Directory and Resource Administrator and Exchange Administrator

Administrator Guide

July 2016

Legal Notice

NetIQ Directory and Resource Administrator and Exchange Administrator are protected by United States Patent No. 6,792,462.

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government’s rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

Check Point, FireWall-1, VPN-1, Provider-1, and SiteManager-1 are trademarks or registered trademarks of Check Point Software Technologies Ltd.

ActiveAudit, ActiveView, Aegis, AppManager, Change Administrator, Change Guardian, Compliance Suite, the cube logo design, Directory and Resource Administrator, Directory Security Administrator, Domain Migration Administrator, Exchange Administrator, File Security Administrator, Group Policy Administrator, Group Policy Guardian, Group Policy Suite, IntelliPolicy, Knowledge Scripts, NetConnect, NetIQ, the NetIQ logo, PSAudit, PSDetect, PSPasswordManager, PSSecure, Secure Configuration Manager, Security Administration Suite, Security Manager, Server Consolidator, VigilEnt, and Vivinet are trademarks or registered trademarks of NetIQ Corporation or its subsidiaries in the USA. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.

For purposes of clarity, any module, adapter or other similar material ("Module") is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

Contents

About this Book and the Library 13
About NetIQ Corporation 15

1 Introduction 17

1.1 What are DRA and ExA? . . . 18
1.2 What DRA and ExA Provide . . . 18
1.3 How DRA and ExA Help You . . . 19
1.3.1 Provide Regulatory Compliance . . . 19
1.3.2 Maintain Control of Active Directory . . . 20
1.3.3 Increase Administration Efficiency . . . 20
1.3.4 Reduce Administration Costs . . . 20
1.3.5 Ensure Data Integrity . . . 21
1.4 How DRA and ExA Work . . . 21
1.4.1 Presentation Layer . . . 22
1.4.2 Business Logic Layer . . . 23
1.4.3 Administration Server . . . 23
1.4.4 Data Layer . . . 24
1.5 Supported Environments . . . 24
1.5.1 Managed and Trusted Domains . . . 24
1.5.2 Microsoft Exchange Support . . . 24
1.5.3 Departmental Support through Managed Subtrees . . . 25
1.5.4 Multiple Administration Servers . . . 25

2 Working with the User Interfaces 27

2.1 Web Console . . . 28
2.1.1 Starting the Web Console . . . 28
2.1.2 Customizing the Web Console . . . 28
2.1.3 Configuring Windows Authentication . . . 28
2.1.4 Configuring Smart Card Authentication . . . 29
2.1.5 Configuring Multi-factor Authentication with NetIQ Advanced Authentication Framework . . . 30
2.2 Account and Resource Management Console . . . 34
2.3 Delegation and Configuration Console . . . 35
2.4 Command-Line Interface . . . 35
2.5 Licensing Affects Available Features . . . 36
2.6 Customizing and Extending the User Interface . . . 36
2.6.1 How User Interface Extensions Work . . . 36
2.6.2 Supported Custom Pages . . . 37
2.6.3 Supported User Interface Controls . . . 38
2.6.4 Accessing the User Interface Extensions Node . . . 39
2.6.5 Implementing User Interface Extensions . . . 39
2.6.6 Creating User Interface Extensions . . . 40
2.6.7 Modifying User Interface Extension Properties . . . 41
2.6.8 Identifying Active Directory Attributes Managed With User Interface Extensions . . . 41
2.6.9 Enabling User Interface Extensions . . . 41
2.6.10 Disabling User Interface Extensions . . . 42
2.6.11 Deleting User Interface Extensions . . . 42
2.7 User Interface Tasks . . . 42
2.7.1 Automatically Logging in to the Web Console with Internet Explorer . . . 42

2.7.2 Accessing a User's Change History . . . 43
2.7.3 Connecting to an Administration Server . . . 43
2.7.4 Connecting to a Managed Domain or Computer . . . 44
2.7.5 Modifying the Console Title . . . 44
2.7.6 Customizing List Columns . . . 45
2.7.7 Using Custom Tools . . . 45
2.7.8 Executing Saved Advanced Queries . . . 46
2.7.9 Enabling Collection of Application Logs . . . 46
2.7.10 Reporting on Object Changes . . . 46
2.7.11 Reporting on Object Lists . . . 47
2.7.12 Reporting on Object Details . . . 47
2.7.13 Saving Console Windows . . . 48
2.7.14 Saving Custom Console Files . . . 48
2.7.15 Restoring Console Settings . . . 48
2.7.16 Using Special Characters . . . 49
2.7.17 Using Wildcard Characters . . . 50
2.7.18 Viewing Your Assigned Powers and Roles . . . 51
2.7.19 Viewing the Product Version Number and Installed Hotfixes . . . 51
2.7.20 Viewing Your Current License . . . 51
2.7.21 Upgrading Your License . . . 52
2.8 DRA Reporting . . . 52

3 Understanding the Dynamic Security Model 55

3.1 What Is Distributed Administration? . . . 55
3.2 What Is the Dynamic Security Model? . . . 56
3.2.1 Assistant Admins . . . 56
3.2.2 Roles . . . 57
3.2.3 Powers . . . 57
3.2.4 ActiveViews . . . 57
3.3 What ActiveViews Provide . . . 57
3.3.1 ActiveViews Include Dynamic Sets of Objects . . . 58
3.3.2 ActiveViews Include Flexible Rules . . . 59
3.4 ActiveViews and Distributed Administration . . . 59
3.5 How the Administration Server Processes Requests . . . 60
3.6 How Powers Can Increase . . . 60
3.7 Understanding How Powers Increase . . . 61
3.7.1 Groups in Multiple ActiveViews . . . 62
3.7.2 Using Powers in Multiple ActiveViews . . . 63
3.7.3 Extending Powers . . . 63

4 Understanding the Default Security Model 65

4.1 What Is the Default Security Model? . . . 65
4.2 What Built-in Security Provides . . . 65
4.2.1 All Powers for DRA Admins . . . 66
4.2.2 Domain Powers for Administrators . . . 66
4.2.3 Built-in Delegations . . . 67
4.3 Understanding Built-in ActiveViews . . . 67
4.3.1 Built-in ActiveViews . . . 67
4.3.2 Accessing Built-in ActiveViews . . . 68
4.3.3 Using Built-in ActiveViews . . . 68
4.4 Understanding Built-in Assistant Admin Groups . . . 69
4.4.1 Built-in Assistant Admin Groups . . . 69
4.4.2 Accessing Built-in Assistant Admin Groups . . . 70
4.4.3 Using Built-in Assistant Admin Groups . . . 70
4.5 Understanding Built-in Roles . . . 70
4.5.1 Built-in Roles . . . 71

4.5.2 Accessing Built-in Roles . . . 77
4.5.3 Using Built-in Roles . . . 77

5 Implementing Advanced Queries 79

5.1 Understanding Advanced Queries . . . 79
5.2 How DRA Helps You Manage Advanced Queries . . . 79
5.3 Advanced Query on Virtual Attributes . . . 79
5.4 Advanced Query Management Tasks . . . 80

6 Implementing Virtual Attributes 81

6.1 Understanding Virtual Attributes . . . 81
6.2 Virtual Attribute Tasks . . . 81
6.3 Accessing The Virtual Attributes Node . . . 81
6.3.1 Creating Virtual Attributes . . . 81
6.3.2 Enabling Virtual Attributes . . . 82
6.3.3 Associating Virtual Attributes with Objects . . . 82
6.3.4 Disassociating Virtual Attributes . . . 83
6.3.5 Disabling Virtual Attributes . . . 83

7 Implementing Custom Tools 85

7.1 Understanding Custom Tools . . . 85
7.1.1 Sample Custom Tools . . . 85
7.2 Understanding File Replication . . . 86
7.3 Custom Tool Tasks . . . 86
7.3.1 Accessing Custom Tools Node . . . 86
7.3.2 Creating a Custom Tool . . . 87
7.3.3 Modifying Custom Tools Properties . . . 87
7.3.4 Enabling a Custom Tool . . . 88
7.3.5 Disabling a Custom Tool . . . 88
7.3.6 Deleting a Custom Tool . . . 88
7.3.7 Uploading Custom Tool Files for Replication . . . 88
7.3.8 Replicating Multiple Files Between Administration Servers . . . 89
7.3.9 Replicating Multiple Files to DRA Client Computers . . . 90
7.3.10 Using a Custom Tool . . . 90

8 Implementing OU and Active Directory Administration 93

8.1 How DRA Helps You Manage OUs . . . 93
8.2 Using ActiveViews to Manage OUs . . . 93
8.2.1 Using OUs to Create and Maintain ActiveViews . . . 93
8.2.2 Built-in Containers in Microsoft Windows Domains . . . 94
8.3 OU Management Tasks . . . 94

9 Implementing User Account Administration 95

9.1 How DRA and ExA Help You Manage User Accounts . . . 95
9.2 Using ActiveViews to Manage User Accounts . . . 95
9.2.1 User Account Naming Conventions . . . 96
9.2.2 Understanding User Account Transfer . . . 96
9.2.3 Transferring User Accounts . . . 97
9.2.4 Using Group Membership to Create and Maintain ActiveViews . . . 97
9.3 User Accounts in Trusted Domains . . . 97
9.4 Managing Clone Exceptions . . . 98
9.4.1 Creating Clone Exceptions . . . 98

9.4.2 Deleting Clone Exceptions . . . 98
9.5 User Account Management Tasks . . . 98

10 Implementing Group Administration 99

10.1 How DRA and ExA Help You Manage Groups . . . 99
10.2 Using ActiveViews to Manage Groups . . . 99
10.2.1 Group Naming Conventions . . . 100
10.2.2 User-Created Local Groups . . . 100
10.3 Groups in Trusted Domains . . . 100
10.4 Managing Native Built-in Security Groups . . . 101
10.4.1 Native Built-in Security Groups You Can Restrict . . . 101
10.4.2 Restricting Actions on Native Built-in Security Groups . . . 102
10.5 Managing Group Membership Security . . . 103
10.5.1 Allowing Users to Manage Group Memberships . . . 103
10.5.2 Delegating Group Membership Security . . . 103
10.6 Temporary Group Assignments . . . 103
10.7 Group Management Tasks . . . 104

11 Implementing Resource Administration 105

11.1 How DRA Helps You Manage Resources . . . 105
11.2 Using ActiveViews to Manage Resources . . . 105
11.2.1 Resource Naming Conventions . . . 106
11.2.2 Computers . . . 106
11.2.3 Services . . . 107
11.2.4 Shares . . . 107
11.2.5 Printers and Print Jobs . . . 108
11.2.6 Published Printers . . . 108
11.2.7 Connected Users . . . 108
11.2.8 Devices . . . 109
11.2.9 Open Files . . . 109
11.2.10 Event Logs . . . 109
11.3 Resource Management Tasks . . . 110

12 Implementing the Recycle Bin 111

12.1 Understanding the Recycle Bin . . . 111
12.2 Accessing the Recycle Bin . . . 111
12.3 Using the Recycle Bin . . . 112
12.3.1 Enabling the Recycle Bin . . . 113
12.3.2 Disabling the Recycle Bin . . . 114

13 Enforcing Policy 115

13.1 Understanding Policy . . . 115
13.1.1 What Is a Policy? . . . 115
13.1.2 How the Administration Server Enforces Policy . . . 116
13.2 Accessing Policy . . . 116
13.3 Creating and Implementing Home Directory Policy . . . 117
13.3.1 Administration Server Requirements . . . 117
13.3.2 Configuring Home Directory Allowable Paths for NetApp Filers . . . 118
13.3.3 Understanding Home Directory Policy . . . 118
13.3.4 Home Directory Automation and Rules . . . 118
13.3.5 Home Share Automation and Rules . . . 121
13.3.6 Home Volume Disk Quota Management Rules . . . 122
13.4 Home Directory Policy Tasks . . . 122

13.4.1 Configuring Home Directory Policies . . . 122
13.4.2 Configuring Home Share Policy . . . 123
13.4.3 Configuring Home Volume Disk Quota Management Policy . . . 123
13.5 Implementing Default Policies . . . 123
13.5.1 Understanding Built-in Policies . . . 124
13.5.2 Available Policies . . . 124
13.5.3 Using Built-in Policy . . . 126
13.6 Creating and Implementing Microsoft Exchange Policy . . . 126
13.6.1 Mailbox Rules . . . 127
13.6.2 Automatic Naming Policy . . . 127
13.6.3 Office 365 Rules . . . 128
13.7 Microsoft Exchange Policy Tasks . . . 128
13.7.1 Enabling Microsoft Exchange Support . . . 128
13.7.2 Specifying an Automated Mailbox Naming Policy . . . 129
13.7.3 Specifying a Resource Naming Policy . . . 129
13.7.4 Specifying an Archive Naming Policy . . . 129
13.7.5 Specifying a Default Email Address Policy . . . 130
13.7.6 Specifying Microsoft Exchange Mailbox Policies . . . 130
13.7.7 Specifying Office 365 Mailbox Policies . . . 131
13.8 Creating and Implementing Custom Policy . . . 131
13.9 Policy Tasks . . . 131
13.9.1 Deleting Policies . . . 131
13.9.2 Disabling Policies . . . 132
13.9.3 Enabling Policies . . . 132
13.9.4 Implementing Built-in Policies . . . 132
13.9.5 Implementing Custom Policies . . . 133
13.9.6 Modifying Policy Properties . . . 133
13.9.7 Writing Custom Policy Scripts or Executables . . . 134

14 Implementing Your Dynamic Security Model 135

14.1 How to Create a Security Model . . . 135
14.1.1 Delegating Administration through a Static Model . . . 135
14.1.2 Delegating Administration through a Dynamic Model . . . 136
14.1.3 Understanding Power Creation . . . 136
14.1.4 Understanding Role Creation . . . 137
14.1.5 Understanding Assistant Admin Group Creation . . . 137
14.1.6 Understanding ActiveView Creation . . . 138
14.1.7 Optimizing Your ActiveView Rules . . . 138
14.2 Delegation Management Node . . . 139
14.2.1 Accessing Delegation Management . . . 139
14.2.2 Using Delegation Management . . . 140
14.3 Allowing Users to Change Personal Information . . . 140
14.4 ActiveView Tasks . . . 140
14.4.1 Adding Managed Objects . . . 141
14.4.2 Assigning ActiveViews to Assistant Admins and Roles . . . 141
14.4.3 Cloning ActiveViews . . . 141
14.4.4 Creating ActiveViews . . . 142
14.4.5 Reviewing ActiveViews . . . 142
14.4.6 Deleting ActiveViews . . . 143
14.4.7 Managing ActiveView Assignments . . . 143
14.4.8 Modifying ActiveView Properties . . . 144
14.4.9 Specifying a Target Container . . . 144
14.4.10 Viewing Managed Objects . . . 145
14.4.11 Removing Managed Objects from ActiveViews . . . 145
14.5 Assistant Admin Tasks . . . 145
14.5.1 Adding Assistant Admin Group Members . . . 146
14.5.2 Assigning Assistant Admins to Roles and ActiveViews . . . 146
14.5.3 Cloning Assistant Admin Groups . . . 146

14.5.4 Creating Assistant Admin Groups . . . 147
14.5.5 Deleting Assistant Admin Groups . . . 147
14.5.6 Managing Assistant Admin Assignments . . . 148
14.5.7 Modifying Assistant Admin Group Properties . . . 148
14.5.8 Removing Assistant Admin Assignments . . . 148
14.5.9 Viewing Powers and Roles Assigned to an Assistant Admin . . . 149
14.6 Power Tasks . . . 149
14.6.1 Understanding the Power Creation Process . . . 149
14.6.2 Creating New Powers . . . 150
14.6.3 Cloning Powers . . . 150
14.6.4 Deleting New Powers . . . 151
14.6.5 Viewing All Power Properties . . . 151
14.6.6 Modifying Custom Power Properties . . . 151
14.7 Role Tasks . . . 151
14.7.1 Cloning Roles . . . 152
14.7.2 Creating Roles . . . 152
14.7.3 Deleting Roles . . . 152
14.7.4 Managing Role Assignments . . . 152
14.7.5 Managing Roles and Powers . . . 153
14.7.6 Modifying Role Properties . . . 153

15 Implementing Microsoft Exchange Administration 155

15.1 Understanding Microsoft Exchange Management . . . 155
15.1.1 Managing Mailboxes . . . 155
15.1.2 Managing Distribution Groups . . . 156
15.1.3 Managing Email Addresses . . . 156
15.1.4 Managing Contacts . . . 157
15.1.5 Managing Resource Mailboxes . . . 157
15.1.6 Managing Dynamic Distribution Groups . . . 157
15.2 Managing Environments Containing Multiple Microsoft Exchange Versions . . . 158
15.2.1 Updating and Deleting Mail-Enabled Objects . . . 158
15.2.2 Creating and Updating Mailboxes . . . 159
15.2.3 Moving Mailboxes . . . 159
15.3 How ActiveViews Simplify Microsoft Exchange Management . . . 160
15.3.1 Microsoft Exchange Management Tasks . . . 160

16 Implementing Microsoft Office 365 Exchange Online Administration 161

16.1 Enabling the Online Policy . . . 161
16.2 Creating an Account to Manage Exchange Online . . . 161
16.3 Managing an Office 365 Tenant and Creating a Service Principal . . . 162
16.4 (Optional) Allowing DRA to Manage your Office 365 Licenses . . . 162
16.4.1 Creating a Policy to Enforce Office 365 Licenses . . . 162
16.4.2 Office 365 License Update Schedule . . . 162

17 Customizing the Administration Server 165

17.1 Understanding Administration Server Configuration . . . 165
17.2 Accessing Configuration Management . . . 165
17.3 Using Administration Server Options . . . 166
17.3.1 Encrypted Communications . . . 167
17.3.2 Client Options . . . 167
17.3.3 Resource Cache . . . 168
17.3.4 Domain Configuration . . . 168
17.4 Administration Server Tasks . . . 169
17.4.1 Encrypting Communications between the Administration Server and User Interfaces . . . 169
17.4.2 Enabling AD Printers Collection . . . 169

17.4.3 Setting Client Options . . . 170
17.4.4 Performing an Immediate Resource Cache Refresh . . . 170
17.4.5 Scheduling a Resource Cache Refresh . . . 170
17.4.6 Performing an Immediate Domain Configuration Refresh . . . 171
17.4.7 Scheduling a Domain Configuration Refresh . . . 171
17.5 Managing a Multi-Master Set Environment . . . 171
17.5.1 What Is a Multi-Master Set? . . . 172
17.5.2 Understanding Server Synchronization . . . 173
17.5.3 Maintaining the Multi-Master Set . . . 174
17.5.4 Disaster Recovery and Location Maintenance . . . 174
17.6 Multi-Master Tasks . . . 174
17.6.1 Adding a Secondary Administration Server . . . 175
17.6.2 Demoting a Primary Administration Server . . . 175
17.6.3 Promoting a Secondary Administration Server . . . 175
17.6.4 Removing a Secondary Administration Server . . . 176
17.6.5 Synchronizing a Secondary Server with the Primary Administration Server . . . 176
17.6.6 Configuring a Refresh Schedule for a Secondary Administration Server . . . 177
17.6.7 Synchronizing a Server Set with the Primary Administration Server . . . 177
17.6.8 Viewing Administration Server Properties . . . 178
17.7 Configuring Managed and Trusted Domains . . . 178
17.7.1 Accounts Cache . . . 178
17.7.2 Access Account . . . 181
17.7.3 Last Logon Statistics . . . 181
17.8 Domain Tasks . . . 181
17.8.1 Adding a Managed Domain . . . 181
17.8.2 Adding a Managed Subtree . . . 182
17.8.3 Gathering Last Logon Statistics . . . 183
17.8.4 Performing a Full Accounts Cache Refresh . . . 183
17.8.5 Performing an Incremental Accounts Cache Refresh . . . 184
17.8.6 Removing a Managed Domain . . . 184
17.8.7 Removing a Managed Subtree . . . 185
17.8.8 Scheduling an Incremental Accounts Cache Refresh . . . 185
17.8.9 Specifying Domain Access Accounts . . . 186
17.8.10 Specifying Exchange Access Accounts . . . 186
17.8.11 Viewing Domain Statistics . . . 187
17.8.12 Viewing Last Logon Statistics for a User Account . . . 187
17.8.13 Viewing Trusted Domains . . . 187
17.9 Office 365 Tenant Tasks . . . 187
17.9.1 Adding a Tenant . . . 188
17.9.2 Removing a Tenant . . . 188
17.9.3 Performing an Office 365 Incremental Accounts Cache Refresh . . . 188
17.9.4 Specifying a Tenant Access Account . . . 188

18 Automating Processes 191

18.1 Understanding Automation Triggers . . . 191
18.1.1 What Is an Automation Trigger? . . . 191
18.1.2 How the Administration Server Automates Processes . . . 191
18.1.3 What Is the ADSI Provider? . . . 192
18.2 Accessing Automation Triggers . . . 192
18.3 Using Automation Triggers . . . 193
18.3.1 Defining an Automation Trigger Workflow . . . 193
18.3.2 Creating a New Automation Trigger . . . 193
18.4 Automation Tasks . . . 194
18.4.1 Deleting Automation Triggers . . . 194
18.4.2 Disabling Automation Triggers . . . 194
18.4.3 Enabling Automation Triggers . . . 194
18.4.4 Implementing Automation Triggers . . . 195
18.4.5 Modifying Automation Trigger Properties . . . 195

18.4.6 Writing Automation Trigger Scripts or Executables . . . 196

19 Auditing and Reporting 197

19.1 How DRA Uses Log Archives . . . 197
19.1.1 Enabling and Disabling Windows Event Log Auditing for DRA . . . 197
19.1.2 Ensuring Auditing Integrity . . . 198
19.1.3 Understanding Log Archives . . . 199
19.2 Managing Data Collection for Reporting . . . 201
19.3 Reporting Configuration Tasks . . . 201
19.3.1 Enabling Reporting and Data Collection . . . 201
19.3.2 Configuring the Active Directory Collector . . . 202
19.3.3 Configuring the DRA Collector . . . 202
19.3.4 Configuring the Office 365 Tenant Collector . . . 203
19.3.5 Configuring the Management Reports Collector . . . 203
19.3.6 Viewing the Collectors Status . . . 203

A The Command-Line Interface 205

A.1 Understanding the CLI . . . 205
A.1.1 CLI Syntax . . . 205
A.1.2 Embedded Spaces and Quotes . . . 206
A.1.3 Date and Time Format . . . 206
A.1.4 Wildcard Characters and Naming Restrictions . . . 206
A.1.5 Special Terms . . . 206
A.1.6 Special Functions and Variables . . . 207
A.1.7 Special Operators and Prefixes . . . 208
A.1.8 Return Codes . . . 208
A.2 CLI Commands . . . 209
A.2.1 AA Command . . . 209
A.2.2 ACCOUNT Command . . . 212
A.2.3 AV Command . . . 214
A.2.4 CACHE Command . . . 218
A.2.5 DOMAIN Command . . . 221
A.2.6 EXEC Command . . . 222
A.2.7 GROUP Command . . . 224
A.2.8 INFO Command . . . 228
A.2.9 ROLE Command . . . 229
A.2.10 SERVER Command . . . 231
A.2.11 USER Command . . . 232
A.2.12 WHOAMI Command . . . 240

B Available Utilities 243

B.1 Diagnostic Utility . . . 243
B.1.1 Accessing the Diagnostic Utility . . . 243
B.1.2 Understanding the Diagnostic Information . . . 243
B.1.3 Configuring Log Settings . . . 245
B.1.4 Collecting Diagnostic Information . . . 245
B.1.5 Viewing APJS Diagnostics . . . 246
B.1.6 Viewing Lock Diagnostics . . . 246
B.1.7 Finding Specific Log Files . . . 246
B.2 Deleted Objects Utility . . . 247
B.2.1 Required Permissions for Deleted Objects Utility . . . 247
B.2.2 Syntax for Deleted Objects Utility . . . 247
B.2.3 Options for Deleted Objects Utility . . . 248
B.2.4 Examples for Deleted Objects Utility . . . 248
B.3 Recycle Bin Utility . . . 249

B.3.1 Required Permissions for the Recycle Bin Utility . . . 249
B.3.2 Syntax for Recycle Bin Utility . . . 250
B.3.3 Options for Recycle Bin Utility . . . 250
B.3.4 Examples for Recycle Bin Utility . . . 250

C Custom Powers 251

C.1 Understanding the Custom Powers . . . 251
C.2 Custom Power Properties . . . 251
C.2.1 User . . . 251
C.2.2 Group . . . 254
C.2.3 Dynamic Distribution Group . . . 255
C.2.4 Computer . . . 255
C.2.5 Contact . . . 256
C.2.6 Organizational Unit . . . 256
C.2.7 Published Printer . . . 256
C.2.8 Resource Mailbox . . . 257

D Ports and Protocols Used in DRA Communications 259

E The Pre-DRA 9.0.1 Web Console 263

E.1 Starting the Web Console . . . 263
E.2 Using Quick Start to Solve Issues . . . 263
E.3 Customizing the Web Console . . . 263

About this Book and the Library

The *Administrator Guide* provides conceptual information about the Directory and Resource Administrator (DRA) and Exchange Administrator (ExA) products. This book defines terminology and includes implementation scenarios.

Intended Audience

This book provides information for individuals responsible for understanding administration concepts and implementing a secure, distributed administration model.

Other Information in the Library

The library provides the following information resources:

Installation Guide

Provides detailed planning and installation information.

User Guide

Provides conceptual information about DRA and ExA. This book also provides an overview of the user interfaces and step-by-step guidance for many administration tasks.

Trial Guide

Provides product trial and evaluation instructions and a product tour.

Help

Provides context-sensitive information and step-by-step guidance for common tasks, as well as definitions for each field on each window.

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate — day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with — for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- Identity & Access Governance
- Access Management
- Security Management
- Systems & Application Management
- Workload Management
- Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. The documentation for this product is available on the NetIQ web site in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **comment on this topic** at the bottom of any page in the HTML version of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

NetIQ Communities, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, NetIQ Communities helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit http://community.netiq.com.

1 Introduction

NetIQ Enterprise Administration solutions provide enterprise customers with the ability to safely and securely delegate administrative privileges across their Windows server, Active Directory, Group Policy and Exchange server environments. Combined with detailed auditing of and reporting on administrative activities, NetIQ Enterprise Administration solutions provide organizations with unprecedented levels of accountability while reducing the costs associated with daily operations, internal policy, and regulatory compliance activities.

Organizations have increasingly relied upon Active Directory for the central management of identities and for the authentication and authorization of those identities to the network and IT services. However, assuring the security, availability and integrity of Active Directory requires more than just delegating permissions or changing group memberships. IT Governance and auditors also require proof that policies and procedures are enforced, that changes are tracked, and that administrators are not able to manage beyond the scope of their responsibilities.

NetIQ Directory and Resource Administrator (DRA) delivers an unparalleled ability to control who can manage what within Active Directory while protecting the consistency and integrity of its information by validating all administrative changes. Through granular delegation of permissions, robust change management policies, and automation that simplifies workflows, DRA reduces down time and operational risks to Active Directory that are posed by the consequences of malicious or accidental changes.

NetIQ Exchange Administrator (ExA) extends the powerful features of DRA to provide seamless management of Microsoft Exchange. Through a single, common user interface, ExA delivers policy-based administration for the management of directories, mailboxes and distribution lists across your Microsoft Exchange environment.

Together, DRA and ExA provide the solutions you need to control and manage your Active Directory, Microsoft Windows, and Microsoft Exchange environments.

Key benefits of DRA include:

Policy and regulation compliance

Involves the assessment, operation, and control of systems and resources in accordance with security standards, best practices, and regulatory requirements and provides logging and auditing capabilities that help demonstrate compliance.

Operational integrity

Prevents malicious or incorrect changes that affect the performance and availability of systems and services by providing granular access control for administrators and managing access to systems and resources.

Process enforcement

Maintains the integrity of key change management processes that help you improve productivity, reduce errors, save time, and increase administration efficiency.

1.1 What are DRA and ExA?

DRA and ExA are comprehensive account and resource management products for the key Microsoft identity and messaging platforms, Active Directory and Exchange. Using a flexible, rules-based management model, both DRA and ExA deliver capabilities that streamline administration, increase security, assure operational integrity, and ease the challenges of regulatory compliance for your Active Directory and Microsoft Exchange messaging environments.

An enterprise-scale directory and resource management product, DRA controls and manages Active Directory administration. Its powerful policy-based management, coupled with its safe, distributed administration, dramatically reduces administration efforts and costs. DRA provides increased data security while protecting the integrity of your Active Directory content.

ExA extends the power and flexibility of DRA to include Microsoft Exchange management. Within the context of account administration, you can manage mailboxes, Microsoft Exchange permissions, contacts, and distribution lists. DRA and ExA provide a single, integrated solution for controlling and managing complex IT environments.

1.2 What DRA and ExA Provide

DRA and ExA allow you to manage your enterprise within the context of a dynamic security model. This model ensures that your enterprise management and security remains current as your enterprise changes and evolves.

DRA and ExA provide advanced delegation and robust, policy-based administration features that improve the security and efficiency of your Microsoft Windows environment. They provide a secure, integrated administration solution for the following environments:

Environment	Supported Versions			
Microsoft Windows Server Active Directory	2008	2008 R2	2012	2012 R2
Microsoft Exchange Server	2007	2010	2013	Microsoft Exchange Online

DRA and ExA offer significant flexibility using patented ActiveView technology and granular delegation. An ActiveView is a dynamic set of objects, such as user accounts or computers, that you want an administrator to collectively manage. ActiveViews can include or exclude objects from multiple domains, OUs, and groups into virtual containers for easy administration. With ActiveViews, administrators only sees the objects they can manage, without exposing them to the other objects present across the managed environment.

Granular delegation lets you securely distribute specific tasks, such as resetting a user password or modifying Microsoft Exchange mailbox rights. The flexibility of ActiveViews helps eliminate many of the problems associated with managing data in difficult-to-change, hierarchical structures.

DRA and ExA also help you assure compliance with internal policies and with regulatory requirements. For example, DRA offers dual-key security, so you can require two people to independently confirm portions of the same workflow. You can delegate one administrator to send a user account to the Recycle Bin, and another administrator to review the action and either approve the decision or revoke the change. DRA provides additional reports, logging, and auditing capabilities to help you demonstrate compliance with policies and with regulatory requirements.

With the Web Console, DRA and ExA provide out-of-the-box relief where you want to delegate administrative tasks, but do not want to deploy the product console. For example, you may want employees to manage their personal information, or provide limited privileges to a Help Desk organization. This easy-to-use, task-based interface significantly reduces administration time and lets you securely delegate specific tasks without additional training. You can quickly and easily customize the scope of the administration tasks you want to make available from the Web Console

These technologies seamlessly join and manage data from multiple sources across your enterprise, including Active Directory, Microsoft Exchange, and computer resources. To further expand these benefits, DRA and ExA let you apply policies to directory updates that can extend beyond the directory itself to other applications and databases, making the task of enterprise management easy.

DRA lets you define administration policies that it then automatically propagates and enforces for all DRA users, increasing security and reducing administration costs. This model is dynamic, so as your enterprise changes, objects inherit the appropriate level of security.

DRA and ExA help you automate and streamline many routine administration tasks, such as creating a user account and home share for a new employee. While many automated Active Directory administration tasks are provided out-of-the-box, you can also extend DRA and ExA using well-known standard interfaces such as the Active Directory Service Interfaces (ADSI) and Windows Terminal Server (WTS). DRA and ExA also provide tools, such as automation triggers and the DRA Software Development Kit (SDK), so you can integrate enterprise administration with your current business systems.

DRA supports the 64-bit platform, which provides you with increased scalability, increased performance, reduced query time, and more effective use of memory.

Using state-of-the-art technology, these products provide the features you need to create a more secure, productive, and manageable Active Directory and Microsoft Exchange environment.

1.3 How DRA and ExA Help You

Managing Active Directory and Microsoft Exchange mailboxes offers specific challenges for administrators. You can benefit from using DRA and ExA regardless of where your enterprise is in the Microsoft Windows evolution.

1.3.1 Provide Regulatory Compliance

DRA and ExA provide a number of features to help you maintain compliance with the ever-increasing number of regulations your organization must meet. For example, DRA provides the following features:

Recycle Bin

Holds certain inactive objects, like user accounts, groups, contacts, and computer accounts to meet retention policy requirements and helps restore these objects to their original state.

Dual-Key Tasks

Let you require task confirmation by two independent administrators to complete the action.

Policy Enforcement and Automation

Help you define and enforce change management processes, access control, and auditing.

Naming Convention Enforcement

Controls data entries so they comply with specific conventions you establish and maintain data consistency.

Transform User Tasks

Help you control access to resources, pruning unnecessary permissions and adding appropriate permissions when users in your organization change positions.

By providing granular access control and change management for Microsoft Windows permissions, your organization can document its compliance with regulations that affect your industry.

1.3.2 Maintain Control of Active Directory

Using DRA and ExA, you can reduce the number of privileged accounts and provide much more granular access control for administrators, Help Desk personnel, and even your employees. Tightly managing access and permissions helps protect your Microsoft Windows environment from the risks of power escalation or inadvertent security threats. With over 60 roles and more than 300 granular powers, you can always delegate *who can do what to whom or what* to exactly the right person.

DRA and ExA help you maintain control by logging all administrator actions and presenting information in clear and comprehensive reports. DRA includes logging before and after values of changed properties and stores data in a tamper-resistant, write-once technology that stands up to the rigors of chain of custody processes. This accountability helps you meet internal and external audit goals. The Recycle Bin lets you disable unused objects but store information about them to meet retention policy requirements.

1.3.3 Increase Administration Efficiency

DRA allows you to create and use a management model that reflects how you think and work rather than confining you to an inflexible directory topology. For example, IT planners can use the Delegation and Configuration Console to design a dynamic ActiveView security model and delegate administration to span OUs, domains, trees, or forests.

By providing multiple user interfaces, DRA lets you easily delegate other operations to the correct administrator in your organization. IT administrators can manage the logically grouped user accounts, computers, mailboxes, and resources in their ActiveViews using the Account and Resource Management Console. Help Desk personnel can use the Web Console to manage routine user account and mailbox changes.

The DRA dynamic security and management model and role-based user interfaces help streamline Active Directory management and increase efficiency for every level of administrator in your organization. Because DRA and ExA each support multiple versions of Microsoft Windows and Microsoft Exchange, the products provide a unified administrative interface for your entire Microsoft Windows and Microsoft Exchange environment.

1.3.4 Reduce Administration Costs

Automation and extensibility features make DRA and ExA the perfect choice as you seek ways to reduce administration expense. By automating repetitive and complex tasks and using granular delegation, you can enhance your security efforts, improve regulatory compliance, and distribute account administration duties to reduce costs and improve service.

The following features help you automate, streamline, control, audit, and unify user account, computer, mailbox, and resource administration:

- Automation triggers that automatically perform specific tasks before and after an administrator action is completed

- Support for automated, rules-based provisioning of Active Directory based on external datasources
- Scriptable LDAP-compatible ADSI provider so you can query Active Directory and run scripts to automate your routine processes
- SDK that supports multiple development languages, making customized workflows accessible to most organizations
- Domain controller-directed actions let you unlock accounts or reset passwords in near real time to minimize end-user down time caused by replication delay

DRA and ExA can help you slash administrative costs enforcing business and security policies.

1.3.5 Ensure Data Integrity

Managing any data set that contains inconsistencies creates security risks and may interfere with efficient operations. You can publish naming policies and permission guidelines for different accounts, but users may not remember to follow the guidelines. DRA can automatically enforce your policies, ensuring Active Directory consistency and reducing data clutter. DRA and ExA help enforce best practices for change management, access control, and auditing to help you maintain a trouble-free and consistent Active Directory environment.

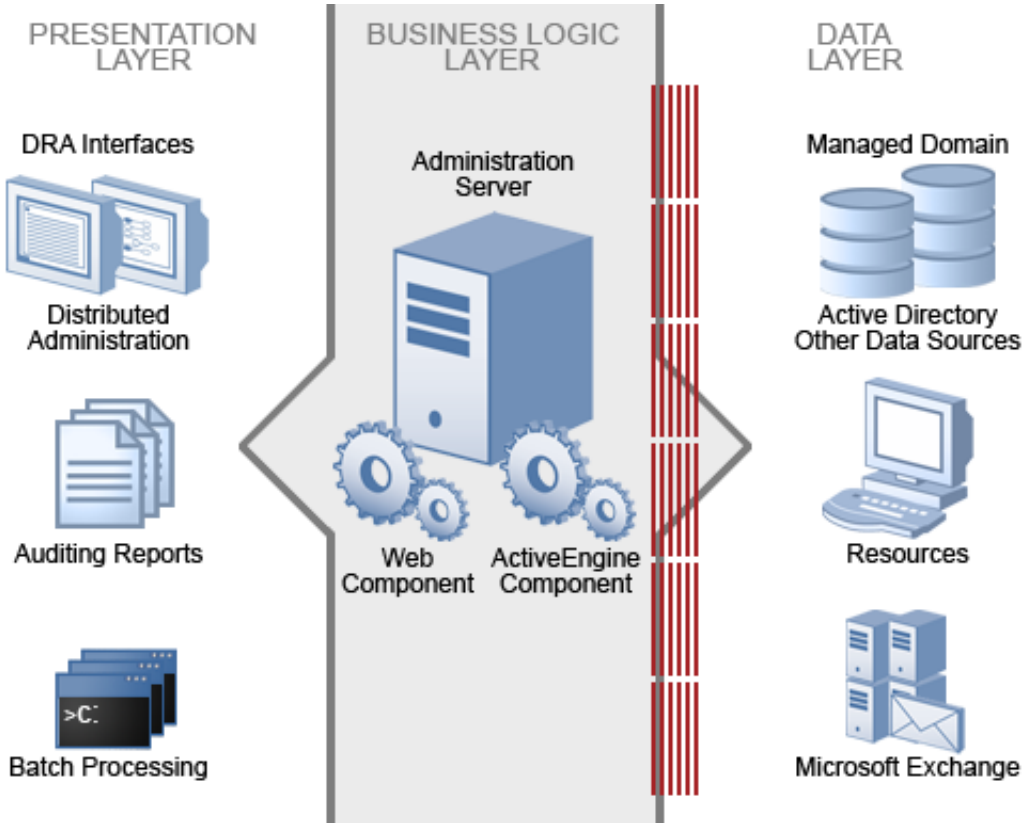
1.4 How DRA and ExA Work

DRA and ExA support several open, extensible standards and services. DRA and ExA include the following user-friendly interfaces for Active Directory and Microsoft Exchange:

- Account and Resource Management Console
- Delegation and Configuration Console
- Web Console
- DRA Reporting (in the DRA consoles and through NetIQ Reporting Center)
- Command-Line Interface (CLI)
- Active Directory Service Interfaces (ADSI)

These products use the same native interfaces as the native Active Directory and Microsoft Exchange administration consoles. Therefore, DRA and ExA are as secure and reliable as Active Directory and Exchange. These products do not modify Active Directory in any way.

DRA and ExA support a three-tiered architecture that efficiently distributes workload into three functional layers, namely the presentation layer, business logic layer, and data layer. Each layer addresses different processes and functions and enables fast performance and reduced network load.



1.4.1 Presentation Layer

The Presentation layer provides a variety of user interfaces to meet various needs, including distributed administration, auditing and reporting, and batch processing across domains. This layer includes the following interfaces:

Delegation and Configuration Console

Allows administrators to define the security model and associated policies, delegate network administration, report on changes, and perform all administration tasks in an object-oriented workflow. This console is intended for full-time system administrators.

Account and Resource Management Console

Allows Help Desk personnel and departmental administrators to perform various day-to-day user administration and provisioning tasks. This console is intended for Help Desk personnel in their primary job function.

Web Console

Allows users to quickly and easily perform common tasks, such as changing an account password or modifying personal information, from a task-based interface. The Web Console is a Web client for Help Desk personnel, data owners, and occasional administrators who perform occasional administration tasks in addition to their primary job functions.

NetIQ Reporting Center Console

Allows administrators to view and deploy Management reports that include activity reports, configuration reports, and summarization reports. Many of these reports can be viewed in a graphical representation.

Command-Line Interface

Allows an administrator to make modifications from the command-line to implement broad administration changes.

DRA ADSI Provider

Allows administrators develop custom user interfaces and applications, as well as custom policy and automation trigger scripts.

1.4.2 Business Logic Layer

The Business Logic layer establishes a virtual firewall, buffering users from direct interaction with the Data layer. This layer performs the central processing and provides information to the user interfaces. The Business Logic layer also manages Web services, business rules and policy, content integrity, embedded best practices, and transactions across data sources in your enterprise.

1.4.3 Administration Server

The Business Logic layer consists of the NetIQ Administration server (Administration server). The Administration server uses transaction processing to identify and authenticate administrators, enforce policy, automate operations, and log all administration activity. To provide fault tolerance, load balancing, and continuous operation, you can install secondary Administration servers on one or more computers.The Administration server runs as a secure Windows service.

This layer includes the following components:

ActiveEngine component

Runs as a service under an administrator account within the Active Directory. The ActiveEngine component accepts requests from multiple clients in the Presentation layer, and then validates and processes these requests. This component interacts with the Data layer components to retrieve or manage the appropriate information.

NetIQ DRA Core

Runs as a service under an administrator account. The NetIQ DRA Core service collects data from Active Directory and DRA for reporting requests. Additionally, the service generates Activity Detail reports when they are requested from clients in the Presentation layer. This service interacts with the Data layer components to retrieve or manage the appropriate information.

Log Archive Service

Runs as a service under an administrator account within the Active Directory. The log archive service tracks all DRA activity, compresses the data, and stores it on the Administration server in a secure, tamper-resistant repository. The service also categorizes the audit events and summarizes events based on these categories.

Web component

Runs on a standard Internet Information Server (IIS) computer to provide administration capabilities across your Intranet. The Web component communicates between the ActiveEngine component and the Web Console. This component is required only if you use the Web Console.

1.4.4 Data Layer

The Data layer comprises every network data source. The Administration server manages data stored in the Active Directory and Microsoft Exchange directory. The Data layer can also include other enterprise data sources, such as a Human Resources database. All these data sources provide important information about your enterprise. When the Administration server receives a request from the Business Logic layer, the server validates this request and allows a client to access and modify this data. This additional layer of authentication ensures that your business data remains protected and secure.

DRA and ExA help you use and manage these data sources. These products also let you define and enforce the business rules and policies that can help you keep these data sources current and correct.

1.5 Supported Environments

DRA and ExA support several different types of environments, including the following installations:

- Managed and trusted domains
- Microsoft Exchange support
- Microsoft Office 365 and Exchange Online support
- Departmental support through managed subtrees
- Multiple Administration servers

You can meet the exact demands of your environment. The power and flexibility of the product architecture allow you to install these products in environments that require special configurations, such as installing the Web component on a separate Web server computer. For more information, see “Installing DRA in Complex Environments” in the *Installation Guide*.

1.5.1 Managed and Trusted Domains

DRA and ExA let you securely administer account and resource objects and Microsoft Exchange mailboxes from multiple managed domains. You can manage Microsoft Windows domains as well as multiple subtrees from specific Microsoft Windows domains. You can also perform the following administration tasks on objects in trusted domains:

- View objects in trusted domains
- Add accounts from trusted domains to groups in your managed domains

For more information about configuring managed and trusted domains, see the *Administrator Guide for Directory Resource Administrator and Exchange Administrator*.

1.5.2 Microsoft Exchange Support

ExA lets you manage the following mailboxes as you manage the associated user accounts, contacts, and groups:

- Microsoft Exchange Server 2007, 2010, and 2013
- Microsoft Exchange Online

You can implement many integrated Microsoft Exchange management features across your enterprise, including the following functions:

- Automatically create, move, and delete mailbox stores when managing accounts
- Automatically generate email addresses based on account naming conventions
- Delegate administration of specific mailbox properties, such as mailbox security settings

ExA supports and extends your security model. By integrating Microsoft Exchange management into your DRA workflow, you save time and money with streamlined administrative processes. For more information about securely managing Microsoft Exchange mailboxes and implementing Microsoft Exchange policy, see the *Administrator Guide for Directory Resource Administrator and Exchange Administrator*.

1.5.3 Departmental Support through Managed Subtrees

Departmental support lets you manage multiple subtrees of specific Microsoft Windows domains. By managing a subtree, you can use DRA to secure a department or division within a larger corporate domain. Departmental support also limits your licensing requirements to only those objects you manage in the subtree.

For example, you can configure DRA to manage the Houston subtree in the Southwest domain. You can control the scope of administration to only those objects contained in the Houston OU and its child OUs. This flexibility lets you manage one or more subtrees without requiring administrative permissions across the entire domain. You can implement departmental support without compromising any of the power and security DRA offers.

For more information about implementing departmental support, see the *Administrator Guide for Directory Resource Administrator and Exchange Administrator*.

1.5.4 Multiple Administration Servers

You can install multiple Administration servers across your managed domain. Called a Multi-Master Set (MMS), these servers help distribute administration loads and provide fault tolerance within a site. Each MMS consists of one primary Administration server and multiple secondary Administration servers.

For example, if the primary Administration server becomes unavailable, secondary Administration servers can fulfill most account and resource administration requests. If you cannot recover an unavailable primary Administration server, or if you need to take the server offline for maintenance, you can promote any secondary Administration server to be the primary Administration server. This flexibility lets you keep important services running.

For more information about Administration servers, see the *Administrator Guide for Directory Resource Administrator and Exchange Administrator*. For more information about implementing an MMS, see “Installing DRA in Complex Environments” in the *Installation Guide*.

2 Working with the User Interfaces

The user interfaces for DRA and ExA address a variety of administration needs. These interfaces include:

Web Console

Allows you to perform common account and resource administration tasks through a Web-based interface. This simple interface allows the occasional administrator to easily perform everyday administration tasks. You can access the Web Console from any computer, iOS device, or Android device running a Web browser.

NOTE: The Web Console was updated with the release of DRA 9.0.1. However, the older version of the Web Console can still be installed and used. For more information about the older Web Console, see Appendix E, “The Pre-DRA 9.0.1 Web Console,” on page 263.

Account and Resource Management Console

Allows you to administer objects in any managed domain. Through the Account and Resource Management console, you can view and modify accounts, resources, temporary group assignments, and Microsoft Exchange mailboxes. This interface addresses enterprise management needs from basic administration to advanced Help Desk issues.

Delegation and Configuration Console

Allows you to securely delegate administrative tasks in the managed domain, set policies and automation triggers, report on real-time changes, and configure the Administration server.

Command-Line Interface

Allows you to perform DRA and ExA operations from the command line. Through the CLI, you can manage multiple objects with a single command and administer batch processes.

REST Services and PowerShell

DRA provides the RESTful interfaces and PowerShell module that allow clients from products other than Directory and Resource Administrator to request DRA operations. To learn how you can develop a client for making DRA requests using .NET managed code or using PowerShell, see the *DRA REST Extensions Technical Reference* that is installed with the REST Services.

User-Developed Interfaces

You can create your own interfaces using the DRA Software Development Kit (SDK). For more information about creating custom applications and user interfaces, see the SDK Help.

NetIQ Reporting Center Console

Allows you to view and deploy Management reports so you can audit your enterprise security and track administration activities. Management reports include activity reports, configuration reports, and summarization reports. Many of these reports can be viewed in a graphical representation.

2.1 Web Console

The Web Console is a Web-based user interface that provides quick and easy access to many user account, group, computer, resource, and Microsoft Exchange mailbox tasks. It is easy to learn and simple to use, which makes it a great tool for occasional or beginning administrators.

2.1.1 Starting the Web Console

You can start the Web Console from any computer, iOS device, or Android device running a Web browser. To start the Console, specify the appropriate URL in your Web browser address field. For example, if you installed the Web component on the HOUserver computer, type `https://HOUserver/draclient` in the address field of your Web browser.

NOTE: To display the most current account and Microsoft Exchange information in the Web Console, set your Web browser to check for newer versions of cached pages at every visit.

2.1.2 Customizing the Web Console

You can quickly and easily customize the Web Console in the following ways:

Modify property pages

You can modify the property page template that is used when creating or editing an object. For example, you can modify the property page for users so that it displaysan additional phone number field,

Modify branding

For example, you can add your comapny's logo to the Web Consoles header.

Create a NetIQ Aegis form

You can create a new form to start an Aegis workflow.

2.1.3 Configuring Windows Authentication

To enable Windows authentication on the Web Console you must configure Internet Information Services (IIS) and the REST services configuration file.

1. Open IIS Manager.
2. In the Connections pane, locate the REST Services web application and select it.
3. In the right pane, go to the IIS section and double-click **Authentication**.
4. Enable **Windows Authentication** and disable all of the other authentication methods.
5. Use a text editor to open the `C:\inetpub\wwwroot\DRAClient\rest\web.config` file and locate the `<authentication mode="None" />` line.
6. Change `"None"` to `"Windows"` and save the file.
7. Restart the IIS server.

2.1.4 Configuring Smart Card Authentication

To configure the web console to accept a user based on the client credentials from his or her smart card you must configure Internet Information Services (IIS) and the REST services configuration file.

IMPORTANT: Make sure the certificates on the smart card are also installed in the root certificate store on the web server because IIS has to be able to find certificates that match those that are on the card.

---

1. Install authentication components on the web server.
   - **1a** Start the Server Manager.
   - **1b** Click **Web Server (IIS)**.
   - **1c** Go to the Role Services section and click **Add Role Services**.
   - **1d** Go to the Security role services node and select **Windows Authentication** and **Client Certificate Mapping Authentication**.
2. Enable authentication on the web server.
   - **2a** Start **IIS Manager**.
   - **2b** Select your web server.
   - **2c** Find the **Authentication** icon under the IIS section and double-click it.
   - **2d** Enable “Active Directory Client Certificate Authentication” and “Windows Authentication”.
3. Configure the DRA client.
   - **3a** Select your DRA client.
   - **3b** Find the **Authentication** icon under the IIS section and double-click it.
   - **3c** Enable “Windows Authentication” and disable “Anonymous Authentication”.
4. Enable SSL and client certificates on the DRA client.
   - **4a** Find the **SSL Services** icon under the IIS section and double-click it.
   - **4b** Select **Require SSL** and select **Require** under Client certificates.

     TIP: If the option is available, select **Require 128-bit SSL**.

     ---
5. Configure the REST services web application.
   - **5a** Select your REST services web application.
   - **5b** Find the **Authentication** icon under the IIS section and double-click it.
   - **5c** Enable “Windows Authentication” and disable “Anonymous Authentication”.
6. Enable SSL and client certificates on the REST services web application.
   - **6a** Find the **SSL Services** icon under the IIS section and double-click it.
   - **6b** Select **Require SSL** and select **Require** under Client certificates.

     TIP: If the option is available, select **Require 128-bit SSL**.

     ---
7. Configure the WCF web service file.
   - **7a** Select your REST services web application and switch to Content View.
   - **7b** Locate the `.svc` file and right-click it.
   - **7c** Select **Switch to Features View**.

7d Find the **Authentication** icon under the IIS section and double-click it.

7e Enable “Anonymous Authentication” and disable all other authentication methods.

8 Edit the REST services configuration file.

8a Use a text editor to open the `C:\inetpub\wwwroot\DRAClient\rest\web.config` file.

8b Locate the `<authentication mode="None" />` line and delete it.

8c Add the following lines below the `<system.serviceModel>` line:

```
<services>
      <service name="NetIQ.DRA.DRARestProxy.RestProxy">
        <endpoint address="" binding="webHttpBinding"
bindingConfiguration="webHttpEndpointBinding"
          name="webHttpEndpoint" contract="NetIQ.DRA.DRARestProxy.IRestProxy" />
      </service>
</services>
```

8d Add the following lines below the `<serviceDebug includeExceptionDetailInFaults="false"/>` line:

```
<serviceAuthorization impersonateCallerForAllOperations="true" />
     <serviceCredentials>
       <clientCertificate>
         <authentication mapClientCertificateToWindowsAccount="true" />
       </clientCertificate>
     </serviceCredentials>
```

8e Add the following lines **above** the `<serviceHostingEnvironment multipleSiteBindingsEnabled="true" />` line:

```
<bindings>
      <webHttpBinding>
        <binding name="webHttpEndpointBinding">
          <security mode="Transport">
            <transport clientCredentialType="Certificate" />
          </security>
        </binding>
      </webHttpBinding>
</bindings>
```

9 Save the file and restart the IIS server.

2.1.5 Configuring Multi-factor Authentication with NetIQ Advanced Authentication Framework

NetIQ Advanced Authentication Framework (NAAF) is our premier software package that lets you move beyond a simple user name and password to a more secure way of protecting your sensitive information—multi-factor authentication.

Multi-factor authentication is a method of computer access control that requires more than one method of authentication from separate categories of credentials to verify a user's identity.

There are three types of authentication categories, or **factors**:

- *Knowledge*. This category requires you to know a specific piece of information, such as a password or activation code.
- *Possession*. This category requires you to have an authenticating device such as a smart card or smartphone.
- *Body*. This category requires you to use a part of your anatomy, such as your fingerprint, as the method of verification.

Each authentication factor contains at least one **authentication method**. An authentication method is a specific technique that you can use to establish a user's identity, such as by using a finger print or requiring a password.

You can consider an authentication process strong if it uses more than one type of authentication method—for instance, if it requires a password and a fingerprint.

NAAF supports the following authetication methods:

- Email
- Emergency Password
- HMAC-based One-time Password (HOTP)
- LDAP password
- Remote Authentication Dial-In User Service (RADIUS)
- Smartphone

  TIP: The Smartphone method requires the user to download an iOS or Android app. For more information, see the *NetIQ Advanced Authentication Framework - Smartphone Applications User Guide*, which is available from the NetIQ Documentation Web site.

- SMS
- Time-based One-time Password (TOTP)
- Voice Call

Use the information in the following sections to configure the Web Console to use multi-factor authentication.

IMPORTANT: While some of the steps in the following sections take place inside the Web Console, the majority of the multi-factor authentication configuration process requires access the NAAF. These procedures assume that you have already installed NAAF and have access to NAAF's help documentation.

Adding Repositories to NetIQ Advanced Authentication Framework

The first step in configuring the Web Console to use multi-factor authentication is to add all of the AD domains that contain the DRA admins and AAs managed by DRA to NAAF. These domains are called **repositories**, and they contain the identity attributes of the users and groups that you want to authenticate.

1. Log in to the NAAF administration portal with an administrator-level username and password.
2. Go to the left panel and click **Repositories**.
3. Click **Add**.
4. Fill out the form.

   TIP: The **LDAP type** is **AD**.

   TIP: Type an administrator-level username and password into the corresponding fields.

5. Click **Add server**.
6. Type the LDAP server's IP address in the **Address** field.
7. Click **Save**.

8 Repeat Steps 3 through 7 for all other AD repositiories managed by DRA.

9 For each repository listed on the Repositories page, click **Sync now** to sync it with the NAAF server.

Creating Authentication Chains

An **authentication chain** contains at least one authentication method. The methods in the chain will be invoked in the order in which they were added to the chain. In order for a user to be authenticated, the user must pass all methods in the chain. For example, you can create a chain that contains the LDAP Password method and the SMS method. When a user tries to authenticate using this chain she must first authenticate using her LDAP Password after which a text message will be sent to her mobile phone with a one-time password. After she enters the password all the methods in the chain will have been fulfilled and the authentication succeeds. An authentication chain can be assigned to a specific user or group.

To create an authentication chain:

1 Log in to the NAAF administration portal with an administrator-level username and password.

2 Go to the left panel and click **Chains**. The right panel displays a list of the currently available chains.

3 Click **Add**.

4 Fill out the form. All fields are required.

IMPORTANT: Add the methods in the order in which they should be invoked—that is, if you want the user to enter an LDAP password first, add LDAP password to the chain first.

IMPORTANT: Make sure the **Apply if used by endpoint owner** switch is OFF.

---

5 Switch **Is enabled** to ON.

6 Type the names of the roles or groups to be subject to the authentication request in to the **Roles & Groups** field.

TIP: If you want the chain to apply to all users type `all users` in to the **Roles & Groups** field and select **All Users** from the resulting drop-down list.

Any user or group that you select will be added beneath the **Roles & Groups** field.

7 Click **Save**.

Creating Authentication Events

An **authentication event** is triggered by an application—in this case, the Web Console—that wants to authenticate a user. At least one authentication chain must be assigned to the event so that when the event is triggered, the methods in the chain associated with the event will be invoked in order to authenticate the user.

An **endpoint** is the actual device—such as a computer or a smartphone—that is running the software that triggers the authentication event. DRA will register the endpoint with NAAF after you create the event.

