Quest®

Binary Tree® Migrator Pro for Active Directory

Security Guide

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our Web site (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal .

Trademarks

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

Legend

! **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

ℹ **IMPORTANT**, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

Migrator Pro for Active Directory - Security Guide
Updated – May 26, 2022

Contents

Introduction 4

About Migrator Pro for Active Directory 5

Architecture Overview 6

Overview of Data Handled by Migrator Pro for Active Directory 7

Location of Customer Data 8

Privacy and Protection of Customer Data 9

Network Communications 10

Authentication of Users 11

Role Based Access Control 12

FIPS 140-2 compliance 13

SDLC and SDL 14

Customer Measures 15

About us 16

1

Introduction

Managing information system security is a priority for every organization. In fact, the level of security provided by software vendors has become a differentiating factor for IT purchase decisions. Quest strives to meet standards designed to provide its customers with their desired level of security as it relates to privacy, confidentiality, integrity, and availability.

This document describes the security features of Binary Tree Migrator Pro for Active Directory. It reviews access control, protection of customer data, secure network communication, cryptographic standards and more.

2

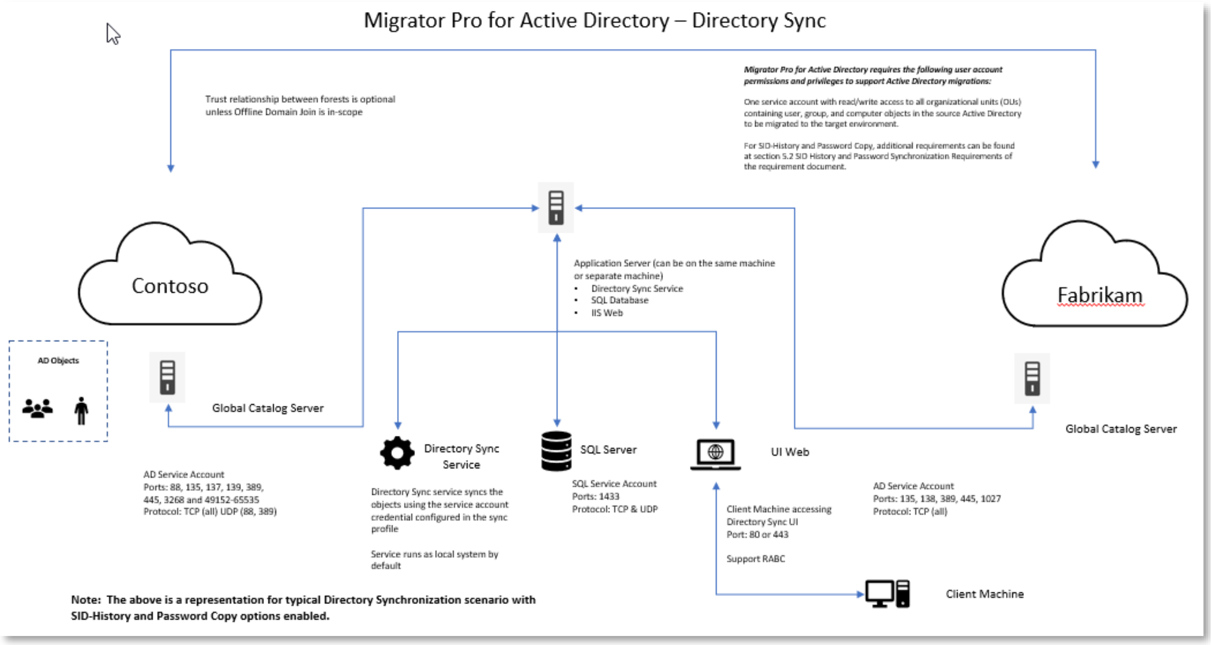
About Migrator Pro for Active Directory

Binary Tree Migrator Pro for Active Directory provides the following functionality:

- Full directory synchronization of users, groups, and devices with configurable profiles.
- Data transformation and customizable mapping of directory attributes.
- Password hash synchronization.
- SID History migration.
- Device migration including permissions and offline domain join.
- Network share permissions migration.

