

User Guide

NetIQ® Domain Migration Administrator™

May 2012



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.

© 2012 NetIQ Corporation and its affiliates. All Rights Reserved.

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	xiii
Conventions	xiv
About NetIQ Corporation	xv

Chapter 1

Introduction	1
What Is Domain Migration Administrator?	1
Premigration Modeling and Impact Analysis	2
Custom Migrations Using ActiveScript Triggers	2
Support for Multiple Operating Systems	2
Support for NetApp Filers	3
Scheduling Domain Migration through the CLI	3
What Is Server Consolidator?	3
Server Consolidation Analysis and Testing	4
Scheduling Server Consolidation through the CLI	4
How These Products Help Your Company	4
Reduces Total Cost of Migration	4
Models and Simulates Migrations	5
Open and Customizable	5
How These Products Help You	6
Simplifies Assessment and Preparation	6
Eases the Transition	6
Project-Based, Controlled Migration	7

Chapter 2

Planning and Performing Your Migration 9

Identifying Your Migration Scenario	10
Migration Checklist	11
Understanding Access and Security Issues	18
Translating Security to Reflect the New SID	19
Using SID History to Maintain Permissions	19
Migrating Well-Known Accounts	20
Understanding Built-in Accounts	21
Copying Local Group Memberships and Domain Controller Security Policy	22
Assessing Your Existing Environment	22
Designing Your New Environment	23
Preparing Your Environment	24
Considering Enterprise Environment Issues	25
Getting Production Data into Your Test Lab	27
Preparing for Recovery and Fault Tolerance	28
Preparing Your Source Domains	29
Preparing to Migrate with SID History	30
Setting Up a Clean Domain	34
Preparing an Existing Target Domain	36
Verifying Name Resolution Services	37
Testing Secure Channel Communication	38
Establishing a Two-Way Trust	38
Establishing Migration Credentials	39
Reviewing Password Policies	42
Considering Other Applications	45
Developing a Migration Plan	45
Determining the Scope of Your Migration	46
Developing a Migration Workflow	48
Planning for Microsoft Exchange	57
Running Migration Tests and Verifying Results	57
Establishing a Migration Time Line	58

Using the Product Most Effectively	59
Using Individual Tasks or Projects	59
Customizing Your Migration Results	61
Notifying Users about Migrating	62
Migrating Objects and Verifying Results	64
Using the Migration Logs	65
Adjusting Agent Error Logging Levels	67
Adjusting Server Consolidator Logging Levels	68

Chapter 3

Installing Domain Migration Administrator and Server Consolidator **69**

Domain Migration Administrator Requirements	69
Computers Running Domain Migration Administrator	70
Database Requirements	71
Computers Running Agents	72
General Requirements	73
Target-Specific Requirements	74
Using SID History Features	74
Permission Requirements for Domain Migration Administrator	74
Firewall Considerations for Domain Migration Administrator	76
Objects that Domain Migration Administrator Migrates	76
Understanding Naming Limitations	77
Server Consolidator Requirements	78
Hardware Requirements for Server Consolidator	78
Software Requirements for Server Consolidator	79
Permission Requirements for Server Consolidator	79
Licensing Considerations	79
Using a Trial License	80
Viewing Your License Information	80
Upgrading Your License	80

Upgrading Domain Migration Administrator and Server Consolidator	81
Installing Domain Migration Administrator and Server Consolidator	81
Installing Agents Separately	83

Chapter 4

Consolidating Servers	85
Best Practices for a Smooth Consolidation	86
Starting Server Consolidator	86
Understanding the Server Consolidator Interface	86
Server Consolidator Task Pad	86
Server Consolidator Wizards	87
Performing Consolidation Tasks	87
Consolidating Files, Folders, and Shares	88
Preparing for NetApp Filer Consolidation	88
Disk Mirroring Using Server Consolidator	89
Copying Files, Folders, and Shares to Cluster Servers	90
Consolidating Printers	91
Consolidating Local Groups	92
Translating Security and Access Settings	93
Generating Server Consolidator Reports	93
Using the CLI for Server Consolidator	94

Chapter 5

Migrating with Projects	95
Starting Domain Migration Administrator	96
Understanding the Domain Migration Administrator Interface	96
Domain Migration Administrator Task Pads	96
Project Task Pad	97
Domain Migration Administrator Wizards	98

Customizing the Project-Based Interface	98
Modifying How Wizards Display Accounts	99
Modifying which Accounts Wizards Display	99
Modifying Advanced Domain Migration Administrator Options	100
Performing Project Tasks	101
Selecting Objects by Importing a CSV File	101
Defining a Migration Project	102
Modifying a Migration Project	105
Refreshing Project Data	105
Performing the Migration Defined in a Project	106
Synchronizing Migrated Objects	107
Deleting a Migration Project	107
Undoing User Account Migrations in Projects	108
Using Reports	108

Chapter 6

Delegating Migration Tasks	111
Understanding the Delegation Interface	111
Delegation Task Pad	112
Delegation Wizards	113
Understanding Project Delegation	113
Performing Delegation Tasks	114
Creating Delegated Migration Projects	114
Exporting a Migration Project	116
Importing a Migration Project	117

Chapter 7

Performing Individual Migration Tasks	119
Understanding the Task-Based Interface	119
Task-Based Task Pad	119
Individual Task Wizards	120
Customizing the Task-Based Interface	120

Performing Individual Tasks	121
Generating and Viewing Reports	121
Migrating Trusts	121
Setting Service Account Migration Options	122
Mapping and Merging Groups	122
Migrating User Accounts	123
Migrating Groups	124
Renaming Computers	124
Migrating Computer Accounts	125
Importing Objects for Post-Migration Tasks	125
Translating Security Access and Profiles	127
Synchronizing Passwords in Two Domains	127
Translating Security for Accounts with SID History	128
Removing SID History Values	129
Translating Security for NetApp Filers	129
Updating ADC Accounts	130
Retrying Failed Migration Tasks	132
Undoing Individual Migration Tasks	132

Chapter 8

Understanding Reporting	133
Special Reports	134
Understanding the Reporting Interface	135
Global and Project-Focused Reports	135
Generating and Viewing One Report	137
No Data to Report	138
Performing Reporting Tasks	138
Generating and Updating Reports	138
Viewing Reports	139
Navigating Reports	140

Chapter 9	
Customizing the Migration Process	141
Using Scripting	141
Scripting Objects	142
Event Triggers	142
Example Script: Populating Active Directory from a Data Source	143
Using Data Modeling	144
Understanding the Data Modeling Interface	145
Importing the Domain Migration Administrator Data	146
Changing the Properties of a Target Account	147
Changing the Target OU for an Account	148
Scheduling Your Migration with the CLI	149
Appendix A	
Using the Command-Line Interface	151
Using the Domain Migration Administrator Command-Line Interface	151
Using the Server Consolidator CLI	154
Appendix B	
Detailed Permission Requirements	157
Domain Migration Administrator Minimum Permissions	157
Understanding Agent Permissions	158
Permission Requirements for Specific Tasks	159
Server Consolidator Minimum Permissions	173
Copying Files, Folders, and Shares	174
Copying Printers	174
Migrating Local Groups	175
Translating Security for Local Groups	175

Appendix C

Understanding How Domain Migration Administrator Works	177
Understanding the Domain Migration Administrator Architecture	177
Console Computer	178
Microsoft SQL Server Databases	178
Agents	178
How Domain Migration Administrator Migrates User Accounts and Groups	181
Copy Versus Move	181
Collision Handling	182
Truncation of Long Names	183
Group Membership	184
Increasing Migration Efficiency	186
Intraforest Migrations	187
Passwords and Related Properties	188
SID History	189
Primary Group	189
User Principal Name (UPN)	190
Domain Controller Security Policy	190
Roaming Profiles	191
Remote Users	192
Previously Migrated Objects	193
Accounts Migrated with Tools Similar to ADC	194
How Domain Migration Administrator Migrates and Renames Computers	194
How Domain Migration Administrator Migrates Service Accounts	195
How Domain Migration Administrator Refreshes Project Data	197
How Domain Migration Administrator Synchronizes Objects	197
How Domain Migration Administrator Migrates Trusts	198
How Domain Migration Administrator Merges and Maps Groups	199

How Domain Migration Administrator Updates Access Control Entries	200
Files and Folders	201
Local Groups	201
Local User Profile	201
Registry	203
Domain Controller Security Policy	203
Default Logon Domain	204
NetApp Filers	204
How Domain Migration Administrator Handles SID History	204
Understanding SID History	205
Understanding the Migration Process and SID History	206
SID History Values	206
SID History Report and Other Migration Tools	207
Methods for Translating Security	208
Additional SID History Considerations	208
How Domain Migration Administrator Synchronizes Passwords	209
How Domain Migration Administrator Changes Domain Affiliation	210
How Domain Migration Administrator Handles Test Mode	212
How Domain Migration Administrator Handles Data Modeling	213
Renaming Objects	214
OU Structure	214
Common Name (CN)	214
How Domain Migration Administrator Handles the Undo Function	215
Appendix D	
Understanding How Server Consolidator Works	217
Understanding the Server Consolidator Architecture	217
How Server Consolidator Handles Files, Folders, and Shares	218
Consolidating Files and Folders	218
Consolidating Shares	219

How Server Consolidator Handles Cluster Servers	220
Cluster Server Requirements	220
Cluster Server Terminology	221
Cluster Information	222
Cluster Resources	222
Why Cluster Server Copies Can Fail	223
How Server Consolidator Handles Printers	224
How Server Consolidator Handles Local Groups	225

Appendix E

Understanding the Domain Migration Administrator Databases	227
Locating the Databases	228
Protar Database	228
Project Databases	229
Creating and Deleting Project Databases	229
Tables in the Protar Database	229
Settings Table	230
Action History Table	230
Migrated Objects Table	231
Security Translation Table	233
Projects Table	234

Appendix F

Native-Mode Source Domain Password Migration	235
Creating a Password Export Server Encryption Key File	236
Installing Password Export Server (PES)	236
Configuring Permissions and Group Policy for Password Migration	239

About This Book and the Library

The *User Guide* provides conceptual and usage information about the NetIQ Domain Migration Administrator (Domain Migration Administrator) and NetIQ Server Consolidator (Server Consolidator) products. This book defines terminology and various related concepts. This book also guides you through the installation process.

Intended Audience

This book provides information for individuals responsible for installing, understanding, and using Domain Migration Administrator to migrate Microsoft Windows computers.

Other Information in the Library

The library provides the following information resources:

User Guide

Provides conceptual information about Domain Migration Administrator and Server Consolidator. This book also provides an overview of the user interfaces and step-by-step guidance for many administration tasks.

Help

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

Conventions

The library uses consistent conventions to help you identify items throughout the documentation. The following table summarizes these conventions.

Convention	Use
Bold	<ul style="list-style-type: none">• Window and menu items• Technical terms, when introduced
<i>Italics</i>	<ul style="list-style-type: none">• Book and CD-ROM titles• Variable names and values• Emphasized words
Fixed Font	<ul style="list-style-type: none">• File and folder names• Commands and code examples• Text you must type• Text (output) displayed in the command-line interface
Brackets, such as [<i>val ue</i>]	<ul style="list-style-type: none">• Optional parameters of a command
Braces, such as { <i>val ue</i> }	<ul style="list-style-type: none">• Required parameters of a command
Logical OR, such as <i>val ue1</i> <i>val ue2</i>	<ul style="list-style-type: none">• Exclusive parameters. Choose one parameter.

About NetIQ Corporation

NetIQ, an Attachmate business, is a global leader in systems and security management. With more than 12,000 customers in over 60 countries, NetIQ solutions maximize technology investments and enable IT process improvements to achieve measurable cost savings. The company's portfolio includes award-winning management products for IT Process Automation, Systems Management, Security Management, Configuration Audit and Control, Enterprise Administration, and Unified Communications Management. For more information, please visit www.netiq.com.

Contacting Sales Support

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

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

Contacting Technical Support

For specific product issues, please 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. If you have suggestions for improvements, please email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

Qmunity, 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, Qmunity helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, please visit <http://community.netiq.com>.

Chapter 1

Introduction

Domain migration tasks can be complicated and require a lot of time. These time requirements can escalate when you perform migration tasks on an enterprise scale. For example, consider the complexity and time requirements of the following tasks:

- Simplifying your Microsoft Windows domain structure for day-to-day operations
- Preparing your Microsoft Windows domain structure to consolidate multiple domains into a single domain
- Converting from one platform to another
- Moving files, folders, and shares from one server to another server
- Consolidating file servers to new higher capacity computers

What Is Domain Migration Administrator?

The NetIQ Domain Migration Administrator product (Domain Migration Administrator) allows you to quickly migrate Microsoft Windows domains. The product addresses several aspects of the migration process, including domain migration and consolidation.

Domain Migration Administrator uses state of the art technology to enable you to copy user accounts, groups, and computer accounts to another domain. Using this product, you can then resolve the related file, folder, share, and printer security issues for the copied user accounts, groups, and computer accounts. Domain Migration Administrator provides the features you need to create a more secure, productive, and manageable environment.

Premigration Modeling and Impact Analysis

Domain Migration Administrator provides a preview evaluation feature that lets you model your selections for migrating one domain to another domain. Before you perform the migration, you can review the changes, evaluate the impact, and clean up your source objects if necessary. You can adjust your selections numerous times to get the best fit based on your network structure and needs. This evaluation feature helps prevent and clean up data pollution as you migrate domains.

Custom Migrations Using ActiveScript Triggers

You can create scripts and customize the migration process for your specific needs. Triggers allow you to run scripts as part of the migration process, giving you complete control and flexibility. This product provides intrinsic objects that allow you to access ADSI objects and settings.

Support for Multiple Operating Systems

Domain Migration Administrator supports migration to the following domains:

- Microsoft Windows 2000 mixed mode
- Microsoft Windows 2000 native mode
- Microsoft Windows 2003 mixed mode
- Microsoft Windows 2003 native mode
- Microsoft Windows 2008 mixed mode
- Microsoft Windows 2008 native mode

Support for NetApp Filers

Domain Migration Administrator can translate security on NetApp filers. This process resolves security-related issues after you migrate user accounts and groups. Domain Migration Administrator uses network drive mappings to access the file system on NetApp filers, and translates security on NetApp folders, files, and shares that are in NTFS mode.

Scheduling Domain Migration through the CLI

You can use the command-line interface and the Microsoft Windows scheduler to schedule various Domain Migration Administrator activities. This capability allows you to collect information and make changes at times that are convenient for you. You can also test a migration project, and then schedule the migration to be performed at a later time.

What Is Server Consolidator?

The NetIQ Server Consolidator product (Server Consolidator) allows you to:

- Copy files, folders, and shares from one server to another
- Copy the access permissions for each object
- Migrate computer local groups from one server to another
- Move printers and printer settings from one server to another

These powerful features allow you to centralize resources on a central server, such as a cluster server. Using the ActiveAgent technology, Server Consolidator handles the copying process in the most efficient way. Server Consolidator is installed automatically with Domain Migration Administrator.

Server Consolidation Analysis and Testing

Server Consolidator allows you to test a consolidation task before you actually make the changes. You can ensure the target system has sufficient disk space before performing the consolidation task.

Scheduling Server Consolidation through the CLI

You can use the command-line interface and the Microsoft Windows scheduler to schedule Server Consolidator functions. This capability allows you to collect information and make changes at times that are convenient for you. You can also test a consolidation task, and then schedule that task to be performed at a later time.

How These Products Help Your Company

Planning and testing the migration process is one of the challenges enterprise planners face today. The following sections highlight how Domain Migration Administrator and Server Consolidator can help your company address these challenges.

Reduces Total Cost of Migration

You can use Domain Migration Administrator and Server Consolidator to help simplify your existing enterprise domain structure and reduce costs. Consolidating from many domains to a few domains, even if you do not yet migrate to a later operating system version, can produce a streamlined network model that is easier to maintain. Simpler operation means cost savings.

Easy to install, implement, and use, Domain Migration Administrator and Server Consolidator provide an immediate return on your investment. You can install Domain Migration Administrator and Server Consolidator in a few minutes and use them to help plan your migration project in a few hours. Using fast, parallel automation techniques, Domain Migration Administrator can quickly cleanse, move, and populate hundreds of accounts. With intuitive, task-based interfaces, these products save time, reduce the cost of planning a migration, and reduce the cost of implementing the plan.

Models and Simulates Migrations

Because you can preview several migration solutions before you commit to one approach, Domain Migration Administrator helps you determine the best migration approach for your enterprise. You can troubleshoot the migration process, anticipate problems, and find solutions before you perform the migration.

Letting you solve the problems using a *what if* technique allows migrations to go more smoothly and results in less downtime for your enterprise. Every hour users are disconnected from the network results in lost productivity. Domain Migration Administrator helps you avoid downtime in a variety of ways:

- Plan the migration and do a trial run. You can view reports of the trial migration to see if problems occur. Domain Migration Administrator lets you plan and test the migration process without disrupting network use.
- Create a project that includes a subset of the user accounts and groups you want to migrate and test the plan. If you experience problems, you can resolve them before you migrate the remaining user accounts and groups.
- Translate and resolve related security issues using automated wizards to ensure that files, accounts, folders, and shares refer to the proper security descriptors in the target domain.

When your planning is complete, Domain Migration Administrator allows you to quickly complete the migration tasks. Your staff do not have to work extended hours and users experience very little impact. Planning, testing, and migrating quickly saves wear and tear on personnel and gets the enterprise up and running in the new environment.

Open and Customizable

Your organization may have unique needs that other products cannot meet. Domain Migration Administrator offers open, scriptable interfaces that let you create scripts to handle your unique needs, and easily integrate them in the migration process. Using standard scripting languages and the sample scripts provided with Domain Migration Administrator, you can quickly customize the migration process to meet your specific migration needs.

How These Products Help You

NetIQ Corporation offers award-winning solutions that help you assess, automate, and consolidate no matter what your migration goals are. These products provide detailed reports that allow you to quickly evaluate the state of your migration during the planning phase, as well as after the migration is underway. The following sections describe a few of the ways Domain Migration Administrator and the Server Consolidator utility help you perform effective migrations.

Simplifies Assessment and Preparation

Domain Migration Administrator uses ActiveAgent technology to collect and consolidate information about your network computers. This technology lets you run Domain Migration Administrator from a central location so you do not need to visit each computer in the enterprise to collect information for your migration plan. ActiveAgent technology automates the discovery and assessment of users, groups, and computer resources, which in turn speeds and simplifies the planning and preparation stages of migrating.

Running Domain Migration Administrator from a central location can save you and your staff footwork and time. Domain Migration Administrator agents locate the computers in the source domain and collect the required security information. Domain Migration Administrator also prepares reports to help you analyze the information you collect and put the information to best use.

Eases the Transition

Domain Migration Administrator reporting and modeling tools help you analyze your needs, perform a trial migration, and evaluate the potential results of the migration. You can review the results, identify potential issues, and resolve those issues. Then, you can modify your migration strategy and run the test migration again before performing the actual migration.

Because you can address potential problems before you migrate, you save valuable time. You do not need to perform time-consuming clean up after the migration. This iterative *analyze-and-model* approach lets you test your migration process and makes sure the process produces the results you want before you commit to making the migration changes.

Project-Based, Controlled Migration

Domain Migration Administrator reduces the risks of migration errors by providing project-based tracking and robust rollback support. Domain Migration Administrator projects let you track the step-by-step progress of your migration. Rollback (undo) support helps you recover from issues discovered during or after the migration process. If you are not satisfied with the results when you migrate user accounts, groups, or computers, you can undo those changes. You can also rollback security translation changes. Complete reporting lets you evaluate progress each step of the way.

Chapter 2

Planning and Performing Your Migration

Companies often discover they have too many domains, or their domains are not optimally configured. You may need to change your domain configuration for several reasons:

- You need to integrate domains created in individual offices or acquired through mergers and acquisitions.
- You can simplify your domain configuration because NetIQ Administration products, such as Directory and Resource Administrator, eliminate many multiple domain requirements.
- You need to migrate from one operating system to another.

Domain Migration Administrator simplifies the reconfiguration of your distributed Microsoft Windows account definitions. Domain Migration Administrator allows you to copy user accounts, groups, and computer accounts to another domain. The product also allows you to resolve the related file, folder, share, and printer security access issues for the copied accounts. Domain Migration Administrator provides a comprehensive set of tools that allow you to analyze the migration impact both before and after the actual migration process.

As with other complex processes, it is important to break the project into a number of components and then divide each component into a list of discrete tasks. Good project management, organization, and communication skills are as important as technical skills because migrations cross multiple technical and political boundaries and affect the entire end-user community.

Although there are many variations of migration scenarios, each scenario involves migrating an account domain and the resource domains. Domain Migration Administrator and Server Consolidator provide support for the tasks required to successfully complete these migration phases.

Identifying Your Migration Scenario

Domain Migration Administrator supports the following source and target domain migration configurations.

Source	Target
Microsoft Windows 2000 Server	Any of the following: <ul style="list-style-type: none"> • Microsoft Windows 2000 Server • Microsoft Windows Server 2003 • Microsoft Windows Server 2008 • Microsoft Windows Server 2008 R2
Microsoft Windows Server 2003	Any of the following: <ul style="list-style-type: none"> • Microsoft Windows Server 2003 • Microsoft Windows Server 2008 • Microsoft Windows Server 2008 R2
Microsoft Windows Server 2008	Either of the following: <ul style="list-style-type: none"> • Microsoft Windows Server 2008 • Microsoft Windows Server 2008 R2
Microsoft Windows Server 2008 R2 (intraforest only)	Microsoft Windows Server 2008 R2 (intraforest only)

Note

The support matrix above lists supported Windows versions for domain controllers in the domain. However, Domain Migration Administrator also supports migrations of desktop computers running Windows XP, Windows Vista, or Windows 7 (32-bit or 64-bit).

Most scenarios follow the same workflow. You should understand how each migration scenario is handled to ensure your migration process is complete. For more information, see “Understanding How Domain Migration Administrator Works” on page 177.

In most scenarios, you can migrate over time and users can log on to the source or target domain during the transition. However, when performing an *intraforest* migration, Domain Migration Administrator moves the account to the target domain rather than copying the source account. In this case, Domain Migration Administrator creates a new account in the target domain, updates the SID History property of the new account with the SID of the source account, and then deletes the source account. Therefore, users must log on to the target domain once you migrate their user accounts. If you perform an *intraforest* migration, some steps in the checklist do not apply.

Migration Checklist

This checklist outlines the important phases of your migration and helps you consider the related issues. The checklist applies to many environments and provides a starting point for your migration. Use this checklist as a guide and be sure to customize this checklist to address the specific issues associated with your environment. Keep the following items in mind when using the checklist:

Specifics for your environment

Your environment may include hardware, software, and network structure issues that are not directly addressed in the checklist. You should enhance the checklist to address all the components and issues of your specific environment.

Microsoft Windows knowledge

Some tasks related to domain migration require you to be familiar with common administration tools for installing, configuring, and controlling services and policies. Become familiar with the Microsoft Windows features, technology, and design considerations before you start the migration planning process. For more information, see the Microsoft documentation.

Consulting services

Consider using migration consultants to save time and money in your planning and migration stages.

<input checked="" type="checkbox"/>	Pre-Migration Planning and Assessment
<input type="checkbox"/>	1. Identify the business and technical goals for your migration. These goals should include costs, training, security, manageability, and availability.
<input type="checkbox"/>	2. Assemble a migration team that includes a project manager, TCP/IP network planner, DNS/WINS name resolution support team, security planners, email and messaging team, LAN and WAN experts, Active Directory experts, help desk and training personnel, and facilities planners. Your team should include members from all your business locations.
<input type="checkbox"/>	3. Review the access issues related to the migration process, such as SIDs and SID History, local groups, well-known accounts, and built-in accounts. For more information, see “Understanding Access and Security Issues” on page 18.
<input type="checkbox"/>	4. Assess your current environment. For more information, see “Assessing Your Existing Environment” on page 22.
<input type="checkbox"/>	5. Design the structure for your new environment. For more information, see “Designing Your New Environment” on page 23.
<input type="checkbox"/>	6. Design your test lab, which should closely emulate the components and scale of your production environment. Include complex components, such as WAN links, remote or intermittently-connected computers, and cluster servers. Review enterprise design and migration performance issues to correctly design your test lab. For more information, see “Considering Enterprise Environment Issues” on page 25, as well as the Test Lab Preparation portion of this checklist.

<input checked="" type="checkbox"/>	Pre-Migration Planning and Assessment
<input type="checkbox"/>	7. Develop a plan for which domains to migrate and in what order. Plan to migrate your account domains first. Then, migrate your resource domains. You can consolidate your resource domains during the migration process.
<input type="checkbox"/>	8. Obtain management support for the project and prepare a preliminary migration budget that includes funding your test lab. Based on testing, you can develop a detailed schedule and a documented migration process for later approval.
<input checked="" type="checkbox"/>	Test Lab Preparation
<input type="checkbox"/>	1. Ensure your test lab is physically separate from your production network.
<input type="checkbox"/>	2. Copy your production environment data, such as user account, group, and computer account information into your test lab. For more information, see “Getting Production Data into Your Test Lab” on page 27.
<input type="checkbox"/>	3. Prepare your source domains. For more information, see “Preparing Your Source Domains” on page 29.
<input type="checkbox"/>	4. Prepare other computers in your source domains to ensure they meet the requirements for the Domain Migration Administrator agent. For more information, see “Computers Running Agents” on page 72.
<input type="checkbox"/>	5. Prepare the target domain. For more information, see “Setting Up a Clean Domain” on page 34 and “Preparing an Existing Target Domain” on page 36.
<input type="checkbox"/>	6. Verify name resolution services for the source and target domains. For more information, see “Verifying Name Resolution Services” on page 37.
<input type="checkbox"/>	7. For all scenarios other than intraforest migrations: Establish a two-way trust between the source and target domain. For more information, see “Establishing a Two-Way Trust” on page 38.
<input type="checkbox"/>	8. For all scenarios other than intraforest migrations: Test the secure channel communication between the source and target domain. For more information, see “Testing Secure Channel Communication” on page 38.

<input checked="" type="checkbox"/>	Test Lab Preparation
<input type="checkbox"/>	9. Define the accounts you need with the appropriate permissions to perform the various migration tasks. For more information, see “Establishing Migration Credentials” on page 39.
<input type="checkbox"/>	10. For all scenarios other than intraforest migrations: Adjust the password policy in the target domain to ensure Domain Migration Administrator can create user accounts and set passwords. For more information, see “Reviewing Password Policies” on page 42.
<input type="checkbox"/>	11. Install Domain Migration Administrator and Server Consolidator in the target domain. For all scenarios other than intraforest migrations: If you will migrate with SID History, install the product on a domain controller in the target domain or on a Microsoft Windows computer in the target domain. For more information, see “Installing Domain Migration Administrator and Server Consolidator” on page 81.
<input type="checkbox"/>	12. Check the NetIQ Web site and install any hotfixes and service packs.
<input type="checkbox"/>	13. For all scenarios other than intraforest migrations: Start Domain Migration Administrator and migrate the source domain trusts to the target domain. The target domain should trust all domains trusted by the source domain. All domains that trust the source domain should also trust the target domain. For more information, see “Migrating Trusts” on page 121.
<input type="checkbox"/>	14. Install the other software you need in the target domain. For more information, see “Considering Other Applications” on page 45.

<input checked="" type="checkbox"/>	Migration Plan Development and Testing
<input type="checkbox"/>	1. Define the scope of your migration. Identify what you need to migrate and the potential issues. For more information, see “Developing a Migration Plan” on page 45 and “Determining the Scope of Your Migration” on page 46.
<input type="checkbox"/>	2. Become familiar with Domain Migration Administrator by defining a project and migrating a few user accounts or groups in your lab. Verify the results of your migration to ensure you understand the various options. For more information, see “Migrating with Projects” on page 95.
<input type="checkbox"/>	3. Review how Domain Migration Administrator migrates various object types and develop a workflow that addresses all the objects you need to migrate. For more information, see “Developing a Migration Workflow” on page 48.
<input type="checkbox"/>	4. Test your proposed workflow in the test lab and verify the results. Adjust your plan to address any issues you identify. For more information, see “Running Migration Tests and Verifying Results” on page 57.
<input type="checkbox"/>	5. Estimate your migration time line and develop a migration schedule. For more information, see “Establishing a Migration Time Line” on page 58.
<input type="checkbox"/>	6. Publish your plan and get the appropriate approval. Be sure to communicate throughout the migration to help users understand the migration purpose and process.
<input checked="" type="checkbox"/>	Production Environment Preparation
<input type="checkbox"/>	1. Prepare a recovery method in case you experience problems during your migration. For more information, see “Preparing for Recovery and Fault Tolerance” on page 28.
<input type="checkbox"/>	2. Prepare your source domains. For more information, see “Preparing Your Source Domains” on page 29.

<input checked="" type="checkbox"/>	Production Environment Preparation
<input type="checkbox"/>	3. Prepare other computers in your source domains to ensure they meet the requirements for the Domain Migration Administrator agent. For more information, see “Computers Running Agents” on page 72.
<input type="checkbox"/>	4. Prepare the target domain. For more information, see “Setting Up a Clean Domain” on page 34 and “Preparing an Existing Target Domain” on page 36.
<input type="checkbox"/>	5. Verify name resolution services for the source and target domains. For more information, see “Verifying Name Resolution Services” on page 37.
<input type="checkbox"/>	6. For all scenarios other than intraforest migrations: Establish a two-way trust between the source and target domain. For more information, see “Establishing a Two-Way Trust” on page 38.
<input type="checkbox"/>	7. For all scenarios other than intraforest migrations: Test the secure channel communication between the source and target domain. For more information, see “Testing Secure Channel Communication” on page 38.
<input type="checkbox"/>	8. Define the accounts you need, with the appropriate permissions, to perform the various migration tasks. For more information, see “Establishing Migration Credentials” on page 39.
<input type="checkbox"/>	9. For all scenarios other than intraforest migrations: Adjust the password policy in the target domain to ensure Domain Migration Administrator can create user accounts and set passwords. For more information, see “Reviewing Password Policies” on page 42.
<input type="checkbox"/>	10. Install Domain Migration Administrator and Server Consolidator in the target domain. For all scenarios other than intraforest migrations: If you will migrate with SID History, install Domain Migration Administrator on a domain controller or other supported Windows computer in the target domain. For more information, see “Installing Domain Migration Administrator and Server Consolidator” on page 81.
<input type="checkbox"/>	11. Check the NetIQ Web site and install any hotfixes and service packs.

<input checked="" type="checkbox"/>	Production Environment Preparation
<input type="checkbox"/>	12. For all scenarios other than intraforest migrations: Start Domain Migration Administrator and migrate the source domain trusts to the target domain. The target domain should trust all domains trusted by the source domain. All domains that trust the source domain should also trust the target domain. For more information, see “Migrating Trusts” on page 121.
<input type="checkbox"/>	13. Install the other software you need in the target domain. For more information, see “Considering Other Applications” on page 45.
<input checked="" type="checkbox"/>	Migration Plan Implementation
<input type="checkbox"/>	<p>1. Select a pilot group of user accounts and groups to migrate. Notify the affected users and define the migration schedule for them. For more information, see “Notifying Users about Migrating” on page 62.</p> <p>For intraforest migrations: Use a set of user accounts and groups that are complete. All user accounts that are members of the groups should be included in the pilot group of user accounts and groups to migrate.</p>
<input type="checkbox"/>	2. Define a project that contains the objects in your pilot group. Migrating IT groups first can help you work through your migration process and any potential issues with a more understanding set of users.
<input type="checkbox"/>	3. Define any customizations you need for your migration process, such as scripts, database modeling, and migration options specified in the project.
<input type="checkbox"/>	4. Run the Domain Status reports as identified in your workflow. For example, the Name Conflicts report helps you identify potential naming conflicts for the objects in the project. Resolve these conflicts and define the migration options as needed. For more information about special reports in this category, see “Special Reports” on page 134.
<input type="checkbox"/>	5. Use the project to perform your migration workflow in test mode , also referred to as no change mode . Test mode allows you to step through migration tasks and resolve some potential issues before you make changes to your production environment.

<input checked="" type="checkbox"/>	Migration Plan Implementation
<input type="checkbox"/>	6. Migrate your pilot group and resolve any problems that occur. Adjust your migration plan, including your migration schedule and project options.
<input type="checkbox"/>	7. Define projects for sets of objects that you will migrate and track as a unit. Use the options you found worked best during your testing.
<input type="checkbox"/>	8. Notify users, based on your migration schedule, and prepare them for your migration. For more information, see “Notifying Users about Migrating” on page 62.
<input type="checkbox"/>	9. Use the projects you defined to migrate portions of your production environment in a similar manner to how you migrated the pilot group. Perform each migration task in a manageable chunk that you can verify to ensure the process was finished correctly. While using your workflow, remember to migrate objects, track your progress, and verify the results. For more information, see “Migrating Objects and Verifying Results” on page 64.
<input type="checkbox"/>	10. Perform post-migration reporting and assessment of your environment to ensure the migration was completed successfully.
<input type="checkbox"/>	11. Perform post-migration clean-up activities, such as SID History-related clean-up tasks and removing older hardware that is no longer needed.
<input type="checkbox"/>	12. Implement management and monitoring tools to ensure a secure and reliable Microsoft Windows infrastructure. For more information about NetIQ products, contact your NetIQ sales representative.

Understanding Access and Security Issues

Each user account, group, and computer account is represented by a unique identifier, known as a security identifier (SID). The SID is independent of the user account, group, or computer account name. Microsoft Windows use these SIDs to record access permission information in the security descriptor for each resource, such as a file, share, or DCOM object. The security descriptor for a file stores the owner, the system access control list (SACL), and the access control list (ACL) for that file.