You can use the Endpoints whitelist box to restrict access to an event to specific endpoints, or you can allow all endpoints to access the event.

To create an authentication event:

1. Log in to the NAAF administration portal with an administrator-level username and password.
2. Go to the left panel and click **Events**. The right panel displays a list of the currently available events.
3. Click **Add**.
4. Fill out the form. All fields are required.

   IMPORTANT: Make sure the **Is enabled** switch is ON.

5. If you want to restrict access to specific endpoints, go to the Endpoints whitelist section and move the targeted endpoints from the *Available* list to the *Used* list.

   TIP: If there are no endpoints in the *Used* list, then the event will be available to all endpoints.

Configuring the Web Console

After you configure chains and events you can log into the Web Console as an administrator and enable NAAF authentication.

Once authentication is enabled, every user will be required to authenticate herself through NAAF before being given access to the Web Console.

IMPORTANT: Before enabling the Web Console you must already be enrolled in the authentication methods that the Web Console will use to authenticate users. See the *NetIQ Advanced Authentication Framework User Guide* to learn how to enroll in authentication methods.

1. Go to the Tasks panel and click **Customize Web Console**.
2. Select **Change Configuration** and then click on the **Advanced Authentication** drop-down arrow.
3. Select **Enabled**.
4. Type the IP address or fully qualified domain name (FQDN) of the NAAF server into the **Service Address** field.
5. Type a name for the endpoint in the **Endpoint Name** field.

   TIP: After you save the configuration, the endpoint will be created in NAAF. To view or edit it, log on to the NAAF administration portal with an administrator-level username and password and click **Endpoints** on the left pane.

6. Type the name of the event that you want to associate with this Web Console. This event will be used to trigger the authentication chain that will be used to authenticate the user.
7. Click **Save**.

Final Steps

1. Log on to the NAAF administration portal with an administrator-level username and password and click **Events** on the left pane.
2. Edit each of the Web Console events:
   - **2a** Open the event for editing.
   - **2b** Go to the Endpoints whitelist section and move the endpoint that you created when you configured the Web Console from the **Available** list to the **Used** list. This will ensure that only the Web Console can use these events.
3. Click **Save**.

2.2 Account and Resource Management Console

The Account and Resource Management console provides access to all tasks, addressing enterprise management needs from basic administration to advanced Help Desk issues. Through the Account and Resource Management console, you can perform all account and resource management tasks and manage Microsoft Exchange mailboxes.

The Account and Resource Management console contains the following nodes:

All My Managed Objects

Allows you to manage objects, such as user accounts, groups, contacts, and resources, for each domain in which you have some power.

Temporary Group Assignments

Allows you to manage group memberships for users who only need group membership for a specific time period.

Advanced Search Queries

Allows you to manage advanced queries available on the Administration server.

Recycle Bin

Allows you to manage deleted user accounts, groups, contacts, and resources, for any Microsoft Windows domain where the Recycle Bin is enabled.

To start the Account and Resource Management console interface, click **Account and Resource Management** in the Directory and Resource Administrator program folder.

When you start the Account and Resource Management console, you initially connect to the best available Administration server in the local domain. The best-available Administration server is the closest server, which is typically a server in the network site. By seeking the best available Administration server, DRA provides a quicker connection and improved performance.

2.3 Delegation and Configuration Console

The Delegation and Configuration console provides access to all configuration and delegation tasks, addressing enterprise management needs from distributed administration to policy enforcement. Through the Delegation and Configuration console, you can set up the security model and server configurations you need to effectively manage your enterprise.

The Delegation and Configuration console contains the following nodes:

Delegation Management

Allows you to implement and maintain your security model by defining and modifying ActiveViews, roles, powers, and Assistant Admin groups.

Policy and Automation Management

Allows you to define policies and create automation triggers. You can define Microsoft Exchange policies, set Home directory rules, and create custom policies.

Configuration Management

Allows you to configure your Administration servers, managed domains, and Office 365 tenants. You can view and modify domain properties, add or remove managed domains, implement user interface extensions, and change the cache refresh schedules for each Administration server. You can create custom tools, manage file replication between Administration servers and DRA client computers, specify clone exceptions to use when cloning user accounts, manage virtual attributes, and manage reporting configuration. You can add or remove Office 365 tenants.

Account and Resource Management

Provides the same administration features available through the Account and Resource Management console.

To start the Delegation and Configuration console interface, click **Delegation and Configuration** in the Directory and Resource Administrator program folder.

To start the Account and Resource Management console interface, click **Account and Resource Management** in the Directory and Resource Administrator program folder. The following sections provide common tasks for the Account and Resource Management console.

When you start the Delegation and Configuration console, you initially connect to the best-available Administration server in the local domain. The best-available Administration server is the closest server, which is typically a server in the network site. By seeking the best available Administration server, DRA provides a quicker connection and improved performance.

2.4 Command-Line Interface

The CLI allows you to access and apply powerful Administration product capabilities using commands or batch files. With the CLI, you can issue one command to implement changes across multiple objects.

For example, if you need to relocate the home directories of 200 employees to a new server, using the CLI, you could enter the following single command to change all 200 user accounts:

```
EA USER @GroupUsers(HOU_SALES),@GroupUsers(HOU_MIS) UPDATE
HOMEDIR:\\HOU2\USERS\@Target()
```

This command directs DRA to change the home directory field of each of the 200 user accounts in the HOU_SALES and HOU_MIS groups to \\HOU2\USERS*user_id*. To accomplish this task with the native Microsoft Windows administration tools, you would need to perform a minimum of 200 separate actions. For more information about the CLI, see Appendix A, “The Command-Line Interface,” on page 205.

2.5 Licensing Affects Available Features

Your license key file determines which DRA and ExA functions you can use. For example, you need a license key file for DRA to create a new user account. Your license key file can also support ExA. The license key file defines an expiration date, a grace period, the number of user accounts you can manage with your current DRA and ExA license. When you reach the license grace period, the Administration server displays warning messages in the DRA console. After the grace period expires, DRA no longer allows you to connect to a DRA server. For more information about licensing, see the *NetIQ Directory and Resource Administrator and Exchange Administrator Installation Guide*.

2.6 Customizing and Extending the User Interface

You can customize and extend the DRA consoles by implementing user interface extensions. User interface extensions allow you to add proprietary account and OU properties, such as Active Directory schema extensions and virtual attributes, to specific wizards and property windows. These extensions allow you to customize DRA to meet your specific requirements. Using the New Custom Page wizard in the Delegation and Configuration console, you can quickly and easily create a custom page to extend the appropriate user interface.

If your AAs require unique powers to securely manage the custom page, you can also create and delegate custom powers. For example, you may want to limit user account management to properties on the custom page only. For more information, see Section 14.1.3, “Understanding Power Creation,” on page 136.

2.6.1 How User Interface Extensions Work

User interface extensions are custom pages DRA displays in the appropriate wizard and properties windows. You can configure custom pages to expose Active Directory attributes, schema extensions, and virtual attributes in the Delegation and Configuration console and the Account and Resource Management console.

When you select any supported Active Directory attribute, schema extension, or virtual attribute, you can use custom pages in the following ways:

- Limit AAs to manage a well-defined and controlled set of properties. This property set can include *standard properties* and schema extensions. Standard properties are Active Directory attributes exposed by default through the Accounts and Resource Management console.
- Expose Active Directory attributes other than the standard properties managed by DRA.
- Extend the Account and Resource Management console and Delegation and Configuration console to include proprietary properties.

You can also configure how DRA displays and applies these properties. For example, you can define user interface controls with default property values.

DRA applies custom pages to all applicable managed objects in your enterprise. For example, if you create a custom page to add Active Directory schema extensions to the Group Properties window, DRA applies the properties on this page to each managed group in a domain supporting the specified schema extensions. Each custom page requires a unique set of properties. You cannot add an Active Directory attribute to more than one custom page.

You cannot disable individual windows or tabs in the existing user interface. An AA can select a property value using either the default user interface or a custom page. DRA applies the most recently selected value for a property.

DRA provides a full audit trail for user interface extensions. DRA logs the following data to the Application event log:

- Changes to custom pages

  IMPORTANT: AAs must manually configure Windows Application Log Auditing. See "How do I re-enable DRA to write events to the Application Event log in DRA 8.5 and later?"

- Creation and deletion of custom pages
- Exposed schema extension, Active Directory attributes, and virtual attributes included on custom pages

You can also run change activity reports to monitor configuration changes for the user interface extensions.

Implement and modify user interface extensions (custom pages) from the primary Administration server. During synchronization, DRA replicates user interface extension configurations across the Multi-Master Set. For more information, see Section 17.5, "Managing a Multi-Master Set Environment," on page 171.

2.6.2 Supported Custom Pages

Each custom page you create allows you to select a set of Active Directory properties, schema extensions, or virtual attributes and expose these properties as a custom tab. You can create the following types of custom pages:

Custom User Page

Allows you to display custom tabs in the following windows:

- User Properties window
- Create User wizard
- Clone User wizard

Custom Group Page

Allows you to display custom tabs in the following windows:

- Group Properties window
- Create Group wizard
- Clone Group wizard

Custom Computer Page

Allows you to display custom tabs in the following windows:

- Computer Properties window
- Create Computer wizard

Custom Contact Page

Allows you to display custom tabs in the following windows:

- Contact Properties window
- Create Contact wizard
- Clone Contact wizard

Custom OU Page

Allows you to display custom tabs in the following windows:

- OU Properties window
- Create OU wizard
- Clone OU wizard

Custom Resource Mailbox Page

Allows you to display custom tabs in the following windows:

- Resource Mailbox Properties window
- Create Resource Mailbox wizard
- Clone Resource Mailbox wizard

Custom Dynamic Distribution Group Page

Allows you to display custom tabs in the following windows:

- Dynamic Distribution Group Properties window
- Create Dynamic Distribution Group wizard
- Clone Dynamic Distribution Group wizard

2.6.3 Supported User Interface Controls

When you add an Active Directory attribute, schema extension, or virtual attribute to a custom page, you also configure the user interface control with which an AA inputs the property value. For example, you can specify property values in the following ways:

- Define specific value ranges
- Set default property values
- Indicate whether a property is required

You can also configure the user interface control to display proprietary information or instructions. For example, if you define a specific range for an employee identification number, you can configure the text box control label to display **Specify employee identification number (001 to 100)**.

Each user interface control provides support for a single Active Directory attribute, schema extension, or virtual attribute. Configure the following user interface controls based on the property type:

Type of Active Directory attribute	Supported User Interface Controls
Boolean	Check box
Date	Calendar control
Integer	Text box (default) Selection list

Type of Active Directory attribute	Supported User Interface Controls
String	Text box (default) Selection list Object selector
Multivalued String	Selection list

2.6.4 Accessing the User Interface Extensions Node

Use the User Interface Extensions node to define and maintain your custom pages. You can access the User Interface Extensions node from the console tree.

To access User Interface Extensions through the console tree:

1. In the left pane, expand **Directory and Resource Administrator**.
2. Expand **Configuration Management**, and then click **User Interface Extensions**.

2.6.5 Implementing User Interface Extensions

User interface extensions, such as custom pages, allow you to extend and customize the user interface. For each customization you want to configure, create a custom page and assign the appropriate power or role to the AA.

To implement user interface extensions:

1. To ensure DRA recognizes your Active Directory attributes, schema extension attributes, or virtual attributes, restart the NetIQ Administration Service service on each Administration server.
2. Identify the type of custom page you want to create and the properties you want AAs to manage with this custom page. You can select any Active Directory attribute, including schema extension attributes and attributes in existing DRA wizards and property windows or any virtual attribute you create. However, each custom page requires a unique set of properties. You cannot add an Active Directory attribute to more than one custom page.

   Custom pages do not replace the existing user interface. For more information, see Section 2.6.1, “How User Interface Extensions Work,” on page 36 and Section 2.6.2, “Supported Custom Pages,” on page 37.
3. Determine how you want AAs to specify these properties. For example, you may want to limit a specified property to three possible values. You can define an appropriate user interface control for each property. For more information, see Section 2.6.3, “Supported User Interface Controls,” on page 38.
4. Determine whether your AAs need proprietary information or instructions to successfully manage these properties. For example, determine whether Active Directory requires a syntax for the property value, such as a distinguished name (DN) or an LDAP path.
5. Identify the order in which these properties should display on the custom page. You can change the display order at any time.
6. Determine how DRA should use this custom page. For example, you can add a user custom page to the New User wizard and the User Properties window.
7. Using your answers from Step 1 on page 39Step 5 on page 39, create the appropriate custom pages. For more information, see Section 2.6.6, “Creating User Interface Extensions,” on page 40.

8 Determine whether your AAs need a custom power to manage the properties on this page. For example, if you add a custom page to the User Properties window, delegating the Modify All User Properties power may give an AA too much power. Create any custom powers needed to implement your custom page. For more information, see Section 14.1.3, “Understanding Power Creation,” on page 136.

9 Use the Assignments tab on the AA details pane to verify that your AAs have the appropriate powers for the correct set of objects. For more information, see Section 14.5.9, “Viewing Powers and Roles Assigned to an Assistant Admin,” on page 149. If you created custom powers for this custom page, delegate those powers to the appropriate AAs.

10 Distribute information about the user interface extensions you implemented to the appropriate AAs, such as your Help Desk.

To implement user interface extensions, you must have the powers included in the DRA Administration role. For more information about custom pages, see Section 2.6.1, “How User Interface Extensions Work,” on page 36.

2.6.6 Creating User Interface Extensions

You can create different user interface extensions by creating different custom pages. By default, new custom pages are enabled.

When you create a custom page, you can disable it. Disabling a custom page hides it from the user interface. If you are creating multiple custom pages, you may want to disable the pages until your customizations are tested and complete.

NOTE: Computer accounts inherit Active Directory attributes from user accounts. If you extend your Active Directory schema to include additional attributes for user accounts, you can select these attributes when you create a custom page to manage computer accounts.

To create a user interface extension:

1 In the left pane, expand **Directory and Resource Administrator**.

2 Expand **Configuration Management**, and then click **User Interface Extensions**.

3 On the Task menu, click **New**, and then click the appropriate menu item for the custom page you want to create. For example, to create a custom page for the Computer Properties window, click **New > Computer Page**.

4 On the General tab, type the name of this custom page, and then click **OK**. If you want to disable this page, clear the **Enabled** check box.

5 For each property you want to include on this custom page, complete the following steps:

5a On the Properties tab, click **Add**.

5b To select a property, click **Browse**.

5c In the **Control label** field, type the property name DRA should use as the label for the user interface control. Ensure the control label is user-friendly and highly descriptive. You can also include instructions, valid value ranges, and syntax examples.

5d Select the appropriate user interface control from the **Control type** menu.

5e Select where in the Account and Resource Management console you want DRA to display this custom page.

5f To specify additional attributes, such as minimum length or default values, click **Advanced**.

5g Click **OK**.

6 To change the order in which DRA displays these properties on the custom page, select the appropriate property, and then click **Move Up** or **Move Down**.

7 Click **OK**.

2.6.7 Modifying User Interface Extension Properties

You can change a custom page by modifying the user interface extension properties.

To modify user interface extension properties:

1 In the left pane, expand **Directory and Resource Administrator**.

2 Expand **Configuration Management**, and then click **User Interface Extensions**.

3 In the list pane, select the appropriate user interface extension.

4 On the Tasks menu, click **Properties**.

5 Modify the appropriate properties and settings for this custom page.

6 Click **OK**.

2.6.8 Identifying Active Directory Attributes Managed With User Interface Extensions

You can quickly identify which Active Directory properties, schema extensions, or virtual attributes are managed using a particular user interface extension.

To identify Active Directory properties managed using user interface extensions:

1 In the left pane, expand **Directory and Resource Administrator**.

2 Expand **Configuration Management**, and then click **User Interface Extensions**.

3 In the list pane, select the appropriate user interface extension.

4 In the details pane, click the **Properties** tab. To view the details pane, click **Details** on the View menu.

5 To verify how DRA displays and applies a property, select the appropriate Active Directory attribute, schema extension, or virtual attribute from the list, and then click the **Properties** icon.

2.6.9 Enabling User Interface Extensions

When you enable a user interface extension, DRA adds this custom page to the associated wizards and windows. To specify which wizards and windows display a custom page, modify the user interface extension properties.

NOTE: To ensure each custom page exposes a unique set of properties, DRA does not enable custom pages that contain properties exposed on other custom pages.

To enable a user interface extension:

1 In the left pane, expand **Directory and Resource Administrator**.

2 Expand **Configuration Management**, and then click **User Interface Extensions**.

3 In the list pane, select the appropriate user interface extension.

4 On the Tasks menu, click **Enable**.

2.6.10 Disabling User Interface Extensions

When you disable a user interface extension, DRA removes the custom page from the associated wizards and windows. DRA does not delete the custom page. To ensure a custom page never displays in the user interface, delete the user interface extension.

To disable a user interface extension:

1. In the left pane, expand **Directory and Resource Administrator**.
2. Expand **Configuration Management**, and then click **User Interface Extensions**.
3. In the list pane, select the appropriate user interface extension.
4. On the Tasks menu, click **Disable**.

2.6.11 Deleting User Interface Extensions

When you delete a user interface extension, DRA removes the custom page from the associated wizards and windows. You cannot restore a deleted custom page. To temporarily remove a custom page from the user interface, disable the user interface extension. For more information, see Section 2.6.10, “Disabling User Interface Extensions,” on page 42.

To delete a user interface extension:

1. In the left pane, expand **Directory and Resource Administrator**.
2. Expand **Configuration Management**, and then click **User Interface Extensions**.
3. In the list pane, select the appropriate user interface extension.
4. On the Tasks menu, click **Delete**.

2.7 User Interface Tasks

You can perform the following common user interface tasks. Most user interface tasks can be performed in the Account and Resource Management console and the Delegation and Configuration console.

2.7.1 Automatically Logging in to the Web Console with Internet Explorer

If you intend to support Windows Authentication, you can also configure Internet Explorer to automatically log you into the Web Console by using the credentials you supplied when logging on to your computer.

To enable automatic login:

1. Start Internet Explorer.
2. On the Tools menu, click **Internet Options**.
3. On the Security tab, select **Local internet**, and then click **Custom Level**.
4. Find the User Authentication section and select **Automatic logon only in Intranet zone**, and then click **OK**.
5. Click **Sites** and then click **Advanced**.
6. Type the Web Console’s URL in the **Add this website to the zone** field, and then click **Add**.

7 Click **Close** and then click **OK**.

8 Click **OK** to close the Internet Options dialog.

2.7.2 Accessing a User's Change History

You can use the Web Console to view a history of the changes made to or by a user. You can view the following types of changes:

- Changes made by the user
- Changes made to the user
- User mailboxes created by the user
- User mailboxes deleted by the user
- Group and contact email addresses established by the user
- Group and contact email addresses deleted by the user
- Virtual attributes created or disabled by the user
- Objects moved by the user

To view or generate the Change History report:

1 Start the Web Console.

2 Search for the object whose history you want to view.

3 Click the **View Change History Reports** icon.

4 To change the report ceneration criteria, click **Modify**.

You can change the start or end dates, the object being tracked, the report type, and other criteria.

5 To create a CSV file of the report, click **Generate**.

2.7.3 Connecting to an Administration Server

By default, DRA connects to the best available Administration server for a managed domain or computer. The best available Administration server is the closest server, which is typically a server in the network site. If the site does not include an Administration server, DRA connects to the first available server in the managed domain or managed subtree. However, you can specify the Administration server to which you want to connect.

The best-available Administration server is the closest server, which is typically a server in the network site. If the site does not include an Administration server, DRA connects to the next available server in the managed domain or managed subtree. You can also specify the Administration server to which you want to connect.

When you first start the user interfaces, DRA initially connects to the domain of your logon account. If you are logged on to a domain that is not managed by an Administration server, or if DRA cannot connect to the Administration server for that domain, DRA may display an error message. Ensure the Administration server is available and try again.

To connect to an Administration server:

1 On the File menu, click **Connect to DRA server**.

2 Click **Connect to this DRA server**.

3 Type the name of the Administration server, using the following format: *computername*.

4 Click **OK**.

2.7.4 Connecting to a Managed Domain or Computer

By default, DRA connects to a managed domain or computer through the best available Administration server. The best available Administration server is the closest server, which is typically a server in the network site. If the site does not include an Administration server, DRA connects to the first available server in the managed domain or managed subtree. However, you can specify the domain or computer to which you want to connect. You can also specify which Administration server you want DRA to use.

By default, the Account and Resource Management console connects to a managed domain or computer by using the best-available Administration server. The best-available Administration server is the closest server, which is typically a server in the network site. If the site does not include an Administration server, DRA connects to one of the servers managing the domain of the client computer. However, you can specify the domain or computer to which you want to connect. You can also specify which Administration server you want DRA to use.

When you first start the user interfaces, DRA initially connects to the domain of your logon account. If you attempt to log on to a domain or computer that is not managed by an Administration server, or if DRA cannot connect to the Administration server for your managed domain or computer, DRA may display an error message. Ensure the Administration server is available and try again.

To connect to a managed domain or computer:

1 On the File menu, click **Connect to DRA server**.

2 Select the appropriate option, and then type the name of the managed domain or computer.

3 For example, to connect to the HOULAB domain, click C**onnect to a DRA server that manages this domain**, and then type `HOULAB`.

4 To specify an Administration server for the managed domain or computer, click **Advanced**, and then select the appropriate option.

5 Click **OK**.

2.7.5 Modifying the Console Title

You can modify the information displayed in the title bar of both the Delegation and Configuration console and the Account and Resource Management console. For convenience and clarity, you can add the user name with which the console was launched and the Administration server to which the console is connected. In complex environments in which you need to connect to multiple Administration servers using different credentials, this feature helps you quickly discern which console you need to use.

To modify the console title bar:

1 Start the Account and Resource Management console.

2 Click **View > Options**.

3 Select the Window Title tab.

4 Specify the appropriate options, and then click **OK**. For more information, click the **?** icon.

2.7.6 Customizing List Columns

You can select which object properties DRA displays in list columns. This flexible feature allows you to customize the user interface, such as lists for search results, to better meet the specific demands of administrating your enterprise. For example, you can set columns to display the user logon name or group type, letting you quickly and effectively find and sort the data you need.

To customize list columns:

1. Select the appropriate node. For example, to choose which columns display when viewing search results on managed objects, select **All My Managed Objects**.
2. On the View menu, click **Choose Columns**.
3. From the list of properties available for this node, select the object properties you want to show.
4. To change the column order, select a column, and then click **Move Up** or **Move Down**.
5. To specify the column width, select a column, and then type the appropriate number of pixels in the provided field.
6. Click **OK**.

2.7.7 Using Custom Tools

DRA enables you to seamlessly integrate the DRA interface with other products by using the custom tools feature. Using custom tools, you can execute external applications, launch scripts, open a web page, and enter parameters for any object from within the DRA interface. For example, if you select a computer in your domain, you can launch any of the custom tools defined and enabled for computers by your DRA Administrator.

To use custom tools:

1. Start the Account and Resource Management console.
2. In the left pane, expand **All My Managed Objects**.
3. To specify the object for which you want to use the custom tool, complete the following steps:
   - **3a** ***If you know the object location***, select the domain and OU that contains this object.
   - **3b** In the search pane, specify the object attributes, and then click **Find Now**.
   - **3c** In the list pane, select the appropriate object.
4. On the Tasks menu, click **Custom Tools**.

   NOTE: When you try to select custom tools for an object, if DRA does not display any custom tools for that object, it implies your DRA administrator has not enabled custom tools for that object.

   ---

5. Select the appropriate custom tool.

2.7.8 Executing Saved Advanced Queries

Using advanced queries, you can search for users, contacts, groups, computers, printers, OUs, and any other object that DRA supports. If you have the Execute Saved Advanced Queries power, you can execute advanced queries available in the **Saved Queries** list for any container in the Account and Resource Management console. For more information about your assigned powers, see Section 2.7.18, “Viewing Your Assigned Powers and Roles,” on page 51.

To execute saved advanced queries:

1. Start the Account and Resource Management console.
2. In the left pane, expand **All My Managed Objects**.
3. Select the appropriate container. For example, if you want DRA to search for user account information, select **Users**.
4. To view the advanced search pane, click **Advanced Search**.
5. In the advanced search pane, select an advanced query from the **Saved Queries** list.
6. Click **Load Query**, and then click **Find Now**.

2.7.9 Enabling Collection of Application Logs

To enable collection of application logs, you can install Dr. Watson to gather debugging information about applications you run on the Administration server computer. The Administration server uses this data to create logs for the Diagnostic Utility.

DRA provides a Diagnostic Utility to gather important data about your environment. For more information, see Section B.1, “Diagnostic Utility,” on page 243.

To enable collection of application logs:

1. Log on with an administrator account to the Administration server computer.
2. On the Start menu, open the Command Prompt window.
3. At the command prompt, enter `DrWtsn32 -i`.
4. Click **OK**.
5. Repeat Steps Step 1 on page 46 through Step 4 on page 46 on each Administration server computer.

2.7.10 Reporting on Object Changes

You can view real-time change information for objects in your domains by generating Activity Detail reports. For example, you can view a list of changes made to an object or by an object during a specified time period. You can also export and print Activity Detail reports.

To report on object changes:

1. Find the objects that match your criteria.
2. Right-click on an object, and select **Reporting > Changes made to objectName** or **Reporting > Changes made by objectName**.
3. Select the start and end dates to specify the changes you want to view.
4. ***If you want to change the number of rows to be displayed***, type a number over the default value of 250.

NOTE: The number of rows displayed applies to each Administration server in your environment. If you include 3 Administration servers in the report and use the default value of 250 rows to display, up to 750 rows can be displayed in the report.

5 ***If you want to include only specific Administration servers in the report***, select **Restrict query to these DRA servers** and type the server name or names you want the report to include. Separate multiple server names with commas.

6 Click **OK**.

2.7.11 Reporting on Object Lists

You can export or print data from object lists. With this feature, you can quickly and easily report on and distribute general information about your managed objects.

When you export an object list, you can specify the file location, name, and format. DRA supports HTML, CSV, and XML formats, so you can export this information to database applications or post list results to a Web page

NOTE: You can also select multiple items in a list and then copy these items to a text application, such as Notepad.

To report on object lists:

1 Find the objects that match your criteria.

2 To export this object list, click **Export List** on the File menu.

3 To print this object list, click **Print List** on the File menu.

4 Specify the appropriate information to save or print this list.

2.7.12 Reporting on Object Details

You can export or print data from details tabs that list object attributes, such as group memberships. With this feature, you can quickly and easily report on and distribute frequently needed details about specific objects.

When you export an object details tab, you can specify the file location, name, and format. DRA supports HTML, CSV, and XML formats, so you can export this information to database applications or post list results to a Web page.

To report on object details:

1 Find the object that matches your criteria.

2 On the View menu, click **Details**.

3 In the details pane, select the appropriate tab.

4 To export these object details, click **Export Details** List on the File menu.

5 To print these object details, click **Print Details List** on the File menu.

6 Specify the appropriate information to save or print this list.

2.7.13 Saving Console Windows

By saving the Account and Resource Management console window, you can quickly create a custom user interface that includes your specific settings. You can save different window configurations to different files, preserving specific console settings for your unique administration needs.

To save your console window, click **Save** on the File menu.

2.7.14 Saving Custom Console Files

By saving the Account and Resource Management console window, you can quickly create a custom user interface that includes your specific settings. You can save different window configurations to different files, preserving specific console settings for your unique administration needs.

To save your console window, click **Save** on the File menu.

2.7.15 Restoring Console Settings

DRA allows you to resize windows and persists your window sizes. DRA also persists many other settings, including the last Administration server to which you connect, the columns you add or remove from list results, and column widths. If you want to restore these settings to the original setting with which you installed DRA, the Restore Default Settings option allows you to do so.

To restore default console settings:

1. Start the appropriate console.
2. Click **View > Options**.
3. Select the Saved Settings tab.
4. Review the information provided on the window, and then click **Restore Default Settings**. For more information, click the **?** icon.

2.7.16 Using Special Characters

You cannot use the following special characters when naming user accounts, groups, contacts, OUs, computers, ActiveViews, AA groups, roles, policies, or automation triggers. These naming restrictions apply to the name of the object as well as the name of the rule that defines the object.

Naming user accounts, groups, and computers

When specifying a pre-Windows 2000 name, you cannot use the following special characters:

Backslash	\
Colon	
Comma	,
Double quote	"
Equal sign	=
Forward slash	/
Greater than	>
Left bracket	[
Less than	<
Plus sign	+
Right bracket	]
Semi colon	;
Vertical bar	|

When naming user accounts, groups, and computers in Microsoft Windows domains, you can use any special character.

Managing groups through the Web Console

When managing a Microsoft Windows domain, the Web Console does not support managing groups whose names contain the following special characters:

- Comma ,
- Double quote "
- Forward slash /

Naming contacts and OUs

When naming contacts and OUs, you can use any special character.

Naming ActiveViews, AA groups, and roles

When naming ActiveViews, AA groups, and roles, you cannot use the backslash (\).

Naming policies and automation triggers

When naming policies and automation triggers, you cannot use the backslash (\).

Invalid Characters in Office 365 Mailboxes

Invalid characters will cause the synchronization between Office 365 and your on-premises directory to fail. See the "Directory object and attribute preparation" subtopic on the Microsoft Office support web site to learn more about these invalid characters.

To ensure that these characters are not used in your online mailbox properties, go to the Policy and Automation Management console and click **Configure Exchange Policies**. Click **Office 365 Rules**, click **Enforce online mailbox policies for invalid characters and character length**, and click **OK**.

You can include wildcard characters (`*, ?, and #`) when naming Microsoft Windows objects. Use wildcard characters when creating rules to narrow or broaden the context of a rule.

2.7.17 Using Wildcard Characters

DRA and ExA support wildcard characters in many fields in the DRA consoles and in CLI commands. Wildcards allow you to define rules that match multiple objects to a specific condition or standard, such as a naming convention. You can use wildcards instead of regular expressions to narrow or broaden the scope of the rule. Wildcard matching is not case-sensitive. You can also use the question mark (?), asterisk (*), or number sign (#) wildcard characters as normal characters by prefixing a backslash (\) to the particular wildcard character. For example, to search for `abc*`, type the search text `abc\*`.

DRA and ExA support the following wildcard characters. You cannot use wildcard characters in names.

Match Item	Character	Definition
Any character	Question mark ?	Matches exactly one character
Any digit	Number sign #	Matches one digit
Any character, 0 or more matches	Asterisk *	Matches zero or more characters

The following table provides examples of wildcard character specifications and what they match and do not match.

Example	Matches	Does Not Match
Den???	Denton and Dennis	Denison
El ????o	El Campo and El Indio	El Paso
Houston, TX #####	Houston, TX 77024	Houston, TX USOFA

DRA and ExA do not support wildcard specifications that contain logical operations.

2.7.18 Viewing Your Assigned Powers and Roles

Roles and powers define how you manage objects. A role is a set of powers that provides the permissions required to perform a specific administration task, such as creating a user account or moving shared directories.

The DRA Admin assigns roles, adds you to specific AA groups, and associates you with ActiveViews (sets of domain objects you can manage). You can view these assignments through the Account and Resource Management console and the Delegation and Configuration console. You do not need any auxiliary powers to view the roles and powers assigned to you.

For more information about the DRA security model, see the *Administrator Guide for Directory and Resource Administrator and Exchange Administrator*.

To view your assigned powers and roles:

1. On the File menu, click **DRA Properties**.
2. Click **Powers**.
3. Select the appropriate view. For example, click **Flat View** to see a table of your AA group memberships, assigned powers and roles, and associated ActiveViews.
4. Expand the appropriate item. For example, under **Has Power** column, expand **Roles and Powers** to view the individual roles or powers assigned to you.
5. Click **OK**.

2.7.19 Viewing the Product Version Number and Installed Hotfixes

You can view the product version number and installed hotfixes from the DRA Properties window. This window provides version numbers and lists of installed hotfixes for the Administration server and the DRA client computer.

To view the product version number and installed hotfixes:

1. On the File menu, click **DRA Properties**.
2. Click **General**.
3. View the information you need. For more information about a particular field, click the **?** icon.
4. Click **OK**.

2.7.20 Viewing Your Current License

DRA and ExA require a license key file. You can view your product license from any Administration server computer. You do not need any auxiliary powers to view the product license.

To view your license:

1. On the File menu, click **DRA Properties**.
2. Click **License**.
3. Review the license properties, and then click **OK**.

2.7.21 Upgrading Your License

DRA and ExA require a license key file. This license key file contains your license information. DRA installs the license key file on the Administration server. When you install the Administration server, the setup program allows you to use the default (trial) license key file or a production license key file (`CustomLicense.lic`) provided for you by NetIQ Corporation. As your administration needs change, you can upgrade your license to accommodate your new requirements.

NOTE

- If you are upgrading your DRA installation, ensure you schedule your upgrade during off-peak hours.
- If you are using multiple Administration servers, you must upgrade your license key file on the primary Administration server and all secondary Administration servers.
- Close all open applications on the Administration server you are upgrading before you start the setup program.

To upgrade your license:

1. Start the DRA Delegation and Configuration console and click **Configuration Management** on the left pane.
2. On the right pane, click **Update License**.
3. Browse to and select your license key and click **OK**.
4. Click **OK** to reconnect to the Administration server.

NOTE

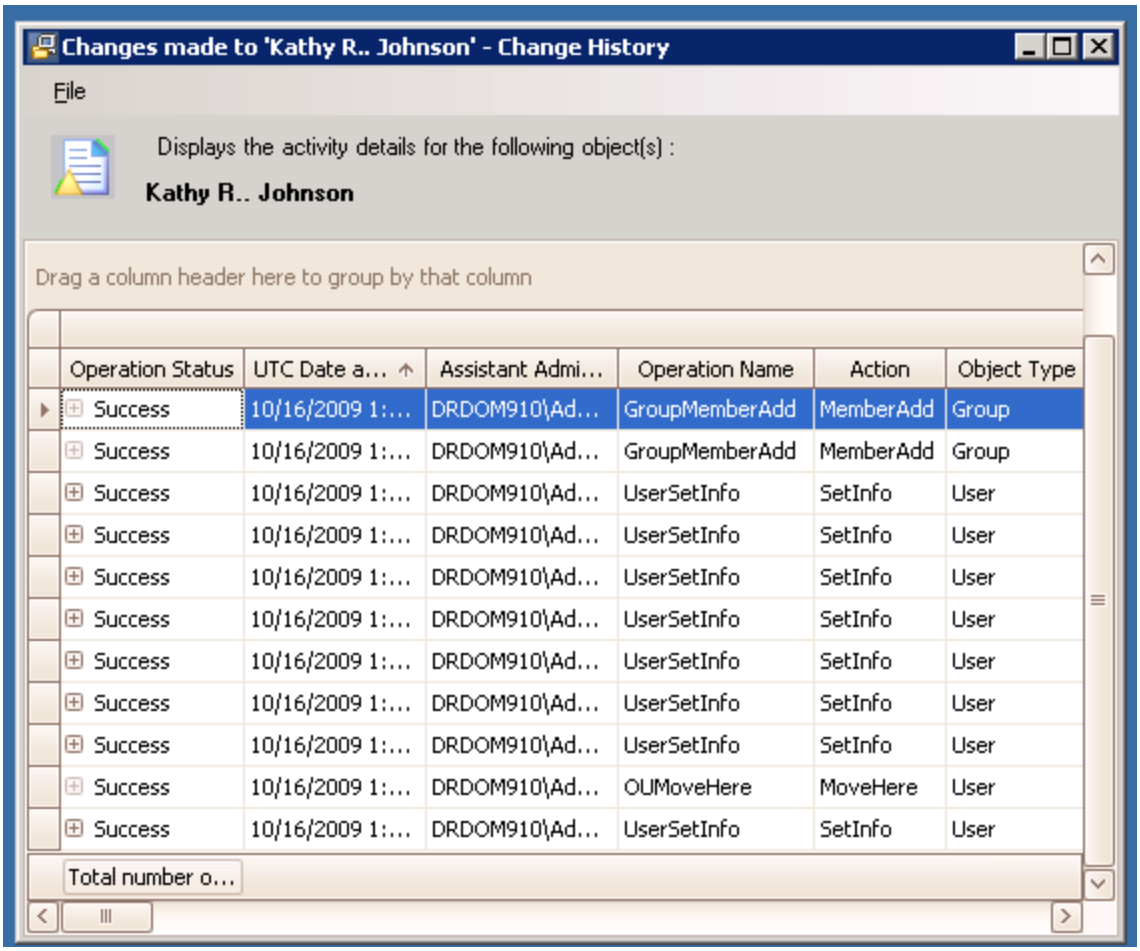
- If you are using a trial license and upgrading to a production license, DRA will replace your trial license with your production license.
- If you are using a production license and upgrading to a new production license, DRA will add your new production license to your existing production license.
- If you are using an existing trial license and you would like to extend your trial license please contact your NetIQ sales representative or an authorized NetIQ reseller or partner to obtain a new trial license.

2.8 DRA Reporting

DRA Reporting provides built-in, ready-to-use reports that let you quickly track duplicate accounts, last account logons, Microsoft Exchange mailbox details, and much more. Reporting also provides real-time details of changes made in your environment, including before and after values for changed properties. You can export, print, or view reports, or publish them to SQL Server Reporting Services.

Directory and Resource Administrator provides two methods of generating reports that allow you to collect and review user account, group, and resource definitions in your domain. **Activity Detail reports**, viewed through the Delegation and Configuration console, provide real-time change information for objects in your domain. For example, you can view a list of changes made to an object or by an object during a specified time period using Activity Detail reports.

The following figure shows a sample Activity Detail report:



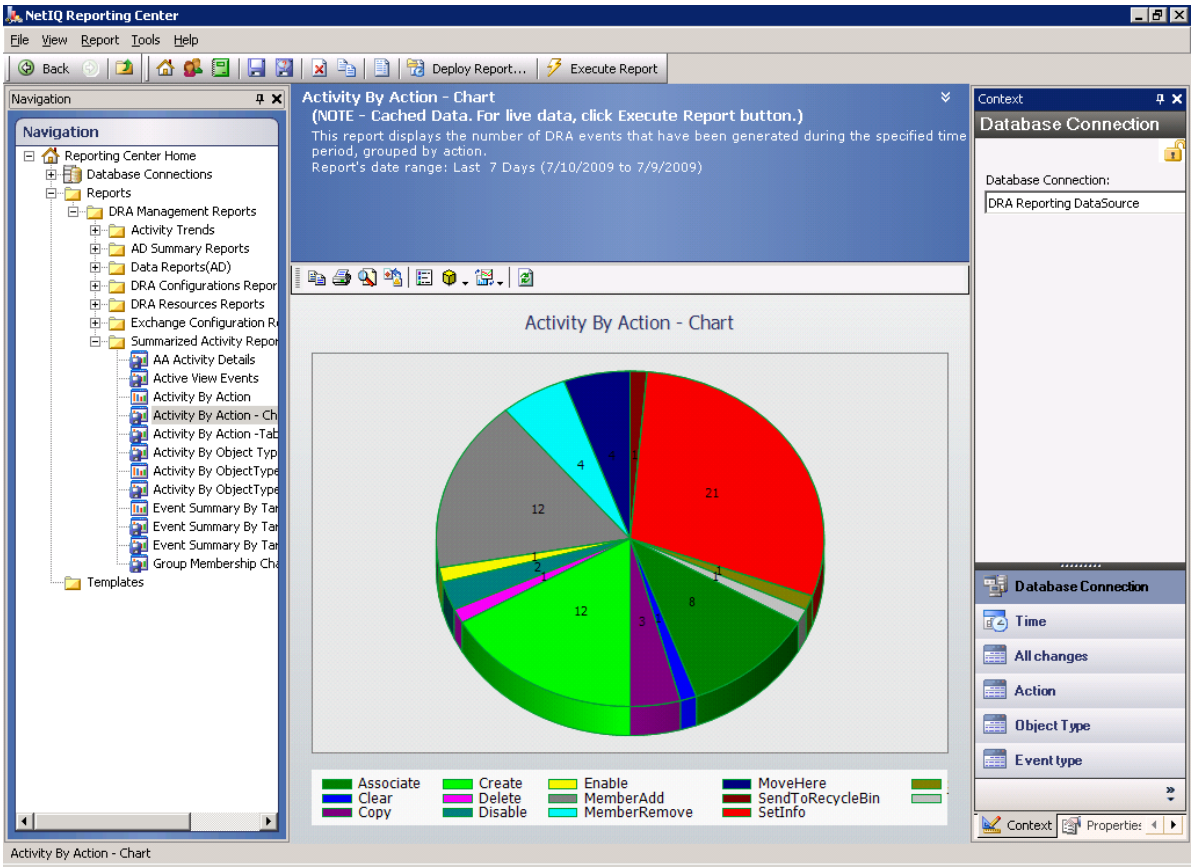
Optional **DRA Management reports**, viewed through the NetIQ Reporting Center (Reporting Center), provide activity, configuration, and summarization information about events in your managed domains. Some Management reports are available as graphical representations of the data. These built-in reports can also be customized to give you exactly the information you need.

For example, you can view a graph showing the number of events in each managed domain during a specified time period using Management reports. Reporting allows you to view details about the DRA security model, such as ActiveView and AA group definitions.

You must install and configure the optional Management reports before you can view these reports. For more information about installing reporting components, see the *Installation Guide*. For more information about configuring data collection for reporting, see Section 19.3, “Reporting Configuration Tasks,” on page 201.For more information about DRA Reporting, see “Generating Reports” in the *User Guide*. .

Start Reporting Center Console in the NetIQ > Reporting Center program group.

The following figure shows the Reporting Center interface with DRA Management reports selected.



3 Understanding the Dynamic Security Model

DRA and ExA allow you to manage your enterprise within the context of a dynamic security model. This model ensures that your enterprise management and security remains current as your enterprise changes and evolves. Dynamic security allows you to control the issues you have today while providing a stable foundation for future solutions.

3.1 What Is Distributed Administration?

Distributed administration allows you to delegate specific authority to one or more people. With distributed administration, you can easily and safely grant powers over a set of objects regardless of your domain or organizational unit (OU) structure.

When you use distributed administration, you create rules that define *who* can do *what* to *whom* or *what*.

who

Assistant Admins (AAs) represent one or more user accounts, groups, or AA groups. AAs manage the user accounts, groups, contacts, OUs, and resources in an ActiveView.

what

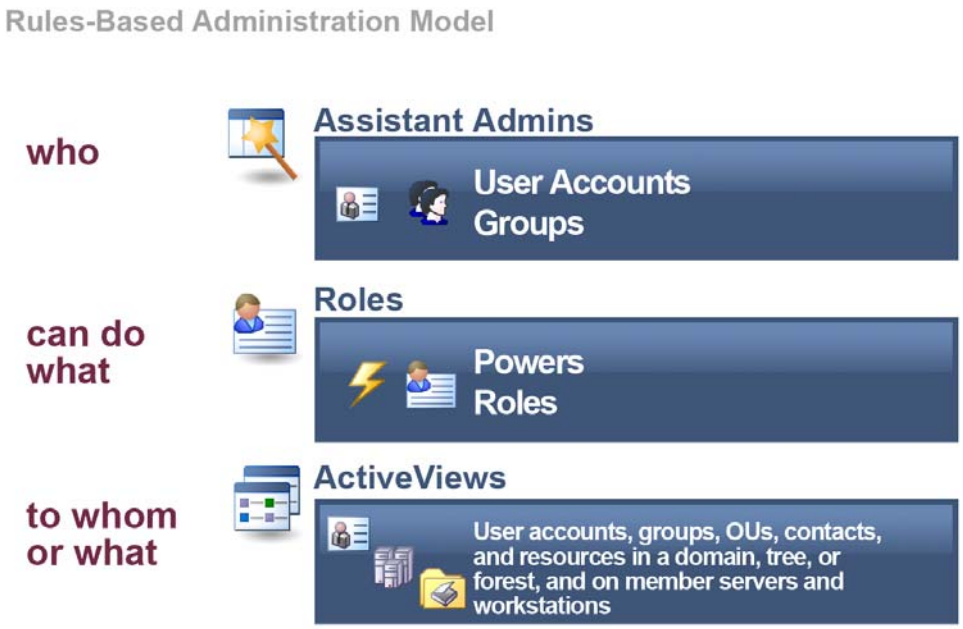
Roles and powers represent subsets of administration authority that you want to grant to AAs.

whom or what

ActiveViews represent a set of objects your AAs can manage collectively.

These rules establish and control your security model. When using a dynamic security model, these rules provide the flexibility you need to automatically maintain security while your enterprise changes.

The following figure illustrates this rules based model.



3.2 What Is the Dynamic Security Model?

The dynamic security model provides powerful and flexible rules based management for your enterprise. This model enhances distributed administration by accommodating change. Rather than delegating a power to a person, you are delegating roles to people. In this way, the dynamic security model more closely represents how your company works, letting you design your enterprise security to support workflows across organizations. You can expand this flexibility by configuring rules that match established naming conventions or group memberships.

In the dynamic security model, roles can be reused in different ActiveViews and assigned to different AAs, user accounts can be moved from one AA group to another, and powers can be moved from one role to another. As these changes occur, DRA and ExA automatically update security settings across your enterprise.

When you develop your administration and security plan, first identify the workflows your company has. Each workflow determines *who* can do *what* to *whom* or *what*. Use your workflow definitions to create the appropriate AA groups, assign the required roles, and configure the corresponding ActiveViews.

3.2.1 Assistant Admins

Assistant Admins (AAs) are the *who* in the dynamic security model. An AA is a user or group who is granted power over a set of objects. You grant power to an AA by associating the account with the appropriate role. For more information about roles, see Section 3.2.2, “Roles,” on page 57.

You can also define Assistant Admin groups. An AA group is a set of AAs that can contain users and groups. An AA group associated with a role in an ActiveView can manage the objects listed in that ActiveView. When you add a user or group to an AA group, the new member automatically receives the powers currently assigned to that AA group. When you associate the AA group with another role, the group members automatically receive the corresponding powers. The same AA group can be

associated with more than one ActiveView, providing access to multiple sets of objects. You can also use the pre-defined built-in AA groups that are installed with the product. For more information about built-in AA groups, see Chapter 4, “Understanding the Default Security Model,” on page 65.

DRA and ExA do not automatically allow AAs power to manage their own accounts. However, you can let AAs manage the personal information, such as street addresses or cell phone numbers, for their accounts. This type of administration is called **self-administration**. For more information about self administration, see Section 14.3, “Allowing Users to Change Personal Information,” on page 140.

3.2.2 Roles

Roles are the *what* in the dynamic security model. A role is a set of powers that provide the permissions required to perform a specific administration task, such as creating a user account or moving shared directories. To create a role, first define the job description. The job description provides the list of powers an Assistant Admin needs to perform a task or complete a workflow.

A role can contain any set of powers you specify. Because you can choose from hundreds of powers, you have the flexibility to create roles that best fit your organization. You can also use the pre-defined built-in roles that are installed with the product. For more information about built-in roles, see Chapter 4, “Understanding the Default Security Model,” on page 65.

When you add a power to a role, any Assistant Admin associated with that role automatically receives the new power. You can add roles to other roles, creating a hierarchical model based on increasing power. You can also associate the same role to different Assistant Admin groups.

Roles by themselves do not grant power. To delegate power, you must associate the role with an Assistant Admin in an ActiveView.

3.2.3 Powers

A power defines the properties of an object an Assistant Admin can view, modify, or create in your managed domain or subtree. A group of powers forms a role. DRA allows you to group powers into roles and delegate the roles and powers to users, group accounts, and Assistant Admin groups.

The Delegation and Management taskpad allows you to list built-in powers, clone and create new powers, assign powers to ActiveViews and Assistant Admin groups, change properties of custom powers, and view all powers. Roles are created from the inclusion of multiple powers.

3.2.4 ActiveViews

ActiveViews are the *whom or what* in the dynamic security model. An ActiveView represents a set of objects. When you create or modify an ActiveView, you specify rules that define which objects you want to manage as a collection. The ActiveView rule also associates AAs with roles and powers to manage this collection of objects.

3.3 What ActiveViews Provide

ActiveViews allow you to implement a security model that has the following features:

- Is independent from your Active Directory structure
- Allows you to assign powers and define policies that correlate to your existing workflows
- Provides automation to help you further integrate and customize your enterprise
- Dynamically responds to change

An ActiveView represents a set of objects within one or more managed domains. You can include an object in more than one ActiveView. You can also include many objects from multiple domains or OUs.

3.3.1 ActiveViews Include Dynamic Sets of Objects

An ActiveView provides real time access to specific objects within one or more domains or OUs. You can add or remove objects from an ActiveView without changing the underlying domain or OU structure.

You may think of an ActiveView as a virtual domain or OU, or the results of a select statement or database view for a relational database. ActiveViews can include or exclude any set of objects, contain other ActiveViews, and have overlapping contents. ActiveViews can contain objects from different domains, trees, and forests. You can configure ActiveViews to meet any enterprise management need.

ActiveViews can include the following types of objects:

- User accounts
- Groups
- Organizational units
- Contacts
- Computers
- Resources, such as:
  - printers
  - print jobs
  - open files
  - connected users
  - event logs
  - shares
  - devices
  - services
- Domains
- Other ActiveViews
- Resource mailboxes
- Exchange Dynamic Groups

You specify which objects DRA will include in an ActiveView by querying the object attributes, much as you would make a query to select items from a database. As your enterprise changes or grows, ActiveViews change to include or exclude the new objects. Thus, you can use ActiveViews to reduce the complexity of your model, provide the security you need, and give you far more flexibility than other enterprise organizing tools.

3.3.2 ActiveViews Include Flexible Rules

An ActiveView can consist of rules that include or exclude objects, such as user accounts, groups, OUs, contacts, resources, and ActiveViews. In addition, ActiveView rules can specify security and policy objects. When you specify a wildcard character in a rule specification, the rule includes all objects that match the specified value. This flexibility makes ActiveViews dynamic.

These matches are called **wildcards**. When you add a rule to an AA group using wildcards, the rule includes all computer accounts that match the specified pattern. For example, you can define a rule to include all computers with names matching `DOM*`. This wildcard specification will search for any computer account whose name begins with the character string DOM. Wildcard matching makes administration dynamic because accounts are automatically included when they match the rule. Thus, when you use wildcards, you do not need to reconfigure the ActiveViews as your organization changes.

Another example is defining ActiveViews based on group membership. You can define a rule that includes all members of groups that begin with the letters NYC. Then, as members are added to any group matching this rule, these members are automatically included in this ActiveView. As your enterprise changes or grows, DRA reapplies the rules to include or exclude the new objects in the proper ActiveViews. For more information about specifying wildcard matches, see Section 2.7.17, “Using Wildcard Characters,” on page 50.

3.4 ActiveViews and Distributed Administration

ActiveViews help you distribute administration tasks to specific people. For example, to allow members of the Atlanta Help Desk group to reset passwords and unlock accounts for users in Atlanta, an administrator at the Houston headquarters defines the following rules:

Atlanta Help Desk Assistant Admins

Rule for this AA group includes all the employees in the Atlanta Help Desk group.

Atlanta User Accounts ActiveView

Rules for this ActiveView include all the user accounts in Atlanta and associate the Reset User Passwords role with the Atlanta Help Desk AAs. By distributing administration through the Atlanta User Accounts ActiveView, the Houston administrator achieves the following benefits:

Improved service to users in Atlanta

Users in Atlanta no longer need to call Houston if they forget their password. Any time a new user account is added in Atlanta, the user account is included automatically in the Atlanta User Accounts ActiveView. Atlanta Help Desk Assistant Admins can now reset passwords for this new user account.

Reduced workload for the central administrators in Houston

Atlanta Help Desk Assistant Admins can reset passwords for users in the Atlanta User Accounts ActiveView while the Houston administrators focus their attention on other issues.

Enhanced security for the corporation

Atlanta Help Desk Assistant Admins are in a better position to determine whether a request to reset a password from a user in Atlanta is valid. Therefore, distributing this portion of the administration workload permits the corporation to run with fewer Microsoft Windows administrators, maintaining a higher level of security.

Reset User Passwords Role

Rules for this role include all the powers needed to unlock user accounts and reset passwords.

In this way, DRA allows you to manage your organization the way you think and work. Once you establish your own security model using ActiveViews, the model can grow and change as your organization does. For more information about implementing help desk administration, see the *Getting Started Guide*.

3.5 How the Administration Server Processes Requests

When the Administration server receives a request for an action, such as changing a user password, it uses the following process:

1. Search all ActiveViews for the object of this action.
2. Validate the powers assigned to the account that is requesting the action.
3. ***If the account has the correct power***, the Administration server allows the action to be performed.

   If the account does not have the correct power, the Administration server returns an error.
4. Update the Active Directory.

For example, when you attempt to set a new password for the JSmith user account, the Administration server finds all ActiveViews that include JSmith. This search looks for any ActiveView that specifies JSmith directly, through a wildcard rule, or through group membership. If an ActiveView includes other ActiveViews, the Administration server also searches these additional ActiveViews. The Administration server determines whether you have the Reset User Account Password power in any of these ActiveViews. If you have the Reset User Account Password power, the Administration server resets the password for JSmith. If you do not have this power, the Administration server denies your request.

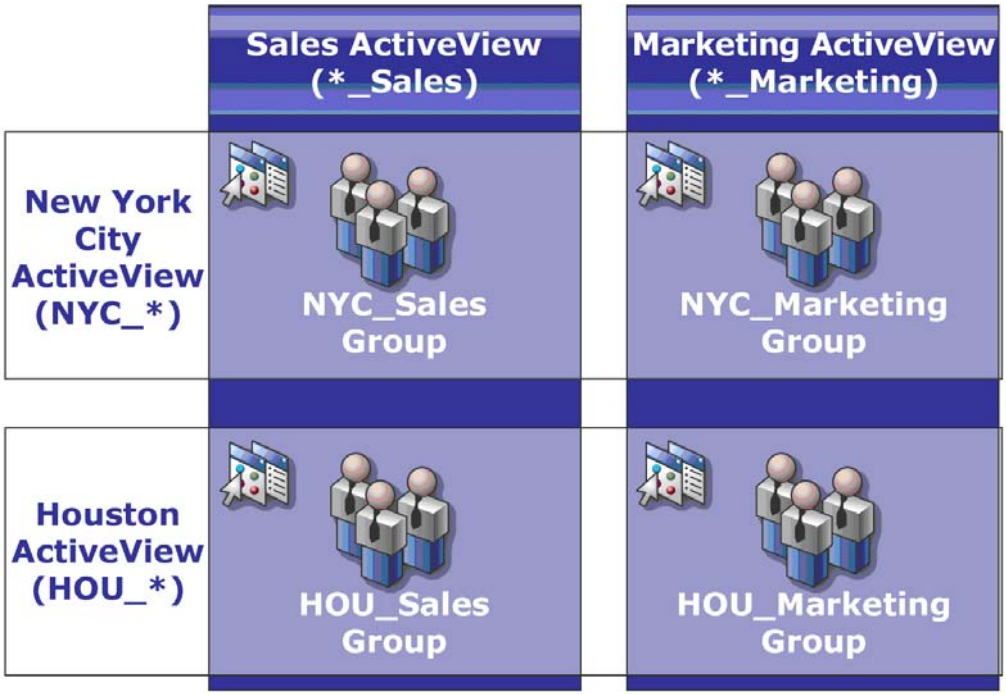
3.6 How Powers Can Increase

A power defines the properties of an object an Assistant Admin can view, modify, or create in your managed domain or subtree. More than one ActiveView can include the same object. This configuration is called **overlapping ActiveViews**.

When ActiveViews overlap, you can accumulate a set of different powers over the same objects. For example, if one ActiveView allows you to add a user account to a domain and another ActiveView allows you to delete a user account from the same domain, you can add or delete user accounts in that domain. In this way, the powers you have over a given object are cumulative.

3.7 Understanding How Powers Increase

It is important to understand how ActiveViews can overlap and you can have increased powers over objects included in these ActiveViews. Consider the ActiveView configuration illustrated in the following figure.



The white tabs identify ActiveViews by location, *New York City* and *Houston*. The black tabs identify ActiveViews by their organizational function, *Sales* and *Marketing*. The cells show the groups included in each ActiveView.

The NYC_Sales group and the HOU_Sales group are both represented in the Sales ActiveView. If you have power in the Sales ActiveView, then you can manage any member of the NYC_Sales and HOU_Sales groups. If you also have power in the New York City ActiveView, then these additional powers apply to the NYC_Marketing group. In this way, powers accumulate as the ActiveViews overlap.

