
3) Press **Enter**.

4) Review the record to ensure you are deleting the correct network.
5) Press **Enter** twice.

See also

Working with Networks

9.3.6. Run Network Groups Report

Use this task to run a report that displays the list of network groups.

- Network group configuration details
- Network group configuration changes

Note: Refer to the TGSecure Report Reference for a complete list of report definitions.

To work with Network Group reports, access the **Network Reports** interface.

9.3.6.1. Access the Network Reports Interface

To access the Network Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.

Note: The **Network Reports** interface is displayed.

9.3.6.2. Run Network Group Configuration Report

Use this task to display user group configuration details.

To run the Network Group Configuration Report

1) Access the **Network Reports** interface.
2) At the **Selection or command** prompt, enter **3** (Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **5** (Network Groups Report).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

9.3.6.3. Run Network Group Configuration Changes Report

Use this task to display the list of configuration changes made to network groups.

Tip: You must enable auditing to produce change reports. See Enable Access Escalation Change Auditing for additional information.

To run the Network Group Configuration Changes Report

1) Access the **Network Reports** interface.
2) At the **Selection or command** prompt, enter **4** (Configuration Changes).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **5** (Network Groups Changes Report).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

See also

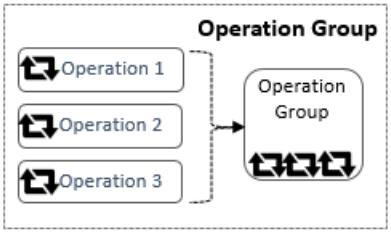
Working with Networks

Working with Reports

9.4. Operations

9.4.1. Working with Operations

This section describes how to work with operations and operation groups.



To work with operations, you must access the **Work with Operation Groups** interface.

To access the Work with Operation Groups interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **3** (Work with Operation Groups).
5) Press **Enter**.

Note: The **Work with Operation Groups** interface displays.

See also

Display List of Operation Groups

Display List of Operations

Manage Operation Groups

Manage Operations

Run Operation Groups Report

9.4.2. Display List of Operation Groups

Use this task to do the following with operation groups:

- Display the list of operations within a group
- Sort the list of operations within a group
- Move to a specific location within the list of operations
- Filter the list of operations within a group

9.4.2.1. Display List

Use this task to display the list of operation groups.

To display the list of operation groups

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **3** (Work with Operation Groups).
5) Press **Enter**.

Note: The **Work with Operation Groups** interface displays.

9.4.2.2. Sort List

Use this task to sort the list. The column on which the list is currently sorted appears in white text. For example, by default, the list is originally sorted by the **Group Name** column so that column heading initially appears in white text.

To sort the list

1) Access the **Work with Operation Groups** interface.
2) Place your cursor on the desired column heading.
3) Press the **F10** (Sort) function key.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

9.4.2.3. Move to Position in List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

To move to a specific position within the list

1) Access the **Work with Operation Groups** interface.

2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.
4) Press **Enter**.

Note: The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

9.4.2.4. Filter List

Use this task to limit the operation groups displayed in the list by defining a subset for filtering purposes.

Tip: Use wildcard asterisk (*) to help define your subset.

-- Add an asterisk before text (e.g., *report) to find list items that end with specific text.

-- Add an asterisk after text (e.g., report*) to find list items that start with specific text.

-- Add asterisks around text (e.g., *report*) to find list items that contain specific text anywhere in the name.

To filter the list using a subset

1) Access the **Work with Operation Groups** interface.
2) Press the **F8** (Subset) function key.
3) Enter the criteria you want to use to define the subset.
4) Press **Enter**.

Note: The system filters the results based on the criteria you defined for the subset.

See also

Working with Operations

Manage Operation Groups

9.4.3. Display List of Operations in a Group

Use this task to do the following with operation groups:

- Display the list of operations within a group
- Sort the list of operations within a group
- Move to a specific location within the list of operations

9.4.3.1. Display List

Use this task to display the list of operations assigned to an operations group.

To display the list of operations assigned to a group

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **3** (Work with Operation Groups).
5) Press **Enter**.
6) In the **OPT** column, enter **10** (Work with Operations).
7) Press **Enter**.

Note: The **Work with Operations** interface is displayed.

9.4.3.2. Sort List

Use this task to sort the list of available operations.

To sort the list

1) Access the **Work with Operations** interface.
2) Place your cursor on the desired column heading.
3) Press the **F10** (Sort) function key.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

9.4.3.3. Move to Position in List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

To move to a specific position within the list

1) Access the **Work with Operations** interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.
4) Press **Enter**.

Note: The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

See also

Working with Operations

Manage Operations within a Group

9.4.4. Manage Operation Groups

Use this task to do the following with operation groups:

- Add operation groups
- Edit operation groups
- Copy operation groups
- Delete operation groups

To manage operation groups, access the **Work with Operation Groups** interface.

To access the Work with Operation Groups interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **4** (Work with Groups).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **3** (Work with Operation Groups).
7) Press **Enter**.

Note: The **Work with Operation Groups** interface is displayed.

9.4.4.1. Add Operation Group

Use this task to add an operation group.

To add operation group

1) Access the **Work with Operation Groups** interface.
2) Press the **F6** (Add) function key.
3) Enter the name (ID) you want to assign the group.

Tip: Group names must begin with a colon (:) and cannot contain spaces.

4) Enter a description for the group.
5) Press **Enter** twice.

9.4.4.2. Edit Operation Group

Use this task to edit an operation group.

To edit operation group

1) Access the **Work with Operation Groups** interface.
2) In the **OPT** column for the desired group, enter **2** (Edit).
3) Press **Enter**.
4) Modify the description as necessary.
5) Press **Enter** twice.

9.4.4.3. Copy Operation Group

Use this task to copy an operation group. This is a fast way to create a new group based on an existing group.

To copy network group

1) Access the **Work with Operation Groups** interface.
2) In the **OPT** column for the desired group, enter **3** (Copy).
3) Press **Enter**.
4) Enter the name (ID) you want to assign the group.

Tip: Group names must begin with a colon (:) and cannot contain spaces.

5) Enter a description for the group.
6) Press **Enter**.

9.4.4.4. Delete Operation Group

Use this task to delete an operation group.

To delete operation group

1) Access the **Work with Operation Groups** interface.
2) In the **OPT** column for the desired group, enter **4** (Delete).
3) Press **Enter**.

4) Review the record to ensure you are deleting the correct group.
5) Press **Enter** twice.

See also

Working with Operations

9.4.5. Manage Operations Within a Group

Use this task to do the following with operation groups:

- Add operations
- Edit operations
- Delete operations

To manage operations, access the **Work with Operations** interface.

To access the Work with Operations interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **3** (Work with Operation Groups).
5) Press **Enter**.
6) In the **OPT** column, enter **10** (Work with Operations).
7) Press **Enter**.

Note: The **Work with Operations** interface is displayed.

9.4.5.1. Add Operation

Use this task to add an operation.

To add operation

1) Access the **Work with Operations** interface.
2) Press the **F6** (Add) function key.
3) Enter the name (ID) you want to assign to the operation.

Tip: Names cannot contain spaces.

4) Enter a description for the operation.
5) Press **Enter** twice.

9.4.5.2. Edit Operation

Use this task to edit an operation.

