

Directory Sync Pro for Active Directory and Migrator Pro
for Active Directory 20.11.2

Requirements and Installation Guide

© 2024 Quest Software Inc.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

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

20 Enterprise, Suite 100

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.

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

Table of Contents

Section 1. Introduction	5
1.1 Purpose	5
1.2 Audience	5
1.3 Certifications	5
Section 2. Directory Sync Pro Prerequisites	6
2.1 Supported Environments.....	6
2.2 Quest Windows Server Requirements.....	6
2.3 SQL Server Database Requirements	8
2.4 General Requirements	8
2.5 Exchange Access Requirements.....	9
2.6 Post Sync PowerShell Script Requirements	9
Section 3. Directory Sync Pro for Active Directory Advanced Network Requirements	10
3.1 Directory Sync Pro for Active Directory to SQL Server Access.....	10
3.2 Directory Sync Pro for Active Directory Profile Specific Scenario Requirements	10
Section 4. Migrator Pro for Active Directory Prerequisites	11
4.1 Migrator Pro for Active Directory Basic Installation Requirements	11
4.2 Workstation and Member Server System Requirements	13
4.3 Admin Agent Device Requirements.....	13
4.4 Networking Requirements	14
4.5 SSL Certificate Requirements	15
4.6 Service Account Requirements	15
4.7 SQL Server Reporting Services (SSRS) Account Requirements.....	16
4.8 DNS SRV Record Requirement	18
4.9 Offline Domain Join (ODJ) Requirements	18
Section 5. Requirements for Both Directory Sync Pro for Active Directory and Migrator Pro for Active Directory.....	20
5.1 Browser Requirements.....	20
5.2 SID History and Password Synchronization Requirements	20
5.3 Password Requirements	22
5.4 Internet Requirement for Online Help and Video Tutorials.....	22
Section 6. Installing Directory Sync Pro for Active Directory and Migrator Pro for Active Directory.....	23
6.1 Installing Directory Sync Pro for Active Directory and Migrator Pro for Active Directory on a	

Windows Server	23
Section 7. Upgrading Directory Sync Pro for Active Directory and Migrator Pro for Active Directory	33
7.1 Supported Upgrade Path.....	33
7.2 Upgrade Process	33
Section 8. Modifying, Repairing and Uninstalling Directory Sync Pro for Active Directory and Migrator Pro for Active Directory	35
Section 9. Migrator Pro for Active Directory Agent Installation	36
9.1 Installing the Migrator Pro for Active Directory Agent on Devices	36
Section 10. Troubleshooting	41
10.1 Migrator Pro for Active Directory Agent Installation Troubleshooting	41
Appendix A: Configuring Directory Sync Pro for Active Directory in a Non-English Active Directory Environment.....	42
Appendix B. Installing and Configuring SQL Server Reporting Services	43
Installing SQL Server Reporting Services	43
Configuring SQL Server Reporting Services	43
Your Report URLs.....	44
Verifying the Report Server URL.....	45
Appendix C. STIG Environments	46
SQL Express.....	46
SID History.....	46
Additional Information	47
Appendix D. Deployment in FIPS Environment.....	48
Cryptographic usage.....	48
Background.....	48
Prerequisites	49
Installation and operation	49
References	50

Section 1. Introduction

1.1 Purpose

This document details the following:

- Requirements for implementing Directory Sync Pro and Migrator Pro for Active Directory. These include the requirements for each of the servers needed to run Directory Sync Pro, as well as any environmental requirements.
- Information on how to install Directory Sync Pro for Active Directory and Migrator Pro for Active Directory.

1.2 Audience

This document assumes the reader has Active Directory and Exchange administration skills. If Active Directory or Exchange Administration topics mentioned in this document are not understood, please reference the product(s) System Administration documentation.

1.3 Certifications

- All AD Functional Levels supported by Microsoft for a Microsoft Windows Server operating system listed below are supported for migration from/to Domain controllers running on that same Operating System. For example, Windows Server 2016 functional levels are supported on Windows Server 2022, Windows Server 2019, and Windows Server 2016. For full details see Microsoft's documentation of [Active Directory Domain Services Functional Levels in Windows Server](#) on Microsoft Learn.



NOTE: Windows Server 2003 functional levels are supported only on Windows Server 2016, Windows Server 2012 R2, and Windows Server 2012. That is, Microsoft does not support Windows Server 2003 functional levels on Windows Server 2019 or Windows Server 2022.