Overlapping ActiveViews can provide a powerful, flexible security model. However, this feature can also have unintended consequences. Carefully plan your ActiveViews to ensure each AA has only the powers you intend over each user account, group, OU, contact, or resource.

3.7.1 Groups in Multiple ActiveViews

In this example, the NYC_Sales group is represented in more than one ActiveView. The members of the NYC_Sales group are represented in the New York City ActiveView because the group name matches the `NYC_*` ActiveView rule. The group is also in the Sales ActiveView because the group name matches the `*_Sales` ActiveView rule. By including the same group in multiple ActiveViews, you can allow different AAs to manage the same objects differently.

3.7.2 Using Powers in Multiple ActiveViews

Assume there is an AA, JSmith, who has the Modify General User Properties power in the New York City ActiveView. This first power allows JSmith to edit all the properties on the General tab of a user properties window. JSmith has the Modify User Profile Properties power in the Sales ActiveView. This second power allows JSmith to edit all the properties on the Profile tab of a user properties window.

The following figure indicates the powers JSmith has for each group.

JSmith has the following powers:

- General Properties in the NYC_* ActiveView
- Profile Properties in the *_Sales ActiveView

The power delegation in these overlapping ActiveViews allows JSmith to modify the General and Profile properties of the NYC_Sales group. Thus, JSmith has all the powers granted in all the ActiveViews that represent the NYC_Sales group.

3.7.3 Extending Powers

You can add permissions or functionality to a power by extending that power.

For example, to allow an AA to create a user account, you can assign either the Create User and Modify All Properties power or the Create User and Modify Limited Properties power. If you also assign the Add New User to Group power, the AA can add this new user account to a group while using the Create User wizard. In this case, the Add New User to Group power provides an additional wizard feature. The Add New User to Group power is the **extension power**.

Extension powers cannot add permissions or functionality by themselves. To successfully delegate a task that includes an extension power, you must assign the extension power along with the power you want to extend.

NOTE

- To successfully create a group and include the new group in an ActiveView, you must have the Add New Group to ActiveView power in the specified ActiveView. The specified ActiveView must also include the OU or built-in container that will contain the new group.
- To successfully clone a group and include the new group in an ActiveView, you must have the Add Cloned Group to ActiveView power in the specified ActiveView. The specified ActiveView must also include the source group as well as the OU or built-in container that will contain the new group.

The following table lists the administration tasks that include extension powers.

To Delegate This Task	Assign This Power	And This Extension Power
Clone a group and include the new group in a specified ActiveView	Clone Group and Modify All Properties	Add Cloned Group to ActiveView
Create a group and include the new group in a specified ActiveView	Create Group and Modify All Properties	Add New Group to ActiveView
Create a mail enabled contact	Create Contact and Modify All Properties Create Contact and Modify Limited Properties	Enable Email for New Contact
Create a mail enabled group	Create Group and Modify All Properties	Enable Email for New Group
Create a mail enabled user account	Create User and Modify All Properties Create User and Modify Limited Properties	Enable Email for New User
Create a user account and add the new account to specific groups	Create User and Modify All Properties Create User and Modify Limited Properties	Add New User to Group

4 Understanding the Default Security Model

DRA and ExA extend your existing native Microsoft Windows security model. For example, DRA uses your existing group memberships to define default permissions. You can meet your specific needs by customizing and extending these permissions across the organization.

The default DRA and ExA security model provides built-in roles, AA groups, policy, and ActiveViews so that you can quickly incorporate DRA and ExA into your current security model. Through the default security model, your team can start using DRA out of the box with little or no additional configuration.

This section describes the key concepts about the default security model and illustrates these concepts with examples and scenarios. These examples and scenarios assume you have the DRA Admin role or the corresponding powers. Review these sections to learn about the following concepts:

- How to extend your security model with DRA and ExA
- How to use the built-in ActiveViews, AA groups, and roles

For more information about built-in policy, see Section 13.5.1, “Understanding Built-in Policies,” on page 124.

4.1 What Is the Default Security Model?

The default security model consists of several built-in ActiveViews, AA groups, and roles. These built-in components let you immediately manage domain objects and customize the Administration server. With these default definitions and rules, you can quickly start planning and implementing your enterprise management model.

You can use the available built-in components as the basis for your own security model. You can easily define ActiveViews and associate the built-in roles with AA groups you create to delegate administration powers within your enterprise. For information about implementing a security model, see Chapter 14, “Implementing Your Dynamic Security Model,” on page 135.

4.2 What Built-in Security Provides

Built-in security provides immediate and secure access to your domains, objects, and policies. The built-in ActiveViews, AA groups, and roles allow you to extend your existing security model. You can start using DRA and ExA to manage your enterprise without redesigning your existing security.

These built-in components provide a starting point. Before you define an ActiveView, decide if you can use one of the built-in roles or if you need to define a new role. When you specify which objects the ActiveView includes, you can quickly associate AAs with roles or powers for this ActiveView. These built-in roles and ActiveViews allow you to begin work immediately, using the full capabilities of DRA and ExA.

For example, members of the Administrators group in the managed domain are automatically empowered with the DRA Administration role in the Objects Current User Manages as Windows Administrator ActiveView. This ensures that Microsoft Windows administrators can start DRA and ExA with the same permissions they have using native tools.

4.2.1 All Powers for DRA Admins

You can grant any group or user account all powers across the enterprise by delegating the following built-in security objects:

- DRA Admins AA group
- DRA Administration role
- All Objects ActiveView

The following table describes the relationship between these security objects.

Object Name	Object Type	Description
DRA Admins	AA group	Includes the user account or group you specified during setup
DRA Administration	Role	Includes all powers
All Objects	ActiveView	Includes all user accounts, groups, resources, contacts, OUs, and Microsoft Exchange mailboxes from all managed domains

With this association, all members of the built-in DRA Admins AA group have all powers for all directory objects across the enterprise.

4.2.2 Domain Powers for Administrators

To grant members of the native Administrators group all powers in domains where they are Administrators, DRA provides the following built-in security objects:

- Administrators from Managed Domains AA group
- DRA Administration role
- Objects Current User Manages as Windows Administrator ActiveView

The following table describes the relationship between these security objects.

Object Name	Object Type	Description
Administrators from Managed Domains	AA group	All members of the native Administrators group for the managed domain
DRA Administration	Role	Includes all powers

Object Name	Object Type	Description
Objects Current User Manages as Windows Administrator	ActiveView	Includes all user accounts, groups, resources, contacts, OUs, and Microsoft Exchange mailboxes in managed domains where the AA is an Administrator

With this association, all members of the native Administrators group have all powers for accounts, resources, and mailboxes in the managed domain.

4.2.3 Built-in Delegations

By default, DRA delegates the built-in ActiveViews and roles to specific AA groups. The following table lists the built-in ActiveViews and identifies the built-in AA groups and roles associated with each ActiveView.

Built-in ActiveView	Built-in AA group	Assigned role
All Objects	DRA Admins	DRA Administration
Objects Current User Manages as Windows Administrator	Administrators from Managed Domains	DRA Administration
Administration Servers and Managed Domains	DRA Configuration Admins	Configure Servers and Domains
DRA Policies and Automation Triggers	DRA Policy Admins	Manage Policies and Automation Triggers
DRA Security Objects	DRA Security Model Admins	Manage Security Model
SPA Users from All Managed and Trusted Domains	SPA Admins	Reset Password and Unlock Using SPA

4.3 Understanding Built-in ActiveViews

Built-in ActiveViews are the default ActiveViews provided by DRA and ExA. These ActiveViews represent all current objects and security settings. Thus, built-in ActiveViews provide immediate access to all your objects and settings as well as the default security model. You can use these ActiveViews to manage objects, such as user accounts and resources, or apply the default security model to your current enterprise configuration.

4.3.1 Built-in ActiveViews

DRA and ExA provide several built-in ActiveViews that can represent your security model. The built-in ActiveView node contains the following ActiveViews:

All Objects

Includes all objects in all managed domains. Through this ActiveView, you can manage any aspect of your enterprise. Assign this ActiveView to the administrator or to an AA who needs auditing powers across the enterprise.

Objects Current User Manages as Windows Administrator

Includes objects from the current managed domain. Through this ActiveView, you can manage user accounts, groups, contacts, OUs, and resources. Assign this ActiveView to native Administrators who are responsible for account and resource objects in the managed domain.

Administration Servers and Managed Domains

Includes Administration server computers and managed domains. Through this ActiveView, you can manage the daily maintenance of your Administration servers. Assign this ActiveView to AAs whose duties include monitoring the synchronization status or performing cache refreshes.

DRA Policies and Automation Triggers

Includes all policy and automation trigger objects in all managed domains. Through this ActiveView, you can manage policy properties and scope, as well as automation trigger properties. Assign this ActiveView to AAs responsible for creating and maintaining your company policies.

DRA Security Objects

Includes all security objects. Through this ActiveView, you can manage ActiveViews, AA groups, and roles. Assign this ActiveView to AAs responsible for creating and maintaining your security model.

SPA Users from All Managed and Trusted Domains

Includes all user accounts from managed and trusted domains. Through this ActiveView, you can manage password of the users.

4.3.2 Accessing Built-in ActiveViews

Access built-in ActiveViews to audit the default security model or manage your own security settings.

To access built-in ActiveViews:

1. In the left pane, select **Delegation Management**.
2. Under Common Tasks in the right pane, click **Manage ActiveViews**.
3. Select the appropriate ActiveView.

4.3.3 Using Built-in ActiveViews

You cannot delete, clone, or modify built-in ActiveViews. However, you can incorporate these ActiveViews into your existing security model or use these ActiveViews to design your own model.

You can use built-in ActiveViews in the following ways:

- Assign the individual built-in ActiveViews to the appropriate AA groups. This association allows the AA group members to manage the corresponding set of objects with the appropriate powers.
- Refer to the built-in ActiveView rules and associations as guidelines towards designing and implementing your security model.

For more information about designing a dynamic security model, see Chapter 14, “Implementing Your Dynamic Security Model,” on page 135.

4.4 Understanding Built-in Assistant Admin Groups

Built-in AA groups provide immediate access to a set of commonly used roles. You can extend your current security configuration by using these default groups to delegate power to specific user accounts or other groups.

Most built-in AA groups do not include any members. Use these groups to quickly let the appropriate people manage objects in the built-in ActiveViews. For example, if you add the AtlantaAdmins group to the DRA Security Model Admins AA group, members of the AtlantaAdmins group can create and modify all the rules that define the administration model. If you add the HoustonAdmins group to the built-in DRA Policy Admins AA group, members of the HoustonAdmins group can create and modify all policies, such as user account naming conventions. A member of the built-in DRA Policy Admins AA group can also create and modify automation triggers.

These groups are already associated with the corresponding built-in role so their members can perform common administration tasks. For example, members of the Administrators from Managed Domains AA group can manage objects in domains where they are administrators. Because built-in AA groups are part of the default security model, you can use the built-in AA groups to quickly delegate power and implement security.

4.4.1 Built-in Assistant Admin Groups

DRA and ExA provide several built-in AA groups that you can use in your security model. The following list describes each built-in AA group and discusses the AAs typically associated with that group. For more information, see Section 4.3, “Understanding Built-in ActiveViews,” on page 67 and Section 4.5, “Understanding Built-in Roles,” on page 70.

DRA Admins

Allows AAs to manage all objects in your managed domain, including the Administration servers, and maintain your security model. By default, the DRA Admins group includes the account or group you specified during setup. Add AAs to this group if they are responsible for managing all aspects of your enterprise.

Administrators from Managed Domains

Allows AAs to manage all user accounts, groups, contacts, OUs, and resources for the domains in which they are administrators. By default, the Administrators from Managed Domains group includes the native Administrators group.

DRA Configuration Admins

Allows AAs to configure the Administration servers and managed domains. This group also allows AAs to create custom user interface extensions and custom tools, manage file replication between Administration servers and DRA client computers, and specify clone exceptions to use when cloning user accounts. By default, the DRA Configuration Admins group includes the Administration server service account. Add AAs to this group if they are responsible for configuring and maintaining your Administration servers, such as performing accounts cache refreshes or server synchronization.

DRA Policy Admins

Allows AAs to manage policies and automation triggers for all managed domains. By default, the DRA Policy Admins group does not have members. Add AAs to this group if they are responsible for establishing and maintaining policies and automating workflows.

DRA Security Model Admins

Allows AAs to manage security objects such as other AA groups, roles, and ActiveViews. By default, the DRA Security Model Admins group does not have members. Add AAs to this group if they are responsible for establishing and maintaining your security model.

SPA Admins

Allows AAs to manage password of the users. It also allows AAs to reset passwords and unlock user accounts. By default, the SPA Admins group does not have members. Add AAs to this group if they are responsible for managing passwords.

4.4.2 Accessing Built-in Assistant Admin Groups

Access built-in AA groups to audit the default security model or manage your own security settings.

To access built-in AA groups:

1. In the left pane, select **Delegation Management**.
2. Under Common Tasks in the right pane, click **Manage Assistant Admins**.
3. Select the appropriate AA group.

4.4.3 Using Built-in Assistant Admin Groups

You cannot delete or clone built-in AA groups. However, you can incorporate the built-in AA groups into your existing security model or use these groups to design and implement your own model.

You can use built-in AA groups in the following ways:

- Add user accounts or other groups to a built-in AA group. These new members are then empowered with built-in roles in the ActiveViews associated with the AA group.
- Associate a built-in AA group with an ActiveView. This association allows the AA group members to manage a specific set of objects.

For more information about designing a dynamic security model, see Chapter 4, “Understanding the Default Security Model,” on page 65.

4.5 Understanding Built-in Roles

Built-in AA roles provide immediate access to a set of commonly used powers. You can extend your current security configuration by using these default roles to delegate power to specific user accounts or other groups.

These roles contain the powers required to perform common administration tasks. For example, the DRA Administration role contains all the powers required to manage objects. To use these powers, however, the role must be associated with a user account or an AA group and the managed ActiveView.

Because built-in roles are part of the default security model, you can use the built-in roles to quickly delegate power and implement security.

4.5.1 Built-in Roles

These built-in roles address common tasks you can perform through the DRA and ExA user interfaces. The following list describes each built-in role and summarizes the powers associated with that role.

Audit All Objects

Provides all the powers required to view properties of objects, policies, and configurations across your enterprise. This role does not allow an AA to modify properties. Assign this role to AAs responsible for auditing actions across your enterprise. Allows AAs to view all nodes except the Custom Tools node.

Audit Limited Account and Resource Properties

Provides all the powers required to view a limited set of properties of objects and managed resources across your enterprise. This role does not allow an AA to modify properties. Assign this role to AAs responsible for auditing actions across your enterprise.

Audit Resources

Provides all the powers required to view properties of managed resources. Assign this role to AAs responsible for auditing resource objects.

Audit Users and Groups

Provides all the powers needed to view user account and group properties, but no powers to modify these properties. Assign this role to AAs responsible for auditing account properties.

Built-in Scheduler - Internal Use Only

Provides all the powers needed to schedule DRA jobs.

Clone User with Mailbox

Provides all the powers required to clone an existing user account along with the account mailbox. Assign this role to AAs responsible for managing user accounts.

NOTE: To allow the AA to add the new user account to a group during the clone task, also assign the Manage Group Memberships role.

Computer Administration

Provides all the powers required to modify computer properties. This role allows AAs to add, delete, and shut down computers, as well as synchronize domain controllers. Assign this role to AAs responsible for managing computers in the ActiveView.

Configure Servers and Domains

Provides all the powers required to modify Administration server options and managed domains. Also provides powers necessary to configure and manage Office 365 tenants. Assign this role to AAs responsible for monitoring and maintaining the Administration servers.

Contact Administration

Provides all the powers required to create a new contact, modify contact properties, or delete a contact. Assign this role to AAs responsible for managing contacts.

Create and Delete Computer Accounts

Provides all the powers required to create and delete a computer account. Assign this role to AAs responsible for managing computers.

Create and Delete Groups

Provides all the powers required to create and delete a group. Assign this role to AAs responsible for managing groups.

Create and Delete Resources

Provides all the powers required to create and delete shares and computer accounts, and clear event logs. Assign this role to AAs responsible for managing resource objects and event logs.

Create and Delete Resource Mailbox

Provides all the powers required to create and delete a a mailbox. Assign this role to AAs responsible for managing mailboxes.

Create and Delete User Accounts

Provides all the powers required to create and delete a user account. Assign this role to AAs responsible for managing user accounts.

Dynamic Group Administration

Provides all the powers required to manage Active Directory dynamic groups.

DRA Administration

Provides all powers to an AA. This role gives a user the permissions to perform all administration tasks within DRA and ExA. This role is equivalent to the permissions of an administrator. An AA associated with the DRA Administration role can access all Directory and Resource Administrator nodes.

Execute Advanced Queries

Provides all the powers required to execute saved advanced queries. Assign this role to AAs responsible for executing advanced queries.

Group Administration

Provides all the powers required to manage groups and group memberships, and view corresponding user properties. Assign this role to AAs responsible for managing groups or account and resource objects that are managed through groups.

Help Desk Administration

Provides all the powers required to view user account properties, and to change passwords and password related properties. This role also allows AAs to disable, enable, and unlock user accounts. Assign this role to AAs responsible for Help Desk duties associated with ensuring users have proper access to their accounts.

Mailbox Administration

Provides all the powers required to manage Microsoft Exchange mailbox properties. If you use Microsoft Exchange, assign this role to AAs responsible for managing Microsoft Exchange mailboxes.

Manage Active Directory Collectors, DRA Collectors, and Management Reporting Collectors

Provides all the powers required to manage Active Directory Collectors, DRA Collectors, Office 365 Tenant Collectors, and Management Reporting Collectors for data collection. Assign this role to AAs responsible for managing reporting configuration.

Manage Active Directory Collectors, DRA Collectors, Management Reporting Collectors, and Database Configuration

Provides all the powers required to manage Active Directory Collectors, DRA Collectors, Management Reporting Collectors, and database configuration for data collection. Assign this role to AAs responsible for managing reporting and database configuration.

Manage Advanced Queries

Provides all the powers required to create, manage, and execute advanced queries. Assign this role to AAs responsible for managing advanced queries.

Manage and Execute Custom Tools

Provides all the powers required to create, manage, and excecute custom tools. Assign this role to AAs responsible for managing custom tools.

Manage Clone Exceptions

Provides all the powers required to create and manage clone exceptions.

Manage Computer Properties

Provides all the powers required to manage all properties for a computer account. Assign this role to AAs responsible for managing computers.

Manage Database Configuration

Provides all the powers required to manage database configuration for Management reports. Assign this role to AAs responsible for managing reporting database configuration.

Manage Dynamic Distribution Groups

Provides all the powers required to manage Microsoft Exchange dynamic distribution groups.

Manage Exchange Mailbox Rights

Provides all the powers required to manage security and rights for Microsoft Exchange mailboxes. If you use Microsoft Exchange, assign this role to AAs responsible for managing Microsoft Exchange mailbox permissions.

Manage Group Email

Provides all the powers required to view, enable, or disable the email address for a group. Assign this role to AAs responsible for managing groups or email addresses for account objects.

Manage Group Membership Security

Provides all the powers required to designate who can view and modify Microsoft Windows group memberships through Microsoft Outlook

Manage Group Memberships

Provides all the powers required to add and remove user accounts or groups from an existing group, and view the primary group of a user or computer account. Assign this role to AAs responsible for managing groups or user accounts.

Manage Group Properties

Provides all the powers required to manage all properties for a group. Assign this role to AAs responsible for managing groups.

Manage Mailbox Move Requests

Provides all the powers required to manage mailbox move requests.

Manage Policies and Automation Triggers

Provides all the powers required to define policies and automation triggers. Assign this role to AAs responsible for maintaining company policies and automating workflows.

Manage Printers and Print Jobs

Provides all the powers required to manage printers, print queues, and print jobs. To manage print jobs associated with a user account, the print job and the user account must be included in the same ActiveView. Assign this role to AAs responsible for maintaining printers and managing print jobs.

Manage Resources for Managed Users

Provides all the powers required to manage resources associated with specific user accounts. The AA and the user accounts must be included in the same ActiveView. Assign this role to AAs responsible for managing resource objects.

Manage Resource Mailbox Properties

Provides all the powers required to manage all properties for a mailbox. Assign this role to AAs responsible for managing mailboxes.

Manage Security Model

Provides all the powers required to define the Administration rules, including ActiveViews, AAs, and roles. Assign this role to AAs responsible for implementing and maintaining your security model.

Manage Services

Provides all the powers required to manage services. Assign this role to AAs responsible for managing services.

Manage Shared Folders

Provides all the powers required to manage shared folders. Assign this role to AAs responsible for managing shared folders.

Manage Temporary Group Assignments

Provides all the powers required to create and manage temporary group assignments. Assign this role to AAs responsible for managing groups.

Manage UI Reporting

Provides all the powers required to generate and export Activity Detail reports for users, groups, contacts, computers, organizational units, powers, roles, ActiveViews, containers, published printers, and Assistant Admins. Assign this role to AAs responsible for generating reports.

Manage User Dial in Properties

Provides all the powers required to modify the dial in properties of user accounts. Assign this role to AAs responsible for managing user accounts that have remote access to the enterprise.

Manage User Email

Provides all the powers required to view, enable, or disable the email address for a user account. Assign this role to AAs responsible for managing user accounts or email addresses for account objects.

Manage User Password and Unlock Account

Provides all the powers required to reset the password, specify password settings, and unlock a user account. Assign this role to AAs responsible for maintaining user account access.

Manage User Properties

Provides all the powers required to manage all properties for a user account, including Microsoft Exchange mailbox properties. Assign this role to AAs responsible for managing user accounts.

Manage Virtual Attributes

Provides all the powers required to create and manage virtual attributes. Assign this role to AAs responsible for managing virtual attributes.

Manage WTS Environment Properties

Provides all the powers required to change the WTS environment properties for a user account. Assign this role to AAs responsible for maintaining the WTS environment or managing user accounts.

Manage WTS Remote Control Properties

Provides all the powers required to change the WTS remote control properties for a user account. Assign this role to AAs responsible for maintaining WTS access or managing user accounts.

Manage WTS Session Properties

Provides all the powers required to change the WTS session properties for a user account. Assign this role to AAs responsible for maintaining WTS sessions or managing user accounts.

Manage WTS Terminal Properties

Provides all the powers required to change the WTS terminal properties for a user account. Assign this role to AAs responsible for maintaining WTS terminal properties or managing user accounts.

OU Administration

Provides all the powers required to manage organizational units. Assign this role to AAs responsible for managing the Active Directory structure.

Rename Group and Modify Description

Provides all the powers required to modify the name and description of a group. Assign this role to AAs responsible for managing groups.

Rename User and Modify Description

Provides all the powers required to modify the name and description of a user account. Assign this role to AAs responsible for managing user accounts.

Replicate Files

Provides all the powers required to upload, delete and modify file information. Assign this role to AAs responsible for replicating files from the primary Administration server to other Administration servers in the MMS and the DRA client computers.

Reset Local Administrator Password

Provides all the powers to reset the local administrator account password and view the name of the computer administrator. Assign this role to AAs responsible for managing the administrator accounts.

Reset Password

Provides all the powers required to reset and modify passwords. Assign this role to AAs responsible for password management.

Reset Password and Unlock Account Using SPA

Provides all the powers required to use Secure Password Administrator to reset passwords and unlock user accounts.

Reset Unified Messaging PIN Properties

Provides all the powers required to reset Unified Messaging PIN properties for user accounts.

Resource Administration

Provides all the powers required to modify properties of managed resources, including resources associated with any user account. Assign this role to AAs responsible for managing resource objects.

Resource Mailbox Administration

Provides all the powers required to manage resource mailboxes.

Self Administration

Provides all the powers required to modify basic properties, such as telephone numbers, of your own user account. Assign this role to AAs to allow them to manage their own personal information.

Start and Stop Resources

Provides all the powers required to pause, start, resume, or stop a service, start or stop a device or printer, shut down a computer, or synchronize your domain controllers. Also provides all the powers required to pause, resume, and start services, stop devices or print queues, and shut down computers. Assign this role to AAs responsible for managing resource objects.

Transform a User

Provides all the powers required to add a user to or remove a user from groups found in a template account, including the ability to modify the user's properties while transforming the user.

User Administration

Provides all the powers required to manage user accounts, associated Microsoft Exchange mailboxes, and group memberships. Assign this role to AAs responsible for managing user accounts.

View Active Directory Collectors, DRA Collectors, Management Reporting Collectors, and Database Configuration Information

Provides all the powers required to view AD collectors, DRA collectors, management reporting collectors, and database configuration information.

View All Computer Properties

Provides all the powers required to view properties of a computer account. Assign this role to AAs responsible for auditing computers.

View All Group Properties

Provides all the powers required to view properties for a group. Assign this role to AAs responsible for auditing groups.

View All Resource Mailbox Properties

Provides all the powers required to view properties for a resource mailbox. Assign this role to AAs responsible for auditing resource mailboxes.

View All User Properties

Provides all the powers required to view properties for a user account. Assign this role to AAs responsible for auditing user accounts.

WTS Administration

Provides all the powers required to manage Windows Terminal Server (WTS) properties for user accounts in the ActiveView. If you use WTS, assign this role to AAs responsible for maintaining the WTS properties of user accounts.

If you have licensed the File Security Administrator product, additional built-in roles are available. For more information about File Security Administrator, see the *User Guide for File Security Administrator*.

4.5.2 Accessing Built-in Roles

Access built-in roles to audit the default security model or manage your own security settings.

To access built-in AA groups:

1. In the left pane, select **Delegation Management**.
2. Under Common Tasks in the right pane, click **Manage Roles**.
3. Select the appropriate role.

4.5.3 Using Built-in Roles

You cannot delete or modify built-in roles. However, you can incorporate the built-in roles into your existing security model or use these roles to design and implement your own model.

You can use built-in roles in the following ways:

- Associate a built-in role with a user account or AA group. This association provides the user or AA group members with the appropriate powers for the task.
- Clone a built-in role and use that clone as the basis for a custom role. You can add other roles or powers to this new role and remove powers originally included in the built-in role.

For more information about designing a dynamic security model, see Chapter 14, “Implementing Your Dynamic Security Model,” on page 135.

5 Implementing Advanced Queries

DRA search functionality allows you to search for attributes of objects in Active Directory such as users, computers, printers, groups, and OUs as well as specify wildcard character searches. However, you cannot use DRA search functionality to search on customized attributes, like the account lockout status or account expired status. Advanced queries enable you to perform customized searches that are not available through DRA search functionality. The kinds of advanced queries you can perform include the following:

- Search for all users whose accounts are locked out
- Search for all users whose accounts have expired
- Search for all users who have been inactive for the past 30 days

You can save, modify, delete, and share advanced queries that you create in DRA. Advanced queries also enables you to perform search on virtual attributes.

5.1 Understanding Advanced Queries

DRA uses LDAP as the protocol for managing and executing advanced queries. You can use advanced queries to search for users, contacts, groups, computers, printers, OUs, and any other object that DRA supports. If you are familiar with the LDAP query language, you can type your LDAP query, validate the query, and share it with other AAs by saving it as a public query. If you are not familiar with the LDAP query language, you can use saved queries or import queries from the Active Directory User and Computers (ADUC) management console. You can manage advanced queries on both the primary Administration server and secondary Administration servers.

5.2 How DRA Helps You Manage Advanced Queries

DRA allows you to manage advanced queries from within DRA, thereby minimizing your dependency on the ADUC management console to search for information. From creating advanced queries to sharing advanced queries with other AAs, DRA allows you to address a wide range of advanced query tasks and issues from within a single application.

DRA allows you to secure advanced query management by controlling the level at which an AA can access and modify advanced queries. For more information about delegating administration powers, see Chapter 14, “Implementing Your Dynamic Security Model,” on page 135.

5.3 Advanced Query on Virtual Attributes

Using advanced queries, you can perform search on virtual attributes that you have created and have associated with users, contacts, groups, computers, printers, OUs, and any other object that DRA supports.

5.4 Advanced Query Management Tasks

The User Guide and Help provide conceptual and management information for advanced queries. The Help provides step-by-step guidance for many advanced query management tasks, such as customizing advanced query results.

To access Help for an advanced query task:

1. On the Help menu, click **Directory and Resource Administrator Help**.
2. Expand **How To**.
3. Expand **Advanced Query Tasks**.
4. Click the appropriate task.

6 Implementing Virtual Attributes

Using virtual attributes, you can create new properties and associate these properties with users, groups, contacts, computers, and OUs. Virtual attributes allow you to create new properties without requiring you to extend the Active Directory schema.

6.1 Understanding Virtual Attributes

Using virtual attributes, you can add new properties to objects in Active Directory. You can only create, enable, disable, associate, and disassociate virtual attributes on the primary Administration server. DRA stores the virtual attributes you create in AD LDS or ADAM. DRA replicates virtual attributes on the primary Administration server to secondary Administration servers during the MMS synchronization process.

6.2 Virtual Attribute Tasks

With the appropriate powers, you can manage virtual attributes. The Manage Virtual Attributes role grants powers to create, enable, associate, disassociate, disable, and view virtual attributes.

6.3 Accessing The Virtual Attributes Node

Use the Virtual Attributes node to define and maintain virtual attributes.

To access Virtual Attributes through the console tree:

1. In the left pane, expand **Directory and Resource Administrator**.
2. Expand **Configuration Management**, and then click **Virtual Attributes**.

6.3.1 Creating Virtual Attributes

You must have the Create Virtual Attributes power to create virtual attributes. You must have the View Virtual Attributes power to view virtual attributes.

To create a virtual attribute:

1. In the left pane, expand **Directory and Resource Administrator**.
2. Expand **Configuration Management**, and then click **Virtual Attributes > Attributes**.
3. On the Tasks menu, click **New Virtual Attribute.**
4. On the Welcome tab, click **Next**.
5. Type the name of the virtual attribute in the **Name** field. When specifying a virtual attribute name, do not use special characters.
6. Type an appropriate description for the virtual attribute in the **Description** field.
7. Select the data type of the virtual attribute in the **Type** list.
8. ***If the virtual attribute should accept more than one value***, select the **Multi-valued** checkbox.

9 Click **Next**.

10 Review the information on the Summary tab, and then click **Finish**.

6.3.2 Enabling Virtual Attributes

You need to enable virtual attributes to associate these attributes with Active Directory objects. Once you enable a virtual attribute, administrators can view and associate the virtual attribute with an object.

To enable a virtual attribute:

1 In the left pane, expand **Directory and Resource Administrator**.

2 Expand **Configuration Management**, and then click **Virtual Attributes > Attributes**.

3 In the list pane, select the virtual attribute you want to enable.

4 On the Tasks menu, click **Enable**.

6.3.3 Associating Virtual Attributes with Objects

You can associate only enabled virtual attributes with Active Directory objects. Once you associate a virtual attribute with an object, the virtual attribute is available as part of the object properties.

To add values to virtual attributes you create, you need to create a new user interface extension page for the associated object and add the virtual attributes you want. After you add a virtual attribute to a user interface extension page, you can add values to the virtual attribute by accessing the Object Properties window of the associated object. For more information about creating user interface extension pages, see the Getting Started Guide.

To associate a virtual attribute with an object:

1 In the left pane, expand **Directory and Resource Administrator**.

2 Expand **Configuration Management**, and then click **Virtual Attributes > Attributes**.

3 In the list pane, select the virtual attribute you want to use.

4 ***If you want to associate the virtual attribute with user accounts***, click **Associate > User** on the Tasks menu.

5 ***If you want to associate the virtual attribute with computers***, click **Associate > Computer** on the Tasks menu.

6 ***If you want to associate the virtual attribute with contacts***, click **Associate > Contact** on the Tasks menu.

7 ***If you want to associate the virtual attribute with OUs***, click **Associate > Organizational Unit** on the Tasks menu.

8 ***If you want to associate the virtual attribute with groups***, click **Associate > Group** on the Tasks menu.

9 ***If you want to associate the virtual attribute with dynamic distribution groups***, click **Associate > Dynamic Distribution Group** on the Tasks menu.

NOTE

- You can only associate virtual attributes with users, groups, dynamic distribution groups, computers, contacts, and OUs.
- When you associate a virtual attribute with an object, DRA automatically creates two default custom powers. Assistant Admins require these custom powers to manage the virtual attribute.

6.3.4 Disassociating Virtual Attributes

You can disassociate virtual attributes from Active Directory objects. Any new object that you create does not display the disassociated virtual attribute as part of the object properties.

NOTE: When you disassociate a virtual attribute from an Active Directory object, ensure you also remove the virtual attribute from the corresponding user interface extension page. For information about user interface extension pages, see the Getting Started Guide.

To disassociate a virtual attribute from an Active Directory object:

1. In the left pane, expand **Directory and Resource Administrator**.
2. Expand **Configuration Management**, and then click **Virtual Attributes > Classes**. For example, to disassociate a virtual attribute from user accounts, click **User**.
3. In the list pane, select the virtual attribute you want to disassociate.
4. On the Tasks menu, click **Disassociate**.

6.3.5 Disabling Virtual Attributes

You can disable virtual attributes if they are not associated with an Active Directory object. When you disable a virtual attribute, administrators cannot view or associate the virtual attribute with an object.

To disable a virtual attribute:

1. In the left pane, expand **Directory and Resource Administrator**.
2. Expand **Configuration Management**, and then click **Virtual Attributes > Attributes**.
3. In the list pane, select the virtual attribute you want to disable.
4. On the Tasks menu, click **Disable**.

7 Implementing Custom Tools

You can seamlessly integrate the DRA console with other products by implementing custom tools. Custom tools allow you to run external applications, launch scripts, and open web pages quickly and easily from the DRA console.

7.1 Understanding Custom Tools

DRA supports two types of custom tools:

- Custom tools that launch common desktop utilities, such as Microsoft Office
- Custom tools that you create and distribute to each DRA client computer

You can create a custom tool that launches an antivirus scan from all computers where DRA client is installed. You can also create a custom tool that launches an external application or a tool that requires DRA to update a script periodically. These periodic updates can be changes in the configuration or changes in the business rule. Subsequently, after the periodic updates, DRA replicates custom tools from the primary Administration server to any secondary Administration servers and DRA client computers.

7.1.1 Sample Custom Tools

DRA provides sample custom tools to help you understand how to configure and use custom tools. Enable these custom tools to make them available for AAs.

Copy Group Members

Allows you to copy members from a selected group to a target group. DRA requires the CLI Utility (EA) installed on the Administration server machine to run the sample custom tool.

Group Policy Objects Report

Generates a report that shows Group Policy Objects (GPOs) linked to a specified OU.

Send Mail

Allows AAs to send emails from the DRA console.

NOTE: By default, DRA installs the sample custom tools Visual Basic scripts in the following folder:

{DRAInstallDir}`\SupportingFiles`

7.2 Understanding File Replication

When you create custom tools, you may need to install supporting files used by the custom tool on the DRA client computer before the custom tool can run. You can use DRA file replication capabilities to quickly and easily replicate custom tool support files from the primary Administration server to secondary Administration servers in the MMS as well as to DRA client computers.

You can use custom tools and file replication together to ensure DRA client computers can access custom tool files. DRA replicates custom tool files to secondary Administration servers to ensure DRA client computers connecting to secondary Administration servers can access custom tools.

DRA replicates the custom tool files on the primary Administration server to secondary Administration servers during the MMS synchronization process. DRA downloads the custom tool files to DRA client computers when the DRA client computers connect to the Administration servers.

NOTE: DRA downloads the custom tool files to the following location on the DRA client computers:

{DRAInstallDir}\{MMS ID}\Download

MMSID is the identification of the Multi-Master Set from which DRA downloads the custom tool files.

7.3 Custom Tool Tasks

With the appropriate powers, you can create, run, and manage custom tools. The Manage Custom Tools and Execute Custom Tools roles grants powers to create, modify, and execute custom tools.

The Manage Custom Tools power allows you to create and modify custom tools. If you do not have the Manage Custom Tools power, the DRA console does not display the Custom Tools node. The Execute Custom Tools power allows you to view and run custom tools.

NOTE

- You must be connected to the primary Administration server in order to create a custom tool or upload a file for replication.
- The primary Administration server must replicate the custom tool files to the secondary Administration servers in the MMS before DRA clients can connect and download the custom tool files from the secondary Administration servers.

7.3.1 Accessing Custom Tools Node

Use the Custom Tools node to define and maintain your custom tools.

To access Custom Tools through the console tree:

1. In the left pane, expand **Directory and Resource Administrator**.
2. Expand **Configuration Management**, and then click **Custom Tools**.

7.3.2 Creating a Custom Tool

You can create a custom tool that launches an external application on DRA client computers. DRA launches the external application from within the DRA console.

To create a custom tool that launches an external application:

1. In the left pane, expand **Directory and Resource Administrator**.
2. Expand **Configuration Management**, and then click **Custom Tools**.
3. On the Tasks menu, click **New Custom Tool**.
4. On the Welcome tab, click **Next**.
5. Type the name of the custom tool in the **Name** field. When specifying a custom tool name, do not use special characters.
6. Type the menu and submenu structure for the custom tool in the **Menu and Submenu Structure** field.
7. Click **Next**.
8. Select the type of object on which you want the custom tool to run.
9. Click **Next**.
10. To specify the location of the external application that the custom tool will run, copy and paste or type the full directory path of the external application in the **Location of the application** field.
11. To define the parameter to pass to the external application, copy and paste or type the parameter in the **Parameters to pass to the application** field.

    NOTE: When providing an object property as a parameter, ensure you have the required Read permission on the object property and the Execute Custom Tools power to run the custom tool.
12. To specify the directory where the external application will run, copy and paste or type the variable path of the directory in the **Directory where the application will run** field.
13. Click **Next**.
14. Review the information on the Summary tab, and then click **Finish**.

7.3.3 Modifying Custom Tools Properties

You can change a custom tool by modifying its properties.

To modify custom tool properties:

1. In the left pane, expand **Directory and Resource Administrator.**
2. Expand **Configuration Management**, and then click **Custom Tools**.
3. In the list pane, select the custom tool you want to modify.
4. On the Tasks menu, click **Properties**.
5. Modify the appropriate properties and settings for this custom tool.
6. Click **OK**.

7.3.4 Enabling a Custom Tool

When you enable a custom tool, the DRA console displays the custom tool menu item on the Tasks menu, the shortcut menu, and on the DRA toolbar. DRA users can run the custom tool on specified DRA objects.

To enable a custom tool:

1. In the left pane, expand **Directory and Resource Administrator.**
2. Expand **Configuration Management**, and then click **Custom Tools**.
3. In the list pane, select the custom tool.
4. On the Tasks menu, click **Enable**.

7.3.5 Disabling a Custom Tool

When you disable a custom tool, the custom tool is not available for DRA users. DRA does not delete the custom tool.

To disable a custom tool:

1. In the left pane, expand **Directory and Resource Administrator.**
2. Expand **Configuration Management**, and then click **Custom Tools**.
3. In the list pane, select the appropriate custom tool.
4. On the Tasks menu, click **Disable**.
5. Click **Yes**.

7.3.6 Deleting a Custom Tool

When you delete a custom tool, DRA removes the tool from the DRA console. You cannot restore a deleted custom tool. To temporarily stop DRA users from accessing the custom tool, disable the custom tool. For more information, see Section 7.3.5, “Disabling a Custom Tool,” on page 88.

To delete a custom tool:

1. In the left pane, expand **Directory and Resource Administrator.**
2. Expand **Configuration Management**, and then click **Custom Tools**.
3. In the list pane, select the appropriate custom tool.
4. On the Tasks menu, click **Delete**.
5. Click **Yes**.

7.3.7 Uploading Custom Tool Files for Replication

When you upload files to the primary Administration server, you specify the files you want to upload and replicate between the primary Administration server and all secondary Administration servers in the MMS set. DRA allows you to upload library files, script files and executable files.

The Replicate Files role allows you to replicate files from the primary Administration server to the secondary Administration servers in the MMS as well as DRA client computers. The Replicate File role contains the following powers:

- Delete Files from Server

- Set File Information
- Upload Files to Server

The Delete Files from Server power allows DRA to delete files that no longer exist on the primary Administration server, on secondary Administration servers, and on DRA client computers. The Set File Information power allows DRA to update file information for files on secondary Administration servers. The Upload Files to Server power allows DRA to upload files from the DRA client computer to the primary Administration server.

NOTE: You can upload only one file for replication at a time using the File Replication user interface in the Delegation and Configuration console. For more information about uploading multiple files for replication, see Section 7.3.8, “Replicating Multiple Files Between Administration Servers,” on page 89.

To upload a custom tool file to the primary Administration server:

1. In the left pane, expand **Directory and Resource Administrator**.
2. Expand **Configuration Management**, and then click **File Replication**.
3. On the Tasks menu, click **Upload File**.
4. To search for and select the file you want to upload, click **Browse**.
5. ***If you want to download the selected file to all DRA client computers***, select the **Download to all client computers** check box.
6. ***If you want to register a COM library***, select the **Register COM library** check box.
7. Click **OK**.

NOTE

- DRA uploads the script file or supporting files that need to be replicated to other secondary Administration servers to *{DRAInstallDir}*\FileTransfer\Replicate folder in the primary Administration server. The *{DRAInstallDir}*\FileTransfer\Replicate folder is also referred as *{DRA_Replicated_Files_Path}*.
- DRA uploads the script file or supporting files that need to be replicated to DRA client computers to *{DRAInstallDir}*\FileTransfer\Download folder in the primary Administration server.
- The custom tool file uploaded to the primary Administration server is distributed to secondary Administration servers during the next scheduled synchronization or by manual synchronization. For more information on how to perform a manual server synchronization, see Section 17.6.7, “Synchronizing a Server Set with the Primary Administration Server,” on page 177.

7.3.8 Replicating Multiple Files Between Administration Servers

If you have multiple files you want to upload and replicate between the primary Administration server and secondary Administration servers in your MMS, you can manually upload these files for replication by copying the files to the primary Administration server replication directory, which is in the following location:

{DRAInstallDir}\FileTransfer\Replicate

The replication directory is created when DRA is installed.

The Administration server automatically identifies the files in the replication directory and replicates the files between Administration servers during the next scheduled synchronization. After synchronization, DRA displays the uploaded files in the File Replication window in the Delegation and Configuration console.

NOTE: If you want to replicate files that contain COM libraries that must be registered, you cannot manually copy the files to the Administration server replication directory. You must use the Delegation and Configuration console to upload each file and register the COM library. For more information, see Section 7.3.7, “Uploading Custom Tool Files for Replication,” on page 88.

7.3.9 Replicating Multiple Files to DRA Client Computers

If you have multiple files you want to replicate between the primary Administration server and DRA client computers, you can copy the files to the client replication directory on the primary Administration server, which is in the following location:

{DRAInstallDir}\FileTransfer\Download

The client replication directory is created when DRA is installed.

The Administration server automatically identifies the files in the `Download` folder and replicates the files to the secondary Administration servers during next scheduled synchronization. After synchronization, DRA displays the uploaded files in the File Replication window in the Delegation and Configuration console. DRA downloads the replicated files to the DRA client computers the first time the DRA client computers connect to the Administration servers after replication.

NOTE: If you want to replicate files that contain COM libraries that must be registered, you cannot copy the files into the Administration server download directory. You must use the Delegation and Configuration console to upload each file and register the COM library. For more information, see Section 7.3.7, “Uploading Custom Tool Files for Replication,” on page 88.

7.3.10 Using a Custom Tool

After DRA uploads custom tool files to the primary Administration server, you must restart the DRA console. Restarting the DRA console downloads the custom tools files to the DRA client computer. After you restart the DRA console, DRA displays the custom tool as a menu option when you select the object in the DRA console.

To use custom tools:

1. In the left pane, expand **Directory and Resource Administrator**.
2. Expand **Account and Resource Management**.
3. Expand **All My Managed Objects**.
4. To specify the object for which you want to use the custom tool, complete the following steps:
   - 4a ***If you know the object location***, select the domain and OU that contains this object.
   - 4b ***If you do not know the object location***, specify the search attributes, and then click **Find Now**.
   - 4c In the list pane, select the appropriate object.
5. On the Tasks menu, click **Custom Tools**.
6. Select the appropriate custom tool.

NOTE: If you select an object and DRA does not display a custom tool for that object, your DRA administrator has not created or enabled a custom tool for the object.

8 Implementing OU and Active Directory Administration

An organizational unit (OU) is a container in the Active Directory. An OU can contain user accounts, groups, computers, contacts, and other OUs from the same domain.

Because an object can exist in only one OU, the Active Directory structure can become large and unwieldy. In an attempt to compensate for this limitation, companies often structure their enterprise to use many OUs or a single OU. This structure becomes a security issue in Microsoft Windows domains, where delegate powers can be inherited. DRA resolves this issue by allowing you to define and distribute administration for custom sets of objects, independent of your OU structure.

8.1 How DRA Helps You Manage OUs

Through DRA, you can directly manage OUs and other objects in the Active Directory. DRA provides an integrated tool that gives you a single, complete picture of the Active Directory and your enterprise. From this single point of reference, you can manage the objects in the OUs, the OUs and Microsoft Windows built-in containers themselves, and other OUs across the domain without changing your established security model. DRA enforces the established policies and power delegations through your ActiveViews definitions. This integration ensures that the Active Directory remains a secure and consistent data source.

You can modify the contents and properties of an OU through the Account and Resource Management console or the Delegation and Configuration console. You can also manage the OU hierarchy, such as creating OUs or moving OUs, and verifying the OU location in the Active Directory tree.

8.2 Using ActiveViews to Manage OUs

DRA extends your enterprise management model through ActiveViews. You can manage objects according to your existing OU hierarchy and permissions or implement a management model that is independent from your Active Directory structure. This flexibility allows you to manage OUs and their objects in ways that correspond to your administration needs. Your security model and your administration processes do not need to follow your Active Directory hierarchy.

8.2.1 Using OUs to Create and Maintain ActiveViews

You can use the combination of OUs and ActiveViews to distribute and manage administration capabilities throughout your organization. ActiveViews can include objects from specific OUs or use wildcard specifications to include more than one OU across your enterprise. You can specify OUs from the same domain or from multiple domains. As the OU contents change, your ActiveViews dynamically update to display the appropriate objects.

For example, you can create an ActiveView that includes objects, such as user accounts, from several OUs specified through a naming convention. When you assign this ActiveView to an AA with a role or power, you distribute administration for a specific set of objects and a specific task. Your AA

can manage only the user accounts included in this ActiveView. DRA enforces this delegation regardless of where the objects exist in OU hierarchy, letting you enforce your security model at the level of the managed object.

For more information about creating ActiveViews that manage objects in multiple OUs, see the Getting Started Guide. For more information about implementing a security model, see Chapter 14, “Implementing Your Dynamic Security Model,” on page 135.

8.2.2 Built-in Containers in Microsoft Windows Domains

Microsoft Windows server operating systems automatically create built-in containers in addition to OUs. You cannot rename these containers, nor can you create another OU with the same name as one of these containers. There may be additional limits on what objects these containers can contain. DRA presents only the valid options for each type of OU, object, or container. Typically, you can open a container or create an object to be included in the selected container.

8.3 OU Management Tasks

This section provides information for administrators who are incorporating DRA into their enterprise. The *User Guide* and Help provide concepts and management tasks for AAs who have been delegated powers through DRA. The Help provides step by step guidance for many OU management tasks, such as creating an OU.

To access Help for an OU task:

1. On the Help menu, click **Directory and Resource Administrator Help**.
2. Expand **How To**.
3. Expand **Organizational Unit Tasks**.
4. Click the appropriate task.

9 Implementing User Account Administration

In most environments, managing user accounts involves more than modifying properties and resetting passwords. User accounts are the smallest unit of your security model. Because user accounts provide access to enterprise data and resources, you need to maintain the integrity of your enterprise by establishing the appropriate security rules and policies. A secure enterprise also depends on secured account management. By controlling the power and access of an AA, you can prevent potential security issues, such as power escalation. DRA and ExA give you the policies and rules you need to effectively control and manage user accounts.

9.1 How DRA and ExA Help You Manage User Accounts

DRA and ExA let you manage all aspects of user account administration. From automating mailbox creation to delegating management of specific user account properties, DRA and ExA allow you to address a wide range of user account management tasks and issues. For example, the Account and Resource Management console and the Web Console integrate Microsoft Exchange management with user account management so you can use a single tool to address an entire workflow.

DRA allows you to specify target domain controllers when performing key account security tasks, such resetting a password or disabling an account. You can also ensure secure account deletion and restoration through the Recycle Bin. If you are managing accounts in a Microsoft Windows domain, you can incorporate the Recycle Bin into your security model. For more information about using the Recycle Bin, see Section 12.1, “Understanding the Recycle Bin,” on page 111.

DRA allows you to secure user account management by controlling the level at which an AA can access and modify these accounts. For more information about delegating administration powers, see Chapter 14, “Implementing Your Dynamic Security Model,” on page 135.

9.2 Using ActiveViews to Manage User Accounts

Through ActiveViews, you can display and change the settings of many user account properties, delete user accounts, transfer user accounts from one ActiveView to another, perform Microsoft Exchange tasks, and add or remove user accounts from groups. DRA also integrates user account management with managing your security model. For example, when you create a user account through the Account and Resource Management console, the Create User Wizard allows you to add the new account to the appropriate groups. This integration allows you to use one process to address multiple goals.

If your product license supports ExA, you can perform Microsoft Exchange management tasks, such as specifying a new email address from within the user account properties window. You can also set Microsoft Exchange policies, such as automating mailbox creation, to further coordinate and streamline your account and Microsoft Exchange administration needs. For more information about Microsoft Exchange policy, see Section 13.6, “Creating and Implementing Microsoft Exchange Policy,” on page 126. For more information about Microsoft Exchange administration, see Chapter 15, “Implementing Microsoft Exchange Administration,” on page 155.

DRA uses ActiveViews to enforce your security model. When you create an ActiveView, you can include user accounts from more than one OU or domain, providing your AAs with sets of related objects they can easily manage. You can also specify which ActiveViews use established polices, such as naming conventions, to ensure consistent data management across sets of objects.

NOTE: If you are working with a user account that has a mailbox and you want to manage both objects, you must have corresponding powers for user accounts and mailboxes. For example, if you are renaming a user account that has a mailbox, you must also have power to rename the mailbox. If you are cloning a user account that has a mailbox, you must also have the power to clone and modify the properties of a mailbox.

9.2.1 User Account Naming Conventions

Naming conventions for groups can be vital for orderly and efficient administration of an enterprise. Through DRA, you can define and enforce a naming policy for many objects, including user accounts. For example, you can use the built-in policy `$UPNUniquenessPolicy` to ensure unique user principal names across your enterprise. If you want to establish a naming convention, you can create a policy that validates object names against a wildcard specification. For best performance, use naming conventions that require a standard prefix or suffix, such as `HOU` or `SALES` or `PC LAB`, for the object name.

DRA enforces these policies within the context of the native Microsoft Windows restrictions. If you do not enable a user account naming policy, DRA uses these native restrictions to validate user names. When you create or maintain user logon names and user account naming policies in Microsoft Active Directory, keep the following restrictions in mind:

- Must be unique from other group and user account names in the managed domain
- Can contain up to 20 characters
- Cannot contain only numbers, periods, or spaces
- Leading periods or spaces are cropped

Additional user account naming constraints can also be applied using policy. If a user account naming policy is enforced for the ActiveView in which you are creating the user, the user name must also match the policy rules. For more information about establishing and enforcing naming conventions, see Section 13.5.2, “Available Policies,” on page 124.

9.2.2 Understanding User Account Transfer

DRA allows you to easily copy, or transfer, a user account from one source ActiveView to another target ActiveView. By transferring a user account, you can quickly address delegation or maintenance issues, giving your AAs immediate access to this account.

When you transfer a user account from the source ActiveView to the target ActiveView, DRA creates a new rule in the target ActiveView to specify this account. Thus, when you transfer a user account, you include the account in both ActiveViews. DRA does not clone the selected user account nor remove this account from the source ActiveView.

Once you transfer a user account to another ActiveView, all AAs assigned to the target ActiveView will have power to manage the transferred user account. For example, if you have the Modify All User Properties power in the source ActiveView and the Delete User Account power in the target ActiveView, you will be able to modify and delete the transferred user account. Keep this potential escalation of power in mind when designing and implementing your security model so you can prevent AAs from gaining more powers than you intended.

You can transfer a user account to another ActiveView only if you have the Copy User to Another ActiveView power in the source ActiveView and you are assigned to the target ActiveView. If the target ActiveView has an exclude rule that prevents the user account from becoming a member, the transfer operation fails.

9.2.3 Transferring User Accounts

To transfer a user account from one ActiveView to another, you must have the Copy User to Another ActiveView power in the source ActiveView and you must be assigned to the target ActiveView. Transferring a user account to another ActiveView does not remove the user account from the source ActiveView.

To transfer user accounts to other ActiveViews:

1. Select the user account you want to transfer.
2. On the Tasks menu, click **Transfer**.
3. Select the ActiveView to which you want to transfer the user account.
4. Click **OK**.

9.2.4 Using Group Membership to Create and Maintain ActiveViews

To dynamically manage user accounts, you can create ActiveViews that include users through group membership. Then, when you need to maintain these ActiveViews, you simply add or remove user accounts from these groups. You no longer need to modify the corresponding ActiveViews to include these accounts. DRA automatically updates the ActiveViews, ensuring that the assigned AAs can manage the appropriate accounts. Using group membership produces a more dynamic management model that changes in response to your changing enterprise. This approach can significantly decrease maintenance while increasing performance.

For more information about creating a more robust security model, see Section 14.1.7, “Optimizing Your ActiveView Rules,” on page 138.

9.3 User Accounts in Trusted Domains

When working with ActiveViews that include user accounts from multiple domains, you can view accounts that exist in trusted domains. By providing access to these accounts, DRA allows you to more effectively manage group membership across your enterprise. For example, you can add accounts from trusted domains to local groups in the managed domains.

NOTE: If the trust between the external domain and the DRA managed domain is broken, DRA still displays the members from the external domain in the local group. You cannot view the properties of these members, but you can remove these members from the local group.

To modify a user account, you must connect to the Administration server managing the domain to which the user account belongs. You also must have the required powers in that domain.

9.4 Managing Clone Exceptions

Clone exceptions allow you to define object properties to use as clone exceptions when AAs clone a user account. Clone exception allows you to control which user properties can be cloned when AAs clone user accounts.

With the appropriate powers, you can manage clone exceptions. The Manage Clone Exception role grants powers to create, delete, and view clone exceptions.

9.4.1 Creating Clone Exceptions

You must have the Modify Clone Exceptions power to create clone exceptions. You must have the View Clone Exceptions power to view clone exceptions.

To create a clone exception:

1. In the left pane, expand **Directory and Resource Administrator**.
2. Expand **Configuration Management**, and then click **Clone Exceptions**.
3. On the Tasks menu, click **New Clone Exception.**
4. On the user properties window, search and select the user properties you want to use as clone exceptions when cloning a user account.
5. Click **OK**.

9.4.2 Deleting Clone Exceptions

You must have the Modify Clone Exceptions power to delete clone exceptions from the DRA Delegation and Configuration console.

To delete a clone exception:

1. In the left pane, expand **Directory and Resource Administrator**.
2. Expand **Configuration Management**, and then click **Clone Exceptions**.
3. In the list pane, select the clone exception you want to delete.
4. On the Tasks menu, click **Delete**.

9.5 User Account Management Tasks

This section provides information for administrators who are implementing DRA in their enterprise. The *User Guide* and Help provide concepts and management tasks for AAs who have been delegated powers through DRA. The Help provides step by step guidance for many user account management tasks, such as modifying user account properties.

To access Help for a user account task:

1. On the Help menu, click **Directory and Resource Administrator Help**.
2. Expand **How To**.
3. Expand **User Account Tasks**.
4. Click the appropriate task.

10 Implementing Group Administration

A group is a collection of user accounts, contacts, computers, and other groups. In a traditional security model, a group allows you to simplify your administration processes by collectively managing objects. For example, you can assign permissions to a group or you can use a group as a distribution list. However, in a traditional model, administration powers may be limited to the organizational unit level. Using DRA, you can use groups to establish a more robust security model. DRA extends the traditional administration model by allowing you to distribute power at the group level. When you incorporate groups into your security model, you can fully exploit naming conventions to provide dynamic delegation. By distributing power at the group level, your security model can more accurately reflect how your organization works and more accurately respond to change.

10.1 How DRA and ExA Help You Manage Groups

DRA and ExA let you manage all aspects of group administration. From setting group email addresses to dynamically defining group membership through naming conventions, DRA and ExA allow you to address a wide range of group management tasks and issues. For example, the Account and Resource Management console and Web Console integrate Microsoft Exchange management within group management so you can use a single tool to address an entire workflow. You can also set policies that limit the powers of Microsoft Windows administrator groups.