To edit operation

1) Access the **Work with Operations** interface.
2) In the **OPT** column for the desired operation, enter **2** (Edit).
3) Press **Enter**.
4) Modify the operation parameters as necessary.

Note: You cannot edit the name.

5) Press **Enter** twice.

9.4.5.3. Delete Operation

Use this task to delete an operation.

To delete an operation

1) Access the **Work with Operations** interface.
2) In the **OPT** column for the desired operation, enter **4** (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the correct operation.
5) Press **Enter** twice.

See also

Working with Operations

9.4.6. Run Operation Groups Report

Use this task to run a report that displays the list of operation groups.

- Operation group configuration details
- Operation group configuration changes

Note: Refer to the TGSecure Report Reference for a complete list of report definitions.

To work with Network Group reports, access the **Network Reports** interface.

9.4.6.1. Access the Network Reports Interface

To access the Network Reports interface

1) Access the TGSecure **Main** menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.

Note: The **Network Reports** interface is displayed.

9.4.6.2. Run Operation Groups Configuration Report

Use this task to display operation group configuration details.

To run the Operation Group Configuration Report

1) Access the **Network Reports** interface.
2) At the **Selection or command** prompt, enter **3** (Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **6** (Operation Groups Report).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

9.4.6.3. Run Operation Group Configuration Changes Report

Use this task to display the list of configuration changes made to operation groups.

Tip: You must enable auditing to produce change reports. See Enable Access Escalation Change Auditing for additional information.

To run the Operation Group Configuration Changes Report

1) Access the **Network Reports** interface.
2) At the **Selection or command** prompt, enter **4** (Configuration Changes).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **6** (Operation Groups Changes Report).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

See also

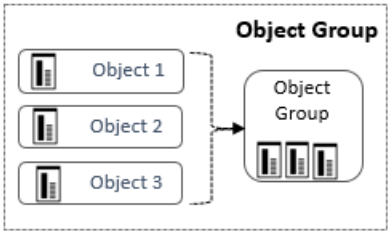
Working with Operations

Working with Reports

9.5. Objects

9.5.1. Working with Objects

This section describes what you need to know about objects and object groups.



To work with object groups, you must access the **Work with Object Groups** interface.

To access the Work with Object Groups interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **4** (Work with Object Groups).
5) Press **Enter**.

Note: The **Work with Object Groups** interface is displayed.

See also

Display List of Object Groups

Display List of Objects

Manage Object Groups

Manage Objects

Run Object Groups Report

9.5.2. Display List of Object Groups

Use this task to do the following with object groups:

- Display the list objects within a group
- Sort the list of objects within a group
- Move to a specific location within the list of objects
- Filter the list of objects within a group

9.5.2.1. Display List

Use this task to display the list of object groups.

To display the list of object groups

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **4** (Work with Object Groups).
5) Press **Enter**.

Note: The **Work with Object Groups** interface is displayed.

9.5.2.2. Sort List

Use this task to sort the list. The column on which the list is currently sorted appears in white text. For example, by default, the list is originally sorted by the **Group Name** column so that column heading initially appears in white text.

To sort the list

1) Access the **Work with Object Groups** interface.
2) Place your cursor on the desired column heading.
3) Press the **F10** (Sort) function key.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

9.5.2.3. Move to a Position in the List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

To move to a specific position within the list

1) Access the **Work with Object Groups** interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.
4) Press **Enter**.

Note: The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

9.5.2.4. Filter List

Use this task to limit the object groups displayed in the list by defining a subset for filtering purposes.

Tip: Use wildcard asterisk (*) to help define your subset.

-- Add an asterisk before text (e.g., *report) to find list items that end with specific text.

-- Add an asterisk after text (e.g., report*) to find list items that start with specific text.

-- Add asterisks around text (e.g., *report*) to find list items that contain specific text anywhere in the name.

To filter the list using a subset

1) Access the **Work with Object Groups** interface.
2) Press the **F8** (Subset) function key.
3) Enter the criteria you want to use to define the subset.
4) Press **Enter**.

Note: The system filters the results based on the criteria you defined for the subset.

See also

Working with Objects

Manage Object Groups

9.5.3. Display a List of Object in a Group

Use this task to do the following with object groups:

- Display the list of objects within a group
- Sort the list of objects within a group
- Move to a specific location within the list of objects

9.5.3.1. Display List

Use this task to display the list of operations assigned to an operations group.

To display the list of operations assigned to a group

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **4** (Work with Object Groups).
5) Press **Enter**.
6) In the **OPT** column, enter **10** (Work with Objects).
7) Press **Enter**.

Note: The **Work with Objects** interface is displayed.

9.5.3.2. Sort List

Use this task to sort the list of available objects.

To sort the list

1) Access the **Work with Objects** interface.
2) Place your cursor on the desired column heading.
3) Press the **F10** (Sort) function key.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

9.5.3.3. Move to Position in List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

To move to a specific position within the list

1) Access the **Work with Objects** interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.
4) Press **Enter**.

Note: The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

See also

Working with Objects

Manage Objects within a Group

9.5.4. Manage Object Groups

Use this task to do the following with object groups:

- Add objects groups
- Edit objects groups
- Copy object groups
- Delete object groups

To manage object groups, access the **Work with Object Groups** interface.

To access the Work with Object Groups interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **4** (Work with Object Groups).
5) Press **Enter**.

Note: The **Work with Object Groups** interface is displayed.

9.5.4.1. Add Object Group

Use this task to add an object group.

To add object group

1) Access the **Work with Object Groups** interface.
2) Press the **F6** (Add) function key.
3) Enter the name (ID) you want to assign the group.

Tip: Group names must begin with a colon (:) and cannot contain spaces.

4) Enter a description for the group.
5) Press **Enter** twice.

9.5.4.2. Edit Object Group

Use this task to edit an object group.

To edit object group

1) Access the **Work with Object Groups** interface.
2) In the **OPT** column for the desired group, enter **2** (Edit).
3) Press **Enter**.
4) Modify the description as necessary.
5) Press **Enter** twice.

9.5.4.3. Copy Object Group

Use this task to copy an object group. This is a fast way to create a new group based on an existing group.

To copy object group

1) Access the **Work with Object Groups** interface.
2) In the **OPT** column for the desired group, enter **3** (Copy).
3) Press **Enter**.
4) Enter the name (ID) you want to assign the group.

Tip: Group names must begin with a colon (:) and cannot contain spaces.

5) Enter a description for the group.
6) Press **Enter**.

9.5.4.4. Delete Object Group

Use this task to delete an object group

To delete object group

1) Access the **Work with Object Groups** interface.
2) In the **OPT** column for the desired group, enter **4** (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the correct group.
5) Press **Enter** twice.

See also

Working with Objects

9.5.5. Manage Objects Within a Group

Use this task to do the following with object groups:

- Add object
- Edit object
- Delete object

To manage objects, access the **Work with Objects** interface.

To access the Work with Objects interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **4** (Work with Object Groups).
5) Press **Enter**.
6) In the **OPT** column, enter **10** (Work with Objects).
7) Press **Enter**.

Note: The **Work with Objects** interface is displayed.

9.5.5.1. Add Object

Use this task to add an object.

To add operation

1) Access the **Work with Objects** interface.
2) Press the **F6** (Add) function key.
3) Enter the name (ID) you want to assign to the object.

Tip: Names cannot contain spaces.

4) Enter a description for the object.
5) Press **Enter** twice.