3

Architecture Overview



Migrator Pro for Active Directory – Directory Sync

Trust relationship between forests is optional unless Offline Domain Join is in-scope

Migrator Pro for Active Directory requires the following user account permissions and privileges to support Active Directory migrations:

One service account with read/write access to all organizational units (OUs) containing user, group, and computer objects in the source Active Directory to be migrated to the target environment.

For SID-History and Password Copy, additional requirements can be found at section 5.2 SID History and Password Synchronization Requirements of the requirement document.

Application Server (can be on the same machine or separate machine)
- Directory Sync Service
- SQL Database
- IIS Web

AD Service Account
Ports: 88, 135, 137, 139, 389, 445, 3268 and 49152-65535
Protocol: TCP (all) UDP (88, 389)

Directory Sync service syncs the objects using the service account credential configured in the sync profile

Service runs as local system by default

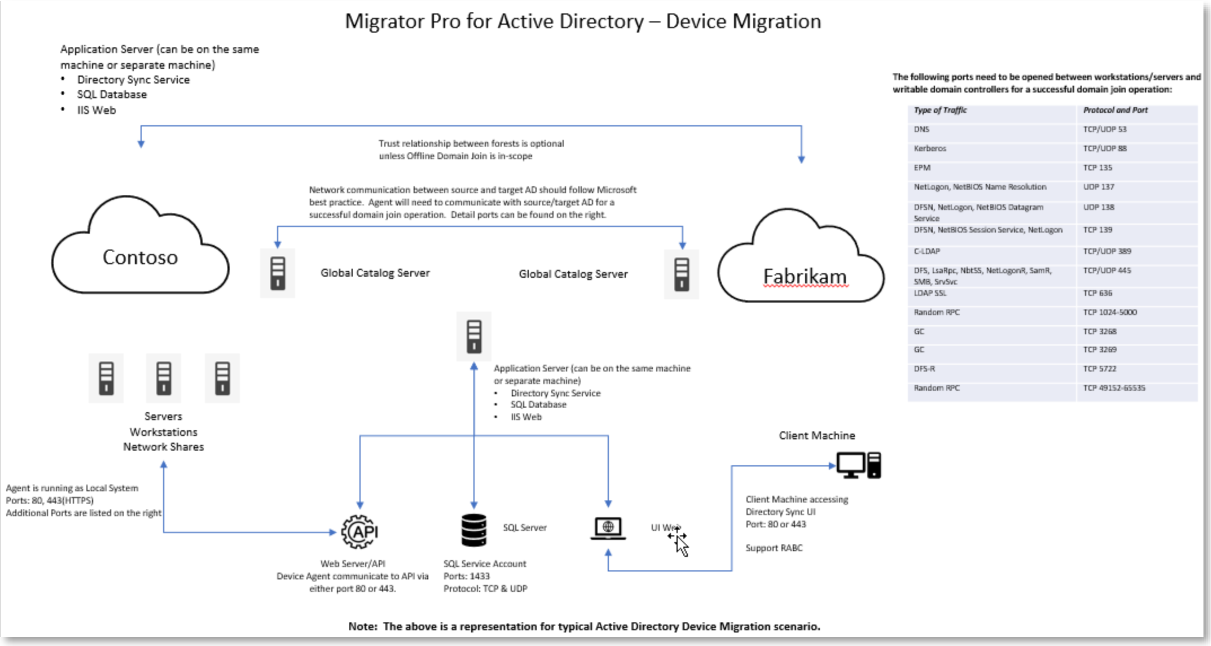
SQL Service Account
Ports: 1433
Protocol: TCP & UDP

Client Machine accessing Directory Sync UI
Port: 80 or 443

Support RABC

AD Service Account
Ports: 135, 138, 389, 445, 1027
Protocol: TCP (all)

Note: The above is a representation for typical Directory Synchronization scenario with SID-History and Password Copy options enabled.



Migrator Pro for Active Directory – Device Migration

Application Server (can be on the same machine or separate machine)
- Directory Sync Service
- SQL Database
- IIS Web

Trust relationship between forests is optional unless Offline Domain Join is in-scope

Network communication between source and target AD should follow Microsoft best practice. Agent will need to communicate with source/target AD for a successful domain join operation. Detail ports can be found on the right.