DRA and ExA manage groups in Microsoft Windows domains and in native mode domains with Microsoft Windows domain controllers. Group type and group scope are handled differently in each mode. For more information about group type and scope see the *User Guide*.

Because DRA allows you to delegate administration powers at the group level, groups provide the foundation for a scalable and dynamic security model. For more information about incorporating groups into your security model, see Chapter 14, “Implementing Your Dynamic Security Model,” on page 135.

10.2 Using ActiveViews to Manage Groups

Through ActiveViews, you can display and change the settings of many group properties, create and clone groups, delete groups, perform Microsoft Exchange tasks, manage group membership, and assign powers. DRA also integrates group management with managing your security model. For example, when you create a group, the Create Group Wizard allows you to add the new group to the appropriate ActiveViews. This integration allows you to use one process to address multiple goals.

If your product license supports ExA, you can perform Microsoft Exchange management tasks, such as hiding group membership and managing distribution lists. You can also set Microsoft Exchange policies, such as automatically generating email addresses, to further coordinate and streamline your group and Microsoft Exchange administration needs. For more information about Microsoft Exchange policy, see Section 13.6, “Creating and Implementing Microsoft Exchange Policy,” on page 126. For more information about Microsoft Exchange administration, see Chapter 15, “Implementing Microsoft Exchange Administration,” on page 155.

When you create an ActiveView, you can include groups from more than one OU or domain, providing your AAs with sets of related objects they can easily manage. You can also limit group management to groups that match a specific type and scope. To ensure consistent data management

across sets of objects, you can specify which ActiveViews use established policies, such as naming conventions. In this way, DRA uses ActiveViews to enforce your security model. For more information about maintaining ActiveViews based on group membership, see Section 9.2.4, “Using Group Membership to Create and Maintain ActiveViews,” on page 97.

10.2.1 Group Naming Conventions

A naming convention for groups is vital for orderly and efficient enterprise administration. Use DRA to define and enforce a naming policy for your groups. For example, you can use the built-in policy `$GroupNameLengthPolicy` to limit group name length to 64 characters. You can also create a policy that validates group names against a wildcard specification. For best performance, use naming conventions that require a standard prefix or suffix, such as `HOU` or `SALES` or `PC LAB`, for the group name.

DRA enforces the group policies you specify within the context of the native Microsoft Windows restrictions. If you do not enable a group naming policy, DRA uses native Microsoft Windows restrictions to validate group names. When you create or maintain group names and group naming policies, keep the following restrictions in mind:

- Group names must be unique from other group and user account names in the managed domain.
- Group names can contain up to 64 characters.
- Group names cannot contain only numbers, periods, or spaces.
- Any leading periods or spaces in group names are cropped.

Additional group naming constraints can also be applied using policy. If a group naming policy is enforced for the ActiveView in which you are creating the group, the group name must also match the policy rules. For more information about establishing and enforcing naming conventions, see Section 13.5.2, “Available Policies,” on page 124.

10.2.2 User-Created Local Groups

When you use DRA to create a group, DRA creates the group using the access account for the managed domain. You can create local or global groups only if the access account has the appropriate powers. This power check ensures secure group management, preventing potential security issues where a user can gain access to sensitive accounts or abuse privileges.

Your ActiveView configurations can also provide an extra level of security. You can use DRA to create an ActiveView that includes all `ABC*` groups. You can also create a new local group, such as ABCL. DRA adds this new user-created local group to the ActiveView, but does not automatically include the group members. If you are associated with the ActiveView and have the appropriate powers, you can manage the ABCL group but you cannot manage the group members. DRA prevents you from inappropriately extending your powers.

10.3 Groups in Trusted Domains

When working with groups from multiple domains, you can view global groups located in trusted domains. By providing access to these groups and their members, DRA allows you to more effectively manage group membership across your enterprise. For example, you can add global groups from trusted domains to groups in the managed domains.

NOTE: If the trust between the external domain and the DRA managed domain is broken, DRA still displays the groups from the external domain in the local groups. You cannot view the properties of these groups, but you can remove these groups from the local group.

To modify a group in a managed domain, you must connect to the Administration server managing the domain to which the group belongs. You also must have the appropriate powers in that domain.

10.4 Managing Native Built-in Security Groups

To provide a more secure environment, DRA allows you to limit the powers given to Microsoft Windows built-in security groups. The ability to modify group membership, built-in security group properties, or properties of the group members can have important security implications. For example, if you can change the password of a user in the Server Operators group, you can then log on as that user and exercise the powers delegated to this built-in security group.

DRA prevents this security issue by providing a policy that checks the powers you have for a native built-in security group and its members. This validation ensures that your requested actions do not escalate these powers. After you enable this policy, an AA who is a member of a built-in security group, such as the Server Operators group, can only manage other members of the same group.

10.4.1 Native Built-in Security Groups You Can Restrict

You can restrict the powers of the following Microsoft Windows built-in security groups using DRA policies:

- Account Operators
- Administrators
- Backup Operators
- Cert Publishers
- DNS Admins
- Domain Admins
- Enterprise Admins
- Group Policy Creator Owners
- Print Operators
- Schema Admins

NOTE: DRA refers to the built-in security groups by their internal identifiers. As a result, DRA supports these groups even if the groups are renamed. This feature ensures that DRA supports built-in security groups with different names in different countries. For example, DRA refers to the Administrators group and the *Administratoren* group with the same internal identifier.

10.4.2 Restricting Actions on Native Built-in Security Groups

DRA uses policy to limit the power native built-in security groups and their members can exercise. This policy, called `$SpecialGroupsPolicy`, restricts the actions a member of a native built-in security group can perform on other members or other native built-in security groups. DRA enables this policy by default. If you do not want to restrict actions on native built-in security groups and their members, you can disable this policy.

When this policy is enabled, DRA uses the following validation tests to determine whether an action is permitted on a native built-in security group or its members:

- If you are a Microsoft Windows administrator, you can perform actions on native built-in security groups and their members for which you have the appropriate powers.
- If you are a member of a built-in security group, you can perform actions on the same built-in security group and its members, as long as you have the appropriate powers.
- If you are not a member of a built-in security group, you cannot modify a built-in security group or its members.

For example, if you are a member of the Server Operators and Account Operators groups and you have the appropriate powers, you can perform actions on members of the Server Operators group, members of the Account Operators group, or members of both groups. However, you cannot perform actions on a user account that is a member of the Print Operators group and the Account Operators group.

DRA restricts you from performing the following actions on native built-in security groups:

- Cloning a group
- Creating a group
- Deleting a group
- Adding a member to a group
- Removing a member from a group
- Moving a group to an OU
- Modifying properties of a group
- Copying a mailbox
- Removing a mailbox
- Cloning a user account
- Creating a user account
- Deleting a user account
- Moving a user account to an OU
- Modifying user account properties

DRA also restricts actions to ensure you do not gain powers over an object. For example, when you add a user account to a group, DRA checks to ensure you do not gain additional powers over the user account because it is a member of that group. This validation helps protect against an escalation of power.

10.5 Managing Group Membership Security

Managing group membership security includes controlling how users interact with distribution groups and security groups, such as through Microsoft Outlook. For example, you may want the Help Desk to grant a project team manager the ability to update the team's distribution list or mail-enabled security group. By allowing users to manage group memberships, you can achieve secure and easy maintenance across distributed departments.

To report on changes to group membership security settings, generate the appropriate Detailed Activities Change report. For more information, see the *User Guide*.

10.5.1 Allowing Users to Manage Group Memberships

You can allow users to manage specific Microsoft Windows group memberships by configuring the following settings:

- Use the `Managedby` Active Directory attribute to grant ownership of a group membership list.
- Use group membership security permission settings to grant or deny the ability to view or modify group memberships through Microsoft Outlook.

By setting these permissions, you can delegate group membership management to a specific user account or group. As project assignments change, or new hires are added to a department, the group manager can independently update the group membership. The group manager does not require additional powers or access to the DRA user interfaces.

10.5.2 Delegating Group Membership Security

To allow your AAs to manage group membership security, delegate the appropriate role or power. Use the Delegation Wizard to set the following assignments:

Assistant Admin	Role or Power	ActiveView
Specify who should audit group membership security	View All Group Properties power	Specify which groups have security permission settings
Specify who should set group membership security	Manage Group Membership Security role	Specify which groups have or need security permission settings
Specify who should set group ownership	Modify All Group Properties	Specify which groups require ownership

For more information, see the *Getting Started Guide*.

10.6 Temporary Group Assignments

DRA allows you to create temporary group assignments that provide authorized users temporary access to resources. AAs can use temporary group assignments to assign users to a target group for a specific time period. At the end of the time period, DRA automatically removes the users from the group.

The Manage Temporary Group Assignments role grants AAs powers to create and manage temporary group assignments.

Use the following powers to delegate the creation and management of temporary group assignments:

- Create Temporary Group Assignments
- View Temporary Group Assignments
- Delete/Modify Temporary Group Assignments
- Add Object to Group
- Remove Object from Group

To create temporary group assignments, AAs must have the Manage Temporary Group Assignments role or the Create/Modify Temporary Group Assignments, Add Object to Group, and Remove Object from Group powers in an ActiveView. The target group and the target users must also be in the same ActiveView.

NOTE

- AAs can create, modify, and delete temporary group assignments only on the primary Administration server. AAs cannot manage temporary group assignments on secondary Administration servers.
- DRA replicates temporary group assignments from the primary Administration server to secondary Administration servers during MMS replication.
- You cannot create a temporary group assignment for a user who is already a member of the target group. If you try to create a temporary group assignment for a user who is already a member of the target group, DRA displays a warning message and does not allow you to create a temporary group assignment for the user.
- If you create a temporary group assignment for a user who is not a member of the target group, DRA removes the user from the group when the temporary group assignment expires.

For more information about creating and using temporary group assignments, see the *User Guide*.

10.7 Group Management Tasks

This section provides information for administrators who are incorporating DRA into their enterprise. The *User Guide* and Help provide concepts and management tasks for AAs who have been delegated powers through DRA. The Help provides step by step guidance for many group management tasks, such as modifying group membership.

To access Help for a group task:

1. On the Help menu, click **Directory and Resource Administrator Help**.
2. Expand **How To**.
3. Expand **Group Tasks**.
4. Click the appropriate task.

11 Implementing Resource Administration

Through DRA, you can quickly and effectively manage many types of resources. Quick and effective resource management is an important part of your security model because resources provide access to your enterprise data. To securely manage each resource, you need to ensure your AAs have the appropriate levels of power.

DRA helps you manage the following resource objects:

- Computers
- Connected Users
- Devices
- Event logs
- Open files
- Printers and print jobs
- Published printers
- Services
- Shares

Because DRA allows you to manage resources across organizational units and domains, you can easily establish policies and delegate power for consistent and secure management.

11.1 How DRA Helps You Manage Resources

DRA allows you to manage all aspects of resource administration. From automating share creation to delegating the shutdown of specific services, DRA allows you to address a wide range of resource management tasks and issues.

DRA allows you to secure resource management by controlling the level at which an AA can access and modify these objects. For more information about delegating administration powers, see Chapter 14, “Implementing Your Dynamic Security Model,” on page 135.

NOTE: DRA uses the Administration server service account or access account to access resources in a managed domain by default. Therefore, to manage computers and resources, the Administration server service account or access account must have administrator permissions, such as being a member of the local Administrators group, on all computers you want to manage.

11.2 Using ActiveViews to Manage Resources

Through ActiveViews, you can display and change the settings of many resource properties, create and clone resources, delete resources, as well as stop and start resources. DRA also integrates resource management with managing your security model. For example, when you create a computer, the Create Computer Wizard allows you to specify which users or groups should be given

permissions to join this object to another domain. You can also assign powers that allow an AA to manage resources associated with a specific user account. This integration allows you to use one process to address multiple goals.

When you create an ActiveView, you can include resources from more than one OU or domain, providing your AAs with sets of related objects they can easily manage. You can also specify which ActiveViews use established policies, such as naming conventions, to ensure consistent data management across sets of resources. In this way, DRA uses ActiveViews to enforce your security model.

To manage resources, the Administration server service account must have the appropriate administrator permissions. For example, the Administration server service account can be a member of the Administrators local group on all the computers for which you want to manage resources. For more information, see the *Installation Guide.*

11.2.1 Resource Naming Conventions

Naming conventions for resources can be vital for orderly and efficient administration of an enterprise. Through DRA, you can define and enforce a naming policy for many objects, including resources. For example, you can create a policy that limits a resource name length to 64 characters. If you want to establish a naming convention for computers, you can create your own policy that validates names against a wildcard specification. For best performance, use naming conventions that require a standard prefix or suffix, such as `HOU` or `SALES` or `PC LAB`, for the object name.

DRA enforces these policies within the context of the native Microsoft Windows restrictions. If you do not enable a resource naming policy, DRA uses these restrictions to validate resource names. When you create or maintain resource names and resource naming policies, keep the following restrictions in mind:

- Resource name must be unique from other account names in the managed domain.
- Append a dollar sign (`$`) to a computer name.
- Resource name cannot contain only numbers, periods, or spaces.
- Any leading periods or spaces in the resource name are cropped.

Additional resource naming constraints can also be applied using home directory policies. If a resource naming policy is enforced for the ActiveView in which you are managing the resource, the resource name must also match the policy rules. For more information about establishing and enforcing naming conventions, see Section 13.5.2, “Available Policies,” on page 124. For more information about using home directory policies, see Section 13.3, “Creating and Implementing Home Directory Policy,” on page 117.

11.2.2 Computers

DRA allows you to add or remove computers from a managed domain, shut down computers, establish trusts with computer accounts for delegation, disable and enable computer accounts, and view and modify properties for computer accounts. If you are managing a Microsoft Windows domain, you can delete computer accounts that contain other objects, such as a shared resource. Because computers provide access to enterprise resources, DRA allows you to manage your resources by managing the associated computers.

DRA allows you to manage computers from multiple OUs and domains. When you add a computer to a domain, DRA creates a computer account in the domain for that computer. You can then connect to the computer and configure the computer to use this account. DRA also automatically adds the Domain Admins global group to the Administrators local group on this computer. Since the

Administration server service account is usually a member of the Domain Admins global group, the Administration server service account is automatically a member of the Administrators local group on each computer in the managed domain.

To manage computers, you must have the appropriate powers, such as those included in the Computer Administration role. Some built-in resource roles also include computer account powers. For example, the Create and Delete Resources role allows you to create computer accounts. For more information about resource roles, see Section 4.5, “Understanding Built-in Roles,” on page 70.

11.2.3 Services

A service is a type of application that gets special treatment from the Microsoft Windows operating system. Because services control background application tasks, services do not have user interfaces and can run even when no user is currently logged on to a computer.

Through DRA, you can start and stop services, and view or modify the properties for services in the managed domain. You can also modify the startup type and specify whether the services use system or user accounts. DRA allows you to manage services through the associated computers.

To manage services, you must have the appropriate powers, such as those included in the Manage Services role. Some built-in resource roles also include service powers, such as the power to modify service properties. For more information about resource roles, see Section 4.5, “Understanding Built-in Roles,” on page 70.

11.2.4 Shares

A share is a way to make resources, such as folders and files, available to other users on the enterprise. Each share has a share name that refers to a shared folder on the server. DRA allows you to manage all shares in a given OU or domain, including hidden shares, administrator shares, common shares, and user created shares. With DRA, you can manage shares by managing the associated computers.

Through DRA, you can create, clone, or delete shares, as well as view or modify the properties of a share in the managed domain. For example, to conform to licensing agreements or reduce activity on busy servers, you can also limit the number of user accounts able to connect to shares at one time.

DRA allows you to manage hidden shares that are not administrator shares. Hidden shares are designated by a dollar sign (`$`) suffix, such as `C$`, `D$`, or `IPC`$. Some hidden shares are administrator shares. When you restart a computer after deleting an administrator share, Microsoft Windows recreates the default administrator shares that may have been deleted. Deleting administrator shares can cause some applications to fail.

You can easily create an ActiveView with a custom exclude rule so that the Account and Resource Management console does not display hidden shares in that ActiveView. To do this, create a custom ActiveView that uses the following rule:

```
Exclude shares with name matching *$ on any computer in any OU in any domain
```

To manage shares, you must have the appropriate powers, such as those included in the Manage Shared Folders role. Some built-in resource roles also include share powers, such as the power to create or clone shares. For more information about resource roles, see Section 4.5, “Understanding Built-in Roles,” on page 70.

11.2.5 Printers and Print Jobs

DRA allows you to manage the logical printers in the managed domains. To fully manage these printers, you need to manage the print queues that service those printers, as well as the print jobs. DRA allows you to manage printers by managing the associated computers.

Through DRA, you can pause, resume, start, modify, and stop printers, as well as view and modify printer properties. DRA also allows you to modify printer priorities. To add or delete a printer, use the native Microsoft Windows tools.

You can pause, resume, restart, or cancel print jobs. You can also view and modify print job properties, such as the document name, status, owner, pages, size, time submitted, and port.

To manage printers and print jobs, you must have the appropriate powers, such as those included in the Manage Printers and Print Jobs role.

Some built-in resource roles also include print job and printer powers. For example, the Start and Stop Resources role allows you to start a printer. The Manage Resources for Managed Users role grants print job powers if you also have power over the user account associated with the print job. To successfully delegate this power, the ActiveView must include the user account and the print job. For more information about resource roles, see Section 4.5, “Understanding Built-in Roles,” on page 70.

11.2.6 Published Printers

DRA allows you to manage published printers in the managed domains. A published printer is a printer published in Active Directory. A published printer can be a network printer that is not directly connected to a server or it can be a printer hosted by cluster server. You can search and manage all printers published in the Active Directory.

Through DRA, you can pause, resume, start, modify, and stop published printers, as well as view and modify certain published printer properties. To add or delete a published printer, use the native Microsoft Windows tools.

You can pause, resume, restart, or cancel print jobs. You can also view print job properties, such as the document name, status, owner, pages, size, time submitted, and port.

With the appropriate powers, you can perform various printer management tasks, such as stopping a printer. The Manage Printers and Print Jobs role grants powers to manage published printers and print jobs. The Manage Resources for Managed Users power grants print job powers if you also have power over the user account associated with the print job. For more information on roles, see Section 4.5, “Understanding Built-in Roles,” on page 70.

11.2.7 Connected Users

A session is established whenever a user connects to a particular resource on a remote computer in the managed domain. DRA refers to these sessions as connected users. DRA allows you to manage these sessions by managing the associated computers.

Through DRA, you can disconnect a user from a resource or view the session properties. When you disconnect a connected user, this action does not log out the user or prevent the user from connecting to the resource again.

To manage a connected user, you must have the appropriate powers, such as those included in the Resource Administration and Manage Resources for Managed Users roles. For more information about resource roles, see Section 4.5, “Understanding Built-in Roles,” on page 70.

11.2.8 Devices

A device is any piece of equipment attached to a network, such as a computer, printer, modem, or any other peripheral equipment. The Microsoft Windows operating system cannot recognize an installed device until you install and configure the appropriate driver. A device driver enables a specific piece of hardware to communicate with the operating system. DRA allows you to manage devices by managing the associated computers.

Through DRA, you can configure and manage any device on a computer in the managed domain. For example, you can specify whether a computer starts devices automatically when the computer starts, or whether a user or dependent device starts devices manually. You can also disable devices. To manage devices, you must have the appropriate powers, such as those included the Resource Administration role. For more information about resource roles, see Section 4.5, “Understanding Built-in Roles,” on page 70.

11.2.9 Open Files

An open file is a connection to a shared resource, such as a file or a pipe. A pipe allows one process to communicate with another local or remote process. Through DRA, you can quickly and effectively manage open files throughout your managed domains. DRA allows you to manage open files by managing the associated computers.

DRA allows you to close open files from resources on the network so you can safely shut down a computer or install a new device or service. You can also view properties for an open file and determine which files users access most often. Before closing an open file, you should notify users and give them time to save their data. You can refresh the open files view to get the latest information, so you know exactly how many open files are being used.

To manage open files, you must have the appropriate powers, such as those included in the Resource Administration role. For more information about resource roles, see Section 4.5, “Understanding Built-in Roles,” on page 70.

11.2.10 Event Logs

Through DRA, you can manage several native event logs. Event logs provide information about your enterprise performance, security, and administration.

An event is an important system or application occurrence. The Microsoft Windows operating system records information about events in event log files. There may be several event logs stored on each computer. Through DRA, you can clear event logs, view log properties, back up logs, or launch the native Event Viewer to display log entries. When you back up a log file, DRA saves the event log with a unique file name in a standard location on the selected computer.

The Administration server uses several native event logs to record, audit, and report your enterprise activity.

DRA allows you to manage the following event logs:

Application	Records events logged by an application on the computer, such as a service startup or failure. For example, DRA and ExA store events in the Application log.
Directory	Records events related to domain controllers maintaining the security database.
DNS	Records events related to resolving Domain Name System (DNS) names from IP addresses.

File Replication	Records events related to file replication services provided by the operating system.
Security	Records events that include logon attempts, file and directory access, and security policy changes based on the audit policy options.
System	Records events logged by the Microsoft Windows system components, such as the failure of a driver and services starting and stopping.

To view these logs, you can start the native Event Viewer through the Account and Resource Management console or the Delegation and Configuration console. To manage event logs and modify event log properties, you must have the appropriate powers, such as those included in the Resource Administration role.

11.3 Resource Management Tasks

This section provides information for administrators who are incorporating DRA into their enterprise. The *User Guide* and Help provide concepts and management tasks for AAs who have been delegated powers through DRA. The Help provides step by step guidance for many resource management tasks, such as managing a print job.

To access Help for a resource task:

1. On the Help menu, click **Directory and Resource Administrator Help**.
2. Expand **How To**.
3. Expand **Resource Tasks**.
4. Click the appropriate task.

12 Implementing the Recycle Bin

The Recycle Bin allows you to securely delete Microsoft Windows user accounts, groups, contacts, and computer accounts. From the Recycle Bin, you can permanently delete these accounts or restore them to their original state with all data, such as SIDs, ACLs, and group memberships, intact. This flexibility provides a safer way to manage user accounts, groups, contacts, and computer accounts.

12.1 Understanding the Recycle Bin

You can enable or disable the Recycle Bin for each Microsoft Windows domain, controlling the management of accounts across your enterprise. If you enable the Recycle Bin and then delete a user account, group, dynamic distribution group, dynamic group, resource mailbox, contact, or computer account, the Administration server disables the selected account and moves it to the Recycle Bin container. Once DRA moves the account to the Recycle Bin, the account does not display in the ActiveViews to which it belonged. If you delete a user account, group, contact, or computer account when the Recycle Bin is disabled, the Administration server permanently deletes the selected account. You can disable a Recycle Bin that contains previously deleted accounts. However, once the Recycle Bin is disabled, these accounts are no longer available in the Recycle Bin node.

NOTE

- To allow an AA to permanently delete accounts from the All My Managed Objects node as well as the Recycle Bin, assign the relevant power from the following list:
  - Delete User Account Permanently
  - Delete Group Permanently
  - Delete Computer Permanently
  - Delete Contact Permanently
  - Delete Dynamic Distribution Group Permanently
  - Delete Dynamic Group Permanently
  - Delete Resource Mailbox Permanently
- If multiple Administration servers manage different subtrees in the same Microsoft Windows domain, you can use the Recycle Bin to view any deleted account from this domain regardless of which Administration server manages that account.

12.2 Accessing the Recycle Bin

You can access the Recycle Bin in either the Account and Resource Management or Delegation and Configuration console. To access the Recycle Bin, click the **Recycle Bin** node in the left pane of the console.

By default, the Recycle Bin is enabled for each Microsoft Windows domain DRA manages.

NOTE: If the account you specify to access a Microsoft Windows subtree does not have native Administrator permissions, DRA disables the Recycle Bin. Use the Recycle Bin Utility to ensure the access account has correct permissions. For more information, see Section B.3, “Recycle Bin Utility,” on page 249.

12.3 Using the Recycle Bin

Use the Recycle Bin to permanently delete accounts, restore accounts, or view properties of deleted accounts. You can also search for specific accounts and track how many days a deleted account has been in the Recycle Bin.

Use the **Restore All** or **Empty Recycle Bin** options to quickly and easily restore or delete these accounts.

When you restore an account, DRA reinstates the account, including all permissions, power delegations, policy assignments, group memberships, and ActiveView memberships. If you permanently delete an account, DRA removes this account from the Active Directory.

To ensure secure account deletion, only AAs who have the following powers can permanently delete the accounts from the Recycle Bin:

- Delete User Account Permanently
- Delete User from Recycle Bin
- Delete Group Account Permanently
- Delete Group from Recycle Bin
- Delete Computer Account Permanently
- Delete Computer from Recycle Bin
- Delete Contact Account Permanently
- Delete Contact from Recycle Bin
- Delete Dynamic Distribution Group Permanently
- Delete Dynamic Distribution Group from Recycle Bin
- Delete Dynamic Group Permanently
- Delete Dynamic Group from Recycle Bin
- Delete Resource Mailbox Permanently
- Delete Resource Mailbox from Recycle Bin
- View all Recycle Bin Objects

To restore an account from the Recycle Bin, AAs must have the following powers in the OU that contains the account:

- Restore User From Recycle Bin
- Restore Group from Recycle Bin
- Restore Dynamic Distribution Group from Recycle Bin
- Restore Dynamic Group from Recycle Bin
- Restore Resource Mailbox from Recycle Bin
- Restore Computer from Recycle Bin

- Restore Contact from Recycle Bin
- View all Recycle Bin Objects

For more information on implementing the Recycle Bin, see "Scenario for Including the Recycle Bin in Your Security Model".

NOTE

- If two AAs act on the same account within the same accounts cache refresh cycle, DRA can inadvertently restore the "deleted" account.
- If you delete an AA account to the Recycle Bin, DRA continues to display the ActiveView and role assignments for this account. Instead of displaying the name of the deleted AA account, DRA displays the security identifier (SID). You can remove these assignments before you permanently delete the AA account. For more information, see Section 14.5.8, "Removing Assistant Admin Assignments," on page 148.
- DRA deletes the home directory after you delete the user account from the Recycle Bin. For more information, see Section 13.3.4, "Home Directory Automation and Rules," on page 118.
- You can delete your own account or an access account.
- If you delete a user who has an Office 365 license, the user account goes to the Recycle Bin and the license is removed. If you later restore the user account, the Office 365 license will also be restored.

12.3.1 Enabling the Recycle Bin

You can enable the Recycle Bin for specific Microsoft Windows domains. By default, DRA enables the Recycle Bin for each domain it manages. You must be a member of the DRA Admins or DRA Configuration Admins AA group to enable the Recycle Bin.

If your environment includes the following configuration, use the Recycle Bin Utility to enable this feature:

- DRA is managing a subtree of this domain
- The Administration server service or access account does not have permission to create the Recycle Bin container, move accounts to this container, and modify accounts in this container.

You can also use the Recycle Bin Utility to verify the Administration server service or access account permissions on the Recycle Bin container. For more information about this utility, see Section B.3, "Recycle Bin Utility," on page 249.

To enable the Recycle Bin:

1. In the left pane, expand **Recycle Bin**.
2. Select the domain for which you want to enable the Recycle Bin.
3. On the Task menu, click **Enable**.

12.3.2 Disabling the Recycle Bin

You can disable the Recycle Bin for specific Microsoft Windows domains. If a disabled Recycle Bin contains accounts, you cannot view, permanently delete, or restore these accounts.

You must be a member of the DRA Admins or DRA Configuration Admins AA group to disable the Recycle Bin.

To disable the Recycle Bin:

1. In the left pane, expand **Recycle Bin**.
2. Select the domain for which you want to disable the Recycle Bin.
3. On the Task menu, click **Disable**.

13 Enforcing Policy

Through DRA and ExA, you can customize policy and automate tasks to help maintain consistent data, provide a more secure environment, and streamline the administration of your enterprise. Use the DRA ADSI Provider to connect DRA or ExA with your company databases or further enhance the built-in policy power in DRA and ExA.

13.1 Understanding Policy

DRA and ExA let you configure various policies that help you secure your enterprise and prevent data corruption. These policies work within the context of the dynamic security model, ensuring that policy enforcement automatically keeps up with your changing enterprise. Establishing policies, such as naming conventions, disk usage limits, and property validation allows you to enforce rules that help maintain the integrity of your enterprise data.

DRA and ExA let you quickly define policy rules for these enterprise management areas:

- Microsoft Exchange policy
- Home directory policy
- Built-in policies for groups, user accounts, and computers

To manage or define policy, you must have the appropriate powers, such as those included in either the DRA Admins or Manage Policies and Automation Triggers roles. To help you manage your policies, DRA provides the Policy Details report. This report provides the following information:

- Indicates whether the policy is enabled
- Lists associated operations
- Lists objects governed by this policy
- Provides policy scope details

You can use this report to ensure that your policies are defined properly. You can also use this report to compare policy properties, catching conflicts and better enforcing policies across your enterprise.

13.1.1 What Is a Policy?

A policy is a rule that the Administration server enforces whenever the specified operation runs. When you define a policy, you set the rule parameters, such as whether the policy must always pass, whether the policy should be enabled for immediate use, and, if applicable, which ActiveViews or AAs should be governed by this policy. Some policies act as automation triggers, extending the associated task while ensuring that your enterprise data remains consistent. These rules determine how the Administration server enforces your policy.

Some example policies include:

- When you create a new user account, the Administration server automatically creates a home directory and names it based on the naming convention you set.
- When you add a user account object to a group, the Administration server verifies that the resulting group size does not exceed the limit you set.

- When you create a new group, the Administration server verifies that the group name does not exceed the length limit you set. This type of policy ensures that the property field is valid.
- When you create a new mailbox, the Administration server automatically creates an email address using the specific protocol and naming convention.

There are a number of built-in verification policies that DRA and ExA implement by default. Some built-in policies, such as the home directory policies, combine policy rules with the power of automation triggers.

You can also create custom policies that combine validation rules with an automation trigger script that performs related tasks. You can customize existing workflows, allowing you to validate, automate, and streamline your administration tasks. For more information about custom policy, see Section 13.8, “Creating and Implementing Custom Policy,” on page 131. For more information about automation triggers, see Section 18.1, “Understanding Automation Triggers,” on page 191.

13.1.2 How the Administration Server Enforces Policy

You can associate each task, or administration operation, with one or more policies. When you perform an operation associated with a policy, the Administration server runs the policy and enforces the specified rules. If the server detects a policy violation, it returns an error message. If the server does not detect a policy violation, it completes the operation. You can limit the scope of a policy by associating it with particular ActiveViews or AA groups.

If an operation is associated with more than one policy, the Administration server enforces the policies in alphabetical order. That is, Policy A will be enforced before Policy B, regardless of the specified rules.

To ensure that your policies do not conflict with each other, use the following guidelines:

- Name the policies so that they execute in the proper order
- Verify that each policy does not interfere with validations or actions performed by other policies
- Thoroughly test custom policies before implementing them in your production environment

The Administration server enters the policy status in the audit log each time a policy runs. These log entries record the return code, associated operations, objects acted on, and whether the custom policy succeeded.

WARNING: Policies are run using the Administration service account. Since the service account has administrator permissions, policies have full access to all enterprise data. Thus, AAs associated with the built-in Manage Policies and Automation Triggers role could obtain more power than you intended.

13.2 Accessing Policy

Through the Policy and Automation Management node, you can access Microsoft Exchange and home directory policies, as well as built-in and custom policies. Use the following common tasks to improve your enterprise security and data integrity.

Configure Exchange Policies

Allows you to define Microsoft Exchange configuration, mailbox policy, automatic naming, and proxy generation rules. These rules can define how mailboxes are managed when an AA creates, modifies, or deletes a user account.

Configure Exchange Online Policies

Allows you to enforce invalid characters and character length policies to prevent directory synchronization failures.

The Office 365 Rules policy allows you to specify how Exchange Online manages Office 365 mailboxes when you create or delete user accounts.

Configure Home Directory Policies

Allows you to automatically create, rename, or delete home directories and home shares when an AA creates, renames, or deletes a user account. Home directory policy also allows you to enable or disable disk quota support for home directories on Microsoft Windows servers as well as on non-Windows servers.

Manage Policies

Allows you to validate or check properties associated with security objects in your enterprise. You can create custom policies or choose from among the built-in policies, including policies for group size, user account name length, native Microsoft Windows special group restrictions, and user principal name uniqueness.

To access Policy and Automation Management through the console tree:

1. In the left pane, expand Directory and Resource Administrator.
2. Select **Policy and Automation Management**.

13.3 Creating and Implementing Home Directory Policy

When you manage a large number of user accounts, creating and maintaining these home directories and shares can require a lot of time and can be a source of security errors. Additional maintenance can be required each time a user is created, renamed, or deleted. Home directory policies help you manage home directory and home share maintenance.

DRA allows you to automate the creation and maintenance of user home directories. For example, you can easily configure DRA so that the Administration server creates a home directory when you create a user account. In this case, if you specify a home directory path when you create the user account, the server automatically creates the home directory per the specified path. If you do not specify a path, the server does not create the home directory.

DRA supports Distributed File System (DFS) paths during creation of user home directories or configuration of home directory policies for users in allowable parent paths. You can create, rename, and delete home directories on Netapp Filers and DFS paths or partitions.

13.3.1 Administration Server Requirements

For each computer where you need to create a home share, the Administration server service account or access account should be an administrator on that computer or a member of the Administrators group in the corresponding domain.

An administration share, such as `C$` or `D$`, must exist for each drive on which DRA manages and stores home directories. DRA uses the administration shares to perform some home directory and home share automation tasks. If these shares do not exist, DRA cannot provide home directory and home share automation.

13.3.2 Configuring Home Directory Allowable Paths for NetApp Filers

To configure the Allowable Parent Paths for a NetApp Filer:

1. In the left pane, expand Directory and Resource Administrator.
2. Open the Deligation and Configuration Console as a DRA Admin, select **Policy and Automation Management**.
3. On the Tasks menu, select **Configure Home Directory Policies...**
4. In the **Allowable parent path**s text box, enter one of the allowable paths from the following table:

Share type	Allowable path
Windows	(*FileName**adminshare:**volumerootpath**directorypath*)
Non-Windows	(*non-windows**share*)

5. Click **Add**.
6. Repeat Steps **1**-**5** for each allowable parent path wherever you want to apply the home directory policies.

13.3.3 Understanding Home Directory Policy

To be consistent with proper Microsoft Windows security policies, DRA creates access control restrictions at the directory level only. Placing access control restrictions at both the share name level and the file or directory object level often leads to a confusing access scheme for administrators and users.

When you change an access control restriction for a home share, DRA does not change the existing security for that directory. In this case, you must ensure that the user accounts have the appropriate access to their own home directories.

13.3.4 Home Directory Automation and Rules

DRA automates home directory maintenance tasks by managing home directories when you modify a user account. DRA can perform different actions when a user account is created, cloned, modified, renamed, or deleted.

To successfully implement your home directory policy, consider the following guidelines:

- Ensure the specified path uses the correct format.
  - To specify a path for a single home directory, use one of the templates from the following table:

Share Type	Path Template
Windows	*computer**share*\. For example, if you want DRA to automatically create a home directory in the `Home Share` folder on the server01 computer, type `\\server01\Home Share\`
Non-Windows	*non-windows**share*

- To standardize home directory administration on the root directory of the corresponding home share, use the Universal Naming Convention syntax, such as *server name**C:**path to root directory*.
- To specify a path for nested home directories, use one of the templates from the following table:

Share Type	Path Template
Windows	*computer**share**first directory**second directory*\ For example, if you want DRA to automatically create a home directory in the existing `JSmith\Home directory` under the Home Share folder on the `server01` computer, type `\\server01\Home Share\JSmith\Home`.
Non-Windows	*non-windows**share**first directory**second directory*\

NOTE: DRA also supports the following formats: *computer**share**username* and *computer**share**%username%*. In each case, DRA automatically creates a home directory for the associated user account.

- When you define a policy or automation trigger for managing home directories on a NetApp filer, you need to use a different format for the directory specification.
  - If you are using NetApp filers, specify the parent directory in the following format: *FilerName**adminshare:**volumerootpat*h*directorypath*
  - The adminshare variable is the hidden share that maps to the root volume on the NetApp filer, such as *c$*. For example, if the local path of the share on a NetApp filer, called usfiler, is `c$\vol\vol0\mydirectory`, you can specify a root path of `\\usfiler\c:\vol\vol0\mydirectory` for the NetApp filer.
- To specify a DFS path while you create user home directories or configure home directory policies for users, use *server**root*\<*link*> `format`, where root can be either the managed domain or a standalone root directory in the following format: *FilerName**adminshare:**volumerootpath**directorypath*.
- Create a shared directory to store the home directory for this user account.
- Ensure that DRA can access the computer or share referenced in the path.

Create home directory when user account is created

This rule allows DRA to automatically create home directories for new user accounts. When DRA creates a home directory, the Administration server uses the path specified in the **Home directory** fields in the Create User Wizard. You can later modify this path through the Profile tab of the user properties window and DRA will move the home directory to the new location. If you do not specify values for these fields, DRA does not create a home directory for that user account.

DRA sets the security for the new directory based on the selected **Home directory permissions** options. These options let you control the general access for all home directories.

For example, you can specify that members of the Administrators group have full control and members of the Help Desk group have read access to the share in which the user home directories are created. Then, when DRA creates a user home directory, the new home directory can inherit these rights from the parent directory. Therefore, members of the Administrators group have Full Control over all user home directories and members of the Help Desk group have read access to all user home directories.

If the specified home directory already exists, DRA does not create the home directory and does not modify the existing directory permissions.

Rename home directory when user account is renamed

This rule allows DRA to automatically perform the following actions:

- Create a home directory when you specify a new home directory path
- Move home directory contents when you change the home directory path
- Rename a home directory when you rename the user account

When you rename a user account, DRA renames the existing home directory based on the new account name. If the existing home directory is currently in use, DRA creates a new home directory with the new name and does not change the existing home directory.

You can rename the home directory if the previous home directory and the new home directory name and location are the same. However, if the directory rename fails, DRA creates a new home directory, moves the contents of the previous home directory to the new home directory, and deletes the existing home directory.

When you change the home directory path, DRA attempts to create the specified home directory and move the contents of the previous home directory to the new location. You can also configure the Home Directory policy to create a home directory without moving the contents from the existing home directory. DRA also applies the assigned ACLs from the previous directory to the new directory. If the specified home directory already exists, DRA does not create this new directory and does not modify the existing directory permissions. If the previous home directory is not locked, DRA deletes it.

When DRA fails to rename the home directory, DRA tries to create a new home directory with a new name and copy the contents from the previous home directory to the new home directory. DRA then attempts to delete the previous home directory. You can configure DRA not to copy the contents from the previous home directory to the new home directory and manually move the contents from the previous home directory to the new home directory to avoid concerns such as copying open files.

While deleting the previous home directory, DRA requires explicit permission to delete read-only files and subdirectories from the previous home directory. You can provide DRA the permission to explicitly delete the read-only files and subdirectories from the previous home directory.

Allow parent directory or path for a home share

DRA allows you to specify the allowable parent directories or paths for home shares on file servers. If you have many directory or file server paths to specify, you can export these paths to a CSV file and add the paths from the CSV file to DRA using the DRA console. DRA uses the information entered in the **Allowable parent paths** field to ensure:

- DRA does not delete the parent directory on the file server when Assistant Admins delete a user account and the user account home directory.
- DRA moves the home directory to a valid parent directory or path on the file server when you rename a user account or change the home directory path for a user account.

Delete home directory when user account is deleted

This rule allows DRA to automatically delete a home directory when you delete the associated user account. If you enable the Recycle Bin, DRA does not delete the home directory until you delete the user account from the Recycle Bin. While deleting the home directory, DRA requires explicit permission to delete read-only files and subdirectories from the previous home directory. You can provide DRA the permission to explicitly delete the read-only files and subdirectories from the previous home directory.

13.3.5 Home Share Automation and Rules

DRA automates home share maintenance tasks by managing home shares when you modify a user account or manage home directories. DRA can perform different actions when a user account is created, cloned, modified, renamed, or deleted.

To be consistent with proper Microsoft Windows security policies, DRA does not create access control restrictions at the share name level. Instead, DRA creates access control restrictions at the directory level only. Placing access control restrictions at both the share name level and the file or directory object level often leads to a confusing access scheme for administrators and users.

NOTE: The specified location must have a common home share, such as `HOMEDIRS`, at one level above the home directories.

For example, the following path is valid: `\\`*`HOUSERV1`*`\`*`HOMEDIRS`*`\%username%`

The following path is invalid: `\\`*`HOUSERV1`*`\%username%`

Specifying Home Share Names

When defining the home share automation rules, you can specify a prefix and suffix for each automatically created home share. By specifying a prefix or suffix, you can enforce a naming convention for home shares.

For example, you enable the Create home directory and Create home share automation rules. For the home share, you specify an underscore prefix and a dollar sign suffix. When you create a user named TomS, you map his new directory to the U drive and specify `\\HOUSERV1\HOMEDIRS\%username%` as the directory path. In this example, DRA creates a network share named `_TomS$` that points to the `\\HOUSERV1\HOMEDIRS\TomS directory`.

Creating Home Shares for New User Accounts

When DRA creates a home share, the Administration server uses the path specified in the **Home directory** fields in the Create User Wizard. You can later modify this path through the Profile tab of the user properties window.

DRA creates the share name by adding the specified prefix and suffix, if any, to the user name. If you use long user account names, DRA may not be able to add the specified home share prefix and suffix. The prefix and suffix, as well as the number of permitted connections, are based on the home share creation options you select.

Creating Home Shares for Cloned User Accounts

If the home share name generated from the newly created user account name already exists, DRA deletes the existing share and create a new share to the specified home directory.

When cloning a user account, the share name of the existing user account must currently exist. When you clone a user account, DRA also clones the home directory information and customizes that information for the new user.

Modifying Home Share Properties

When you change the home directory location, DRA deletes the existing share and creates a new share to the new home directory. If the original home directory is empty, DRA deletes the original directory.

Renaming Home Shares for Renamed User Accounts

When you rename a user account, DRA deletes the existing home share and creates a new share based on the new account name. The new share points to the existing home directory.

Deleting Home Shares for Deleted User Accounts

When you permanently delete a user account, DRA deletes the home share.

13.3.6 Home Volume Disk Quota Management Rules

DRA allows you to manage disk quotas for home volumes. You can implement this policy in native domains where the home directory resides on a Microsoft Windows computer. When you implement this policy, you should specify a disk quota of at least 25MB, to allow for ample room.

13.4 Home Directory Policy Tasks

The following step procedures provide instructions for home directory policy tasks that help you establish and maintain home directory policies.

13.4.1 Configuring Home Directory Policies

To configure home directory policies, you must have the appropriate powers, such as those included in the built-in Manage Policies and Automation Triggers role. Each home directory policy automatically manages home directories based on how you manage the associated user accounts.

To configure home directory policies:

1. In the left pane, click **Policy and Automation Management**.
2. Under Common Tasks in the right pane, click **Configure Home Directory Policies**.
3. Click **Home directory**.

4 Select the appropriate home directory options.

5 Click **OK**.

13.4.2 Configuring Home Share Policy

To configure a home share policy, you must have the appropriate powers, such as those included in the built-in Manage Policies and Automation Triggers role. Home share policy automatically manages home shares based on how you manage the associated user accounts.

To configure a home share policy:

1 In the left pane, click **Policy and Automation Management**.

2 Under Common Tasks in the right pane, click **Configure Home Directory Policies**.

3 Click **Home share**.

4 Select the appropriate home share options.

5 Click **OK**.

13.4.3 Configuring Home Volume Disk Quota Management Policy

To configure a home volume disk quota management policy, you must have the appropriate powers, such as those included in the built-in Manage Policies and Automation Triggers role.

To configure a home volume disk quota management policy:

1 In the left pane, click **Policy and Automation Management**.

2 Under Common Tasks in the right pane, click **Configure Home Directory Policies**.

3 Click **Home Volume Disk Quota**.

4 Select the appropriate home volume disk quota options.

5 Click **OK**.

13.5 Implementing Default Policies

Built-in policies are implemented when you install the Administration server. When you work with these policies, you may encounter the following terms:

Policy scope

Defines the objects or properties to which DRA and ExA apply the policy. For example, some policies allow you to apply a policy to specific AAs in specific ActiveViews. Some policies let you choose from different classes of objects, such as user accounts or groups.

Global policies

Enforce policy rules on all objects of the specified class or type in the managed domains. Global policies do not let you limit the scope of the objects to which the policy applies.

Policy relationship

Defines whether the policy applies jointly or by itself. To establish a policy relationship, define two or more rules that apply to the same action, and choose the member of a policy group option. If the operation parameters or property matches any of the rules, the operation succeeds.

13.5.1 Understanding Built-in Policies

Built-in policies provide business rules to address common security and data integrity issues. These policies are part of the default security model, allowing you to integrate DRA and ExA security features into your existing enterprise configuration.

DRA provides two ways to enforce policy. You can create custom policies or choose from several built-in policies. Built-in policies make it easy to apply policy without having to develop custom scripts. If you need to implement a custom policy, you can adapt an existing built-in policy to fit your needs. Most policies allow you to modify the error message text, rename the policy, add a description, and specify how to apply the policy.

A number of built-in policies are enabled when you install DRA. The following policies are implemented by default. If you do not want to enforce these policies, you can disable them or delete them.

Policy Name	Default Value	Description
$ComputerNameLengthPolicy	64 15 (pre-Windows 2000)	Limits the number of characters in the computer name or the pre-Windows 2000 computer name
$GroupNameLengthPolicy	64 20 (pre-Windows 2000)	Limits the number of characters in the group name or the pre-Windows 2000 group name
$GroupSizePolicy	5000	Limits the number of members in a group
$NameUniquenessPolicy	None	Ensures pre-Windows 2000 and CN names are unique in all managed domains
$SpecialGroupsPolicy	None	Prevents unchecked escalation of powers in the environment.
$UCPowerConflictPolicy	None	Prevents escalation of power by making User Clone and User Create powers mutually exclusive
$UPNUniquenessPolicy	None	Ensures UPN names are unique in all managed domains
$UserNameLengthPolicy	64 20 (down-level logon name)	Limits the number of characters in the user logon name or the down-level logon name

13.5.2 Available Policies

DRA provides several polices you can customize for your security model.

NOTE: You can create a policy that requires an entry for a property that is not currently available from the DRA and ExA user interfaces. If an entry is required by policy and the user interface does not provide a field to enter the value, such as a department for new user account, you will not be able to create or manage the object. To avoid this issue, configure policies that require only those properties that can be accessed from the user interfaces.

Create a Custom Policy

Allows you to link a script or executable to a DRA or ExA operation. Custom policies let you validate any operations you choose. For more information about creating a custom policy, see Section 13.8, “Creating and Implementing Custom Policy,” on page 131.

Enforce a Maximum Name Length

Allows you to globally enforce maximum name length for user accounts, groups, OUs, contacts, or computers.

The policy checks the name container (common name, or `cn`) and the pre-Windows 2000 name (user logon name).

Enforce Maximum Number of Group Members

Allows you to globally enforce limits on the number of members in a group.

Enforce Unique Pre-Windows 2000 Account Names

Verifies that a pre-Windows 2000 name is unique across all managed domains. In Microsoft Windows domains, pre-Windows 2000 names must be unique within a domain. This global policy enforces this rule across all managed domains.

Enforce unique User Principal Names (UPNs)

Verifies that a user principal name (UPN) is unique across all managed domains. In Microsoft Windows domains, UPNs must be unique within a domain. This policy enforces this rule across all managed domains. Because this is a global policy, DRA provides the policy name, description, and policy relationship.

Limit actions on members of special groups

Prevents you from managing members of an administrator group unless you are a member of that administrator group. This global policy is enabled by default.

When you limit actions on members of the administrator groups, the Create Policy Wizard does not require additional information. You can specify a custom error message. Because this is a global policy, DRA provides the policy name, description, and policy relationship.

Prevent AAs from Creating and Cloning Users in Same AV

Prevents possible escalation of powers. When this policy is enabled, you can either create user accounts or clone user accounts, but you cannot have both powers. This global policy ensures that you cannot create and clone user accounts in the same ActiveView.

This policy does not require additional information. For more information about accumulating powers, see Section 3.6, “How Powers Can Increase,” on page 60.

Set Naming Convention Policy

Allows you to establish naming conventions that apply to specific AAs, ActiveViews, and classes of objects, such as user account or groups.

You can also specify the exact names monitored by this policy.

Create a Policy to Validate a Specific Property

Allows you to create a policy to validate any property of an OU or an account object. You can specify a default value, a property format mask, and valid values and ranges.

Use this policy to enforce data integrity by validating particular entry fields when you create, clone, or modify properties of specific objects. This policy provides tremendous flexibility and power to validate entries, provide default entries, and limit entry choices for various property fields. By using this policy, you can require that a correct entry be made before the task is completed, thereby maintaining data integrity across your managed domains.

For example, assume you have three departments: Manufacturing, Sales, and Administration. You can limit the entries DRA will accept to just these three values. You can also use this policy to enforce proper telephone number formats, supply a range of valid data, or require an entry for the email address field. To specify multiple format masks for a telephone number, such as `(123)456 7890` as well as `456 7890`, define the property format mask as `(###)### ####,### ####`.

For more information about specifying property format masks, see Section 2.7.17, “Using Wildcard Characters,” on page 50.

Create Policy to Enforce Office 365 Licenses

Allows you to create a policy to assign Office 365 licenses based on Active Directory group membership. This policy also enforces the removal of Office 365 licenses when a member is removed from the relevant Active Directory group.

If a user who is not synced to the cloud is added to the Active Directory group, the user will be synced before an Office 365 license is assigned to the user.

During the creation of the policy you can specify several properties and settings, such as the name of the policy and the wording of the error message that appears when an AA attempts an action that violates this policy.

By default, policies that you create to enforce Office 365 licenses will not be applied when changes are made outside of DRA unless you also enable the License update schedule on the tenant properties page. For more information, see Section 16.4.2, “Office 365 License Update Schedule,” on page 162.

13.5.3 Using Built-in Policy

Because built-in policy is part of the default security model, you can use these policies to enforce your current security model or modify them to better meet your needs. You can change the name, rule settings, scope, policy relationship, and error message of several built-in policies. You can enable or disable each built-in policy.

You can also easily create new policies. For more information about standard policies you can create, see Section 13.5.2, “Available Policies,” on page 124. For more information about implementing custom policies, see Section 13.8, “Creating and Implementing Custom Policy,” on page 131.

13.6 Creating and Implementing Microsoft Exchange Policy

ExA provides several policies to help you more effectively manage Microsoft Exchange objects. Microsoft Exchange policy allows you to automate mailbox management, enforce naming conventions for aliases and mailbox stores, automatically generate email addresses, and configure Microsoft Exchange support.

These policies can help you streamline your workflows and maintain data integrity. For example, you can specify how ExA manages mailboxes when you create, modify, or delete user accounts. To define and manage Microsoft Exchange policies, you must have the appropriate powers, such as those included in the built-in Manage Policies and Automation Triggers role.

13.6.1 Mailbox Rules

Mailbox rules let you specify how ExA manages mailboxes when AAs create, clone, modify, or delete user accounts. Mailbox rules automatically manage Microsoft Exchange mailboxes based on how the AA manages the associated user accounts.

NOTE: When enabling the **Do not allow Assistant Admins to create a user account without a mailbox** option in Microsoft Windows domains, ensure the AA has power to either clone or create a user account. Enabling this option requires AAs to create Windows user accounts with a mailbox.

13.6.2 Automatic Naming Policy

Automatic naming policy allows you to specify automated naming rules for specific properties of a mailbox. These options allow you to establish naming conventions and quickly generate standard values for the display name, directory name, and alias properties. ExA allows you to specify substitution strings, such as `%First` and `%Last`, for several automated naming options.

When ExA generates a directory name or alias, it checks whether the generated value is unique. If the generated value is not unique, ExA appends a hyphen (-) and a two digit number, starting with `-01`, to make the value unique. When ExA generates a display name, it does not check whether the value is unique.

ExA supports the following substitution strings for automatic naming and proxy generation policies:

`%First`	**Indicates the value of the First name property for the associated user account.**
`%Last`	Indicates the value of the Last name property for the associated user account.
`%Initials`	Indicates the value of the Initials property for the associated user account.
`%Alias`	Indicates the value of the Alias mailbox property.
`%DirNam`	Indicates the value of the Directory name mailbox property. When generating email addresses for Microsoft Exchange mailboxes, ExA does not support proxy generation strings that specify the `%DirName` variable.
`%UserName`	Indicates the value of the User name property for the associated user account.

You can also specify a number between the percent sign (`%`) and the substitution string name to indicate the number of characters to include from that value. For example, `%2First` indicates the first two characters from the **First** name property of the user account.

Each automatic naming rule or proxy generation policy can contain one or more substitution strings. You can also specify characters in each rule as a prefix or suffix for a specific substitution string, such as a period and space (`.`) following the `%Initials` substitution string. If the property for the substitution string is blank, the ExA does not include the suffix for that property.

For example, consider the following auto naming rule for the **Display** name property:

```
%First %1Initials. %Last
```

If the **First** name property is `Susan`, the **Initials** property is `May`, and the **Last** name property is `Smith`, ExA sets the **Display** name property to `Susan M. Smith`.

If the **First** name property is `Michael`, the **Initials** property is blank, and the **Last** name property is `Jones`, ExA sets the **Display** name property to `Michael Jones`.

13.6.3 Office 365 Rules

The Office 365 Rules policy allows you to enforce invalid characters and character length policies to prevent directory synchronization failures.

13.7 Microsoft Exchange Policy Tasks

The following step procedures provide instructions for Microsoft Exchange policy tasks that help you establish and maintain Microsoft Exchange policies.

13.7.1 Enabling Microsoft Exchange Support

Enabling Microsoft Exchange support allows you to leverage ExA features, such as Microsoft Exchange policies and integrated mailbox and mail-enabled object management. You can enable or disable Microsoft Exchange support for each Administration server. You can also enable support for the following Microsoft Exchange versions on the same Administration server:

- Microsoft Exchange Server 2007, 2010, and 2013
- Microsoft Exchange Online

To enable Microsoft Exchange support, you must have the appropriate powers, such as those included in the built-in Manage Policies and Automation Triggers role, and your license must support the ExA product. For more information about Microsoft Exchange requirements, see the *Administration Installation Guide*.

To enable Exchange Administrator:

1. In the left pane, click **Policy and Automation Management**.
2. Under Common Tasks in the right pane, click **Configure Exchange Policies**.
3. Select **Enable Exchange Policy** and click **Apply**.

   DRA verifies which versions of the Exchange management tools are installed on the Administration Server and enables the options that allow you to select Exchange support for the appropriate versions.
4. ***If Enable Exchange Policy was already selected and the options that allow you to select Exchange support are not enabled,*** click Refresh to have DRA verify which versions of the Exchange management tools are installed on the Administration Server.
5. To enable Exchange administration support, select the options to enable support of the versions of Exchange you intend to manage with this Administration server.
6. ***If you want to use Exchange Server 2010 or Exchange Server 2013 management tools to manage all versions of Exchange objects in your environment,*** select **Update objects using Exchange 2010 or Exchange 2013 tools if earlier versions of Exchange Management Tools are not available**.

   NOTE: Managing an object in the Exchange Server 2010 or 2013 Exchange Control Panel can upgrade the object. As a result, earlier versions of Exchange management tools can no longer manage the object. If you have Exchange environments that you intend to manage with earlier versions of Exchange management tools, do not select this option.
7. Click **OK**.

13.7.2 Specifying an Automated Mailbox Naming Policy

To specify automated mailbox naming options, you must have the appropriate powers, such as those included in the built-in Manage Policies and Automation Triggers role, and your license must support the ExA product.

To specify an automated mailbox naming policy:

1. In the left pane, click **Policy and Automation Management**.
2. Under Common Tasks in the right pane, click **Configure Exchange Policies**.
3. Click **Alias naming** under the **Exchange** tab.
4. Specify the appropriate name generation information.

   For more information about supported substitution strings for auto naming rules, see Section 13.6.2, “Automatic Naming Policy,” on page 127.
5. Select **Enforce alias naming rules during mailbox updates**.
6. Click **OK**.

13.7.3 Specifying a Resource Naming Policy

To specify resource naming options, you must have the appropriate powers, such as those included in the built-in Manage Policies and Automation Triggers role, and your license must support the ExA product.

To specify a resource naming policy:

1. In the left pane, click **Policy and Automation Management**.
2. Under Common Tasks in the right pane, click **Configure Exchange Policies**.
3. Click **Resource naming** under the **Exchange** tab.
4. Specify the appropriate resource name generation information.