NOTE: Microsoft's lifecycle for Windows Server 2012 ends extended support on October 10, 2023. Customers should be planning to move their Domain Controllers off of Windows Server 2012 and Windows Server 2012 R2 by that date.

- Directory Sync Pro for Active Directory and Migrator Pro for Active Directory supports TLS 1.2 only connections.

Section 2. Directory Sync Pro Prerequisites

2.1 Supported Environments

The following is a list of supported and unsupported environments. If implementing directory synchronization between two Active Directory environments, you will need a Quest Windows Server and an SQL Server database server.

	Supported	Not Supported
Binary Tree Windows Server	Windows Server 2016, Windows Server 2019, or Windows Server 2022; US English Operating System	All other versions of Windows Server
SQL Server Database	<p>SQL Server can be a new or existing database server in the customer's environment. The following SQL Server versions (English versions) are supported:</p> <ul style="list-style-type: none"> • SQL Server 2012 SP2 • SQL Server 2012 SP2 Express with Advanced Services • SQL Server 2014 • SQL Server 2014 Express with Advanced Services • SQL Server 2016 • SQL Server 2016 Express with Advanced Services • SQL Server 2017 • SQL Server 2017 Express with Advanced Services • SQL Server 2019 • SQL Server 2019 Express with Advanced Services • SQL Server 2022 • SQL Server 2022 Express with Advanced Services 	<p>SQL Server 2008 R2 or previous</p> <p>Reporting using SQL Server Reporting Services 2016 or SQL Server Express Reporting Services 2016</p>
Domain	<p>The following Windows Server versions are supported:</p> <ul style="list-style-type: none"> • Windows Server 2012 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022 	

NTLM Authentication is required for the product to function. NTLM Authentication options are typically controlled via Group Policy. These three settings should be verified:

- Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers
 - Microsoft Outlines this setting here: <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-restrict->

[ntlm-outgoing-ntlm-traffic-to-remote-servers](#)

- The registry key for this setting is located at:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0
- The RestrictSendingNTLMTraffic key, with DWORD value will be present. If the key is missing, then this setting is not being leveraged. If the key is set to 2, the “deny all” option has been set to restrict all out going NTLM Traffic. If the key is set to 1, the “audit all” option has been set, which will only log when outgoing NTLM traffic is detected. If the key is set to 0, then “allow all” is configured and there are not restrictions on sending NTLM traffic in place.
- Network security: Restrict NTLM: Incoming NTLM traffic
 - Microsoft Outlines this setting here: <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-restrict-ntlm-incoming-ntlm-traffic>
 - The registry key for this setting is located at:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0
 - The RestrictReceivingNTLMTraffic key, with a DWORD value will be present. If the key is missing, then this setting is not being leveraged. If the key is set to 2, the “deny all” option has been set to restrict all incoming NTLM Traffic. If the key is set to 1, the “audit all” option has been set, which will only log when Incoming NTLM traffic is detected. If the key is set to 0, then “allow all” is configured and there are not restrictions on receiving NTLM traffic in place.
- Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication
This allows for exclusions from the two policies below for a computer
 - Microsoft Outlines this setting here: <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-restrict-ntlm-add-remote-server-exceptions-for-ntlm-authentication>
 - The registry key for this setting is located at:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0
 - The ClientAllowedNTLMServers key, with REG_MULTI_SZ values will be present. If the key present, but is empty, there are no allowed exceptions. If they key is present, and lists servers, these are the servers that allow NTLM communication to. If the key is missing, then this setting is not being leveraged.

2.2 Quest Windows Server Requirements

- .NET 4.8 or greater. The installer will install .NET 4.8 if the target machine does not already have it. All system patches, service packs, and security updates should be applied to you operating system to ensure compatibility with .NET 4.8.
- IPv4 Only
- The user running the Directory Sync service (full name BinaryTree.DirSync.Exchange.exe) must have the following rights:
 1. Administrator rights to SQL Server with sysadmin role (during installation).
 2. Local administrative rights to the Quest Windows server (during installation).
- Exchange cannot be installed on an Exchange Server.

- The Quest Windows Server must be a dedicated server for the Quest solutions.
- The Quest Windows Server can be a workgroup (non-domain joined) server. Note, in order to use Migrator Pro for Active Directory's Role Based Access Control functionality, product must be installed and configured on a Domain Joined server.