Application Server (can be on the same machine or separate machine)
- Directory Sync Service
- SQL Database
- IIS Web

Agent is running as Local System
Ports: 80, 443(HTTPS)
Additional Ports are listed on the right

Web Server/API
Device Agent communicate to API via either port 80 or 443.

SQL Service Account
Ports: 1433
Protocol: TCP & UDP

Client Machine accessing Directory Sync UI
Port: 80 or 443

Support RABC

The following ports need to be opened between workstations/servers and writable domain controllers for a successful domain join operation:

Type of Traffic	***Protocol and Port***
DNS	TCP/UDP 53
Kerberos	TCP/UDP 88
EPM	TCP 135
NetLogon, NetBIOS Name Resolution	UDP 137
DFSN, NetLogon, NetBIOS Datagram Service	UDP 138
DFSN, NetBIOS Session Service, NetLogon	TCP 139
C-LDAP	TCP/UDP 389
DFS, LsaRpc, NbtSS, NetLogonR, SamR, SMB, SrvSvc	TCP/UDP 445
LDAP SSL	TCP 636
Random RPC	TCP 1024-5000
GC	TCP 3268
GC	TCP 3269
DFS-R	TCP 5722
Random RPC	TCP 49152-65535

Note: The above is a representation for typical Active Directory Device Migration scenario.

4

Overview of Data Handled by Migrator Pro for Active Directory

Migrator Pro for Active Directory collects data for a variety of directory objects. The directory objects and properties collected are configurable to ensure only the desired objects and properties are processed.

- A directory sync service, running within the customers network, processes Active Directory objects using LDAP. Objects include users, groups, contacts, and computers. Properties include account name, email addresses, contact information, department, membership and more.
- LDAP credentials, provided by migration operators, are encrypted with AES-256 and stored in SQL Server.
- When the optional password sync feature is enabled, the NTLM password hash of all user accounts in scope are collected, encrypted with AES-256 and stored in SQL Server.
- Device agents running locally on the end user’s workstation collect device properties using WMI and PowerShell. Device properties include device name, domain name, user profile locations and more.
- Migrator Pro for Active Directory optionally stores credentials required for network share re-permission and Active Directory domain joins. These credentials, provided by migration operators, are encrypted with AES-256 and stored in SQL Server.

5

Location of Customer Data

- All computation is performed on server(s) provided by the customer.
- All data and application logs are stored in a SQL server provided by the customer.

6

Privacy and Protection of Customer Data

The most sensitive customer data collected and stored by Migrator Pro for Active Directory is the Active Directory data including users, password hashes, groups, contacts, and devices.

- SQL Server Transparent Data Encryption (TDE) can be enabled to encrypt all data at rest. For more information see https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption?view=sql-server-ver15.
- LDAP account passwords and NTLM password hashes (while already encrypted at-rest by TDE) are additionally encrypted by the application with AES-256.

7

Network Communications

- All communication from the Migrator Pro for Active Directory user interface is secured with HTTPS TLS 1.2.
- The directory sync service communicates with Active Directory using LDAP.
- Device agents communicate securely with the Migrator Pro for Active Directory web service using HTTPS TLS 1.2 to retrieve job details.

Migrator Pro for Active Directory relies on the following network ports to enable full functionality:

Source	Target	Port/Protocol
Workstations and Member Servers	Migrator Pro for Active Directory Server	443 (TCP) or 80 (TCP)
Migrator Pro for Active Directory Server	Source and Target Domain Controllers running Windows Server 2003	135, 137, 389, 445, 1024-5000 (TCP) and 389 (UDP)
Migrator Pro for Active Directory Server	Source and Target Domain Controllers running Windows Server 2008 or newer	135, 137, 389, 445, 49152-65535 (TCP) and 389 (UDP)
Target domain controllers listed in the Target DCs tab	Domain controller in the source environment holding the PDC Emulator Active Directory FSMO role	135, 137, 139, 389, 445, 3268 and 49152-65535 (TCP) and 389 (UDP)