   For more information about supported substitution strings for auto naming rules, see Section 13.6.2, “Automatic Naming Policy,” on page 127.
5. Select **Enforce resource naming rules during mailbox updates**.
6. Click **OK**.

13.7.4 Specifying an Archive Naming Policy

To specify archive naming options, you must have the appropriate powers, such as those included in the built-in Manage Policies and Automation Triggers role, and your license must support the ExA product.

To specify an archive naming policy:

1. In the left pane, click **Policy and Automation Management**.
2. Under Common Tasks in the right pane, click **Configure Exchange Policies**.
3. Click **Archive naming** under the **Exchange** tab.
4. Specify the appropriate archive name generation information for user accounts.

   For more information about supported substitution strings for auto naming rules, see Section 13.6.2, “Automatic Naming Policy,” on page 127.

5 Select **Enforce archive naming rules during mailbox updates**.

6 Click **OK**.

13.7.5 Specifying a Default Email Address Policy

To specify default email address policy, you must have the appropriate powers, such as those included in the built-in Manage Policies and Automation Triggers role, and your license must support the ExA product.

To specify a default email address policy:

1 In the left pane, click **Policy and Automation Management**.

2 Under Common Tasks in the right pane, click **Configure Exchange Policies**.

3 Click **Proxy generation** under the **Exchange** tab.

4 Specify the domain of the Microsoft Exchange server.

- **4a** Click **Browse**.
- **4b** Specify additional search criteria as needed, and then click **Find Now**.
- **4c** Select the domain to configure, and then click **OK**.

5 Specify the proxy generation rules for the selected domain.

- **5a** Click **Add**.
- **5b** Select a proxy type. For example, click **Internet Address**.
- **5c** Accept the default value or type a new proxy generation rule, and then click **OK**.

  For more information about supported substitution strings for proxy generation rules, see Section 13.6.2, “Automatic Naming Policy,” on page 127

6 Click **Custom attributes** to edit the custom name of custom mailbox properties.

- **6a** Select the attribute and click the **Edit** button.
- **6b** In the Attribute Properties window, enter the attribute name in the **Custom name** field, and click **OK**.

7 Click **OK**.

NOTE: DRA Policy Admins should have Manage Custom Tools power to modify custom attributes in the Microsoft Exchange policy.

13.7.6 Specifying Microsoft Exchange Mailbox Policies

To specify Microsoft Exchange mailbox policies, you must have the appropriate powers, such as those included in the built-in Manage Policies and Automation Triggers role, and your license must support the ExA product.

To specify Exchange mailbox policies:

1 In the left pane, click **Policy and Automation Management**.

2 Under Common Tasks in the right pane, click **Configure Exchange Policies**.

3 Click **Mailbox rules**.

4 Select the mailbox policies you want ExA to enforce when you create or modify user accounts.

5 Click **OK**.

13.7.7 Specifying Office 365 Mailbox Policies

To specify Office 365 mailbox policies, you must have the appropriate powers, such as those included in the built-in Manage Policies and Automation Triggers role, and your license must support the ExA product.

To specify Office 365 mailbox policies:

1. In the left pane, click **Policy and Automation Management**.
2. Under Common Tasks in the right pane, click **Configure Exchange Policies**.
3. Click **Office 365 rules**.
4. Select the mailbox policies you want ExA to enforce when you create or modify user accounts.
5. Click **OK**.

13.8 Creating and Implementing Custom Policy

Custom policies allow you to fully exploit the power and flexibility of the default security model. By using custom policies, you can integrate DRA and ExA with existing enterprise components while ensuring that your proprietary rules are enforced. You can use the custom policy feature to extend your enterprise policies.

You create and enforce custom policies by associating an executable or script to an administration operation. For example, a policy script associated with the UserCreate operation could check your human resource database to see if the specified employee exists. If the employee exists in the human resources database and does not have an existing account, the script retrieves the employee ID, first name, and last name from the database. The operation completes successfully and populates the user account property window with the proper information. However, if the employee already has an account, the operation fails.

Scripts give you a tremendous amount of flexibility and power. To create your own policy scripts, you can use the Directory and Resource Administrator ADSI Provider (ADSI provider) and Software Development Kit (SDK). For more information about creating your own policy scripts, see the SDK Help. For more information about other ways to customize your enterprise management using scripting, see Chapter 18, “Automating Processes,” on page 191.

13.9 Policy Tasks

The following step procedures provide instructions for policy tasks that help you establish and maintain your company policies.

13.9.1 Deleting Policies

To delete policies, you must have the appropriate powers, such as those included in the built-in Manage Policies and Automation Triggers role.

To delete a policy:

1. In the left pane, expand **Policy and Automation Management**.
2. Click **Policy**.
3. In the right pane, select the policy you want to delete.
4. On the Tasks menu, click **Delete**.

13.9.2 Disabling Policies

To disable policies, you must have the appropriate powers, such as those included in the built-in Manage Policies and Automation Triggers role.

To disable a policy:

1. In the left pane, expand **Policy and Automation Management**.
2. Click **Policy**.
3. In the right pane, select the policy you want to disable.
4. On the Tasks menu, click **Disable**.

13.9.3 Enabling Policies

To enable policies, you must have the appropriate powers, such as those included in the built-in Manage Policies and Automation Triggers role.

To enable a policy:

1. In the left pane, expand **Policy and Automation Management**.
2. Click **Policy**.
3. In the right pane, select the policy you want to enable.
4. On the Tasks menu, click **Enable**.

13.9.4 Implementing Built-in Policies

To implement built-in policies, you must have the appropriate powers, such as those included in the built-in Manage Policies and Automation Triggers role. For more information about built-in policies, see Section 13.5.1, “Understanding Built-in Policies,” on page 124.

NOTE: Before associating the built-in policy with an AA and an ActiveView, first verify that the AA is assigned to that ActiveView.

To implement built-in policies:

1. In the left pane, expand **Policy and Automation Management**.
2. Click **Policy**.
3. On the Tasks menu, click **New Policy**, and then select the type of built-in policy you want to create.
4. On each wizard window, specify the appropriate values, and then click **Next**. For example, you can associate this new policy with a specific ActiveView, allowing DRA to enforce this policy on objects included by that ActiveView.
5. Review the summary, and then click **Finish**.

13.9.5 Implementing Custom Policies

To implement a custom policy, you must have the appropriate powers, such as those included in the built-in Manage Policies and Automation Triggers role.

To successfully implement a custom policy, you must write a script that runs during a specific operation (administrative task). In the custom policy script, you can define error messages to display whenever an action violates the policy. You can also specify a default error message through the Create Policy Wizard.

For more information about writing custom policies, viewing a list of Administration operations, or using argument arrays, see the SDK. For more information, see Section 13.9.7, “Writing Custom Policy Scripts or Executables,” on page 134.

NOTE

- Before associating the custom policy with an AA and an ActiveView, first ensure that the AA is assigned to that ActiveView.
- If the path of the custom policy script or executable contains spaces, specify quotation marks (") around the path.

To implement a custom policy:

1. Write a policy script or executable.
2. Log on to a DRA client computer with an account that is assigned the built-in Manage Policies and Automation Triggers role in the managed domain.
3. Start the Delegation and Configuration console.
4. Connect to a primary Administration server.
5. In the left pane, expand **Policy and Automation Management**.
6. Click **Policy**.
7. On the Tasks menu, click **New Policy > Create a Custom Policy**.
8. On each wizard window, specify the appropriate values, and then click **Next**. For example, you can associate this new policy with a specific ActiveView, allowing DRA to enforce this policy on objects included by that ActiveView.
9. Review the summary, and then click **Finish**.

13.9.6 Modifying Policy Properties

To modify all the properties of a policy, you must have the appropriate powers, such as those included in the built-in Manage Policies and Automation Triggers role.

To modify policy properties:

1. In the left pane, expand **Policy and Automation Management**.
2. Click **Policy**.
3. In the right pane, select the policy you want to modify.
4. On the Tasks menu, click **Properties**.
5. Modify the appropriate properties and settings for this policy.
6. Click **OK**.

13.9.7 Writing Custom Policy Scripts or Executables

For more information about writing a custom policy scripts or executables, see the SDK.

To access the SDK:

1. Ensure that you have installed the SDK on your computer. The setup program creates a shortcut to the SDK in the Directory and Resource Administrator program group. For more information, see the *Installation Guide*.
2. Click the SDK shortcut in the Directory and Resource Administrator program group.

14 Implementing Your Dynamic Security Model

By designing and implementing an environment that is both secure and easy to manage, you can maximize the power and flexibility DRA and ExA offer. Through a dynamic security model, you can distribute and automate many administration tasks and duties.

This section describes key concepts about dynamic, distributed administration and illustrates these concepts with examples and scenarios. These examples and scenarios assume you have the DRA Administration role or the corresponding powers. Review these sections to learn about the following concepts:

- How to implement your security model with DRA and ExA
- How to build dynamic, self maintaining ActiveViews
- How to harness the power of overlapping and hierarchical ActiveViews

DRA and ExA provide powerful tools for distributing specific administration permissions. In addition, these products provide policy and automation features to help you streamline your security model.

14.1 How to Create a Security Model

When you design and implement your security model, consider the following questions:

- Which objects need to be managed?
- Which actions need to be performed to complete a specific task?
- Which people need to perform these tasks and manage these objects?

How you answer these questions determines what types of ActiveViews, roles, and AA groups you need. Your answers also determine what type of security model you should create.

NOTE: If you are managing a subtree of a domain, you can implement the DRA security model on the Administration server in the corresponding domain or in another domain managed by DRA.

For more information about these security model components, see Chapter 3, “Understanding the Dynamic Security Model,” on page 55 and Chapter 4, “Understanding the Default Security Model,” on page 65.

14.1.1 Delegating Administration through a Static Model

When you distribute administration through a static security model, you define rules that include specific objects, delegate specific powers, and assign specific AAs to manage these objects. You define a unique rule for each object, power, and AA.

A static model can be appropriate for situations in which the enterprise scope is unlikely to change. However, this approach has limitations. It can prevent your security model from automatically responding to change, and it can require more maintenance.

For example, suppose JSmith, the Executive Assistant for Engineering, needs to change the home addresses and phone numbers for the five engineering managers. You can create an ActiveView that includes these five user accounts by defining a rule for each account. You can assign the individual powers to JSmith. However, when the Executive Assistant for Marketing needs to change personal information for the marketing managers, you must duplicate your original efforts. If you need to limit powers later, you must manually remove the unwanted powers from each ActiveView in which the Executive Assistants have power.

14.1.2 Delegating Administration through a Dynamic Model

When you distribute administration through a dynamic security model, you define rules that include multiple objects, delegate reusable sets of powers, and assign multiple AAs to manage these objects. You define rules that specify these objects, powers, and AAs through naming conventions, wildcard matching, group memberships, and roles. In this way, a dynamic model allows you to more effectively respond to change and decrease maintenance.

Using groups can help simplify your security model while providing a more dynamic solution. Instead of assigning individual powers to individual user accounts, you assign roles to a group. Each group member inherits the powers assigned to the group. In this model, when you add a user account to the group, the user automatically gains the set of powers associated with this group. When you add a power to the role, each group member automatically gains that power. You do not need to redefine your security model to accommodate a changing enterprise environment.

For example, suppose JSmith, the Executive Assistant for Engineering, needs to change the home addresses and phone numbers for all engineering managers.

You can create the following objects:

- A group called Engineering Managers
- A group called Executive Assistants With Power
- A role called Modifying Home Information

You can assign the Modifying Home Information role to the Execute Assistants With Power group, delegating the same set of powers to all members of that group. You can also create an ActiveView that includes user accounts from the Engineering Managers group. Thus, when a new manager is hired, you can immediately allow JSmith to access the account properties by adding this new user to the Engineering Managers group. This dynamic delegation occurs because the ActiveView rule uses group membership to automatically include the new account.

14.1.3 Understanding Power Creation

A power defines the properties of an object an Assistant Admin can view, modify, or create in your managed domain or subtree. You can create custom powers. Custom powers allow you to delegate power over specific object properties.

You can create custom powers for many different scenarios. You can create or clone specific powers you need to include in roles for common administration tasks. For example, you may need a power to control some properties that have been added to your schema or to grant power over an Active Directory property that is exposed in the DRA consoles with a UI extension. Custom powers can include access to multiple powers, such as the View All User Properties power, so a custom power should contain all the necessary properties to control the object you want to manage or modify. To create a power, you must have the appropriate powers, such as those included in the Manage Security Model role. For more information about custom powers, see Section 14.6.1, “Understanding the Power Creation Process,” on page 149.

14.1.4 Understanding Role Creation

A role should contain all the necessary powers to complete a particular job or workflow. In this way, a role presents a job description. You can create new roles that group together specific powers you need or use the provided built-in roles for common administration tasks. For example, you may need a role that includes the powers to only reset passwords of user accounts.

When implementing roles in a dynamic security model, you can take advantage of this flexibility by assigning roles to AA groups. This delegation helps your model ensure that the proper people have the required permissions.

For more information about built-in roles, see Section 4.5, “Understanding Built-in Roles,” on page 70.

14.1.5 Understanding Assistant Admin Group Creation

An AA group contains all the user accounts and groups you want to grant powers. AA groups typically have roles within your security model. When you create AA groups, you can include user accounts, groups, and other AA groups. You can specify accounts and groups by name or use a wildcard specification that matches multiple accounts and groups.

If you create a static AA group that includes specific user accounts, you must maintain the group definition each time you want to add or remove someone from that AA group. For example, each time you add a user to a static AA group, you must define a rule that specifies the user account.

An easier way to implement your model is to create dynamic AA groups based on naming conventions or group memberships. Dynamic AA groups reduce and simplify your enterprise maintenance.

For example, wildcard specifications allow you to define dynamic AA groups that include user accounts and groups based on criteria, such as naming conventions. These definitions are self maintained. When you define AA group membership through a wildcard specification, DRA automatically updates the AA group membership whenever a new account matches the wildcard specification.

Another way to incorporate flexibility into your model is to define groups based on group membership. For example, you could create an AA group that includes all Help Desk personnel in the New York City office. If you have a group, such as NYC_HelpDesk, that includes these user accounts, you can include that group in an AA group. Then, when you update the membership of the NYC_HelpDesk group, DRA automatically updates the AA group membership.

NOTE: To fully grant powers to an AA group, you must create an ActiveView and associate the AA group with a role in that ActiveView.

14.1.6 Understanding ActiveView Creation

ActiveViews provide access to defined sets of objects, such as contacts or print jobs. When you create an ActiveView, you are creating an ActiveView object that has basic properties, such as a name and a description. To use this ActiveView, you must add objects, assign AAs, and assign roles or powers. The result is an ActiveView containing objects that particular AAs can view and manage.

For example, you can create a NYC_Sales People ActiveView that represents a set of user accounts, such as all the user accounts in the NYC_Sales group. Then, you can assign the NYC Help Desk AA group to the Update User Addresses role and the NYC_Sales People ActiveView. Through this delegation, you are giving the NYC_HelpDesk group members the ability to modify the address fields of all user accounts in the NYC_Sales group.

DRA provides a Delegation Wizard that allows you to easily and quickly define and assign ActiveViews. For more information, see the Getting Started Guide.

You also can use ActiveView rule restrictions to limit how an AA manages a set of objects. When defining which objects an ActiveView will include, you can select a restriction that designates these objects as **source objects** or **target objects**. For example, when the AA adds a user account to a group, the user account is the source object and the group is the target object. If you select the **Do not allow the users to be added to groups or moved to OUs** restriction, the AA cannot manage these user accounts as source objects. If you select this restriction, DRA will not allow the AA to add a user account in this ActiveView to any group in the enterprise.

14.1.7 Optimizing Your ActiveView Rules

You can configure your ActiveView rules to optimize performance for your enterprise. The following optimization tips can significantly increase performance when managing domains that contain over 250,000 objects.

Specific Matches

Specific matches let you identify the exact objects to include in an ActiveView. For example, you can create an ActiveView that includes user accounts from a specific OU. If your Active Directory structure allows you to specify objects by OU or domain, define rules that include objects from the specific OU or domain. If you need to specify objects from several OUs, and these OUs are unlikely to change, define a rule for each OU. For example, if you want to create an ActiveView that includes computers from the Sales and Marketing OUs, define a rule for each OU.

All rules that define a specific object, such as an OU, group, user, computer, resource type, contact, or domain, can optimize your model. You can also optimize a wildcard rule, such as including all user accounts whose description matches Sales, by specifying the domain of these accounts. Rules that specify a user principal name or logon name may not optimize your model.

Wildcards

If your security model uses a naming convention, wildcards offer tremendous power and flexibility. For example, you can create an ActiveView that includes computers whose pre-Windows 2000 names match ATL*. When using a naming convention, keep in mind that wildcard matches that look for prefixes (`ATL*`), groups, or pre-Windows 2000 names provide better performance. For more information about wildcards, see Section 2.7.17, “Using Wildcard Characters,” on page 50.

Groups

Groups can help you implement a dynamic security model while optimizing performance. For example, if you need to configure an ActiveView that includes many objects from multiple OUs or domains, you can create a group that contains these objects and then create an ActiveView that includes members of this group. In this case, the ActiveView has one rule that acts on one specific object (the group), even though it includes multiple objects (the group members).

If the Active Directory structure and group set are unlikely to change, you can define a rule for each group, specifying the group and its members.

To make your security model dynamic, the ActiveView can be maintained through a wildcard specification that acts on established group naming conventions. For example, if the pre-Windows 2000 names of your groups have a common prefix, you can define a single rule that matches this prefix.

14.2 Delegation Management Node

Use the Delegation Management node to define and maintain your security model. Delegation Management consists of the following nodes:

ActiveViews

Allows you to list current ActiveViews, create and clone ActiveViews, delegate administration, define ActiveView rules, and view managed objects. You can also view assigned AA groups and roles.

Roles

Allows you to list current roles, create roles, delegate administration, add powers to roles, nest roles within a role, clone individual roles or nested roles, delete roles, and view the properties of a role. You can also view assigned AA groups and ActiveViews.

Powers

Allows you to list built-in and custom powers, create and clone powers, and view and change power properties. Directory and Resource Administrator offers you the ability to quickly and efficiently manage and create custom powers. New powers allow you to delegate power over specific object properties. A power defines the properties of an object an Assistant Admin can view, modify, or create in your managed domain or subtree. Custom powers can include access to multiple properties, such as the View All User Properties power.

Assistant Admins

Allows you to list current AAs and AA groups, create and clone AA groups, delegate administration, define AA group rules, and view AA properties. You can also view AA group members and assigned roles and ActiveViews.

14.2.1 Accessing Delegation Management

You can access the Delegation Management node from the console tree or the Directory and Resource Administrator task pad.

To access Delegation Management through the console tree:

1. In the left pane, expand **Directory and Resource Administrator**.
2. Select **Delegation Management**.

14.2.2 Using Delegation Management

Use the Delegation Management node to define your security model components, such as ActiveViews, AA groups, and roles. You can create new components or modify existing components.

The Delegation Wizard provides multiple ways to delegate power. You can delegate the appropriate roles and powers "on the fly" when you assign AAs to a new ActiveView. You can assign the ActiveView to an AA group, an AA account, or any other group or user account. You can also give AAs the power to manage themselves. For more information about granting AAs power over themselves, see Section 14.3, “Allowing Users to Change Personal Information,” on page 140.

The Create Power Wizard allows DRA Administrators to create new powers for viewing, modifying, creating, and cloning Active Directory objects.

The Powers node lists all the powers available for delegation in DRA. The views in the Powers node allow you to view the details of a power's action, object attributes, and additional permissions a power grants. You can also delete, create, and modify custom powers in this list view.

You must have the appropriate powers, such as those included in the DRA Administration or Manage Security Model roles to use these features. For more information about using the built-in ActiveViews, AA groups, and roles, see Chapter 4, “Understanding the Default Security Model,” on page 65.

14.3 Allowing Users to Change Personal Information

You can allow users to manage personal information for their own accounts. This type of administration is called **self administration**. AAs with self administration permissions can change their basic account properties, such as telephone numbers and street addresses.

To delegate self administration:

1. In the left pane, select **Delegation Management**.
2. Under Common Tasks in the right pane, click **Delegate Administration**.
3. On the Welcome window, click **Next**.
4. Add the user accounts or groups to whom you want to delegate self-administration, and then click **Next**.
5. Add the Self Administration role, and then click **Next**.

   For more information, see Section 4.5.1, “Built-in Roles,” on page 71.
6. On the Add menu, click **Objects that match a rule**.
7. Click **Self Administration**, and then click **OK**. This rule automatically includes the AAs you assigned.
8. Click **Next**.
9. Specify the name, description, and comment for this new ActiveView.
10. Click **Finish**.

14.4 ActiveView Tasks

The following step procedures provide instructions for ActiveView tasks that help you implement and maintain your dynamic security model. You can perform these tasks in the Delegation and Configuration console.

14.4.1 Adding Managed Objects

You can add managed objects to existing ActiveViews. You can also include managed objects that are currently excluded by an ActiveView rule. When you add a rule or modify a rule to include objects, associated AAs can view or modify objects specified by that rule. To add or modify an ActiveView rule, you must have the appropriate powers, such as those included in the Manage Security Model role. You can add managed objects to built-in ActiveViews.

NOTE: You can also specify managed objects during delegation. Use the Delegation Wizard to create ActiveViews and assign the appropriate AAs and roles. For more information, see the Getting Started Guide.

To add managed objects:

1. In the left pane, expand **Delegation Management**.
2. Click **ActiveViews**.
3. In the right pane, select the ActiveView to which you want to add managed objects.
4. On the Tasks menu, click **Add Managed Objects**.
5. To add objects to this ActiveView, click **Add**, and then specify which objects you want to add.
6. To modify a rule to include objects in this ActiveView, select the appropriate rule, and then click **Options > Include Objects**.
7. Click **OK**.

14.4.2 Assigning ActiveViews to Assistant Admins and Roles

You must assign ActiveViews to AAs and roles in order for AAs to manage objects specified by the ActiveView. This assignment is called delegation. To assign ActiveViews to AAs and roles, you must have the appropriate powers, such as those included in the Manage Security Model role.

NOTE: To allow Assistant Admins to create or clone objects in an ActiveView, you must define a target container rule for this ActiveView. For more information, see Section 14.4.9, “Specifying a Target Container,” on page 144.

To assign ActiveViews to AAs and roles:

1. In the left pane, expand **Delegation Management**.
2. Click **ActiveViews**.
3. In the right pane, select the ActiveView to whom you want to assign a role or AA.
4. On the Tasks menu, click **Delegate power over**.
5. On the Assistant Admins tab, add the AAs you want to assign.
6. On the Roles and Powers tab, add the roles you want to assign.
7. Review the summary, and then click **Finish**.

14.4.3 Cloning ActiveViews

Cloning ActiveViews allows you to use a previously defined ActiveView as a template for a new ActiveView. Cloning allows you to change only the ActiveView properties you need, while maintaining the properties you do not want to change. The cloned ActiveView is not associated with any AA

groups or roles. For more information on associating a new ActiveView with AA groups and roles, see Section 14.4.2, “Assigning ActiveViews to Assistant Admins and Roles,” on page 141. To clone an ActiveView, you must have the appropriate powers, such as those included in the Manage Security Model role.

To clone an ActiveView:

1. In the left pane, expand **Delegation Management**.
2. Click **ActiveViews**.
3. In the right pane, select the ActiveView you want to clone. You cannot clone built-in ActiveViews.
4. On the Tasks menu, click **Clone**.
5. On each wizard window, specify the appropriate values, and then click **Next**. For example, you can add other objects to this new ActiveView.
6. Click **Finish**.

14.4.4 Creating ActiveViews

To create ActiveViews, you must have the appropriate powers, such as those included in the Manage Security Model role.

NOTE

- If the AA will use this ActiveView to create or clone objects, ensure that the ActiveView has a container rule. Container rules specify which containers, such as an OU, should include the new object. For more information, see Section 14.4.9, “Specifying a Target Container,” on page 144.
- Wildcard specifications allow you to include objects from several domains or OUs while making your security model more dynamic. If you need to manage objects across multiple domains or OUs, and you have established naming conventions, wildcard specifications may be more appropriate for your enterprise.
- When creating ActiveViews to manage objects from a specific domain subtree, specify the OU and domain of the objects you want to include. This specification optimizes performance and ensures your Assistant Admins can manage the appropriate objects.

To create an ActiveView:

1. In the left pane, expand **Delegation Management**.
2. On the Tasks menu, click **New > New ActiveView**.
3. On each wizard window, specify the appropriate values, and then click **Next**. For example, you can add objects to this new ActiveView.
4. Review the summary, and then click **Finish**.

14.4.5 Reviewing ActiveViews

Reviewing ActiveViews involve deleting the unused ActiveViews, modifying the existing ActiveViews and creating new ActiveViews.

To review ActiveViews:

- Delete the unused ActiveViews. Look for ActiveViews that are not delegated to anyone or used in any trigger, policy, or nested in another ActiveView. Delete these ActiveViews.
- Identify the high impact ActiveViews.

- Run the `DRAAVPerf Utility` and look at the timings and number of objects managed.
- Identify the object types that should be included in the ActiveViews. Look at the power assigned in the ActiveView.

NOTE: If there are only user and group powers assigned to an ActiveView, then the ActiveView rule should not include computer objects or contact objects.

- Make a backup copy of the ActiveView to reference by using the ActiveView clone feature.
- Modfiy the existing ActiveView to remove redundancy.

To Modify the existing ActiveView:

- Emphasize on Group rules, OU rules and domain rules.
- Consolidate resource rules into a single rule, if possible.

NOTE: Resource rules to manage printers and print jobs are usually defined as separate rules. If you are managing the same resources on the same computers, in a resource rule, specify the specific resource types to manage.

- If you are managing resources only and not the computer object, then you don't need a computer rule but only a resource rule.
- If you have an auditor ActiveView which includes all objects, consider using the **All Objects ActiveView**.

14.4.6 Deleting ActiveViews

Deleting an ActiveView deletes all the rule specifications for that ActiveView, including the AA assignments. Deleting AA assignments prevents AAs from managing objects specified by this ActiveView. When deleting an ActiveView, the Administration server does not delete the actual user accounts, groups, resources, and OUs that were in the ActiveView. To delete ActiveViews, you must have the appropriate powers, such as those included in the Manage Security Model role.

To delete an ActiveView:

1. In the left pane, expand **Delegation Management**.
2. Click **ActiveViews**.
3. In the right pane, select the ActiveView you want to delete.
4. On the Tasks menu, click **Delete**.

14.4.7 Managing ActiveView Assignments

You can view and modify delegated assignments for a specific ActiveView. To manage the assigned AAs and roles, you must have the appropriate powers, such as those included in the Manage Security Model role.

When viewing these delegated assignments, you can perform one of the following tasks:

- Delegate a new assignment
- Remove an existing assignment

- View properties of an assigned AA
- View properties of an assigned role

To manage role assignments:

1. In the left pane, expand **Delegation Management**.
2. Click **ActiveViews**.
3. In the list pane, select the appropriate ActiveView.
4. In the details pane, click **Assignments**. To view the details pane, click **Details** on the View menu.
5. View the delegated assignments, and then perform the appropriate action.

14.4.8 Modifying ActiveView Properties

To modify ActiveView properties, you must have the appropriate powers, such as those included in the Manage Security Model role.

To modify the properties of an ActiveView:

1. In the left pane, expand **Delegation Management**.
2. Click **ActiveViews**.
3. In the right pane, select the ActiveView you want to modify.
4. On the Tasks menu, click **Properties**.
5. Modify the appropriate properties and settings for this ActiveView.
6. Click **OK**.

14.4.9 Specifying a Target Container

A **target container** is the OU or built-in container where you want AAs to create and clone accounts. To successfully delegate create or clone powers to an AA, you must specify a target container rule in the corresponding ActiveView. For example, if you want an AA to clone user accounts from the Templates OU to the Users built-in container, specify a target container rule for the Users built-in container.

To specify a target container rule, you must have the appropriate powers, such as those included in the Manage Security Model role.

NOTE: This task discusses how to add a target container rule to an existing ActiveView. You can also specify target containers during delegation. Use the Delegation Wizard to create ActiveViews and define rules. For more information, see the Getting Started Guide.

To specify a target container:

1. In the left pane, expand **Delegation Management**.
2. Click **ActiveViews**.
3. In the right pane, select the ActiveView to which you want to add a target container rule.
4. On the Tasks menu, click **Add Managed Objects**.
5. On the Rules tab, click **Add > Target containers for create operations**.
6. Select the appropriate OU or built-in container, and then click **OK**.
7. Click **OK**.

14.4.10 Viewing Managed Objects

You can view which objects are currently managed by an existing ActiveView. To view managed objects, you must have the appropriate powers, such as those included in the Audit All Objects role.

NOTE: You can use the details pane to quickly view managed objects. You can also view managed objects when using the Delegation Wizard, to verify assignments as you implement your security model.

To view managed objects:

1. In the left pane, expand **Delegation Management**.
2. Click **ActiveViews**.
3. In the right pane, select the ActiveView whose managed objects you want to view.
4. On the Tasks menu, click **Show Managed Objects**.
5. Click **Close**.

14.4.11 Removing Managed Objects from ActiveViews

You can remove managed objects from ActiveViews by removing the corresponding rule. You can also remove managed objects by excluding them from the ActiveView rule. When you remove a rule or modify a rule to exclude objects, associated AAs can no longer view or modify objects specified by that rule. To remove or modify an ActiveView rule, you must have the appropriate powers, such as those included in the Manage Security Model role. You cannot remove rules from built-in ActiveViews.

NOTE: Another ActiveView may qualify AAs to manage objects specified through the rule you want to remove. To check whether several ActiveViews manage the same objects, use Directory and Resource Administrator to generate the Active Overlaps report. You can also use the Rules and Assignments tabs on the ActiveView Properties window.

To remove managed objects:

1. In the left pane, expand **Delegation Management**.
2. Click **ActiveViews**.
3. In the right pane, select the ActiveView from which you want to remove managed objects.
4. On the Tasks menu, click **Properties**.
5. On the Rules tab, select the rule that specifies the managed objects you want to remove or exclude from this ActiveView.
6. To modify the selected rule to exclude objects from this ActiveView, click **Options > Exclude Objects**.
7. To remove the selected rule from this ActiveView, click **Remove**.
8. Click **OK**.

14.5 Assistant Admin Tasks

The following step procedures provide instructions for AA group tasks that help you implement and maintain your dynamic security model. You can perform these tasks in the Delegation and Configuration console.

14.5.1 Adding Assistant Admin Group Members

You can specify which user accounts and groups you want to include in an AA group. These user accounts and groups receive powers when you assign the AA group to one or more roles in an ActiveView. For more information about assigning the AA group to an ActiveView, see Section 14.5.2, “Assigning Assistant Admins to Roles and ActiveViews,” on page 146. To add AA group members, you must have the appropriate powers, such as those included in the Manage Security Model role.

To create Assistant Admin rules:

1. In the left pane, expand **Delegation Management**.
2. Click **Assistant Admins**.
3. In the right pane, select the AA group to which you want to add members.
4. On the Tasks menu, click **Add Members**.
5. Click **Rules**.
6. Use the Add menu to select the user accounts and groups you want to add to this Assistant Admin group.
7. Click **OK**.

14.5.2 Assigning Assistant Admins to Roles and ActiveViews

You must assign AAs to roles and ActiveViews in order for AAs to manage objects specified by the ActiveView. This assignment is called delegation. Through delegation, you specify which tasks AAs can perform on the managed objects. To assign AAs to roles and ActiveViews, you must have the appropriate powers, such as those included in the Manage Security Model role.

To assign Assistant Admins to roles and ActiveViews:

1. In the left pane, expand **Delegation Management**.
2. Click **Assistant Admins**.
3. In the right pane, select the AA to whom you want to assign a role or ActiveView.
4. On the Tasks menu, click **Delegate > Delegate power to**.
5. On the Roles and Powers tab, add the roles you want to assign.
6. On the ActiveViews tab, add the ActiveViews you want to assign.
7. Review the summary, and then click **Finish**.

14.5.3 Cloning Assistant Admin Groups

By cloning an AA group, you can create a new AA group with the same properties as the original group. Cloning AA groups allows you to use a previously defined AA group as a template for a new AA group. To clone an AA group, you must have the appropriate powers, such as those included in the Manage Security Model role.

To clone an AA group:

1. In the left pane, expand **Delegation Management**.
2. Click **Assistant Admins**.
3. In the right pane, select the AA group you want to clone.
4. On the Tasks menu, click **Clone**.

5 On each wizard window, specify the appropriate values, and then click **Next**. For example, you can add other user accounts to this new AA group.

6 Click **Finish**.

14.5.4 Creating Assistant Admin Groups

You can create an AA group that contains one or more users or groups. You can also assign one or more AA groups to an ActiveView. To grant powers to an AA group, assign the group to an ActiveView and a role. For more information, see Section 14.5.2, “Assigning Assistant Admins to Roles and ActiveViews,” on page 146. To create an AA group, you must have the appropriate powers, such as those included in the Manage Security Model role.

TIP

- This new AA group is not specific to the AAs you specify. To expand the scope and flexibility of your security model, you can add other user accounts and groups to this AA group, or associate this AA group with other roles and ActiveViews.
- To improve performance, use a group membership definition to add user accounts to an AA group. For more information about optimizing rules, see Section 14.1.7, “Optimizing Your ActiveView Rules,” on page 138.

To create an AA group:

1 In the left pane, select **Delegation Management**.

2 On the Tasks menu, click **New > New Assistant Admin Group**.

3 On each wizard window, specify the appropriate values, and then click **Next**. For example, you can add user accounts to this new AA group.

4 Click **Finish**.

14.5.5 Deleting Assistant Admin Groups

When you delete AA groups, you do not delete the AA group members. However, the AA group members will no longer be able to act on objects in the assigned ActiveViews. To delete an AA group, you must have the appropriate powers, such as those included in the Manage Security Model role.

Deleting an AA group also deletes the SID principal associated with the AA group assignment. You do not need to delete an AA group to remove its assignment to an ActiveView or role. For more information, see Section 14.5.8, “Removing Assistant Admin Assignments,” on page 148.

To delete an AA group:

1 In the left pane, expand **Delegation Management**.

2 Click **Assistant Admins**.

3 In the right pane, select the AA group you want to delete.

4 On the Tasks menu, click **Delete**.

14.5.6 Managing Assistant Admin Assignments

You can view and modify delegated assignments for a specific AA. To manage the assigned roles and ActiveViews, you must have the appropriate powers, such as those included in the Manage Security Model role.

When viewing these delegated assignments, you can perform one of the following tasks:

- Delegate a new assignment
- Remove an existing assignment
- View properties of an assigned role
- View properties of an assigned ActiveView

To manage Assistant Admin assignments:

1. In the left pane, expand **Delegation Management**.
2. Click **Assistant Admins**.
3. In the right pane, select the AA whose assignments you want to manage.
4. In the details pane, click **Assignments**. To view the details pane, click **Details** on the View menu.
5. View the delegated assignments, and then perform the appropriate action.

14.5.7 Modifying Assistant Admin Group Properties

To modify the properties of AA groups, you must have the appropriate powers, such as those included in the Manage Security Model role.

To modify the properties of an AA group:

1. In the left pane, expand **Delegation Management**.
2. Click **Assistant Admins.**
3. In the right pane, select the Assistant Admin group you want to modify.
4. On the Tasks menu, click **Properties**.
5. Modify the appropriate properties and settings for this AA group.
6. Click **OK**.

14.5.8 Removing Assistant Admin Assignments

Removing assigned ActiveViews from an AA prevents this AA from managing objects specified by the selected ActiveView. To remove the assignment between an AA and an ActiveView, you must have the appropriate powers, such as those included in the Manage Security Model role.

To remove AAs from ActiveViews:

1. In the left pane, expand **Delegation Management**.
2. Click **Assistant Admins**.
3. In the right pane, select the AA from whom you want to remove the assigned ActiveViews.
4. On the Tasks menu, click **Properties**.
5. On the Assignments tab, select the rule that specifies the ActiveView you want to remove from this AA.

6 On the Options menu, click **Remove Assignment**.

7 Click **OK**.

14.5.9 Viewing Powers and Roles Assigned to an Assistant Admin

Roles and powers define how your AAs manage objects. You can view roles and powers assigned to a specific user account. The view roles and powers, you must have the appropriate powers, such as those included in the Manage Security Model role.

To view powers and roles assigned to an AA:

1 In the left pane, expand **Delegation Management**.

2 Click **Assistant Admins**.

3 In the right pane, select the Assistant Admin you want to view.

4 On the Tasks menu, click **Show Powers**.

5 Select the appropriate view. For example, click **List View** to see a table of AA group memberships, assigned powers and roles, and associated ActiveViews.

6 Expand the appropriate item. For example, in the **Has Power** column, expand **Roles & Powers** to view the individual roles or powers assigned to this AA.

7 Click **OK**.

14.6 Power Tasks

The following sections provide procedures for the following tasks:

- Create a new power
- Clone an existing power to create a new power
- Delete a new power
- View properties of a power
- Modify properties of a new power

Powers help you implement and maintain your dynamic security model. You perform these procedures in the Delegation and Configuration console. For more information, see Section 14.1.3, “Understanding Power Creation,” on page 136.

14.6.1 Understanding the Power Creation Process

Use power management capabilities to fulfill any of the following needs:

- Create new specific, limited powers over existing default Active Directory properties.
- View the details of a power: operation, object properties, and additional permissions a power grants.
- Create new powers for viewing, modifying, creating, and cloning Active Directory objects.
- Audit events related to the creation, deletion, and modification of custom powers.

Consider the following process before attempting to create a new power.

1. Review the powers supplied with DRA.
2. Decide whether you need a custom power. If applicable, you can clone an existing custom power.
3. Complete the appropriate wizard-driven procedures. For example, complete the New Power Wizard.
4. View your new power. For more information, see Section 14.6.5, “Viewing All Power Properties,” on page 151.
5. Modify you new power, if necessary. For more information, see Section 14.6.6, “Modifying Custom Power Properties,” on page 151.

14.6.2 Creating New Powers

You can create custom powers by using the Create Power Wizard. To create a power, you must have the appropriate powers, such as those included in the Manage Security Model role.

To create a new power:

1. In the left pane, expand **Delegation Management**.
2. Click the Powers node in the left pane.
3. Click **Tasks > New Power**.
4. On each wizard window, specify the appropriate values, and then click **Next**.
5. On the Summary window, click **Finish**.

14.6.3 Cloning Powers

You can clone a power by picking an existing power and using the Clone Power Wizard. By cloning an existing power, you can use an existing power as a template for new power delegations. A power defines the properties of an object an Assistant Admin can view, modify, or create in your managed domain or subtree. Custom powers can include access to multiple properties, such as the View All User Properties power. To clone a power, you must have the appropriate powers, such as those included in the Manage Security Model role.

NOTE: It is not possible to clone all of the built-in powers.

To clone a power:

1. In the left pane, expand **Delegation Management**.
2. Click **Powers**.
3. Click **Tasks > Clone Power**.
4. On each wizard window, specify the appropriate values, and then click **Next**.
5. On the Summary window, click **Finish**.

14.6.4 Deleting New Powers

You can delete custom powers you have created. To ensure the core functionality of DRA, you cannot delete built-in powers. To delete a custom power, you must have the appropriate powers, such as those included in the Manage Security Model role.

To delete a power:

1. In the left pane, expand **Delegation Management**.
2. Click **Powers**.
3. In the right pane, select the power you want to delete.
4. Click **Tasks > Delete**.
5. Click **OK**.

14.6.5 Viewing All Power Properties

Complete the following procedure to view the properties of a power. To view the properties of a power, you must have the appropriate powers, such as those included in the Manage Security Model role.

To view power properties:

1. In the left pane, expand **Delegation Management**.
2. Click **Powers**.
3. In the right pane, select the appropriate power.
4. Click **Tasks > Properties**.
5. View the appropriate properties and settings for this new power.
6. Click **OK**.

14.6.6 Modifying Custom Power Properties

You can modify a custom power at any time. To modify the properties of new power, you must have the appropriate powers, such as those included in the Manage Security Model role.

To modify new power properties:

1. In the left pane, expand **Delegation Management**.
2. Click **Powers**.
3. In the right pane, select the appropriate power.
4. Click **Tasks > Properties**.
5. Modify the appropriate properties and settings for the custom power. For more information, see the Help.
6. Click **OK**.

14.7 Role Tasks

The following step procedures provide instructions for role tasks that help you implement and maintain your dynamic security model. You can perform these tasks in the Delegation and Configuration console.

14.7.1 Cloning Roles

The clone function creates a new role with the same properties as the original role. Cloning roles allows you to use a previously defined role as a template for a new role. To clone a role, you must have the appropriate powers, such as those included in the Manage Security Model role.

To clone a role:

1. In the left pane, expand **Delegation Management**.
2. Click **Role**s.
3. In the right pane, select the role you want to clone.
4. On the Tasks menu, click **Clone**.
5. On each wizard window, specify the appropriate values, and then click **Next**. For example, you can add other powers to this new role.
6. Click **Finish**.

14.7.2 Creating Roles

By creating a role, you can quickly and easily delegate a set of powers that represents an administrative task or workflow. To create roles, you must have the appropriate powers, such as those included in the Manage Security Model role.

To create a role:

1. In the left pane, select **Delegation Management**.
2. On the Tasks menu, click **New > New Role**.
3. On each wizard window, specify the appropriate values, and then click **Next**. For example, you can add powers and other roles to this new role.
4. Click **Finish**.

14.7.3 Deleting Roles

Deleting a role removes power from the assigned AA group or ActiveView. To delete roles, you must have the appropriate powers, such as those included in the Manage Security Model role.

To delete a role:

1. In the left pane, expand **Delegation Management**.
2. Click **Roles**.
3. In the right pane, select the role you want to delete.
4. On the Tasks menu, click **Delete**.

14.7.4 Managing Role Assignments

You can view and modify delegated assignments for a specific role. To manage the assigned AAs and ActiveViews, you must have the appropriate powers, such as those included in the Manage Security Model role.

When viewing these delegated assignments, you can perform one of the following tasks:

- Delegate a new assignment

- Remove an existing assignment
- View properties of an assigned AA
- View properties of an assigned ActiveView

To manage role assignments:

1. In the left pane, expand **Delegation Management**.
2. Click **Roles**.
3. In the right pane, select the appropriate role.
4. In the details pane, click **Assignments**. To view the details pane, click **Details** on the View menu.
5. View the delegated assignments, and then perform the appropriate action.

14.7.5 Managing Roles and Powers

You can manage the roles and powers included in a role, allowing you to quickly change the administrative scope a role provides. You can add other powers, nest roles, or remove powers and roles. To manage a role, you must have the appropriate powers, such as those included in the Manage Security Model role.

To manage roles and powers:

1. In the left pane, expand **Delegation Management**.
2. Click **Roles**.
3. In the right pane, select the role you want to manage.
4. On the Tasks menu, click **Properties**.
5. Click **Roles and Powers**.
6. To add a role or power, complete the following steps:
   - **6a** Click **Add**.
   - **6b** Select the appropriate role or power, and then click **OK**.
7. To remove a role or power, select the appropriate power or role from the list, and click **Remove**.
8. Click **OK**.

14.7.6 Modifying Role Properties

To modify the properties of a role, you must have the appropriate powers, such as those included in the Manage Security Model role.

To modify role properties:

1. In the left pane, expand **Delegation Management**.
2. Click **Roles**.
3. In the right pane, select the role you want to modify.
4. On the Tasks menu, click **Properties**.
5. Modify the appropriate properties and settings for this role.
6. Click **OK**.

15 Implementing Microsoft Exchange Administration

ExA allows you to manage many Microsoft Exchange objects, including mailboxes, email addresses, and distribution lists. ExA is seamlessly integrated into the Account and Resource Management console, Delegation and Configuration console, and Web Console user interfaces. For example, when Microsoft Exchange support is enabled, the user properties window includes settings for mailboxes and email addresses. In this way, ExA extends features already available through DRA, allowing you to perform Microsoft Exchange tasks while managing your account objects.

15.1 Understanding Microsoft Exchange Management

Because you are performing Microsoft Exchange tasks within the context of managing accounts, ExA provides an integrated, single point of reference that corresponds to your existing workflow. Whether you are modifying user accounts, distribution groups, or contacts, you can access Microsoft Exchange tasks directly from the Tasks menu or from the object properties window. ExA lists the Microsoft Exchange tasks available for the selected account.

To use ExA with DRA, you must enable Microsoft Exchange support on the Administration server. When Microsoft Exchange support is enabled, you can manage mailboxes, email addresses, distribution group memberships, and Microsoft Exchange policies. For more information about Microsoft Exchange policy, see Section 13.6, “Creating and Implementing Microsoft Exchange Policy,” on page 126.

NOTE

- For more information about ExA requirements, see the *Installation Guide*.
- Ensure that the access account you are using meets the requirements for ExA. For more information about access account requirements, see the *Installation Guide*.

15.1.1 Managing Mailboxes

Through ExA, you can manage mailboxes for user accounts. Because ExA extends existing DRA features, you can manage mailboxes when creating or cloning a user account or modifying user account properties. For example, the Clone User and Modify Limited Properties power allows you to specify some mailbox properties when cloning an existing user account with a mailbox or cloning a mailbox for an existing user account. You can also manage mailboxes through the Exchange tasks tab in the user account properties window.

ExA allows you to create or delete a mailbox, move a mailbox, set mailbox rights and security, set delivery restrictions and options, and set storage limits. For more information about mailbox policy, see Section 13.6.1, “Mailbox Rules,” on page 127.

To manage Microsoft Exchange mailboxes using ExA, you must have the appropriate powers, such as those included in the Mailbox Administration and Manage Exchange Mailbox Rights roles. To modify specific mailbox properties, you must have the Exchange Mailbox power associated with the corresponding tab. For example, to manage delivery options for a Microsoft Exchange mailbox, you

must have the Modify Exchange Mailbox Delivery Options power. To modify specific mailbox security permissions in Microsoft Exchange, you must have the power associated with the appropriate permission, such as the Modify Mailbox Ownership Rights power.

NOTE

- When you create a mailbox, ExA generates any proxy addresses. Microsoft Exchange also generates default proxy addresses. As a result, when you view the properties of the newly created mailbox, you will see both types of proxy addresses. For more information about proxy generation policy, see Section 13.7.5, “Specifying a Default Email Address Policy,” on page 130.
- When you manage mailbox rights and security, disabled permissions may indicate inherited permissions.

15.1.2 Managing Distribution Groups

Distribution groups allow you to mail enable a group. By using distribution groups, you can send email to a single group, distributing this email to all group members. Through ExA, you can hide or expose group membership, manage email addresses, and clone existing groups. This flexibility allows you to create new Microsoft Exchange distribution groups whose membership includes a subset of the original group.

ExA integrates Microsoft Exchange management with group management. For example, when you establish or modify an email address for a distribution group, or clone a group that is mail enabled, ExA verifies that the email address is unique across domains in the forest. ExA also integrates distribution group management with managing your security model. For example, when you create a distribution group, the Create Group wizard allows you to add the new group to the appropriate ActiveViews and hide group membership. This integration allows you to use one process to address multiple goals.

15.1.3 Managing Email Addresses

Through ExA, you can manage email addresses for user accounts, contacts, and groups. ExA supports the following types of email addresses:

- cc:Mail
- Internet Mail
- MacMail
- Microsoft Mail
- X.400
- SMTP
- Custom

Because ExA extends existing DRA features, you can manage email addresses when performing account management tasks, such as managing account properties, creating new accounts, and cloning existing accounts. When you establish or modify an email address for an account, or clone a mail enabled account, ExA verifies that the email address is unique across the domains in the forest. You can create and delete email addresses through the Exchange Tasks feature, or let ExA automatically generate email addresses. For more information about automatically generating email addresses, see Section 13.7.5, “Specifying a Default Email Address Policy,” on page 130.

To manage email addresses, you must have the appropriate powers, such as those included in the Mailbox Administration role.

15.1.4 Managing Contacts

Contacts are offered in Microsoft Windows domains as a way to manage email and telephone information about people without providing them a security account on your enterprise. You can also use contacts to add members to distribution lists or groups without granting them access to services. Contacts do not have a security identifier (SID), as do user accounts and groups, so you do not need to incorporate them into your security model.

DRA and ExA integrate Microsoft Exchange and administration tasks so you can use a single workflow or process to seamlessly manage contacts across multiple OUs and domains. You can display and change the settings of many contact properties, create contacts, delete contacts, perform Microsoft Exchange tasks, and manage group membership. For example, when you create a contact through the Account and Resource Management console, the Create Contact Wizard allows you to add the new contact to the appropriate distribution groups. To manage contacts, you must have the appropriate powers, such as those included in the Contact Administration role.

You can also set Microsoft Exchange policies, such as automatically generating email addresses, to further coordinate and streamline your contact and Microsoft Exchange administration needs. For more information, see Section 13.6, “Creating and Implementing Microsoft Exchange Policy,” on page 126.

15.1.5 Managing Resource Mailboxes

Microsoft Exchange's resource mailbox feature allows you to create a mailbox that represents a resource such as a conference room so that you can reserve it by sending it a meeting invitation, just as you would a person.

DRA contains a set of roles, powers, and policies that allow you to manage your resource mailboxes efficiently.

You can perform the following resource mailbox management tasks with DRA:

- Create or update a resource mailbox
- Clone a resource mailbox
- Delete a resource mailbox
- Restore a resource mailbox
- Create a resource mailbox for an existing user
- Search for a resource mailbox room or equipment in the Delegation and Configuration console

DRA has UI extension support for resource mailboxes as well as support for generating audit or UI reports. Support for ADSI scripts is also integrated into DRA.

15.1.6 Managing Dynamic Distribution Groups

A dynamic distribution group is a mail-enabled Active Directory group object that you can create to expedite the mass sending of email messages and other information.

The membership list for a dynamic distribution group is calculated each time a message is sent to the group, based on the filters and conditions that you define. This differs from a regular distribution group, which contains a defined set of members. When an email message is sent to a dynamic distribution group, it is delivered to all recipients in the organization that match the criteria defined for that group.

DRA contains a set of roles, powers, and policies that allow you to manage your dynamic distribution groups efficiently.

You can perform the following dynamic distribution group management tasks with DRA:

- Create a dynamic distribution group
- Modify a dynamic distribution group
- Clone a dynamic distribution group
- Delete a dynamic distribution group
- Restore a dynamic distribution group from the NetIQ Recycle Bin container

DRA also supports the following features:

- Audit and UI reporting
- Enumeration support for dynamic distribution groups
- NetIQ Reporting Center (NRC) report for dynamic distribution groups
- Trigger operation support for dynamic distribution groups
- UI extension support for Exchange dynamic distribution groups

15.2 Managing Environments Containing Multiple Microsoft Exchange Versions

If you are managing an environment that contains multiple versions of Microsoft Exchange, ExA manages objects using the version of Exchange management tools that matches the object, if available. If the same version of Exchange management tools is not available, ExA can use a later version of Exchange management tools to manage objects, with some exceptions.

In all scenarios, to use Exchange 2010 management tools to update objects created with earlier versions of Exchange, you must enable the checkbox on the Exchange policy page allowing this behavior. For more information, see Section 13.7.1, “Enabling Microsoft Exchange Support,” on page 128.

15.2.1 Updating and Deleting Mail-Enabled Objects

ExA supports deleting and updating mail-enabled user accounts, group accounts, and contacts. ExA can delete and update these mail-enabled objects using the version of Exchange management tools that were used to create the object or a later version of the Exchange management tools. To update objects created with Exchange 2007 by using Exchange 2010 or 2013 management tools, you must enable the checkbox on the Exchange policy page allowing this behavior.

15.2.2 Creating and Updating Mailboxes

ExA supports creating, cloning, deleting, and updating mailboxes. The following tables show which actions you can perform with different versions of Exchange management tools when your environment contains objects created by more than one version of Microsoft Exchange.

Using	Exchange 2007 Mailbox				Exchange 2010 Mailbox			
	Create	Clone	Delete	Update	Create	Clone	Delete	Update
Exchange 2007 SP2 tools	Y	Y	Y	Y	N	N	N	N
Exchange 2010 SP2 tools	N	Y	Y	Y	Y	Y	Y	Y
Exchange 2013 tools	N	Y	Y	Y	N	Y	Y	Y

Using	Exchange 2013 Mailbox			
	Create	Clone	Delete	Update
Exchange 2007 SP2 tools	N	N	N	N
Exchange 2010 SP2 tools	N	Y	Y	Y
Exchange 2013 tools	Y	Y	Y	Y

15.2.3 Moving Mailboxes

ExA supports moving mailboxes to a different version of Exchange Server. The following table shows which mailboxes you can move when the source and target Exchange versions are different using different versions of Exchange management tools.

Using	Source Mailbox	Target Mailbox		
		Exchange 2007	Exchange 2010	Exchange 2013
Exchange 2007 tools	Exchange 2000	Y	N	N
	Exchange 2003 SP 2	Y	N	N
	Exchange 2007 SP 2	Y	N	N
	Exchange 2010	N	N	N
	Exchange 2013	N	N	N
Exchange 2010 tools	Exchange 2000	N	Y	N
	Exchange 2003 SP 2	N	Y	N
	Exchange 2007 SP 2	N	Y	N
	Exchange 2010	Y	Y	N
	Exchange 2013	N	Y	Y

Using	Source Mailbox	Target Mailbox		
		Exchange 2007	Exchange 2010	Exchange 2013
Exchange 2013 tools	Exchange 2007 SP 2	N	N	Y
	Exchange 2010	N	N	Y
	Exchange 2013	N	N	Y

15.3 How ActiveViews Simplify Microsoft Exchange Management

You can create ActiveViews that include specific user accounts, distribution groups, and contacts located across your enterprise. You can use each ActiveView to delegate the relevant Microsoft Exchange tasks for the account object. Because Microsoft Exchange management is integrated into account management, your AAs can use the Account and Resource Management console or Web Console to perform either task.

For example, you can create an ActiveView that includes contacts and their corresponding groups. In native mode domains, you can add contacts to security or distribution groups. Because security groups can be used as distribution lists in Microsoft Windows, you may want to add contacts to these groups. Having a contact in a global security group does not prevent the group from being converted to a universal security group when you migrate to a native mode Microsoft Windows domain.

ActiveViews can also help you provide templates for your AAs. For example, you can create an ActiveView that contains a template user account that has a mailbox already configured. When you need to create a mail-enabled user account, you can clone the template and move the new account into the appropriate OU. By delegating only certain powers, you can also limit which properties the AA can change. You can create similar templates for distribution groups and contacts. Configuring templates can help you decrease redundancies in your workflows while preventing errors.

15.3.1 Microsoft Exchange Management Tasks

This section provides information for administrators who are incorporating DRA into their enterprise. The *User Guide* and Help provide concepts and management tasks for AAs who have been delegated powers through DRA. The Help provides step-by-step guidance for many user account management tasks, such as modifying user account properties.

To access Help for a Microsoft Exchange task:

1. On the Help menu, click **Directory and Resource Administrator Help**.
2. Expand **How To**.
3. For Help on managing Microsoft Exchange mailboxes, expand **Exchange Tasks**.
4. For Help on managing contacts, expand **Contact Tasks**.
5. Click the appropriate task.

16 Implementing Microsoft Office 365 Exchange Online Administration

DRA allows you to administer and manage your users with mailboxes in the cloud using the Delegation and Configuration console. You can enable and disable Exchange Online mailboxes, manage Exchange Online mailbox delegation, and manage Exchange Online mail flow. To learn more about these tasks, see the *Directory and Resource Administrator Exchange Administrator User Guide*.

16.1 Enabling the Online Policy

To enable support for Exchange Online Administration, you must install Windows Azure Active Directory Module for Windows PowerShell as well as Microsoft Online Services Sign-in Assistant. These modules can be installed onto the following operating systems:

- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

NOTE: Windows Server 2008 R2 users must also upgrade to .NET Framework 4.5.2 or later.

For more information, refer to the NetIQ Knowledge Base article 7016493 or contact Technical Support.

To manage Exchange Online with DRA, you must first enable the online policy in DRA. You can find the **Exchange Online Administration support** option in the **Configure Exchange Policies** task under **Policy and Automation Management** in the Delegation and Configuration console.

16.2 Creating an Account to Manage Exchange Online

Before you configure DRA to manage your Exchange Online tenants, you must create an account in the Office 365 portal that has the following permissions:

- User management administrator in Office 365
- Receipt management in Exchange Online

DRA will use this account to perform all Exchange Online management tasks.