9.5.5.2. Edit Object

Use this task to edit an object.

To edit object

1) Access the **Work with Objects** interface.
2) In the **OPT** column for the desired object, enter **2** (Edit).
3) Press **Enter**.
4) Modify the object parameters as necessary.

Note: You cannot edit the name.

5) Press **Enter** twice.

9.5.5.3. Delete Object

Use this task to delete an object.

To delete an object

1) Access the **Work with Objects** interface.
2) In the **OPT** column for the desired object, enter **4** (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the correct object.
5) Press **Enter** twice.

See also

Working with Objects

9.5.6. Run Object Groups Report

Use this task to run a report that displays the list of object groups.

- Object group configuration details
- Object group configuration changes

Note: Refer to the TGSecure Report Reference for a complete list of report definitions.

To work with Network Group reports, access the **Network Reports** interface.

9.5.6.1. Access the Network Reports Interface

To access the Network Reports interface

1) Access the **TGSecure Main** menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.

Note: The **Network Reports** interface is displayed.

9.5.6.2. Run Object Group Configuration Report

Use this task to display operation group configuration details.

To run the Object Group Configuration Report

1) Access the **Network Reports** interface.
2) At the **Selection or command** prompt, enter **3** (Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **7** (Object Groups Report).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

9.5.6.3. Run Object Group Configuration Changes Report

Use this task to display the list of configuration changes made to object groups.

Tip: You must enable auditing to produce change reports. See Enable Access Escalation Change Auditing for additional information.

To run the Object Groups Configuration Changes Report

1) Access the **Network Reports** interface.
2) At the **Selection or command** prompt, enter **4** (Configuration Changes).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **7** (Object Groups Changes Report).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.
8) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

See also

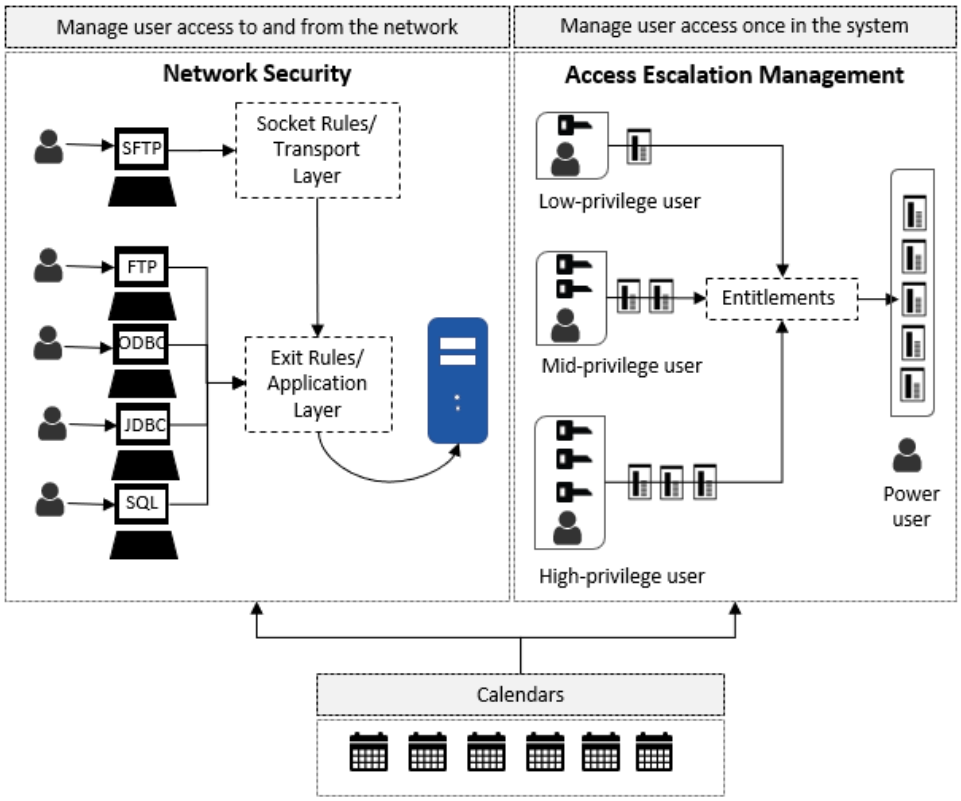
Working with Objects

Working with Reports

10. Calendars

10.1. Working with Calendars

This section describes how to work with calendars. Calendars allow you to enable a rule or entitlement for a specific duration (e.g., after hours, during weekends, on a holiday, etc.).



To work with calendars, you must access the **Work with Calendar Interface**.

To access the Work with Calendar interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **32** (Work with Calendars).
3) Press **Enter**.

Note: The **Work with Calendar** interface is displayed.

See also

Display List of Calendars

Manage Calendars

Manage Day/Time Access

10.2. Display List of Calendars

Use this task to do the following with calendars:

- Display the list of calendars
- Sort the list of calendars
- Move to a specific location within the list of calendars
- Filter the list of calendars

10.2.1. Display List

Use this task to display the list of calendars.

To display the list of calendars

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **32** (Work with Calendars).
3) Press **Enter**.

Note: The **Work with Calendar** interface is displayed.

10.2.2. Sort List

Use this task to sort the list. The column on which the list is currently sorted appears in white text. For example, by default, the list is originally sorted by the **Calendar** column so that column heading initially appears in white text.

To sort the list

1) Access the **Work with Calendar** interface.
2) Place your cursor on the desired column heading.
3) Press the **F10** (Sort) function key.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

10.2.3. Move to a Position in the List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

To move to a specific position within the list

1) Access the **Work with Calendar** interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.
4) Press **Enter**.

Note: The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

10.2.4. Filter List

Use this task to limit the calendars displayed in the list by defining a subset for filtering purposes.

Tip: Use wildcard asterisk (*) to help define your subset.

-- Add an asterisk before text (e.g., *report) to find list items that end with specific text.

-- Add an asterisk after text (e.g., report*) to find list items that start with specific text.

-- Add asterisks around text (e.g., *report*) to find list items that contain specific text anywhere in the name.

To filter the list using a subset

1) Access the **Work with Calendar** interface.
2) Press the **F8** (Subset) function key.
3) Enter the criteria you want to use to define the subset.
4) Press **Enter**.

Note: The system filters the results based on the criteria you defined for the subset.

See also

Working with Calendars

Manage Calendars

10.3. Manage Calendars

Use this task to do the following with calendars:

- Display calendar duration details
- Display calendar day/time access details
- Edit calendar duration details
- Edit calendar day/time access details
- Add calendar
- Copy calendar
- Delete calendar

To manage calendars, access the **Work with Calendar** interface.

To access the Work with Calendar interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **32** (Work with Calendars).
3) Press **Enter**.

Note: The **Work with Calendar** interface is displayed.

10.3.1. Display Calendar Duration Details

Use this task to display the calendar duration details. The duration details identify the period for which a calendar is valid. For example, you could create a calendar to enable a rule or entitlement to be valid only during the month of December in the calendar year 2020.

To display the calendar duration details

1) Access the **Work with Calendar** interface.
2) In the **OPT** column for the desired calendar, enter **5** (Display).
3) Press **Enter**.

4) Review the duration details for the selected calendar.

10.3.2. Display Calendar Day/Time Access Details

Use this task to display the calendar day/time access details. The day/time access details identify the days of the week and specific time for which the calendar is valid. For example, you could create a calendar to enable a rule or entitlement to be valid only on Sundays between 12:00am to 6:00am.