The following ports need to be opened between workstations/servers and writable domain controllers for a successful domain join operation:

Type of Traffic	Protocol and Port
DNS	TCP/UDP 53
Kerberos	TCP/UDP 88
EPM	TCP 135
NetLogon, NetBIOS Name Resolution	UDP 137
DFSN, NetLogon, NetBIOS Datagram Service	UDP 138
DFSN, NetBIOS Session Service, NetLogon	TCP 139
C-LDAP	TCP/UDP 389
DFS, LsaRpc, NbtSS, NetLogonR, SamR, SMB, SrvSvc	TCP/UDP 445
LDAP SSL	TCP 636
Random RPC	TCP 1024-5000
GC	TCP 3268
GC	TCP 3269
DFS-R	TCP 5722
Random RPC	TCP 49152-65535

8

Authentication of Users

- Migrator Pro for Active Directory relies upon Windows Authentication and Active Directory group membership to authenticate users.

9

Role Based Access Control

Migrator Pro for Active Directory restricts access to features, functions and data based on role membership described below.

Global Administrator

- Allows creation of new profiles
- Allows modification of configuration in the application/database for all profiles
- Allows creation or modification of Cutover activities and custom actions for all profiles
- Can submit migration events, including ReACL and Cutover actions for workstations, as well as user Cutover actions (enable/disable) for all profiles
- All configuration pages can be accessed

Profile Administrator

- Cannot create of new profiles
- Can submit migration events, including ReACL and Cutover actions for workstations, as well as user cutover actions (enable/disable)
- All configuration pages can be accessed
- Allow modification of configuration in the application/database
- Allow creation or modification of Cutover activities and custom actions

Migration Operator

- Can submit migration events, including ReACL and Cutover actions for workstations, as well as user cutover actions (enable/disable)
- Configuration pages cannot be accessed
- Cannot modify configuration in the application/database
- Cannot create or modify Cutover activities and custom actions

Read Only User

- Can view directory synchronization results and logs
- Can view Active Directory Cutover status
- Configuration pages cannot be accessed
- Cannot modify configuration in the application/database
- Cannot create or modify Cutover activities and custom actions

10

FIPS 140-2 compliance

Migrator Pro for Active Directory cryptographic usage is based on FIPS 140-2 compliant cryptographic functions. Migrator Pro for Active Directory makes use of FIPS 140-2 compliant encryption keys stored locally.

More information:

- Microsoft and FIPS: https://docs.microsoft.com/en-us/compliance/regulatory/offering-FIPS-140-2?view=o365-worldwide

11

SDLC and SDL

The Migrator Pro for Active Directory Development team follows a managed Software Development Lifecycle (SDLC).

The Migrator Pro for Active Directory team follows a strict Quality Assurance cycle.

- Access to source control and build systems is protected by domain security. Only employees on Quest's corporate network have access to these systems. If a developer leaves the company, they will no longer be able to access Quest systems.
- All code is versioned in source control.
- All product code is reviewed by another developer before check in.

The Migrator Pro for Active Directory team follows a managed Security Development Lifecycle (SDL) which includes:

- MS-SDL best practices
- Threat modeling
- OWASP guidelines
- Static code analysis scanning is performed on regular basis
- Software composition analysis scanning is performed on regular basis
- Migrator Pro for Active Directory has been validated in a Secure Technical Implementation Guidelines (STIG) environment. See https://public.cyber.mil/stigs/ for more information.
- As an additional layer of security against possible development environment threats, and as part of its sandbox testing environment the development team monitors traffic of Migrator Pro for Active Directory on a continuous basis. This monitoring includes an evaluation of the outgoing traffic for any malicious communications.

Migrator Pro for Active Directory developers go through the same set of hiring processes and background checks as other Quest employees.

12

Customer Measures

Migrator Pro for Active Directory security features are only one part of a secure environment. Customers should follow their own security best practices when deploying Migrator Pro for Active Directory.

About us

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation™.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece — you — to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit www.quest.com/contact.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product.