NOTE: This account can either be synced with your Active Directory environment or hosted in the Microsoft Office 365 cloud. DRA does not require that this account be in Active Directory to perform management tasks.

16.3 Managing an Office 365 Tenant and Creating a Service Principal

Once you have enabled the online policy in DRA, you can access a new node under **Configuration Management** named **Office 365 Tenants** where you can manage new Office 365 tenants.

DRA requires a Service Principal with Directory Readers permissions in order to collect data about the objects in the tenant.

To create the Service Principal, you can either provide DRA with the credentials for a user account with the Company Administrator role in Office 365 and DRA will create the Service Principal for you, or you can create the Service Principal offline.

NOTE

- DRA does not store Company Administrator credentials provided to create the Service Principal.
- If you create the Service Principal offline, you must provide the service principal identifier and password in the wizard.

Adding an Office 365 tenant may take several minutes. Once the tenant is successfully added, DRA will perform a full accounts cache refresh (FACR) for the tenant. When the cache refresh is complete you can start to manage your Office 365 licenses and mailboxes for the tenant.

16.4 (Optional) Allowing DRA to Manage your Office 365 Licenses

If you want to allow DRA to manage your Office 365 licenses, you must do the following:

- Create a license enforcement policy.
- Enable the **License update schedule** on the tenant properties page.

16.4.1 Creating a Policy to Enforce Office 365 Licenses

Select **New Policy** > **Create New Policy to Enforce Office 365 Licenses** under **Policy and Automation Management** in the Delegation and Configuration console.

For more information about this policy, see “Create Policy to Enforce Office 365 Licenses” on page 126.

16.4.2 Office 365 License Update Schedule

Policies that you create to enforce Office 365 licenses are not applied when changes are made outside of DRA unless you also enable the **License update schedule** on the tenant properties page. The license update job ensures that the Office 365 licenses assigned to users match your Office 365 license policies.

The license update job and Office 365 license policies work together to ensure that all of your managed users are assigned only the Office 365 licenses they are supposed to have.

NOTE

- DRA does not manage Office 365 licenses for online-only user accounts. In order for DRA to manage your users with Office 365 licenses, those users must be synced with Active Directory.
- If you choose to use DRA to manage your Office 365 licenses, DRA will override any manual changes to Office 365 licenses made outside of DRA the next time the license update job runs.
- If you enable the Office 365 license update job before ensuring that your Office 365 license policies are configured properly, your assigned licenses might be incorrect after the license update job runs.

17 Customizing the Administration Server

Using DRA, you can configure your Administration servers to run as smoothly as possible by gathering logon statistics, refreshing caches, and synchronizing data. Whether your enterprise environment contains a single Administration server or several MMS configurations at remote locations, you can effectively and quickly manage server computers throughout the enterprise.

17.1 Understanding Administration Server Configuration

You can customize how each Administration server runs. For example, you can configure different accounts cache refresh schedules for different Administration servers, depending on the level of usage. This flexibility allows you to maintain enterprise data while minimizing disruptions in your daily activities.

Connect to the primary Administration server for the managed domain before you set or change the following settings:

- Domain configuration
- MMS configuration
- Tenant configuration

When changing these settings, be sure to synchronize the primary Administration servers with the secondary Administration servers in each MMS.

To manage an Administration server configuration, you must have the appropriate powers, such as those included in the built-in Configure Servers and Domains role.

NOTE: The Delegation and Configuration console displays scheduled times in the local time on the Administration server computer.

17.2 Accessing Configuration Management

Through the Configuration Management node, you can configure your Administration servers and manage your domains. You can also create custom user interface extensions and custom tools, manage file replication between Administration servers and DRA client computers, and specify clone exceptions to use when cloning user accounts.

New Managed Domain

Allows AAs to add a managed domain, managed subtree, or member server to Directory and Resource Administrator. To immediately begin managing objects in this new domain, subtree, or member server, refresh the domain configuration.

New Office 365 Tenant

Allows AAs to add an Office 365 tenant to Directory and Resource Administrator.

Update Administration Server Options

Allows AAs to configure Administration server operation settings, including enabling encrypted communications and resource cache refresh options.

Manage Administration Servers

Allows AAs to manage properties of the selected Administration server, configure an MMS, synchronize servers in an MMS, promote a secondary Administration server, or demote a primary Administration server.

Manage Domains

Allows AAs to view properties of a selected domain, refresh the accounts cache, schedule the refresh interval for DRA and ExA domain and accounts caches, or gather last logon statistics.

Manage Office 365 Tenants

Allows AAs to view properties of a selected tenant, refresh the accounts cache, schedule the refresh interval for DRA and ExA domain and accounts caches, or delete the tenant account.

Manage User Interface Extensions

Allows AAs to manage user interface extensions, such as custom pages, that expose Active Directory attributes and schema extensions.

Manage Custom Tools

Allows you to run external applications, launch scripts, and open web pages quickly and easily from the DRA console.

Manage File Replication

Allows you to upload and manage files you want to replicate across all Administration servers and DRA client computers.

Manage Clone Exceptions

Allows you to define object properties to use as clone exceptions when cloning a user account.

Manage Virtual Attributes

Allows you to manage virtual attributes in your environment.

Update Reporting Service Configuration

Allows you to enable DRA Reporting and enable and configure data collectors.

To access Configuration Management through the console tree:

1. In the left pane, expand **Directory and Resource Administrator**.
2. Select **Configuration Management**.

17.3 Using Administration Server Options

Use Administration server options to specify the following settings:

- Enable encrypted communication and authentication between the user interfaces and the Administration server.
- Enable AD printers collection for DRA and the database.
- Control how the DRA consoles allow AAs to search for and view managed objects.
- Schedule the resource cache refresh or immediately refresh the resource cache.

- Schedule the domain configuration refresh or immediately refresh the domain configuration.
- View AD LDS and ADAM information for your managed domains.

For more information on configuring options for your managed domain, such as scheduling an accounts cache refresh, see Section 17.7, “Configuring Managed and Trusted Domains,” on page 178.

17.3.1 Encrypted Communications

This function allows you to enable or disable use of encrypted communication between the user interfaces and the Administration server. When enabled, this option encrypts all server and client communications, except Web Console communications. By default, DRA encrypts account passwords.

Using encrypted communications can impact performance. Encrypted communication is disabled by default. If you enable this option, data is encrypted during communication between the user interfaces and the Administration server. DRA and ExA use the Microsoft standard encryption for Remote Procedure Call (RPC).

17.3.2 Client Options

Through the client options, you can control how the DRA consoles allow AAs to search for and view managed objects. You can set any of the following client options:

- Limit search results by setting the maximum number of items to show in a list. By default, this option is set to 1000.
- Specify whether AAs can search for objects using the object type and common object properties, such as name or description.
- Specify whether AAs can use ActiveViews to search for managed objects. By default, this option is enabled.
- Specify whether DRA hides source objects from lists, such as search results and group memberships. By default, this option is disabled.
- Specify whether DRA provides access to additional user account security settings managed through Directory Security Administrator and File Security Administrator. When this option is enabled, the Security task is available in each console connected to this Administration server.
- Specify whether DRA shows advanced Active Directory objects. Advanced Active Directory objects are Microsoft Windows objects for which the showInAdvancedViewOnly property is set to true, such as the System built-in container. By default, this option is disabled.
- Specify whether AAs can search for objects using all object types.
- Specify whether AAs can search for objects using all columns.

DRA applies these settings to the Account and Resource Management console and the Delegation and Configuration console.

17.3.3 Resource Cache

The Administration server stores and maintains a **resource cache** that contains information on available computers and resources in the managed domain. You can manage and schedule resource cache refreshes for the connected Administration server. To view or modify this information, you must have the appropriate powers, such as those included in the built-in Configure Servers and Domains role.

Refreshing the resource cache keeps DRA synchronized with your enterprise configuration. You can refresh the cache immediately or schedule a regular refresh interval, such as once a day. By default, the Administration server refreshes the resource cache at half hour intervals throughout the day.

The time required to refresh the resource cache depends on several variables:

- Size of the managed domains
- Speed of the Administration server computer
- Whether the Administration server is running on a PDC, DC, or other computer

How often you should refresh the resource cache depends on how often your enterprise changes. If possible, refresh the resource cache often to ensure that DRA has the most up to date information about the Administration servers, member servers, and workstations they manage. The Administration server is continuously available during resource cache refreshes.

DRA and ExA also maintain an accounts cache, which contains data for user accounts, groups, contacts, and computer accounts, and a domain configuration, which contains data about the managed domains. For more information about the accounts cache, see Section 17.7.1, “Accounts Cache,” on page 178. For more information about the domain configuration, see Section 17.3.4, “Domain Configuration,” on page 168.

17.3.4 Domain Configuration

The Administration server builds and maintains a **domain configuration** that contains the following data about domains in your enterprise:

- All domain controllers in the managed and trusted domains
- Availability of all trusted and managed domains, and managed computers
- Domain controller used to refresh the accounts cache

DRA uses the domain configuration to improve performance when managing domains. You can manage and schedule domain configuration refreshes for the connected Administration server. To view or modify this information, you must have the appropriate powers, such as those included in the built-in Configure Servers and Domains role.

DRA automatically refreshes the domain configuration when the Administration server starts. The Administration server can refresh the domain configuration only for domain controllers that are running when the cache refresh occurs. Although refreshing the domain configuration can require several minutes, the Administration server remains available to the Administration user interfaces. The default scheduled interval for a domain configuration refresh is every 4 hours. You can reset this schedule to a time or interval that is more convenient for your enterprise. You can also refresh the cache immediately.

How often you should refresh the domain configuration depends on how often your enterprise changes. If possible, refresh the domain configuration often to ensure that DRA has the most up to date information about the domains, member servers, and workstations they manage.

NOTE

- If you install a new domain controller, the Administration server cannot communicate with this computer until it refreshes the domain configuration. You can perform a manual cache refresh to update your enterprise information.
- DRA and ExA cannot automatically determine when changes are made through other tools, such as Microsoft Directory Services Administrator. Operations performed outside of DRA or ExA can affect the accuracy of the cached information. For example, if you use another tool to specify trust between two domains, you cannot use DRA to view this trusted domain until you update the domain configuration.
- If the domain controller you use to manage your domain becomes unavailable, the Administration server cannot manage this domain until the domain controller becomes available or it refreshes the domain configuration.

DRA and ExA also maintain a resource cache, which contains data about available computers, and an accounts cache, which contains data for user accounts, groups, contacts, and computer accounts. For more information about the resource cache, see Section 17.3.3, “Resource Cache,” on page 168. For more information about the accounts cache, see Section 17.7.1, “Accounts Cache,” on page 178.

17.4 Administration Server Tasks

The following procedures provide instructions for Administration server tasks that help you establish and maintain your servers.

17.4.1 Encrypting Communications between the Administration Server and User Interfaces

To encrypt all communications between the Administration server and user interfaces, you must have the appropriate powers, such as those in the built-in Configure Servers and Domains role.

To encrypt communications between the Administration server and user interfaces:

1. In the left pane, click **Configuration Management**.
2. Under Common Tasks in the right pane, click **Update Administration Server > Options**.
3. On the General tab, enable encrypted communications.
4. Click **OK**.

17.4.2 Enabling AD Printers Collection

AD printers collection is disabled by default.

To enable AD printers collection:

1. In the left pane, right-click **Configuration Management** and select **Update Administration Server Options**.
2. On the General tab, enable AD printer collection.
3. Run an IACR now or wait until the next scheduled IACR.

17.4.3 Setting Client Options

Client options let you can control how the DRA consoles allow AAs to search for and view managed objects. To set these options, you must have the appropriate powers, such as those included in the built-in Configure Servers and Domains role.

To modify the client options:

1. In the left pane, click **Configuration Management**.
2. Under Common Tasks in the right pane, click **Update Administration Server Options**.
3. On the Client Options tab, set the appropriate options.
4. Click **OK**.

17.4.4 Performing an Immediate Resource Cache Refresh

You can perform an immediate the resource cache refresh for the connected Administration server. To refresh the resource cache, you must have the appropriate powers, such as those included in the built-in Configure Servers and Domains role.

For more information about scheduling resource cache refreshes, see Section 17.4.5, “Scheduling a Resource Cache Refresh,” on page 170. For more information about the resource cache, see Section 17.3.3, “Resource Cache,” on page 168.

To perform an immediate resource cache refresh:

1. In the left pane, expand **Directory and Resource Administrator**.
2. Expand **Configuration Management**.
3. On the Tasks menu, click **Refresh Resource Cache**.

17.4.5 Scheduling a Resource Cache Refresh

You can set a different resource cache refresh schedule for each Administration server. The resource cache refresh does not include resources that are unavailable during the refresh time. To schedule a resource cache refresh, you must have the appropriate powers, such as those included in the built-in Configure Servers and Domains role.

For more information about performing an immediate resource cache refresh, see Section 17.4.4, “Performing an Immediate Resource Cache Refresh,” on page 170. For more information about the resource cache, see Section 17.3.3, “Resource Cache,” on page 168.

To schedule a resource cache refresh:

1. In the left pane, click **Configuration Management**.
2. Under Common Tasks in the right pane, click **Update Administration Server Options**.
3. On the Resource Cache tab, select the time of day or time interval at which you would like the refresh to occur.

   For example, to refresh the resource cache every day at 4 AM, click **Daily** and type `04:00` in the provided field.
4. Click **OK**.

17.4.6 Performing an Immediate Domain Configuration Refresh

You can perform an immediate the domain configuration refresh for the connected Administration server. You can also schedule this refresh to occur automatically at regular intervals. To refresh the domain configuration, you must have the appropriate powers, such as those included in the built-in Configure Servers and Domains role.

For more information about scheduling domain configuration refreshes, see Section 17.4.7, “Scheduling a Domain Configuration Refresh,” on page 171. For more information about the domain configuration, see Section 17.3.4, “Domain Configuration,” on page 168.

To perform an immediate domain configuration refresh:

1. In the left pane, expand **Directory and Resource Administrator**.
2. Expand **Configuration Management**.
3. On the Tasks menu, click **Refresh Domain Configuration**.

17.4.7 Scheduling a Domain Configuration Refresh

You can set a different domain configuration refresh schedule for each Administration server. To schedule a domain configuration refresh, you must have the appropriate powers, such as those included in the built-in Configure Servers and Domains role.

For more information about performing an immediate domain configuration refresh, see Section 17.4.6, “Performing an Immediate Domain Configuration Refresh,” on page 171. For more information about the domain configuration, see Section 17.3.4, “Domain Configuration,” on page 168.

To schedule a domain configuration refresh:

1. In the left pane, click **Configuration Management**.
2. Under Common Tasks in the right pane, click **Update Administration Server Options**.
3. On the Domain Configuration tab, select the time of day or time interval at which you would like the refresh to occur.

For example, to refresh the domain cache every day at 4 AM, click **Daily** and type `4:00 AM` in the provided field.

1. Click **OK**.

17.5 Managing a Multi-Master Set Environment

An MMS environment uses multiple Administration servers to manage the same set of domains and member servers. An MMS consists of one primary Administration server and multiple secondary Administration servers.

Multi-master functionality provides the following benefits:

- Minimizes network traffic by allowing you to distribute tasks and workflows across multiple Administration servers at different sites.
- Directs Administration servers to update local domain controllers when managing distributed Active Directory installations. This avoids replication delays when updating a remote domain controller.

- Improves fault tolerance by allowing multiple Administration servers to manage the same set of objects concurrently.
- Improves response time and task completion time by automatically directing the user interfaces to the closest Administration server.

The default mode for the Administration server is primary. As you add secondary servers to your MMS environment, keep in mind that a secondary Administration server can belong to only one server set.

NOTE: Before adding a secondary server to the MMS, review the following considerations:

- The DRA server should be installed on the secondary server.
- The access account provided by you should be valid.
- The access account provided should have the permissions to access the registry of the secondary server.

To ensure that each server in the set is managing the same data, periodically synchronize the secondary servers with the primary Administration server. To reduce maintenance, use the same service account for all Administration servers in the domain forest. For more information about synchronization, see Section 17.5.2, “Understanding Server Synchronization,” on page 173.

17.5.1 What Is a Multi-Master Set?

An MMS is a set of multiple Administration servers. Each MMS consists of a primary Administration server and one or more secondary Administration servers. The primary server provides security and domain management as well as account and Microsoft Exchange management. Each secondary server acts as a supplemental server, providing additional access to enterprise data while allowing you to balance loads and traffic across local or remote locations.

See the following table for a summary of tasks you can perform on primary and secondary Administration servers.

Tasks Performed on Primary Server	Tasks Performed on Secondary Server
Manage account objects	Manage account objects
Manage ActiveViews	View ActiveView rules and contents
Manage Administration servers and server options	View Administration server properties and edit the following server options: ◆ Enable encrypted communications ◆ Schedule domain configuration refresh ◆ Schedule resource cache refresh
Manage automation triggers	View trigger properties
Manage domains	View domain configuration and status, and set the accounts cache refresh schedule
Manage Microsoft Exchange mailboxes and email addresses	Manage Microsoft Exchange mailboxes and email addresses
Manage policies	View policy properties
Manage resource objects	Manage resource objects

Tasks Performed on Primary Server	Tasks Performed on Secondary Server
Specify the access account	Specify the access account
Manage the Recycle Bin	View Recycle Bin properties, and delete or restore accounts from the Recycle Bin
Manage tenants	View tenant configuration and status; set the tenant cache refresh schedule

17.5.2 Understanding Server Synchronization

When the Administration servers in an MMS environment synchronize, the primary Administration server sends the latest information to the secondary Administration servers. Synchronization is a three step process:

1. The primary Administration server sends security and policy information, as well as the domain configuration, to each secondary Administration server.
2. Each secondary server updates the stored security and policy configuration settings.
3. Each secondary server refreshes the domain configuration. If you added a domain since the last synchronization, the secondary server adds the accounts for the new domain to the accounts cache. If you removed a domain since the last synchronization, the secondary server deletes the accounts for that domain from the accounts cache. The secondary server does not refresh the accounts cache.

To ensure each secondary Administration server has your latest security, policy, and account information, you can periodically synchronize the MMS. Each secondary Administration server must have the server service installed and running. Use the Administration servers node to configure the synchronization schedule. By default, DRA synchronizes the Administration servers every four hours.The synchronization rules and configuration options determine where and how often Administration information is replicated. These options are not enabled until you install a secondary server or specify a secondary server through the server properties window.

NOTE

- The Administration registry information can be replicated only to a computer on which the Administration server is installed. The automatic replication process replicates only changes in the Data registry keys. The automatic replication process does not replicate the Setup key values. These values are unique for each Administration installation.
- A primary Administration server may not synchronize with a secondary Administration server that is in a different, untrusted domain. In this case, the secondary server does not recognize the service account for the primary server. To synchronize across domains, the primary Administration server must have an access account that is an Administrator on the target computer. In general, an access account should be either the service account for that Administration server or another account that has configuration powers.
- The synchronization process does not replicate policy and automation trigger scripts. When you add, change, rename, or delete a script, you must update the primary and secondary Administration servers.

- The synchronization process does not replicate the preferred Microsoft Exchange server settings. If you change the Microsoft Exchange server configuration on one Administration server, you must update the server set.
- The synchronization process does not replicate the domain service account and password. You must update the domain service account for the secondary server after replication is complete.

17.5.3 Maintaining the Multi-Master Set

An MMS allows you to better manage your enterprise, but only if the Administration servers have the latest data. The Administration server stores its security and policy information in the Microsoft Windows registry. To keep your servers up to date, ensure that you regularly synchronize the MMS and perform cache refreshes.

If the primary Administration server computer becomes unavailable, you can easily promote a secondary Administration server. You can also demote a primary Administration server or add a new secondary server to the set. Synchronization automatically occurs after you add a secondary server. You can install an Administration server as a secondary server or specify secondary servers through the Delegation and Configuration console.

NOTE: The primary Administration server and the secondary Administration server should have the same version of DRA and ExA installed. If you upgrade your primary Administration server, you should also upgrade your secondary Administration servers.

When changing the configuration of an Administration server in an MMS environment, connect to the primary Administration server to specify the new settings. Then synchronize the server set. Ensure all Administration servers in an MMS have the same settings. For example, if the primary Administration server has Microsoft Exchange support enabled then all secondary Administration servers should have Microsoft Exchange support enabled.

17.5.4 Disaster Recovery and Location Maintenance

DRA and ExA are mission critical applications. Therefore, you need to keep the Administration server service available at all times. If the Administration server for a domain is no longer available, you should make another Administration server available.

For each managed domain, you can set up an MMS configuration. This configuration allows multiple Administration servers to manage a single domain set. If the primary Administration server computer becomes unavailable, you can easily promote a secondary server to continue operations with minimal disruption to your organization. If you want to move the Administration server to a different computer, you can install a new Administration server on a different computer.

To ensure a smoother transition when maintaining your enterprise or undergoing disaster recovery, you should synchronize the primary Administration server with the secondary Administration server on a regular schedule. For more information about synchronization, see Section 17.5.2, “Understanding Server Synchronization,” on page 173.

17.6 Multi-Master Tasks

The following step procedures provide instructions for Administration server tasks that help you establish and maintain your MMS environment.

17.6.1 Adding a Secondary Administration Server

You can add a secondary Administration server to a new or existing MMS. To add a secondary server, you must have the appropriate powers, such as those included in the built-in Configure Servers and Domains role.

NOTE: To successfully add a new secondary server, you must first install the Directory and Resource Administrator product on the Administration server computer. For more information, see the *Installation Guide*.

To add a secondary Administration server:

1. In the left pane, expand **Directory and Resource Administrator**.
2. Expand **Configuration Management**, and then click **Administration Servers**.
3. On the Tasks menu, click **Add Secondary Server**.
4. Specify the computer you want to add as a secondary server.
5. Specify the appropriate access account credentials. By default, DRA uses the Administration server service account to access secondary servers.
6. Click **OK**.

17.6.2 Demoting a Primary Administration Server

You can demote a primary Administration server to a secondary Administration server. To demote a primary Administration server, you must have the appropriate powers, such as those included in the built-in Configure Servers and Domains role.

To demote a primary Administration server:

1. Connect to the primary Administration server. For more information, see Section 2.7.3, “Connecting to an Administration Server,” on page 43.
2. In the left pane, expand **Directory and Resource Administrator**.
3. Expand **Configuration Management**, and then click **Administration Servers**.
4. .In the right pane, select the primary Administration server you want to demote.
5. On the Tasks menu, click **Advanced > Demote Server**.
6. Specify the computer you want to designate as the new primary Administration server.
7. Click **OK**.

17.6.3 Promoting a Secondary Administration Server

You can promote a secondary Administration server to a primary Administration server. When you promote a secondary Administration server to a primary Administration server, the existing primary Administration server becomes a secondary Administration server in the server set. To promote a secondary Administration server, you must have the appropriate powers, such as those included in the built-in Configure Servers and Domains role.

NOTE: A newly promoted primary server can only connect to secondary servers that were available during the promotion process. If a secondary server became unavailable during the promotion process, contact NetIQ Technical Support.

To promote a secondary Administration server:

1. Connect to the secondary Administration server. For more information, see Section 2.7.3, “Connecting to an Administration Server,” on page 43.
2. In the left pane, expand **Directory and Resource Administrator**.
3. Expand **Configuration Management**, and then click **Administration Servers**.
4. In the right pane, select the secondary Administration server you want to promote.
5. On the Tasks menu, click **Advanced > Promote Server**.
6. ***If DRA uses custom pages that expose Active Directory schema extensions***, restart the NetIQ Administration Server service on each Administration server.

17.6.4 Removing a Secondary Administration Server

You can remove a secondary Administration server from the MMS. To remove a secondary Administration server from a server set, you must have the appropriate powers, such as those included in the built-in Configure Servers and Domains role.

To remove a secondary Administration server:

1. Connect to the primary Administration server. For more information, see Section 2.7.3, “Connecting to an Administration Server,” on page 43.
2. In the left pane, expand **Directory and Resource Administrator**.
3. Expand **Configuration Management**, and then click **Administration Servers**.
4. In the right pane, select the secondary Administration server you want to remove from the server set.
5. On the Tasks menu, click **Remove Server**.

17.6.5 Synchronizing a Secondary Server with the Primary Administration Server

You can synchronize a specific secondary Administration server with the primary Administration server. Synchronization ensures that all Administration servers in the MMS use the same configuration data. To synchronize all secondary Administration servers at once, see Section 17.6.7, “Synchronizing a Server Set with the Primary Administration Server,” on page 177.

To synchronize a secondary Administration server, you must have the appropriate powers, such as those included in the built-in Configure Servers and Domains role.

To synchronize a secondary Administration server with the primary Administration server:

1. Connect to the primary Administration server. For more information, see Section 2.7.3, “Connecting to an Administration Server,” on page 43.
2. In the left pane, expand **Directory and Resource Administrator**.
3. Expand **Configuration Management**, and then click **Administration Servers**.
4. In the right pane, select the secondary server you want to synchronize.
5. On the Tasks menu, click **Synchronize**.

17.6.6 Configuring a Refresh Schedule for a Secondary Administration Server

During synchronization, when the primary Administration server sends the latest information to the secondary Administration server, it also sends a refresh request to the secondary Administration server. If the secondary Administration server is in a different time zone, ensure that the secondary Administration server has its own refresh schedule to prevent the primary Administration server from sending the refresh request during periodic synchronization.

To configure a separate refresh schedule for the secondary Administration server:

1. Connect to the primary Administration server. For more information, see Section 2.7.3, “Connecting to an Administration Server,” on page 43.
2. In the left pane, expand **Directory and Resource Administrator**.
3. Expand **Configuration Management**, and then click **Administration Servers**.
4. In the right pane, select the primary Administration server.
5. On the Tasks menu, click **Properties**.
6. Select the Sychronization schedule tab, and then clear the **Refresh secondary Administration servers when refreshing the primary Administration server** check box.
7. Click **OK**.

17.6.7 Synchronizing a Server Set with the Primary Administration Server

You can synchronize all Administration servers in the MMS at the same time. Synchronization ensures that all Administration servers in the MMS use the same configuration data.

To synchronize the server set with the primary Administration server, you must have the appropriate powers, such as those included in the built-in Configure Servers and Domains role.

NOTE: This task performs an immediate server synchronization. You can also configure regular synchronizations through the Synchronization schedule tab on the server properties window.

To synchronize the server set with the primary Administration server configuration:

1. Connect to the primary Administration server. For more information, see Section 2.7.3, “Connecting to an Administration Server,” on page 43.
2. In the left pane, expand **Directory and Resource Administrator**.
3. Expand **Configuration Management**, and then click **Administration Servers**.
4. In the right pane, select the primary Administration server to which you want to synchronize the server set.
5. On the Tasks menu, click **Synchronize All Servers > Full Refresh** or **Synchronize All Servers > Incremental Refresh**.

17.6.8 Viewing Administration Server Properties

You can view the properties of any Administration server. To view domain properties, you must have the appropriate powers, such as those included in the built-in Audit All Objects role.

To view Administration server properties:

1. In the left pane, expand **Directory and Resource Administrator**.
2. Expand **Configuration Management**, and then click **Administration Servers**.
3. In the right pane, select the Administration server whose properties you want to view.
4. On the Tasks menu, click **Properties**.
5. Select the tab for the properties you want to view, and then click **OK**.

17.7 Configuring Managed and Trusted Domains

DRA allows you to manage multiple domains as well as multiple subtrees from a specific Microsoft Windows 2008 or later domain. By managing a subtree of a Microsoft Windows 2008 or later domain, you can use DRA to secure a department or division within a larger corporate domain.

For example, you can specify the Houston subtree in the `SOUTHWEST` domain, allowing DRA to securely manage only those objects contained in the Houston OU and its child OUs. This flexibility allows you to manage one or more subtrees without requiring administrative permissions for the entire domain. For more information about required permissions for managed subtrees, see the *Installation Guide*.

You can view properties and statistics for managed and trusted domains. You can also perform the following essential tasks:

- Add and remove managed domains
- Add and remove managed subtrees in a specific Microsoft Windows 2008 or later domain
- Specify the access account for the Administration server
- Check the status of the domain and view any error messages
- Specify the default domain controller to which DRA connects
- Check the status of the accounts cache refresh
- Schedule how often the Administration server gathers last logon statistics
- Perform an accounts cache refresh immediately
- Manage the accounts cache refresh schedule

17.7.1 Accounts Cache

The Administration server builds and maintains an **accounts cache** that contains portions of the Active Directory for the managed domains. DRA and ExA use the accounts cache to improve performance when managing user accounts, groups, contacts, and computer accounts.

To schedule a cache refresh time or view the cache status, you must have the appropriate powers, such as those included in the built-in Configure Servers and Domains role.

NOTE: To perform incremental accounts cache refreshes in domains that contain managed subtrees, ensure the service account has read access to the Deleted Objects container as well as all objects in the domain of the subtree. You can use the Deleted Objects Utility to verify and delegate the

appropriate permissions. For more information about this utility, see Section B.2, “Deleted Objects Utility,” on page 247. For more information about service account configurations, see the *Installation Guide*.

Full and Incremental Refreshes

An incremental accounts cache refresh updates only the data that changed since the last refresh. The incremental refresh provides a streamlined way to keep up with your changing Active Directory. Use the incremental refresh to quickly update the accounts cache while incurring the least impact on your enterprise.

An incremental refresh updates the following data:

- New and cloned objects
- Deleted and moved objects
- Group memberships
- All cached object properties

A full accounts cache refresh loads the entire Active Directory. Use the full refresh to maintain consistency between your Active Directory and the accounts cache for your managed domain.

DRA offers the full accounts cache refresh for all managed domains, and the incremental accounts cache refresh for Microsoft Windows domains. You can manually perform an immediate cache refresh for a managed or trusted domain at any time. You can also schedule regular, automatic refreshes.

Default Scheduled Times

How often you should refresh the accounts cache depends on how often your enterprise changes. Use the incremental refresh to update the accounts cache often, ensuring that DRA has the most up to date information about the Active Directory.

By default, the Administration server performs an incremental accounts cache refresh at the following times:.

Domain Type	Default Scheduled Refresh Time
Managed Windows	Every 5 minutes
Trusted Windows	Every hour

You cannot schedule a FACR; however, DRA runs an automatic FACR under the following circumstances:

- After you configure a managed domain for the first time.
- After you upgrade DRA to a new full version from a previous version.
- After you install a DRA service pack.

Performing a full accounts cache refresh can require several minutes.

If the full accounts cache refresh fails, the Administration server retries every 30 minutes until the refresh succeeds. If the incremental accounts cache refresh fails, the Administration server retries four times, at 15 minute intervals. If the Administration server fails to perform an incremental accounts cache refresh because the specified domain is unavailable, DRA immediately attempts a full

accounts cache refresh. You can also specify a timeout period for incremental cache refresh. If the incremental cache refresh takes longer than this specified timeout period, DRA immediately attempts a full accounts cache refresh.

Considerations

You must periodically refresh the accounts cache to ensure DRA and ExA have the latest information. Before performing or scheduling an accounts cache refresh, review the following considerations:

- The Administration server can refresh the accounts cache only for computers that are running when the cache refresh occurs.
- To perform an incremental accounts cache refresh, the Administration server service account or access account must have permission to access deleted objects in the Active Directory of the managed or trusted domain. For more information, see Section B.2, “Deleted Objects Utility,” on page 247.
- The Administration server does not allow you to modify objects in the managed domain during an incremental accounts cache refresh. However, you can view Active Directory data for the managed domain.
- The Administration server allows you to modify objects in the managed domain during a full accounts cache refresh. Then the Administration server performs an incremental refresh to detect those latest changes. If you access the managed domain before the incremental refresh begins, the accounts cache may not reflect changes made during the refresh process.
- When DRA performs an accounts cache refresh, the Administration server does not include domain local security groups from trusted domains. Because the cache does not contain these groups, DRA does not allow you to add a domain local security group from the trusted domain to a local group on the managed member server.
- The incremental accounts cache refresh may not detect when you move an object to or from an OU for which the Administration server service account or access account does not have permissions. To ensure the accounts cache accurately reflects these changes, perform a full accounts cache refresh.
- If you omit a trusted domain from an accounts cache refresh, the Administration server also omits that domain from the domain configuration refresh. For more information about the trusted domains and the domain configuration, see Section 17.3.4, “Domain Configuration,” on page 168.
- If you include a previously omitted trusted domain in the accounts cache refresh, perform a full accounts cache refresh for the managed domain. This ensures that the accounts cache on the Administration server for the managed domain correctly reflects group membership data in your managed and trusted domains.
- If you set the incremental accounts cache refresh interval to **Never**, the Administration server performs full accounts cache refreshes only. A full account cache refresh may take some time, during which you cannot manage objects in this domain.
- DRA and ExA cannot automatically determine when changes are made through other tools, such as Microsoft Directory Services Administrator. Operations performed outside DRA and ExA can affect the accuracy of the cached information. For example, if you use another tool to add a mailbox to a user account, you cannot use ExA to manage this mailbox until you update the accounts cache.

- The time required to complete a full accounts cache refresh depends on several variables:
  - Size of the managed domains
  - Speed of the Administration server computer
- Performing a full accounts cache refresh deletes the last logon statistics maintained in the cache. The Administration server then collects the latest logon information from all the domain controllers.

17.7.2 Access Account

The access account allows you to override the Administration service account you configured for the Administration server when you installed DRA and ExA. The Administration server uses the access account to read and write data from other managed and trusted domains. When you modify the access account, be sure to manually refresh the accounts cache for this domain so that the server uses the correct account.

Before you specify an access account, verify that the account has the appropriate privileges to access data on all managed and trusted domains. For more information about required permissions, see the *Installation Guide*.

NOTE: The Administration server stores account information locally for access accounts. If you change the name or password of a managed access account, you must also update the override account specifications through the Delegation and Configuration console on the Administration server. For more information, see Section 17.8.9, “Specifying Domain Access Accounts,” on page 186.

17.7.3 Last Logon Statistics

The last logon time for a user is stored only on the specific domain controller that validated the user logon. Other domain controllers, including the PDC, have only the timestamp of when that domain controller last validated the user. DRA can gather and consolidate last logon statistics from domain controllers. By consolidating the last logon statistics, DRA enables you to identify user accounts that have not been used for a period of time. You can specify how often DRA polls the domain controllers using the Last logon schedule tab in the domain properties window.

To collect and consolidate the last logon information, DRA periodically polls all domain controllers in the managed domains. DRA collects the last logon timestamp for each user since the most recent poll and stores this information in the domain configuration. DRA uses the values in the domain configuration to report the last logon information. By default, last logon statistics are disabled.

17.8 Domain Tasks

The following step procedures provide instructions for domain tasks that help you establish and maintain your managed and trusting domains.

17.8.1 Adding a Managed Domain

You can add new managed domains and computers after you install the Administration server. You can add any missing domains, member servers, or workstations through the Delegation and Configuration console. To add managed domains and computers, you must have the appropriate powers, such as those included in the built-in Configure Servers and Domains role.

NOTE

- You can add a managed domain or computer through the setup program. For more information, see the *Installation Guide*.
- After you finish adding managed domains, ensure that the accounts cache refresh schedules for these domains are correct. For more information about modifying the accounts cache refresh schedule, see Section 17.8.8, “Scheduling an Incremental Accounts Cache Refresh,” on page 185.

To add managed domains and computers:

1. In the left pane, click **Configuration Management**.
2. Under Common Tasks in the right pane, click **New Managed Domain**.
3. On the Domain or server tab, specify whether you want to manage a domain or a computer (member server or workstation).
4. Specify the name of the domain or computer you want to manage, and then click **Next**.
5. On the Access account tab, specify the account credentials you want DRA to use to access this domain or computer. By default, DRA uses the Administration server service account.
6. Review the summary, and then click **Finish**.
7. To begin managing objects from this domain or computer, refresh the domain configuration. For more information, see Section 17.4.6, “Performing an Immediate Domain Configuration Refresh,” on page 171.

17.8.2 Adding a Managed Subtree

You can add managed subtrees from specific Microsoft Windows domains after you install the Administration server. You can add any missing subtrees you want to manage through the Delegation and Configuration console. To add managed subtree, you must have the appropriate powers, such as those included in the built-in Configure Servers and Domains role.

NOTE

- To ensure the specified account has permissions to manage this subtree and perform incremental accounts cache refreshes, use the Deleted Objects utility to verify and delegate the appropriate permissions. For more information about using this utility, see Section B.2, “Deleted Objects Utility,” on page 247. For more information about setting up the service account, see the *Installation Guide*.
- You can add a managed subtree through the setup program. For more information, see the *Installation Guide*.
- After you finish adding managed subtrees, ensure that the accounts cache refresh schedules for the corresponding domains are correct. For more information about modifying the accounts cache refresh schedule, see Section 17.8.8, “Scheduling an Incremental Accounts Cache Refresh,” on page 185.

To add a managed subtree:

1. In the left pane, click **Configuration Management**.
2. Under Common Tasks in the right pane, click **New Managed Domain**.
3. On the Domain or server tab, click **Manage a domain**.
4. Specify domain of the subtree you want to manage.

5 Select **Manage a subtree of this domain**, and then click **Next**.

6 On the Subtrees tab, click **Add** to specify the subtree you want to manage. You can specify more than one subtree.

7 On the Access account tab, specify the account credentials you want DRA to use to access this subtree. By default, DRA uses the Administration server service account.

8 Review the summary, and then click **Finish**.

9 To begin managing objects from this subtree, refresh the domain configuration. For more information, see Section 17.4.6, “Performing an Immediate Domain Configuration Refresh,” on page 171.

17.8.3 Gathering Last Logon Statistics

You can configure DRA to collect last logon statistics from all domain controllers in the managed domain. To enable and schedule last logon statistics gathering, you must have the appropriate powers, such as those included in the built-in Configure Servers and Domains role.

By default, the last logon statistics gathering feature is disabled. If you want to gather last logon statistic data, you must enable this feature. Once you enable last logon statistics gathering, you can view last logon statistics for a particular user or display the status of the last logon statistics gathering. For more information about last logon statistics, see Section 17.7.3, “Last Logon Statistics,” on page 181.

To gather last logon statistics:

1 In the left pane, expand **Directory and Resource Administrator**.

2 Expand **Configuration Management**, and then click **Managed Domains**.

3 In the right pane, select the domain for which you want to configure last logon statistics gathering.

4 On the Tasks menu, click **Properties**.

5 On the Last logon schedule tab, select the time of day or time interval at which you would like DRA to gather logon statistics.

For example, to gather logon statistics every day at 4 AM, click **Daily** and type `04:00` in the provided field.

6 To gather statistics immediately, click **Refresh Now**.

7 Click **OK**.

17.8.4 Performing a Full Accounts Cache Refresh

The accounts cache refresh does not include objects that are unavailable during the refresh time. To refresh the accounts cache, you must have the appropriate powers, such as those included in the built-in Configure Servers and Domains role.

For more information about scheduling an accounts cache refresh, see Section 17.8.8, “Scheduling an Incremental Accounts Cache Refresh,” on page 185. For more information about the accounts cache, see Section 17.7.1, “Accounts Cache,” on page 178.

To perform an immediate full accounts cache refresh:

1 In the left pane, expand **Directory and Resource Administrator**.

2 Expand **Configuration Management**, and then click **Managed Domains**.

3 In the right pane, right-click the domain for which you want to refresh the accounts cache and select **Properties**.

4 Click **Full refresh** and then click **Refresh Now**.

NOTE: Search results for the specific domain may not be accurate during a full accounts cache refresh. Please wait for the cache refresh to complete before attempting to query this domain for objects.

17.8.5 Performing an Incremental Accounts Cache Refresh

The accounts cache refresh does not include objects that are unavailable during the refresh time. To refresh the accounts cache, you must have the appropriate powers, such as those included in the built-in Configure Servers and Domains role. The Administration server performs incremental accounts cache refreshes for Microsoft Windows domains only.

For more information about scheduling an accounts cache refresh, see Section 17.8.8, “Scheduling an Incremental Accounts Cache Refresh,” on page 185. For more information about the accounts cache, see Section 17.7.1, “Accounts Cache,” on page 178.

To perform an immediate incremental accounts cache refresh:

1 In the left pane, expand **Directory and Resource Administrator**.

2 Expand **Configuration Management**, and then click **Managed Domains**.

3 In the right pane, select the domain for which you want to refresh the accounts cache.

4 On the Tasks menu, click **Refresh Accounts Cache > Incremental Refresh**.

5 Click **Yes**.

6 Click **OK**.

17.8.6 Removing a Managed Domain

You can remove any managed domain, member server, or workstation from DRA. By removing a domain, you prevent DRA from managing objects in that domain. To remove a managed domain or computer, you must have the appropriate powers, such as those included in the built-in Configure Servers and Domains role.

NOTE

- After you finish removing a managed domain, refresh the accounts cache and domain configuration on the Administration server to ensure DRA applies your changes.
- Ensure the managed domain you want to remove does not include any administrator or service accounts you use to manage other domains or subtrees through DRA.
- Once you remove a managed domain, you cannot manage objects in that domain.

To remove a managed domain:

1 In the left pane, expand **Directory and Resource Administrator**.

2 Expand **Configuration Management**, and then click **Managed Domains**.

3 In the right pane, select the domain you want to remove.

4 On the Tasks menu, click **Remove**.

17.8.7 Removing a Managed Subtree

You can remove any managed subtree of your Microsoft Windows domain. By removing a subtree, you prevent DRA from managing objects in that subtree. To quickly and easily remove all managed subtrees of a domain, remove the domain. For more information about removing domains, see Section 17.8.6, “Removing a Managed Domain,” on page 184.

To remove managed subtrees, you must have the appropriate powers, such as those included in the built-in Configure Servers and Domains role.

NOTE

- After you finish removing a managed subtree, refresh the accounts cache and domain configuration on the Administration server to ensure DRA applies your changes.
- Ensure the managed subtree you want to remove does not include any administrator or service accounts you use to manage other domains or subtrees through DRA.
- Once you remove a managed subtree, you cannot manage objects in that subtree.

To remove a managed subtree:

1. In the left pane, expand **Configuration Management**.
2. Click **Managed Domains**.
3. In the right pane, select the domain that contains the managed subtree you want to remove.
4. On the Tasks menu, click **Properties**.
5. On the Subtrees tab, select the subtree you want to remove. You can remove more than one subtree. If you remove all the managed subtrees in a particular domain, DRA automatically removes the domain.
6. Click **Remove**.
7. Click **OK**.

17.8.8 Scheduling an Incremental Accounts Cache Refresh

For each managed domain or subtree, you can schedule incremental accounts cache refreshes so DRA regularly updates your account data with the Active Directory. To schedule an incremental accounts cache refresh, you must have the appropriate powers, such as those included in the built-in Configure Servers and Domains role.

For more information, see Section 17.8.5, “Performing an Incremental Accounts Cache Refresh,” on page 184 and Section 17.7.1, “Accounts Cache,” on page 178.

NOTE

- If you set the incremental accounts cache refresh interval to **Never**, the Administration server performs full accounts cache refreshes only. A full account cache refresh may take some time, during which you cannot manage objects in this domain or subtree.
- DRA supports incremental accounts cache refreshes for Microsoft Windows domains only.

To schedule an incremental accounts cache refresh:

1. In the left pane, expand **Configuration Management**.
2. Click **Managed Domains**.

3. In the right pane, select the domain for which you want to schedule a incremental accounts cache refresh.
4. On the Tasks menu, click **Properties**.
5. On the Incremental schedule tab, select the frequency and interval at which DRA should refresh the accounts cache.

   For example, to refresh the accounts cache every day at 4 AM, click **Daily** and type `4:00 AM` in the provided field.
6. Click **OK**.

17.8.9 Specifying Domain Access Accounts

For each managed domain or subtree, you can specify an access account other than the current Administration server service account. This alternative access account is called an access account. To configure an access account, you must have the appropriate powers, such as those included in the built-in Configure Servers and Domains role.

To specify an override account for a member server, you must have permission to manage the domain in which the domain member exists. You can only manage domain members if they exist in a managed domain that you can access through the Administration server.

To specify an access account:

1. In the left pane, expand **Configuration Management**.
2. Click **Managed Domains**.
3. In the right pane, select the domain or subtree for which you want to specify an access account.
4. On the Tasks menu, click **Properties**.
5. On the Domain access account tab, click **Use the following account to access this domain**.
6. Specify and confirm the credentials for this account.
7. Click **OK**.

17.8.10 Specifying Exchange Access Accounts

DRA is configured for Exchange 2010 management with a domain access account. All Administration servers in the MMS use this account by default. You can specify a different Exchange access account on any secondary Administration server. To configure an Exchange access account, you must have the appropriate powers, such as those included in the built-in Configure Servers and Domains role.

To specify an Exchange access account:

1. In the left pane, expand **Configuration Management**.
2. Click **Managed Domains**.
3. In the right pane, select the domain or subtree for which you want to specify an access account.
4. On the Tasks menu, click **Properties**.
5. On the Exchange access account tab, click **Use the following account to access all Exchange servers**.
6. Specify and confirm the credentials for this account.
7. Click **OK**.

17.8.11 Viewing Domain Statistics

To view domain statistics, you must have the appropriate powers, such as those included in the built-in Audit All Objects role.

To view domain statistics:

1. In the left pane, expand **Configuration Management**.
2. Click **Managed Domains**.
3. In the right pane, select the domain for which you want to view statistics.
4. On the Tasks menu, click **Properties**.
5. On the Statistics tab, review the appropriate domain statistics, and then click **OK**.

17.8.12 Viewing Last Logon Statistics for a User Account

Before viewing last logon statistics for a particular user account, ensure you enable last logon statistics gathering. For more information, see Section 17.8.3, “Gathering Last Logon Statistics,” on page 183. To view last logon statistics, you must have the appropriate powers, such as those included in the Audit All Objects role.

To view last logon statistics for a user account:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the user account you want to view, complete the following steps:
   - **2a** ***If you know the account location,*** select the domain and OU that contains this user account.
   - **2b** In the search pane, specify the account attributes, and then click **Find Now**.
   - **2c** In the list pane, select the appropriate user account.
3. In the details pane, click **Logon**. To view the details pane, click **Details** on the View menu.

17.8.13 Viewing Trusted Domains

To view trusted domains, you must have the appropriate powers, such as those included in the built-in Audit All Objects role.

To view trusted domains:

1. In the left pane, expand **Configuration Management**.
2. Click **Managed Domains**.
3. In the right pane, select the managed domain for which you want to view trusted domains.
4. In the details pane, click **Trusted domains**. To view the details pane, click **Details** on the View menu.

17.9 Office 365 Tenant Tasks

The following procedures provide instructions for tasks that help you manage your Office 365 tenants.

17.9.1 Adding a Tenant

To add managed domains and computers, you must have the appropriate powers, such as those included in the built-in Configure Servers and Domains role.

Too add a tenant:

1. In the left pane, expand **Configuration Management**.
2. Right-click **Office 365 Tenants** and select **New Office 365 Tenant**.
3. Specify the appropriate credentials for the tenant account.

   For more information about DRA Service Principal, see Section 16.3, “Managing an Office 365 Tenant and Creating a Service Principal,” on page 162
4. Click **Finish**.

17.9.2 Removing a Tenant

You can remove any Office 365 tenant from DRA. To remove a tenant, you must have the appropriate powers, such as those included in the built-in Configure Servers and Domains role.

To remove a tenant:

1. In the left pane, expand **Configuration Management**, and click **Office 365 Tenants**.
2. In the right pane, right-click the tenant you want to remove and select **Remove**.
3. Click **Yes**.

17.9.3 Performing an Office 365 Incremental Accounts Cache Refresh

The accounts cache refresh does not include objects that are unavailable during the refresh time. To refresh the accounts cache, you must have the appropriate powers, such as those included in the built-in Configure Servers and Domains role.

For more information about scheduling an accounts cache refresh, see Section 17.8.8, “Scheduling an Incremental Accounts Cache Refresh,” on page 185. For more information about the accounts cache, see Section 17.7.1, “Accounts Cache,” on page 178.

To perform an incremental accounts cache refresh:

1. In the left pane, expand **Configuration Management**, and click **Office 365 Tenants**.
2. In the right pane, right-click the tenant you want to remove and select **Refresh Accounts Cache > Incremental Refresh**.
3. Click **Yes**.
4. Click **OK**.

17.9.4 Specifying a Tenant Access Account

Exchange Online only allows three concurrent connections using the same account; therefore, you should use a different tenant access account for each secondary server. To configure a tenant access account, you must have the appropriate powers, such as those included in the built-in Configure Servers and Domains role.

To specify a tenant access account:

1. In the left pane, expand **Configuration Management**, and click **Office 365 Tenants**.
2. In the right pane, right-click the tenant you want to remove and select **Properties**.
3. Click Tenant access and specify and confirm the credentials for this account.
4. Click **Yes**.

18 Automating Processes

Through DRA and ExA, you can customize policy and automate tasks to help maintain consistent data, provide a more secure enterprise environment, and streamline the administration of your enterprise. Use the DRA ADSI Provider to connect DRA or ExA with your company databases or further enhance the automation functionality in DRA and ExA.

18.1 Understanding Automation Triggers

DRA and ExA provide transaction based automation triggers to help you automate routine administrator tasks, ensure data consistency, and tap other data sources in your enterprise. Automation triggers allow you to launch a script or program in response to an AA request to complete a task. An automation trigger can run before or after a specific operation.

For example, you may want to add a user to a group every time an AA creates a new user account. You can write a script that adds the new user account to the appropriate group and then associate that script with a trigger.

You can also combine policies with automation triggers, validating the related tasks. You can extend existing workflows to implement your custom policies and automation triggers to validate, automate, and streamline your administration tasks.

18.1.1 What Is an Automation Trigger?

An automation trigger is a rule that associates a script or executable file with one or more operations. Through the script or executable file, you can automate an existing workflow, establish an information bridge between DRA and other data repositories, or create custom user interfaces. Automation triggers allow you to extend the functionality and security that DRA and ExA offer.

When you define an automation trigger, you set the rule parameters, which operations should be associated with the trigger, which script or executable to run, and, if applicable, which ActiveViews or AAs should be associated with this trigger. These rules determine how the Administration server applies your trigger.

You can also specify an undo script or executable for your trigger. An **undo script** allows you to rollback your changes if the operation fails. Typically, an undo script checks whether the operation succeeded and performs the necessary clean up if the operation did not succeed.

18.1.2 How the Administration Server Automates Processes

In addition to ActiveView rules based administration, DRA and ExA allow you to automate your existing workflows and automatically run related tasks through automation triggers. Automating existing workflows can help you streamline your enterprise while providing better and faster services.

When the Administration server runs the operation associated with your automation trigger, the server also runs the trigger script or executable. If your trigger is a pre task trigger, the server runs the script or executable before running the operation. If your trigger is a post task trigger, the server runs the script or executable after running the operation. This process is called a transaction. A

transaction represents the full implementation cycle for each task, or operation, the Administration server performs. A transaction includes the actions required to complete an operation along with any undo actions the Administration server should perform if the operation fails.

The Administration server enters the trigger status in the Audit log each time an automation trigger runs. These log entries record the return code, associated operations, objects acted on, and whether the trigger script succeeded.

WARNING: Automation triggers are run using the Administration server service account. Since the service account has administrator permissions, policies and automation triggers have full access to all enterprise data. To define automation triggers, you must have the appropriate powers, such as those included in the built-in Manage Policies and Automation Triggers role. These automation triggers will run within the service account security context. Thus, AAs associated with the built-in Manage Policies and Automation Triggers role could obtain more power than you intended.

18.1.3 What Is the ADSI Provider?

Through the ADSI provider, you can expand DRA and ExA by creating custom applications that integrate these products with existing proprietary applications in various departments. Custom applications and user interfaces utilize the ADSI provider to communicate with the Administration server. You can create automation triggers to automate repetitive and routine tasks.

You can also increase the power of DRA and ExA by creating custom policies to regulate data format and requirements. For more information about custom policies, see Section 13.8, “Creating and Implementing Custom Policy,” on page 131.

The Directory and Resource Administrator Software Development Kit (SDK) provides the basic concepts and instructions you need to create custom user interfaces or policy and trigger scripts. The SDK guides you through the design, development, and implementation of customization projects. Use the SDK to acquire basic knowledge about how to use the ADSI provider in your customization projects. The SDK also contains references, such as prerequisite information sources and sample scripts.

You do not need special equipment or a dedicated computer to run the SDK. For more information about software and hardware requirements for developing customized applications, see the SDK Help.

18.2 Accessing Automation Triggers

Through Policy and Automation Management, you can access the **Automation Triggers** node. The Automation Triggers node allows you to attach a script or program to a DRA or ExA operation, automating tasks and customizing workflows.

To access the Automation Triggers node through the console tree:

1. Expand **Policy and Automation Management**.
2. Click **Automation Triggers**.

18.3 Using Automation Triggers

When incorporating automation triggers into your workflows, think about what defines the workflow. Defining a workflow allows you to identify the type of trigger you need to create.

For example, you could create a post task trigger associated with the UserCreate operation. The script could read information about the new user from the human resources database, populating user account properties, such as employee ID, telephone, fax number, and manager.

To help you manage your automation triggers, DRA provides the Trigger Details report in the Managemet reports available in NetIQ Reporting Center. This report provides the following information:

- Indicates whether the trigger is enabled
- Lists associated operations
- Lists associated scripts or executables
- Provides trigger scope details
- Lists arguments and error messages

You can use this report to ensure that your triggers are defined properly. You can also use this report to compare trigger properties, catching conflicts and better streamlining processes across your enterprise.

18.3.1 Defining an Automation Trigger Workflow

Automation triggers also allow you to customize and automate workflows. A workflow is a set of tasks normally performed in sequence. An automation trigger could automate the setup process for new employees.

For example, when you create a user account for a new employee, there are many other tasks that need to be done:

- Add the new user account to a departmental group
- Set up a Microsoft Exchange mailbox
- Add the user to a distribution list
- Inform the user of the password for the account

An automation trigger can consolidate this workflow into a process that occurs "behind the scenes", running whenever the AA creates a new user account. You can create the automation you need using the ADSI provider and the Automation Triggers node.

18.3.2 Creating a New Automation Trigger

You can write your own scripts to create automation triggers. Scripts give you a tremendous amount of flexibility and power. The SDK will assist you to develop scripts for use with policy or automation. For more information about writing policy and trigger automation scripts, see the SDK Help.

Once you have written a script, you can easily implement this script as an automation trigger. The Create Trigger Wizard guides you through the steps of linking your script to an operation and creating a trigger. For more information about implementing an automation trigger, see Section 18.4.4, “Implementing Automation Triggers,” on page 195.

The Create Trigger Wizard allows you to specify these important options:

- Which operations, AA groups, and ActiveViews to associate with the trigger
- Whether the trigger should be run before or after the associated operation
- Which arguments you want to pass to the script
- What error message you want conveyed to the AA
- Which undo script to use if the operation fails

To fully implement automation triggers, you need to install the ADSI provider and understand how to write ADSI enabled scripts. For more information about the ADSI provider, see the SDK Help.

18.4 Automation Tasks

The following step procedures provide instructions for automation tasks that help you establish and maintain your automation triggers and customized workflows.

18.4.1 Deleting Automation Triggers

To delete automation triggers, you must have the appropriate powers, such as those included in the built-in Manage Policies and Automation Triggers role.

To delete an automation trigger:

1. In the left pane, expand **Policy and Automation Management**.
2. Click **Automation Triggers**.
3. In the right pane, select the trigger you want to delete.
4. On the Tasks menu, click **Delete**.

18.4.2 Disabling Automation Triggers

To disable automation triggers, you must have the appropriate powers, such as those included in the built-in Manage Policies and Automation Triggers role.

To disable an automation trigger:

1. In the left pane, expand **Policy and Automation Management**.
2. Click **Automation Triggers**.
3. In the right pane, select the trigger you want to disable.
4. On the Tasks menu, click **Disable**.

18.4.3 Enabling Automation Triggers

To enable automation triggers, you must have the appropriate powers, such as those included in the built-in Manage Policies and Automation Triggers role.

To enable an automation trigger:

1. In the left pane, expand **Policy and Automation Management**.
2. Click **Automation Triggers**.

3 In the right pane, select the trigger you want to enable.

4 On the Tasks menu, click **Enable**.

18.4.4 Implementing Automation Triggers

To implement automation triggers, you must first write trigger scripts or executables and have the appropriate powers, such as those included in the built-in Manage Policies and Automation Triggers role.

To successfully implement a custom trigger, you must write a script that runs during a specific operation (administrative task). You can specify whether DRA applies the trigger before (pre-task) or after (post-task) an operation runs. In the custom policy script, you can define error messages to display whenever an action violates the policy. You can also specify a default error message through the Create Automation Trigger Wizard.