When you copy a user account, group, or computer account from domain A to domain B, a new account is created in domain B. This new account has the same name as the original account in domain A, but the new account has a different SID. Therefore, the new account does not have the same permissions as the original account.

Translating Security to Reflect the New SID

Domain Migration Administrator allows you to change the security descriptors for various files, folders, shares, printers, and DCOM objects to reflect the SID for the new account in the target domain (domain B). This process ensures the new account provides the same access to files, folders, shares, and printers that the original account provided. Domain Migration Administrator also translates security for user profiles, registry items, local groups, and local security policies.

Using SID History to Maintain Permissions

In a common migration configuration, migrating from a mixed mode domain to native mode domain, Domain Migration Administrator allows you to set the SID History property during the migration process. This property allows the new account to use the permissions assigned for the SID of the old, migrated account. Therefore, this property provides the access without changing the security descriptors for various files, folders, shares, and printers to reflect the SID for the new account.

When you migrate with SID History, Domain Migration Administrator copies the SID of the original source account into the SID History property of the new target account. You can use Domain Migration Administrator to translate the security for accounts with their SID History property set. When the migration and security translation is complete, you can then use Domain Migration Administrator to remove the SID History property values to clean up these directory entries.

To migrate with SID History, Domain Migration Administrator has specific configuration requirements. You can either perform this configuration manually or allow Domain Migration Administrator to perform the steps for you. For more information about these requirements, see “Preparing to Migrate with SID History” on page 30. For more information about how Domain Migration Administrator sets the SID History property, see “SID History” on page 189.

Migrating Well-Known Accounts

Microsoft Windows provide several **well-known** default user accounts and groups that exist in every domain. The SIDs for these accounts are the same in every domain except for a unique domain identifier. Domain Migration Administrator recognizes the following well-known accounts:

- Cert Publishers
- Domain Admins
- Domain Users
- Domain Guests
- Domain Computers
- Domain Controllers
- Enterprise Admins
- Group Policy Creator Owners
- Guest (user account)
- RAS and IAS Servers
- Schema Admins

To migrate well-known accounts and use the SID History migration option, migrate them using the **Replace** mode. You can add SID History values to a well-known account in the target domain only from the same well-known account in the source domain.

By default, Domain Migration Administrator displays well-known accounts in the wizards. To hide well-known accounts, adjust the **DMA Settings** available from the View menu.

Notes

- If you migrate a user account that is a member of a well-known group, the membership of the well-known group is not updated unless you also migrate the well-known group.
 - When you migrate a user account that is a well-known account, Domain Migration Administrator migrates the password to the target account and sets the **User must change password at next logon** property of the target account.
-

Understanding Built-in Accounts

Microsoft Windows provide several **built-in** user accounts and groups that exist in every domain. The SIDs for these accounts are the same in every domain, *including* the domain identifier that indicates the built-in domain. Domain Migration Administrator recognizes the following built-in accounts:

- Account Operators
- Administrator (user account)
- Administrators
- Backup Operators
- Guests
- Power Users
- Pre-Windows 2000 Compatible Access
- Print Operators
- Replicator

- Server Operators
- Users

Notes

- If you use Domain Migration Administrator to migrate the Administrator user account, review the password option to ensure you know what the password for the migrated account will be.
 - You cannot add SID History to built-in accounts.
-

Copying Local Group Memberships and Domain Controller Security Policy

Domain Migration Administrator also copies local group memberships and domain controller security policy for migrated accounts. If you migrate a local group and its members to another domain, Domain Migration Administrator copies the local group and the member accounts to the target domain. Domain Migration Administrator also makes the new accounts members of the local group in the target domain.

Assessing Your Existing Environment

Before starting a migration project, you need to review your existing environment and identify your current resources. You should identify your needs and what you want to accomplish during the migration. For example, you may need to consolidate some servers and their resources.

Domain Migration Administrator provides reports to help you assess your environment. The following steps guide you through the assessment process:

1. Assess your current domain structure, including master account domains, resource domains, and trusts.
2. Inventory your existing network, including types of connectivity, hosts, subnets, DNS locations, and client count per subnet. Create a network diagram.

3. Identify special servers, such as IIS, SQL Server, DHCP, messaging systems, and other special company-wide applications.
4. Identify special characteristics about your environment, including remote users, WAN links, WINS configuration, Microsoft Windows special roles, FSMOs, and Global catalog.
5. Identify your existing hardware. Your new environment may require new or additional hardware.

Designing Your New Environment

Good planning can help prevent problems in resource placement and connectivity as you migrate to your new environment. You need to have a realistic vision of your resulting network load and structure. You must be very familiar with the benefits of Active Directory to properly structure your new forest and domains. The following list identifies some of the key considerations:

1. Design a network structure that includes a plan for the following items:
 - Forest structure
 - Domain structure
 - DNS, WINS, Microsoft Windows roles, and other critical services
2. Consider special servers, such as IIS, SQL Server, DHCP, messaging systems, and other special company-wide applications. You may not be able to migrate some types of application servers, such as Microsoft Exchange servers. If you will decommission your source domain, reestablish those servers in the new domain. To migrate to Microsoft Exchange, consider using NetIQ Exchange Migrator.
3. Determine how you will distribute network services, including DHCP, DNS, WINS, and Microsoft Windows roles in the new domain. Be sure to address WAN link design issues.

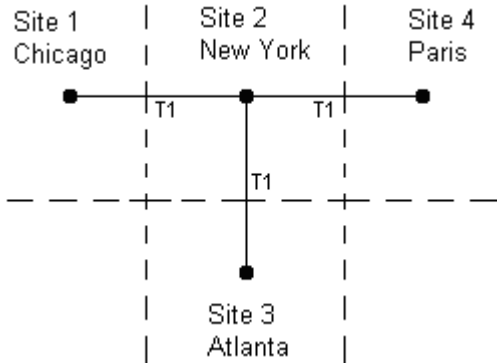
4. Review enterprise design and migration performance issues to ensure you correctly design and prepare your new environment. For more information, see “Considering Enterprise Environment Issues” on page 25.
5. Plan the network infrastructure so it will be in good working order and ready for the loads that may be placed on remote WAN links from the implementation of the new domain structure.
6. Plan your new domain structure and Active Directory, including whether you will consolidate domains.
7. Determine whether you will replace server or workstation hardware. If you will replace hardware, determine whether you will replace it before, during, or after the migration. For more information, see “Domain Migration Administrator Requirements” on page 69 and “Server Consolidator Requirements” on page 78.
8. Develop a plan to secure, monitor, and administer the new environment.

Preparing Your Environment

You need to prepare both your test lab and your production environment. There are several items to consider in both cases. The following sections summarize the issues to consider and help guide you through the preparation process.

Considering Enterprise Environment Issues

Enterprise environments include many complex configurations, such as multiple sites and WAN links. Review your environment and consider how it may affect the performance and ease of your migration.



This section identifies some of the important configuration issues to consider. Be sure to review all aspects of your environment and consider how they may affect your specific migration needs.

Verify Your Network

Make sure the network is operating and stable when migrating objects. Review and verify available bandwidth, connectivity, and name resolution. Your network needs to meet the minimum RPC communication requirements. For more information, see the RPC documentation. In addition, make sure objects and computers involved in a migration task are available when you perform that task.

Communication Issues

During the migration process, Domain Migration Administrator processes many objects. For each object, the product needs to collect information, process and validate the object, and write new information. You should try to limit communication issues, especially across WAN links. Consider the following configuration issues to simplify your migration process, limit WAN traffic, and improve your migration performance:

- Install important services in the same site as the Domain Migration Administrator computer to reduce WAN traffic:
 - PDC emulator
 - RID pool allocator for Microsoft Windows intraforest migrations
 - Domain controller for root domain of target forest
 - Domain controller for root domain of source forest
 - Global catalog for the target forest
 - Infrastructure Master FSMO role for the target domain
 - Name resolution, including DNS server or DNS caching and WINS. For better performance, configure your DNS server to use WINS reverse lookup.
- Install the important services for your source domain as well as your target domain.
- If you are changing any objects in the source domain during the migration, such as disabling or expiring accounts or using scripting, put the PDC Emulator role for the source domain in the same site as the Domain Migration Administrator computer. You can install an Additional Domain Controller for the source domain and then transfer your PDC Emulator Role to the Additional Domain Controller for use during the migration process.
- Before you migrate objects, configure your WAN link for the Domain Migration Administrator computer site to replicate at night, after the local migration is finished. This configuration limits WAN traffic as you migrate and update objects. Then, all the migration changes can be replicated during non-business hours.

- Consider the following for Microsoft Windows intraforest migrations:
 - To improve performance, use direct trusts rather than transitive trusts.
 - Install a domain controller for the source domain in the local site.
 - Install a domain controller for the target domain in the local site.
 - Install Domain Migration Administrator on the Relative ID (RID) pool master in the target domain for efficient operations. When you migrate users and groups between domains in the same forest, Domain Migration Administrator communicates with the RID pool master in the target domain. By default, the RID pool master is the first domain controller installed in the domain. You can use Active Directory Users and Computers or the `Ntdsutil .exe` utility to identify the RID pool master computer.
- For better migration performance, locate the computer roles already noted in the same physical IP subnet as the Domain Migration Administrator computer. This layout reduces the router hops required during the migration process.
- To help future corporate mergers and acquisitions, and to limit security issues related to the Enterprise Admins group in the forest root domain, Microsoft recommends you create an empty forest root domain.
- To address potential security issues, give your forest root domain a different name than your published domain name. For example, if your published domain name is `acme.com`, consider naming your forest root domain `acme.local`.

Getting Production Data into Your Test Lab

The tests you perform in your test environment should closely match the tasks you will perform while migrating your production environment. You should identify potential issues in your test lab and determine how to resolve each issue before you start migrating in your production environment. The following process can help you get your production data into your test lab.

To get your production account definitions into your test lab:

1. Select a domain controller in a production domain that you can remove from your production environment. For example, you could add an additional domain controller to your production environment and then remove that computer when needed.
2. Force a domain replication in the production domain. Allow enough time so that your selected domain controller has a complete replica of the account information for the production account domain. Check the event log on the domain controller to ensure the replication occurred and finished successfully.
3. Remove the domain controller from the production network and connect it in the test lab. This process ensures you have a copy of your accounts database, and that most of your unique migration cases can be tested in the lab.

Preparing for Recovery and Fault Tolerance

Before you start your migration, you should record configuration information about your current environment and prepare a method for quickly recovering from potential problems. Consider the following process to help you create a recovery plan and method.

To prepare for recovery from a migration issue:

1. Add a domain controller to your production source domain. Use the domain controller to store important source domain information and to provide a way to quickly bring your source domain back online in its previous state, if needed.
2. Document the configuration information and services in your source domain.
3. Back up all the applications in your source domain.
4. Fully synchronize all the domain controllers in your source domain. Check the event log to ensure the replication has finished successfully.
5. Remove the domain controller you added to your source domain in Step 1 from your production environment. Reserve this computer for recovery until you have finished the migration process and no longer need a recovery method.

For more information about migration recovery and fault tolerance methods, see the Microsoft best practices information.

Preparing Your Source Domains

You need to perform several tasks to ensure Domain Migration Administrator can migrate information from domain controllers in the source domains. This section outlines the source domain preparation tasks.

To prepare a source domain:

1. To simplify the migration process, change your network protocol to TCP/IP. Microsoft Windows requires TCP/IP and most other operating systems support it.
2. If you are migrating to a mixed-mode domain, ensure the source domain is in a different forest than the target domain.
3. Use the Network application in Control Panel to verify your TCP/IP protocol properties, including your IP address, subnet mask, default gateway, DNS host name, and primary and secondary WINS servers.
4. *If you will migrate with SID History*, review the configuration requirements. For more information, see “Preparing to Migrate with SID History” on page 30.
5. Configure DNS and WINS name resolution services. Verify that the services are running properly. For more information, see “Verifying Name Resolution Services” on page 37.
6. Restart the domain controller so all changes, including the SID History configuration changes, take effect.

Preparing to Migrate with SID History

When migrating from a Microsoft Windows mixed mode domain to a Microsoft Windows native mode domain, Domain Migration Administrator allows you to set the SID History property during the migration process. The SID History property allows the new account to use the permissions assigned for the SID of the original, migrated account. Therefore, this property provides the access without changing the security descriptors for various files, folders, shares, and printers to reflect the SID for the new account. For more information, see “Using SID History to Maintain Permissions” on page 19. For more information about migrating objects with SID History and potential issues, see “Objects that Domain Migration Administrator Migrates” on page 76.

To update the SID History of migrated accounts in the target domain, consider performing the following steps on the domain controller of the source domain to simplify the migration process. If you do not perform these configuration steps, Domain Migration Administrator makes these changes for you:

1. Enable user account and group management auditing in both the source and target domains for success and failure events. For more information, “Enabling Account Management Auditing” on page 31.
2. Create the `TcpipClientSupport` registry key in the following registry location and set it to 1 to enable TCP/IP transport support. If you create this registry key, restart the domain controller to activate this value. For more information, see “Enabling TCP/IP Transport Support” on page 33:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\
```

3. Ensure Domain Migration Administrator can create the *SourceDomain* local group in the source domain. For example, if the source domain is named *DomainA*, Domain Migration Administrator creates the *DomainA* local group. This group should not have any members. If a global group or other type of group already exists with this name, Domain Migration Administrator cannot create the required local group. Domain Migration Administrator creates this group in the Users container.

Notes

- To update the SID History of migrated accounts in the target domain, you should install and run Domain Migration Administrator on a domain controller or other supported Windows computer in the target domain. For more information, see “Installing Domain Migration Administrator and Server Consolidator” on page 81.
 - The source domain must have a secure channel for communicating the SID. Domain Migration Administrator prompts you to ensure the required settings, such as the `TcpipClientSupport` registry entry, are correctly set to establish the secure channel.
 - The target domain must have access to the Global catalog server.
-

Enabling Account Management Auditing

To assist with the migration process, you should enable user account and group management auditing for success and failure events. The following steps outline the process for enabling account management auditing on a Microsoft Windows domain controller.

To enable account management auditing:

1. *If the computer is running Microsoft Windows 2000 Server or Windows Server 2003*, complete the following steps:
 - a. Open **Active Directory Users and Computers**.
 - b. Select the **Domain Controllers** container in the target domain.
 - c. On the Action menu, click **Properties**.
 - d. Click the **Group Policy** tab.

- e. Select the **Default Domain Controllers Policy** and click **Edit**.
- f. In the left pane of the Group Policy window, expand **Computer Configuration**.
- g. Expand **Windows Settings**.
- h. Expand **Security Settings**.
- i. Expand **Local Policies**.
- j. Expand **Audit Policy**.
- k. In the right pane, select **audit account management**.
- l. On the Action menu, click **Security**.
- m. Check **Define these policy settings**.
- n. Check both **Success** and **Failure**, and then click **OK**.
- o. Close the Group Policy window and close Active Directory Users and Computers.

To enforce the policy immediately, restart the domain controller. You can also wait for the domain controller to automatically refresh group policy.

2. *If the computer is running Microsoft Windows Server 2008*, complete the following steps:
- a. Run Gpmc.msc.
 - b. Select the **Domain Controllers** container in the target domain.
 - c. Select **Default Domain Controllers Policy**.
 - d. On the Action menu, click **Edit**.
 - e. In the left pane of the Group Policy window, expand **Computer Configuration**.
 - f. Expand **Windows Settings**.
 - g. Expand **Security Settings**.

- h. Expand **Local Policies**.
- i. Expand **Audit Policy**.
- j. In the right pane, select **audit account management**.
- k. On the Action menu, click **Security**.
- l. Check **Define these policy settings**.
- m. Check both **Success** and **Failure**, and then click **OK**.
- n. Close the Group Policy window and close the Group Policy Management Console.

Enabling TCP/IP Transport Support

To assist with the migration process, you should create the `Tcpi pCl i entSupport` registry key and set the key appropriately. You should set the registry key on the domain controller of the source domain to simplify the migration process. If you do not create this registry key, Domain Migration Administrator creates the `Tcpi pCl i entSupport` registry key automatically when you migrate accounts using SID History.

To create and set the `Tcpi pCl i entSupport` registry key:

1. Run `Regedt32`.
2. Select the following node:
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA`
3. On the Edit menu, click **Add Value**.
4. Type `Tcpi pCl i entSupport` in the **Value Name** text box.

5. Select **REG_DWORD** from the **Data Type** list, and then click **OK**.
6. Type 1 in the **Data** text box, and then click **OK**.

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.

Setting Up a Clean Domain

For the target domain, you can set up a new Microsoft Windows domain or use an existing domain. A clean and pristine Microsoft Windows domain environment ensures the migrated objects are correctly established in Active Directory. For more information about using an existing target domain, see “Preparing an Existing Target Domain” on page 36.

The following process outlines how to set up a new Microsoft Windows domain and identifies several important considerations. You should also consider requirements specific to your environment. For more information, see “Considering Enterprise Environment Issues” on page 25.

To set up a clean Microsoft Windows domain:

1. Select a computer with the appropriate hardware requirements for your version of Microsoft Windows server. For more information, see “Domain Migration Administrator Requirements” on page 69.
2. Establish a new Microsoft Windows domain by installing Microsoft Windows server and the latest service packs. For more information about service packs and requirements, see the Microsoft Web site and the *Domain Migration Administrator Release Notes*.
3. To take best advantage of Microsoft Windows file security features, format the drive partitions using NTFS rather than FAT or FAT32.

4. Evaluate which Microsoft Windows service components you need and install those components. You should install at least DNS, TCP/IP, and WINS. Also consider IIS and DHCP. Verify that these components work properly. For more information, see the Microsoft Windows server documentation.

Note

After you migrate a DHCP server, you must authorize the server. To have permission to authorize a DHCP server, you must be a member of the DHCP Admin group in your environment.

5. Run DCPromo to promote the server to domain controller of the local domain. This step establishes the server as the first domain controller with the Global catalog and all Flexible Single Master Operations (FSMO) roles.
6. Configure at least one more domain controller in this domain. Having at least two domain controllers in the target domain provides fault tolerance and is suggested but not required. However, you also need to consider Active Directory replication issues when migrating to a target domain with multiple domain controllers.
7. Synchronize the time on all computers involved in the migration. Domain controllers must be within 5 minutes of each other during the migration process.
8. Use Active Directory Users and Computers to move the FSMO Infrastructure role from the Global catalog domain controller (first domain controller) to the second domain controller that is *not* a Global catalog server. For more information about FSMO roles, see the Microsoft Windows documentation.
9. *If you want to migrate with SID History*, use Active Directory Domains and Trusts to change the domain from Microsoft Windows mixed to native mode.

Note

Changing the domain designation from mixed mode to native mode is a permanent change and you cannot undo it. For more information, see the Microsoft Windows documentation.

10. Ensure **File and Printer Sharing for Microsoft Networks** is enabled and the **Server service** is running for the local area network connection on the Domain Migration Administrator computer and on all computers to which Domain Migration Administrator dispatches agents. Domain Migration Administrator dispatches agents to collect data for reports and to translate security for files, folders, shares, and other objects.
11. Enable auditing for account management for both success and failure events on the domain controller. Domain Migration Administrator enables auditing if it is not already enabled. For more information, see “Enabling Account Management Auditing” on page 31.

Preparing an Existing Target Domain

When you migrate to an existing target domain instead of a new clean domain, be sure your target environment supports the new configuration. You also need to resolve issues, such as naming conventions, in the target domain before you migrate to that domain. Resolving these issues in advance can simplify your migration process and ensure the migrated objects are correctly established in Active Directory or the SAM database. Consider the following issues:

- Multiple domain controllers provide fault tolerance and can provide key functions in the target domain. Carefully consider the roles for each server and where the servers are located. For more information, see “Considering Enterprise Environment Issues” on page 25.
- Ensure your target domain has adequate hardware to support the environment you are creating. Carefully review the Microsoft Windows requirements and related features.
- Synchronize the time on all computers involved in the migration. Domain controllers must be within 5 minutes of each other during the migration process.
- Review the requirements outlined for a new clean target domain to ensure the existing domain can support the migration process. For more information, see “Setting Up a Clean Domain” on page 34.

Verifying Name Resolution Services

The DNS and WINS name resolution services must be in place and properly functioning to successfully use Domain Migration Administrator. DNS service problems are one of the most common problems encountered when attempting to migrate from domain to domain. Rigorously checking and verifying your DNS services before starting your migration can prevent many problems and frustrations.

Notes

- Domain names must be unique. Domain Migration Administrator does not support migrating between two domains whose DNS or NetBIOS names are identical.
 - For more information about installing and implementing DNS, see Microsoft article Q301192 and Q323419 at www.support.microsoft.com/kb/301192/en-us and www.support.microsoft.com/kb/323419/en-us respectively. You can also use the `DNScmd` utility to help identify and resolve DNS-related issues.
-

To verify that DNS is working properly:

1. Verify every domain controller IP address in the DNS *forward* and *reverse* lookup zones. Make sure there are no missing or unneeded host records.
2. Verify that the secondary DNS server has replicated every change in both the forward and reverse lookup zones. Make sure there are no missing or unneeded records.
3. On the primary DNS server, stop and restart the DNS server service, and then stop and restart the DNS client service. Repeat the process for the secondary DNS server.
4. Use the `NSLOOKUP` command at the primary and secondary DNS servers to verify that the host name and IP address of the computer where you will install Domain Migration Administrator are both resolved properly. For more information about the `NSLOOKUP` command, see the Microsoft Windows documentation.
5. Use the `NSLOOKUP` command at the computer where you will install Domain Migration Administrator to verify that the primary and secondary DNS servers, the Global catalog server, and all five FSMO role servers are properly resolved for both host name and IP address.

6. Use the `NSLOOKUP` command on all other domain controllers involved in the migration to verify the primary and secondary DNS servers are properly resolved for both host name and IP address.
7. For best results, switch your source Domain Controller to register in and point to your Microsoft Windows domain DNS and WINS servers.

Testing Secure Channel Communication

To migrate with SID History, Domain Migration Administrator requires a secure channel. To test secure channel communication, you can use the following Microsoft utilities:

- `DCDi ag`
- `NetDi ag`
- `NLTest`

For more information about these utilities, see the Microsoft documentation.

Establishing a Two-Way Trust

Establish a two-way trust between the source and target domains. If your DNS or WINS services are not working properly, you may have problems establishing a two-way trust.

You can also use the `NetDom` tool. For more information, see the Microsoft Windows documentation.

To establish a two-way trust:

1. On the target domain controller, add the source domain to the list of trusted and trusting domains.
2. On the source domain controller, add the target domain to the list of trusted and trusting domains.
3. Verify that you have a bi-directional, external trust established between the source and target domains.

You do not need to establish all trusts in the target domain. Domain Migration Administrator allows you to migrate other trust relationships between the source domain and other domains to the target domain.

Establishing Migration Credentials

To perform a migration, Domain Migration Administrator needs specific permissions to objects in the source and target domains. Domain Migration Administrator agents also need specific permissions to perform tasks, such as translating security and collecting information for impact analysis reports. For some tasks, the agents use the Local System account. For more information, see “Agents” on page 178.

When you perform a migration task, Domain Migration Administrator uses your user account and password, also called **credentials**. For agent tasks that use an account other than the Local System account, Domain Migration Administrator prompts you for the credentials the agents should use.

The agent uses these credentials to establish a connection to the Domain Migration Administrator console. The credentials are also used to change domain affiliation.

Microsoft Windows uses specific local and global groups to control access to important resources. You need to use the model to ensure your user account has the required permissions to perform various migration tasks. The following sections identify your options, as well as the strengths and tradeoffs of each option. For more information about specific requirements and limiting the migration account permissions, see “Detailed Permission Requirements” on page 157.

Notes

- By default, the Domain Admins group in a domain is a member of the Administrators local group on each computer in that domain. This membership ensures members of the Domain Admins group in a domain have administrator permissions on all computers in that domain. If you change this default membership, you may need to assign additional permissions to the user account you will use to perform the migration tasks.
 - To perform an intraforest migration to the domain located at the root of the forest, the migration account must be a member of the Enterprise Admins group in that forest.
-

One Migration Account

This approach is the easiest to use, but it can require more time to set up.

When to use	When migrating over time or in phases. In this scenario, you may have source domain accounts with permissions on objects in the target domain and you may need to translate security on those objects several times or run impact analysis reports for all computers in the source domain.
Benefits	<ul style="list-style-type: none">• One account to use throughout the migration.• You have administrator permissions on all computers in the source and target domains using one account.
Tradeoffs	You need to add the user account to the Administrators local group on each member server and workstation in each source domain.

To define one migration account with the required permissions:

1. Log on to the target domain and create a user account to use as the migration account. You will use the new user account to perform the migration tasks. The agents can also use this account.
2. Add the migration account to the Domain Admins group in the target domain.
3. Log on to each source domain and complete the following steps:
 - a. Add the target migration account to the Administrators local group in the source domain.
 - b. Add the target migration account to the Administrators local group on each member server and workstation in the source domain.
4. *If you will delegate project definition tasks*, make sure the user accounts for the users who will define migration projects have the permissions to view objects in both the source and target domains. These users do not need administrator permissions unless they will perform the migration.

Multiple Migration Accounts

This approach requires less time to set up, but you need to use the correct account to perform each migration task.

When to use	When migrating all the accounts from a source domain at one time. In this scenario, you do not need to perform a task more than once, so the number of times you may need to log off and log on with a different account are limited.
Benefits	You need to grant permissions on fewer computers.
Tradeoffs	<ul style="list-style-type: none">• You need to use the right account to perform each migration task.• You have one migration account in the target domain and one migration account in each source domain.

To perform the following migration tasks for objects in a source domain, you need to log on with the migration account for that source domain:

- Translate security on files, folders, shares, or DCOM objects in the source domain
- Collect information for some reports related to the source domain, such as the Domain Status reports
- Migrate or rename computers in the source domain
- Migrate service accounts for the source domain
- Consolidate servers in the source domain
- Migrate local groups for member servers and workstations in the source domain

To define multiple migration accounts:

1. Log on to the target domain and create a user account to use as the target migration account. You will use this user account to perform most migration tasks.
2. Add the target migration account to the Domain Admins group in the target domain.

3. Log on to each source domain and complete the following steps:
 - a. Add the target migration account to the Administrators local group in the source domain.
 - b. Create a user account to use as a source migration account. You will use the account to perform tasks that require permissions on all computers in the source domain.
 - c. Add the source migration account to the Domain Admins group in the source domain.
4. Log on to the target domain and add the source migration accounts to the Administrators local group in the target domain.
5. *If you will delegate project definition tasks*, make sure the user accounts for the users who will define migration projects have the permissions to view objects in both the source and target domains. These users do not need administrator permissions unless they will perform the migration.

Reviewing Password Policies

Domain Migration Administrator can migrate passwords for user accounts. Domain Migration Administrator can also generate a complex password or assign the user ID as the password. However, the password policies in the source and target domains must be compatible. Domain Migration Administrator cannot copy weak passwords into a domain that requires strong, complex passwords.

In most cases, you should migrate the existing password along with the user account. You may need to temporarily change the password policy in the target domain to simplify the migration process. You could also set the password policy in the source domain to match the target domain. Then, you could notify users of the new password requirements and set the **User must change password** property for all user accounts. After all users have changed their password, the new passwords will match the new requirements for the target domain.

When preparing for user account and password migration, review the following considerations:

- Review the password policy in the source and target domains. Ensure the password policy on the target domain is the same or less restrictive than the password policy for the source domain. If you migrate a user account more than once, you need to set the password each time. To avoid password history issues for changing passwords, set the password history requirement to zero, if possible, in the target domain.

Note

If the password history requirement is set to anything other than zero, you will need to wait until the temporary password that Domain Migration Administrator sets during migration expires before you can change it.

- When you migrate user accounts between domains in the same forest and the target domain is Microsoft Windows native mode, Domain Migration Administrator migrates the passwords to the target domain. Make sure the passwords in the source domain will comply with the password policy in the target domain.
- If SYSKEY encryption is enabled on only the source domain, and the target domain, Domain Migration Administrator can migrate passwords given an additional domain controller in the source domain that does not have SYSKEY encryption enabled. To help resolve SYSKEY encryption issues, contact Technical Support.
- If the source user account has a blank password, Domain Migration Administrator generates a complex password instead of copying a blank password.
- The migrated passwords may not comply with the password policy in the target domain.

- If you cannot change the password policy in the target domain, consider having Domain Migration Administrator generate a password. The passwords Domain Migration Administrator generates have at least 3 lowercase letters, 3 uppercase letters, 3 numbers, and 3 special characters. If the generated password does not comply with the password policy for the target domain, the target account is disabled. If you use this Domain Migration Administrator option, you also need to consider how to distribute the generated passwords to the users.

Note

If you clear the Microsoft Windows password policy check box, Microsoft Windows still enforces the policy.

- If you cannot arrange a method for distributing passwords, consider using the option that sets the password for each migrated user account to the user ID. This Domain Migration Administrator option sets the password to the first 14 characters of the user ID in lowercase letters. Setting the password to the first 14 characters of the user ID presents some security risks, but a staged migration plan may sufficiently reduce this risk. If you use this option, review the minimum password length and password complexity policies in the target domain to ensure the user accounts can be created with the user ID as a password. For example, the passwords will be set using all lowercase letters, and they may be short because user IDs are short in many cases.

Considering Other Applications

You may need to install other software on the target domain computers to emulate or complete your production environment. Consider the following items to help you decide which other software you may want to install:

- Using other NetIQ migration and management products:
 - You can use NetIQ Exchange Migrator to simplify your various migration tasks. For more information about installing NetIQ Exchange Migrator, see the NetIQ Exchange Migrator documentation.
 - You can use NetIQ administration products to effectively manage your migrated environment. These products can be installed before or after you complete the migration process.
 - NetIQ Corporation provides other products to help you monitor and manage your environment. For more information, contact your NetIQ sales representative.
- Other products, such as Microsoft SQL Server, may be needed in your new environment. Review the specific product requirements and install the other applications you need.

Developing a Migration Plan

To perform a successful migration, you should have a detailed plan that addresses many migration considerations. The topics in this section help you create a comprehensive migration plan for your environment. You have several key goals:

- Develop a detailed migration plan including prototyping, step-by-step guidelines, pilot testing, and an overall schedule. Your schedule should include migration start, duration, cutover, and decommission dates.
- Develop a plan that includes strategies for implementing security and management solutions in your new environment. You also need to plan for moving network-wide applications to your new structure.

Determining the Scope of Your Migration

Knowing the scope of your migration project helps you estimate the amount of time your migration will take. Identify the types and number of objects you need to migrate.

To determine the scope of your migration:

1. Estimate the number of objects you need to migrate. Be sure to include the following types of objects and considerations:
 - Users, groups, and computers
 - Obsolete users and computers that should not be migrated
 - Duplicate user IDs in more than one domain
 - Users using machine local profiles or roaming profiles
 - GPO security policies
 - Objects previously migrated using the ADC tool
 - Computers running other operating systems, such as Microsoft Windows 98
 - Whether to migrate domain controller security policy
 - Whether to migrate passwords
 - Whether to migrate service accounts

Note

To identify this information, run the Domain Status, Impact Analysis, and Disabled/Expired reports from the Global Reports wizard. Include the source domain, all domains that the source domain trusts, and all computers in the domain as sources for these reports. For more information about special reports in the Domain Status folder, see “Special Reports” on page 134.

2. Determine how many files, folders, and shares you need to copy. Also consider any special equipment in your enterprise, such as NetApp filers, cluster servers, and systems using Distributed File System (DFS) shares.

3. Determine whether you want to consolidate any servers before you migrate them to the new domain. You can consolidate servers before or after you migrate to the target domain. If you consolidate before you migrate, be sure your hardware can support the consolidated resources.
4. Run the Domain Status Last Logon/Last Logoff Times report to identify any potentially obsolete accounts. Decide whether to delete or disable obsolete accounts before migration.
5. Run the Disabled/Expired reports for Disabled Accounts, Expired Accounts, and Expired Computers to identify disabled or expired accounts. These reports allow you to detect computers that may be offline or are no longer in the domain. Domain Migration Administrator does not prevent you from migrating these computer accounts. You can identify and remove unused computer accounts before migration, which results in a more pristine target domain. You can use User Manager for Domains or Active Directory Users and Computers to delete the computer accounts.
6. Identify duplicate user accounts, groups, and computer accounts by running the Domain Status Name Conflicts report. Users may have accounts in multiple domains, or you may have two accounts in different domains that have the same name. You need to identify overlapping account names and determine whether the accounts map to the same user or to different users.

If you have duplicate user accounts, you need to determine how to handle these user accounts. To resolve the naming conflict, you need to decide whether to merge the accounts or to rename the accounts.

7. Run the Impact Analysis reports to identify all the computers for which you need to run the Translate Security wizard. This wizard enables you to resolve access permissions for the migrated accounts and for the profiles where each user logged on.
8. Run the Service Account reports to identify the service accounts you need to migrate and on which computers those accounts are used.

Developing a Migration Workflow

During testing, one primary goal is to collect information and migrate sample objects, including user accounts, groups, and computers. During this phase, you develop and document a migration workflow for your environment. Then, during pilot testing, you may have to further refine this workflow.

Important Considerations

Be sure to document the final workflow that provides the best results for your environment. Identify the migration options that work best for you. For example, you may decide to migrate all the groups first, then migrate all user accounts. You could also decide to migrate groups and automatically include all user accounts that are members of those groups. While you develop your migration plan and workflow, you need to identify and test the various options that Domain Migration Administrator provides.

You should review and address the following considerations:

- Run test-mode migrations, as well as directory and security translations, to identify potential issues. These test-mode migrations help you address any issues before you make changes to your production environment.
- Be sure to include accounts with special characters, such as \: , " -/>{<+}; | () in their names. To understand the migration process, test all cases that exist in your production environment.
- Since user accounts with names that contain more than 255 characters are not displayed in the Migrate User Accounts wizard, consider shortening these user names before migration.

- When migrating between two domains in the same forest (intraforest), consider the following issues:
 - If you migrate service accounts, make sure all computers with services that use those accounts are available during the migration process.
 - You cannot migrate locked out accounts. To migrate a locked out account, you must first unlock that account.
 - Follow the steps in the workflow for the intraforest scenario. For more information about how the intraforest migration scenario is different, see “Identifying Your Migration Scenario” on page 10.
- Make sure objects and computers involved in a migration task are available when you perform that task.
- Consider using the Map and Merge Groups wizard in Domain Migration Administrator to merge the source Domain Admin group and the target Domain Admin group before you begin the migration process. You can then use an account that is a member of the target Domain Admin group to perform all of your migration tasks. The account will have the source and target Domain Admins group SIDs in its token and therefore can be used for tasks that require domain administration privileges in the source and target domains.

Note

After you migrate a DHCP server, you must authorize the server. To have permission to authorize a DHCP server, you must be a member of the DHCP Admin group in your environment.

Workflow

The following migration workflow is an example to help you devise and test your own workflow. The following sample workflow identifies some important steps to consider:

1. *If you want to implement a new computer naming convention*, use the Rename Computers wizard to rename workstations and member servers.

Note

Do not use Domain Migration Administrator to rename servers running BackOffice services, such as Microsoft Exchange, SQL Server, and SMS. Instead, follow the procedures outlined by Microsoft Premier Software Support (PSS) when renaming these computers.

2. Create migration projects for unique sets of objects. Each project allows you to define a set of objects that you will migrate and track as one unit and process in a similar manner.

Create projects for user accounts and groups. To simplify the permission requirements for the account you log on with when you perform the migration, create separate projects for computers. Each project can include only one source domain. To help you quickly verify the results of a migration, limit the number of objects in each project. You can then more easily verify that the objects in a project were migrated correctly.

3. *If you want to distribute the project creation part of the migration process*, you can use delegation mode. Delegation mode allows users in remote locations to select the objects to include in a migration project and to specify the appropriate settings. Then, they can export the project to the SQL Server computer and notify a central domain administrator of the exported file name. The central domain administrator can import the project and actually perform the migration. The central administrator can also use the CLI to schedule the defined migration tasks. For more information, see “Delegating Migration Tasks” on page 111.
4. Periodically back up your project database files to save the settings for future reference and problem resolution. You can use the export function to export each project, or you can copy the appropriate files. For more information about the project database files, see “Understanding the Domain Migration Administrator Databases” on page 227.

5. Perform the appropriate maintenance tasks for SQL Server databases following Microsoft best practice guidance. For more information, see the Microsoft SQL Server documentation.
6. *If you have service accounts that you want to migrate to the new domain and update the services to use the new accounts*, collect service account information by completing the following steps:
 - a. Generate reports about service accounts on your servers. This information can help you determine which servers to include in your service account migration.
 - b. Run the Service Account Configuration wizard for the servers identified in the service account reports. Domain Migration Administrator uses this information when you migrate the service accounts.

Note

Instead of using Domain Migration Administrator to update service accounts for Microsoft BackOffice services, such as SQL Server and Microsoft Exchange Server, you should follow procedures outlined by Microsoft Premier Software Support (PSS).

- c. After you migrate the accounts, use the Security Translation wizard to update the service account permissions and translate the domain controller security policy. To ensure service accounts are members of the appropriate local groups, select **Local groups** on the Translate Objects window in the Security Translation wizard.
 - d. Stop and restart services to ensure they use the new service accounts.
7. Run the following Domain Status reports:
 - Domain Trust Report
 - Group Membership
 - Last Logon Times
 - Name Conflicts
 - Recursive Group Membership

For example, the Name Conflicts report helps you identify potential naming conflicts for the objects in the project. Develop plans and identify the migration options to resolve these conflicts. For more information about special reports, see “Special Reports” on page 134.

Ensure all account names will be unique in your target domain. Compare computer account and user account names to ensure you identify potential conflicts in your target domain.

8. *If you have computers that you want to migrate to the new domain*, generate the Pre-Migration Check Report for Workstation. The report enables you to check whether the computers you have selected for migration meet all the prerequisites for a successful migration. For more information about reports, see “Understanding Reporting” on page 133.
9. *If you need to modify user accounts and groups as part of your migration*, you can set options to add a prefix or suffix to each migrated account name. You can also use database modeling and scripting to customize the migration process to meet your specific needs. For example, you can use scripting to set account properties based on values in a Human Resources database. For more information, see “Renaming or Moving Objects” on page 60.
10. *If you need to adjust your group structure and memberships*, use the Map and Merge Groups wizard. This wizard allows you to combine groups before or during the migration process.
11. Migrate the appropriate groups (local and global) using the Group Migration wizard. To quickly validate the results of the migration and simplify the process, do not check the option to migrate associated users. You will migrate the user accounts in the next step. If possible, you should migrate with SID History to ensure continued access to files, shares, printers, system registries, and other resources. For more information, see “Using SID History to Maintain Permissions” on page 19.

12. Migrate the appropriate user accounts using the User Migration wizard. To quickly validate the results of the migration and simplify the process, do *not* check the option to migrate associated groups. If possible, you should migrate with SID History to ensure continued access to files, shares, printers, system registries, and other resources. Consider the following additional options when migrating user accounts:

- You can translate roaming profiles for user accounts. However, translating roaming profiles for large environments can require an extended period of time. If you are not migrating with SID History, you must translate roaming profiles. Domain Migration Administrator translates roaming profiles only for non-DFS shares.
- Do not log on while Domain Migration Administrator migrates your profile or translates security for your profile.
- You can translate Microsoft Windows Terminal Server profiles for the user accounts you are migrating.
- You can disable the source or target user accounts during the migration. To provide a smoother transition to the new domain, set an expiration date on the source user accounts and encourage users to switch to the new logon domain.
- You can choose to not migrate the domain controller security policy, in which case the user account inherits default rights.

The new user accounts and groups have new SIDs. To ensure users have the same access they did using their old accounts, you can translate security to grant access to the new SIDs. Translating security applies to many resources, including files, shares, user profiles, printers, system registries, and Distributed Component Object Model (DCOM) objects. The process of providing the new target accounts with the same permissions as the associated source accounts is called security translation or re-ACLing.

Note

Domain Migration Administrator dispatches agents to remote computers. Make sure replication is up to date across all domain controllers in the target domain before you translate security or migrate computers.

If you migrated with SID History, this security translation is optional for everything but User Profiles, but it is recommended so you can clean up SID History and reduce Active Directory clutter. If you migrated with SID History and you have local profiles, you must translate security on the local profiles. The following steps outline the process based on whether you migrated with SID History. If you performed an intraforest migration, see Step 15 for the *intraforest* migration steps.

13. *If you did not migrate with SID History*, complete the following steps:
 - a. Use the Security Translation wizard to **Add** permissions for the new target accounts. Translate security on all computers, including workstations and member servers. If you previously ran the Impact Analysis reports and you are using migration projects, you can use the **Analyze** button to populate the list of computers.
 - b. *If you want to migrate user workstations and member servers to the new domain*, use the Computer Migration wizard to migrate computers from one domain to another. You can also use Server Consolidator to move the important data from a computer in the source domain to a computer in the target domain.
 - c. Make sure all users are logging on with their target domain account and they can access the resources they need.
 - d. Use the Security Translation wizard to **Remove** permissions for the old source accounts. Translate security on *all* computers, including workstations and member servers. If you previously ran the Impact Analysis reports and you are using migration projects, you can use the **Analyze** button to populate the list of computers.

14. *If you migrated with SID History and you want to maintain a way to recover quickly from any issues*, complete the following steps:
- a. Use the Security Translation wizard to **Add** permissions for the new target accounts. Translate security on *all* computers, including workstations and member servers. If you previously ran the Impact Analysis reports and you are using migration projects, you can use the **Analyze** button to populate the list of computers.
 - b. *If you want to migrate user workstations and member servers to the new domain*, use the Computer Migration wizard to migrate computers from one domain to another. You can also use Server Consolidator to move the important data from a computer in the source domain to a computer in the target domain.
 - c. Make sure all users are logging on with their target domain account and they can access the resources they need.
 - d. When all access in the new domain is working well, you can remove SID History from all migrated objects.

Note

Remove SID History with caution. You must translate security on all files, shares, registries, DCOM objects, and other migrated objects on all affected computers before you remove the SID History attribute. Removing SID History can cause users to lose access to resources they need. You should remove SID History for limited sets of users and monitor their access permissions before removing SID History for the next set of users. If you will migrate to Microsoft Exchange in future, you should *not* remove the SID History information until NetIQ Exchange Migrator finishes migrating the Microsoft Exchange objects.

- e. Decommission the source domain and ensure no problems occur.
- f. Recommission the source domain and then use the Security Translation wizard to **Remove** permissions for the old source accounts.

15. *If you performed an intraforest migration, or you migrated with SID History and you want to translate security more quickly*, complete the following steps:

- a. Use the Security Translation wizard to **Add** permissions for **user profiles only**. Translate security on all computers, including workstations and member servers. If you previously ran the Domain Status reports and you are using migration projects, you can use the **Analyze** button to populate the list of computers.
- b. *If you want to migrate user workstations and member servers to the new domain*, use the Computer Migration wizard to migrate computers from one domain to another. You can also use Server Consolidator to move the important data from a computer in the source domain to a computer in the target domain.
- c. Use the Security Translation for Accounts with SID History wizard. This wizard replaces permissions for the source accounts with permissions for the new target accounts. Translate security on *all* computers, including workstations and member servers. If you previously ran the Impact Analysis reports and you are using migration projects, you can use the **Analyze** button to populate the list of computers.
- d. Make sure all users are logging on with their target domain account and they can access the resources they need.
- e. When all access in the new domain is working well, you can remove SID History from all migrated objects.

Note

Remove SID History with caution. You must translate security on all files, shares, registries, DCOM objects, and other migrated objects on all affected computers before you remove the SID History attribute. Removing SID History can cause users to lose access to resources they need. You should remove SID History for limited sets of users and monitor their access permissions before removing SID History for the next set of users. If you will migrate to Microsoft Exchange in the future, you should *not* remove the SID History information until NetIQ Exchange Migrator finishes migrating the Microsoft Exchange objects.

16. **For all scenarios other than intraforest migrations:** Decommission the obsolete domains. To enable yourself to quickly recover from potential migration errors, turn off the computers for some period of time before formatting them or releasing the hardware. This process maintains the information if you need to put computers back on the network while you resolve some migration issues.
17. Consider how you can customize, automate, and delegate the migration process. For more information, see “Renaming or Moving Objects” on page 60.

Planning for Microsoft Exchange

If you are using Microsoft Exchange in your current environment, you need to address several additional considerations in your migration plan. You can also use NetIQ Exchange Migrator to help you move existing mailboxes to Microsoft Exchange in the new domain. For more information, see the *User Guide for NetIQ Exchange Migrator*.

Address the following Microsoft Exchange-related considerations in your migration plan:

- Determine whether to maintain your existing Microsoft Exchange system or to migrate to a later version.
- Determine how and when you will migrate Microsoft Exchange mailboxes, distribution lists, custom recipients, and public folders.
- Determine whether to use NetIQ Exchange Migrator to migrate to Microsoft Exchange.
- If you plan to use NetIQ Exchange Migrator to migrate to a later version of Microsoft Exchange in the future, you need to migrate with SID History and not remove the SID History information before you migrate to Microsoft Exchange, or you need to keep the account names the same in the source and target domains.

Running Migration Tests and Verifying Results

To test your workflow and ensure your migration process is successful, you should perform real migration tasks using the computers in your lab. These test migrations help you identify potential issues so you can address them before you make changes to your production environment.

As you perform tests in the lab, verify the results of each migration task. As you run through your workflow, modify your migration plan to address any issues you identify. Then, when you are ready to begin migrating your production environment, you have a comprehensive guide for successfully completing your migration. For more information, see “Migrating Objects and Verifying Results” on page 64.

In addition, as you perform tests in the lab, collect throughput performance data for the time required to migrate user accounts and groups, as well as translating security. The performance data should apply to your specific environment and give you the best data on which to base your production migration. Be sure to plan for and test migrations that involve WAN connections and computers that are not always available.

Establishing a Migration Time Line

Part of a migration plan includes when to start, how long the transition will take, how long to maintain dual resources, and other considerations. Address the following scheduling tasks to establish a migration time line and schedule to include in your migration plan:

- Plan time for pilot testing in your production environment and refining your migration plan.
- Limit the scope of specific portions of your migration and develop a schedule that identifies start and end dates for each portion of your migration.
- Remember that two or more users in the same domain should not use Domain Migration Administrator at the same time to migrate objects.
- Base your schedule on the throughput performance data collected in your test lab. Verify these performance numbers as you migrate your pilot groups in your production environment and adjust your schedule as needed.
- Include some buffer time for potential problems that may cause delays.
- Expect delays and surprises, such as users who are on vacation or out of the office when you scheduled to move them.
- Include time in your plan for existing server maintenance work that may take time away from the migration.
- Continue to use your test lab to work through potential issues that may arise during the migration.

- Consider how you will migrate remote or intermittently-connected users. These types of users and computers require specific plans to ensure their access is not interrupted.
- Include time for training, testing, and the actual migration tasks based on the number of objects you need to migrate.

Using the Product Most Effectively

Domain Migration Administrator and Server Consolidator provide a flexible environment to help you achieve the migration and consolidation results you need. Domain Migration Administrator provides projects to help you group and track objects through the migration process. You can also perform the individual migration tasks without creating projects. Both products provide a command-line interface to allow you to schedule migration and consolidation activities to meet your specific needs. This section provides several topics to help you understand these products and use them effectively. For more information about the command-line interfaces, see “Using the Command-Line Interface” on page 151.

Using Individual Tasks or Projects

Migration projects enable you to migrate and track sets of objects you want to handle in a similar way. You specify the objects, as well as the migration settings to use for those objects in the project. Then, as you migrate the objects from the source domain to the target domain, you can track the progress of the migration for the objects in that project. A project also limits the tasks to only those required to migrate the object types included in the project. If you have multiple source or target domains, you must use multiple projects.

Delegation Mode

Migration projects also support delegation mode, which allows you to delegate the project definition part of the migration process to multiple users. In delegation mode, a user *without* administrator permissions in the target domain can define and test the following parts of a project:

- Included objects
- Migration settings
- Modeling data

Once the migration project has been defined, the user can export the project and send the file name of the exported project to an administrator. Then, the administrator can import the project and perform the defined migration.

Renaming or Moving Objects

In migration projects, Domain Migration Administrator stores account-mapping information based on container path in Microsoft Windows. If your migration is not finished and you move or rename objects, your project information will not be up to date. This condition can cause problems during various migration tasks, such as security translation and password synchronization.

If you move or rename source objects after selecting them in a project and before migrating them, remove the objects from the project and then add them again.

If you move or rename source objects after migrating them, run the Refresh Migrated Objects report to refresh the Domain Migration Administrator mapping information, remove the objects from the project, and then add them again.

If you move or rename target objects created by Domain Migration Administrator, run the Refresh Migrated Objects report.

Customizing Your Migration Results

Domain Migration Administrator provides many options to allow you to customize your results for your specific needs. For example, you can add prefixes or suffixes to account names. You can also adjust groups during the migration process. In addition, you can use scripting and data modeling to further customize your migration and achieve the results you need.

Adding Prefixes and Suffixes

When you migrate accounts, you can specify options to add a prefix or suffix to each account you migrate. This option can help you track accounts as you move them from one domain to another. For example, you can prefix specific accounts with the source domain name, and later rename those accounts as needed.

Note

When using prefixes or suffixes, do not create account names longer than 20 characters. Domain Migration Administrator truncates longer account names by default to ensure the account names are compatible. For more information about naming conventions and conflict resolution, see “How Domain Migration Administrator Migrates User Accounts and Groups” on page 181.

Mapping and Merging Groups

Domain Migration Administrator allows you to merge groups, or map specific source groups to other target groups. This capability allows you to adjust group memberships during the migration process to create the target environment you need. For more information, see “How Domain Migration Administrator Merges and Maps Groups” on page 199.

Using Scripting

Domain Migration Administrator provides a flexible environment in which you can customize the migration process to meet your specific needs. You can write customized processing scripts. Domain Migration Administrator can then run these scripts when specific events occur during the migration process:

- Pre-migration events allow a script to check each user account, group, or computer and determine whether they should be migrated.
- Post-migration events allow you to set additional custom properties for an object after that object has been migrated to a Microsoft Windows domain.

Domain Migration Administrator supports both VBScript and JScript so you can leverage your existing expertise. For more information, see “Using Scripting” on page 141.

Data Modeling

Data modeling allows you to specify custom property values for objects before those values are set in the target domain. You can import information about your migration, and customize that information through data modeling. Then, Domain Migration Administrator can use that customized information to define objects in the target domain. This process gives you more detailed control of the migration process. For more information, see “Using Data Modeling” on page 144.

Notifying Users about Migrating

As you select various user accounts to migrate, notify users so they can be aware of the changes that may occur. Providing the following information to users can help them be prepared for the process:

- Expected migration schedule, including the following items:
 - Date the migration will occur
 - Date the users should log on to the new domain
 - When the old domain will be unavailable

- Instructions to help the users prepare their computers for the migration:
 - The users need to connect their laptops to the network. If they cannot connect to the network during the migration, they should schedule a time when their computers and user profiles can be migrated.
 - They should log off, but leave their computers turned on.
 - To migrate user profiles, the Domain Admins global group must be a member of the Administrators local group on each computer in the domain. Provide instructions to help the users verify that the Domain Admins group is a member of the Administrators local group on their computer.
- Brief description of the migration plan, including new log on domain and resource names.
- Any expected user account naming changes you have planned.
- If you are migrating passwords, how the users can get their new password.
- How to access printers, shares, and home directories in the new domain.

Migrating Objects and Verifying Results

When you perform a migration task, such as migrating a set of user accounts, you need to verify the results to ensure the task completed successfully. Detailed reporting and assessment of your environment, both before and after you perform a migration task, helps you ensure the results are what you expected. Consider the following methods for verifying the results of a migration task:

- After migrating user accounts, run Active Directory Users and Computers and verify that the accounts you migrated are in Active Directory. You can use ADSI Edit or the Active Directory Administration Tool (LDP) to verify that the SID History attribute is now populated. You can also check the Application event log to verify the SID History-related events.

Note

To read Domain Migration Administrator event log entries, view the Application event log from the computer on which Domain Migration Administrator is installed.

- After migrating groups, run Active Directory Users and Computers and verify that the groups you migrated are in Active Directory and they contain the user accounts you expect.
- After mapping and merging groups, run Active Directory Users and Computers and verify that the groups you migrated have the proper members.
- After renaming computers, run Server Manager in the source domain and verify that the computers are renamed.
- After migrating computers, run Active Directory Users and Computers and verify that the computers you migrated are in Active Directory.
- After translating security, test user accounts in the target domain and ensure they have access to the same resources that the associated user account in the source domain had.
- After synchronizing passwords, ensure you can log on to the target domain using the target user account and appropriate password.

- After running tasks that use agents, review the agent detail log in the agent monitor. Results are stored in the `DCTLog.txt` file in the system TEMP directory on the agent computer.
- While migrating objects or translating security, review the Migration Progress and Agent Progress windows and click **View Log** to review the log files. Domain Migration Administrator appends information to each log file when you perform migration tasks. After you finish performing a migration task, you can review the log files in the `Program Files\NetIQ\DMAN\Logs` folder. Security translation events are stored in the `DCTLog.txt` file in the system TEMP directory on the agent computer. After the agent dispatch is finished, you can access the agent details and view the log.
- If you made any changes to user accounts outside of Domain Migration Administrator, such as renaming the SAM account name or moving the account to a different OU, run the Refresh Migrated Objects report located in `Reports\Domain Status`. The Refresh Migrated Objects report compares the relative identifiers (RIDs) to the migrated account information in the database to see if they match. If the account information for those RIDs do not match the migrated account information in the migration database, the report updates the migration database with the correct information. The Refresh Migrated Objects report checks the RIDs of all migrated objects in the migration database, even if you run the report from a project. For more information about migration databases, see “Understanding the Domain Migration Administrator Databases” on page 227.
- Check the agent and migration logs and note any accounts that were not handled as you expected. Take corrective action on these accounts or consider removing them from this project and creating a separate project to handle these specific accounts.

Using the Migration Logs

Domain Migration Administrator and Server Consolidator provide several log files to help you track and review migration and consolidation activities. You can also use these log files to help resolve issues that arise:

ADCCollection.log

Includes entries for information collected when you run the Update Active Directory Connector Accounts wizard.

DCTI og. txt

Includes entries for agent-related activities that occur on a target computer, such as file security translation. Server Consolidator also adds entries to this log file. The log is stored on each target computer in the system TEMP directory.

Di spatch. l og

Includes entries for agent dispatcher-related activities, such as when an agent is installed and when the dispatcher has finished dispatching agents. This log is stored on the Domain Migration Administrator console computer in the Program Files\NetIQ\DMA\Logs directory.

I mport. l og

Includes entries for each step that Domain Migration Administrator performs while importing information from a . csv file. You can import lists of objects and associations from a . csv file to include those objects in migration projects and to allow you to translate security for objects migrated with a tool other than Domain Migration Administrator. This log is stored on the Domain Migration Administrator computer in the Program Files\NetIQ\DMA\Logs directory.

Mi grati on. l og

Includes entries for each step that Domain Migration Administrator performs during a migration task. The ADC Update function also creates entries in this log file. The log is stored on the Domain Migration Administrator console computer in the Program Files\NetIQ\DMA\Logs directory.

PropMap. l og

Includes entries for Active Directory schema mismatches that Domain Migration Administrator identifies between separate Microsoft Windows forests.

Trust. l og

Includes entries for information collected about trusts and their ages.

Domain Migration Administrator Error Codes

Domain Migration Administrator provides several error codes to help you identify potential issues. The following error codes identify general categories of events.

Error Code	Definition
I0	Information
W1	Warning
E2	Error
S3	Severe error
U5	Unrecoverable error

Server Consolidator Log Entries

Server Consolidator provides the following categories of log entries.

Marker	Categories of Log Entries
No marker	Matched files
C	Created files
U	Updated files

Adjusting Agent Error Logging Levels

You can increase the level of logging for the agent installed on target computers. These log entries are stored in the `DCT1 og.txt` file on the target computers. Since increased error logging can create large log files, you should increase the level of logging only during the testing phase of your migration, or while troubleshooting a specific issue.

To increase agent error logging to include file-level details:

1. Click **Domain Migration Administrator** in the left pane.
2. On the View menu, click **DMA Settings**.
3. Select **Log file-level detail of changes in security translation**.
4. Click **OK**.

Adjusting Server Consolidator Logging Levels

Server Consolidator provides several levels of error logging. These levels help you track the consolidation process at the detail level you need. If you increase the logging level, ensure the target computers where the agents are installed have enough disk space available for the larger log files.

The Migrate Files, Folders, and Shares wizard allows you to specify the appropriate level of logging. The following logging options are available on the Advanced Server Options window:

Errors only

Logs only the errors that Server Consolidator identifies during the transfer process.

Changed files only

Logs the errors that Server Consolidator identifies, as well as any files, folders, or shares that have changed since the previous transfer process.

Matched and changed files

Logs the errors that Server Consolidator identifies, as well as any files, folders, or shares that Server Consolidator previously transferred.

Chapter 3

Installing Domain Migration Administrator and Server Consolidator

Before installing Domain Migration Administrator and Server Consolidator, ensure your environment meets all requirements for these products. These requirements include trusts, DNS, and migration account permissions. For more information about the various requirements, see “Preparing Your Environment” on page 24.

Domain Migration Administrator and Server Consolidator also have specific hardware, software, and permission requirements. Carefully review the requirements in the following sections to ensure you have the required configuration to support the migration path you need.

Domain Migration Administrator Requirements

The following sections outline the requirements for running Domain Migration Administrator. For more information about supported migration scenarios, see “Identifying Your Migration Scenario” on page 10.

If you plan to use the SID History features of Domain Migration Administrator, Domain Migration Administrator has additional requirements. To use these features, review the additional requirements before you begin to install Domain Migration Administrator. For more information, see “Preparing to Migrate with SID History” on page 30 and “Considering Other Applications” on page 45.

Computers Running Domain Migration Administrator

The following table describes the minimum hardware and software requirements for the computer where you install Domain Migration Administrator.

Element	Requirements
Processor	Intel Pentium computer, 200 MHz or higher.
RAM	128 MB minimum (256 MB recommended). Memory requirements depend on the number and size of the objects you migrate at one time. Domain Migration Administrator requires 10 MB plus 4 KB for each account to be migrated.
Disk space	100 MB minimum. Domain Migration Administrator uses the disk space for log files during the migration process. <i>If you plan to install Microsoft SQL Server on the same computer with Domain Migration Administrator, ensure the computer has adequate disk space for both the SQL Server software and the Domain Migration Administrator databases. For more information, see “Database Requirements” on page 71 and the Microsoft SQL Server documentation.</i>

Element	Requirements
Operating system	<p>Any of the following:</p> <ul style="list-style-type: none"> • Microsoft Windows 7 (32-bit or 64-bit) • Microsoft Windows Server 2008 R2 • Microsoft Windows Server 2008 (32-bit or 64-bit) • Microsoft Windows Vista (32-bit or 64-bit) • Microsoft Windows XP Professional (32-bit or 64-bit) • Microsoft Windows Server 2003 R2 (32-bit or 64-bit) • Microsoft Windows Server 2003 Standard or Enterprise Edition (32-bit or 64-bit) • Microsoft Windows 2000 Advanced Server • Microsoft Windows 2000 Server • Microsoft Windows 2000 Professional Edition
Other software	<p><i>If you plan to install Microsoft SQL Server on the same computer with Domain Migration Administrator, ensure you install one of the supported SQL Server versions. For more information, see “Database Requirements” on page 71.</i></p>

Database Requirements

Domain Migration Administrator requires Microsoft SQL Server for its databases. You can run Microsoft SQL Server on the same computer as Domain Migration Administrator, or on a separate database computer. The following table describes the database requirements for Domain Migration Administrator.

Element	Requirements
Database software	<p>Either of the following:</p> <ul style="list-style-type: none"> • Microsoft SQL Server 2008 R2 (32-bit or 64-bit) • Microsoft SQL Server 2008 (32-bit or 64-bit) <p>Note: Each edition of Microsoft SQL Server has prerequisites you must install separately before you install SQL Server. For more information, see the Microsoft SQL Server documentation.</p>

Element	Requirements
Disk space	The Microsoft SQL Server databases that Domain Migration Administrator creates are relatively small, but SQL Server itself requires a significant amount of disk space. You also need more disk space if you plan to create multiple projects, since each project requires its own database. For more information about SQL Server space requirements, see the Microsoft SQL Server documentation.

Computers Running Agents

The following table describes the operating system and hardware requirements for computers running the Domain Migration Administrator agent. For more information about when agents are used, see “Agents” on page 178.

Element	Requirements
Processor	Intel Pentium computer
Disk space	15 MB minimum for the agent and agent log files
Operating system	<p>The agent computer must be running one of the following operating systems:</p> <ul style="list-style-type: none"> • Microsoft Windows 7 (32-bit or 64-bit) • Microsoft Windows Server 2008 R2 (32-bit or 64-bit) • Microsoft Windows Server 2008 (32-bit or 64-bit) • Microsoft Windows Vista (32-bit or 64-bit) • Microsoft Windows XP Professional (32-bit or 64-bit) • Microsoft Windows Server 2003 (32-bit or 64-bit) • Microsoft Windows 2000 Server • Microsoft Windows 2000

Agent computers must also meet the following requirements:

- The agent computer must be a valid member of a valid domain. Some computers may have expired passwords. If a computer has been disconnected from the domain for some time, its password may have expired.
- The user account you log on with when you run Domain Migration Administrator must have Administrator permissions on the agent computer.
- The `ADMIN$` share must exist to translate WTS or roaming profiles or to translate security.
- The size of the registry must be large enough to accommodate security translation. For information about increasing the size of your registry, see Microsoft Windows Help.
- The Remote Procedure Call (RPC) Locator and the Remote Registry services must be running.

In addition, NetBIOS should be enabled and the TCP/IP NetBIOS Helper service should be running on agent computers.

For more information about agent permission requirements, see “Understanding Agent Permissions” on page 158.

General Requirements

The following requirements apply when you use Domain Migration Administrator in all migration configurations:

- All domains or computers you plan to migrate must be online and available.
- You must have administrator rights for the objects you intend to migrate. For more information, see “Establishing Migration Credentials” on page 39.
- Your network must meet the minimum RPC communication requirements. For more information, see the RPC documentation.
- Administrative shares must be enabled on the computer where you install Domain Migration Administrator or its agents.

- Disconnect any mapped network drives between the source and target domain controllers to prevent credential conflict problems.
- Domain Migration Administrator migrates Mac files if the target volume is Mac-enabled before the migration.

Target-Specific Requirements

You must correctly configure your target domains to ensure the migration process is successful. For more information about the specific requirements and recommendations, see the following sections:

- “Considering Enterprise Environment Issues” on page 25
- “Setting Up a Clean Domain” on page 34
- “Preparing an Existing Target Domain” on page 36

Using SID History Features

When your target domain is a Microsoft Windows native mode domain and has access to the Global catalog, you can use the SID History features of Domain Migration Administrator. For more information about migrating with SID History, see “Understanding Access and Security Issues” on page 18. For more information about the SID History requirements, see “Preparing to Migrate with SID History” on page 30.

Permission Requirements for Domain Migration Administrator

The user account you use to log on when you run Domain Migration Administrator must have specific permissions to connect to SQL Server, as well as to ensure you can perform the migration tasks.

To connect to SQL Server, whether SQL Server is installed on the same computer with Domain Migration Administrator or on a separate computer, your account must have `db_owner` permissions for the SQL Server databases that Domain Migration Administrator creates. The easiest way to grant these permissions to the appropriate users is to add the users to the `ServerAdmin` role on the SQL Server database computer.

- *If you use Windows authentication to connect to SQL Server*, the Windows user account you use to run Domain Migration Administrator must have the `db_owner` role.
- *If you use SQL authentication to connect to SQL Server*, the SQL Server account you specify must have the `db_owner` role.

Domain Migration Administrator also prompts you for additional credentials for specific tasks, such as the tasks that require agents. For more information about the specific permission requirements for each task, see “Detailed Permission Requirements” on page 157. For more information about correctly setting your user account and agent account permissions, see “Establishing Migration Credentials” on page 39.

Firewall Considerations for Domain Migration Administrator

To migrate through a firewall, Domain Migration Administrator uses specific Microsoft APIs that require specific ports to be open. The port numbers are customizable and may vary depending on your operating system, security settings, and configuration requirements. At a minimum, the following table identifies the port numbers on the firewall that should be open during the migration.

Port Number	Protocol	Service
88	UDP	Kerberos
137-139	TCP and UDP	RPC locator
389	TCP	LDAP
445	UDP	Kerberos authentication
464	UDP	Kerberos password
3268	TCP	Global catalog

Objects that Domain Migration Administrator Migrates

Domain Migration Administrator can migrate the following types of objects:

- User accounts
- Security-enabled groups including the following groups:
 - Local groups
 - Domain local groups
 - Global groups
 - Universal groups (available only in Microsoft Windows 2000, Microsoft Windows Server 2003, and Microsoft Windows Server 2008 native mode)
- Computer accounts
- Well-known accounts, such as Domain Admins and Enterprise Admins

The objects you migrate with SID History information must also meet the following criteria:

- You cannot migrate built-in accounts, such as Administrator or Guest, with SID History. Because the SIDs of built-in accounts are identical in every domain, adding the SID of a built-in account to the SID History for another account would violate the SID-uniqueness requirement of the forest.
- The SIDs of the source objects must not already exist in the target forest, either as a primary account SID or in the SID History of an account.
- You cannot translate SID History for clustered share resources.

For more information, see “Translating Security for Accounts with SID History” on page 128.

Understanding Naming Limitations

Microsoft Windows does not support the following special characters in the name of most objects, including user accounts, groups, contacts, OUs, computers, common names (CN), and SAM account names. In addition to the special characters identified in the following table, you cannot use wildcard characters (*, ?, and #) in any names. Domain Migration Administrator migrates parentheses characters () in user names by setting the character to zero 0 in the downlevel logon name. For example, if you migrate a user named Henry(143) Domain Migration Administrator migrates the downlevel logon name to Henry01430.

Microsoft Windows	
Backslash	\
Comma	,
Double-quote	"
Equal sign	=
Forward slash	/
Semi-colon	;

Become familiar with Microsoft Windows property length limits. Any objects in Microsoft Windows domains with names over 65 characters can be problematic. For more information about special character and name length limitations, see your Microsoft Windows product documentation.

Note

Domain Migration Administrator supports object paths up to 1024 characters long. If the path to an object included in a migration is more than 1024 characters, such as objects in deeply-nested long-named OUs, Domain Migration Administrator may not function properly.

Server Consolidator Requirements

Server Consolidator allows you to move files, folders, shares, printers, local groups, and their access permissions from one server to another. The following sections describe the hardware, software, and permissions requirements for running Server Consolidator.

Hardware Requirements for Server Consolidator

The following table describes the hardware requirements for the computer where you install Server Consolidator.

Element	Requirements
Processor	Intel Pentium computer, 200 MHz or higher.
RAM	128 MB minimum (256 MB recommended). Memory requirements depend on the number and size of the files, folders, and shares you consolidate at one time.
Disk space	100 MB minimum on the source server and the target server. If Server Consolidator detects less than 100 MB of free space on the target server, it stops copying files. Hard disk requirements depend on the number and size of the files, folders, and shares you consolidate at one time. Server Consolidator uses the disk space for log files during the consolidation process.

Software Requirements for Server Consolidator

Server Consolidator has the following software configuration requirements:

- Server Consolidator must be installed on a computer running Microsoft Windows.
- The Server Consolidator agent must run on a Microsoft Windows computer.
- To consolidate files, the source and target computers must be running Microsoft Windows.
- When consolidating to a NetApp filer network appliance, the Server Consolidator agent must be running on a separate Windows computer.
- The ADMIN\$ share must exist on the source, target, and agent computers.

Permission Requirements for Server Consolidator

The user account you log on with when you run Server Consolidator must have specific permissions to ensure you can perform the consolidation tasks. Server Consolidator also prompts you for additional credentials for specific tasks, such as the tasks that require agents. For more information about permissions required for specific tasks, see “Server Consolidator Minimum Permissions” on page 173.

Licensing Considerations

Domain Migration Administrator and Server Consolidator provide a trial license that allows you to explore the various functions provided by each product. You can purchase a license to continue using the products after the trial license has expired. After purchasing a license, you need to upgrade from the trial license to the purchased license. For more information about upgrading a license, see “Upgrading Your License” on page 80.

Using a Trial License

A trial license enables Domain Migration Administrator and Server Consolidator to operate for a limited number of days from the initial installation. With this license, you can migrate up to 50 user accounts. When the trial license expires, Domain Migration Administrator and Server Consolidator display a trial license expiration message, and no longer start. If the 50-user limit has been reached, Domain Migration Administrator no longer migrates user accounts.

Viewing Your License Information

You can view information about your currently installed license. This information includes the expiration date, the number of accounts migrated, and the total number of accounts you are allowed to migrate.

To view your license information:

1. Click **Domain Migration Administrator** or **Server Consolidator** in the left pane of the main window.
2. On the View menu, click **About Domain Migration Administrator** or **About Server Consolidator**.

Upgrading Your License

A purchased license enables Domain Migration Administrator and Server Consolidator to operate within the license limits. Keep a backup copy of your license file in a separate directory.

To upgrade your license:

1. Copy the purchased license file to the `Program Files\NetIQ\DMA` folder.
2. Click **Domain Migration Administrator** or **Server Consolidator** in the left pane of the main window.
3. On the View menu, click **About Domain Migration Administrator** or **About Server Consolidator**.

4. Click **Upgrade License**.
5. Follow the instructions until you have finished installing the new license.

Upgrading Domain Migration Administrator and Server Consolidator

This version supports console and database upgrades only from Domain Migration Administrator 8.0. If you are using a pre-8.0 version of the product, ensure you complete any migrations started in that version and then uninstall that version before installing a newer version.

Note

Uninstalling a pre-8.0 version of Domain Migration Administrator does not remove the existing Microsoft Access databases. If you want to remove the Access databases, uninstall Domain Migration Administrator and then remove the Access databases manually.

Installing Domain Migration Administrator and Server Consolidator

Domain Migration Administrator and Server Consolidator provide one integrated setup program, which installs both products automatically. Domain Migration Administrator also offers a separate agent installer. For more information about the agent installer, see “Installing Agents Separately” on page 83.

Before you install Domain Migration Administrator and Server Consolidator, review the following planning and requirements sections:

- “Planning and Performing Your Migration” on page 9
- “Domain Migration Administrator Requirements” on page 69
- “Server Consolidator Requirements” on page 78

Note

Microsoft SQL Server is a prerequisite for Domain Migration Administrator, but the Domain Migration Administrator setup program does not install SQL Server. Domain Migration Administrator prompts you for the location of SQL Server the first time you launch the console after installation, so ensure you have already installed a supported version of SQL Server. For more information, see “Database Requirements” on page 71.

To install and start Domain Migration Administrator and Server Consolidator:

1. Run the **Setup.exe** file in the root folder of the Domain Migration Administrator installation kit.
2. Click **Begin Setup** on the Setup tab.
3. Follow the instructions until you have finished installing the products.
4. When you have successfully installed the products, start **Domain Migration Administrator** in the NetIQ Migration program folder.
5. In the Connect to Database window, specify the SQL Server computer name and database instance.
6. Specify whether to use Windows authentication or SQL Server authentication.
7. *If you specified SQL Server authentication*, provide the user name and password of an account with `db_owner` permissions on the Domain Migration Administrator database.
8. Click **OK**.

9. *If Domain Migration Administrator displays an error*, verify the SQL Server computer name and the user account credentials. Ensure the SQL Server computer is online and available.
10. *If connection to SQL Server is successful*, Domain Migration Administrator tries to detect a Protar database on the specified SQL Server instance and offers to create it for you. Click **Yes** and then click **OK**.

Installing Agents Separately

For some tasks, such as reporting, security translation, and computer migration, Domain Migration Administrator dispatches agents to remote computers on an as-needed basis. The agents perform the tasks and are uninstalled when the tasks are finished. However, Domain Migration Administrator also offers the option of installing permanent agents locally on computers. By deploying agents in advance you can avoid pushing them out temporarily over a limited bandwidth WAN.

To install an agent separately:

1. Using a local or domain administrator account, log on to the computer where you want to install the agent.
2. In the install package, locate the file named `NETIQDMAgent.exe`.
3. Follow the instructions in the setup program to finish installing the agent.

The agent installer installs the agent files in the following folder: `C:\Program Files\OnePointDomainAgent`.

Chapter 4

Consolidating Servers

There are many reasons companies need to consolidate files, folders, shares, and printers from one server to another:

- You have a large number of file servers running on older hardware that you would like to consolidate onto one faster server
- You have a number of member servers that you would like to convert to a cluster server configuration
- Your organization has merged with another and you need to restructure and streamline your network operations

Server Consolidator allows you to quickly move files, folders, shares, printers, and their access permissions from one server to another. This powerful capability allows you to centralize resources on a central server, such as a cluster server. Using the ActiveAgent technology, Server Consolidator efficiently handles the process by running the consolidation directly from the source computer.

You can independently consolidate files and folders, shares, or printers. In addition, you can choose from a number of options to handle naming conflicts. When you consolidate files and folders, you can choose whether to preserve the file and folder security descriptors.

Best Practices for a Smooth Consolidation

Before using Server Consolidator, be sure you are familiar with how it works and the related issues. For more information, see “Understanding How Server Consolidator Works” on page 217.

Starting Server Consolidator

When you install Server Consolidator, the installation program creates a shortcut in the NetIQ Migration program group. You can change the default location. The following steps indicate how to start Server Consolidator using the default program group.

To start Server Consolidator:

1. Click **Start** on the Windows taskbar.
2. Click **Programs > NetIQ Migration > Server Consolidator**.

Understanding the Server Consolidator Interface

Server Consolidator provides a Microsoft Management Console (MMC) interface. This interface is an MMC snap-in that provides an easy-to-use task pad and many standard MMC features.

Server Consolidator Task Pad

The Server Consolidator **console window** provides a left pane and a right pane. When you select **Server Consolidator** in the left pane, the MMC interface displays the Server Consolidator task pad in the right pane.

The task pad displays descriptions of each Server Consolidator task. To perform a task, click the icon for that task. Server Consolidator displays a wizard that guides you through the task.

Server Consolidator Wizards

Server Consolidator provides wizards to help you perform consolidation tasks. When you select a task in the right pane, Server Consolidator displays a wizard.

The wizards provide step-by-step direction about the consolidation task you are performing. Some windows provide detailed options to help you customize the task to meet your specific needs. To display additional information about an option on a window, click the **Help** button on that window.

Performing Consolidation Tasks

Server Consolidator has several requirements to ensure it can perform the required tasks. For more information about these requirements, see “Server Consolidator Requirements” on page 78.

Note

When you consolidate files, folders, shares, and printers from one server to another, you can specify options to control how Server Consolidator handles each object. To become familiar with the consolidation options and process, first consolidate a small number of files, folders, shares, or printers. Then, when you understand the options, consolidate the remaining objects.

If you have not already done so, start Server Consolidator. For more information, see “Starting Server Consolidator” on page 86.

Consolidating Files, Folders, and Shares

Before you migrate files, folders, or shares, you should understand the related options and interdependencies. For more information, see “How Server Consolidator Handles Files, Folders, and Shares” on page 218. If you are migrating to a NetApp filer, you must first add a registry key and edit the setting for the key. For more information, see “Preparing for NetApp Filer Consolidation” on page 88.

To migrate files, folders, and shares from one server to another server:

1. Click **Server Consolidator** in the left pane of the main window.
2. Click **Migrate Files, Folders, and Shares** in the right pane of the main window.
3. Follow the instructions until you have finished migrating the appropriate files, folders, and shares. For more information about an option, click **Help**.

When the consolidation process begins, Server Consolidator displays the Agent Monitor window. To monitor the agent activity on the server during the consolidation process, display the Server List tab. To view the status of the consolidation process, display the Summary tab. You can also view the log files to identify the actions Server Consolidator has performed.

Preparing for NetApp Filer Consolidation

You can use Server Consolidator to migrate files and folders to and from a NetApp filer storage appliance. To consolidate files and folders, you must first add a registry key and edit the setting for the key. After you create and edit the registry key, see “Copying Files, Folders, and Shares to Cluster Servers” on page 90.

Warning

Be careful when editing your Microsoft Windows registry. If there is an error in your Registry, your computer may become nonfunctional. Before you edit the registry, export a backup copy of the registry. Then, 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 Microsoft Windows Registry Editor.

To prepare for NetApp filer consolidation:

1. Start the Windows Registry Editor.
2. Expand **HKEY_LOCAL_MACHINE > SOFTWARE > NetIQ > DMA**.
3. Click **Edit** and select **New**.
4. Click **DWORD**.
5. Type **Ski pServerCheck** for the key name.
6. Click **Edit** and select **Modify**.
7. Type **1** for Value Data.
8. Click **OK**.
9. Close the Windows Registry Editor.

Disk Mirroring Using Server Consolidator

Server Consolidator allows you to back up your files, folders, and shares by copying these objects to a secure location. You can back up objects as needed, or you can save the migration options and schedule the backup process as a recurring event. A scheduled backup process provides many of the same benefits as disk mirroring. To schedule the backup process, use the Server Consolidator **SCCLI** command and the Windows Scheduler service to run your saved task. For more information, see “Using the Server Consolidator CLI” on page 154.

The first time Server Consolidator runs a saved task, the product copies all objects in the saved task to the target server. You can set subsequent backup tasks to copy only changed files to the target server, so Server Consolidator is able to complete the backup process in less time.

To back up your files, folders, and shares:

1. Click **Server Consolidator** in the left pane of the main window.
2. Click **Migrate Files, Folders, and Shares** in the right pane of the main window.
3. Click **Next**.

4. *If you want to back up your files, folders, and shares without scheduling the backup process*, complete the following steps:
 - a. Click **Migrate now** on the Test or Make Changes window.
 - b. Click **Next** and follow the instructions until you finish backing up your files, folders, and shares. For more information about an option, click **Help**.
5. *If you want to schedule the backup process*, complete the following steps:
 - a. Click **Save migration task and migrate later** on the Test or Make Changes window.
 - b. Click **Next** and follow the instructions until you finish selecting the options for the backup process and save the backup task. For more information about an option, click **Help**.
 - c. Use the SCCLI command to list your saved tasks. Identify the number of the backup task you want to schedule.
 - d. Use the Windows Scheduler service to run the SCCLI command when needed, identifying the number of the backup task with the /TASK option.
6. Verify the backed up files, folders, and shares.

Copying Files, Folders, and Shares to Cluster Servers

Server Consolidator can copy files, folders, and shares to stand-alone file servers or to cluster servers. Cluster servers allow you to balance your network load between servers in the cluster and they provide fault tolerance if any servers in the cluster fail. You must specify the group name of the cluster server in the wizard. For more information, see “How Server Consolidator Handles Cluster Servers” on page 220.

To copy files, folders, and shares to a cluster server:

1. Click **Server Consolidator** in the left pane of the main window.
2. Click **Migrate Files, Folders, and Shares** in the right pane of the main window.

3. On the Path Selection window, click **the target server is a cluster, so enable cluster options**.
4. Follow the instructions until you have finished migrating the desired files, folders, and shares. For more information about an option, click **Help**.

Consolidating Printers

Server Consolidator can migrate both local and network printers from one server to another. The process includes the printer port, print monitor, printer drivers, print queues, and printer shares. Server Consolidator creates a printer port on the target server when a printer connected to that port is migrated and the port is not currently installed on the target server. Server Consolidator uses the port name to match the printer to the correct port on the target server.

Server Consolidator migrates standard Microsoft Windows 2000 and Microsoft Windows 2003 printer monitors. If a printer requires a printer monitor that is not installed by Microsoft Windows 2000 or Microsoft Windows 2003, install the correct .dll files on the target server before you migrate the printer. The following table lists non-standard ports and their requirements.

Port	Printer	Requirement
Apple Talk	Apple Talk	Install Apple Talk protocol
HP network port	Printers that use older HP JetDirect adapters	Install DLC network protocol
LPR port	TCP/IP printers connected to a UNIX server	Install print services for Unix
Port for NetWare	NetWare printing resources	Install NWLink protocol and Client services for NetWare

Server Consolidator can migrate printers to or from individual computers in a cluster. However, this does not result in a fault-tolerant resource printer. For example, if *ClusterServer1* includes *\\Computer1* and *\\Computer2*, Server Consolidator can migrate printers to *\\Computer1* or *\\Computer2* but not to *ClusterServer1* as a managed cluster resource.

To migrate printers from one server to another server:

1. Click **Server Consolidator** in the left pane of the main window.
2. Click **Migrate Printers** in the right pane of the main window.
3. Follow the instructions until you have finished migrating the appropriate printers. For more information about an option, click **Help**.

When the consolidation process begins, Server Consolidator displays the Agent Monitor window. To monitor the agent activity on the server during the consolidation process, display the Server List tab. To view the status of the consolidation process, display the Summary tab.

Consolidating Local Groups

Microsoft Windows provide two types of local groups:

Machine local groups

Groups used only on the computer where they are created to control access to resources on that computer. These groups are stored in the security account manager (SAM) database on the computer where they are created.

Domain local groups

Groups used in the domain where they are created to control access to resources in that domain. Since all domain controllers share the same SAM database, these groups are stored in the SAM database on each domain controller in the domain where they are created.

When you migrate files, folders, and shares from one computer to another, you may need to migrate the machine local groups to provide the same access on the target computer. Then, you need to translate the security on the target computer to provide the same access for the migrated groups as the original groups had.

To migrate local groups:

1. Click **Server Consolidator** in the left pane of the main window.
2. Click **Migrate Machine Local Groups** in the right pane of the main window.
3. Follow the instructions until you have finished migrating the desired local groups. For more information about an option, click **Help**.

Translating Security and Access Settings

After you migrate files, folders, and shares from one computer to another, you may need to update permissions on the migrated objects to allow migrated user accounts and groups to access these objects. After you migrate machine local groups, you need to translate security on the target computer to provide the same access for the migrated groups as the original groups had. Translating security changes the access control list (ACL) on each file, folder, and share to reference the SID for the new, migrated account.

To translate security settings for migrated objects:

1. Click **Server Consolidator** in the left pane of the main window.
2. Click **Translate Local Security Settings** in the right pane of the main window.
3. Follow the instructions until you have finished translating the security settings. For more information about an option, click **Help**.

Generating Server Consolidator Reports

You can generate a report that lists all the tasks you have completed using Server Consolidator. The Reporting option generates a new report each time you select this option.

To generate a report for Server Consolidator tasks:

1. Click **Server Consolidator** in the left pane of the main window.
2. Click **Reporting** in the right pane of the main window.
3. View reports in the right pane of the window.

Using the CLI for Server Consolidator

The Server Consolidator command-line interface allows you to run saved consolidation tasks. The `SCCLI` command allows you to perform other activities. For example, you can use the Windows Scheduler service to schedule the `SCCLI` command to back up files to a backup server on a regular basis. You can also test and prepare tasks, and then run those tasks at a later time that is convenient for you. For more information, see “Using the Server Consolidator CLI” on page 154.

To use the CLI for Server Consolidator:

1. Click **Server Consolidator** in the left pane of the main window.
2. Click the consolidation task you want to perform using the CLI in the right pane of the main window.
3. Click **Next**.
4. Select **Save migration task and migrate later**.
5. Follow the instructions until you have finished translating the security settings. For more information about an option, click **Help**.
6. Use the Server Consolidator command-line interface to run the saved consolidation task. For more information, see “Using the Server Consolidator CLI” on page 154.

Chapter 5

Migrating with Projects

Domain Migration Administrator allows you to define migration projects and use these projects to perform and track migration tasks for manageable sets of objects. The project wizards guide you through the migration process and help you analyze the impact of specific portions of the process. You can specify different migration settings for each migration project. You can define specific migration settings to use for each set of objects identified by a project. Projects also enable you to use data modeling and further customize the property values set for the new objects in the target domain. For more information, see “Using Data Modeling” on page 144.

You can also delegate the project definition and preparation portion of the migration process. For example, you can allow someone to define the migration project for each department without allowing that individual to perform the migration itself. Then, you can import the project, verify the migration settings, and perform the actual migration. For more information, see “Delegating Migration Tasks” on page 111.

Domain Migration Administrator also allows you to perform individual migration tasks. If you are familiar with the tasks you need to perform and you do not need to define a limited set of objects to migrate, you can perform individual migration tasks without using projects. For more information, see “Performing Individual Migration Tasks” on page 119.

Starting Domain Migration Administrator

When you install Domain Migration Administrator, the installation program creates a shortcut in the NetIQ Migration program group. You can change the default location. The following steps indicate how to start Domain Migration Administrator using the default program group.

To start Domain Migration Administrator:

1. Click **Start** on the Windows taskbar.
2. Click **Programs > NetIQ Migration > Domain Migration Administrator**.

Understanding the Domain Migration Administrator Interface

Domain Migration Administrator provides a Microsoft Management Console (MMC) interface. The interface is an MMC snap-in that provides easy-to-use task pads and many standard MMC features.

Domain Migration Administrator Task Pads

The Domain Migration Administrator **console window** provides a left pane and a right pane. When you select a node in the left pane, Domain Migration Administrator displays the details for the selected node, such as the associated task pad or list of reports, in the right pane. For more information about the reporting interface, see “Understanding Reporting” on page 133.

Domain Migration Administrator provides task pads for two types of tasks:

Individual migration tasks

Allows you to perform individual migration tasks. If you are familiar with the tasks you need to perform and you do not need to define a limited set of objects to migrate, you can perform individual migration tasks without using projects. For more information, see “Performing Individual Migration Tasks” on page 119.

Project-based migration tasks

Allows you to perform tasks on defined sets of objects. You can specify migration settings and refine those settings to meet your specific needs. The project task pad identifies the migration tasks you need to perform, in the order you need to perform those tasks.

Project Task Pad

To use the project task pad, you must first create a migration project. To create a project, use the Create Migration Project wizard. Then, when you select the project in the left pane, Domain Migration Administrator displays the project task pad in the right pane.

The project task pad provides the following information areas:

Project Status

Displays summary information about the selected project, such as project name, dates, source and target domains, and number of objects selected and migrated. This area allows you to toggle Delegation mode on and off, based on your needs.

The project status area also displays a list of the migration tasks already performed. The migration history allows you to undo some migration tasks, if needed.

Project Tasks

Displays the migration tasks to perform for the objects selected in the project. The interface separates the tasks into the phases of the migration process and lists the tasks in the order you should perform them. When you click a task, Domain Migration Administrator runs the wizard for that task. Domain Migration Administrator displays only the tasks that apply to the objects selected in the project.

Domain Migration Administrator Wizards

Domain Migration Administrator provides wizards to help you perform migration tasks. When you select a task in the right pane, Domain Migration Administrator displays a wizard.

The wizards provide step-by-step direction about the migration task you are performing. Some windows provide detailed options to help you customize the migration task to meet your specific needs. To display additional information about an option on a window, click the **Help** button on that window.

Customizing the Project-Based Interface

The MMC interface lets you assemble tools, monitoring controls, World Wide Web pages, tasks, wizards, documentation, and other snap-ins into one console. You can then save your changes as an .msc file to preserve your custom console.

This feature lets you customize your interface by adding the tools you use, such as Active Directory Users and Computers and Domain Migration Administrator, into the same MMC console. With both of these tools in the same console, you can perform a migration task with Domain Migration Administrator and then quickly look at the results of the task in Active Directory Users and Computers. For more information about customizing the MMC interface, see the MMC Help.

Domain Migration Administrator provides additional support to let you customize the user interface to meet your specific needs. You can specify how the user interface displays accounts, as well as which accounts are displayed. You can also adjust several advanced options.

Modifying How Wizards Display Accounts

You can modify how the wizards display accounts on the Object Selection window in each wizard. You can view accounts organized in the following ways:

Flat view

Displays all available accounts in the source domain in one long list. This view organization is the default.

Organizational unit (OU)

Allows you to view accounts from each OU in a Microsoft Windows source domain.

To modify how wizards display accounts:

1. Click **Domain Migration Administrator** in the left pane of the main window.
2. On the View menu, click **DMA Settings**.
3. Select the appropriate view option.
4. Click **OK**.

Modifying which Accounts Wizards Display

You can modify which accounts the wizards display on the Object Selection window in each wizard. Since you can select and migrate only the accounts that Domain Migration Administrator displays in the wizards, these options help you simplify and customize the migration wizards. You can choose to display or hide the following types of accounts:

Previously migrated accounts

Displays previously migrated accounts in project-related wizards. By default, the project-related wizards display only unmigrated accounts. To remigrate one or more accounts, you must select this option, which displays both migrated and unmigrated accounts. Individual wizards not related to a project are not affected by this option. Those wizards always display all accounts in the source domain.

Well-known user accounts and groups

Displays well-known accounts in the wizards. If you want to migrate these special accounts using different migration options than when you migrate other accounts, you can hide these accounts while you select and migrate the other accounts. By default, all wizards display well-known user accounts and groups. For more information, see “Migrating Well-Known Accounts” on page 20.

Computer accounts for Microsoft Windows Servers

Displays computer accounts for only Microsoft Windows server computers. This option can reduce the number of computer accounts listed in the wizards by hiding accounts for workstations in the domain. By default, Domain Migration Administrator displays all computer accounts in the wizards, except domain controllers.

To modify which accounts the wizards display:

1. Click **Domain Migration Administrator** in the left pane of the main window.
2. On the View menu, click **DMA Settings**.
3. Select the appropriate check boxes for the accounts you want displayed.
4. Click **OK**.

Modifying Advanced Domain Migration Administrator Options

Domain Migration Administrator provides several additional options to allow you to further customize how it handles migrations. You can specify whether Domain Migration Administrator closes the Agent Monitor window after dispatching agents to perform an action for a CLI command. By keeping this window open, you can later review the status of the agents to determine how the migration task proceeded. You can also optimize migrations over slow WAN links by adjusting how agents send information back to the Domain Migration Administrator computer.

To adjust the advanced settings:

1. Click **Domain Migration Administrator** in the left pane of the main window.
2. On the View menu, click **DMA Advanced Settings**.

3. Select the appropriate options.
4. Click OK.

Performing Project Tasks

Projects allow you to migrate sets of objects and track the progress for those specific objects. Projects also enable you to use data modeling to further customize how the migrated object property values are set. Once you define a project, you can then perform the migration defined by that project. You can also export the project and allow a central domain administrator to import the project and perform the migration. For more information about these delegation-related tasks, see “Delegating Migration Tasks” on page 111.

Selecting Objects by Importing a CSV File

Domain Migration Administrator allows you to populate your projects from external sources by importing object information. You can export objects into a . csv file from an application, such as Configuration Assessor, or you can manually create a . csv file. Domain Migration Administrator supports some Configuration Assessor reports, such as the List of Users report.

The . csv file must be formatted as either ANSI or unicode and the first row of text in the file (header row) must contain the `SAMAccountName` keyword. The rest of the file lists one object SAM account name record per row. The text in your file should be similar to the following example:

```
SAMAccountName  
Administrator  
TestUser01  
TestUser02
```

Domain Migration Administrator provides a sample . csv file named `SampleImportObjects.csv` to illustrate the correct formatting. This file is located in the `Documentation` folder on the Domain Migration Administrator computer.

This formatting is valid only if you are using a .csv file to import objects that have not yet been migrated. The formatting requirements for .csv files used for adding objects migrated by a third-party tool such as ADMT are different because they map the source and target objects based on the `samAccountName` property. For more information, see “Importing Objects for Post-Migration Tasks” on page 125.

Notes

- When you import a .csv file into a project, the existing objects in the project are replaced with the objects in the .csv file.
 - To include computer accounts, type in the name of the computer followed by a dollar sign (\$). You can include computer accounts and user accounts in the same .csv file.
-

To import objects into a project:

1. Click the project in the left pane of the main window.
2. On the Action menu, click **Select objects using a CSV file**.
3. Select the .csv file that contains the objects you want to add to the project.
4. Click OK.

Defining a Migration Project

When you create a project, you specify which objects to include and the migration settings to use for that project. This part of the migration process allows you to specify the various options, such as user account, group, and computer account migration settings to use for the objects identified by that project.

To create a migration project:

1. Click **Domain Migration Administrator** in the left pane of the main window.
2. Click **Create Migration Project** in the right pane of the main window.
3. Follow the instructions until you have finished creating the project.
4. Click the newly-created project in the left pane of the main window.

5. *If you are defining the migration project and are not performing the migration,* set the delegation mode to **On**, which limits the tasks to only those required to define the project. To change the delegation mode from **Off** to **On**, click **Off** and then click **OK**.
6. Click **Select Objects** and follow the instructions until you have finished selecting the user accounts, groups, and computer accounts to include in the project. You can also import objects into the project. For more information, see “Selecting Objects by Importing a CSV File” on page 101.
7. Click **Specify Migration Settings** and follow the instructions until you have finished specifying the migration settings to use for that project.
8. Complete the **Preparing the Migration** tasks, in order. These tasks allow you to review the selected objects and the migration projects settings to ensure you have correctly defined the project. Some of the tasks for **Preparing the Migration** are defined as follows:

Reporting

Collects information from source and target domains, including the computers specified in the project. This information identifies the user accounts and groups referenced in file and share security descriptors on each computer. To collect this information, Domain Migration Administrator installs an agent on each computer specified in the computer options. After Domain Migration Administrator collects this information, you can view reports about potential migration issues, such as account naming conflicts.

Service Account Configuration

Allows you to collect and view service account information. You can select the Service Control Manager (SCM) entries you want to automatically update when a service account is migrated. During the user migration process, you can also specify whether you want any of the service accounts migrated.

Modeling: Import Data

Imports information about the objects you selected to migrate. To perform data modeling, check the data modeling option in the Select Objects wizard for the project. You must first import the data before you can perform other modeling tasks. For more information, see “Using Data Modeling” on page 144.

Modeling: Edit User Data

Allows you to specify settings for several user account properties when you migrate the user accounts to the target domain. By setting the user account properties, you can resolve potential migration conflicts. For example, you can resolve naming conflicts by providing different target user account names, which do not conflict with existing accounts in the target domain.

Modeling: Edit Group Data

Allows you to specify settings for several group properties when you migrate the groups to the target domain. By setting the group properties, you can resolve potential migration conflicts. For example, you can resolve naming conflicts by providing different target group names, which do not conflict with existing accounts in the target domain.

Modeling: Edit Computer Data

Allows you to specify settings for several computer account properties when you migrate the computer accounts to the target domain. By setting the computer account properties, you can resolve potential migration conflicts. For example, you can resolve naming conflicts by providing different target computer account names, which do not conflict with existing accounts in the target domain.

Note

To use data modeling when you perform user account, group, or computer account migration, select the **Migrate data using modeling database as source** check box in that specific migration wizard.

9. *If you are performing the migration you defined*, complete the **Performing the Migration** tasks, in order. The wizards guide you through each migration task. To perform the migration tasks, you must be an administrator in both the source and target domains.

Modifying a Migration Project

You can modify an existing project to change the objects and migration settings for that project. You should run Reporting after you modify the project and review the reports to ensure the migration project settings are correct. For example, Pre Migration check for Workstations report generate reports to check whether the computers you have selected for migration meet all the prerequisites for a successful migration.

To modify an existing migration project:

1. Click the appropriate migration project in the left pane of the main window.
2. Click the task in the right pane of the main window associated with the settings you want to modify.
3. Follow the instructions until you have finished specifying the objects and migration settings for that project.
4. Complete the **Preparing the Migration** tasks, in order. These tasks allow you to review the selected objects and the migration projects settings to ensure you have correctly defined the project. For example, **Reporting** collects information from the source and target domains, and then generates reports. For more information about these tasks, see “Defining a Migration Project” on page 102.

Note

To use data modeling when you perform user account, group, or computer account migration, select the **Migrate data using modeling database as source** check box in that specific migration wizard. For more information, see “Using Data Modeling” on page 144.

Refreshing Project Data

You can refresh project data to reflect changes to objects that occur during the course of a migration. You can refresh project data to reflect the correct location of objects that have moved in the source domain and delete objects from the project that have been deleted from the source domain.

To refresh project data:

1. Select the project you want to refresh in the left pane.
2. On the Action menu, click **Refresh Project Data**.
3. Select the objects to be moved or deleted on the Select Objects window.
4. Click **Add**, and then click **Refresh**. Domain Migration Administrator displays the number of objects deleted and moved in the Summary window.

Performing the Migration Defined in a Project

The project lists the tasks, in order, to perform the migration defined by the project settings. Perform each task, in the specified order. To perform the migration tasks, you must be an administrator in both the source and target domains.

To perform the migration defined in a project:

1. Click the appropriate migration project in the left pane of the main window.
2. Review the project information in the right pane of the main window.
3. Complete the **Preparing the Migration** tasks, in order. These tasks allow you to review the selected objects and the migration project settings to ensure the project is correctly defined. For example, **Reporting** collects information from the source and target domains, and then generates reports. For more information about these tasks, see “Creating Delegated Migration Projects” on page 114.

Note

To use data modeling when you perform user account, group, or computer account migration, check the **Migrate data using modeling database as source** check box in that specific migration wizard. For more information, see “Using Data Modeling” on page 144.

4. Complete the **Performing the Migration** tasks, in order. The wizards guide you through each migration task. Several migration tasks provide progress windows that allow you to view the migration logs. These logs help you track the changes made during each migration task.
5. Click **Reporting** to collect the information again and regenerate the reports. Then, review the reports that summarize the changes that were made, including the number of accounts that were successfully copied and the number of objects whose security settings were translated for the copied objects.

Synchronizing Migrated Objects

You can synchronize changes made to object attributes in the source domain with the target domain when you run the Synchronize Migrated Object wizard after migration.

To synchronize migrated objects:

1. In the left pane, select a project that has migrated objects.
2. In the right pane, select the **Synchronize Migrated Object** link.
3. Follow the instructions in the Object Synchronization wizard to synchronize the migrated objects. For more information, see “How Domain Migration Administrator Synchronizes Objects” on page 197.

Note

Domain Migration Administrator displays the **Synchronize Migrated Object** link only for projects that have migrated objects.

Deleting a Migration Project

You can delete an existing migration project. Domain Migration Administrator deletes the project and the associated migration settings. Once you delete a migration project, you cannot recover the migration settings specified in that project.

To delete a migration project:

1. Click the appropriate migration project in the left pane of the main window.
2. On the Action menu, click **Remove Project**.
3. Click **Yes** on the confirmation window.

Undoing User Account Migrations in Projects

You can undo migrations of selected user accounts using the Granular Undo Migration Tasks wizard. The wizard allows you to select the user account in the source and target domains that you previously migrated and want to delete. For more information about the issues to consider, see “How Domain Migration Administrator Handles the Undo Function” on page 215.

Notes

- You can undo only user account migrations using the Granular Undo wizard.
 - If you migrate a user account with a prefix or a suffix, and then undo the migration to move the object back to the source, the user account name shows the prefix or suffix and the target domain name in the suffix of the user account name.
-

To use the Granular Undo wizard:

1. Click the project name in the left pane of the main window.
2. Click **Granular Undo Migration Tasks** in the right pane of the main window.
3. Follow the instructions until you have finished undoing the appropriate migration operation. For more information about an option, click **Help**.

Using Reports

Reporting collects information and then generates reports that help you plan the migration process or analyze the results of the migration. These reports can be useful before, during, and after the migration.

You can generate and view one report at a time, or you can use the Reporting wizard to generate several different reports at once. When you select a single report that you have previously generated, Domain Migration Administrator displays the report. If you have not previously generated that report, Domain Migration Administrator allows you to generate and view that report. For more information, see “Understanding Reporting” on page 133 and “Performing Reporting Tasks” on page 138.

Chapter 6

Delegating Migration Tasks

Domain Migration Administrator lets you delegate the migration project definition. Defining the migration project includes selecting objects to include and specifying migration settings for these objects. Delegation allows users who may be more familiar with the objects being migrated in a specific location to define the migration projects for those objects. The users create and export the projects. Then, central domain administrators import the projects, verify the settings, and perform the migration.

Understanding the Delegation Interface

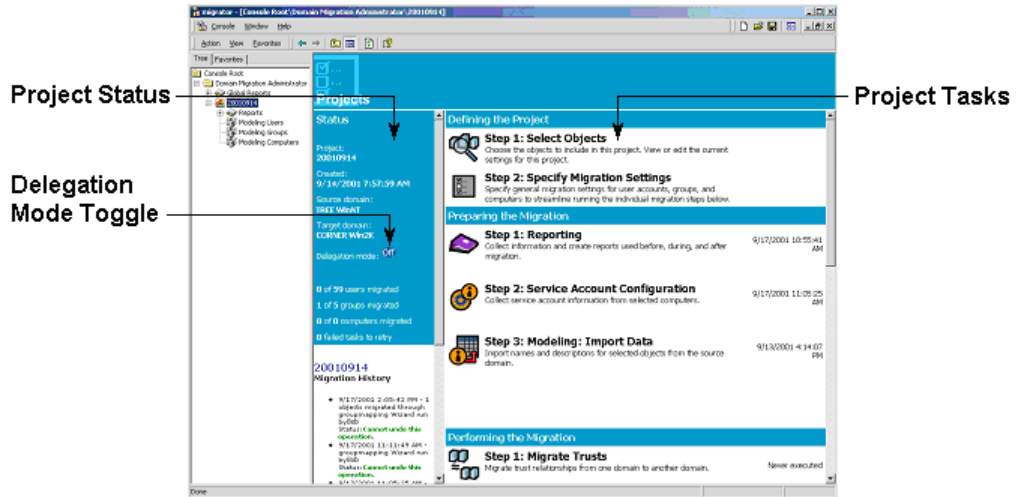
Domain Migration Administrator provides a Microsoft Management Console (MMC) interface. This interface is an MMC snap-in that provides easy-to-use task pads and many standard MMC features.

The Domain Migration Administrator **console window** provides a left pane and a right pane. When you select the Domain Migration Administrator node in the left pane, Domain Migration Administrator displays the individual migration tasks in the right pane.

To use delegation mode, you must first create a project using the Create Migration Project wizard.

Delegation Task Pad

After you create a migration project, or select an existing project in the left pane, Domain Migration Administrator displays the project task pad in the right pane. This task pad allows you to turn delegation mode on or off. To enable delegation mode, click **Off** in the Project Status area, and then click **OK**. The delegation mode indicator changes to **On**.



When delegation mode is on, the task pad displays the delegation tasks in the Project Tasks area. The interface separates the tasks into the phases of the migration process and lists the tasks in the order you should perform them. When you click a task, Domain Migration Administrator runs the wizard for that task. Domain Migration Administrator displays only the tasks that apply to the objects selected in the project. When defining a delegated migration project, perform all the tasks in **Defining the Project** and **Preparing the Migration** sections of the Project Tasks area.

After defining and preparing the project, export the project and notify a central domain administrator who will import it, verify it, and perform the actual migration. For more information about projects, see “Migrating with Projects” on page 95.

Delegation Wizards

Domain Migration Administrator provides many wizards to help you perform migration tasks. When you select a task in the right pane, Domain Migration Administrator displays a wizard.

The wizards provide step-by-step direction about the task you are performing. Some windows provide detailed options to help you customize the task to meet your specific needs. To display additional information about an option on a window, click **Help**.

Understanding Project Delegation

Administrators can use migration projects to delegate the project definition and preparation portion of the migration process. Then, administrators can use the defined migration projects to perform the migration in controlled stages. The following steps outline the general process for delegating the migration process. The sections after these steps provide more details about the steps identified in this general process.

To delegate the migration process:

1. The person responsible for defining and preparing the migration project completes the following tasks:
 - a. Create a migration project.
 - b. Set the delegation mode to **On**. The delegation mode controls which tasks are available in the project and lists only the tasks required to define and prepare the project.
 - c. Complete the **Defining the Migration** tasks, in order.
 - d. Complete the **Preparing the Migration** tasks, in order. These tasks allow you to review the settings to ensure the project is correctly defined.
 - e. Export the migration project to a backup file on the SQL Server computer.
 - f. Notify the administrator who will perform the migration that the migration project is ready, and the name of the exported project file.

2. The administrator responsible for performing the defined migration completes the following tasks:
 - a. Import the migration project from the exported project backup file.
 - b. Set the delegation mode to **Off**. When the delegation mode is **Off**, the project lists all the tasks required to perform the migration.
 - c. Complete the **Preparing the Migration** tasks, in order. These tasks allow you to review the settings to ensure the project is correctly defined.
 - d. Complete the **Performing the Migration** tasks, in order.
3. The administrator and the person who defined the migration project then verify the migration results.

Performing Delegation Tasks

The delegation tasks involve projects. You define the migration project, including selecting the appropriate objects and specifying the migration settings. Then, you export the project file and notify a central domain administrator of its file name. For more information about projects, see “Migrating with Projects” on page 95.

Creating Delegated Migration Projects

The first step is to create a migration project. Then, you complete steps to define and prepare for the migration.

To create a delegated migration project and prepare the migration:

1. Click **Domain Migration Administrator** in the left pane of the main window.
2. Click **Create Migration Project** in the right pane of the main window.
3. Follow the instructions in the wizard until you have finished creating the project.
4. Click the newly-created project in the left pane of the main window.

5. Set the delegation mode to **On**, which limits the tasks to only those required to define the project. To change the delegation mode from **Off** to **On**, click **Off** and then click **OK**.
6. Click **Select Objects** and follow the instructions until you have finished selecting the user accounts, groups, and computer accounts to include in the project. You can also import objects into the project. For more information, see “Selecting Objects by Importing a CSV File” on page 101.
7. Click **Specify Migration Settings** and follow the instructions until you have finished specifying the migration settings to use for the project.
8. Complete the **Preparing the Migration** tasks, in order. These tasks allow you to review the selected objects and the migration project settings to ensure you have correctly defined the project. Some of the tasks for **Preparing the Migration** are defined as follows:

Reporting

Collects information from source and target domains, including the computers specified in the project. The information identifies the user accounts and groups referenced in file and share security descriptors on each computer. To collect this information, Domain Migration Administrator installs an agent on each computer specified in the computer options. After Domain Migration Administrator collects this information, you can view reports about potential migration issues, such as account naming conflicts.

Service Account Configuration

Allows you to collect and view service account information. You can select which Service Control Manager (SCM) entries you want to automatically update when a service account is migrated. During the user migration process, you can also specify whether you want any of the service accounts migrated.

Modeling: Import Data

Imports information about the objects you selected to migrate. To perform data modeling, check the data modeling option in the Select Objects wizard for the project. You must first import the data before you can perform other modeling tasks. For more information, see “Using Data Modeling” on page 144.

Modeling: Edit User Data

Allows you to specify settings for several user account properties when you migrate the user accounts to the target domain. By setting the user account properties, you can resolve potential migration conflicts. For example, you can resolve naming conflicts by providing different target user account names, which do not conflict with existing accounts in the target domain.

Modeling: Edit Group Data

Allows you to specify settings for several group properties when you migrate the groups to the target domain. By setting the group properties, you can resolve potential migration conflicts. For example, you can resolve naming conflicts by providing different target group names, which do not conflict with existing accounts in the target domain.

Modeling: Edit Computer Data

Allows you to specify settings for several computer account properties when you migrate the computer accounts to the target domain. By setting the computer account properties, you can resolve potential migration conflicts. For example, you can resolve naming conflicts by providing different target computer account names, which do not conflict with existing accounts in the target domain.

Note

To use data modeling when you perform user account, group, or computer account migration, select the **Migrate data using modeling database as source** check box in that specific migration wizard.

9. When you have completed the **Preparing the Migration** tasks, export the project and notify a central domain administrator of its file name.

Exporting a Migration Project

After you define a migration project, you can export the project file to the SQL Server database computer. Then, an administrator can import that project and perform the migration defined by the project.

To export an existing migration project:

1. Click the appropriate migration project in the left pane of the main window.
2. On the Action menu, click **Export Project**.
3. Specify a file name for the exported project, such as `myproj . bak`. You can export the project using the default `. bak` file format, or you can use another format such as `. txt` or `. doc`. The exported project file is saved to the default SQL Server backup folder on the SQL Server computer.
4. Click **OK**.
5. Once the export succeeds, Domain Migration Administrator displays a confirmation message with the full path and file name of the exported file. Make a note of the file name so you can send this information to an administrator.

Importing a Migration Project

After a migration project is defined and exported to the SQL Server database computer, an administrator can import the project file and perform the migration defined by the project. To import a migration project, you need to create a project and import the settings into that new project.

To import a migration project:

1. Click **Domain Migration Administrator** in the left pane of the main window.
2. Click **Create a Migration Project** in the right pane of the main window.
3. Click **Next** on the Welcome window.
4. Click **Import**, and then click **Next**.
5. In the **Location** field, specify the file name of the exported project on the SQL Server computer. For example, `myproj . bak`. If you moved the exported project from the default SQL Server backup folder to a different folder, specify the full path. For example, `c: \DMAExports\myproj . bak`.
6. Click **Next**.

7. Specify the name for the project you are creating and into which you are importing the settings, and then click **Next**.
8. Review the summary information, and then click **Finish**.

After importing the project, you can perform the migration defined by that project. For more information, see “Performing the Migration Defined in a Project” on page 106.

Chapter 7

Performing Individual Migration Tasks

Domain Migration Administrator allows you to define migration projects, or you can perform individual migration tasks. The project wizards guide you through the migration process and help you analyze the impact of specific portions of the process. If you are familiar with the tasks you need to perform and you do not need to define a limited set of objects to migrate, you can perform individual migration tasks without using projects. For more information about migration projects, see “Migrating with Projects” on page 95.

Understanding the Task-Based Interface

Domain Migration Administrator provides a Microsoft Management Console (MMC) interface. The interface is an MMC snap-in that provides easy-to-use task pads and many standard MMC features.

Task-Based Task Pad

The Domain Migration Administrator **console window** provides a left pane and a right pane. When you select the Domain Migration Administrator node in the left pane, the MMC interface displays the task-based task pad in the right pane.

The task pad displays descriptions of each individual migration task. The tasks are listed in the order you usually use them. To perform a task on the objects in the source domain, click the icon for that task. Domain Migration Administrator displays a wizard that guides you through the task. Domain Migration Administrator does not save the selections you make for future uses of that task.

If you want to establish sets of objects and perform the migration tasks on those objects, Domain Migration Administrator provides migration projects. A project guides you through the migration tasks based on the objects you include in that project. Domain Migration Administrator also saves the settings so you can adjust and refine them to meet your specific needs. In addition, you can use project delegation and data modeling to further customize your migration process. For more information, see “Migrating with Projects” on page 95.

Individual Task Wizards

Domain Migration Administrator provides wizards to help you perform migration tasks. When you select a task in the right pane, Domain Migration Administrator displays a wizard.

The wizards provide step-by-step direction about the migration task you are performing. Some windows provide detailed options to help you customize the task to meet your specific needs. To display additional information about an option on a window, click **Help**.

Customizing the Task-Based Interface

The MMC interface lets you assemble tools, monitoring controls, World Wide Web pages, tasks, wizards, documentation, and other snap-ins into one console. You can then save your changes as an .msc file to preserve your custom console. For more information about customizing the MMC interface, see the MMC Help.

Domain Migration Administrator provides additional support to let you customize the user interface to meet your specific needs. You can specify how the user interface displays accounts, as well as which accounts are displayed. You can also adjust several advanced options. For more information, see “Customizing the Project-Based Interface” on page 98.

Performing Individual Tasks

Individual migration tasks apply to the objects in the specified in the source and target domains. If you want to define limited sets of objects, or specify migration settings that are saved and continue to refine those settings, you should use projects. For more information, see “Migrating with Projects” on page 95.

Generating and Viewing Reports

Reporting collects information and then generates reports that help you plan the migration process or analyze the results of the migration. These reports can be useful before, during, and after the migration.

You can generate and view one report at a time, or you can use the Reporting wizard to generate several different reports at once. When you select a single report that you have previously generated, Domain Migration Administrator displays the report. If you have not previously generated that report, Domain Migration Administrator allows you to generate and view that report. For more information, see “Understanding Reporting” on page 133 and “Performing Reporting Tasks” on page 138.

Migrating Trusts

Domain Migration Administrator allows you to migrate trust relationships from one domain to another domain. A trust relationship connects two or more domains and allows users in one domain to access resources in another domain. For more information about trusts and the related migration issues, see “How Domain Migration Administrator Migrates Trusts” on page 198.

To migrate trusts:

1. Click **Domain Migration Administrator** in the left pane of the main window.
2. Click **Migrate Trusts** in the right pane of the main window.
3. Follow the instructions until you have finished migrating the appropriate trusts. For more information about an option, click **Help**.

Setting Service Account Migration Options

The Service Account Migration wizard collects information about service accounts. Then, you can specify whether to include or skip each service account when you migrate other accounts. These settings apply to all migration tasks performed after you specify these service account settings. To handle service accounts in a different manner than the user accounts, groups, or computer accounts you select to migrate, run this task before you use other migration wizards. For more information about issues to consider, see “How Domain Migration Administrator Migrates Service Accounts” on page 195.

To set the service account migration options for all migration tasks:

1. Click **Domain Migration Administrator** in the left pane of the main window.
2. Click **Service Account Configuration** in the right pane of the main window.
3. Follow the instructions until you have finished setting the service account migration options. For more information about an option, click **Help**.

Mapping and Merging Groups

Domain Migration Administrator allows you to map one or more groups in one domain to a single group in another domain. This feature enables you to reduce duplicate groups during the migration process. Run this wizard once for each set of groups that you want to map to a single group in the target domain. For more information about the issues to consider, see “How Domain Migration Administrator Merges and Maps Groups” on page 199.

To map or merge groups from one domain to another domain:

1. Click **Domain Migration Administrator** in the left pane of the main window.
2. Click **Map and Merge Groups** in the right pane of the main window.
3. Follow the instructions until you have finished mapping or merging the appropriate groups. For more information about an option, click **Help**.

Migrating User Accounts

Domain Migration Administrator allows you to copy user accounts from one domain to another. When you migrate user accounts, you can also migrate the groups of which the user accounts are members. Domain Migration Administrator provides many options to help you migrate the user accounts and groups exactly as you need. For example, you can specify how Domain Migration Administrator handles the passwords for the copied user accounts. For more information about the issues to consider, see “How Domain Migration Administrator Migrates User Accounts and Groups” on page 181.

When copying passwords from Microsoft Windows native-mode domains to a Microsoft Windows domain in a different forest, Domain Migration Administrator uses a Password Export Server. For more information, see “Native-Mode Source Domain Password Migration” on page 235.

To migrate user accounts from one domain to another domain:

1. Click **Domain Migration Administrator** in the left pane of the main window.
2. Click **Migrate User Accounts** in the right pane of the main window.
3. Follow the instructions until you have finished migrating the appropriate user accounts. For more information about an option, click **Help**.

Warning

When you migrate user accounts and groups, Domain Migration Administrator creates all the accounts before copying the properties of those accounts. This process ensures Microsoft Windows accounts that reference the distinguished names of other Microsoft Windows objects in their properties, such as the Manager property, are correctly migrated.

For example, if UserA is the manager of UserB, and you migrate both accounts at the same time, UserA and UserB need to exist before Domain Migration Administrator can correctly set the Manager property of UserB. If you interrupt the migration process before it is finished, accounts may exist without the properties correctly set. Allow the migration process to finish completely.

Migrating Groups

Domain Migration Administrator allows you to copy groups from one domain to another. When you migrate groups, you can also migrate the user accounts that are members of those groups. Domain Migration Administrator provides many options to help you migrate the user accounts and groups exactly as you need. For more information about the issues to consider, see “How Domain Migration Administrator Migrates User Accounts and Groups” on page 181.

To migrate groups from one domain to another domain:

1. Click **Domain Migration Administrator** in the left pane of the main window.
2. Click **Migrate Groups** in the right pane of the main window.
3. Follow the instructions until you have finished migrating the appropriate groups. For more information about an option, click **Help**.

Renaming Computers

Domain Migration Administrator allows you to rename computers in a domain by renaming the computer accounts for those computers. Domain Migration Administrator also updates the computer to use the new name and allows you to restart the computer. For more information about the issues to consider, see “How Domain Migration Administrator Migrates and Renames Computers” on page 194.

To rename computers and the associated computer accounts:

1. Click **Domain Migration Administrator** in the left pane of the main window.
2. Click **Rename Workstation** in the right pane of the main window.
3. Follow the instructions until you have finished renaming the appropriate computers. For more information about an option, click **Help**.

Migrating Computer Accounts

Domain Migration Administrator allows you to change the domain membership for member server and workstation computers. Domain Migration Administrator copies the computer account from one domain to another domain. Then, Domain Migration Administrator changes the domain membership and restarts the migrated computer to make the change take effect. For more information about the issues to consider, see “How Domain Migration Administrator Migrates and Renames Computers” on page 194.

Note

To migrate a computer with dual operating systems, you must log on to each operating system on the computer to migrate the computer.

To migrate computer accounts and change domain membership:

1. Click **Domain Migration Administrator** in the left pane of the main window.
2. Click **Migrate Computers** in the right pane of the main window.
3. Follow the instructions until you have finished migrating the appropriate computer accounts. For more information about an option, click **Help**.

Importing Objects for Post-Migration Tasks

You can import a list of objects into the list of migrated objects stored in the Domain Migration Administrator database. Then, you can perform post-migration tasks on those objects, such as translating security. This feature allows you to resolve migration issues for accounts created in the target domain using tools other than Domain Migration Administrator.

You can export a list of objects into a . csv file from an application and modify the file so that it contains the required information, or you can manually create the . csv file. The file must be formatted as either ANSI or unicode and tab delimited.

The first row of text in the file (header row) must contain the following keywords:

- SourceDomain
- SourceSam

- SourceType
- TargetDomain
- TargetSam
- TargetType

The following table provides an example of correct formatting.

SourceDomain	SourceSam	SourceType	TargetDomain	TargetSam	TargetType
MYSOURCE	TestUser01	User	MYTARGET	TestUser01	User
MYSOURCE	TestUser02	User	MYTARGET	TestUser02	User

List one object per row in a tab-delimited format under the header row with the appropriate information for each field.

Note

Domain Migration Administrator provides a sample .csv file named SampleAccountMapping.csv to illustrate the correct formatting. This file is located in the Documentation folder on the Domain Migration Administrator computer.

To import a list of objects in the migrated objects table:

1. Click **Domain Migration Administrator** in the left pane of the main window.
2. On the Action menu, click **Import migrated objects from a CSV file**.
3. Select the .csv file that contains the objects you want to add to the migrated objects table.
4. Click **OK**.

Translating Security Access and Profiles

Domain Migration Administrator allows you to change file, folder, share, and printer security descriptors that reference one user account or group in a source domain to reference another user account or group with the same name in a target domain. You can also translate local group memberships, domain controller security policy, user profiles, and security for DCOM objects. Domain Migration Administrator provides many options to help you resolve the related security issues exactly as you need. For more information about the issues to consider, see “How Domain Migration Administrator Updates Access Control Entries” on page 200.

Note

Domain Migration Administrator can translate security only for shares on the active node.

To resolve related security issues:

1. Click **Domain Migration Administrator** in the left pane of the main window.
2. Click **Translate Security Settings** in the right pane of the main window.
3. Follow the instructions until you have finished resolving the related security issues. For more information about an option, click **Help**.

Synchronizing Passwords in Two Domains

Domain Migration Administrator allows you to synchronize the password of a migrated user account with the password of the user account in the source domain. The target user account must not be locked out. For more information about the issues to consider, see “How Domain Migration Administrator Synchronizes Passwords” on page 209.

To synchronize the password of a migrated user account:

1. Click **Domain Migration Administrator** in the left pane of the main window.
2. Click **Synchronize Passwords** in the right pane of the main window.
3. Follow the instructions until you have finished synchronizing the passwords. For more information about an option, click **Help**.

Translating Security for Accounts with SID History

After you migrate accounts with the SID History information, you need to translate the security only on the user profiles. SID History ensures the accounts have the same access as the original accounts. However, SID History information creates extra entries in your Global catalog, which increases the size of your Global catalog. Therefore, you may want to clean up this SID History information.

To clean up the SID History information, you *must* first resolve the security and access issues for the accounts with SID History information. This process is known as **translating security**. Then, after all file, folder, share, and printer security descriptors reference only the SID for the migrated account, you can remove the SID History information for all migrated accounts. For more information about the issues to consider, see “How Domain Migration Administrator Updates Access Control Entries” on page 200 and “How Domain Migration Administrator Handles SID History” on page 204.

Note

The Translate Security for Accounts with SID History wizard translates security only in **Replace** mode.

To resolve the security issues for accounts with SID History:

1. Click **Domain Migration Administrator** in the left pane of the main window.
2. Click **Translate Security for Accounts with SID History** in the right pane of the main window.
3. Follow the instructions until you have finished resolving the security issues for accounts with SID History property values. For more information about an option, click **Help**.

Removing SID History Values

After you resolve the security issues for the migrated accounts with SID History information, you can remove the SID History information.

Warning

To ensure the migrated accounts maintain the same access as the original accounts, you must first translate the security for the accounts with SID History before you remove the SID History values. If you remove the SID History values before translating security, the migrated accounts may no longer provide the needed access permissions.

To remove the SID History property values:

1. Click **Domain Migration Administrator** in the left pane of the main window.
2. Click **Remove SID History** in the right pane of the main window.
3. Follow the instructions until you have finished removing the SID History property values. For more information about an option, click **Help**.

Translating Security for NetApp Filers

After you migrate user accounts and groups, you may need to translate the security on network attached storage devices and mapped network drives. You need to modify the security descriptors that reference one user account or group in the source domain to reference another user account or group with the same name in the target domain. Domain Migration Administrator provides many options to help you resolve the related security access issues exactly as you need.

To resolve the security issues for NetApp filers:

1. Click **Domain Migration Administrator** in the left pane of the main window.
2. Click **Translate Security on NetApp Filers** in the right pane of the main window.
3. Follow the instructions until you have finished resolving the security issues for NetApp filers. For more information about an option, click **Help**.

Updating ADC Accounts

Microsoft Active Directory Connector (ADC) lets you create accounts in Active Directory of a domain and populate those accounts with Microsoft Exchange mailbox properties. When you use ADC, you can migrate some important information, such as phone number and address. When you copy mailbox information from your source organization to your target domain, a new account is created in your target domain. The new account has the same SAM account name as the alias of the source mailbox. If you are using Microsoft Exchange 2003 or later, ADC names the account *ADC_SeriesOfLetters*. Since the new account most likely has a different SID than the account associated with the source mailbox, the new account does not have the same permissions as the account associated with the source mailbox. The differing SAM account names also prevent Domain Migration Administrator from properly merging the ADC-created target accounts.

If ADC creates the target accounts in a disabled state, the Update Active Directory Connector Accounts wizard collects the mapping information about these accounts and identifies which source account is associated with each target account. The Update Active Directory Connector Accounts wizard allows you to use Domain Migration Administrator to complete your migration and resolve the issues ADC does not address:

- You can merge account properties, such as the **Password** property, from your source accounts into your ADC-created target accounts.
- You can enable the target account, translate user profiles, migrate the source account SAM account name, and update group memberships without overwriting the Active Directory properties already provided by ADC.

Note

If you migrate a local group from a Microsoft Windows mixed mode source server to a Microsoft Windows native mode target server, the group membership is automatically updated.

- You can update Active Directory accounts only for *intraforest* scenarios where ADC created the target accounts in a disabled state. Active Directory Connectors must agree between the sites in the same Microsoft Exchange organization.

- You can copy the SID of a source account into the SID History property of the associated target account. This process provides the target accounts with the same permissions as the source accounts. You must correctly prepare your source domain PDC before Domain Migration Administrator can populate the SID History property for the target accounts. For more information, see “Preparing Your Source Domains” on page 27. If a SID History configuration problem is found, Domain Migration Administrator stops the migration process.
- You can translate security for the new target accounts so they provide the same access permissions as the source accounts. Then, you can clean up the SID History information and maintain the correct access permissions.

The first time you run the wizard, Domain Migration Administrator collects information about your target accounts. If you run the wizard again, you can choose to collect new information or use previously collected information.

To merge properties from the source accounts to the ADC-created target accounts:

1. Click **Domain Migration Administrator** in the left pane of the main window.
2. Click **Update Active Directory Connector Accounts** in the right pane of the main window.
3. Click **Next** on the Welcome window.
4. Specify the name of the target domain that contains your ADC-created accounts, and then click **Next**.
5. Select **Yes, update the information**, and then click **Next**.
6. Select the domain of the mailbox owners for the original user accounts, and then click **Next**.
7. Select to skip or include user accounts to update, and then click **Next**.
8. Select all the options that apply on the ADC User Options window, and then click **Next**.

9. *If you selected to migrate SID information to the target domain*, the ADC Update wizard prompts you for account credentials with administrator permissions in the source and target domains. Specify the credentials, and then click **Next**.
10. Review the summary information, and then click **Finish**.

Retrying Failed Migration Tasks

Domain Migration Administrator installs agents to perform some migration tasks. If the agent cannot be successfully dispatched to perform a task, Domain Migration Administrator allows you to retry the failed task.

To retry a task involving an agent:

1. Click **Domain Migration Administrator** in the left pane of the main window.
2. Click **Retry Failed Tasks** in the right pane of the main window.
3. Follow the instructions until you have finished retrying tasks involving agents. For more information about an option, click **Help**.

Undoing Individual Migration Tasks

Domain Migration Administrator allows you to undo a previously performed migration operation. For more information about the issues to consider, see “How Domain Migration Administrator Handles the Undo Function” on page 215.

Note

To undo a user migration within a project, see “Undoing User Account Migrations in Projects” on page 108.

To undo a previously performed migration operation:

1. Click **Domain Migration Administrator** in the left pane of the main window.
2. Click **Undo Migration Task** in the right pane of the main window.
3. Follow the instructions until you have finished undoing the appropriate migration operation. For more information about an option, click **Help**.

Chapter 8

Understanding Reporting

The following table lists some of the available Domain Migration Administrator reports.

Category	Some Reports in this Category
Migration Tasks Performed	Action History Migrated Accounts Migrated Computers Objects Overlapping in Projects Migrated Service Accounts Translated Security Translated User Profiles
Disabled or Expired	Disabled Accounts Expired Accounts Expired Computers
Domain Status	Domain Trust Report Group Membership Last Logon Times Name Conflicts Recursive Group Membership Refresh Migrated Objects SID History

Category	Some Reports in this Category
Impact Analysis	Security References User Profiles Service Accounts
Tasks to Do	Migrated User Profiles not Translated Untranslated Security Unmigrated Service Accounts Unmigrated Computers Unmigrated Groups Unmigrated Users
Project Information	Failed Tasks Pre-Migration Check for Workstation Selected Computers Selected Groups Selected Users

Special Reports

Some reports are for specific situations to help you identify and address issues related to those situations. Consider the following reports:

SID History

Identifies all target domain accounts that have at least one SID in its SID History property. If you run the SID History report before migrating with Domain Migration Administrator, the migration database is populated with SID History from migrations that you may have previously performed. The overpopulated database can slow Domain Migration Administrator performance.

Refresh Migrated Objects

Updates previously migrated accounts whose target accounts have been moved or modified outside of Domain Migration Administrator. The Refresh Migrated Objects report requires time to execute. You should run the report only if you moved or renamed target domain accounts without using Domain Migration Administrator.

Understanding the Reporting Interface

Domain Migration Administrator allows you to view reports about your environment. Before you can view a report, Domain Migration Administrator must collect information and generate that report. You can generate and view one report at a time or you can run the Reporting wizard to collect information and generate multiple reports at one time. Once you have generated a report, run the Reporting wizard to update the information in that report.

Global and Project-Focused Reports

Domain Migration Administrator provides reports in the following sections of the user interface:

Global Reports

Reports in this section provide information about all the objects in the source domain.

Projects

Reports in a project provide information about only the objects included in that project. Each project provides reports focused on the objects in that project.

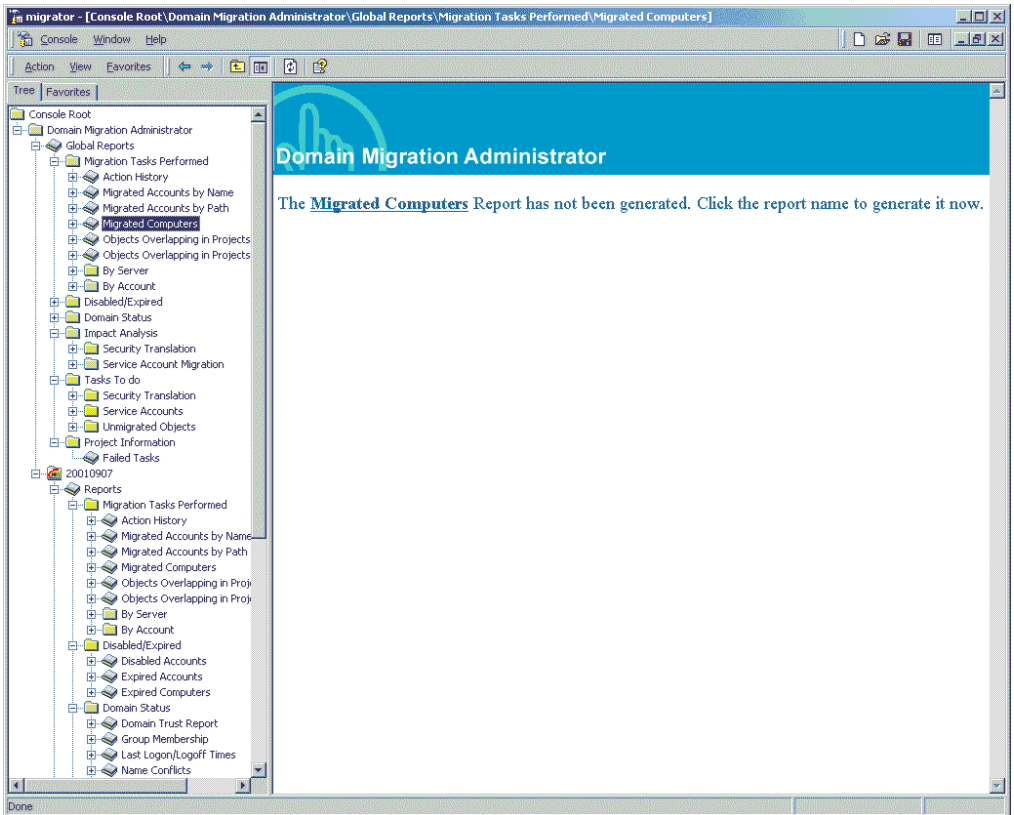
The following figure shows the reports available within a project.

The screenshot shows the 'migrator' console window. The left pane displays a tree view of reports under 'Domain Migration Administrator > 20010907 > Reports > Domain Status > Group Membership'. The main pane displays the 'netIQ' logo and a table titled 'Group Membership'.

Group Name	Member Name	Member Fullname	Member Type
DMAsportsAntoAZ	AlfonA57	Antonio Alfonseca	user
	AlmanA	Armando Almanza	user
	AmbroA33	Ashley Ambrose	user
	AndemWi16	Andem William	user
	AnderA96	Antonio Anderson	user
	AndertoDa14	Anderton Darren	user
	AngibeaDi8	Angibeaud Didier	user
	ArandaAr8	Aranda Aristides Rojas	user
	AranzabAg3	Aranzabal Agustin	user
	ArceFr2	Arce Francisco	user
	ArellanJe21	Arellano Jesus	user
	AristizVi15	Aristizabel Victor	user
	ArminFu6	Armin Fuad	user
	ArosMa16	Aros Mauricio	user
	AsadiAl15	Asadi Ali Akbar Ostad	user
	AsanoviAl7	Asanovic Aljosa	user
	AshbyA43	Andy Ashby	user
	AspeAl8	Aspe Alberto Garcia	user
	AsprillFa11	Asprilla Faustino	user
	AstradaLe15	Astrada Leonardo	user
	AugustiBr12	Augustine Brendan	user
	AyalaCe5	Ayala Celso	user
	AyalaRo2	Ayala Roberto	user
	AziziKh11	Azizi Khodadad	user
AzzouziRa16	Azzouzi Rachid	user	
BenesA40	Andy Benes	user	
BenitA49	Armando Benitez	user	

Generating and Viewing One Report

When you select a report that has not yet been generated, Domain Migration Administrator provides an option in the right pane to generate and display that report. For example, the following figure shows the Managed Computers report selected but not yet generated.



No Data to Report

Sometimes when Domain Migration Administrator collects information for a report, no objects meet the criteria or query for the report. For example, if you generate all reports before you migrate any objects, none of the migrated accounts reports have any objects to report. In this case, Domain Migration Administrator displays a message in the right pane indicating there is no data to report.

After you perform tasks that would cause objects to meet the criteria of the report, run the Reporting wizard to collect new information and generate the updated report.

Performing Reporting Tasks

Reporting collects information and then generates reports that help you plan the migration process or analyze the results of the migration. These reports can be useful before, during, and after the migration.

For example, the Disabled and Expired Accounts reports and the Last Logon/Logoff Times report can help you identify accounts you may want to delete before the migration. The Project Information reports help you identify which objects are included in a migration project. These reports are valuable when you need to review a project created in delegation mode by someone else. The Tasks to Do reports inform you which migration and translation tasks are not yet complete.

Generating and Updating Reports

You can generate and view one report at a time, or you can use the Reporting wizard to generate several different reports at once. When you select a report, Domain Migration Administrator displays the previously generated version of that report. To update previously generated reports, you need to run the Reporting wizard. For more information about generating and viewing one report, see “Viewing Reports” on page 139.

To generate or update reports using the Reporting wizard:

1. In the left pane, click **Domain Migration Administrator** or the appropriate project.
2. Click **Reporting** in the right pane.
3. Follow the instructions until you have finished generating the appropriate reports. For more information about an option, click **Help**.

Note

If you have a large number of user accounts, groups, or computers in your domain or project, generating all reports can require an extended period of time.

When the wizard has successfully completed collecting the information and generating the reports, click a report name to display that report in the right pane.

Viewing Reports

You can generate and view one report at a time, or you can use the Reporting wizard to generate several different reports at once. You may want to view one report without collecting information for multiple reports. Domain Migration Administrator provides this flexibility to collect only the information you need. For more information about generating several reports, see “Generating and Updating Reports” on page 138.






When you select a single report that you have previously generated, Domain Migration Administrator displays the report. If you have not previously generated that report, Domain Migration Administrator allows you to generate and view that report. Once you have generated a report, run the Reporting wizard to update the information in that report.

To view or generate one report:

1. In the left pane, expand the **Global Reports** item, or the **Reports** item under the appropriate project.
2. Navigate to the appropriate report and click the name of the report you want to view. Domain Migration Administrator displays the report in the right pane.
3. *If the report has not been previously generated*, click the report name link in the right pane to generate and display the report.

Navigating Reports

Domain Migration Administrator reports provide a navigation toolbar. The toolbar helps you navigate reports as described in the following table.

Icon or Toolbar Element	Description
	Click this icon to view the previous page of the report.
	Type a page number in the entry box and click Go to display the page.
	Displays the total number of pages in this report.
	Click this icon to view the next page of the report.
	Click this icon to print the report.

Chapter 9

Customizing the Migration Process

Domain Migration Administrator provides a powerful, flexible migration environment to enable you to achieve the specific results you need. You can customize your migration process using the options provided in the wizards. You can also use scripting and data modeling to further customize the process to ensure you get the results you need.

Using Scripting

Domain Migration Administrator provides a flexible environment that lets you customize the migration process to meet your specific needs. Domain Migration Administrator can run scripts that you supply either before or after an object is migrated. Domain Migration Administrator supports both VBScript and JScript so you can leverage your existing expertise.

Note

Domain Migration Administrator does not run scripts when you select **Test the migration settings and migrate later** on the Test or Make Changes window.

Scripting Objects

Domain Migration Administrator supports the following objects for scripts.

sourceObject	User account, group, or computer account defined in the source domain.
targetObject	User account, group, or computer account defined in the target domain. This object represents the migrated object in the target domain.
settings	Migration settings currently stored in the Domain Migration Administrator database. You can read (Get) these settings to perform some intelligent processing. You should not change the values.

For more information about methods and properties using the ADSI interface, see the ADSI documentation available from Microsoft.

Event Triggers

Domain Migration Administrator supports the following events for scripts:

- Pre-migration of a user account
- Pre-migration of a group
- Pre-migration of a computer account
- Post-migration of a user account
- Post-migration of a group
- Post-migration of a computer account

You can create and run scripts to perform additional or special tasks during the migration process. The following sample can help you understand how Domain Migration Administrator scripting works so that you can create scripts to meet your own special needs.

Example Script: Populating Active Directory from a Data Source

This sample script allows you to populate properties of migrated accounts in Active Directory from an external data source, such as a .csv file or an ODBC database. This sample script is written in VBScript and uses the ODBC OLE DB provider to request information from an ODBC-compliant data source. You need to modify the script to meet your specific needs, such as specifying the appropriate data source connection and the data SELECT statement, and run it as a post user migration (**User Post**) script.

This script demonstrates how to use a .csv file called `PropList.csv` as an external data source. The first line of the .csv file must provide Active Directory property names. The first property must be `objName`, which uniquely identifies each account. The `objName` property value must match the `samAccountName` property of the account. Then, each additional line in the .csv file provides the property values for the target accounts in Active Directory. After migrating a user, the script will populate user properties based on the values in the .csv file.

For example, the `PropList.csv` file could be similar to the following example:

```
objName, givenName, sn, telephoneNumber, streetAddress, L, st, postal Code
ashley, Ashley, Mueller, 713-555-1212, 5100 Carew St, Houston, Texas, 77096
frankw, Frank, West, 281-555-1212, 5200 Indigo St, Houston, Texas, 77096
janeg, Jane, Getz, 713-548-1700, 13939 NW Frwy, Houston, Texas, 77040
```

The following script reads the values in this `PropList.csv` file, and uses those values to populate the properties of the identified accounts in Active Directory.

```
' This script updates properties of accounts in Active Directory
' using values from an external data source, such as a CSV file.
```

```
Sub Process()
```

```
    Dim con
```

```
    Dim rs
```

```
    Dim name
```

```
    Dim fieldNum
```

```
    ' Get the name of the account being processed by DMA
    name = Settings.get("CopiedAccount.TargetSam")
```

```
    ' Open the connection to the data source
    Set con = CreateObject("ADODB.Connection")
```

```
    ' Open the data source.
```

```
    ' In this sample, the data source name is PropList.
```

```
    ' This ODBC data source identifies the PropList.csv file.
```

```

' You can change the following open connection call to connect
' to any OLE DB provider.
con.Open "DSN=PropList"

' Collect a recordset from the open data source.
' The following query provides a recordset from the data source.
' The first column name is objName, which uniquely identifies
' each account. The objName property value must match the
' samAccountName property of the account in the source domain.
' You can customize this SELECT statement for your specific
' data source table name and your OLE DB provider.
Set rs = con.Execute("Select * from PropList.csv")

' Search the recordset for the account being processed by DMA
rs.Filter = "objName = '" + name + "'"
rs.Requery
' If the record exists, update the account properties
' with the associated values in the recordset.
If (Not rs.EOF) Then
    For fieldNum = 1 To rs.Fields.Count - 1
        TargetObject.Put rs.Fields(fieldNum).name,
rs.Fields(fieldNum).Value
    Next
    TargetObject.SetInfo
End If
End Sub

```

Using Data Modeling

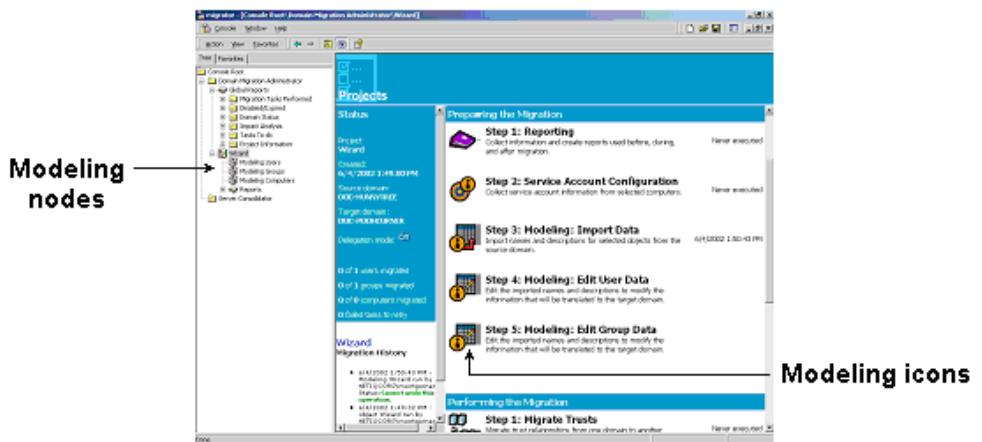
When you migrate objects from one domain to another, you may want to change some information for the objects in the new domain. For example, you may want to implement a new user account naming convention, or you may want to use different OUs to create your new hierarchical structure of user accounts, groups, or computers.

As you migrate user accounts, groups, and computers to the new domain, Domain Migration Administrator allows you to customize (model) specific properties of the objects you are migrating. You can use data modeling to customize your migration to achieve the results you need. For more information about how data modeling is implemented and supported, see “How Domain Migration Administrator Handles Data Modeling” on page 213.

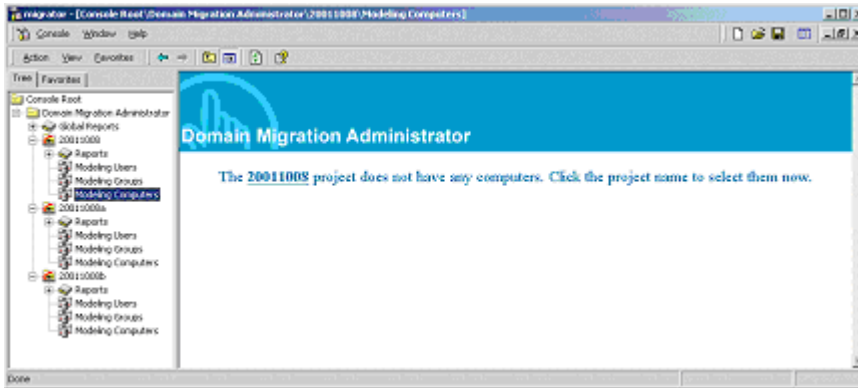
Understanding the Data Modeling Interface

To use data modeling, you must first create a project and select the user accounts, groups, and computers to include in the project. Then, you can run the **Modeling: Import Data** wizard to collect information about the user accounts, groups, and computers in the project.

After you import the modeling data, expand the project node in the left pane to display the data modeling nodes for user accounts, groups, and computers. To display a list of objects in the right pane, click a modeling node in the left pane as shown in the following figure.



If the project does not include any objects of the type you selected, the modeling interface displays a message as shown in the following figure.



This message allows you to run the **Select Objects** wizard again to add objects to the project, and then you can import the modeling data again.

Importing the Domain Migration Administrator Data

You must create a project and select objects to include in the project before you can import modeling data for those objects. When you import data, Domain Migration Administrator adds information about the objects in your project to the Domain Migration Administrator database. Domain Migration Administrator queries the source SAM or Active Directory to obtain the modeling attributes.

If you previously migrated a user account with Domain Migration Administrator, the Modeling: Import Data wizard overwrites most of the modeling fields for that account with data from the target account. You can run the Modeling: Import Data wizard to remigrate an account and keep the target OU, prefix, or suffix of that specific account.

To import data:

1. Create a project and select objects for that project.
2. Click the project name in the left pane of the main window.

3. Click **Step 3: Modeling: Import Data** in the right pane of the main window.
4. Follow the instructions until you have finished collecting the modeling data. For more information about an option, click **Help**.

Note

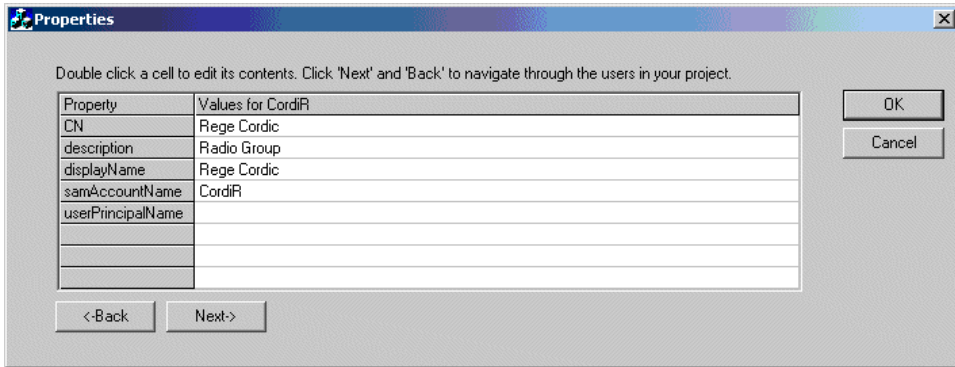
When you click **Finish** in the Import wizard, Domain Migration Administrator implements a locking mechanism on the database so only one user at a time can import data for a given project. Other users can continue to perform tasks in the same project on other computers, but they cannot import data for that project until the data import has completed. Since the data import process usually does not take long, the locking mechanism is designed to time out after a reasonable period to allow for scenarios such as server failures.

Changing the Properties of a Target Account

After you import data for objects in a project, you can change the values for some object properties, such as the target account name. Then, you can use the modified data during your migration to control the actual values assigned to properties for accounts in the target domain. Changing the value of a property in the modeling data does not change the target object until you migrate that object. In addition, you cannot use data modeling to change property values for source accounts.

To change the properties of a target account through modeling:

1. Import modeling data using the import wizard.
2. Expand the project node in the left pane of the main window to display the data modeling nodes for user accounts, groups, and computers.
3. Click a modeling node to display objects.
4. Click the account you want to change in the right pane of the main window.
5. On the Action menu, click **Edit Modeling Data**.



6. Double-click the value you want to edit. For example, to change the name of the target account, double click the **displayName** value.
7. *If you want to edit another account*, click **Back** or **Next**.
8. Click **OK** to close the Properties window.

Changing the Target OU for an Account

You can specify a target organizational unit (OU) for one or more accounts in a project. Data modeling allows you to specify an existing OU or create a new one. OUs created through data modeling are immediately created in the target domain. Objects specified for a target OU are not placed in that OU until you migrate those objects.

You can also use data modeling to delete an existing target OU. You cannot delete required containers, such as the Users container. OUs deleted through data modeling are immediately deleted in the target domain.

To specify a target OU for an account:

1. Import modeling data using the import wizard.
2. Expand the project node in the left pane of the main window to display the data modeling nodes for user accounts, groups, and computers.
3. Click a modeling node to display objects.

4. Select the accounts you want to change in the right pane of the main window. You can change the target OU for multiple accounts at the same time by selecting multiple accounts in the right pane of the main window.
5. On the Action menu, click **Update Target OU**.
6. *If you need to create a new OU*, complete the following steps:
 - a. Type a name for the OU in the text box.
 - b. Click **Create OU**.
7. Click a target OU to select it from the list.
8. Click **OK** to accept the change.

Scheduling Your Migration with the CLI

Domain Migration Administrator provides a command line interface (CLI). The CLI allows you to run migration projects through batch files and schedule them as needed. For more information, see “Using the Domain Migration Administrator Command-Line Interface” on page 151.

Domain Migration Administrator allows you to complete all the steps in a wizard and save it as a task to be performed at a later time. This is especially useful for if you want to schedule the migration task to run during off-peak hours.

To use the CLI for Domain Migration Administrator:

1. Click **Domain Migration Administrator** in the left pane of the main window.
2. Create a project for the migration task you want to use with the CLI.

3. Turn on Delegation Mode for the project by completing the following steps:
 - a. Expand **Domain Migration Administrator** in the left pane of the main window.
 - b. Select the project.
 - c. If Delegation mode in the right pane is set to **Off**, click **On**, and then click **OK**.
4. Complete the **Select Objects** and **Specify Migration Settings** wizards from the **Defining the Project** section of the Projects window.
5. Complete the **Migrate User Accounts** and **Migrate Groups** wizards from the **Performing the Migration** section of the Projects window.
6. Turn off Delegation Mode for the project.
7. Use the Domain Migration Administrator command-line interface to run the saved migration task. For more information, see “Using the Domain Migration Administrator Command-Line Interface” on page 151.

Appendix A

Using the Command-Line Interface

Both Domain Migration Administrator and Server Consolidator provide command-line interfaces (CLIs). The CLI for each product allows you to perform specific tasks. You can also use the Windows Task Scheduler to run saved tasks or perform migrations at specific times.

For example, you can use the Server Consolidator CLI to run a saved task that copies files, folders, shares, and their associated permissions to a backup server. The process ensures you have your data available if the primary computer fails. For more information, see “Disk Mirroring Using Server Consolidator” on page 89.

Using the Domain Migration Administrator Command-Line Interface

The Domain Migration Administrator command-line interface (CLI) allows you to perform saved migration tasks in migration projects. You can also perform other related actions, such as listing and removing tasks.

You can use the CLI and the Microsoft Windows scheduler to schedule various Domain Migration Administrator activities. This capability allows you to collect information and make changes at times that are convenient for you. You can also test a migration project, and then schedule the migration to be performed at a later time.

Syntax

DMACLI [*action*] [/PROJECT: *name*] [/TASK: *number*] [/WAIT] [/CREDENTIALS: *account*] [/P: *password*] [/?]

Options

action

Specifies one of the following actions to perform:

LISTPROJECTS	Lists the projects defined on this computer.
LISTTASKS	Lists the saved migration tasks for the project specified by the /PROJECT option.
REMOVETASK	Deletes the task specified by the /PROJECT and /TASK options from the task list.
RUNTASK	Performs the saved task specified by the /TASK option from the migration project specified by the /PROJECT option. This action requires the /TASK option.
SHOWTASK	Displays the summary text for the saved migration task specified by the /PROJECT and /TASK options.

/PROJECT: *name*

Specifies the name of a saved migration project. If the project name contains spaces, enclose the project name in double quotes (“”).

/TASK: *number*

Specifies the number of a saved task in the migration project specified by the /PROJECT option.

/WAIT

Directs Domain Migration Administrator to pause one minute after completing the specified task. Then, Domain Migration Administrator can perform another task through the command-line interface.

/CREDENTIALS: account

Specifies the user account to use to perform agent-related tasks that do not use the Local System account. For more information, see “Agents” on page 178. If you specify the RUNTASK action, you must specify the /CREDENTIALS and /P options. Specify this value in the following format:

domain\account

/P: password

Specifies the password associated with the user account specified by the /CREDENTIALS option. If you specify an asterisk (*), Domain Migration Administrator prompts you for the password. If you specify the RUNTASK action, you must specify the /CREDENTIALS and /P options.

/?

Displays this Help information.

Example 1

To display the names of the saved migration projects, enter:

```
DMACLI LISTPROJECTS
```

Example 2

To display the summary text for the third saved task in the Domain A to B project, enter:

```
DMACLI SHOWTASK /PROJECT: "Domain A to B" /TASK: 3
```

Example 3

To run the third saved task in the Test1 project using the DomainA\User account and prompting the user for the password, enter:

```
DMACLI RUNTASK /PROJECT: Test1 /TASK: 3 /CREDENTIALS: DomainA\User /P: *
```

Using the Server Consolidator CLI

Server Consolidator provides a command-line interface (CLI). This interface allows you to perform saved consolidation tasks. You can save consolidation tasks when you click **Save migration task and migrate later?** on a Server Consolidator wizard window. The Server Consolidator CLI also performs other related actions, such as listing, showing, and removing tasks.

You can use the Server Consolidator CLI and the Microsoft Windows scheduler to schedule Server Consolidator activities. This capability lets you collect information and prepare the task, and then run consolidation tasks at a time convenient for you.

Syntax

```
SCCLI [action] [/TASK: number] [/WAIT] [/CREDENTIALS: account] [/P: password] [/?]
```

Options

action

Specifies one of the following actions to perform:

LISTTASKS	Lists all saved consolidation tasks
REMOVETASK	Deletes the task specified by the /TASK option from the task list
RUNTASK	Performs the saved task specified by the /TASK option. This action requires the /TASK option
SHOWTASK	Displays the summary text for the saved migration task specified by the /TASK option

/TASK: *number*

Specifies the number of a saved task.

/WAIT

Directs Server Consolidator to pause one minute after completing the specified task. Server Consolidator can then perform another task through the command-line interface.

/CREDENTIALS: *account*

Specifies the user account to use to perform agent-related tasks that do not use the Local System account. If you specify the **RUNTASK** action, you must specify the **/CREDENTIALS** and **/P** options. Specify this value in the following format:

domain\account

/P: *password*

Specifies the password associated with the user account specified by the **/CREDENTIALS** option. If you specify an asterisk (*), Server Consolidator prompts you for the password. If you specify the **RUNTASK** action, you must specify the **/CREDENTIALS** and **/P** options.

/?

Displays this Help information.

Example 1

To display all the currently saved Server Consolidator tasks, enter:

```
SCCLI LI STTASKS
```

Example 2

To display the summary text for the saved task number 51, enter:

```
SCCLI SHOWTASK /TASK: 51
```

Example 3

To run a saved task using the `Domain\User` account and prompt the user for the password, enter:

```
SCCLI RUNTASK /TASK: number /CREDENTIALS: Domain\User /P: *
```

Appendix B

Detailed Permission Requirements

This section identifies the permission requirements for specific Domain Migration Administrator and Server Consolidator operations. Review these requirements and ensure your user account, and the credentials you provide during each task, have the appropriate permissions.

Domain Migration Administrator Minimum Permissions

Domain Migration Administrator has specific permission requirements for your user account. For some tasks, Domain Migration Administrator uses agents to provide better performance. During these tasks, you need to specify a user account and password, referred to as **credentials**, for the agent to use. These credentials also have specific permission requirements.

Understanding Agent Permissions

Domain Migration Administrator uses agents on remote computers to perform certain migration tasks. You can either install agents in advance to perform those tasks when needed, or you can allow Domain Migration Administrator to dispatch agents temporarily to remote computers to perform those tasks. When you perform a task that uses agents, Domain Migration Administrator prompts you for a user ID and password. Every agent task uses these credentials to write its results back to the Domain Migration Administrator computer. Some agent tasks also use these credentials to access computer resources. However, most agent tasks use the Local System account to access computer resources. For more information about how agents work, see “Agents” on page 178.

Note

Agent permission requirements are the same whether Domain Migration Administrator dispatches agents on an as-needed basis, or you use the agent installer to install agents on remote computers in advance.

Migration Tasks Performed Without Agents

The following migration tasks do *not* use agents:

- Migrating user accounts, groups, or service accounts.
- Migrating trusts
- Merging and mapping groups
- Synchronizing passwords
- Removing SID History
- Collecting information for many reports
- Updating ADC-created accounts

Migration Tasks Requiring Write Back Credentials

For the following tasks, Domain Migration Administrator deploys agents to remote computers:

- Gathering data for some detailed reports, such as impact analysis reports
- Collecting service account information for service account configuration
- Renaming computers
- Translating security for objects other than NetApp filers

For these tasks, Domain Migration Administrator prompts you for credentials with the following permissions to write the results back to the Domain Migration Administrator computer:

- **Log on locally** on the computer where the agent is deployed
- **Access this computer from the network** on the Domain Migration Administrator computer

Permission Requirements for Specific Tasks

The following sections identify specific tasks you can perform with Domain Migration Administrator. For each task, the section identifies the minimum permission requirements for the account you log on with when you perform the task, as well as the agent credentials:

- Configuring Service Account Migration
- Merging and Mapping Groups
- Migrating Trusts
- Migrating Microsoft Windows Computers
- Removing SID History
- Renaming Computers
- Reporting
- Retrying Failed Migration Tasks

- Synchronizing Passwords
- Translating Security
- Translating Security for Accounts with SID History
- Translating Security for NetApp Filers
- Undoing a Migration Task
- Updating ADC-Created Accounts
- Using Individual Tasks to Migrate Accounts
- Using Projects to Migrate Groups
- Using Projects to Migrate Service Accounts
- Using Projects to Migrate User Accounts
- Using Projects to Translate Security on Roaming Profiles

Configuring Service Account Migration

When you run the Service Account Configuration wizard, Domain Migration Administrator installs an agent on each selected computer to collect information about the services on that computer.

Security Context	Required Permissions
Your account in the source domain	Administrator permissions on the computers where agents are installed to collect data.
Your account in the target domain	Administrator permissions on the computers where agents are installed to collect data.
Agent credentials	<ul style="list-style-type: none"> • Log on locally on the computer where the agent is installed • Access this computer from the network on the Domain Migration Administrator computer

Merging and Mapping Groups

You can merge several source groups into a single target group. You can also map a source group to a specific target group.

Security Context	Required Permissions
Your account in the source domain	<ul style="list-style-type: none">• User, such as a member of the Users local group.• To migrate with SID History, you must have Migrate SID history permissions at a domain level in Active Directory.
Your account in the target domain	<ul style="list-style-type: none">• Full control on the target OU. If you are replacing an existing account, you also need Full control on the OU that contains the account being replaced.• To perform an intraforest migration to the domain located at the root of the forest, you must be a member of the Enterprise Admins group in that forest.• To migrate with SID History, you must have Migrate SID history permissions at a domain level in Active Directory.
Agent credentials	This task does not use an agent.

Migrating Trusts

Domain Migration Administrator allows you to migrate trusts from a source domain to a target domain. You can migrate trusts so that all domains trusted by the source domain are trusted by the target domain. You can also migrate trusts so that all domains that trust the source domain trust the target domain.

Security Context	Required Permissions
Your account in the source domain	<ul style="list-style-type: none">• Administrator permissions.• If you do not have Administrator permissions in a trusted or trusting domain for which you are migrating the trust, Domain Migration Administrator prompts you for credentials with Administrator permissions in that domain.
Your account in the target domain	<ul style="list-style-type: none">• Administrator permissions.• If you do not have Administrator permissions in a trusted or trusting domain for which you are migrating the trust, Domain Migration Administrator prompts you for credentials with Administrator permissions in that domain.
Agent credentials	This task does not use an agent.

Migrating Microsoft Windows Computers

When migrating Microsoft Windows computers, Domain Migration Administrator prompts you for credentials with permissions to write the results back to the Domain Migration Administrator computer and apply the change on the target computer.

Removing SID History

After you migrate accounts with SID History and resolve security-related issues, you can remove the SID History information from the target accounts.

Security Context	Required Permissions
Your account in the source domain	None. This task does not modify any source accounts.
Your account in the target domain	Full control on the accounts from which you are removing the SID History information.
Agent credentials	This task does not use an agent.

Renaming Computers

You can rename computers in one domain. Domain Migration Administrator deploys an agent to each computer it renames to perform the related tasks.

Security Context	Required Permissions
Your account in the source domain	Administrator permissions and full control on the OU that contains the computer account.
Your account in the target domain	None. This task does not apply to a target domain.
Agent credentials	<ul style="list-style-type: none">• Log on locally on the computer where the agent is deployed• Access this computer from the network on the Domain Migration Administrator computer

Reporting

For many reports, Domain Migration Administrator does not use agents to collect information. For some detailed reports, such as the impact analysis reports, Domain Migration Administrator deploys agents to computers to collect the information for those reports.

Security Context	Required Permissions
Your account in the source domain	<ul style="list-style-type: none">• User, such as a member of the Users group.• Administrator permissions on the computers where agents are installed to collect data.
Your account in the target domain	<ul style="list-style-type: none">• User, such as a member of the Users group.• Administrator permissions on the computers where agents are installed to collect data.
Agent credentials	If Domain Migration Administrator needs to use an agent, the agent credentials must have the following permissions: <ul style="list-style-type: none">• Log on locally on the computer where the agent is deployed• Access this computer from the network on the Domain Migration Administrator computer

Retrying Failed Migration Tasks

To retry a failed migration task, you need the same permissions that were required for the original task in both the source and target domains.

Security Context	Required Permissions
Your account in the source domain	Same permissions that were required for the original migration task.
Your account in the target domain	Same permissions that were required for the original migration task.
Agent credentials	Same agent credentials that were required for the original migration task.

Synchronizing Passwords

You can synchronize passwords for two associated accounts in different domains.

Security Context	Required Permissions
Your account in the source domain	Administrator permissions.
Your account in the target domain	Full control on the target accounts.
Agent credentials	This task does not use an agent.

Translating Security

To translate security for files, folders, and shares on a computer, Domain Migration Administrator deploys an agent to that computer. The permission requirements in this section do not apply when translating security for NetApp filers.

Security Context	Required Permissions
Your account in the source domain	<ul style="list-style-type: none">• User, such as a member of the Users local group.• Administrator permissions on the computers where you are translating security.
Your account in the target domain	<ul style="list-style-type: none">• User, such as a member of the Users local group.• Administrator permissions on the computers where you are translating security.
Agent credentials	<ul style="list-style-type: none">• Log on locally on the computer where the agent is deployed• Access this computer from the network on the Domain Migration Administrator computer

Translating Security for Accounts with SID History

When you run the Translate Security for Accounts with SID History wizard, Domain Migration Administrator processes ACLs that contain SIDs of accounts that were migrated with SID History. Domain Migration Administrator replaces source account SIDs in ACLs on selected computers with the SIDs of the associated target accounts.

Security Context	Required Permissions
Your account in the source domain	<ul style="list-style-type: none">• User, such as a member of the Users local group, in all source domains referenced by SID History entries.• Administrator permissions on the computers where you are translating security.• Migrate SID History on the computers where you are translating security.
Your account in the target domain	<ul style="list-style-type: none">• User, such as a member of the Users local group, in all target domains containing accounts being processed.• Administrator permissions on the computers where you are translating security.
Agent credentials	<ul style="list-style-type: none">• Log on locally on the computer where the agent is deployed• Access this computer from the network on the Domain Migration Administrator computer

Translating Security for NetApp Filers

To translate security for NetApp filers, Domain Migration Administrator deploys an agent to a computer from which it can access the NetApp filer. The agent needs to access both the computer and the NetApp filer. Domain Migration Administrator prompts you for credentials with permissions to write the results back to the Domain Migration Administrator computer and to apply the changes on the NetApp filer.

Security Context	Required Permissions
Your account in the source domain	Administrator permissions on the computer where Domain Migration Administrator deploys the agent to access the NetApp filer.
Your account in the target domain	Administrator permissions on the computer where Domain Migration Administrator deploys the agent to access the NetApp filer.
Agent credentials	<ul style="list-style-type: none">• Log on locally on the computer where the agent is deployed• Access this computer from the network on the Domain Migration Administrator computer• Administrator permissions on the NetApp filer

Undoing a Migration Task

To undo a migration task, you need the same permissions that were required for the original task in both the source and target domains. For example, to migrate a computer you need Administrator permissions on that computer. To undo the computer migration, you need Administrator permissions on the migrated computer. Since migrating a computer to a new domain removes the Domain Admins group for the source domain from the Administrators local group on that computer, you may no longer have Administrator permissions on that computer.

Security Context	Required Permissions
Your account in the source domain	Same permissions that were required for the original task.
Your account in the target domain	Same permissions that were required for the original task.
Agent credentials	Same agent credentials that were required for the original migration task.

Updating ADC-Created Accounts

When you update accounts created by the Microsoft Active Directory Connector, you can set several properties. The permissions you need depend on the properties you set.

Security Context	Required Permissions
Your account in the source domain	<ul style="list-style-type: none">• To copy passwords when updating these accounts, you need Administrator permissions.• To set SID History when updating these accounts, Domain Migration Administrator prompts you for credentials with Administrator permissions.• To copy properties other than passwords, you need to be a User, such as a member of the Users group.
Your account in the target domain	<ul style="list-style-type: none">• To copy passwords, enable accounts, or copy properties, you need Full control on the target accounts.• To set SID History when updating these accounts, you must be a member of the Domain Admins group.
Agent credentials	This task does not use an agent.

Using Individual Tasks to Migrate Accounts

When you migrate user accounts, groups, or service accounts through individual migration tasks, without using projects, Domain Migration Administrator requires you to have specific permissions in the source and target domains. Projects allow you to perform some of these tasks with fewer permissions.

Security Context	Required Permissions
Your account in the source domain	Administrator permissions.
Your account in the target domain	<ul style="list-style-type: none">• Administrator permissions.• To perform an intraforest migration to the domain located at the root of the forest, you must be a member of the Enterprise Admins group in that forest.
Agent credentials	This task does not use an agent.

Using Projects to Migrate Groups

When you migrate groups through projects, Domain Migration Administrator requires you to have specific permissions in the source and target domains.

Security Context	Required Permissions
Your account in the source domain	<ul style="list-style-type: none">• User, such as a member of the Users local group.• To migrate with SID History, you must have Migrate SID history permissions at a domain level in Active Directory.
Your account in the target domain	<ul style="list-style-type: none">• Full control on the target OU. If you are replacing an existing account, you also need Full control on the OU that contains the account being replaced.• To perform an intraforest migration to the domain located at the root of the forest, you must be a member of the Enterprise Admins group in that forest.• To migrate with SID History, you must have Migrate SID history permissions at a domain level in Active Directory.
Agent credentials	This task does not use an agent.

Using Projects to Migrate Service Accounts

When you migrate service accounts through projects, Domain Migration Administrator requires you to have specific permissions.

Security Context	Required Permissions
Your account in the source domain	Administrator permissions on the computers where you are updating the services.
Your account in the target domain	Administrator permissions on the computers where you are updating the services.
Agent credentials	This task does not use an agent.

Using Projects to Migrate User Accounts

When you migrate user accounts through projects, Domain Migration Administrator requires you to have specific permissions in the source and target domains.

Security Context	Required Permissions
Your account in the source domain	<ul style="list-style-type: none">• User, such as a member of the Users group.• To disable or expire Microsoft Windows source accounts during the migration, you need permissions to set the expiration date and disabled property of the source account.• To copy passwords during the migration, you need Administrator permissions.• To migrate with SID History, you must have Migrate SID history permissions at a domain level in Active Directory.
Your account in the target domain	<ul style="list-style-type: none">• Full control on the target OU. If you are replacing an existing account, you also need Full control on the OU that contains the account being replaced.• To perform an intraforest migration to the domain located at the root of the forest, you must be a member of the Enterprise Admins group in that forest.• To migrate with SID History, you must have Migrate SID history permissions at a domain level in Active Directory.
Agent credentials	This task does not use an agent.

Using Projects to Translate Security on Roaming Profiles

While migrating user accounts, you can translate security on the roaming profiles for those user accounts.

Security Context	Required Permissions
Your account in the source domain	Administrator permissions on the computer where the roaming profiles are stored.
Your account in the target domain	Administrator permissions on the computer where the roaming profiles are stored.
Agent credentials	This task does not use an agent.

Server Consolidator Minimum Permissions

The following sections identify specific tasks you can perform with Server Consolidator. For each task, the section identifies the minimum permission requirements for the account you log on with when you perform the task.

For some consolidation tasks, Server Consolidator deploys agents to remote computers to perform those tasks, or uses agents that you installed on those remote computers. When you perform a task that uses agents, Server Consolidator prompts you for a user ID and password, referred to as **credentials**. The agents use these credentials in many cases to access computer resources. In some cases, the agents use the Local System account to access computer resources.

Note

Agent permission requirements are the same whether Server Consolidator deploys agents on an as-needed basis, or you use the agent installer to install agents on remote computers in advance.

Copying Files, Folders, and Shares

When you copy files, folders, or shares, you specify where to deploy an agent to perform the task.

Security Context	Required Permissions
Your account on the source computer	Administrator permissions on the computer where you choose to deploy the agent.
Your account on the target computer	Administrator permissions on the computer where you choose to deploy the agent.
Agent credentials	Administrator permissions on the source and target computers.

Copying Printers

When you copy printers, Server Consolidator deploys an agent to the source computer.

Security Context	Required Permissions
Your account on the source computer	Administrator permissions on the source computer.
Your account on the target computer	Administrator permissions on the target computer.
Agent credentials	Administrator permissions on the source and target computers.

Migrating Local Groups

After you copy files, folders, and shares, you may need to migrate local groups from the source computer to the target computer to ensure you provide the same access to the copied objects.

Security Context	Required Permissions
Your account on the source computer	User, such as a member of the Users local group.
Your account on the target computer	Administrator permissions.
Agent credentials	This task does not use an agent.

Translating Security for Local Groups

To translate security for local groups from one computer to another computer, the product deploys an agent to that computer.

Security Context	Required Permissions
Your account on the source computer	Administrator permissions on the computers where you are translating security for local groups.
Your account on the target computer	Administrator permissions on the computers where you are translating security for local groups.
Agent credentials	<ul style="list-style-type: none">• Log on locally on the computer where the agent is deployed• Access this computer from the network on the Server Consolidator computer

Appendix C

Understanding How Domain Migration Administrator Works

Domain Migration Administrator provides a powerful architecture to help you migrate objects quickly and effectively. Domain Migration Administrator handles each type of object in a specific way to address migration issues related to those objects. You should understand the architecture and how Domain Migration Administrator handles each object type during the migration process.

This section provides technical details about how Domain Migration Administrator handles specific types of objects during the migration tasks. This information can help you understand the product and improve your migration process and results.

Understanding the Domain Migration Administrator Architecture

The setup program installs Domain Migration Administrator on one computer, referred to as the **console computer**. You perform all the migration tasks from the console computer. To perform some tasks, Domain Migration Administrator dispatches agents to remote computers.

Console Computer

The console computer provides a powerful, wizard-driven user interface. The wizards guide you through various migration tasks. If you are migrating with SID History, the console computer must be a domain controller in the target domain or a Microsoft Windows computer in the target domain. Domain Migration Administrator connects to the source and target domains to copy and write account information during the migration process.

Microsoft SQL Server Databases

Domain Migration Administrator uses Microsoft SQL Server databases to configure, manage, and track all migration project information. You can install SQL Server on the same computer as Domain Migration Administrator, or on a separate computer, as appropriate for your environment. A single SQL Server installation can support multiple Domain Migration Administrator consoles, allowing distributed deployment of Domain Migration Administrator across large enterprises. For more information about SQL Server supported versions and requirements, see “Database Requirements” on page 71. For more information about the databases Domain Migration Administrator uses, see “Locating the Databases” on page 228.

Agents

For some tasks, such as reporting, security translation, and computer migration, Domain Migration Administrator uses agents on remote computers. These agents enable Domain Migration Administrator to process many computers at the same time, which improves the speed of your migration. The agents also reduce network bandwidth requirements, especially for security translation, by performing the processing locally rather than over the network.

Domain Migration Administrator deploys agents to remote computers to perform the following tasks:

- Gathering data for various reports, such as impact analysis reports
- Translating security, including NetApp filers and accounts with SID History

- Collecting service account information
- Migrating or renaming computers

You can install agents on remote computers so they are already there when you need them, or you can just allow Domain Migration Administrator to dispatch agents as needed on a temporary basis. When agents are needed to perform tasks, Domain Migration Administrator determines if agents are already installed and current on remote computers. If agents are already installed and current on those computers, Domain Migration Administrator uses the pre-deployed agents and does not uninstall them when tasks are completed. If agents are not already installed and current, Domain Migration Administrator dispatches agents to those computers on a temporary basis, and then removes them when tasks are completed.

For more information, see “Using Temporarily Deployed Agents” on page 179 and “Using Permanently Installed Agents” on page 179.

Using Temporarily Deployed Agents

When Domain Migration Administrator dispatches an agent on a temporary basis, it installs about 2 MB of agent files in the `Program Files\OnePointDomainAgent` directory on the remote computer. The agent then runs as a service on the remote computer. Each time Domain Migration Administrator needs to perform a task on a remote computer, Domain Migration Administrator dispatches an agent to that computer. The agent logs its actions in the `DCTLog.txt` file stored in the system `temp` directory on the agent computer. When the agent completes the task, the agent removes itself from the computer. Domain Migration Administrator runs a thread pool of 20 agents to enable the processing of multiple computers at the same time.

Using Permanently Installed Agents

Domain Migration Administrator provides the option to install agents locally on remote computers. By installing agents locally on remote computers, you can reduce usage of a limited bandwidth WAN, since agents are already deployed at migration time and do not have to be removed once tasks have been completed.

The agent installer is not part of the main Domain Migration Administrator setup program and must be launched separately. For more information about installing agents separately, see “Installing Agents Separately” on page 83.

Agent Permission Requirements

Whether you install agents on remote computers in advance or Domain Migration Administrator temporarily deploys agents to those computers, when you perform a task that uses agents, Domain Migration Administrator prompts you for a user ID and password, referred to as **credentials**. Every agent task uses these credentials to write its results back to the Domain Migration Administrator console computer. Some agent tasks also use these credentials to access computer resources. However, most agent tasks use the Local System account to access computer resources.

The following agent tasks use the specified credentials rather than the Local System account to access computer resources:

Security translation for NetApp filers

When you translate security for NetApp filers, Domain Migration Administrator allows you to specify another computer on which to install the agent. The Domain Migration Administrator agent cannot run on a NetApp filer network appliance because the NetApp filer runs a Microsoft Windows NT emulator. Since the agent runs on a separate computer, the agent requires network access, which the Local System account does not provide. To translate security for a NetApp filer, use the Translate Security for NetApp Filer wizard rather than the Translate Security Settings wizard. The Translate Security for NetApp Filer wizard lets you specify a computer running Microsoft Windows 2000 or later where the agent can be installed.

Microsoft Windows computer migration

When you change the domain affiliation of a Microsoft Windows computer, Microsoft Windows checks the status of the computer account. This process requires network access, which the Local System account does not provide.

Server consolidation

Copying files, shares, or printers from one computer to another requires network access, which the Local System account does not provide.

How Domain Migration Administrator Migrates User Accounts and Groups

Domain Migration Administrator allows you to copy user accounts and groups from one domain to another. When you migrate user accounts, you can also migrate the groups of which the user accounts are members. When you migrate groups, you can also migrate the user accounts that are members of those groups.

Domain Migration Administrator provides many options to help you migrate the user accounts and groups. For example, you can specify how Domain Migration Administrator handles the passwords for the copied user accounts.

Copy Versus Move

In most migration scenarios, Domain Migration Administrator copies the account to the target domain, which creates a new account with a different SID. You then need to resolve security access issues for the new SID. However, when you migrate between two Microsoft Windows domains in the same forest, Microsoft Windows enables you to move the account and avoid the access issues. The target domain must be Microsoft Windows native mode.

When you move an account, the original SID is not retained. Domain Migration Administrator moves an account by creating a new account in the target domain. Then, before deleting the source account, Domain Migration Administrator copies the SID of the source account to the SID History of the target account. If you remove SID History before translating security, the target account loses the access of the original source account. You should always translate security before you remove SID History.

Collision Handling

When Domain Migration Administrator copies accounts to the target domain, a naming collision occurs if an account with the same SAM account name exists in the target domain. If an account with the same common name (CN) property exists in the target OU, no naming collision occurs. If conflicting common names are encountered during migration, Domain Migration Administrator appends a number to the common name to make it unique. During migrations, Domain Migration Administrator uses one of the following methods of collision handling:

Ignore conflicting accounts and don't migrate

Domain Migration Administrator does not migrate accounts that exist in the target domain.

Rename and update conflicting accounts

Domain Migration Administrator renames the account with a specified prefix or suffix. You can use the collision prefix or suffix to attempt to make the copied account unique. For example, if you migrated a user account named UserA that existed in the target domain and you set the collision suffix to 123, the migrated user account would be UserA123.

Notes

- Collision handling is processed after the global renaming option. If you migrate accounts with a global prefix or suffix, naming collisions occur for only migrated accounts that match after the global prefix or suffix is added.
 - If the source and target domains are in the same forest, the **Rename and update conflicting accounts** option is not available.
-

Replace and update existing accounts

Domain Migrations Administrator replaces an account in the target domain if the account has the same SAM account name as the source account. The properties of the target account are overwritten by the properties of the source account. If a property is not defined in the source account, the corresponding property in the target account keeps its original value. Domain Migration Administrator can replace accounts only with accounts of the same object class.

Notes

- For security reasons, do not use the replace option if different people use accounts with the same name.
 - If the replaced account existed in a different OU in the target domain, Domain Migration Administrator moves the account to the target OU. If the replaced account cannot be moved due to a CN naming conflict, Domain Migration Administrator does not move the account and logs a message. You can prevent Domain Migration Administrator from moving migrated accounts using the **Leave migrated groups and/or group members in original containers** option. This option applies only to accounts migrated indirectly because of their group membership.
 - If the source group has a different group type than the target group, Domain Migration Administrator replaces the properties in the target group and attempts to update the membership of the target group. Because of varying membership rules, Domain Migration Administrator may not add all the members to the target group.
-

Truncation of Long Names

Microsoft Windows does not allow user account names longer than 20 characters. Domain Migration Administrator truncates long Microsoft user logon names during migration. If multiple user accounts are migrated that are not unique within the first 20 characters, Domain Migration Administrator truncates the account name to 18 characters and appends a two digit number to make the account name unique.

User Manager for Domains supports group names containing up to 20 characters. If you are migrating groups to a Microsoft Windows NT target domain and you want to use User Manager for Domains, you should consider truncating group names at 20 characters. If you want to maintain longer group names, you should clear the **Truncate account names containing more than 20 characters** option.

Domain Migration Administrator supports SAM account names for group accounts up to 64 characters, and names for migrated computer accounts up to 15 characters. Domain Migration Administrator supports Microsoft Windows container names up to 64 characters. When appending a prefix or suffix to migrated accounts, Domain Migration Administrator may need to truncate account names even if the original account does not exceed the maximum length.

Group Membership

Local groups can contain members defined in other domains. Therefore, processing local groups can be a bit more complicated than processing global groups and user accounts. When adding a local group member in the target domain, Domain Migration Administrator processes the group members in the following manner:

1. If the member has been migrated or is currently being migrated, Domain Migration Administrator adds the new account to the local group in the target domain.
2. If the member has been migrated to a domain other than the target domain, Domain Migration Administrator attempts to add the account from the other domain to the local group in the target domain.
3. If the member has *not* been migrated, but the source member is known in the target domain, Domain Migration Administrator adds the source account to the local group in the target domain. To be known by the target domain, the user account or group must be defined in a domain trusted by both the source and target domains.
4. If the member has *not* been migrated and the source member is *not* known in the target domain, Domain Migration Administrator does *not* add the source account to the local group in the target domain. The user account is not known if the account is not defined in a domain trusted by both the source and target domains.

When you migrate user accounts and groups, Domain Migration Administrator creates all the accounts before copying the properties of those accounts. This process ensures Microsoft Windows accounts that reference the distinguished names of other Microsoft Windows objects in their properties, such as the Manager property, are correctly migrated. For example, if UserA is the manager of UserB, and you migrate both accounts at the same time, UserA and UserB need to exist before Domain Migration Administrator can correctly set the Manager property of UserB. If you interrupt the migration process before it is finished, accounts may exist without the properties correctly set. You should allow the migration process to finish completely.

If you migrate groups and their members, Domain Migration Administrator migrates only the members that are defined in the source domain. If local groups have members from other domains, Domain Migration Administrator does not migrate those members. In addition, if computer accounts are members of the migrated groups, Domain Migration Administrator does not migrate the computer accounts.

If you have mapped a group to a different group in the target domain, and then you migrate the group from the source domain to the target domain, you have the option to replace the mapping information. You can map the source group to the migrated group in the target domain or maintain the source group original mapping.

When you map and merge a group, Domain Migration Administrator creates an entry in the migrated objects table, which maps the source groups to the target group. When you migrate the members of the source groups, the members are added to the target group specified in the migrated objects table. If you migrate the source group again using a different wizard, the new mapping overwrites the previous mapping in the migrated objects table and is used for all subsequent migrations.

Increasing Migration Efficiency

You can perform an incremental migration where some user accounts and groups are moved every day, week, or month until the entire population is migrated to the new domain structure. For an incremental migration, consider the following suggestions:

- Plan the group structure in the new domain. For example, identify the groups you plan to migrate and any groups you plan to retire. You may find that some groups in the source domains can be merged into a single group in the target domain.
- Use the Impact Analysis reports to help you identify groups you do not want to migrate. The reports can help you determine if any users will lose access to resources if you do not migrate any particular group.
- If access permissions could be lost, use the Map and Merge Groups wizard in Domain Migration Administrator to assign the permissions to a different group in the target. Migrate the affected groups using the Map and Merge Groups wizard.
- Use the Migrate Groups wizard to migrate all the groups you want to migrate to the target domain. Adding all the groups to a migration project can help you track your progress and ensure all the groups you want to migrate are included.
- Begin migrating user accounts. If your source domain is actively changing during the migration process (particularly if new groups are being created), you may want to choose the option to migrate users and their associated groups. Using this option is common during long incremental migration projects and helps ensure that all the groups necessary to grant resource access are copied to the target domain.
- If you are implementing a group naming convention in the target domain, you can migrate the groups separately using the Map and Merge Groups wizard.

Domain Migration Administrator provides many options to let you customize and optimize the migration process so you can migrate in the most efficient way possible to meet your objectives.

Intraforest Migrations

You can use Domain Migration Administrator to move user accounts and groups from one domain to another within the same forest. Domain Migration Administrator preserves the properties of the migrated accounts, including the password, SID History, and GUID. If a naming conflict occurs, Domain Migration Administrator can either rename or skip the account.

During migration, Domain Migration Administrator removes each user account from its groups in the source domain and tracks these group memberships. After the objects are migrated to the target domain, Domain Migration Administrator restores the group memberships.

Existing universal groups are simply migrated to the target domain. Global groups are converted into universal groups and moved to the target domain. If all the members of a global group are also migrated at the same time, Domain Migration Administrator can convert the group back into a global group. However, if some group members remain in the source domain, the group remains a universal group.

To move local groups, Domain Migration Administrator first removes the members from the group. The product then moves the local group to the target domain and restores its members.

Note

For mixed mode source domains, Domain Migration Administrator cannot always move global groups to the target domain. If some of the members of the group remain in the source domain, Domain Migration Administrator clones the global group to the target domain. You must then run security translation to add a reference to the target group in each place the source group is referenced. You cannot use SID History because each SID must be unique within the forest.

Passwords and Related Properties

When Domain Migration Administrator migrates user accounts, the product sets the **User must change password at next logon** property for each migrated user account. If the **Password never expires** property is set for a user account, Domain Migration Administrator clears this property for that user account. However, if Domain Migration Administrator is set to copy passwords from source accounts, the password flags of the source accounts are preserved.

Domain Migration Administrator sets the passwords for the migrated accounts using one of the following options:

- **Complex passwords**
- **Same as user name (SAM name)**
- **Copy password from source user**

If you use the SAM account name option, set the password policy on the target domain to allow SAM account names to meet the policy. Verify the minimum password length and password complexity policy settings in the target domain. If the new passwords do not meet the policy of the target domain, Domain Migration Administrator generates random passwords.

If you do not copy the existing passwords or SAM account name passwords do not meet the policy of the target domain, Domain Migration Administrator generates passwords for the migrated user accounts. Domain Migration Administrator can generate complex passwords that meet the minimum password length requirement and contain at least 3 lowercase letters, 3 uppercase letters, 3 numerical digits, and 3 symbols. If the generated password does not comply with the password complexity rules in the target domain, Domain Migration Administrator disables the migrated user account.

Domain Migration Administrator can copy passwords from Microsoft Windows native-mode domains to Microsoft Windows domains in a different forest by using a Password Export Server (PES). For more information, see “Native-Mode Source Domain Password Migration” on page 235.

Domain Migration Administrator may not copy blank passwords depending on the password strength policy of the target domain. If Domain Migration Administrator does not copy a blank password, it sets the password in the target domain to a complex password.

If, for any reason, Domain Migration Administrator creates a complex password, Domain Migration Administrator records the password in a tab-delimited file for administrators to reference. You can specify the location of this file during the migration process. If the password file is located on an NTFS volume, Domain Migration Administrator sets the file permissions to allow access only by administrators.

Notes

- If the **User cannot change password** property is set for a user account, that migrated user account will be locked because the user will not be able to reset the password.
 - Domain Migration Administrator does not copy the password age property when it migrates user accounts.
 - Domain Migration Administrator does not set the **User must change password at next logon** property for service accounts.
-

SID History

If you migrate accounts using SID History, you do not need to translate security for those accounts until you are ready to clean up and remove the SID History information. SID History allows the new user account to access resources, such as files and folders, using the old SID. For more information, see “Using SID History to Maintain Permissions” on page 19 and “How Domain Migration Administrator Handles SID History” on page 204.

Primary Group

Domain Migration Administrator sets the primary group for migrated user accounts to Domain Users. If you use the **Migrate associated user groups** option and the source user account is assigned to a different primary group, Domain Migration Administrator migrates the primary group and assigns the user to this group in the target domain. However, the primary group of the migrated user is still set to Domain Users.

Note

Domain Migration Administrator does not migrate the primary group in the source domain if the group is a built-in group.

User Principal Name (UPN)

When Domain Migration Administrator migrates a user account to a Microsoft Windows domain, the product updates the user principal name to reflect the new domain name. Domain Migration Administrator enforces the uniqueness of the user principal names. If the new user principal name is already being used in the target domain, Domain Migration Administrator appends a number to the name portion of the user principal name, incrementing the number until a unique name is found.

For accounts migrated from Microsoft Windows source domains, Domain Migration Administrator replaces the domain portion of the user principal name with the DNS name of the new domain. If the account is renamed during migration because of collision handling or global prefixes and suffixes, Domain Migration Administrator adds the new string to the user principal name.

Domain Controller Security Policy

When you migrate the domain controller security policy, Domain Migration Administrator copies domain controller security policy for migrated accounts from the source domain to the target domain. Migrating domain controller security policy affects the Default Domain Controllers Policy for Microsoft Windows domains and the domain controller security policy

If you select the **Copy User Rights** option, Domain Migration Administrator appends the domain controller security policy of the source account to the existing domain controller security policy in the target account. If you select both the **Copy User Rights** and **Remove existing user rights** options, Domain Migration Administrator overwrites the existing domain controller security policy for the migrated accounts in the target domain.

Roaming Profiles

When you migrate user accounts, Domain Migration Administrator always copies the roaming profile and WTS profile paths as part of the directory object. If you migrate with SID History, you do not need to translate security for the roaming profiles until you are ready to clean up and remove the SID History information. SID History allows the new user account to access the roaming profile using the old SID, so you do not have to translate security (reACL) until you want to remove the SID History information. If you migrate without SID History, the target user cannot access the roaming profile until you translate security for that profile.

Note

You must translate security before disabling computers in your source domain.

Domain Migration Administrator provides the following options for translating security on roaming profiles:

Perform the translation during the account migration

Domain Migration Administrator performs this translation in add mode, so the source and target users can access the profile. This translation may add significant time and network traffic to the migration because Domain Migration Administrator must process every file in each profile and the processing occurs over the network.

Translate the profiles after migrating the accounts

Domain Migration Administrator provides a profile translation utility that you can use to translate the profiles after the accounts have been migrated. This option is helpful when the roaming profiles are stored on servers across slow WAN links from the Domain Migration Administrator console computer. You can run the profile translation utility from the remote site, greatly increasing the speed and reducing the network traffic.

If you do not want the target user accounts to use the roaming profiles of the source users, you can update the target accounts to no longer use roaming profiles. You can use scripting to customize the process and make this change during the migration, or you can make the change as a separate manual step. The disadvantage of this approach is that the users lose any customizations they have made to their roaming profiles.

Remote Users

During migration, computers must be connected to the network and available for Domain Migration Administrator to migrate them. If an account is not available, Domain Migration Administrator skips the account. Before you begin your migration project, you should locate and prepare for migrating computers that are not always connected to the network. Often these computers are laptop computers or other intermittently connected computers.

To migrate remote computers, you can choose one of the following scenarios:

Connect for migration

Many employees normally work in the office but also have laptop computers. Before starting a migration of user and computer accounts for onsite employees, coordinate with the IT group to inform users of the migration schedule. Advise employees with laptop computers to connect them to the network and leave them turned on.

Phone support over high-speed connections

If the remote user has a high-speed connection, an IT representative can talk the user through the process of connecting to the new domain, using native tools to copy user profiles, and restarting the computer.

Bring in the computer

For remote users without high speed connections, coordinate with the IT group to direct these users to bring in their computers at their earliest possible convenience or the next time they are in the local office. You can then connect the computer to the network and perform the migration.

Gaining access to remote computers and their associated user accounts is half the battle. After you migrate the remote user account and computer account, translate security as you would with a normal migration to update the related security descriptors. To complete the migration, restart the computer. If you are migrating the computer to a new domain, you also need to change the domain affiliation of the computer.

Note

If the remote user logs on using cached credentials, you should change the account to a local machine account before you migrate that account. This change is necessary if the computer is offsite and you are using Domain Migration Administrator to migrate the computer and translate the local profiles.

Previously Migrated Objects

Domain Migration Administrator tracks all the objects it migrates, enabling Domain Migration Administrator to update group memberships for renamed users and groups during incremental migrations. Objects selected in the wizards for migration are always migrated. If an object was previously migrated, the old object mappings are replaced with the new mappings.

Objects not explicitly selected for migration, but included because of the **Copy group members** or **Copy specified user groups** options, are not always migrated. When expanding its account list to include these accounts, Domain Migration Administrator checks whether these accounts have already been migrated. If the accounts have already been migrated, Domain Migration Administrator does not attempt to migrate them again. However, you can use the **Migrate Previously Migrated Objects** option to force Domain Migration Administrator to migrate the objects again.

Accounts Migrated with Tools Similar to ADC

If you used another tool to migrate your accounts and you want to use Domain Migration Administrator for security translation, password synchronization, and other tasks, you need to import the account mapping information for the migrated accounts. If you used a tool such as the Active Directory Migration Tool (ADMT) and migrated the accounts with SID History, you can add the mapping information by running the SID History report. If you did not migrate the accounts with SID History, you need to import the mapping information using the CSV Import function. For more information, contact Technical Support.

How Domain Migration Administrator Migrates and Renames Computers

Domain Migration Administrator allows you to change the domain membership for member server and workstation computers. Domain Migration Administrator copies the computer account from one domain to another domain. Then, Domain Migration Administrator changes the domain membership and reboots the migrated computer to make the change take effect. Renaming computers, before or after migration, allows you to clean up your environment and create computer names that match your naming policy.

Domain Migration Administrator also allows you to rename computers in a domain by renaming the computer accounts for those computers. Domain Migration Administrator then updates the computer to use the new name and allows you to reboot the computer.

Domain Migration Administrator migrates computer accounts that are members of a domain. This product does not migrate computer accounts that are members of a workgroup. You can use the Rename Computer option to rename workstations and member servers. However, you cannot rename domain controllers.

Notes

- Before you migrate or rename a computer, make sure you know the local administrator password for that computer. If the migration process does not finish successfully, the computer can be locked out of the domain.
 - Microsoft Windows does not allow you to rename a computer account at the same time as you migrate that account. If needed, you should rename Microsoft Windows computer accounts before you migrate those accounts.
 - The new computer account name cannot be more than 15 characters.
 - To migrate a computer with dual operating systems, you must log on to each operating system on the computer to migrate that computer.
 - Do not attempt to rename any computer that is running software that depends on the computer name, such as SQL Server. If you rename a computer that runs SQL Server, SQL Server may not work properly. For more information about renaming SQL Server computers, see the SQL Server documentation.
-

How Domain Migration Administrator Migrates Service Accounts

The Service Account Migration wizard collects information about service accounts. Then, you can specify whether to include or skip each service account when you migrate other accounts. These settings apply to all migration tasks performed after you specify these service account settings.

The Service Account Migration wizard also allows you to identify which services were updated to use the migrated service accounts. You can retry the failed update attempts to ensure the services use the migrated accounts.

To handle service accounts differently than the user accounts, groups, or computer accounts you select to migrate, run this task before you use other migration wizards. When a service account is migrated using the User Migration or Group Migration wizards, Domain Migration Administrator performs the following additional steps:

- Clears the **User must change password** flag to prevent the service account from being disabled.
- Generates a 14-character random password that is stored in the password file.
- Grants the **Logon As A Service** right for each computer where the service account is used.
- Updates the SCM entry for the service on each computer to use the new account and password.
- Saves the password of the service account in the regular password file for any of the services that it cannot update due to denied access or offline computers.

Notes

- Service accounts for some applications, such as BackOffice applications, cannot be migrated using Domain Migration Administrator. Refer to the documentation for each product before you migrate service accounts for those products.
 - Domain Migration Administrator updates service account entries using the *domai n\name* format, not the UPN or *.\account* formats.
 - Do not move the password file containing service account passwords if you want to use the **Update SCM now** feature.
 - If you use Domain Migration Administrator to migrate service accounts and change the services to use the new service accounts, you cannot use the undo function to change the services to use the old service accounts.
-

How Domain Migration Administrator Refreshes Project Data

Domain Migration Administrator enables you to refresh project data to reflect changes to objects that occur during the course of a migration. Domain Migration Administrator first compares the objects you have selected in the project with objects that have been moved or deleted from the source domain. Domain Migration Administrator then updates the project with the correct location of any objects that have moved in the source domain and deletes objects from the project that have been deleted from the source domain.

How Domain Migration Administrator Synchronizes Objects

The Synchronize Object Wizard updates the changes made to object attributes in the source domain with the target domain. When you select the objects which are to be synchronized, Domain Migration Administrator replaces all attributes of the selected objects in the target server with the attributes of the objects in the source server.

Notes

- Domain Migration Administrator does not synchronize trusts and SID history.
 - Domain Migration Administrator displays the Synchronize Migrated Object link only for projects that have migrated objects.
-

How Domain Migration Administrator Migrates Trusts

Domain Migration Administrator allows you to migrate trust relationships from one domain to another domain. A trust relationship connects two or more domains and allows users in one domain to access resources in another domain.

Groups can contain members from trusted domains. To migrate groups with members from trusted domains, you should establish the same trust relationships in the target domain as exist in the source domain. If Domain Migration Administrator cannot identify a member account in the target domain, Domain Migration Administrator does not add the member to the group.

The Trust Migration wizard resolves this issue. The Trust Migration wizard compares the trust relationships in the source domain to the trust relationships in the target domain. The Trust Migration wizard establishes in the target domain any trust relationships that exist in the source domain but not in the target domain. The wizard does not affect trusts that exist in the target domain but not in the source domain.

Domain Migration Administrator can create inbound, outbound or bi-directional trusts between the target domain and the domains that trust or are trusted by the source domain. The direction of the trust is determined by the direction of trust to the source domain. If the migrated trust to the target domain partially exists, Domain Migration Administrator deletes the old trust and establishes a new trust.

Note

Domain Migration Administrator does not support creating trusts to non-Windows domains, such as Kerberos Realm trusts.

How Domain Migration Administrator Merges and Maps Groups

Domain Migration Administrator allows you to map one or more groups in one domain to a single group in another domain. This feature enables you to reduce duplicate groups during the migration process. Run this wizard once for each set of groups that you want to map to a single group in the target domain.

If you specify a target group that does not already exist, Domain Migration Administrator creates the target group in the specified OU. If you specify a target group that does already exist, the target group is moved to the specified OU. The properties of the target group are not modified. However, if you migrate with SID History, the SID of each source group is added to the SID History of the target group.

If the members of the source groups have already been migrated, the group mapping option adds the users to the target group. If the members of the source groups have not been migrated, Domain Migration Administrator retains the mappings from the source groups to the target group to enable the users to be added to the target group when they are migrated.

If you have mapped a group to a different group in the target domain, and then you migrate the group from the source domain to the target domain, you have the option to replace the mapping information. You can map the source group to the migrated group in the target domain or maintain the source group original mapping.

Notes

- Due to Microsoft Windows restrictions on group types, members from a source group cannot be added to a target group of a different type. If the target group does not exist when merging groups of different types, the type of the first source group in alphabetical order is used.
 - Domain Migration Administrator can add SID History only when the source group and target group are the same type.
-

How Domain Migration Administrator Updates Access Control Entries

Domain Migration Administrator allows you to change file, folder, share, and printer security descriptors that reference one user account or group in a source domain to reference another user account or group in a target domain. The mapping between user accounts and groups is stored in the migrated objects table. You can also translate local group memberships, domain controller security policy, and user profiles. Domain Migration Administrator provides many options to help you resolve the related security issues.

When you copy a user account or group from domain A to domain B, a new account is created in domain B. This new account may have the same name as the original account in domain A, but this new account has a different SID. Domain Migration Administrator changes the security descriptors for various files, folders, shares, and printers to refer to the SID for the new account in domain B. This process ensures the new user account or group provides the same access to files, folders, shares, and printers that the original user account or group provided.

You can use Domain Migration Administrator to translate security on the objects you migrate. You can translate security from only one source domain to one target domain in each operation. If you migrated objects from several source domains, you must translate security for each source domain.

Notes

- If you updated the SID History property during the migration, you need to translate the security only on the user profiles. SID History ensures the accounts have the same access as the original accounts.
 - When performing security translation using SID History, you can select mappings from multiple source domains to multiple target domains. You do not need to run security translation for each domain pair.
 - If Domain Migration Administrator finds a SID from the source domain that it cannot resolve, such as a SID for a user account that does not have a matching user account in the target domain, Domain Migration Administrator leaves the SID unchanged and continues searching.
-

Files and Folders

Domain Migration Administrator translates the security descriptors for NTFS volumes on the computer. The product can handle deeply nested files and folders, with paths of up to 1,200 characters. You cannot selectively choose which files and folders are translated. Domain Migration Administrator does not translate security for FAT volumes, volumes that do not support security, or mapped network drives.

Domain Migration Administrator uses backup and restore privileges to translate security for files and folders. Using these privileges allows the product to update files and folders without explicit access to them.

Local Groups

Domain Migration Administrator updates the membership of local groups on member servers, workstations, and domain controllers in resource domains during security translation. To update the local groups in a resource domain, run the security translation on the domain controller of the resource domain.

Local User Profile

Local user profile translation is required for Microsoft Windows computers when user accounts are copied or moved. When a user logs on to a computer, the operating system searches for the user profile using the primary SID of the logged-on account without referring to the SID History property. When you translate security, Domain Migration Administrator updates the profile list in the registry with the SID of the target account.

You can perform profile migration using the following modes:

- | | |
|----------------|--|
| Add | Domain Migration Administrator translates the security of files and registry entries for the profile and adds the target user to the profile list in the registry. Add mode allows both the source and target users to use the same profile. |
| Replace | Domain Migration Administrator translates the security of files and registry entries to allow access by only the target user. The source user is removed from the profile list. If the source user logs on, Microsoft Windows creates a blank profile. |
| Remove | Domain Migration Administrator simply removes the source user from the profile list, without translating security of the files and registry keys. |

Warning

Remove mode deletes all references to source accounts. Do not remove user profiles from the source domain before adding them to the target domain.

Domain Migration Administrator translates all the files and folders in the Recycle Bin during local user profile migration. Using **Add** or **Replace** mode, Domain Migration Administrator renames the Recycle Bin folder to the SID of the target user, allowing the target user to access data placed in the Recycle Bin by the source user.

Domain Migration Administrator also examines the list of mapped drives in the registry during local user profile migration. If any registry entries use the source account as its credentials for the mapped drive, Domain Migration Administrator resets the value to an empty string. Resetting the value causes Microsoft Windows to use the credentials of the logged on user to establish a connection.

Note

Local user profile translation is not required for moved accounts on Microsoft Windows computers. Domain Migration Administrator retains the GUID and uses this value to look up the corresponding SID in the profile list. *This process applies only to intraforest migrations.*

Registry

Registry security translation updates the security on the registry keys. Domain Migration Administrator processes security for the entire registry of the computer being migrated. Domain Migration Administrator does not replace any references in the registry values with the new domain names, computer names, or account names.

Domain Migration Administrator uses backup and restore privileges to translate security for registry keys. Using these privileges allows the product to update registry keys without explicit access to them.

Note

The HKEY_CURRENT_USER registry entry is not translated with the registry. These entries are translated during the local profile translation.

Domain Controller Security Policy

Domain Migration Administrator translates the domain controller security policy entries on the servers you migrate. Because all domain controllers share the same domain controller security policy, you only need to translate one domain controller.

For Microsoft Windows member servers, the domain controller security policy are updated in the local security policy on the computer. For Microsoft Windows domain controllers, the domain controller security policy are updated in the default domain controllers policy.

Note

Domain Migration Administrator translates the domain controller security policy only in **Add** mode if the source account no longer exists. If you select a different mode, Domain Migration Administrator still translates the domain controller security policy using **Add** mode. All other security translations use the mode selected except for Recycle Bins, which are always translated in **Replace** mode.

Default Logon Domain

Domain Migration Administrator can update the default logon domain used in the Logon Information window. You can set the default logon domain to minimize user impact and allow users to accept this domain as the default when they log in.

NetApp Filers

Domain Migration Administrator allows you to translate security for files, folders, and shares on network appliances. Only network appliances that have full emulation of NTFS and Net Share APIs are supported. The Translate Appliance Security wizard allows you to specify a computer on which to run the agent.

Because filers do not have default administrative shares, Domain Migration Administrator does not translate the entire contents of the filer. When you specify the share to translate, Domain Migration Administrator translates the share and all files and folders below the share. Only the shares you specify in the wizard are updated. If you use the Process sub-shares option, shares that reference folders below the selected share are also updated.

How Domain Migration Administrator Handles SID History

Each user account, group, and computer account is represented by a unique identifier, known as a security identifier (SID). Microsoft Windows use these SIDs to record access permission information in the security descriptor for each resource, such as a file or share.

When you copy a user account, group, or computer account from domain A to domain B, a new account is created in domain B. This new account has a different SID. Therefore, the new account does not have the same permissions as the original account.

To resolve the access issues and ensure the new account has the same permissions as the original account, Domain Migration Administrator provides the following options:

Translate security

This feature changes the security descriptors for selected resources, such as files, to reflect the SID for the new account in the target domain. This process ensures the new account provides the same access to these resources that the original account provided.

Update SID History during migration

When you migrate to a Microsoft Windows native mode domain, Domain Migration Administrator allows you to set the SID History property of each account during the migration process. This property allows the new account to use the permissions assigned for the SID of the old, migrated account. Therefore, the SID History property provides the access without changing the security descriptors for various resources to reflect the SID for the new account.

Understanding SID History

User accounts and groups in Microsoft Windows native mode domains have a property called **SID History**. This property can identify additional SIDs to check when evaluating the access permissions for that account.

When a user logs on, Microsoft Windows creates an access token for the user. This token includes the following information:

- SID of the user account
- SIDs for all the groups of which that user account is a member
- SIDs in the SID History property of the user account
- SIDs for all the groups of which the SID History SIDs are a member

Then, when a user attempts to access a resource, such as a file, Microsoft Windows compares the SIDs in the access token with the entries in the access control list for that resource to identify the permissions that user has for the resource. In this way, the SID History property can provide access to various resources.

Understanding the Migration Process and SID History

After you migrate accounts with the SID History information, you need to translate the security only on the user profiles. SID History ensures the accounts have the same access as the original accounts. However, SID History information creates extra entries in your Global catalog, which increases the size of your Global catalog. You may want to remove this SID History information from the Global catalog. Removing the SID History information decreases the size of the Global catalog and may improve logon performance for your users.

To remove the SID History information, you must *first* resolve the security and access issues for the accounts with SID History information. This process is known as **translating security**. Then, after all file, folder, share, printer, and DCOM security descriptors reference only the SID for the migrated account, you can remove the SID History information for all migrated accounts. For more information about how to correctly address SID History in your migration workflow, see “Developing a Migration Workflow” on page 48.

Note

You can translate security only for source objects that have previously been migrated.

SID History Values

The SID History property can have multiple values. When you merge multiple source domains into one target domain, each account in the target domain may have multiple values in the SID History property for that account.

When you migrate an account that already has entries in its SID History property, Domain Migration Administrator appends the SID History entries of the source account, as well as the SID of the source account, to the SID History property of the target account. If you try to migrate with SID History and Domain Migration Administrator detects a configuration or permissions problem, Domain Migration Administrator stops the migration process for all selected accounts. However, if Domain Migration Administrator detects one of the following problems, Domain Migration Administrator stops the migration only for the affected account and continues the migration with the next account:

- The SID already exists in the target forest.
- The target account is not the same type of object as the source account. For example, you cannot add a user account SID to the SID History of a group.
- A problem exists that applies only to the individual account and not to the overall migration.
- The SID is recognized as a well-known account in the source domain, and the target account is not the same well-known account as the source account.

SID History Report and Other Migration Tools

The SID History report identifies all target domain accounts that have at least one SID in their SID History property. Before you migrate with Domain Migration Administrator, this report can help you identify accounts you migrated with other tools, such as the Active Directory Migration Tool (ADMT).

Run the SID History report after you migrate user accounts and groups with SID History. The report lists the SID for the migrated account, the account type, and the target path for the account. For more information, see “Accounts Migrated with Tools Similar to ADC” on page 194.

Methods for Translating Security

Domain Migration Administrator allows you to translate security based on the account mappings stored during account migration, or based on SID History information.

Domain Migration Administrator provides the following wizards to translate security:

Translate Security Wizard

Checks the access control lists for the files, folders, shares, printers, registry, local groups, profiles, DCOM objects, and domain controller security policy on the computers you select. When Domain Migration Administrator finds a reference to the source domain account SID, it modifies the ACL to include the SID for the target domain account. You specify an option that determines whether the source SID is replaced.

Translate Security for Accounts with SID History Wizard

Allows you to translate security based on SID History values instead of account mapping information stored during account migration. With this wizard, you can translate security for all SID History-based mappings, rather than one source and target domain pair at a time. This wizard is available only for Microsoft Windows native mode target domains.

Additional SID History Considerations

The following list provides additional SID History considerations and references to additional information:

- To migrate with SID History, Domain Migration Administrator requires specific configuration requirements. For example, to migrate with SID History in scenarios other than intraforest migrations, you need to install the product on a domain controller in the target domain or on a Microsoft Windows computer in the target domain. For more information, see the following sections:
 - “Preparing to Migrate with SID History” on page 30
 - “Testing Secure Channel Communication” on page 38
 - “Objects that Domain Migration Administrator Migrates” on page 76
 - “Detailed Permission Requirements” on page 157

- During intraforest migrations, Domain Migration Administrator maintains SID History values for migrated accounts.
- The SIDs of the source objects must not already exist in the target forest, either as a primary account SID or in the SID History of an account.
- You cannot translate SID History for clustered share resources.
- Using SID History does not automatically give the target user account access to the profile of the source user account on Microsoft Windows computers. When a user logs on to a computer, the operating system searches for the user profile using the primary SID of the logged-on account without referring to the SID History property. For more information, see “Local User Profile” on page 201.
- You cannot add SID History to built-in accounts. For more information, see “Understanding Built-in Accounts” on page 21.
- To migrate well-known accounts and use the SID History migration option, you must migrate them using the **Replace** mode. You can add SID History values to a well-known account in the target domain only from the same well-known account in the source domain. For more information, see “Migrating Well-Known Accounts” on page 20.

How Domain Migration Administrator Synchronizes Passwords

Domain Migration Administrator allows you to synchronize the password of a migrated user account with the password of the user account in the source domain. If any of the following conditions are *true*, Domain Migration Administrator does *not* synchronize the passwords for the affected user accounts:

- A user account in the source or target domain has a blank password.
- A user account password is longer than 14 characters.
- The target user account is locked.

- The **User Cannot Change Password** property is set for a user account in the source domain.
- The source domain and the domain where Domain Migration Administrator is running do not have a properly established trust.

Note

The copied passwords may *not* comply with the password policy in the target domain. To address this issue after you synchronize the passwords, you can set the **User must change password** property for the user accounts to make the users change their passwords when they log on. Microsoft Windows ensures the new password specified by each user matches the password policy.

How Domain Migration Administrator Changes Domain Affiliation

After migrating computer accounts, Domain Migration Administrator dispatches an agent to each selected computer to add the computer to the new domain. If the computer was renamed during the migration, the computer name is updated. Then, you can perform security translation on the computer. After security is translated, the computer needs to be rebooted. You can specify a reboot delay to determine how long the agent waits to restart the computer after the processing is completed.

Before dispatching agents, Domain Migration Administrator checks whether the computer account was successfully cloned to the target domain. If cloning was unsuccessful, Domain Migration Administrator still dispatches the agent but does not attempt to change the domain affiliation of the computer. Also, the computer does not require a reboot.

When Domain Migration Administrator changes the domain affiliation of computers, Domain Migration Administrator performs the following operations:

- Updates the computer to join the target domain.
- Removes the source domain Domain Admins group from the local Administrators group.

- Adds the target domain Domain Admins group to the local Administrators group.
- Removes the source domain Domain Users group from the local Users group.
- Adds the target domain Domain Users group to the local Users group.
- Reboots the computer, after waiting the specified reboot delay.
- Updates the default logon domain in the Logon Information window, if this option is selected.

Domain Migration Administrator uses the specified credentials to change the domain affiliation of the computer to the target domain. The credentials you specify must have administrator rights on both the computer being migrated and on the target domain.

Notes

- When you change the domain affiliation of a computer, make sure you know the credentials for its local administrator account. If an error occurs during the domain affiliation change, you can get locked out of the computer without these credentials.
 - Domain Migration Administrator does not migrate Workgroups.
 - If you do not select the **Update default logon domain** option, administrators should tell users to change the value in the Domain field the first time they log in.
 - You cannot rename and change domain affiliation in the same operation for Microsoft Windows computers. To rename and change domain affiliation for a Microsoft Windows computer, you must run the Computer Rename wizard and the Computer Migration wizard separately.
-

How Domain Migration Administrator Handles Test Mode

You can run several wizards in **test** or **no change** mode to test the success of a migration task before you actually perform the task. Test mode allows you to preview the migration results and make adjustments before you run an actual migration procedure. Domain Migration Administrator handles the following items differently in test mode than during an actual migration:

License limit

Verification of the number of users allowed by a trial license occurs only during an actual migration.

Migrate Files, Folders and Shares

The Migrate Files, Folders, and Shares wizard does not verify ACL access during test mode.

Password copy

Passwords are copied only during an actual migration.

Scripts

Scripts are run only during an actual migration.

SID History credentials

Credentials for migrating SID History are verified only during an actual migration.

The following wizards do not support test mode:

- Remove SID History
- Update Active Directory Connector Accounts
- Service Account Configuration
- Synchronize Passwords

How Domain Migration Administrator Handles Data Modeling

You can use modeling to update certain account attributes during migration. Modeling is available only when you use migration projects. The object attributes are imported from the source domain into the database for the migration project. You can then edit the values in the database and apply these values to the target objects when you migrate. Using modeling, you can rename objects and standardize or clean up your data during the migration process.

The following attributes are supported for modeling.

Object Type	Attributes	Microsoft Windows
Users	Description	X
	FullName	
	Display name	X
	SAM account name	X
	Common name (CN)	X
	User principal name (UPN)	X
Groups	Description	X
	SAM account name	X
	Common name (CN)	X
Computers	Description	X
	SAM account name	X
	Common name (CN)	X

You can extend modeling to handle additional properties by modifying the `PropList` and `PropMap` tables in the project database. For more information about extending modeling, contact Technical Support.

Renaming Objects

Using modeling, you can rename objects by changing their SAM account name and common name (CN). Modeling enables you to resolve name conflicts before you migrate the project. The Name Conflicts report can help you identify the conflicting accounts.

OU Structure

By default, Domain Migration Administrator migrates accounts into a single target organizational unit (OU). By specifying a target OU for each object, you can model your OU hierarchy instead of migrating all objects to a single OU.

To interactively edit the modeling data or select target OUs, use the Modeling Users, Modeling Groups, and Modeling Computers nodes in the MMC interface. To make global changes to a large number of objects, use the data modeling interface and select all the accounts you want to modify. On the Action menu, click **Update Target OU** to assign a different target OU to all the selected accounts. For more information about modeling, click **Help**.

Common Name (CN)

The Microsoft Windows Active Directory Users and Computers snap-in displays and sorts objects by common name.

How Domain Migration Administrator Handles the Undo Function

Before you run any migration tasks, check the value of the **Undo task limit** field on the Domain Migration Administrator Advanced Settings window. The **Undo task limit** field specifies how many tasks Domain Migration Administrator saves. These tasks can be saved only if the task history is saved in the Domain Migration Administrator database.

Notes

- Domain Migration Administrator saves each task you perform, including some tasks that cannot be undone, such as selecting objects and generating reports. Be sure to set the **Undo task limit** field to a large enough value to save the important migration tasks that you may need to undo.
- To preserve all migrated objects, replicate all domain controllers in the target domain before you undo a migration task.
- When you undo an *intraforest* migration, the accounts are returned to the source domain. Since an intraforest migration is a move operation instead of a copy operation, all changes made to the target accounts, including any modeling changes, are retained and cannot be undone. SID History values are also retained and stored in the database.

If you perform more tasks in a single project than the specified undo limit, the oldest task is deleted from the database. This process helps prevent the database from growing excessively large. However, to ensure you can undo tasks as needed, set the **Undo task limit** field to as large as a value as possible in your environment.

You can use the undo function to restore most of the tasks you perform with Domain Migration Administrator. However, because of limitations of the operating system or the tasks Domain Migration Administrator performs during migration, certain tasks cannot be undone. Domain Migration Administrator cannot undo the following tasks:

- Roaming profile security translation
- Replace mode migration tasks

- Service Account migration changes in the Service Configuration Manager (SCM)
- Active Directory Connector Accounts wizard tasks

To provide additional safety, periodically back up your databases to maintain a complete record of the tasks you performed. These backup copies can help you undo problematic changes. However, make sure Domain Migration Administrator is not running when you back up the databases, or those databases will not be usable. For more information, see “Understanding the Domain Migration Administrator Databases” on page 227.

Appendix D

Understanding How Server Consolidator Works

Server Consolidator simplifies and automates most of the consolidation process for moving printers, shares, folders, and files from multiple servers to one location. To ensure your network maintains its integrity, you should understand how Server Consolidator handles each consolidation issue. The following sections identify potential consolidation issues and outline how Server Consolidator handles each issue. This information can help you understand the product and improve your process and results.

Understanding the Server Consolidator Architecture

Server Consolidator optimizes use of network bandwidth by installing an ActiveAgent on the source computer to initiate the consolidation process.

How Server Consolidator Handles Files, Folders, and Shares

Server Consolidator allows you to quickly move files, folders, shares, printers, and their access permissions from one server to another. You can independently consolidate files and folders, shares, and printers. In addition, you can choose from a number of options to handle naming conflicts. When you consolidate files and folders, you can select whether to preserve the file and folder security descriptors.

You can also choose to move files, folders, and shares on the same server. In the Migrating Files, Folders, and Shares wizard, you can select the same server name to transfer objects within the server itself.

Consolidating Files and Folders

Server Consolidator copies files and folders from the source computer and creates new folders on the target computer. When you consolidate files and folders from one server to another, Server Consolidator offers the option to also copy the file and folder security descriptors. Server Consolidator replicates all file attributes except the compressed file attribute and also sets the archive bit on. This action ensures all migrated files are included in the next backup on the target server. Server Consolidator properly handles system, hidden, and read-only files.

You can optimize the file and folder consolidation process to meet your needs. The default setting, **Replace if source object dates are more recent**, directs Server Consolidator to compare the size, time, and date of each source file and copy the file to the target location only if the source file was created more recently than the target file.

The **Assume files are identical if size and date match** option directs Server Consolidator to check the file and folder contents even when the size and date match. In this case, Server Consolidator copies files from the source folder only if the source file contents differ from the target file. This option takes added time but gives you the flexibility to consolidate to a central server over time, if needed.

The **Always replace** option overwrites like named files and folders on the target server whether the source file or folder is older or newer than the target file or folder. Use this option with care.

The **Compare file content if size and date match** option specifies that when the name, size, time, and date of a file or folder are the same on both the source and target computers, Server Consolidator compares the contents on both the source and the target computers. If the contents of the source file or folder are different from the target file or folder, overwrite the target copy with the source copy. Selecting this option can slow the consolidation process.

The **Replicate permissions even if the files or directories are identical or the target object date is more recent** option specifies to compare permissions between files and folders that have the same name, size, time, and date.

Consolidating Shares

When you use Server Consolidator to consolidate shares from one server to another, Server Consolidator replicates the name, description, connected user limits, and permissions of the share. If the share name already exists on the target computer, share permissions are not copied but permissions for the folders and files it contains are copied. If you plan to consolidate shares onto a cluster server, be sure you know the group name of the cluster server before you begin the consolidation process.

Server Consolidator offers two name resolution options when consolidating shares. If the share name already exists on the target computer, you can direct Server Consolidator to omit copying the source share or to replace the target share with the source share. This option gives you added flexibility when consolidating shares.

Note

If the source or the target computer path is *drive:\path*, and you run the agent on the source or target computer, Server Consolidator preserves the specified path. If you run the agent on another computer, the administrative share, such as C\$ or D\$, must exist on the specified drive. If the administrative share does not exist, you must either change the share designation or run the agent only on the local computer.

How Server Consolidator Handles Cluster Servers

Server Consolidator is designed to copy files, folders, and shares to stand-alone file servers or to cluster servers. A cluster server is a group of computers that work together to look like one computer to other applications. The computers run cluster software to provide load balancing for high availability and scalability.

The Server Consolidator agent must run on a server that is running the Microsoft Windows operating system. You may want to specify a different server for the agent other than the source server.

To specify a server other than the source server:

1. Click **Migrate Files, Folders, and Shares** in the right pane of the main window.
2. Select **Run the agent on the following computer** on the Advanced Server Options window.
3. Click **Browse** to specify a computer running the Microsoft Windows operating system. You may want to consider specifying a cluster server.
4. Proceed through the rest of the **Migrate Files, Folders, and Shares** wizard.

Cluster Server Requirements

To copy files, folders, or shares to a cluster, you must provide Administrator and Domain Admin permissions on the cluster. The cluster where Server Consolidator copies files should be configured as a Clustering Service rather than a Network Load Balancing (NLB) cluster.

Note

You can also copy files, folders, and shares to any computer in a cluster by addressing the individual node instead of the cluster server.

The cluster server must be running one of the following environments:

- Microsoft Windows 2003
- Microsoft Windows XP Professional
- Microsoft Windows 2000 *without* Service Pack 1 or 2

Cluster Server Terminology

You should be familiar with the following cluster server terminology:

Cluster

Hardware and software managed by the cluster service software.

Node

Individual server computers within a cluster. A cluster can include two or four nodes.

Resource Group

Physical or logical hardware and software entities within a cluster that are managed by the cluster service and can be owned and accessed by only one node at a time.

Local resource

Hardware or software associated with a particular node and not shared by the cluster.

Common resource

Hardware or software shared by the cluster, such as a shared drive array. Only an active node can access common resources.

Shared Drive Array

Hard drive or group of drives managed by the cluster services and accessible only by the active node of the cluster.

Virtual Server Name

Common name for accessing the failover protected resources and applications on a cluster. The virtual server has an IP address separate from the individual node IP addresses. Users know the cluster by this name over the network.

Cluster Information

To correctly consolidate files, folders, and shares from standalone servers to clusters and preserve the benefits of cluster failover protection, you must carefully specify the following information in the Server Consolidator Copy Files, Folders, and Shares wizard:

- Virtual server name
- Target path (`\\virtual_machine\target_share_on_shared_drive_array\`)
- Group name
- Resource to depend on

If you do not have this information, you can locate the information by running the Cluster Administrator application in the Administrative Tools program group. When you correctly specify this information, Server Consolidator copies the files, folders, and shares to the cluster server shared drive array and creates the proper cluster resources for each migrated share.

Cluster Resources

If you use the **Copy subdirectories as shares** option, Server Consolidator migrates shares located beneath the source share as subdirectory shares within the specified cluster resource.

Without the **Copy subdirectories as shares** option enabled, multiple shares are migrated to the cluster server when you migrate the `Fo l d e r 1` source share. The cluster resources are all created at the same level. The following example demonstrates consolidating without this option:

```
Fo l d e r 1 (w i t h S h a r e 1 d e f i n e d)           S h a r e 1
  S u b F o l d e r 1 (w i t h S h a r e 2 d e f i n e d)  - - - - >  S h a r e 2
  S u b F o l d e r 2 (w i t h S h a r e 3 d e f i n e d)           S h a r e 3
```

However, the **Copy subdirectories as shares** option preserves the fault tolerance of the cluster server array for all newly created shares and consolidates the newly created shares under a single top-level share. Using this option, the only cluster resource Server Consolidator creates is `Share1`. Server Consolidator still creates the subdirectory shares, but they are not created as separate cluster resources.

Note

If you use the **Create subdirectories as hidden shares** option, the subdirectory shares are created as hidden shares.

Why Cluster Server Copies Can Fail

Server Consolidator does not support copying to DFS cluster shares. If the cluster is configured with DFS shares, Server Consolidator detects this configuration and displays an error message.

If you specify a local resource, such as a local hard drive, Server Consolidator may successfully copy data, but the data will not be failover protected. Similarly, if you specify a shared drive array but do not provide the cluster virtual server name, the data is copied but it is not failover protected.

If you specify the following combinations, Server Consolidator may actually fail when it attempts to copy files, folders, or shares:

- Passive node and shared drive array (passive nodes cannot access the shared drive array)
- Virtual server, the local drive of either the active or passive node, and valid group name (invalid target path or resource group)
- Virtual server, local drive of the passive node, and no group name (invalid target path)

There may be cases when you want to copy data to the local drive of a cluster node, but these cases are not typical. If you copy data in this manner, ensure you can identify the target UNC path to the local drive of the active node and omit the cluster group name and resource.

How Server Consolidator Handles Printers

Server Consolidator can migrate both local and network printers from one server to another. When you migrate a printer, Server Consolidator performs the following tasks:

- Copies the printer driver to the target server
- Creates a print queue on the target server
- Copies the print shares and permissions to the target server
- Creates a printer port on the target server (if there is no port currently present) when you migrate a printer from the source server

Understanding the following printer terminology can help you understand the process of printer migration:

Printer

A logical device that acts as an intermediary between user applications and the print device.

Print device

A physical printer, such as an HP LaserJet printer.

Print queue

A group of documents waiting to be printed.

Print server

The computer on which printers and print drivers reside.

Network interface printer

A printer directly connected to the network using a built-in network card.

Print spooler

A set of .dll files that work with the spooler service and include the following components: print router, print provider, print processors, and print monitors.

Server Consolidator provides an option to overwrite printers that already exist on the target server. When you check this option, if a printer with the same name exists on the target server, Server Consolidator removes the printer on the target server, copies the drivers and settings from the source printer, and writes a message to the log file. Some applications may not support server and printer name combinations of more than 31 characters. If you have printers with long names, you may want to rename them before you migrate these printers.

Note

If a printer uses a non-standard print monitor or port, you need to install the print monitor or port on the target computer before migrating printers.

Server Consolidator can migrate printers to or from individual computers in a cluster. However, this ability does not result in a fault-tolerant resource printer. For example, if ClusterServer1 includes \\Computer1 and \\Computer2, Server Consolidator can migrate printers to \\Computer1 or \\Computer2 but not to ClusterServer1 as a managed cluster resource.

How Server Consolidator Handles Local Groups

You can use Server Consolidator to copy local groups from one computer to another computer to maintain access to migrated resources. After migrating the local groups defined on that computer, run the Translate Local Security Settings wizard to update the access control lists on the migrated resources.

Appendix E

Understanding the Domain Migration Administrator Databases

Domain Migration Administrator databases provide much of the flexibility and functionality of the product. This section describes some of the Domain Migration Administrator databases and their tables. This information can help you use scripts to obtain the results you want during your migration efforts.

Note

You should not directly edit the Domain Migration Administrator database files.

Locating the Databases

To perform, track, and configure migrations, Domain Migration Administrator uses SQL Server databases. The databases contain information such as migration settings, history of actions, and reporting data. Domain Migration Administrator uses the following SQL Server databases:

Protar database

A global database that contains information pertinent to your Domain Migration Administrator installation. This database also contains mappings for objects you have migrated. You should not migrate objects from multiple computers, since the mapping information could be incomplete on each computer and cause problems with group memberships and security translation.

Project database

A project-specific database that contains data specific to one project you defined using Domain Migration Administrator.

There is one Protar database for each Domain Migration Administrator installation. For each project you define, Domain Migration Administrator creates a project database using the project name you supply when you create the project. The following sections describe the functions of these database files.

Protar Database

Domain Migration Administrator creates and stores the Protar database on the SQL Server computer you specify. The Protar database contains global information about Domain Migration Administrator and all the projects you define using this installation of Domain Migration Administrator.

The Protar database tracks information such as which objects have been migrated, their target location, and the time they were migrated. The Protar database also tracks information about defined projects. For more information about how Domain Migration Administrator uses the Protar database, see “Tables in the Protar Database” on page 229.

Project Databases

Project database files contain information specific to each project, such as the objects you selected to migrate and modeling information.

Since project-specific database files are automatically named using the name you specify for the project, you should carefully consider the naming conventions you will use *before* you begin creating projects. SQL Server offers great flexibility in naming databases, but does have some basic rules you should follow. For more information about best practices for database names in SQL Server, see the Microsoft SQL Server documentation.

Creating and Deleting Project Databases

To create or delete project databases, use Domain Migration Administrator. The product creates entries in the Protar database to identify the database for each project. If you copy an existing project database or create a new database, Domain Migration Administrator does not recognize that database unless the appropriate entries exist in the Protar database. If you delete a database, the entry for that project still exists in the Protar database.

Tables in the Protar Database

Domain Migration Administrator uses the Protar database to store information about its current state. For example, the Protar database includes tables to store migration actions, project settings, source and target information, and report data. The following sections provide information about some of the tables in the Protar database.

Settings Table

The Protar database maintains a settings table to store the many settings you specify as you run Domain Migration Administrator. When you choose options in a wizard, Domain Migration Administrator writes your choices into the settings table. The stored setting can then maintain a record of your choices from one operation to another within Domain Migration Administrator. Each record in the settings tables has three fields defined as follows:

Property

Specifies the name of a wizard setting option, such as `OptionsSourceDomain`.

Variable Type

Identifies the type of information stored in the value field, such as 8 to indicate a string value or 3 to indicate a numeric value.

Value

Specifies the property value for this property as a logical value, string value, or numeric value. For example, this value could be `Yes` or `No`, a numeric value such as 15, or a string such as `pathname`.

Domain Migration Administrator stores these settings to direct its migration operations and to maintain the values as you work through a migration.

Project databases also contain a settings table. Using the settings table, each project can maintain its own set of migration values from one migration to the next.

Action History Table

Domain Migration Administrator uses the action history table to track all the settings used to perform a particular action. When you run a wizard, Domain Migration Administrator generates an action ID for that particular run and stores the settings in the action history table. This table stores every action from every project.

The action history table stores the same information as the settings table, with the addition of the action ID. The information in this table lets you retry or undo actions or perform migration actions using the Domain Migration Administrator command line interface (DMACLI).

Migrated Objects Table

Domain Migration Administrator uses the migrated objects table to store information about every object that is migrated and track which objects have been migrated during various actions. This tracking allows Domain Migration Administrator to update group memberships, for example, even when you migrate groups and their members during different sessions. The migrated objects table includes the following fields:

ActionID

Specifies a unique identifier for the action when this object was migrated.

Time

Specifies the date and time Domain Migration Administrator performed this action.

SourceDomain

Identifies the name of the source domain of the objects that were migrated.

TargetDomain

Identifies the name of the target domain.

SourceAdsPath

Identifies the Active Directory path of the source account, such as `\\DomainA\TestAcct`

TargetAdsPath

Identifies the Active Directory path of the target account, such as `LDAP://DomainB.com/CN=TestAcct,CN=Users,DC=DomainB,DC=com`

Status

Indicates whether the account has been created or replaced and some additional information. For example, a status of 1 indicates a created account and 6 indicates a replaced account.

SourceSamName

Specifies the `SamAccountName` property of the source object.

TargetSamName

Specifies the `SamAccountName` property of the target object.

Type

Specifies whether the account is a User, Group, or Computer object.

GUID

Specifies the target domain GUID for the object.

SourceRid

Specifies the RID of the object in the source domain.

TargetRid

Specifies the RID of the object in the target domain.

SidHistory

Specifies **Yes** or **No** to indicate whether the SID History information is attached to the object being migrated.

SourceComment

Provides a comment area for the source account.

TargetComment

Provides a comment area for the target account.

SourceFullname

Specifies the Fullname property of the source account.

TargetFullname

Specifies the Fullname property of the target account.

GUID

Identifies the type of information stored in the value field. Choices are 8 to indicate a string value or 3 to indicate a numeric value.

DisplayFlags

Specifies whether to display a User, Group, or Computer icon for the object. For example, a local group specifies 268443648 and a global group specifies 268439552.

Security Translation Table

The security translation table contains information about all the security translation operations performed using the current installation of Domain Migration Administrator. Information from this table helps track migration complete and incomplete migration tasks. This table specifies the following information:

ActionID

Specifies a unique identifier for the action when this object was migrated.

Server

Specifies the name of the server where the translation occurred.

DomainName

Identifies the name of the source domain of the objects that were migrated.

Account

Specifies the SamAccountName property of the source object.

Reference Type

Specifies the type of object being translated, such as files, shares, or printers.

Status

Specifies the translation mode. Domain Migration Administrator assigns the values for the status field as shown in the following table.

Status Value	Meaning
0	Not translated
1	Added
2	Removed
3	Replaced

Projects Table

The projects table in the Protar database identifies all project databases. Each project you create with Domain Migration Administrator has an entry in the projects table with the following fields:

ProjectID

Identifies a unique project ID for each project.

ProjName

Identifies the name you assigned for the project when you defined the project using Domain Migration Administrator.

Description

Specifies a description of the project.

Created

Specifies the creation time and date of the project.

Appendix F

Native-Mode Source Domain Password Migration

Migrating passwords from a native-mode domain to a domain in a different forest requires the use of the Password Export Server (PES) installed on a domain controller in the source domain. Domain Migration Administrator interfaces with the PES to migrate passwords between domains.

<input checked="" type="checkbox"/>	Migrating Passwords Between Forests
<input type="checkbox"/>	1. Generate a Password Export Server encryption key file. For more information, see “Creating a Password Export Server Encryption Key File” on page 236.
<input type="checkbox"/>	2. Install the appropriate version of PES on the source domain controller. For more information, see “Installing Password Export Server (PES)” on page 236.
<input type="checkbox"/>	3. Configure permissions and group policy. For more information, see “Configuring Permissions and Group Policy for Password Migration” on page 239.
<input type="checkbox"/>	4. Migrate user accounts. For more information, see “Migrating User Accounts” on page 123.

Creating a Password Export Server Encryption Key File

When Domain Migration Administrator migrates users from a native-mode domain to a domain in a different forest, it uses PES in the source domain to change the password in the target domain. To maintain the integrity of the passwords in the source domain, PES requires a trusted connection with whatever is requesting the password change. Domain Migration Administrator establishes this trusted connection by generating a PES encryption key file. This key file is specific to the source domain and the Domain Migration Administrator computer on which you generated the file. When you install PES, use this file to secure a trusted communication between PES and Domain Migration Administrator.

To create a PES encryption key file:

1. Install the Microsoft 128-bit high encryption pack on the Domain Migration Administrator computer.
2. Click **Domain Migration Administrator** or a specific project in the left pane of the main window.
3. Select **Create Password Export Server Encryption Key** from the Action menu.
4. Specify the information in the Password Export Server (PES) Encryption Key Creation window, and then click **Create Key**. For more information about an option, click **Help**.

Installing Password Export Server (PES)

When Domain Migration Administrator migrates user accounts from a native-mode domain to a domain in a different forest, it uses Password Export Server (PES) to change the password in the target domain. To enable Domain Migration Administrator to copy passwords from the source domain, install PES on a domain controller in the source domain.

Domain Migration Administrator provides an installer for both PES 2.0 and PES 3.1. Install the version of PES that is appropriate for the operating system of the Domain Migration Administrator console computer, as described in the following procedure.

Note

Password Export Server (PES) 2.0, which is appropriate for Domain Migration Administrator installed on a computer running Microsoft Windows Server 2003, Windows XP, or an earlier supported operating system, does not support 64-bit systems.

To install PES:

1. Log on with an administrator account to a domain controller in the source domain.
2. Install the Microsoft 128-bit high encryption pack on the domain controller.
3. *If Domain Migration Administrator is installed on a computer running Microsoft Windows Server 2003, Windows XP, or an earlier supported operating system*, copy the following PES 2.0 files from the Domain Migration Administrator computer to the domain controller:

- pwdmi g. exe
- pwdmi g. i ni
- pwdmi g. msi

By default, these files are located in the Program Files\NetIQ\DMA\PES\Version 2.0 folder.

4. *If Domain Migration Administrator is installed on a computer running Microsoft Windows Vista or a later supported operating system and the source domain controller is a 32-bit computer*, copy the following PES 3.1 file from the Domain Migration Administrator computer to the domain controller:

- pwdmi g. msi

By default, this file is located in the Program Files\NetIQ\DMA\PES\Version 3.1 folder.

5. *If Domain Migration Administrator is installed on a computer running Microsoft Windows Vista or a later supported operating system and the source domain controller is a 64-bit computer*, copy the following PES 3.1 file from the Domain Migration Administrator computer to the domain controller:

- pwdmi g64. msi

By default, this file is located in the Program Files\NetIQ\DMA\PES\Version 3.1 folder.

6. Be prepared to supply the PES encryption key file you created for the source domain and the Domain Migration Administrator computer. For more information, see “Creating a Password Export Server Encryption Key File” on page 236.
7. Run the appropriate `pwdmi g. msi` or `pwdmi g64. msi` program on the source domain controller.
8. Follow the instructions until you have finished installing PES.
9. Set the `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\AllowPasswordExport` registry value to 1. Setting this value to 1 enables the PES to accept password migration requests. To disable the PES, set this registry value to 0.

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.

10. *If you installed PES 3.1 on the source domain controller*, manually start the Password Export Server Service before doing any password migration.

Configuring Permissions and Group Policy for Password Migration

Using PES to copy passwords when migrating from a native-mode domain to a domain in a different forest requires certain permissions and group policy settings on the target domain. Configure the following permissions and group policy settings on the target domain:

- Allow Anonymous access group policy on the target domain controllers.
 - On a Microsoft Windows 2000 target domain, set the **Additional restrictions for anonymous connections** group policy to **None** or **undefined**.
 - On a Microsoft Windows Server 2003 or Microsoft Windows Server 2008 target domain, set all of the **Security Options** group policies that restrict anonymous access to **allow access**. For example, set the **Network access: Do not allow anonymous enumeration of SAM accounts** and **Network access: Restrict anonymous access to Named Pipes and Shares** to **allow access**.
- Grant the Pre-Windows 2000 Compatible Access group Read permissions to the CN=Server, CN=System, DC=*targetdom*, DC=*t/d* object, where DC=*targetdom*, DC=*t/d* is the distinguishedName of the target domain.
- Make the Everyone group a member of the Pre-Windows 2000 Compatible Access group. Active Directory Users and Computers application blocks this action. To add the Everyone group to the Pre-Windows 2000 Compatible Access group, run the following command:

```
NET LOCALGROUP "PRE-WINDOWS 2000 COMPATIBLE ACCESS" EVERYONE /ADD
```
- On a Microsoft Windows Server 2003 or Microsoft Windows Server 2008 target domain, make the ANONYMOUS LOGON user account a member of the Pre-Windows 2000 Compatible Access group.