To display the calendar day/time access details

1) Access the **Work with Calendar** interface.
2) In the **OPT** column for the desired calendar, enter **10** (Day/Time Access).
3) Press **Enter**.
4) Review the day/time access details for the selected calendar.

10.3.3. Edit Calendar Duration Details

Use this task to edit the duration of a calendar.

To edit calendar duration

1) Access the **Work with Calendar** interface.
2) In the **OPT** column for the desired calendar, enter **2** (Edit).
3) Press **Enter**.
4) Modify the duration details as necessary.
5) Press **Enter** twice.

10.3.4. Edit Calendar Day/Time Access Details

Use this task to edit the day/time access for a calendar

To edit calendar day/time access

1) Access the **Work with Calendar** interface.
2) In the **OPT** column for the desired group, enter **10** (Day/Time Access).
3) Press **Enter**.
4) In the **OPT** column for the desired day/time access entry, enter **2** (Edit).
5) Modify the day/time access details as necessary.

Tip: You can add a new day/time access entry by pressing the **F6** (Add) function key. For example, your calendar might require two day/time access entries: the first entry for Monday-Friday with a start time of 08:00:00 and an end time of 17:00:00, and the second entry for Saturday only with a start time of 08:00:00 and an end time of 12:00:00.

6) Press **Enter** twice.

See also

Manage Calendar Day/Time Access

10.3.5. Add Calendar

Use this task to add a calendar.

To add calendar

1) Access the **Work with Calendar** interface.
2) Press the **F6** (Add) function key on your keyboard.
3) Enter the parameters necessary to define the duration for which the calendar is valid.

Tip: Press **F1** (Help) to access field descriptions.

Field	Description
Calendar Name	ID used to identify the calendar
Start Date	Start date on which the calendar is valid
Start Time	Start time on which the calendar is valid
End Date	End date on which the calendar becomes invalid
End Time	End time on which the calendar becomes invalid
Description	Short description identifying the purpose of the calendar

4) Press **Enter** twice.
5) Enter the days of the week for which the calendar is valid.

Tip: For example, to limit the application of a rule or entitlement to Monday-Friday, remove the **X** value beside Saturday and Sunday.

6) Enter the start and end time for which the calendar is valid for the selected day(s).

Note: The system applies the start/end time to all selected days. To enter different day/time access combinations, you must edit the calendar once it is saved.

7) Press **Enter**.

See also

Manage Calendar Day/Time Access

10.3.6. Copy Calendar

Use this task to copy a calendar. This is a fast way to create a new calendar based on an existing calendar.

To copy a calendar

1) Access the **Work with Calendar** interface.
2) In the **OPT** column for the desired calendar, enter **3** (Copy).
3) Press **Enter**.
4) Modify the calendar details as necessary.
5) Press **Enter** twice.

10.3.7. Delete Calendar

Use this task to delete a calendar.

To delete calendar

1) Access the **Work with Calendar** interface.

2) In the **OPT** column for the desired calendar, enter **4** (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the correct calendar.
5) Press **Enter** twice.

See also

Working with Calendars

10.4. Manage Calendar Day/Time Access

Use this task to do the following with calendars:

- Display day/time details
- Add day/time details
- Edit day/time requirement
- Copy a day/time requirement
- Delete a day/time requirement

To manage the calendar day/time details, access the **Work with Calendar** interface.

To access the Work with Calendar interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **32** (Work with Calendars).
3) Press **Enter**.

Note: The **Work with Calendar** interface is displayed.

10.4.1. Display Day/Time Details

Use this task to display the details for a specific day/time access requirement.

To display the day/time requirement details

1) Access the **Work with Calendar** interface.
2) In the **OPT** column for the desired calendar, enter **10** (Day/Time Access).
3) Press **Enter**.
4) In the **OPT** column for the desired day/time requirement, enter **5** (Display).

Note: The **Day/Time Access** interface is displayed.

10.4.2. Add Day/Time Requirement

Use this task to add a day/time access requirement.

To add day/time requirement

1) Access the **Day/Time Access** interface.
2) Press the **F6** (Add) function key on your keyboard.
3) Add an **X** beside the day(s) of the week for which you want to add a requirement.
4) Enter a start and time.

Tip: For example, enter 00:00:00 as the start time and 24:00:00 as the end time to indicate 24 hours.

5) Press **Enter** twice.

10.4.3. Edit Day/Time Requirement

Use this task to edit a day/time access requirement.

To edit day/time requirement

1) Access the **Day/Time Access** interface.
2) In the **OPT** column, enter **2** (Edit) for the desired day/time requirement.
3) Press **Enter**.
4) Modify the day/time requirement as necessary.
5) Press **Enter** twice.

10.4.4. Copy Day/Time Requirement

Use this task to copy a day/time access requirement. This is a fast way to create a requirement based on an existing requirement.

To copy day/time requirement

1) Access the **Day/Time Access** interface.
2) In the **OPT** column for the desired requirement, enter **3** (Copy).
3) Press **Enter**.
4) Modify the requirement details as necessary.
5) Press **Enter**.

10.4.5. Delete Day/Time Requirement

Use this task to delete a day/time access requirement.

To delete day/time requirement

1) Access the **Day/Time Access** interface.
2) In the **OPT** column for the desired requirement, enter **4** (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the correct requirement.
5) Press **Enter** twice.

See also

Working with Calendars

11. Save and Restore Configuration

The **Save/Restore TG Configuration** tool allows you to save the configuration of a specific instance of TGSecure or TGAudit. Once you save a configuration, you can then use that saved configuration file to do the following:

- Create a back-up (archive) of the current configuration to be used later to restore the configuration of an agent (server)
- Create multiple instances with identical configuration

Note: A saved file store the configuration for the following:

- Calendars
- Entitlement
- Groups
- Networks
- Reports
- Rules

See also

Manager Configuration

11.1. Manage Configuration

Use the **Save/Restore TG Configuration** feature to do the following:

- Save the configuration definition of a specific agent
- Restore the configuration of an agent
- Copy the configuration of an agent

11.1.1. Save Configuration

Use this task to save the configuration of a specific agent for later restoration or to transfer the configuration to another agent.

Caution: If you have TGDetect installed and licensed, end the TGDetect subsystem before attempting to save a configuration. If you are running TGDetect subsystems at the time you attempt to save your configuration, you will receive an error message.

To save the configuration

1) Access the **IBM i Main** menu.
2) At the **Selection or command** prompt, enter **TGMENU**.
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Save/Restore Configuration).

Note: The **Save/Restore TG Configuration (TGSAVRST)** interface is displayed.

5) Complete the following fields:

Field	Description

Product component	Identify the configuration component(s) you want to save. The options available are as follows: ***ALL** - Save all components ***RPT** - Save reports, report cards settings, and audit configuration ***JAM** - Save JAM (Job Activity Monitoring) rules, groups, monitored subsystems, and monitored commands ***NTW** - Save network socket and exit rules, groups, calendars, exit point configuration, and defaults ***ACC** - Save AEM (Access Escalation Manager) entitlements, groups, calendars, editors, defaults, and access control ***ISL** - Save ISL (Inactive Session Lockdown) defaults, rules, options ***RSC** - Save Resource Manager defaults, schemas, collections configuration ***PRF** - Save Profile Manager defaults, blueprints, user exclusions, password rules, etc. ***DET** - Save TGDetect defaults **Tip:** If you want to add multiple of components (RPT + JAM), then in the **+ for more values** field, enter a plus sign (+) and then press **Enter**. A column of empty rows appears. Enter each component on a separate row. When you have entered all the desired components, press **Enter** again to return to the **Save/Restore TG Configuration** interface.
Operation to perform	Enter ***SAVE** to create a configuration file--which creates an archive of the current configuration settings-- for the selected product components.