For more information about writing custom triggers, viewing a list of Administration operations, or using argument arrays, see the *SDK*. For more information, see Section 18.4.6, “Writing Automation Trigger Scripts or Executables,” on page 196.

NOTE

- Before associating the custom automation trigger with an AA and an ActiveView, first ensure that the AA is assigned to that ActiveView.
- If the path of the custom policy script or executable contains spaces, specify quotation marks (") around the path.

To implement an automation trigger:

1 Write a trigger script or executable.

2 Log on to a DRA client computer with an account that is assigned the built-in Manage Policies and Automation Triggers role in the managed domain.

3 Start the Delegation and Configuration console.

4 Connect to a primary Administration server.

5 In the left pane, expand **Policy and Automation Management**.

6 Click **Automation Triggers**.

7 On the Tasks menu, click **New Trigger**.

8 On each wizard window, specify the appropriate values, and then click **Next**. For example, you can associate this new trigger with a specific ActiveView, allowing DRA to apply this trigger when AAs manage objects included by that ActiveView.

9 Review the summary, and then click **Finish**.

18.4.5 Modifying Automation Trigger Properties

To modify automation trigger properties, you must have the appropriate powers, such as those included in the built-in Manage Policies and Automation Triggers role.

To modify automation trigger properties:

1 In the left pane, expand **Policy and Automation Management**.

2 Click **Automation Triggers**.

3 In the right pane, select the trigger you want to modify.

4 On the Tasks menu, click **Properties**.

5 Change the appropriate trigger information. For more information about a field, mouse over the field.

6 Click **OK**.

18.4.6 Writing Automation Trigger Scripts or Executables

For more information about writing trigger scripts or executables, see the *SDK*. For more information about the ADSI provider, see Section 18.1.3, “What Is the ADSI Provider?,” on page 192.

To access the SDK:

1 Ensure that you have installed the SDK on your computer. The setup program creates a shortcut to the SDK in the Directory and Resource Administrator program group. For more information, see the *Installation Guide*.

2 Click the SDK shortcut in the Directory and Resource Administrator program group.

19 Auditing and Reporting

Auditing user actions is among the most important aspects of a sound security implementation. To allow you to review and report on Assistant Admin (AA) actions, DRA logs all user operations in the log archive on the Administration server computer. DRA provides clear and comprehensive reporting that includes before and after values of the audited events so that you can see exactly what changed.

19.1 How DRA Uses Log Archives

To allow you to review and report on Assistant Admin (AA) actions, DRA logs all user operations in the log archive on the Administration server computer. User operations include all attempts to change definitions, such as updating user accounts, deleting groups, or redefining ActiveViews. DRA also logs specific internal operations, such as Administration server initialization and related server information. In addition to logging these audit events, DRA logs the before and after values for the event so that you can see exactly what changed.

DRA uses a folder, **NetIQLogArchiveData**, called a **log archive** to securely store archived log data. DRA archives the logs over time and then deletes older data to make room for newer data through a process called grooming.

DRA uses the audit events stored in the log archive files to display Activity Detail reports, such as showing what changes have been made to an object during a specified time period. You can also configure DRA to export information from these log archive files to a SQL Server database that NetIQ Reporting Center uses to display Management reports.

DRA always writes audit events to the log archive. You can enable or disable having DRA write events to the Windows event logs as well.

19.1.1 Enabling and Disabling Windows Event Log Auditing for DRA

When you install DRA, audit events are not logged in the Windows event log by default. You can enable this type of logging by modifying a registry key.

WARNING: Be careful when editing your Windows Registry. If there is an error in your Registry, your computer may become nonfunctional. If an error occurs, you can restore the Registry to its state when you last successfully started your computer. For more information, see the Help for the Windows Registry Editor.

To enable event auditing:

1. Click **Start > Run**.
2. Type `regedit` in the **Open** field and click **OK**.
3. Expand the following registry key: `HKLM\Software\WOW6432Node\Mission Critical Software\OnePoint\Administration\Modules\ServerConfiguration\`.
4. Click **Edit > New > DWORD Value**.
5. Enter `IsNTAuditEnabled` as the key name.

6 Click **Edit > Modify**.

7 Enter `1` in the **Value data** field and click **OK**.

8 Close Registry Editor.

To disable event auditing:

1 Click **Start > Run**.

2 Type `regedit` in the **Open** field and click **OK**.

3 Expand the following registry key: `HKLM\Software\WOW6432Node\Mission Critical Software\OnePoint\Administration\Modules\ServerConfiguration\`.

4 Select the `IsNTAuditEnabled` key.

5 Click **Edit > Modify**.

6 Enter `0` in the **Value data** field and click **OK**..

7 Close Registry Editor.

19.1.2 Ensuring Auditing Integrity

To ensure that all user actions are audited, DRA provides alternate logging methods when the product cannot verify logging activity. When you install DRA, the AuditFailsFilePath key and path are added to your registry to ensure the following actions:

- If DRA detects that audit events are no longer being logged in a log archive, DRA logs the audit events in a local file on the Administration server.
- If DRA cannot write audit events to a local file, DRA writes audit events to the Windows event log.
- If DRA cannot write audit events to the Windows event log, the product writes audit events to the DRA log.
- If DRA detects that audit events are not being logged, it blocks further user operations.

To enable write operations when the log archive is unavailable, you must also set a registry key value for the AllowOperationsOnAuditFailure key.

WARNING: Be careful when editing your Windows Registry. If there is an error in your Registry, your computer may become nonfunctional. If an error occurs, you can restore the Registry to its state when you last successfully started your computer. For more information, see the Help for the Windows Registry Editor.

To enable write operations:

1 Click **Start > Run**.

2 Type `regedit` in the **Open** field and click **OK**.

3 Expand the following registry key: `HKLM\Software\WOW6432Node\Mission Critical Software\OnePoint\Administration\Audit\`.

4 Click **Edit > New > DWORD Value**.

5 Enter `AllowOperationsOnAuditFailure` as the key name.

6 Click **Edit > Modify**.

7 Enter `736458265` in the **Value data** field.

8 Select **Decimal** in the **Base** field and click **OK**.

9 Close Registry Editor.

19.1.3 Understanding Log Archives

DRA logs user activity data in log archives on the Administration server. DRA creates daily log archive partitions to store data collected and normalized that day. DRA uses the date in local time on the Administration server (*YYYYMMDD*) as the naming convention for daily log archive partitions.

If you have enabled the Management Reports Collector, DRA exports log archive data to a SQL Server database as the source for DRA Management reports.

Initially, DRA retains log data in the log archive indefinitely by default. The log archive size can reach a maximum size that is determined at installation time based on available hard drive space. When the log archive exceeds this maximum size, no new audit events are stored. You can set a time limit for data retention, and DRA removes the oldest data to make room for newer data through a process called grooming. Ensure you have a backup strategy in place before you enable grooming. You can configure the log archive retention period using the Log Archive Configuration utility. For more information, see “Modifying Log Archive Grooming Settings” on page 200.

Using Log Archive Viewer Utility

You use the Log Archive Viewer utility to view data stored in log archive files. The NetIQ DRA Log Archive Resource Kit (LARK), which you can choose to install with DRA, provides the Log Archive Viewer utility. For more information, see the *NetIQ DRA Log Archive Resource Kit Technical Reference*.

Backing up Log Archive Files

A **log archive file** is a collection of record blocks. Because log archive files are compressed binary files that are located outside of a physical database, you do not need to use Microsoft SQL Server Management Studio to back up log archives. If you have an automated file backup system in place, your log archive files are backed up automatically like any other file.

Keep in mind the following best practices when planning your backup strategy:

- A single partition is created each day that contains event data for that day. When you enable grooming, the Log Archive Service will groom the data from these partitions automatically every 90 days by default. The backup strategy should take into account the grooming schedule to determine the frequency of the backups. When the log archive partitions are groomed, DRA deletes the binary files. You cannot retrieve groomed data. You must restore groomed data from a backup. For more information, see “Modifying Log Archive Grooming Settings” on page 200.
- You should only back up partitions after they have been closed. Under normal conditions, a partition is closed within 2 hours of midnight the next day.
- Back up and restore partition folders and all their subfolders as a unit. Backup the `VolumeInfo.xml` file as part of the partition backup.
- If you want to restore log archive partitions for reports, ensure backed up log archives retain or can be restored to their original format.
- When configuring your process for backing up log archive files, NetIQ recommends you exclude both the `index_data` and `CubeExport` subfolders located in the main log archive folder. These subfolders contain temporary data and should not be backed up.

Modifying Log Archive Grooming Settings

When you install DRA, log archive grooming is disabled by default. When you establish regular backup procedures for your log archive files, you should enable log archive grooming to conserve disk space. You modify the number of days before log archive partitions are groomed using the Log Archive Configuration utility.

To change the number of days before log archive partitions are groomed:

1. Log on to the Administration server using an account that is a member of the Local Administrators group.
2. Start **Log Archive Configuration** in the NetIQ Security Manager > Configuration program group.
3. Click **Log Archive Server Settings**.
4. ***If you want to enable partition grooming,*** set the value of the **Partition Grooming Enabled** field to True.
5. Type the number of days you want to retain log archive partitions before grooming in the **Number of Days before Grooming** field.
6. Click **Apply**.
7. Click **Yes**.
8. Click **Close**.
9. Locate the <*path to LogArchiveData*>\<*Partition Name*> folder and

If value is	
Checked	Click **Yes** on the confirmation message to restart the NetIQ Security Manager Log Archive service. **NOTE:** If you modify any log archive setting, you must restart the Log Archive service for the change to take effect.
Not checked	Click **No** on the confirmation message. See "To enable the DRA Log Archive Server to groom unarchived data:" on page 200.

If the "File is ready for archiving" attribute on the files or folders within the specified partitions is not checked, you must edit the CONFIG file to enable log archive grooming. To understand why this attribute might or might not be checked, see the **Additional Information** section of the How do you configure the data retention period for DRA Logarchival Data? knowledgebase article.

To enable the DRA Log Archive Server to groom unarchived data:

1. Log on locally to each DRA server windows console as a member of the local administrators group.
2. Use a text editor to open the `C:\ProgramData\NetIQ\Directory Resource Administrator\LogArchiveConfiguration.config` file and locate the `<Property name="GroomUnarchivedData" value="false" />` line.
3. Change `"false"` to `"true"` and save the file.
4. Restart the NetIQ DRA LogArchive Service.

NOTE: If you modify any log archive setting, you must restart the Log Archive service for the change to take effect.

19.2 Managing Data Collection for Reporting

DRA Reporting provides two methods of generating reports that allow you to see the latest changes in your environment and to collect and review user account, group, and resource definitions in your domain.

Activity Detail reports

Accessed through the ARM console and the Delegation and Configuration console, these reports provide real-time change information for objects in your domain.

DRA Management reports

Accessed through NetIQ Reporting Center (Reporting Center), these reports provide activity, configuration, and summarization information about events in your managed domains. Some reports are available as graphical representations of the data.

For example, you can view a list of changes made to an object or by an object during a specified time period using Activity Detail reports. You can also view a graph showing the number of events in each managed domain during a specified time period using Management reports. Reporting also allows you to view details about the DRA security model, such as ActiveView and AA group definitions.

DRA disables functions and reports that your license does not support. You must also have the appropriate powers to run and view reports. Therefore, you may not have access to some reports.

Activity Detail reports are available as soon as you install DRA through the ARM console and the Delegation and Configuration console to provide the latest details on your network changes.

DRA Management reports can be installed and configured as an optional feature and are viewed in Reporting Center. When you enable and configure data collection, DRA collects information about audited events and exports it to a SQL Server database on a schedule that you define. When you connect to this database in Reporting Center, you have access to over 60 built-in reports:

- Activity reports that show who did what, and when
- Configuration reports that show the state of AD or DRA at a specific point in time
- Summarization reports that show activity volume

For more information about configuring data collection for Management reports, see Section 19.3, “Reporting Configuration Tasks,” on page 201.

19.3 Reporting Configuration Tasks

The following step procedures provide instructions to help you enable and configure reporting and data collection for DRA Management reports.

19.3.1 Enabling Reporting and Data Collection

After installing the DRA Reporting components, enable and configure reporting a data collection to access Reporting Center reports.

To enable reporting and data collection:

1. Connect to the primary Administration server. For more information, see Section 2.7.3, “Connecting to an Administration Server,” on page 43.
2. In the left pane, expand **Directory and Resource Administrator**.
3. Expand **Configuration Management**, and then click **Update Reporting Service Configuration**.

4 On the Storage Server tab, select Enable DRA Reporting support.

5 Click Browse in the Server Name field and select the computer where SQL Server is installed.

6 On the Credentials tab, specify the appropriate credentials to use for the SQL Server interactions.

7 If this is the same account that can be used to create the database and initialize the schema, select the Use the above credentials for creating a database and initializing the database schema check box.

8 If you want to specify a different account for creating a database, on the Admin Credentials tab, specify that user account and password.

9 Click OK.

19.3.2 Configuring the Active Directory Collector

Enable and configure the Active Directory Collector to make activity data available in Reporting Center.

To configure the Active Directory Collector:

1 Expand **Configuration Management**, and then click **Update Reporting Service Configuration**.

2 On the Active Directory Collector tab, click **Not Configured** in the Managed Domains group and click **Configure**.

3 Complete the Active Directory Collector Configuration wizard.

NOTE: For more information about scheduling resource data collection, see the Help.

4 When you schedule the collector schedule for the first time, set it for daily collection a few minutes later than when you are configuring it. Doing this gives you the shortest time to wait for data to populate reports.

5 Click **Finish** when you have completed all required fields.

19.3.3 Configuring the DRA Collector

Enable and configure the DRA Collector to make adetails about the DRA configuration available in Reporting Center.

To configure the DRA Collector:

1 Expand **Configuration Management**, and then click **Update Reporting Service Configuration**.

2 On the DRA Collector tab, click **Not Configured** in the Server group and click **Configure**.

3 Complete the DRA Collector Configuration wizard.

4 When you schedule the collector schedule for the first time, set it for daily collection a few minutes later than when you are configuring it. Doing this gives you the shortest time to wait for data to populate reports.

5 Click **Finish** when you have completed all required fields.

19.3.4 Configuring the Office 365 Tenant Collector

Enable and configure the Office 365 Tenant Collector to make activity data available in Reporting Center.

To configure the Office 365 Tenant Collector:

1. Expand **Configuration Management**, then click **Update Reporting Service Configuration**.
2. On the Office 365 Tenant Collector tab, click **Not Configured** in the Office 365 Tenants group and click **Configure**.
3. Complete the Office 365 Tenant Collector Configuration wizard.
4. When you schedule the collector schedule for the first time, set it for daily collection a few minutes later than when you are configuring it. Doing this gives you the shortest time to wait for data to populate reports.

   NOTE: To prevent a failure of the Office 365 Tenant Collector, schedule the Active Directory Collector to run before the Office 365 Tenant Collector.
5. Click **Finish** when you have completed all required fields.

19.3.5 Configuring the Management Reports Collector

Enable and configure the Management Reports Collector to make activity data available in Reporting Center.

To configure the Management Reports Collector:

1. Expand **Configuration Management**, and then click **Update Reporting Service Configuration**.
2. On the Management Reports Collector tab, click **Not Configured** in the Server group and click **Configure**.
3. Complete the Management Reports Collector Configuration wizard.
4. When you schedule the collector schedule for the first time, accept the default collection and export settings. Doing this gives you the shortest time to wait for data to populate reports.
5. Click **Finish** when you have completed all required fields.

19.3.6 Viewing the Collectors Status

You can view details of each data collector on the Collectors Status tab.

To view the status of the collectors:

1. Expand **Configuration Management**, and then click **Update Reporting Service Configuration**.
2. On the Collectors Status tab, click each entry to view additional information about data collection, such as when data was last collected and whether the last data collection was successful.
3. If you see no data in the Server list, click **Refresh**.

A The Command-Line Interface

These sections describe the syntax and operation of the command-line interface (CLI). You can use the CLI to create the delegation model and perform account and server administration tasks for multiple objects at one time. The CLI supports basic administration commands for DRA and ExA.

A.1 Understanding the CLI

You can install the CLI through the user interface part of the Setup program. By default, the Setup program places the `EA.EXE` file in the `Program Files (x86)\NetIQ\DRA` folder on the DRA client computer. This file allows you to run DRA and ExA commands from the command prompt on Microsoft Windows computers.

The CLI processes the commands from the command prompt. You can run the CLI commands from the `\Program Files (x86)\DRA\` directory. By default, this location is not added to your path statement. For more information about adding this location to your path statement, see your Microsoft Windows documentation.

The CLI provides a way to quickly create AVs with rules matching the OUs.

The CLI uses several conventions to help you use the available commands. The following sections define these conventions. These sections also describe several specific characteristics of the CLI. Making mass changes through the CLI can cause other user interfaces, such as the Account and Resource Management console, to wait while the Administration server applies these changes.

A.1.1 CLI Syntax

This section uses a specific syntax for documenting CLI commands. For example, the syntax for using the `GROUP` command to update group properties is:

`EA [/DOMAIN:`*domain* `[/SERVER:`*computername*`|/MASTER]] GROUP target UPDATE {NAME:group|CN:`*"commonname"*`|COMMENT:`*"comment"*`}`

The following table lists the conventions and how they apply to this `GROUP` command.

Convention	Represents	Example
`CAPITAL LETTERS`	Commands and options	The command is `GROUP`. This command allows you to manage group accounts. The `/DOMAIN` and `UPDATE` parameters provide additional controls you can use with this command.
Italics	Variable names and values	Specify the appropriate domain name and computer name in place of the domain and computername variables.
Brackets, such as [*value*]	Optional parameters.	You are not required to specify the `/DOMAIN` or `/SERVER` parameter.

Convention	Represents	Example
Braces, such as {*value*}	Required parameters.	You must specify which properties you want to update.
Logical OR, such as *val1* | *val2*	Exclusive parameters. Choose one parameter.	You can update only one of the following properties: `NAME, CN, COMMENT`.

TIP: If you specify an incomplete command, the CLI displays syntax and option descriptions. For example, to display the syntax and help information for the `GROUP` command, enter:

```
EA GROUP
```

A.1.2 Embedded Spaces and Quotes

The CLI uses spaces to separate keywords and arguments. If you want to specify a value that contains one or more embedded spaces, enclose the value in quotation marks (`" . "`). For example, to set the fullname property of the `JaneSmith` user account to `Jane Smith`, enter:

```
EA USER JaneSmith UPDATE FULLNAME:"Jane Smith"
```

The quotation marks ensure the CLI treats `Jane Smith` as a single value. Without the quotation marks, the CLI treats `Jane` and `Smith` as separate terms and generates an error message.

A.1.3 Date and Time Format

The CLI uses a consistent date and time format for input and output. Use the following format with the CLI:

```
YYYY MM DD,hh:mm:ss
```

For example, to set the expiration date of the `MWest` user account to May 1, 2002 at 5:00 PM, enter:

```
EA USER MWest UPDATE EXPIRES:2002 05 01,17:00:00
```

A.1.4 Wildcard Characters and Naming Restrictions

DRA and ExA support wildcard characters in AA group names and many other CLI options. Names of some objects, such as user accounts, groups, resources, ActiveViews, AAs, and Administrators, cannot contain specific characters. These restrictions apply throughout the DRA and ExA user interfaces.

A.1.5 Special Terms

The following terms provide a consistent way to refer to types of command parameters:

name

Indicates a single name that includes no wildcard characters. For example, to indicate the `TomB` user account, specify `TomB`.

wildcard

Indicates a name that includes wildcard characters. The CLI expands wildcard characters in context, similar to the DOS and Microsoft Windows command line file name wildcard specifications. For example, to indicate all groups that begin with `Sales_`, specify `Sales_*`.

A.1.6 Special Functions and Variables

The CLI provides tremendous expressive power. Use the following special functions and variables to reference common sets of objects. These functions and variables enable you to perform a single command on multiple objects.

`@GroupMembers(`*`"wildcard"`*`)`

Returns a list of contacts, computers, groups, and user accounts that are members of any group matching the specified *wildcard.* You can use this function with the `ACCOUNT` and `GROUP` commands.

`@GroupMembersR(`*`"wildcard"`*`)`

Returns a list of contacts, computers, groups, and user accounts that are members of any group matching the specified *wildcard.* This function is recursive, which means it will enumerate group memberships for groups that are members of the *wildcard* group. You can use this function only with the `ACCOUNT` and `GROUP` command.

`@GroupUsers(`*`"wildcard"`*`)`

Returns a list of user accounts that are members of any group matching the specified *wildcard.*

`@GroupUsersR(`*`"wildcard"`*`)`

Returns a list of user accounts that are members of any group matching the specified *wildcard*. This function is recursive, which means it will enumerate group memberships for groups that are members of the *wildcard* group.

`@Target()`

Represents the current target of the command. This function allows you to include the target name in the specified command. For example, to set the home directory path of each user account in the `Atlanta Users` group to `\\ATLHOME\USERS\`*username*, enter:

```
EA USER @GroupUsers("Atlanta Users") UPDATE HOMEDIR:\\ATLHOME\USERS\@Target()
```

NOTE: The console allows you to use `%username%` to represent the current target. However, when the `%username%` variable is used in the CLI, Microsoft Windows defines the `%username%` variable as the currently logged on user.

`@TerritoryAccounts(`*`"wildcard"`*`)`

Returns a list of all groups and user accounts included in any ActiveView matching the specified *wildcard.*

`@TerritoryGroups(`*`"wildcard"`*`)`

Returns a list of all groups included in any ActiveView matching the specified *wildcard*.

`@TerritoryMembers(`*`"wildcard"`*`)`

Returns a list of all groups and user accounts included in any ActiveView matching the specified *wildcard*. This function is the same as the `@TerritoryAccounts(`*wildcard*`)` special function.

`@TerritoryUsers(`*`"wildcard"`*`)`

Returns a list of all user included in any ActiveView matching the specified *wildcard.*

A.1.7 Special Operators and Prefixes

When you specify some options, you may also need to specify a prefix. The CLI supports the following prefixes:

domain	Allows you to identify a user account or group in a different domain. For example, if you manage multiple domains, members of local groups can be user accounts or groups in any managed or trusted domain. If the user accounts and groups are in a domain other than the connected domain, the user account and group specifications must contain the `domain\` prefix, where domain identifies the name of this other domain. For example, to add the TomB user account from the Houston trusted domain to the Sales group, enter: `EA GROUP Sales MEMBERADD Houston\TomB` If you do not specify a domain, the CLI defaults to the connected domain.
/UNICODE	Allows you to output unicode text to the console or a file. If you want unicode output from a batch file to be redirected to a file, you should include both the "/unicode" flag as well as the redirected filename within the batch file.
/NOCR	Removes the extra CR character sequence from the CLI command output when you direct the output of the CLI command to a text file. If you use the `/UNICODE` option, type the `/NOCR` option before the `/UNICODE` option. For example, if you use the `USER` command and want to direct the output to the `temp.txt` file, enter: `EA /DOMAIN:acct04 /MASTER /NOCR /UNICODE USER DISPLAY > temp.txt`
g:	Identifies a new rule or AA as a *group.* When you specify a new rule or AA that includes a wildcard character, you need to indicate whether the rule or AA is a user account, group, or ActiveView specification. Specify `xg:` for an exclude group rule.
t:	Identifies a new rule as an *ActiveView.* When you specify a new rule that includes a wildcard character, you need to indicate whether that new rule is a user account, group, or ActiveView specification. Specify `xt:` for an exclude ActiveView rule.
u:	Identifies a new rule or AA as a *user*. When you specify a new rule or AA that includes a wildcard character, you need to indicate whether that new rule or AA is a user account, group, or ActiveView specification. Specify `xu:` for an exclude user rule.

A.1.8 Return Codes

You can create batch files with CLI commands. The CLI commands return codes depending on the success or failure of the commands. You can use these return codes to write conditional statements. The return codes are:

0	Information
1	Warning
2	Error
3	Severe error
4	Very severe error
5	Unrecoverable error
6	Extremely unrecoverable error

A.2 CLI Commands

The following sections provide details about each of the CLI commands, including the following:

- Required powers and permissions
- Syntax statements
- Supported options
- Several usage examples

A.2.1 AA Command

The AA command creates a custom Assistant Admin Group with the name, comment, and description you provide. The AA command allows you to create user and group rules with the `ADD` verb.

You must associate AAs with roles and ActiveViews to ensure AAs manage objects included in ActiveViews. This association is called delegation. Through delegation, you specify the tasks AAs can perform on the managed objects. To assign roles to AAs and ActiveViews, you must have the appropriate powers, such as those included in the Manage Security Model role.

Required Powers and Permissions

To manage assigned roles and ActiveViews, you must have the appropriate powers, such as those included in the DRA Administration and Manage Security Model roles.

Syntax

```
EA [/DOMAIN:domain [/SERVER:computername|/MASTER]] AA target CREATE [fields]
EA [/DOMAIN:domain [/SERVER:computername|/MASTER]] AA target DELETE [mode:{I|B}]
EA [/DOMAIN:domain [/SERVER:computername|/MASTER]] AA target UPDATE [NAME:newname]
[mode:{I|B}] [fields]
EA [/DOMAIN:domain [/SERVER:computername|/MASTER]] AA target DISPLAY [fields]
EA [/DOMAIN:domain [/SERVER:computername|/MASTER]] AA target ADD ruleName [OU:]
{TYPE:ruleType} {MATCH:matchString} [MEMBERS:] [RECURSIVE:] [SELECTBASE:]
[ACTION:{include|exclude}] [RESTRICTION:] [GROUPSCOPE:] [GROUPTYPE:][MODE:{I|B}]
EA [/DOMAIN:domain [/SERVER:computername|/MASTER]] AA target REMOVE rulename
[MODE:{I|B}]
EA [/DOMAIN:domain [/SERVER:computername|/MASTER]] AA target DISPLAYRULES
ruleTarget [ruleFields]
EA [/DOMAIN:domain [/SERVER:computername|/MASTER]] AA target UPDATERULES
ruleTarget [ruleFields] [NAME:newname] [MODE:{I|B}]
```

NOTE: It is not possible to create an Assistant Admin Group of type "principal".

Verbs:

CREATE — Creates a custom Assistant Admin Group with the given name, comment, and description. It is not possible to create an Assistant Admin Group of the type principal. An Assistant Admin Group becomes *principal* when assigning a user or group to an ActiveView.

DELETE	Deletes all custom Assistant Admin Groups with name matching target. When you delete Assistant Admin groups, you do not delete the Assistant Admin group members. However, Assistant Admin group members can no longer act on objects in the previously associated ActiveViews. Deleting an Assistant Admin group also deletes the Security Identifier (SID) associated with the Assistant Admin group assignment. You do not need to delete an Assistant Admin group to disassociate it from an ActiveView or role.
UPDATE	Updates all custom Assistant Admin Groups with name matching *target*.
DISPLAY	Displays any custom or built-in Assistant Admin Groups with a name matching *target*. The "name" parameter is always returned. However, by specifying only "name" on the command line, only the name field will be returned. "Assigned" corresponds to the "In Use" column of the Delegation and Configuration user interface. "Type" indicates built-in or custom.
ADD	Creates a user or group rule and associates it with an Assistant Admin. You cannot create rules matching all domains or all OUs matching wildcard in all managed domains. You cannot create a wildcard match where only a single object matches.
REMOVE	Removes the association between an Assistant Admin and an ActiveView, preventing this Assistant Admin from managing objects specified by the specified ActiveView.
DISPLAYRULES	Displays rules matching the match parameter in the target Assistant Admin. Target Assistant Admins can include both custom and built-in types.
UPDATERULES	Updates rules matching the match parameter in the target Assistant Admin. Only custom Assistant Admins will be considered for a match.

Options

/DOMAIN:*domain*	Specifies the name of the managed domain. If you do not specify this option, the CLI provides information about the domain to which the consoles last connected. If you have not used a console on this computer and you do not specify this option, the CLI connects to the domain where your user account resides. You can use wildcard characters to specify multiple domains.
/SERVER:*computername*	Specifies the name of an Administration server managing the specified domain. If you specify a domain without a server, the CLI automatically locates the closest Administration server in the specified domain. You can prefix the specified computer name with two backslashes (\\)
/MASTER	Specifies the primary Administration server managing the specified domain.
/DELI:{TAB|x}	Specifies the delimiter character you want the CLI to use to separate displayed field values. You can use this option to format output redirected to a file, easing the import of the file into a database or spreadsheet program for further analysis and reporting. You can specify any delimiter character. To specify a tab as the delimiter character, type TAB.
fields	Specifies the fields or options you want to modify or display for an Assist Admin account. When you specify one or more fields with the DISPLAY verb, type the field name without a value. For example, to display the user account comment, type COMMENT. You can specify the following field values: ALL Displays all fields.

	ASSIGNED Specifies whether the rule is in use. COMMENT:*text* Specifies the comment for the Assistant Admin group. To display comments, type COMMENT with the DISPLAY verb. DESCRIPTION:*text* Specifies the description for the Assistant Admin group. To display comments, type Description with the DISPLAY verb. NAME Specifies the new Assistant Admin name. TYPE Specifies the Assistant Admin type.
ruleFields	Specifies the rule fields or options you want to modify or display that pertain to the specified AA account. COMMENT Specifies the rule comment. DESCRIPTION Provides the rule description. The description is read-only. NAME Specifies the rule name.
TYPE:*ruleType*	[G|GROUP] Specifies a group rule. [U|USER] Specifies a user rule.
MATCH:*accountname*	Specifies the user account characters on which to match. You can use domain\AccountName format or wildcards. Uses the NetBIOS name of the current CLI focus domain.
ACTION:{include|exclude}	Specifies whether to include or exclude objects. Excludes overrule includes. For example, specifically excluding Marketing\Bob overrules an include of Marketing\B*.
RESTRICTION: {S|T|ST}	Specifies whether the rule is source or target. Default is source and target.
RECURSIVE:{Y|N}	Specifies whether to match objects in sub-containers or not. Default is yes.
SELECTBASE:{YES|NO}	Specifies whether the rule matches the group itself. Default is yes. For rules matching containers or groups, specifies whether to match base object. Default is yes.
GROUPSCOPE[[U|Universal] [G|Global] [L|Local]]	Specifies any combination of [[U|Universal] [G|Global] [L|Local]] or [All]. Multiple entries should be separated by commas.
GROUPTYPE:{S|D|ALL}	Specifies Security, Distribution, or All. Default is “All”.
MEMBERS:*memberTypes*	Specifies which type of member objects to manage. Group rules can specify group member types. Container and domain rules can specify managed object types. OU Specifies OU objects. U|USER Specifies user account objects. C|COMPUTER Specifies the computer member object. G|GROUP Specifies group objects. CT|CONTACT Specifies contact objects. ALL|NONE Specifies the all or none parameter.
MATCHNESTED:{YES|NO}	Specifies whether group rules match objects in nested groups. Adding one ActiveView to another is called **nesting**. By using nested ActiveViews in your security model, you can divide administration power and scope into smaller pieces and then assemble these pieces to meet different needs.

MODE:{I|B}	B|BATCH Specifies batch mode. Batch mode runs silently and processes without confirmation. I:Interactive Specifies interactive mode. Interactive mode provides confirmation and allows you to see the rule sentence. This is the default mode.

AA Example 1

To create an AA, enter:

```
EA AA SeattleAdmins CREATE comment:testComment description:"Admins in Seattle"
```

AA Example 2

To delete an AA, enter:

```
EA AA SeattleAdmins Delete
```

AA Example 3

To update an AA, enter:

```
EA AA "SeattleAdmins" UPDATE comment:"Seattle Printer Admins"
```

AA Example 4

To rename an AA, enter:

```
EA AA "SeattleAdmins" RENAME
```

AA Example 5

To display an AA, enter:

```
EA AA b* DISPLAY
```

AA Example 6

To display the Assistant Admin group properties, enter

```
EA AA "SeattleAdmins" DISPLAY type
```

AA Example 7

To create and associate a group rule with an AA, enter:

```
EA AA us-los* ADD groupRule type:g match:a* ou:testou*
```

A.2.2 ACCOUNT Command

The ACCOUNT command displays a list of all user accounts and groups in the specified domain.

Required Powers and Permissions

To run this command, you must have the appropriate powers, such as those included in the built-in User Administration and Group Administration roles.

Syntax

`EA [/DOMAIN:`*domain* `[/SERVER:`*computername*`|/MASTER]] ACCOUNT` *targetdomain*`\"`*accountname*`" DISPLAY`

NOTE: If the value for an option contains spaces, such as a user account name of `Jane Smith`, you must surround the option value with quotation marks. In this case, to specify a value for the *accountname* option, type *"Jane Smith".*

Verbs

DISPLAY	Displays the list of user accounts and groups in the specified domain.

Options

/DOMAIN:*domain*	Specifies the name of the managed domain. If you do not specify this option, the CLI provides information about the domain to which the consoles last connected. If you have not used a console on this computer and you do not specify this option, the CLI connects to the domain where your user account resides. You can use wildcard characters to specify multiple domains.
/SERVER:*computername*	Specifies the name of an Administration server managing the specified domain. If you specify a domain without a server, the CLI automatically locates the closest Administration server in the specified domain. You can prefix the specified computer name with two backslashes (`\\`)
/MASTER	Specifies the primary Administration server managing the specified domain.
targetdomain	Specifies the name of the domain that contains the accounts you want to display. If the target domain is the same as the domain specified by `/DOMAIN`, then you do not need to specify this option. You can use wildcard characters to specify multiple domains.
"*accountname*"	Specifies the accounts the CLI displays. The specified account name can contain wildcard characters.

ACCOUNT Example 1

To display all user accounts in the managed domains, enter:

```
EA ACCOUNT * DISPLAY
```

ACCOUNT Example 2

To display all user accounts in managed domains with names that start with HOU, enter:

```
EA ACCOUNT HOU*\* DISPLAY
```

ACCOUNT Example 3

To display all user accounts managed by the HOU_ADMIN02 secondary Administration server in the CITIES domain, enter:

```
EA /DOMAIN:CITIES /SERVER:\\HOU_ADMIN02 ACCOUNT * DISPLAY
```

ACCOUNT Example 4

To display all user accounts managed by the Primary Administration server in the SPACE domain, enter:

```
EA /DOMAIN:SPACE /MASTER ACCOUNT * DISPLAY
```

A.2.3 AV Command

The ActiveView command can create, delete, update, and rename ActiveViews. You can also use the ActiveView command to display the properties of an ActiveView, including the name, comment, description and type fields.

The ActiveView command allows for the creation of rules in conjunction with the ADD verb.

An ActiveView creates a virtual domain containing only those objects you want. You can then associate Assistant Admins with these ActiveViews and grant extremely granular control over the included objects. For more information, see Section 3.3, “What ActiveViews Provide,” on page 57.

Required Powers and Permissions

To create or delete an ActiveView or assign rules to ActiveViews, you must have the appropriate powers, such as those included in the built-in DRA Administration or Manage Security Model roles.

Syntax

EA [/DOMAIN:*domain* [/SERVER:*computername*|/MASTER]] AV *target* CREATE [fields]

EA [/DOMAIN:*domain* [/SERVER:*computername*|/MASTER]] AV *target* DELETE [mode:{I|B}]

EA [/DOMAIN:*domain* [/SERVER:*computername*|/MASTER]] AV *target* UPDATE [mode:{I|B}] [fields] [NAME:*target*]

EA [/DOMAIN:*domain* [/SERVER:*computername*|/MASTER]] AV *target* DISPLAY [fields]

EA [/DOMAIN:*domain* [/SERVER:*computername*|/MASTER]] AV *target* ADD ruleName [ruleFields] {TYPE:ruleType} {MATCH:matchString} [OU:ouString] [ACTION:] [RESTRICTION:] [RECURSIVE:] [SELECTBASE:] [MEMBERS:memberType,...] [MODE:] [MATCHWILDCARD]

EA [/DOMAIN:*domain* [/SERVER:*computername*|/MASTER]] AV *target* ADD ruleName [ruleFields] {TYPE:ruleType} {MATCH:matchString} [OU:ouString] [ACTION:] [RESTRICTION:] [RECURSIVE:] [SELECTBASE:] [MEMBERS:memberType,...] [MODE:] [MATCHWILDCARD] Resource rules only, {RESOURCES:resourceType,...} required parameter

EA [/DOMAIN:*domain* [/SERVER:*computername*|/MASTER]] AV *target* ADD ruleName [ruleFields] {TYPE:ruleType} {MATCH:matchString} [OU:ouString] [ACTION:] [RESTRICTION:] [RECURSIVE:] [SELECTBASE:] [MEMBERS:memberType,...] [MODE:] [MATCHWILDCARD] Group rules only, [matchNested], [groupScope], [groupType] optional parameters may be specified

EA [/DOMAIN:*domain* [/SERVER:*computername*|/MASTER]] AV *target* REMOVE ruleName [MODE:{I|B}]

EA [/DOMAIN:*domain* [/SERVER:*computername*|/MASTER]] AV *target* DISPLAYRULES ruleTarget [ruleFields]

EA [/DOMAIN:*domain* [/SERVER:*computername*|/MASTER]] AV *target* UPDATERULES ruleTarget [ruleFields] [NAME:newname] [MODE:{I|B}]

Verbs

CREATE	Creates an ActiveView and specifies the name and the properties for the ActiveView including the comment and description.
DELETE	Deletes a custom AV that matches the *target*. You can automate large deletes using a matching target in MODE:*batch*.
UPDATE	Updates any custom AV that matches *target.*
RENAME	Renames any custom AV that matches *target*.
DISPLAY	Displays any custom or built-in AVs matching *target*. The name parameter is always returned. However, by specifying only "name" on the command line, then only the name field will be returned (by default other fields are displayed). The display command can be used to enumerate ActiveViews matching a certain name, including wildcards.
ADD	Creates and assigns rules in conjunction with the AV command to cover the most frequent types of delegation. You use the ADD command with the following options and parameters: ruleName, [ruleFields], {TYPE:ruleType}, {MATCH:matchString}, [OU:ouString], [ACTION:], [RESTRICTION:], [RECURSIVE:], [SELECTBASE:], [MEMBERS:memberType,...], [MODE:], {RESOURCES:resourceType,...}, [matchNested], [groupScope], and [groupType]
REMOVE	Removes the associated rule from the AV.
DISPLAYRULES	Displays rules and rule properties for a given AV. Properties for a rule include the name, comment, and description.
UPDATERULES	Updates rules and rule properties for a given AV. Properties for a rule include the name, comment, and description.

Options

/DOMAIN:*domain*	Specifies the name of the managed domain. If you do not specify this option, the CLI provides information about the domain to which the consoles last connected. If you have not used a console on this computer and you do not specify this option, the CLI connects to the domain where your user account resides. You can use wildcard characters to specify multiple domains.
/SERVER:*computername*	Specifies the name of an Administration server managing the specified domain. If you specify a domain without a server, the CLI automatically locates the closest Administration server in the specified domain. You can prefix the specified computer name with two backslashes (\\).
/MASTER	Specifies the primary Administration server managing the specified domain.
target	Specifies the name of the AV you want to manage. The AV name can contain wildcard characters. You can also precede the AV name with a trusted domain or wildcard character, such as **, which targets all groups in the managed domains and trusted domains. When using the CREATE verb, the specified AV must not already exist and you cannot specify wildcard characters. When using the DISPLAY verb, specify the target as * to list all AVs in the specified OU.
commonfields	Specifies the fields or options that you want to specify, modify, or display for the ActiveView group. When you specify one or more of fields with the DISPLAY verb, specify the field name without any value. For example, to display the ActiveView comment, specify COMMENT. You can specify the following field values: ALL Displays all fields. COMMENT:"*text*" Specifies the comment for the ActiveView group. To display comments, type COMMENT with the DISPLAY verb. DESCRIPTION:"*text*" Specifies the description for the ActiveView group. To display comments, type DESCRIPTION with the DISPLAY verb. NAME:"*name*" Specifies the new name of the ActiveView. TYPE: Specifies the type of ActiveView.
RuleName:	Specifies the name of the rule you want to create or manage.
ruleFields	Specifies the rule properties that you want to modify or display for the ActiveView. These are universal rule parameters. COMMENT Specifies the comment for the specified rule. DESCRIPTION Provides the rule description. The description is read-only. NAME Specifies the name for the rule.
TYPE:{*ruleType*}	G|GROUP Specifies a group rule. OU Specifies an OU rule. DOMAIN Specifies a domain rule. U|USER Specifies a user rule. COMPUTER Specifies a computer rule. RESOURCE Specifies a resource rule.
MATCH:*matchString*	Specifies domain or wildcard name match. Must be at least one character, though that character can be a *. For ActiveViews it matches by name.
OU:*ouname*	Specifies the name of either a DN path to an OU, container, built-in, or a wildcard matching at most one OU by name. If this is specified, then the match will be evaluated only within this OU. In the case of resource rules, note that the "match" that this will apply to is the "compMatch" parameter. Default is any OU. Note that if an OU is specified for an NT4 domain, the CLI should return an error message to the client indicating that this is an invalid argument.
ACTION:{include|exclude}	Specifies whether the rule is include or exclude. This is a universal rule parameter. The default is include.

RESTRICTION:{S|T|ST}	Specifies whether the rule is source or target only (or both). This is a universal rule parameter. The default is both.
RECURSIVE:{Y|N}	Specifies whether the container rule manages groups from children OUs and containers. Default is yes. Specifies whether the rule manages nested OUs and members. Default is yes. This parameter applies to either groups or OU rules.
SELECTBASE:{YES|NO}	Specifies whether the rule matches the group itself. Default is yes. For rules matching containers or groups, specifies whether to match base object. Default is yes.
MEMBERS:memberType	Specifies which type of member objects is managed. There are group member types for group rules or managed object types for container or domain rules. Default is `ALL`. `OU` Specifies OU objects. `U|USER` Specifies account objects. `C|COMPUTER` Specifies computer objects. `G|GROUP` Specifies group objects. `CT|CONTACT` Specifies contact objects. `ALL|NONE` Specifies the all or none parameter.
MATCHNESTED:{Y|N}	Specifies whether the rule manages nested groups and members. Default is yes.
GROUPSCOPE	Specifies any combination of [`[U|Universal] [G|Global] [L|Local]]` (multiple entries must be separated by commas) or `[All]`.
GROUPTYPE:{S|D}	Specifies Security, Distribution, or All. Default is "All".
MODE: [I|B]	B specifies batch mode. The default is interactive. This mode will allow the client to see the rule sentence. By setting mode to batch, the command is processed without confirmation.
MATCHWILDCARD	Specifies whether to include all groups that do not exactly match the string specified in the `MATCH:`*matchString* option.

AV Example 1

To create a custom AV with the given name, comment, and description, enter:

```
EA AV ouComputers CREATE comment:testComment description:"Contents of computers OU"
```

AV Example 2

To delete all custom AVs matching "g*", enter:

```
EA AV g* DELETE
```

AV Example 3

To update or rename any custom AVs matching "h*", enter:

```
EA AV h* UPDATE comment:"This AV starts with letter h"
```

AV Example 4

To add a group rule, enter:

```
EA AV us-los* add groupRule type:g match:a* ou:testou*
```

AV Example 5

To create an exclude rule for ou1, which is the only OU matching ou* within testou2, enter:

```
EA AV kt* add ouRule type:ou match:ou* ou:testou2 action:exclude
```

AV Example 6

To create a rule that manages the domain and only OUs and Groups in the domain, enter:

```
EA AV d* ADD domainRule type:d match:schwamx-dom members:OU,G
```

AV Example 7

To create a rule that excludes the CEO from management in any custom AV, enter:

```
EA AV * ADD ceoExcludeRule type:u match:netiqus\boesenb* action:exclude
```

AV Example 8

To exclude objects from the K* AVs in the L* AVs, enter:

```
EA AV L* Add ExcludeKAvs type:av match:K* action:exclude
```

AV Example 9

To add a rule to the "Domain Controllers" AV to match computers named "dc*" in the OU "domain controllers" in domain netiq.local, enter:

```
EA AV "Domain Controllers" Add DCRule1 type:c match:dc* ou:"ou=domain
controllers,dc=netiq,dc=local"
```

AV Example 10

To add a rule to the "Resources" AV to match services on computer "HOULAGOS" in the current CLI focus domain, enter:

```
EA AV Resources ADD type:resource resources:services match:houlagos
```

NOTE: Through ActiveViews, you can display and change the settings of many resource properties, create and clone resources, delete resources, as well as stop and start resources. Wildcard specifications allow you to include objects from several domains or OUs while making your security model more dynamic.

A.2.4 CACHE Command

The `CACHE` command refreshes the accounts cache and the resource cache on the Administration server.

The accounts cache contains information about user accounts, groups, computer accounts, and contacts. The Administration server builds and maintains the accounts cache, which contains portions of the Microsoft Windows 2008 or higher Active Directory. The Administration server uses the

accounts cache to improve performance when validating requests. The Administration server maintains the coherency of this cache for all account administration performed through DRA and ExA.

The resource cache contains computer information. The Administration server uses the resource cache to improve performance when managing computers.

NOTE: When you use the `CACHE` command to refresh the accounts cache, the Administration server performs an incremental cache refresh by default. An incremental accounts cache refresh updates only the data that changed since the previous refresh.

For more information about the accounts cache, see Section 17.7.1, “Accounts Cache,” on page 178. For more information about the resource cache, see Section 17.3.3, “Resource Cache,” on page 168.

Required Powers and Permissions

To perform a manual refresh of the accounts and resource caches, you must have the appropriate powers, such as those included in the built-in Configure Servers and Domains role. Other AAs can only view cache refresh information.

Syntax

```
EA [/DOMAIN:domain [/SERVER:computername|/MASTER]] CACHE {targetdomain} [/FULL|/
SYSTEM]
EA [/DOMAIN:domain [/SERVER:computername|/MASTER]] CACHE {targetdomain} [DISPLAY]
```

Verbs

DISPLAY	Displays the time of the last refresh and the time of the next refresh.

Options

/DOMAIN:*domain*	Specifies the name of the managed domain for which you want to refresh or display the accounts and resource caches. If you do not specify this option, the CLI refreshes the cache for the domain to which the consoles most recently connected. If you have not used the CLI before and you do not specify this option, the CLI connects to the domain where your user account resides. You can use wildcard characters to specify multiple domains.
/SERVER:*computername*	Specifies the name of an Administration server that manages the specified domain. If you specify a domain and do not specify a server, the CLI automatically locates the best available Administration server in the specified domain. You can prefix the specified computer name with two backslashes (\\).
/MASTER	Specifies the primary Administration server that manages the specified domain.
targetdomain	Refreshes the accounts or resource cache for the specified domain, domain member, or computer.
/FULL	Performs a full accounts cache refresh. By default, the CLI performs an incremental accounts cache refresh.
/SYSTEM	Performs a resource cache refresh.

CACHE Example 1

To perform an incremental accounts cache refresh for the NORTHEAST domain, enter:

```
EA /DOMAIN:NORTHEAST CACHE NORTHEAST
```

CACHE Example 2

To perform a full accounts cache refresh on the LAB01 server in the NORTHEAST domain, enter:

```
EA /DOMAIN:NORTHEAST /SERVER:\\LAB01 CACHE NORTHEAST /FULL
```

CACHE Example 3

To refresh the resource cache for the PITTSBURGH child domain in the NORTHEAST domain, enter:

```
EA /DOMAIN:NORTHEAST CACHE PITTSBURGH /SYSTEM
```

CACHE Example 4

To display the last and next cache refresh times for the primary Administration server in the NORTHEAST domain, enter:

```
EA /DOMAIN:NORTHEAST /MASTER CACHE NORTHEAST DISPLAY
```

A.2.5 DOMAIN Command

The DOMAIN command displays an alphabetical list of all managed and trusted domains. The domain list includes the workstation, the domain to which the workstation belongs, and all the domains the workstation trusts.

Required Powers and Permissions

You must have the appropriate powers, such as those included in the built-in Computer Administration role, to run this command.

Syntax

```
EA [/DOMAIN:domain [/SERVER:computername|/MASTER]] DOMAIN namespec DISPLAY
[CONFIG]
```

Verbs

DISPLAY	Displays the information about the specified domain.

Options

/DOMAIN:*domain*	Specifies the name of the managed domain. If you do not specify this option, the CLI displays the information for the domain to which the consoles most recently connected. If you have not used the CLI before and you do not specify this option, the CLI connects to the domain where your user account resides. You can use wildcard characters to specify multiple domains.
/SERVER:*computername*	Specifies the name of an Administration server that manages the specified domain. If you specify a domain and do not specify a server, the CLI automatically locates the best available Administration server in the specified domain. You can prefix the specified computer name with two backslashes (\\).
/MASTER	Specifies the primary Administration server that manages the specified domain.
namespec	Specifies the domains you want to include in the displayed list. The *namespec* variable can include wildcard characters. To display all managed and trusted domains, specify an asterisk (*).
CONFIG	Displays domain information, such as the number of user accounts and groups, and the scheduled accounts cache refresh time.

DOMAIN Example 1

To display information for all managed and trusted domains, as well as the PDC computer names, enter:

```
EA DOMAIN * DISPLAY
```

The CLI displays the domain names and the PDC computer names:

```
EA 7.50.00 (c) Copyright 2011 NetIQ Corporation; all rights reserved.
LAB_HOULAB_HOU               LAB_HOULAB_HOU.COM
HOUSTON_LABHOUSTON_LAB     HOUSTON_LABHOUSTON_LAB.LOCAL
NORTH_HOUNORTH_HOU         NORTH_HOUNORTH_HOU.COM
```

DOMAIN Example 2

To display the configuration information for the `HOUTX` domain, enter:

```
EA DOMAIN HOUTX DISPLAY CONFIG
```

A.2.6 EXEC Command

The `EXEC` command allows you to apply actions to large numbers of objects. This command differs from other CLI commands because it does not inherently perform specific administrative tasks. Use the `EXEC` command to run a command against a result set built through CLI wildcard characters and special functions. For more information about special functions, see Section A.1.6, “Special Functions and Variables,” on page 207. The `EXEC` command runs a specified command at the CLI client where you enter the `EXEC` command. The `EXEC` command also allows you to run commands other than CLI commands.

NOTE: Use caution when using this command. Before using this command to make major system changes, back up your complete system. You can create a user account that has specific permissions and then sign on with this user account to restrict the use of this command to a limited number of objects.

Required Powers and Permissions

You must have the appropriate powers to run this command. The command you choose to run with the `EXEC` command may require specific powers for the objects affected by that command. If you do not have the required powers, the command fails and the CLI displays an error message.

Syntax

`EA [/DOMAIN:`*`domain`* `[/SERVER:`*`computername`*`|/MASTER]] EXEC [`*`"userspec" command [command_options]`*`]`

NOTE

- If the value for an option contains spaces, such as a user account name of `Jane Smith`, you must surround the option value with quotation marks. In this case, to specify a value for the userspec option, type userspec:`"Jane Smith"`.
- The *userspec, command,* and *command_options* parameters can include up to a total of 256 characters. If these parameters total more than 256 characters, the Administration server processes only the first 256 characters that you specify.

Options

/DOMAIN:*domain*	Specifies the name of the managed domain. If you do not specify this option, the CLI executes the specified command in the domain to which the consoles most recently connected. If you have not used the CLI before and you do not specify this option, the CLI connects to the domain where your user account resides. You can use wildcard characters to specify multiple domains.
/SERVER:*computername*	Specifies the name of an Administration server that manages the specified domain. If you specify a domain and do not specify a server, the CLI automatically locates the best available Administration server in the specified domain. You can prefix the specified computer name with two backslashes (\\).
/MASTER	Specifies the primary Administration server that manages the specified domain.
targetdomain	Refreshes the accounts or resource cache for the specified domain, domain member, or computer.
"userspec"	Specifies an explicit user account or list of user accounts on which to execute the command. This option is often a list of user account specifications that you generate using wildcard characters or the `@GroupUsers` filter.
command	Specifies a command to run against the users you specified for the *userspec* variable.
command_options	Specifies an option for the command you specified. This option often references the `@Target()` set operation function. For example, you can use the `@Target()` set operation to create a home directory using the user account name as part of the directory path.

EXEC Example 1

To move the home directories for all user accounts in the `SALES` group from the `\\TREK1` server to the `\\TREK2` server, enter the following commands:

```
EA EXEC @GroupUsers(SALES) XCOPY /O \\TREK1\USERS\@Target()
\\TREK2\USERS\@Target()
EA USER @GroupUsers(SALES) UPDATE HOMEDIR:\\TREK2\USERS\@Target()
EA EXEC @GroupUsers(SALES) DELTREE \\TREK1\USERS\@Target()
```

Administrators often need to reconfigure systems and relocate files and user account directories as system capacities and usages change. In this example, the first command runs the `XCOPY /O` command for each user account in the `SALES` group. The `XCOPY` command copies the home directory data for each user from the `\\TREK1` server to the `\\TREK2` server.

The second command (the `USER` command) changes the user account information to point the home directory to this new location.

The third command runs the `DELTREE` command for each user account in the `SALES` group. The `DELTREE` command deletes all the previous home directory data for these users on the `\\TREK1` server.

NOTE: The EXEC command allows you to run commands other than CLI commands. The XCOPY and DELTREE commands in this example are not CLI commands. This example outlines how the EXEC command allows you to run the XCOPY and DELTREE commands.

EXEC Example 2

Rather than separately specifying each of these commands, combine the three commands from the previous example into a single script file (.bat or .cmd) and use the EXEC command to run the script file.

To perform the actions in the previous example using a single script file, enter:

```
EA EXEC @GroupUsers(SALES) MOVEHD @Target()
```

In this example, the MOVEHD.cmd file contains the following lines:

```
XCOPY /O \\TREK1\USERS\%1 \\TREK2\USERS\%1
EA USER %1 UPDATE HOMEDIR:\\TREK2\USERS\%1
DELTREE \\TREK1\USERS\%1
```

A.2.7 GROUP Command

The GROUP command allows you to create, clone, modify, display, and delete groups.

Required Powers and Permissions

The different tasks you can perform with the GROUP command require different powers. The following table identifies the powers required for each task.

Tasks	Required Powers
Creating a new group	Create Group and Modify All Properties In order to create a group in an ActiveView, the AA must be associated with the ActiveView.
Cloning a group	Clone Group and Modify All Properties
Adding a member	Add a Member Modify Group Memberships Both the new member and the group must exist in the same ActiveView.
Removing a member	Add Object to Group
Updating the group description	Modify General Group Properties
Renaming a group	Modify Group Name
Displaying group information	View All Group Properties
Deleting a Group	Delete Group

Syntax

```
EA [/DOMAIN:domain [/SERVER:computername|/MASTER]] GROUP target CREATE {OU:ouname}
{CN:commonname} [GLOBAL|LOCAL|UNIVERSAL|LOCALDIST|GLOBALDIST|UNIVERSALDIST]
[CLONE:{"group"}] [COMMENT:"comment"] [TERRITORIES:"activeview"]
EA [/DOMAIN:domain [/SERVER:computername|/MASTER]] GROUP target MEMBERADD "member"
EA [/DOMAIN:domain [/SERVER:computername|/MASTER]] GROUP target MEMBERREMOVE
"member"
EA [/DOMAIN:domain [/SERVER:computername|/MASTER]] GROUP target DISPLAY
[OU:ouname] ["member"] [ALLMEMBERS]
EA [/DOMAIN:domain [/SERVER:computername|/MASTER]] GROUP target UPDATE
{[NAME:newname]|[COMMENT:"comment"]|[CN:commonname]}EA [/DOMAIN:domain [/
SERVER:computername|/MASTER]] GROUP target DELETE
```

NOTE: If the value for an option contains spaces, such as an OU name of `Sales and Marketing Consultants`, you must surround the option value with quotation marks. In this case, to specify a value for the `OU` option, type `OU:OU="Sales and Marketing Consultants",DC=Houston,DC=local`.

Verbs

CREATE — Creates a new global or local group. The required `GLOBAL` or `LOCAL` keyword specifies whether the group is global or local. You can also specify `UNIVERSAL`, `LOCALDIST`, `GLOBALDIST`, or `UNIVERSALDIST` instead. There is no default group type.

MEMBERADD — Adds the specified members to the specified group. You can add multiple accounts to a group. To specify multiple accounts, use the following syntax: `MEMBERADD` *accountA*,*accountB*

MEMBERREMOVE — Removes the specified members from the specified group. This verb does not delete the group member or group itself. You can remove multiple accounts from a group. To specify multiple accounts, use the following syntax: `MEMBERADD` *accountA*,*accountB*

DISPLAY — Displays the specified group names, as well as the group comments. If you specify an OU of a Microsoft Windows domain, the CLI lists all groups contained in the specified OU.

UPDATE — Updates the specified group information for the specified group. The group name specification can be a list of *wildcards*. If you rename a group, the Administration server does not rename the non wildcard rules that identify this group. However, the rule will match the renamed group because the Administration server uses the group SID to identify the group. If you rename a group that is included in ActiveViews through wildcard specifications, that group may no longer be included in the same ActiveViews. The Administration server ensures that a renamed group remains in at least one ActiveView in which the AA has one or more powers. The Administration server also ensures that the ActiveView that includes the renamed group does not give the AA more powers over the renamed group.

DELETE Deletes the specified group. When you delete a group, the Administration server also deletes all group rules that exactly match the deleted group in all ActiveViews. The Administration server does not delete the group members. If the Recycle Bin is disabled for the specified domain, the Administration server permanently deletes the group when you delete a group. If the Recycle Bin is enabled for the specified domain, the deleted group is transferred to the Recycle Bin and can be restored or permanently deleted later. If you permanently delete a group, you cannot return access capabilities for that group simply by creating a new group with the same name. Microsoft Windows uses an internal Security Identifier (SID) to refer to a group. When you create a group, Microsoft Windows assigns a unique SID to that group, rather than generating the SID from the group name.

Options

/DOMAIN:*domain* Specifies the name of the managed domain. If you do not specify this option, the CLI displays the information for the domain to which the consoles most recently connected. If you have not used the CLI before and you do not specify this option, the CLI connects to the domain where your user account resides. You can use wildcard characters to specify multiple domains.

/SERVER:*computername* Specifies the name of an Administration server that manages the specified domain. If you specify a domain and do not specify a server, the CLI automatically locates the best available Administration server in the specified domain. You can prefix the specified computer name with two backslashes (\\).

/MASTER Specifies the primary Administration server that manages the specified domain.

target Specifies the name of the group you want to manage. The group name can contain wildcard characters. You can also precede the group name with a trusted domain or wildcard character, such as `*\*`, which targets all groups in the managed domains and trusted domains. When using the `CREATE` verb, the specified group must not already exist and you cannot specify wildcard characters. When using the `DISPLAY` verb, specify the target as `*` to list all groups in the specified OU.

CLONE:"*group*" Specifies the group you want to clone. The Administration server uses the specified group as a template to create a new group. The Administration server then adds all members from the cloned group to the new group. If applicable, the Administration server also adds the new group to the ActiveViews of the original group. In a Microsoft Windows 2000 domain, you can specify the group type.

COMMENT:"*comment*" Specifies the comment for the specified group. This comment is usually a description of the group.

OU:*ouname* Specifies the name of a Microsoft Windows OU.

If you want to specify the name of an enterprise OU, use the following format: `OU=`*ou*`,DC=`*domain*`,DC=`*toplevel* For example, to specify the `SALES OU` in the `HOUSTON.LOCAL` domain, type:
`OU:OU=SALES,DC=HOUSTON,DC=LOCAL`

If you want to specify the name of a built-in OU, use the following format: `CN=`*ou*`,DC=`*domain*`,DC=`*toplevel* For example, to specify the `Users OU` in the `HOUSTON.LOCAL` domain, type: `OU:CN=Users,DC=HOUSTON,DC=LOCAL` When you create or clone a group, you must specify a Microsoft Windows OU. You do not need to specify an OU for a Microsoft Windows 2000 member server.

`CN:"`*commonname*`"` Specifies the common name (display name) of the group.

`NAME:"`*group*`"` Specifies the new account name of the group. This option allows you to rename an existing group. The powers you have in the selected ActiveView determine whether you can rename the group and the name you can assign to the group.

"*member*" Specifies the name of the group member. When you use the `MEMBERADD` or `MEMBERREMOVE` verbs, use this option to specify which members should be added or removed from the group. If the Administration server does not find the specified member in the group, the CLI displays an error.

If you specify the `DISPLAY` verb, this option specifies which group members the CLI displays. For local groups, the member specification can include a *domain/* prefix. If you do not specify this option, the CLI does not display any member information. You can use wildcard characters to specify the list of members you want to display.

You can also use the `@GroupUsers` set operation to specify all members of a group.

To add or remove a computer from group, enter the computer name in the following format: `[`*domainname*`\]`*computername*`[$]`

If you are managing Microsoft Windows domains and want to add computer accounts created by either the DRA user interfaces or the native Windows 2000 Active Directory Users and Computers, append the computer name with a $. If you are managing Microsoft Windows domains and want to add computer accounts created with the NetIQ and LDAP ADSI providers, do not append the computer name with a $.

`ALLMEMBERS` Displays group members the group contains, and includes group members in domains that DRA does not manage. To display all group members from the `EasternRegion` group, enter: `EA GROUP EasternRegion DISPLAY ALLMEMBERS`

GROUP Example 1

To create the `EasternRegion` global group in the `SalesRegions` OU of the USRegion domain and populate that group with the members of the `Boston`, `Phila`, and `NYC` groups, enter the following commands:

```
EA GROUP EasternRegion CREATE OU:OU=SalesRegions,DC=USRegion,DC=ACME,DC=COM GLOBAL
EA GROUP EasternRegion MEMBERADD
@GroupUsers(Boston),@GroupUsers(Phila),@GroupUsers(NYC)
```

GROUP Example 2

To create the `WesternRegion` group on the primary Administration server by cloning the `EasternRegion` group, enter:

```
EA /DOMAIN:USRegion /MASTER GROUP WesternRegion CREATE
OU:OU=SalesRegions,DC=USRegion,DC=ACME,DC=COM CLONE:EasternRegion
```

GROUP Example 3

To populate the EasternRegion group with members of the `Boston` group, enter:

```
EA GROUP EasternRegion MEMBERADD @GroupUsers(Boston)
```

GROUP Example 4

To add all members of the `TXPoliticians` global group to the `Friends` local group, enter:

```
EA GROUP Friends MEMBERADD @GroupUsers(TXPoliticians)
```

GROUP Example 5

To remove all members of the `Players` group from the `Cleveland` group, enter:

```
EA GROUP Cleveland MEMBERREMOVE @GroupUsers(Players)
```

GROUP Example 6

To update the comment for the `Programmers` local group, enter:

```
EA GROUP Programmers UPDATE COMMENT:"very unique individuals"
```

GROUP Example 7

To display all instances of a `SmithJL` user account in any domain in a group beginning with `NYC_`, enter:

```
EA GROUP NYC_* DISPLAY *\SmithJL
```

GROUP Example 8

To display all groups that contain members' names beginning with the letter `m`, enter:

```
EA GROUP * DISPLAY m*
```

GROUP Example 9

To display a list of all groups in the `Sales` OU of the SW domain, enter:

```
EA /DOMAIN:SW GROUP * DISPLAY OU:OU=Sales,DC=Houston,DC=SW,DC=US
```

GROUP Example 10

To delete the `Mammoth` group, enter:

```
EA GROUP Mammoth DELETE
```

A.2.8 INFO Command

The `INFO` command displays information about the Administration server to which you are connected, the DRA client computer, and your current user account.

Required Powers and Permissions

The Administration server does not require any powers or permissions to run this command.

Syntax

```
EA [/DOMAIN:domain [/SERVER:computername]] INFO
```

Options

/DOMAIN:*v*	Specifies the name of the managed domain for which you want to refresh or display the accounts and resource caches. If you do not specify this option, the CLI refreshes the cache for the domain to which the consoles most recently connected. If you have not used the CLI before and you do not specify this option, the CLI connects to the domain where your user account resides. You can use wildcard characters to specify multiple domains.
/SERVER:*computername*	Specifies the name of an Administration server that manages the specified domain. If you specify a domain and do not specify a server, the CLI automatically locates the best available Administration server in the specified domain. You can prefix the specified computer name with two backslashes (\\).

INFO Example 1

To display information about the NORTHEAST domain, enter:

```
EA /DOMAIN:NORTHEAST INFO
```

INFO Example 2

To display information about the NORTHEAST domain by connecting to the PIT SERVER01 computer, enter:

```
EA /DOMAIN:NORTHEAST /SERVER:PIT SERVER01 INFO
```

A.2.9 ROLE Command

The ROLE command displays roles and role properties, enumerates roles matching a certain name, delegates and revokes roles to AVs. Properties for a role include the name, comment, description, type, and whether the role is assigned.

A role and role properties can be displayed. You can enumerate the roles with the DISPLAY command. The command is interpreted as a wildcard match of roles.

A role is a set of powers that provide the permissions required to perform a specific administration task, such as creating a user account or moving shared directories. To create a role, first define the job description. The job description provides the list of powers an AA needs to perform a task or complete a workflow.

A role can contain any set of powers you specify. Because you can choose from hundreds of powers, you have the flexibility to create roles that best fit your organization.

Required Powers and Permissions

To run these commands, you must have the appropriate powers, such as those included in the built-in DRA Administration and Manage Security Model roles.

Syntax

```
EA [/DOMAIN:domain [/SERVER:computername|/MASTER]] AV target DELEGATE {role:}
{admin:} [mode:]
EA [/DOMAIN:domain [/SERVER:computername|/MASTER]] AA target DISPLAY
EA [/DOMAIN:domain [/SERVER:computername|/MASTER]] AV target REVOKE {role:}
{admin:} [mode:]
```

Verbs

DELEGATE	Delegates a specific role to a specific admin in a given AV or AV wildcard match. The DELEGATE command can clearly distinguish the AA as a user, group, or AA Group. Specify users or groups by their Account Name or a wildcard that matches at most one user or group. Roles can be delegated or revoked, but cannot be defined.
DISPLAY	Displays any custom or built-in roles and role properties with name matching target. Properties for a role include the name, comment, description, type, and whether the role is assigned. The name parameter is always returned. By specifying only "name" on the command line, then only the name field will be returned. By default other fields are displayed
REVOKE	Revokes a specific role from a specific admin in a given AV or AV wildcard match. An error message is returned, if the delegation is not found on the Administration server.

Options

/DOMAIN:*domain*	Specifies the name of the managed domain. If you do not specify this option, the CLI provides information about the domain to which the consoles last connected. If you have not used a console on this computer and you do not specify this option, the CLI connects to the domain where your user account resides. You can use wildcard characters to specify multiple domains.
/SERVER:*computername*	Specifies the name of an Administration server managing the specified domain. If you specify a domain without a server, the CLI automatically locates the closest Administration server in the specified domain. You can prefix the specified computer name with two backslashes (\\)
/MASTER	Specifies the primary Administration server managing the specified domain.
{ADMIN:}	Specifies the *domain**Account Name* match, or the AA name. This must match only one object or the command will not be processed. This required option is used with the DELEGATE and REVOKE command.

commonfields	ALL Displays all fields. ASSIGNED Specifies whether the rule assigned or in use. COMMENT:"*text*" Specifies the comment for the ActiveView group. To display comments, specify COMMENT with the DISPLAY verb. DESCRIPTION:"*text*" Specifies the description for the ActiveView group. To display comments, specify COMMENT with the DISPLAY verb. NAME Specifies the new AV name of the ActiveView. TYPE Specifies the type of AV.
{ROLE:}	Specifies the role alias or role name that the client wants to assign to the target AV match. This is interpreted as a role name match. This must match only one object or the command will not be processed. This required option is used with the DELEGATE and REVOKE command.
MODE:{B|BATCH}	Allows you to display GUID information for the specified Administration servers.

ROLE Example 1

To delegate a role to the target AV match, enter:

```
EA AV kt* DELEGATE role:helpdesk* admin:dep1
```

ROLE Example 2

To enumerate roles matching a certain name, enter:

```
EA ROLE "a*" DISPLAY type
```

A.2.10 SERVER Command

The SERVER command displays Administration server information.

Required Powers and Permissions

The Administration server does not require any powers or permissions to run this command.

Syntax

```
EA SERVER {BEST|MASTER|*} DISPLAY [ADVANCED]
```

Verbs

DISPLAY	Displays a list of Administration servers for the user's domain as well as information for each server.

Options

BEST	Specifies the closest Administration server for the user's domain. Specify an asterisk (*) to display information for all Administration servers managing the domain.
MASTER	Specifies the primary Administration server for the user's domain. Specify an asterisk (*) to display information for all Administration servers managing the domain.
ADVANCED	Allows you to display GUID information for the specified Administration servers.

SERVER Example 1

To display information about the primary Administration server for the managed domain, enter:

```
EA SERVER MASTER DISPLAY
```

SERVER Example 2

To display information, including GUID information, about all Administration servers for the managed domain, enter:

```
EA SERVER * DISPLAY ADVANCED
```

A.2.11 USER Command

The USER command allows you to create, clone, modify, display, and delete user accounts on an Administration server.

Required Powers and Permissions

The different tasks you can perform with the USER command require different powers. The following table identifies the powers you need for each task.

Tasks	Required Powers
Creating or cloning a user account	◆ Add New User to Group ◆ Clone User and Modify All Properties ◆ Create User and Modify All Properties
Adding a mailbox for an existing user account	Create Exchange mailbox and modify all properties.
Updating user account or mailbox properties	The powers required to update user account properties depends on what properties you want to update.
Displaying user account properties	View All User Properties
Deleting a user account	Delete User Account

Syntax

```
EA [/DOMAIN:domain [/SERVER:computername|/MASTER]] USER target CREATE  {OU:ouname}
{PASSWORD:password} [fields] [CLONE:"username"] [mailboxfields] [MBDIRNAME]
[GROUPS:"groupname"]
EA [/DOMAIN:domain [/SERVER:computername|/MASTER]] USER target MBCLONE
[CLONE:"username"] [Code1Variable] [MBDIRNAME]
EA [/DOMAIN:domain [/SERVER: computername |/MASTER]] USER target UPDATE [fields]
[mailboxfields] [wtsfields] [NAME:newname] [PASSWORD:password]
EA [/DOMAIN:domain [/SERVER: computername |/MASTER]] USER target DELETE
EA [/DOMAIN:domain [/SERVER: computername |/MASTER]] USER target GROUPS
EA [/DOMAIN:domain [/SERVER: computername |/MASTER]] [/DELI:{TAB|x}] USER target
DISPLAY {OU:ouname} [fields] [wtsfields] [displayfields]
```

NOTE: If the value for an option contains spaces, such as an OU name of Sales and Marketing Consultants, you must surround the option value with quotation marks. In this case, to specify a value for the `OU` option, type `OU:OU="Sales and Marketing Consultants",DC=Houston,DC=local`.

Verbs

CREATE	Creates the specified user account.
MBCLONE	Creates a mailbox for the specified user account by cloning the existing mailbox for the user account identified by the `CLONE:`*username* option.
UPDATE	Updates the specified attributes of an existing user account. You can update only the properties for which you have the required powers to modify.
GROUPS	Displays the groups to which the specified user account belongs.
DISPLAY	Displays the existing user account information. If you do not identify specific field names, the CLI displays the values for the user name, comment, and user comment fields. The CLI always displays the user name field. If you specify an OU of a Microsoft Windows 2000 domain, the CLI lists all user accounts contained in the specified OU.

DELETE

Deletes the specified user accounts.

When you delete a user, the Administration server automatically deletes all user rules that exactly match (not through a wildcard rule specification) the deleted user in all ActiveViews.

If the Recycle Bin is disabled for the specified domain, the Administration server permanently deletes the user account when you delete a user account.

If the Recycle Bin is enabled for the specified domain, the deleted user account is transferred to the Recycle Bin and can be restored or permanently deleted later.

If you permanently delete a user account, you cannot return access capabilities for that account simply by creating a new user account with the same name. Microsoft Windows uses an internal Security Identifier (SID) to refer to a user account. When you create a user account, Microsoft Windows assigns a uniue SID to that account, rather than generating the SID from the user account name.

You can use policy to configure the Administration server to also delete the associated home directory or mailbox. For more information about policy, see Chapter 13, “Enforcing Policy,” on page 115.

Options

/DOMAIN:*domain*

Specifies the name of the managed domain. If you do not specify this option, the CLI uses the domain to which the consoles most recently connected. If you have not used the CLI before and you do not specify this option, the CLI connects to the domain where your user account resides. You can use wildcard characters to specify multiple domains.

/SERVER:*computername*

Specifies the name of an Administration server that manages the specified domain. If you specify a domain and do not specify a server, the CLI automatically locates the best available Administration server in the specified domain. You can prefix the specified computer name with two backslashes (\\).

/MASTER

Specifies the primary Administration server that manages the specified domain.

/DELI:{TAB|x}

Specifies the delimiter character that the CLI uses to separate the displayed field values. This option allows you to format the output when you redirect the results to a file. You can then import the file into a database or spreadsheet program for further analysis and reporting. You can specify any delimiter character. To specify a tab as the delimiter character, type TAB.

OU:*ouname*

Specifies the name of a Microsoft Windows 2000 OU. ***If you want to specify the name of an enterprise OU***, use the following format: OU=*ou*,DC=*domain*,DC=*toplevel* For example, to specify the SALES OU in the HOUSTON.LOCAL domain, type: OU:OU=SALES,DC=HOUSTON,DC=LOCAL ***If you want to specify the name of a built-in OU***, use the following format: CN=*ou*,DC=*domain*,DC=*toplevel* For example, to specify the Users OU in the HOUSTON.LOCAL domain, type: OU:CN=Users,DC=HOUSTON,DC=LOCAL When you create or clone a user, you must specify a Microsoft Windows 2000 OU. You do not need to specify an OU for a Microsoft Windows 2000 member server.

target Specifies the user account name or logon name for the user account you want to create or manage. If you are creating a new user account, you must specify a single user account name. You can specify wildcard characters with all verbs except the `CREATE` verb. When using the `DISPLAY` verb, specify the target as `*` to list all users in the specified OU.

`CLONE:"`*username*`"` Specifies the user account to use as a template for the new user account. The Administration server copies the field values and group memberships from the specified user account and uses them as defaults for the new user account. The Administration server sets any fields not specified in this `USER` command, except the password field, to the value of the specified user account you want to clone.

`GROUPS:"`*groupname*`"` Specifies the groups to which you want to add the new user account as a member.

`NAME:"`*name*`"` Specifies a new common name for the user account. This option allows you to rename an existing user account.

fields Specifies the fields or options that you want to specify, modify, or display for the specified user account. When you specify one or more of fields with the `DISPLAY` verb, specify the field name without any value. For example, to display the user account comment, specify `COMMENT`. You can specify the following field values:

`ACTIVE:{Y|:N}` Specifies whether the account is enabled (`:Y`) or disabled (`:N`). The default is enabled (`Y`).

`CODEPAGE:`*nnn* Specifies the code page you want to use to display characters. The default is `0`, which specifies the code page configured for the local computer.

`COMMENT:"`*text*`"` Specifies the comment for the user account. To display comments, specify `COMMENT` with the `DISPLAY` verb.

`COUNTRYCODE:`*nnn* Specifies the country code number. The default is `0`.

`DIALCALLBACK:`*telephonenumber* Specifies the telephone number for the `AdminSetCallBack` value of the `DIALFLAGS` field.

`DIALFLAGS:[DialinPrivilege,]callbacksetting` Specifies the dial-in privileges for the user account. If you do not specify the `DialinPrivilege` option, the Administration server disables the dial-in privileges. You can use the following values for the *callbacksetting* value:

`AdminSetCallBack` Directs the server to call the user at the telephone number specified by the `DIALCALLBACK` field. The server calls the user back only at the specified number. `CallerSetCallBack` Directs the server to prompt the user for a telephone number. `NoCallBack` Disables the call back function for the user account. This is the default setting.

`DISPName:"`*displayname*`"` Specifies the display name of a Microsoft Windows user account.

`EXPIRES:{`*date*`|NEVER}` Specifies an expiration date and time for the user account. Specify dates in the following format: `YYYY MM DD,hh:mm:ss` You can truncate the date at any point, after which the Administration server completes the specification with the lowest allowable value. For example, if you specify `2002-1`, the Administration server sets the expiration date to `2002-1 01,00:00:00`. If you specify `NEVER`, the Administration server sets no expiration date for the user account.

`FIRSTNAME:"`*givenname*`"` Specifies the first name of the user account.

FULLNAME:"*name*" Specifies the full name of a Microsoft Windows user account.

HOMEDIR:"*path*" Specifies the UNC path of the home directory. If you want to map a drive letter to a location, you must specify the HOMEDIRDRIVE and the HOMEDIR options to identify the mapping. DRA allows you to use %username% to represent the current target. However, when you use the %username% variable in the CLI, Microsoft Window 2000 defines the %username% variable as the currently logged on user.

HOMEDIRDRIVE:"*x*:" Specifies the drive letter you want to map to the home directory (HOMEDIR:) when the user logs on. To clear the mapped home directory for a user account, specify a space instead of a drive letter.
HOMEDIRREQ:{Y|N} Specifies whether a home directory is required for a user account. The default is Yes (Y).

INITIALS:"*initials*" Specifies the initials of the user account.

LASTNAME:"*sn*" Specifies the last name of the user account.

MIDDLENAME:"*middlename*" Specifies the middle name of the user account.

PASSWORDCHG:{Y|N} Specifies whether the user can change the user account password. The default is Yes (Y).

PASSWORDEXPIRED:{Y|N} Specifies whether the user must change the password the next time the user logs on. The default is No (N). If you specify Yes (Y), the user must change the password. If you specify PASSWORDNOEXPIRE:Y for a user account, you cannot specify PASSWORDEXPIRED:Y for the same user account.

PASSWORDNOEXPIRE:{Y|N} Specifies whether the user account password never expires (Y). The default is No (N).

PASSWORDREQ:{Y|N} Specifies whether the user account must have a password. The default is Yes (Y).

PRIMARYGROUP:"*group*" Specifies the primary group for the user account. The primary group must be a global group. In addition, the user account must be a member of the group before you can specify the group as the primary group for the user account. You cannot remove a user account from the primary group. Use primary groups mainly for POSIX compatibility

PROFILEPATH:"path" Specifies the path of the logon profile for the user account. To specify a path that ends with a backslash (\), such as "C:\PROFILE\", you must specify two backslashes: C:\PROFILE\\. A specified share cannot end with a backslash.

SCRIPTPATH:"*path*" Specifies the location of the logon script for the user account relative to the %SYSTEMROOT%\SYSTEM32\REPL\IMPORT\SCRIPTS directory. This script is run when the identified user logs on. Do not specify a file name with a UNC or drive letter.

TIMES:{times|ALL} Specifies the times during which a user account can log on. Specify the times value in 1 hour increments and in the following format: *day[day][,day[day]], time[time][,time[time]]* Abbreviate the name of the day. Specify hour values from 0 to 24, based on a 24 hour clock. If you specify 4-8, the user can log on from 4:00 AM until 7:59 AM. If you specify ALL, the user can log on at any time of the day. If you do not specify any value, the user can never log on. Separate day and time entries with a comma (,), and separate multiple day and time entries with a semicolon (;). For example, to allow a user to log on any time except from 4:00 PM to 8:00 PM on Sundays, specify: `sun,0 16;sun,20 24;mon sat,0 24`

UNLOCK:Y Unlocks a locked user account.

USERCOMMENT:"*comment*" Sets the user account comment. If a comment contains a space, such as "Sales and Marketing", you must surround the comment with quotation marks.

WORKSTATIONS:*computername* Lists as many as eight computers from which a user account can log on to the network. Separate each workstation name with a comma (,). If you do not specify any computer names, the user account can log on from any computer.

WTSProfilePath:"*path*" Specifies the location of the Microsoft Windows terminal services profile path for the specified user account.

mailboxfields Specifies the properties of the mailbox for the specified user account. You can use the following values to specify the mailbox properties you want to create or change.

MBALIAS:"*alias*" Specifies the alias for the mailbox.

MBDIRNAME:"*directory*" Specifies the directory where you want to store the mailbox. You can specify this field only when cloning a user account or mailbox. You cannot specify this field when using the UPDATE verb.

MBFIRSTNAME:"*firstname*" Specifies the first name for the mailbox.

MBLASTNAME:"*lastname*" Specifies the last name for the mailbox.

MBINITIALS:*initials* Specifies the initials for the mailbox.

wtsfields Specifies the Windows Terminal Server (WTS) properties for the specified user account.

WTSALLOW:{Yes|No} Specifies whether the user can log on to the Terminal Server.

WTSHOMEDIR:"*path*" Specifies the UNC path of the home directory for the user when that user logs on to the Terminal Server. If you want to map a drive letter to the location, you must specify the WTSHOMEDIR and the WTSHOMEDIRDRIVE options. If you do not specify this option, the Administration server assigns the user account home directory to the WTSHOMEDIR option.

WTSHOMEDIRDRIVE:"*x:*" Specifies the drive letter you want to map to the WTS home directory (WTSHOMEDIR) when the user logs on to the Terminal Server. To clear the mapped WTS home directory for a user account, specify a space instead of a drive letter.

WTSPROFILEPATH:"*path*" Specifies the path and name of the user profile to use when the user logs on to Terminal Services.

WTSCLIENTDRIVES:{Yes|No} Specifies whether Windows Terminal Services reconnects mapped drives after the user logs on, for Citrix ICA clients. This setting does not apply to RDP clients.

WTSCLIENTPRINTERS:{Yes|No} Specifies the Terminal Services server to download and install the printer driver for the local client printer when the user logs on to a Terminal Services session.

WTSPRINTERDEFAULT:{Yes|No} Specifies that the Terminal Services session default to the main client printer. Selecting this option prevents Terminal Server from downloading and installing multiple printer drivers when users log on to a Terminal Services session.

displayfields Specifies the fields for which you want the CLI to display information. You cannot specify these fields when you create or update a user account. Use the following values to specify the information you want to display:

ALL Displays all user account fields, except the password field.
BADPWCOUNT Displays the number of invalid passwords currently outstanding for this user account. This count is cleared once the user enters a valid password.

DISPNAME Displays the display name, or friendly name, of this user account.

LASTLOGON Displays the last time the user logged on and the domain controller that validated the log on. The Administration server periodically consolidates this information from all domain controllers.

NAME Displays the name of the user account. Specify this field if you want to display only the user account name. If you specify any other fields, the CLI automatically displays the user account name.

NETWARE Displays the NetWare compatibility information of this user account. Specifying this field displays all the NetWare compatibility fields.

NUMLOGONS Displays the number of times the PDC has validated a logon attempt for that user account. The BDC also validates logon attempts, so this number is not an indicator of how many times a user actually logged on.

PASSWORDAGE Displays the time interval since the user, Administrator, or AA last set the password.

USERID Displays the RID of the user account. The RID is an internal numeric identifier for the user account.

USER Example 1

To create the JASmith user account on the primary Administration server for the SPACE domain, and add the account to the Sales Personnel group, enter:

```
EA /DOMAIN:SPACE /MASTER USER JASmith CREATE OU:OU=Jupiter,DC=Space,DC=com
FULLNAME:"Jane A. Smith" COMMENT:President GROUPS:"Sales Personnel"
```

NOTE: The Administration server sets all fields (*commonfields* and *mailboxfields*) that you did not specify to the default values.

USER Example 2

To create the JohnDoe user account and mailbox on the primary Administration server for the SPACE domain by cloning the JaneDoe user account, enter:

```
EA /DOMAIN:SPACE /MASTER USER JohnDoe CREATE OU:OU=Jupiter,DC=Space,DC=com
FULLNAME:"John Q. Doe" CLONE:JaneDoe MBALIAS:"John Doe" MBFIRSTNAME:John
MBLASTNAME:Doe PASSWORD:1234 GROUPS:"Western Region"
```

NOTE: If you defined proxy generation rules for this domain, use the FIRSTNAME, LASTNAME, MIDDLENAME, and INITIALS fields to specify a unique email address for the target account.

USER Example 3

To unlock the JASmith user account enter:

```
EA USER JASmith UPDATE UNLOCK:Y
```

NOTE: This example does not update any other properties.

USER Example 4

To change the LBond logon name to LDoe, and change the mailbox last name to Doe, enter:

```
EA USER LBond UPDATE NAME:LDoe MBLASTNAME:Doe
```

USER Example 5

To clone the JSmith user account mailbox to create a mailbox for the LBond user account, enter:

```
EA USER LBond CREATE OU:OU=agents,DC=london,DC=uk CLONE:JSmith PASSWORD:Phooey
MBFIRSTNAME:Lisa MBLASTNAME:Bond
```

To add more information about the LBond user account, use the UPDATE verb once the Administration server completes creating the LBond user account.

USER Example 6

To display a list of all user accounts in the Sales OU of the SW domain, enter:

```
EA /DOMAIN:SW USER * DISPLAY OU:OU=Sales,DC=Houston,DC=SW,DC=US
```

USER Example 7

To save a tab delimited list of all user accounts, along with the last logon timestamp for each user account, in the D:\TEMP\USERS.TXT file, enter:

```
EA /DELI:TAB USER * DISPLAY LASTLOGON > D:\TEMP\USERS.TXT
```

Directory and Resource Reporting provides last logon statistic reports to help you view this important last logon information.

USER Example 8

To delete the `JASmith` user account, enter:

```
EA USER JASmith DELETE
```

WARNING: If you delete a user account, you cannot return access capabilities for that user simply by creating a new user account with the same name. Microsoft Windows 2008 or later uses an internal Security Identifier (SID) to refer to a user account. When you create a user account, Microsoft Windows 2008 or later assigns a SID to that user account. Microsoft Windows 2008 or later does not generate the SID from the user account name.

A.2.12 WHOAMI Command

The `WHOAMI` command displays information, such as the total number of managed domains and user accounts, about both the DRA client computer and the Administration server. This information is often important when diagnosing problems or when reporting any problems to NetIQ Technical Support.

Required Powers and Permissions

You do not need any special powers or permissions to run this command.

Syntax

```
EA [/DOMAIN:domain [/SERVER:computername|/MASTER]] [/POWERS] WHOAMI
```

Options

/DOMAIN:*domain*	Specifies the name of the managed domain. If you do not specify this option, the CLI displays the information for the domain to which the consoles most recently connected. If you have not used the CLI before and you do not specify this option, the CLI connects to the domain where your user account resides. You can use wildcard characters to specify multiple domains.
/SERVER:*computername*	Specifies the name of an Administration server that manages the specified domain. If you specify a domain and do not specify a server, the CLI automatically locates the best available Administration server in the specified domain. You can prefix the specified computer name with two backslashes (\\).
/MASTER	Specifies the primary Administration server that manages the specified domain.
/POWERS	Displays the powers of the user account logged on to the DRA client computer. This option displays all the powers that an AA has in a domain. It does not display the powers for each ActiveView. Therefore, the AA may not have all the displayed powers in each ActiveView.

WHOAMI Example 1

To retrieve information for the MARS Administration server in the SPACE domain, enter:

```
EA /DOMAIN:SPACE /SERVER:MARS WHOAMI
```

WHOAMI Example 2

To retrieve information for the primary Administration server in the SPACE domain, enter:

```
EA /DOMAIN:SPACE /MASTER WHOAMI
```

WHOAMI Example 3

To display all the powers of the user account logged on to the Administration CLI computer, enter:

```
EA /POWERS WHOAMI
```

B Available Utilities

These sections discuss the Diagnostic Utility, Deleted Object Utility, and Recycle Bin Utility provided with DRA and ExA.

B.1 Diagnostic Utility

The Diagnostic Utility gathers information from your Administration server to help diagnose issues with DRA and ExA. Use this utility to provide log files to your NetIQ Technical Support representative. The Diagnostic Utility provides a wizard interface that guides you through setting log levels and collecting diagnostic information.

B.1.1 Accessing the Diagnostic Utility

You can access the Diagnostic Utility from any Administration server computer. However, you should run the Diagnostic Utility on the Administration server where you are experiencing the issue.

By default, the setup program installs the Diagnostic Utility with the Administration server component. You cannot copy the utility to another folder and run the utility from the new folder.

To access the Diagnostic Utility:

1. Log on to the Administration server computer using the DRA Admin account.
2. Run `DRADiagnosticUtil.exe` from the `Program Files (x86)\NetIQ\DRA` folder.

B.1.2 Understanding the Diagnostic Information

You can select which diagnostic information you want to collect or let the Diagnostic Utility collect the recommended data for a specific failure type. Based on the failure type you choose, the Diagnostic Utility gathers the following information from your Administration server:

ADSI logs

Collects diagnostic information about the DRA ADSI provider from Administration registry entries under `HKEY_Local_Machine\Software\WOW6432Node\Mission Critical Software\OnePoint\ADSI`.

APJS diagnostics

Collects diagnostic information about the Accounts Provider Job Scheduler and the tasks this provider controls.

Application Event log

Collects diagnostic information from the Windows server hosting the DRA server application Windows Application Event Log.

Automation scripts

Collects diagnostic information about scripts running for automation triggers.

Domain cache files

Collects the domain cache files on this Administration server.

Domain cache logs

Collects diagnostic information about the domain cache on this Administration server.

DRA registry settings

Collects diagnostic information from the entire Administration registry entry under `HKEY_Local_Machine\Software`.

Dr. Watson logs

Collects debugging information about applications you run on this computer. To enable this option, install and set up Dr. Watson as your default debugging tool. For more information about using Dr. Watson as your default debugging tool, see the *Admnistration Installation Guide*.

File times and sizes

Collects the time stamp and size for each file in the `Program Files (x86)\NetIQ\DRA` folder on your Administration server.

IIS service logs

Collects diagnostic information about IIS application settings.

Install information

Collects diagnostic information from a subset of the entire registry.

Licensing information

Collects information about the current effective license.

Server state information

Collects internal Administration server information. If the Administration server is not currently running, the utility is unable to collect any server state information. In addition the data collection process fails. If the collection process fails, deselect **Server State Information** and re-run the utility.

Server logs

Collects diagnostic information from the Administration server logs. The `McsAdminSvc_Startup.nq1` file logs service initialization data and the `McsAdminSvc.nq1` file logs general Administration server data.

Services configurations

Collects a list of the services running on the Administration server including the service type, status, and logon parameters.

System Event log

Collects diagnostic information from the Windows server hosting the DRA Server Application Windows System Event Log.

Web Console logs

Collects diagnostic information about event log entries, performance metrics, and the virtual directory settings for the Web Console.

Win32 console log files

Collects diagnostic information about the Account and Resource Management console and the Delegation and Configuration console.

Win32 console settings

Collects the client options and other settings for the Account and Resource Management console and the Delegation and Configuration console.

B.1.3 Configuring Log Settings

You can configure different log settings, such as logging levels, for individual DRA components on each Administration server computer. The logging level determines the quantity and detail of the diagnostic information you can collect. For example, if you set a high logging level, DRA logs additional information that can be used to help diagnose a more complex issue. Before collecting diagnostic information, ensure the log level is appropriate for the issue you are experiencing.

To configure log settings:

1. Start the Diagnostic Utility. For more information, see Section B.1.1, “Accessing the Diagnostic Utility,” on page 243.
2. Click **Enable or change logging for a DRA component**, and then click **Next**.
3. Specify the appropriate log level for the DRA component about which you want to collect diagnostic information.
4. To specify additional settings, such as the log file location, complete the following steps:
   - **4a** Click **Settings** for the appropriate DRA component.
   - **4b** Specify which settings you want to the Diagnostic Utility to use when logging information about this component.
   - **4c** Click **OK**.
5. To apply these settings, click **Finish**.

B.1.4 Collecting Diagnostic Information

You can select which diagnostic information you want to collect or let the Diagnostic Utility collect the recommended data for a specific failure type. Based on the failure type you choose, the Diagnostic Utility gathers the appropriate information from your Administration server.

By default, the Diagnostic Utility outputs information as `a.zip` file. When you call NetIQ Technical Support, you may need to provide this file to your Technical Support representative By default, DRA puts log files in the following location on the Administration server computer: `C:\Documents and Settings\`*`username`*`\Local Settings\Application Data\NetIQ\DRA\Logs`. For more information, see Section B.1.7, “Finding Specific Log Files,” on page 246.

For more information about which diagnostics to select, see Section B.1.2, “Understanding the Diagnostic Information,” on page 243or consult your Technical Support representative.

To collect diagnostic information:

1. Start the Diagnostic Utility. For more information, see Section B.1.1, “Accessing the Diagnostic Utility,” on page 243.
2. Click **Collect diagnostics information about a DRA failure**, and then select the failure type that best represents your issue.
3. Click **Next**.
4. Review the diagnostic settings for the selected failure type, and then click **Next**. You can select or clear a setting, or choose another failure type.

5 Specify the name and location of the `zip` file.

6 To begin collecting diagnostics, click **Finish**.

B.1.5 Viewing APJS Diagnostics

The Accounts Provider Job Scheduler (APJS) is part of the Administration server component. APJS controls schedules and records the status of various domain and server tasks, such as accounts cache refreshes and synchronization across multiple Administration servers. APJS diagnostics provide detailed information about these server and domain activities.

To view Accounts Provider diagnostics:

1 Start the Diagnostic Utility. For more information, see Section B.1.1, “Accessing the Diagnostic Utility,” on page 243.

2 Click **View Accounts Provider Job Scheduler diagnostics**.

3 To update the diagnostic information, click **Refresh**.

4 Click **Finish**.

B.1.6 Viewing Lock Diagnostics

You can use the Diagnostic Utility to view the status of read and write locks on this Administration server. Locks occur during server synchronizations and some cache refreshes. During a lock, an Assistant Admin may not be able to view (read) or modify (write) managed objects. Lock diagnostics provide a count of pending read and write operations, as well as the last time the Administration server successfully released a lock.

To view lock diagnostics:

1 Start the Diagnostic Utility. For more information, see Section B.1.1, “Accessing the Diagnostic Utility,” on page 243.

2 Click **View lock diagnostics for Read/Write and Replication locks**.

3 To update the diagnostic information, click **Refresh**.

4 Click **Finish**.

B.1.7 Finding Specific Log Files

You can use the Diagnostic Utility to find specific log files for a DRA component. By default, DRA puts log files in the following location on the Administration server computer: `C:\Documents and Settings\`*`username`*`\Local Settings\Application Data\NetIQ\DRA\Logs`. You can configure the log file location for individual DRA components. For more information, see Section B.1.3, “Configuring Log Settings,” on page 245.

To find a specific log file:

1 Start the Diagnostic Utility. For more information, see Section B.1.1, “Accessing the Diagnostic Utility,” on page 243.

2 Click **Enable or change logging for a DRA component**, and then click **Next**.

3 Click **Find Logs** for the appropriate DRA component.

4 To view a log file, select the file, and then click **File > Open**.

5 To print a log file, select the file, and then click **File > Print**.

6 Close the file view window, and then click **Finish**.

B.2 Deleted Objects Utility

This utility allows you to enable incremental accounts cache refresh support for a specific domain when the domain access account, such as the access account, is not an administrator. If the domain access account does not have read permissions on the Deleted Objects container in the domain, DRA cannot perform an incremental accounts cache refresh. For more information about the accounts cache, see Section 17.7.1, “Accounts Cache,” on page 178.

You can use this utility to perform the following tasks:

- Verify that the specified user account or group has read permissions on the Deleted Objects container in the specified domain
- Delegate or remove read permissions to a specified user account or group
- Delegate or remove the Synchronize directory service data user right to a user account
- Display security settings for the Deleted Objects container

By default, you can run the Deleted Objects Utility from the `Program Files (x86)\NetIQ\DRA` folder on your Administration server. You can install and run the Deleted Objects Utility on a computer that is not an Administration server. To install this utility, choose custom installation in the setup program. For more information about performing a custom installation, see the *Installation Guide*.

B.2.1 Required Permissions for Deleted Objects Utility

To use this utility, you must have the following permissions:

If you want to …	You need this permission …
Verify account permissions	Read Permissions access to the Deleted Objects container
Delegate read permissions on the Deleted Objects container	Administrator permissions in the domain where the Deleted Objects container is located
Delegate the Synchronize directory service data user right	Administrator permissions in the domain where the Deleted Objects container is located
Remove previously delegated permissions	Administrator permissions in the domain where the Deleted Objects container is located
Display security settings for the Deleted Objects container	Read Permissions access to the Deleted Objects container

B.2.2 Syntax for Deleted Objects Utility

`DRADELOBJSUTIL /DOMAIN:`*DOMAINNAME* `[/DC:`*COMPUTERNAME*`] {/DELEGATE:`*ACCOUNTNAME* `| /VERIFY:`*ACCOUNTNAME* `| /REMOVE:`*ACCOUNTNAME* `| /DISPLAY [/RIGHT]}`

B.2.3 Options for Deleted Objects Utility

You can specify the following options:

/DOMAIN:*domain*	Specifies the NETBIOS or DNS name of the domain where the Deleted Objects container is located.
/SERVER:*computername*	Specifies the name or IP address of the domain controller for the specified domain.
/DELEGATE:*accountname*	Delegates permissions to the specified user account or group.
/REMOVE:*accountname*	Removes permissions previously delegated to the specified user account or group
/VERIFY:*accountname*	Verifies permissions of the specified user account or group.
/DISPLAY	Displays security settings for the Deleted Objects container in the specified domain
/RIGHT	Ensures the specified user account or group has the Synchronize directory service data user right. You can use this option to delegate or verify this right. The Synchronize directory service data user right allows the account to read all objects and properties in the Active Directory. For DRA version 6.60 or earlier, this right is optional.

NOTE

- If the name of the user account or group you want to specify contains a space, enclose the account name in quotation marks. For example, if you want to specify the Houston IT group, type "Houston IT".
- When specifying a group, use the pre-Windows 2000 name for that group.

B.2.4 Examples for Deleted Objects Utility

The following examples demonstrate sample commands for common scenarios.

Example 1

To verify that the `MYCOMPANY\JSmith` user account has read permissions on the Deleted Objects container in the `hou.mycompany.com` domain, enter:

```
DRADELOBJSUTIL /DOMAIN:HOU.MYCOMPANY.COM /VERIFY:MYCOMPANY\JSMITH
```

Example 2

To delegate read permissions on the Deleted Objects container in the `MYCOMPANY` domain to the `MYCOMPANY\DraAdmins` group, enter:

```
DRADELOBJSUTIL /DOMAIN:MYCOMPANY /DELEGATE:MYCOMPANY\DRAADMINS
```

Example 3

To delegate read permissions on the Deleted Objects container and the Synchronize directory service data user right in the `MYCOMPANY` domain to the `MYCOMPANY\JSmith` user account, enter:

```
DRADELOBJSUTIL /DOMAIN:MYCOMPANY /DELEGATE:MYCOMPANY\JSMITH /RIGHT
```

Example 4

To display security settings for the Deleted Objects container in the `hou.mycompany.com` domain using the `HQDC` domain controller, enter:

```
DRADELOBJSUTIL /DOMAIN:HOU.MYCOMPANY.COM /DC:HQDC /DISPLAY
```

Example 5

To remove read permissions on the Deleted Objects container in the `MYCOMPANY` domain from the `MYCOMPANY\DraAdmins` group, enter:

```
DRADELOBJSUTIL /DOMAIN:MYCOMPANY /REMOVE:MYCOMPANY\DRAADMINS
```

B.3 Recycle Bin Utility

This utility allows you to enable Recycle Bin support when you are managing a subtree of a domain. If the domain access account does not have permissions on the hidden NetIQRecycleBin container in the specified domain, DRA cannot move deleted accounts to the Recycle Bin. For more information about the Recycle Bin, see Section 12.1, “Understanding the Recycle Bin,” on page 111.

NOTE: After using this utility to enable the Recycle Bin, perform a full accounts cache refresh to ensure the Administration server applies this change. For more information about refreshing the accounts cache, see Section 17.8.4, “Performing a Full Accounts Cache Refresh,” on page 183.

You can use this utility to perform the following tasks:

- Verify that the specified account has read permissions on the NetIQRecycleBin container in the specified domain
- Delegate read permissions to a specified account
- Display security settings for the NetIQRecycleBin container

By default, you can run the Recycle Bin Utility from the `Program Files (x86)\NetIQ\DRA` folder on your Administration server. You can install and run the Recycle Bin Utility on a computer that is not an Administration server. To install this utility, choose custom installation in the setup program. For more information about performing a custom installation, see the *Installation Guide*.

B.3.1 Required Permissions for the Recycle Bin Utility

To use this utility, you must have the following permissions:

If you want to …	You need this permission …
Verify account permissions	Read Permissions access to the NetIQRecycleBin container

Delegate read permissions on the NetIQRecycleBin container	Administrator permissions in the specified domain
Display security settings for the NetIQRecycleBin container	Read Permissions access to the NetIQRecycleBin container

B.3.2 Syntax for Recycle Bin Utility

DRARECYCLEBINUTIL /DOMAIN:*DOMAINNAME* [/DC:*COMPUTERNAME*] {/DELEGATE:*ACCOUNTNAME* | /VERIFY:*ACCOUNTNAME* | /DISPLAY}

B.3.3 Options for Recycle Bin Utility

The following options enable you to configure the Recycle Bin Utility:

/DOMAIN:domain	Specifies the NETBIOS or DNS name of the domain where the Recycle Bin is located.
/SERVER:*computername*	Specifies the name or IP address of the domain controller for the specified domain.
/DELEGATE:*accountname*	Delegates permissions to the specified account.
/VERIFY:*accountnam*e	Verifies permissions of the specified account.
/DISPLAY	Displays security settings for the NetIQRecycleBin container in the specified domain.

B.3.4 Examples for Recycle Bin Utility

The following examples demonstrate sample commands for common scenarios.

Example 1

To verify that the MYCOMPANY\JSmith user account has read permissions on the NetIQRecycleBin container in the hou.mycompany.com domain, enter:

```
DRARECYCLEBINUTIL /DOMAIN:HOU.MYCOMPANY.COM /VERIFY:MYCOMPANY\JSMITH
```

Example 2

To delegate read permissions on the NetIQRecycleBin container in the MYCOMPANY domain to the MYCOMPANY\DraAdmins group, enter:

```
DRARECYCLEBINUTIL /DOMAIN:MYCOMPANY /DELEGATE:MYCOMPANY\DRAADMINS
```

Example 3

To display security settings for the NetIQRecycleBin container in the hou.mycompany.com domain using the HQDC domain controller, enter:

```
DRARECYCLEBINUTIL /DOMAIN:HOU.MYCOMPANY.COM /DC:HQDC /DISPLAY
```

C Custom Powers

You can use the Custom Power Wizard to granularize the delegation model. The Custom Power Wizard supports building specific powers in DRA and ExA.

C.1 Understanding the Custom Powers

The Custom Power Wizard provides a way to quickly create Powers with specific properties matching the actions you want to delegate to roles.

The Custom Powers Wizard uses several conventions to help you build a custom power. The following sections define these conventions and several specific characteristics of the custom power.

During the creation of a new Custom Power in DRA, you have the ability to specify object types, actions, and properties over which you can grant access with the new power. Furthermore, you have the option to select all properties, specific properties, on no properties for the object type the power will be associated with. By default, if you selected Include all object properties you Custom Power will work without incident. If you select Include only listed properties, you should review the list of required, minimum property fields below to make sure the Custom Power will work.

C.2 Custom Power Properties

The following sections list the object types and associated actions that require a minimum set of properties to successfully create a new Custom Power. These are the minimum required properties for each object type in a new Custom Power.

C.2.1 User

The following table lists the action, additional permissions, and required properties of the User object type to show the required properties for the power to work without incident.

Action	Additional permissions	Required Properties
Sets the properties of a user	Disables the user account	`AccountDisabled`
Sets the properties of a user	Enables the user account	`AccountDisabled`

Creates a user	None selected	`givenName`
		`fullName`
		`displayName`
		`sn`
		`samAccountName`
		`userPrincipalName`
		`userPassword`

Action	Additional permissions	Required Properties
Creates a user	Enable email during user creation	givenName fullName displayName sn samAccountName userPrincipalName userPassword homeMDB mailNickName legacyExchangeDN
Creates a user	Add object to groups during user creation	givenName fullName displayName sn samAccountName userPrincipalName userPassword
Creates a user	Create Exchange 2007 or later mailbox for created user account	homeMDB mailNickName givenName fullName displayName sn samAccountName userPrincipalName userPassword

Action	Additional permissions	Required Properties
Clones a user	None selected	cn description displayName FullName givenName name samAccountName sn userPassword userPrincipalName
Clones a user	Enable email for the cloned user	cn description displayName EmailAddress FullName givenName homeMDB legacyExchangeDN mailNickName name samAccountName sn userPassword userPrincipalName

Action	Additional permissions	Required Properties
Clone a user	Create Exchange 2007 or later mailbox for the cloned user	cn description displayName EmailAddress FullName givenName homeMDB legacyExchangeDN mailNickName name samAccountName sn userPassword userPrincipalName

C.2.2 Group

The following table lists the action, additional permissions, and required properties of the Group object type to show the required properties for the power to work without incident.

Action	Additional permissions	Required Properties
Creates a group	None selected	displayName groupType name samAccountName
Creates a group	Enable email for the group you create	displayName groupType name samAccountName legacyExchangeDN mailNickName msExchHideFromAddressLists

Action	Additional permissions	Required Properties
Creates a group	Add the group you create to an ActiveView	displayName groupType name samAccountName
Clones a group	None selected	displayName name samAccountName
Clones a group	Add the group to an ActiveView during group clone	displayName name samAccountName

C.2.3 Dynamic Distribution Group

The following table lists the action, additional permissions, and required properties of the Dynamic Distribution Group object type to show the required properties for the power to work without incident.

Action	Additional permissions	Required Properties
Sets the properties of an Exchange Dynamic Distribution Group	No additional permissions available	
Gets the properties of an Exchange Dynamic Distribution Group	No additional permissions available	
Creates an Exchange Dynamic Distribution Group	No additional permissions available	
Clones an Exchange Dynamic Distribution Group	No additional permissions available	

C.2.4 Computer

The following table lists the action, additional permissions, and required properties of the Computer object type to show the required properties for the power to work without incident.

Action	Additional permissions	Required Properties
Creates a computer in the specified domain	No additional permissions available	AccountDisabled samAccountName $McsAllowPreW2K $McsCanbeJoinedBy

C.2.5 Contact

The following table lists the action, additional permissions, and required properties of the Contact object type to show the required properties for the power to work without incident..

Action	Additional permissions	Required Properties
Creates a contact	No additional permissions available	`givenName` `sn`

Creates a contact	Enable email for the contact you create	`givenName`
		`sn`
		`legacyExchangeDN`
		`mailNickName`

Creates a contact	Add the contact you create to groups	`givenName` `sn`
Clones a contact	No additional permissions available	`givenName` `sn`

C.2.6 Organizational Unit

The following table lists the action, additional permissions, and required properties of the Organizational Unit object type to show the required properties for the power to work without incident.

Action	Additional permissions	Required Properties
Creates an organizational unit	No additional permissions available	`name`
Clones an organizational unit	No additional permissions available	`name`

C.2.7 Published Printer

The following table lists the action, additional permissions, and required properties of the Published Printer object type to show the required properties for the power to work without incident.

Action	Additional permissions	Required Properties
Sets the properties for an ADprinter	No additional permissions available	
Retrieves information about an ADprinter	No additional permissions available	

C.2.8 Resource Mailbox

The following table lists the action, additional permissions, and required properties of the resource mailbox object type to show the required properties for the power to work without incident.

Action	Additional permissions	Required Properties
Updates a resource mailbox	No additional permissions available	
Gets the properties for a resource mailbox	No additional permissions available	
Creates a resource mailbox	Create resource mailbox for created user account	
Copy a resource mailbox	No additional permissions available	

D Ports and Protocols Used in DRA Communications

DRA and ExA use the following ports and protocols for communication.

Communication path	Protocol and port	Use
DRA primary Administration server to secondary servers	DCOM 135	End-point mapper, a basic requirement for DRA communication; allows Administration servers to locate each other in an MMS
	DCOM 445	Delegation model replication; file replication during MMS synchronization
	LDAP 50000	Attribute replication and DRA server-ADAM communication. This port number can be configured during installation.
	LDAP 50001	SSL attribute replication (ADAM) (if enabled). This port number can be configured during installation.
DRA secondary servers to primary Administration server	DCOM 135	End-point mapper, a basic requirement for DRA communication
	DCOM 445	Delegation model replication (disabled, but performed on service start); file replication during MMS synchronization
	LDAP 50000	Attribute replication and DRA server-ADAM communication. This port number can be configured during installation.
	LDAP 50001	SSL attribute replication (ADAM) (if enabled). This port number can be configured during installation.
	RPC all ports from 1024-65535 as served by the DCOM server	DCOM Service communication

Communication path	Protocol and port	Use
between DRA secondary Administration servers	LDAP 50000	Attribute replication and DRA server-ADAM communication. This port number can be configured during installation.
	LDAP 50001	SSL attribute replication (ADAM) (if enabled). This port number can be configured during installation.
DRA to domain controllers	LDAP 389	Active Directory object management
	Port 53	Name resolution
	Kerberos Port 88	Allows authentication from the DRA server to the domain controllers
DRA to and from 32-bit clients	DCOM 135	End-point mapper, a basic requirement for DRA communication
DRA to and from DRA Web service	DCOM 135	End-point mapper, a basic requirement for DRA communication
	RPC all ports from 1024-65535 as served by the DCOM server	DCOM Service communication
DRA Web service to and from DRA Web Console	HTTP SSL 443	Web client access
DRA clients to NetIQ DRA Core Service	TCP 50101	Communication between DRA Client and NetIQ DRA Core Service and also between NetIQ DRA Core Service components in an MMS. Used for generating a UI Report from DRA Client. This port number can be configured during installation.
DRA to Log Archive Server	TCP 1801	Log archive communication using Microsoft Message Queueing (MSMQ)
	TCP 50102	Log archive communication. You can configure this port using the Log Archive Configuration wizard.
DRA to SQL Server	TCP 1433	Database setup and configuration; XML check-in
	UDP 1434	If using a SQL Server instance, the browser service uses UDP 1434 to identify the port for the named instance.

Communication path	Protocol and port	Use
DRA to the Exchange Server	LDAP 389	Mailbox management
	TCP 80	Needed for all on-premise Exchange Servers 2007 through 2013.
DRA to Exchange Online	TCP 80	Remote PowerShell access
	HTTP SSL 443	Graph API access
DRA Cache Service	Any TCP port between 50000 and 66535. The default port is TCP 50103.	Cache service communication on the DRA server (does not need to be opened through the firewall)
REST Service	The default REST Service port is 8755. The default DRA Host Service port is 11192.	These ports can be changed by the user; however, the new ports must be open to allow clients to connect to them.

E The Pre-DRA 9.0.1 Web Console

The pre-DRA 9.0.1 Web Console is still available for use. Consult the *NetIQ Directory and Resource Administrator and Exchange Administrator Installation Guide* for information about installing this version of the Web Console.

The Web Console is a Web-based user interface that provides quick and easy access to many user account, group, computer, resource, and Microsoft Exchange mailbox tasks. You can also manage general properties of your own user account, such as the street address or cell phone number.

The Web Console is easy to learn and simple to use, which makes it a great tool for occasional or beginning administrators. The Web Console provides step-by-step help as it guides you through each task. When you complete a task, it displays links to other related tasks, so you can quickly address an entire workflow. The Web Console displays a task only if you have the power to perform that task.

E.1 Starting the Web Console

You can start the Web Console from any computer running Internet Explorer. To start the Web Console, specify the appropriate URL in your Web browser address field or use the link provided in the Account and Resource Management console. For example, if you installed the Web component on the HOUserver computer, type `http://HOUserver/dra` in the address field of your Web browser.

NOTE: To display the most current account and Microsoft Exchange information in the Web Console, set your Web browser to check for newer versions of cached pages at every visit.

You can also start the Web Console from the DRA program group, and from the File menu in the Account and Resource Management console and the Delegation and Configuration console.

E.2 Using Quick Start to Solve Issues

Quick Start allows you to quickly and easily resolve account issues. You can view vital statistics and properties for a specific user account, computer, or group. You can then link to the appropriate task, such as resetting the password for a user account, which addresses your problem.

E.3 Customizing the Web Console

You can quickly and easily customize the Web Console in the following ways:

Modify provided tasks

For example, you can modify the update user's properties task to include a new field that manages a proprietary setting. You can hide specific tasks you do not want Assistant Admins (AAs) to use regardless of their delegated powers. You can also publish reports generated from Directory and Resource Reporting.

Develop new tasks

For example, you can develop a new update user's properties task that meets your unique administration needs. You can replace provided tasks with custom tasks without losing built-in functionality.

Modify workflows

For example, you can modify the Web Console framework and navigation, changing how AAs step through a given task. This flexibility allows you to add, remove, or move steps to create the exact solution you require.

Deploy multiple Web Console applications

You can install and configure multiple Web Console applications. For example, you can deploy one custom Web Console application for your Houston facility and another custom Web Console application for your Atlanta facility. Each application can support a unique set of tasks that meet the specific needs of your facility. For more information, see the Deploying DRA in Unique Environments Technical Reference. For more information about customizing the Web Console, see the Directory and Resource Administrator Software Development Kit.