6) Click **Enter**.
7) Complete the following fields:

Field	Description
Save file	Enter the name you want to assign the save file or enter ***DEFAULT** to use the default name (i.e., TGSAVCFG).
Library	Enter the name of the library in which to store the save file or enter ***CURLIB** to store the file in the current library.
Clear Save File	Whether to override the save file (if it exists) ***YES** - Override the existing file ***NO** - Do not override an existing save file **Tip**: If this setting is set to ***NO** and you attempt to create a save file with the same name as an existing save file, you will receive an error message. You have two options if you receive an error message: --If you want to override the existing save file, change the option to ***YES** --If you do not want to override the existing save file, leave the option set to ***NO** and change the name of the save file you want to create, thereby, avoiding the override of the existing save file
Target Release	Enter the release for which you want to save a configuration: ***CURRENT** - Save the configuration for the currently installed operating system (OS) ***PRV** - Save the configuration to work with the previous OS **Tip**: Use the **F4** keyboard function to see the complete list of available OS versions. **Note**: The max number of previous OS versions for which you can create a save file are two. For example, if you are running V7R3M0 currently, you could do the following:

	-- Enter ***CURRENT** to create a save file compatible with V7R3M0 (currently installed OS in this example) -- Enter ***PRV** to create a save file compatible with V7R2M0 (one version older than current OS in this example) -- Manually enter **V7R1M0** (two versions older than current OS version in this example). If you attempt to create a save file for a version greater than two previous OS releases, you will receive an error message.
Run interactively	Whether to run interactively or add to batch: ***YES** - Run the report immediately ***NO** - Add the report to a batch job to be run when most efficient for the system

8) Click **Enter**.

Note: If a saved configuration file already exists with the defined name in the preferred library, you will receive an information message. You can choose to cancel the save (C) or replace (G) the file.

11.1.2. Restore Configuration

Use this task to restore the configuration of your agent to a previous state using an existing save file.

Caution: If you have TGDetect installed and licensed, end the TGDetect subsystem before attempting to restore a configuration. If you are running TGDetect subsystems at the time you attempt to restore your configuration, you will receive an error message.

To restore the configuration

1) Access the **IBM i Main** menu.
2) At the **Selection or command** prompt, enter **TGMENU**.
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Save/Restore Configuration).

Note: The **Save/Restore TG Configuration (TGSAVRST)** interface is displayed.

5) Complete the following fields:

Field	Description
Product component	Identify the configuration component(s) you want to restore. Your options are as follows: ***ALL** - Restore all components ***RPT** - Restore reports, report cards settings, and audit configuration ***JAM** - Restore JAM (Job Activity Monitoring) rules, groups, monitored subsystems, and monitored commands ***NTW** - Restore network socket and exit rules, groups, calendars, exit point configuration, and defaults ***ACC** - Restore AEM (Access Escalation Manager) entitlements, groups, calendars, editors, defaults, and access control ***ISL** - Restore ISL (Inactive Session Lockdown) defaults, rules, options ***RSC** - Restore Resource Manager defaults, schemas, collections configuration ***PRF** - Restore Profile Manager defaults, blueprints, user exclusions, password rules, etc. ***DET** - Restore TGDetect defaults **Tip:** If you want to add multiple of components (RPT + JAM), then in the **+ for more values** field, enter a plus sign (+) and then press **Enter**. A column of empty rows appears. Enter each

	component on a separate row. When you have entered all the desired components, press **Enter** again to return to the **Save/Restore TG Configuration** interface.
Operation to perform	Enter ***RESTORE** to use an existing save file to restore the configuration to a previous state.

6) Click **Enter**.
7) Complete the following fields:

Field	Description
Save file	Enter the name of the save file you want to use to restore the configuration or enter ***DEFAULT** to use the default name (i.e., TGSAVCFG).
Library	Enter the name of the library in which the save file is stored.
Run Interactively	Enter one of the following options: ***YES** - Run the restore job immediately ***NO** - Add the restore job to the queue

8) Click **Enter**.

11.1.3. Copy Configuration

Use this task to copy the configuration of one agent to another agent.

To copy the configuration

1) Follow the instructions to save a configuration instance.
2) Use whatever method (e.g., FTP) you are most comfortable with to transfer the save file (e.g., TGSAVCFG).

Tip: You must transfer the save file manually onto each server on which you want to restore a specific configuration.

3) Follow the instruction to restore a configuration instance.

See also

Save/Restore TG Configuration

12. Troubleshooting

12.1. FAQ

This section provides troubleshooting information you can use to resolve issues you might encounter.

12.1.1. Why does my report have no data?

If you generate a report and it contains no data, you need to ensure that auditing has been enabled (see Audit Configuration).

12.2. Error Messages

12.2.1. IBM Error Messages

Use this section to learn more about error messages you might encounter.

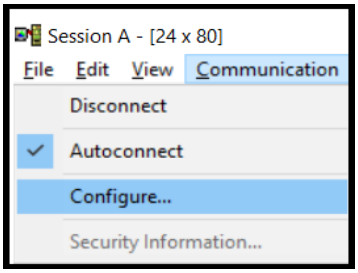
- CPF4169_while_accessing_menu_options
- Exit_program_NTW70006P_could_not_be_found_in_library

12.2.1.1. CPF4169 while accessing menu options

If you encounter a run-time error with message ID CPF4169 while accessing any of the menu options, it is likely that the emulator you are using has a display size of 24x80. The TG interface requires the use of a larger screen size (27x132). To resolve the issue, simply change the emulator session size to 27x132.

To change the emulator display size

1) Access the IBM i **Main** menu.
2) From the session menu, click **Communication | Configure.**



3) In the **Type of emulation** group box, change **Size** to **27x132**.
4) Click **OK**.
5) From the **Session** menu, select **File| Save**. This will update your .ws (Windows JScripit) file.

12.2.1.2. Exit program NTW[ID] could not be found in library

If you encounter this message, it's like the upgrade was performed without first cycling the *FILE or *DATABASE servers.

To cycle the server(s)

1) Access the IBM i **Main** menu.
2) At the **Selection or command** prompt, enter **TGMENU**.
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **2** (TGSecure).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **1** (Network Security).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **10** (Exit Point Configuration).
9) Press **Enter**.
10) At the **Selection or command** prompt, enter **13** (Cycle Server).
11) Press **Enter**.

Alternatively, select keyboard function **F19** to cycle multiple servers at once.

12.3. Fixes

12.3.1. Fix Files

TGFix is a tool introduced in version 2.0 that allows you to install fixes via the TG menu quickly and easily. The feature also includes verification features that ensure the fix is installed properly.

See also

Save Fix to Agent Server

Manage Fixes

Display List of Fixes

12.3.2. Save Fix to Agent Server

Use this task to save the TGFix file to the agent server. You must FTP the fix file to the server before you can apply it.

To save the fix to the agent server

1) Open a DOS or command window.
2) Type the following command, substituting the name of the iSeries server for [system-name].

    FTP [system-name]

Alternatively: You can use the iSeries IP (internet address) instead of the system name.

3) Use the iSeries command **GO TCPADM** to find the address.
4) Select option **7**.
5) Select option **1**.
6) Type a user ID at the FTP prompt and press **Enter**.
7) Type the password at the FTP prompt and press **Enter**.
8) Type the following command to create the TGFIX library if it does not exist on your iSeries server:

    quote rcmd crtlib TGFIX

9) Type the following command to create the save file if it does not exist on your iSeries server:

    quote rcmd crtsavf TGFIX/TGF018001

10) Type the following command to transfer the file using binary image mode:

binary

11) Type the following command to identify the path, where [path] is the folder where you saved the file in Step 2:

lcd [path]

12) Type the following command to transfer the file from the PC to the iSeries:

put TGF018001.svf TGFIX/TGF018001

13) Type the following command to end FTP:

quit

14) Type the following command to close the DOS window:

exit

See also

Fix Files

Apply Fix

Display List of Fixes

12.3.3. Manage Fixes

Use this task to do the following:

- Apply fix
- Remove fix

Note: If you are working with a newly release version, there might not be fixes necessary/available. You will be notified as fixes become available.

12.3.3.1. Apply Fix

Use this task to apply a fix.

Tip: The fix file must be saved on the agent server before attempting to apply it.

To apply a fix

1) Access the **TG Main** menu.
2) At the **Selection or command** prompt, enter **TGFIX**.
3) Press the **F4** (Prompt) function key.

Note: The **TG Fix Manager (TGFIX)** interface is displayed.

4) Complete the following fields:

Field	Description
Fix ID	Enter the fix ID, which should be provided to you in the following format: (TGFVVVXXX) Where: **TGF** = TG Fix

	VVV = Three-digit version number. **FFF** = Three-digit numeric number (assigned sequentially) to each fix **Note**: For example, TGF020001 would be the 1st (001) TG fix for version 2.0 (020)
Fix action to perform	Enter ***APY**

5) Press **Enter**.

Note: The TGFix program performs validations before applying the fix (e.g., is the fix file present on the agent server, has the fix already been applied, etc.)

12.3.3.2. Remove Fix

Use this talk to remove a fix.

To remove a fix

1) Access the **TG Main** menu.
2) At the **Selection or command** prompt, enter **TGFIX**.
3) Press the F4 (Prompt) function key on your keyboard.

Note: The **TG Fix Manager (TGFIX)** interface is displayed.

4) Complete the following fields:

Field	Description
Fix ID	Enter the fix ID, which should be provided to you in the following format: (TGFVVVXXX) Where: **TGF** = TG Fix **VVV** = Three-digit version number. **FFF** = Three-digit numeric number (assigned sequentially) to each fix **Note**: For example, TGF020001 would be the 1st (001) TG fix for version 2.0 (020)
Fix action to perform	Enter ***RMV**

5) Press **Enter**.

See also

Fix Files

Save Fix to Agent Server

Display List of Fixes

12.3.4. Display List of Fixes

Use this task to display the list of fixes applied to the agent.

To display the list of fixes

1) Access the **TG Main** menu.

2) At the **Selection or command** prompt, enter **80** (Licensing Status).
3) Press **Enter**.
4) Press the **F6** (Add Key) function key on your keyboard.
5) Enter the license key.
6) Press **Enter**.

Field	Description
Fix ID	The Fix ID is based on the following nomenclature: **TGFVVVFFF** Where: **TGF** = TG Fix **VVV** = Three-digit version number. **FFF** = Three-digit numeric number (assigned sequentially) to each fix **Note**: For example, TGF020001 would be the 1st (001) TG fix for version 2.0 (020)
Applied Date	Date on which the fix was applied to the system
Apply User	User who applied the fix

See also

Fix Files

Manage Fixes

13. APPENDIX - Collectors

Collector ID	Collector Name	Collector Category
ACCESS_ESCAL_ACC_CONTROLS	Access Escalation Access Controls	Network
ACCESS_ESCAL_DEFAULTS	Access Escalation Defaults	Network
ACCESS_ESCAL_ENTITLEMENTS	Access Escalation Entitlements	Network
ACCESS_ESCAL_FILE_EDITORS	Access Escalation File Editors	Network
ACCESS_ESCALATION_USAGE	Access Escalation Usage	Network
AUTH_USERS_VIA_AUTH_LISTS	Authorized Users through Authorization Lists	Resource
AUTHORITY_COLLECTION	Authority Collection Data	Journal
AUTHORITY_COMPLIANCE	Authority Compliance	Resource
AUTHORITY_LIST	Authority List Data	System
BLUEPRINT_3RD_PARTY_FILE	Blueprint 3rd Party Integration File	Profile
BLUEPRINT_AUTH_SETTINGS_FILE	Blueprint Authority List Settings File	Profile
BLUEPRINT_MASTER	Blueprint Master	Profile
BLUEPRINT_NON_COMPLIANCE_USER	Blueprint Non-Compliance User Profiles	Profile
BLUEPRINT_OBJECT_AUTH_FILE	Blueprint Object Authority File	Profile
BLUEPRINT_PARAMETER_FILE	Blueprint Parameter File	Profile
CONTROLLER_ATTACHED_DEVICES	Controller Attached Device Information	Network
CONTROLLER_DESCRIPTION_DATA	Controller Description Information	Network
DATA_AREA_AUDITING	Audit data area changes	Network
DATABASE_AUDITING	Monitor Database changes	Network
DATABASE_CONTENT	Database Content	Configuration
DET_ACT_HISTORY	Detect Activity History	Network
DET_CMD_RULES	Command Monitor Rules	Configuration
DET_JRN_SEIM_RULES	Journal Monitor Rules for SEIM	Configuration
DET_JRNMON_ALERTS	Journal Monitor Alerts	Configuration
DET_JRNMON_RULES	Journal Monitor Rules	Configuration
DET_MON_MASTER	Monitor Master	Configuration
DET_MSQ_CMD_ALR	Message Queue and Command Alerts	Configuration

Collector ID	Collector Name	Collector Category
DET_MSQ_RULES	Message Queue Rules	Configuration
DET_SEIM_PROVIDERS	SEIM Providers	Configuration
DET_SNMP_TRP_PCKG	SNMP Trap Packages	Configuration
DEVICE_DESCRIPTION_APPC	Device Description APPC Information	Network
DEVICE_DESCRIPTION_DATA	Device Description Information	Network
EXIT_POINTS	Display Exit Point Data	Network
FIELD_AUTHORITY	Display Field Level Authorities	Object
IFS_ATTRIBUTES	Display the attributes for the IFS objects	Resource
IFS_AUTHORITIES	Display the public and private authorities associated with the object	Resource
IFS_CONTENT	IFS Content	Configuration
IFS_JOURNALING	Display extended journaling information for the IFS object	Resource
IFS_STATUS	Display status information about an IFS file	Resource
ISL_CONFIGURATION_SETTINGS	ISL Configuration Settings	Network
ISL_DISCONNECT_OPTIONS	ISL Disconnect Options	Network
ISL_RULES	ISL Inclusion Exclusion Rules	Network
JOB_ACTIVITY_DETAILS	Job Activity Details	Log
JOB_ACTIVITY_SUMMARY	Job Activity Summary	Log
JOB_DESCRIPTIONS	Job Description Data	Configuration
JOURNAL_AD	Object Auditing Attribute Changes	Configuration
JOURNAL_AF	Authority Failures	Profile
JOURNAL_AP	Programs that Adopt Authority were Executed	Configuration
JOURNAL_AU	EIM Attribute Changes	Configuration
JOURNAL_AX	Row and Column Access Control	Resource
JOURNAL_CA	Authorization List or Object Authority Changes	Profile
JOURNAL_CD	Commands Executed	Resource
JOURNAL_CO	Create Operations	Resource
JOURNAL_CP	User Profile Changes	Configuration
JOURNAL_CQ	Change Request Descriptor Changes	Configuration
JOURNAL_CU	Cluster Operation	Network
JOURNAL_CV	Connection Verification	Profile

Collector ID	Collector Name	Collector Category
JOURNAL_CY	Cryptographic Configuration Changes	Configuration
JOURNAL_DI	LDAP Operations	Resource
JOURNAL_DO	Delete Operations	Resource
JOURNAL_DS	Changes to Service Tools Profiles	Profile
JOURNAL_EV	Environment Variable Changes	Profile
JOURNAL_GR	Exit Point Maintenance Operations	Resource
JOURNAL_GS	Socket Descriptor Details	Resource
JOURNAL_IM	Intrusion Monitor Events	Network
JOURNAL_IP	Inter-process Communication Events	Network
JOURNAL_IR	Actions to IP Rules	Network
JOURNAL_IS	Internet Security Management Events	Network
JOURNAL_JD	Job Descriptions – USER Parameter Changes	Resource
JOURNAL_JS	Job Changes	Resource
JOURNAL_KF	Key Ring File Changes	Configuration
JOURNAL_LD	Directory Link, Unlink, and Search Operations	Resource
JOURNAL_M0	Db2 Mirror Setup Tools	Resource
JOURNAL_M6	Db2 Mirror Communication Services	Resource
JOURNAL_M7	Db2 Mirror Replication Services	Resource
JOURNAL_M8	Db2 Mirror Product Services	Resource
JOURNAL_M9	Db2 Mirror Replication State	Resource
JOURNAL_ML	OfficeVision Mail Services Actions	Configuration
JOURNAL_NA	Network Attribute Changes	Profile
JOURNAL_ND	Directory Search Violations	Resource
JOURNAL_NE	APPN Endpoint Filter Violations	Network
JOURNAL_O1	Single Optical Object Accesses	Resource
JOURNAL_O2	Dual Optical Object Accesses	Resource
JOURNAL_O3	Optical Volume Accesses	Resource
JOURNAL_OM	Object Management Changes	Resource
JOURNAL_OR	Objects Restored	Resource
JOURNAL_OW	Object Ownership Changes	Resource
JOURNAL_PA	Program Changes to Adopt Owner Authority	Configuration

Collector ID	Collector Name	Collector Category
JOURNAL_PF	PTF Operations	Resource
JOURNAL_PG	Primary Group Changes	Resource
JOURNAL_PO	Printer Output Changes	Resource
JOURNAL_PS	Swap Profile Events	Configuration
JOURNAL_PU	PTF Object Changes	Profile
JOURNAL_PW	Invalid Sign-on Attempts	Profile
JOURNAL_RA	Authority Changes to Restored Objects	Configuration
JOURNAL_RJ	Job Descriptions that Contain User Profile Names were Restored	Configuration
JOURNAL_RO	Ownership Changes for Restored Objects	Profile
JOURNAL_RP	Programs Restored that Adopt Owner Authority	Configuration
JOURNAL_RQ	Change Request Descriptors Restored	Resource
JOURNAL_RU	Authority Restored for User Profiles	Profile
JOURNAL_RZ	Primary Group Changes for Restored Objects	Configuration
JOURNAL_SD	System Directory Changes	Resource
JOURNAL_SE	Subsystem Routing Entry Changes	Configuration
JOURNAL_SF	Spooled File Actions	Resource
JOURNAL_SG	Asynchronous Signals Processed	Network
JOURNAL_SK	Secure Socket Connections	Network
JOURNAL_SM	Systems Management Changes	Configuration
JOURNAL_SO	Server Security User Information Actions	Configuration
JOURNAL_ST	Service Tools Actions	Configuration
JOURNAL_SV	System Values Changes	Configuration
JOURNAL_VA	Access Control List Changes	Configuration
JOURNAL_VC	Connections Started, Ended, or Rejected	Network
JOURNAL_VF	Close Operations on Server Files	Resource
JOURNAL_VL	Exceeded Account Limit Events	Profile
JOURNAL_VN	Network Log On and Off Events	Configuration
JOURNAL_VO	Actions on Validation Lists	Resource
JOURNAL_VP	Network Password Errors	Profile
JOURNAL_VR	Network Resource Accesses	Resource

Collector ID	Collector Name	Collector Category
JOURNAL_VS	Server Sessions Started or Ended	Network
JOURNAL_VU	Network Profile Changes	Profile
JOURNAL_VV	Service Status Change Events	Network
JOURNAL_X0	Network Authentication Events	Network
JOURNAL_X1	Identity Token Events	Profile
JOURNAL_XD	Directory Server Extensions	Profile
JOURNAL_YC	DLO Object Changes	Resource
JOURNAL_YR	DLO Object Reads	Resource
JOURNAL_ZC	Object Changes	Resource
JOURNAL_ZR	Object Reads	Resource
KEYSTORE_DATA	KeyStore	Configuration
LINE_DESCRIPTION_DATA	Line Description Information	Configuration
MESSAGE_QUEUE	Message Queue Details	Configuration
MESSAGE_QUEUE_DATA	Message Queue Data	Configuration
NETWORK_ATTRIBUTES	Network Attribute Information	Network
NETWORK_CONNECTIONS	Network Connections Ipv4 and Ipv6	Network
NETWORK_EXIT_CONFIG	Exit Point Configuration Report	Network
NETWORK_INTERFACE_IPV4	Network Interface Data Ipv4	Network
NETWORK_INTERFACE_IPV6	Network Interface Data Ipv6	Network
NETWORK_ROUTE_IPV4	Network Route Data Ipv4	Network
NETWORK_ROUTE_IPV6	Network Route Data Ipv6	Network
NETWORK_SERVER_DESCRIPTIONS	Network Server Description Data	Network
NETWORK_SVR_ENCRYPT_STATUS	Network Server Encryption Status	Network
NETWORK_TCPIP_IPV4	TCP/IP Ipv4 Stack Attributes	Network
NETWORK_TCPIP_IPV4	Remote Exit Rules	Network
NETWORK_TCPIP_IPV6	TCP/IP Ipv6 Stack Attributes	Network
NETWORK_TCPIP_IPV6	Remote Exit Rules	Network
NETWORK_TRANS_CENTRAL	Central Server Transactions	Network
NETWORK_TRANS_COMMAND	Remote Command Transactions	Network
NETWORK_TRANS_DATABASE	Remote Exit Rules	Network
NETWORK_TRANS_DATAQ	Remote Exit Rules	Network

Collector ID	Collector Name	Collector Category
NETWORK_TRANS_DDM	Remote Exit Rules	Network
NETWORK_TRANS_SHOWCASE	Network Trans Showcase	Network
NETWORK_TRANSACTIONS_FILE	Remote Exit Rules	Network
NETWORK_TRANSACTIONS_FTP_REXEC	Remote Exit Rules	Network
NETWORK_TRANSACTIONS_PRINTER	Remote Exit Rules	Network
NETWORK_TRANSACTIONS_SIGNON	Remote Exit Rules	Network
NETWORK_TRANSACTIONS_TELNET	Remote Exit Rules	Network
OBJECT_AUTHORITY	Display Object Authority	Resource
OBJECT_DETAILS	Display Object Details	Resource
OUTPUT_QUEUE	Output Queue Information	Configuration
PRODUCT_INFO	Basic Information about a software product	Configuration
PROFILE_COMPLIANCE	Profile Compliance Data	Profile
PROFILE_INACTIVITY_SETTINGS	Profile Inactivity Settings	Profile
PROFILE_MANAGER_DEFAULTS	Profile Manager Defaults	Profile
PROGRAM_ADOPT	Programs that Adopt Authority	Resource
PROGRAM_REFERENCE_DATA	Program Reference Data	Resource
PTF_DATA	Program Temporary Fix Data	Configuration
QSYS2.ACTIVE_JOB_INFO	Active job information	Configuration
QSYS2.DRDA_AUTHENTICATION	DRDA and DDM User access	Configuration
QSYS2.FUNCTION_INFO	Function usage identifiers	Configuration
QSYS2.FUNCTION_USAGE	Function usage configuration details.	Configuration
QSYS2.GROUP_PTF_INFO	Group PTFs Information	Configuration
QSYS2.JOURNAL_INFO	Journal and remote journal information	Configuration
QSYS2.LICENSE_INFO	Products license information.	Configuration
QSYS2.MEDIA_LIBRARY_INFO	Media Library Status details	Configuration
QSYS2.MEMORY_POOL	Memory pool details	Configuration
QSYS2.MEMORY_POOL_INFO	Active memory pools	Configuration
QSYS2.NETSTAT_JOB_INFO	IPv4 and IPv6 network connection details.	Configuration
QSYS2.OBJECT_LOCK_INFO	Object lock information	Configuration
QSYS2.OUTPUT_QUEUE_ENTRIES	Spooled file in output queue	Configuration
QSYS2.RECORD_LOCK_INFO	Record lock information	Configuration

Collector ID	Collector Name	Collector Category
QSYS2.REPLY_LIST_INFO	Current job's reply list entry information	Configuration
QSYS2.SCHEDULED_JOB_INFO	Job Schedule Entry information	Configuration
QSYS2.SERVER_SBS_ROUTING	Alternate subsystem configurations	Configuration
QSYS2.SYSCONTROLS	Permissions or column mask defined	Configuration
QSYS2.SYSCONTROLSDEP	Dependencies of row permissions and column masks	Configuration
QSYS2.SYSDISKSTAT	Disk Information	Configuration
QSYS2.SYSTEM_STATUS_INFO	Partition information	Configuration
QSYS2.SYSTMPSTG	IBM i temporary storage pool detail	Configuration
QSYS2.USER_INFO	User Profile Information	Configuration
QSYS2.USER_STORAGE	Storage usage by user profile	Configuration
REMOTE_TRAN_SUMMARY_BY_SERVER	Remote Summary Server	Network
REMOTE_TRAN_SUMMARY_BY_USER	Remote Summary User	Network
RSC_MGR_COMPLIANCE_DATA	Resource Manager Authority Out of compliance data	Network
RSC_MGR_CONFIG	Resource Manager Configuration	Network
RSC_MGR_SCHEMA_DETAILS	Resource Manager Authority Schema Details	Network
RSC_MGR_SCHEMA_HEADER	Resource Manager Authority Schema Header	Network
SERVICE_TOOL_SECURITY_ATTR	Service Tool Security Attributes	Profile
SERVICE_TOOL_USERS	Service Tool User Data	Profile
SOCKET_SUMMARY_BY_SERVER	Socket Summary by Server	Network
SOCKET_SUMMARY_BY_USER	Socket Summart by User	Network
SOCKET_TRAN_RULES	Socket Rules	Network
SOCKET_TRANSACTIONS	Socket Transactions	Network
SOFTWARE_RESOURCES	Installed Software Resources Data	Configuration
SUBSYSTEM_AUTOSTART	Subsystem Autostart Jobs	Configuration
SUBSYSTEM_COMMUNICATIONS	Subsystem Communication Entries	Configuration
SUBSYSTEM_INFORMATION	Subsystem Information Details	Configuration
SUBSYSTEM_JOB_QUEUE	Subsystem Job Queue	Configuration
SUBSYSTEM_POOL_DATA	Subsystem Pool Data	Configuration
SUBSYSTEM_PRESTART	Subsystem Prestart Jobs	Configuration
SUBSYSTEM_REMOTE	Subsystem Remote Entries	Configuration

Collector ID	Collector Name	Collector Category
SUBSYSTEM_ROUTING	Subsystem Routing Entries	Configuration
SUBSYSTEM_WORKSTATION_NAMES	Subsystem Workstation Names	Configuration
SUBSYSTEM_WORKSTATION_TYPES	Subsystem Workstation Types	Configuration
SYSCOLAUTH	Privileges granted on a column	Configuration
SYSCONTROLS	Permission or column mask defined	Configuration
SYSCONTROLSDEP	Dependencies of row permissions and column masks	Configuration
SYSCONTROLSDEP	Privileges granted on a row	Configuration
SYSFIELDS	Columns with field procedures	Configuration
SYSPACKAGEAUTH	Privileges granted on a package	Configuration
SYSPROGRAMSTAT	Program, service program, and module with SQL statements	Configuration
SYSROUTINEAUTH	Privileges granted on a routine	Configuration
SYSSCHEMAAUTH	Privileges granted on a schema	Configuration
SYSSEQUENCEAUTH	Privileges granted on a sequence	Configuration
SYSTABAUTH	Privileges granted on a table or view	Configuration
SYSTABLESTAT	Table statistics include all partitions and members	Configuration
SYSTEM_VALUES	Display System Value Data	System
SYSTOOLS.GROUP_PTF_CURRENCY	PTF Groups installed per IBM Recommendations	Configuration
SYSTOOLS.GROUP_PTF_DETAILS	PTFs within PTF Groups installed per IBM Recommendations	Configuration
SYSUDTAUTH	Privileges granted on a type	Configuration
SYSVARIABLEAUTH	Privileges granted on a global variable	Configuration
SYSXSROBJECTAUTH	Privileges granted on an XML schema	Configuration
TGMOBJINF	Object Information	Resource
TG_NETWORK_GROUPS	TG Network Groups	Network
TG_OBJECT_GROUPS	TG Object Groups	Network
TG_OPERATION_GROUPS	TG Operation Groups	Network
TG_USER_GROUPS	TG User Groups	Network
USER_OBJECT_AUTHORITIES	User Profile Object Authorities	Profile
USER_PRF_VIA_BLUEPRINT	User Profile via Blueprint	Profile

Collector ID	Collector Name	Collector Category
USER_PROFILE_ACTIVITY	User Profile Activity	Profile
USER_PROFILE_EXCLUSIONS	User Profile Exclusions	Profile
USER_PROFILES	Display User Profile Data	Profile