2.3 SQL Server Database Requirements

- The IP address and either the default SQL port (1433) or an alternate port must be open to all Quest servers.
- The ability to create and modify tables in the Dirsync database on the SQL Server database server.
- It is strongly recommended that the SQL Server database server is dedicated to SQL Server. This server can host other SQL databases, but should serve no other purpose than being a SQL Server database server.
- SQL Server must be configured using Mixed Mode authentication.
- Using the default system administrator SQL Server login account is not recommended. A Directory Sync SQL Server login account should be created. This account must have sysadmin and database owner rights to create the Dirsync database. The sysadmin right can be removed from this account once the install is complete.
- If using a Remote Named Instance of SQL Server:

The incoming firewall rules on the machine that hosts the SQL Server instance must be modified.

Using the SQL default of dynamic ports for named instances:

1. Create an inbound firewall "Program" rule whose program path is the named SQL database engine (ex: %ProgramFiles%\Microsoft SQL Server\MSSQL14.<INSTANCE-NAME>\MSSQL\Binn\sqlservr.exe)
2. Create an inbound firewall "Port" rule for UDP port 1434.
3. The "SQL Server Browser" must be running.

Alternatively, you can setup a fixed port for the SQL instance following these [instructions](#).

2.4 General Requirements

- All components of Directory Sync Pro are fully functional on physical as well as virtual machines. When setting up Proof of Concept or Pilot environments, the use of virtual machines as a means of lowering the expense of such projects is fully supported and recommended. However, when it comes to production environments, sufficient information to determine whether virtual environments have the same stability and performance characteristics as physical machines has not yet been gathered. Because a majority of production environments have been and are deployed on physical machines, potential customers are advised of these facts, but defers to them to make the final decision. Product support will be provided in both physical and virtual environments. However, if either stability or performance issues are found in a virtual environment, switching to a physical one as a means of issue correction may be recommended.
- Quest Servers must be connected via a LAN (10MB or higher) connection. A high-speed WAN (5MB or higher) connection may be acceptable, but is not recommended. Where possible, it is recommended to have these servers, as well as Exchange on the same physical network.

2.5 Exchange Access Requirements

To deploy Directory Sync Pro on the Quest Windows Server, an AD account with Server Administration rights must be able to log on to the server interactively. The account must be able to run programs with Administration-level access on the target Exchange Server and specifically be able to open the Exchange Management Shell (PowerShell).

The following setup for the service account is recommended:

Active Directory

- Minimum membership of Domain Users (least privilege) built-in security group
- Read & List Contents rights to "Deleted Objects" container. You may follow these steps if your account is not a Domain Administrator or equivalent (see KB892806):

Using a domain admin account, open a command prompt and confirm the successful execution of the following commands:

```
dsacls "CN=Deleted Objects,DC=domain,DC=com" /takeownership
```

```
dsacls "CN=Deleted Objects,DC=domain,DC=com" /g Domain\ServiceAccount:LCRP
```

- Full Control rights to destination OU in Active Directory

Exchange

- Administrative rights to Exchange

SQL Server

- Create a new login in the SQL Server Management Studio. In Server Roles, grant public and sysadmin rights (you may remove these rights after the **database** has been created). In User Mapping, select the Dirsync database and grant public and database owner rights.

Quest Windows Server

- Member of local Built-In Administrators group

2.6 Post Sync PowerShell Script Requirements

The following requirements must be met if using the Post Sync PowerShell Script option:

- PowerShell 4
- The credentials specified on the AD Target tab must have rights to run PowerShell.
- The following must be enabled on the DC defined on the AD Target tab:
 - Remote PowerShell commands (Unrestricted methods must be enabled if required)
 - Windows Remote Management (WinRM)
 - Active Directory Web Services

Section 3. Directory Sync Pro for Active Directory Advanced Network Requirements

3.1 Directory Sync Pro for Active Directory to SQL Server Access

Source	Target	Ports	Protocol
Directory Sync Pro for Active Directory	SQL Server holding the primary database	1433	TCP & UDP
Directory Sync Pro for Active Directory	SQL Server holding the logging database	1433	TCP & UDP

3.2 Directory Sync Pro for Active Directory Profile Specific Scenario Requirements

Directory Sync Pro for Active Directory Match Only or Update Only Profile (no object creation)

Source	Target	Ports	Protocol
Directory Sync Pro for Active Directory	Source Domain controllers	88, 389, 445*, 3268	TCP (all) UDP (88, 389)
Directory Sync Pro for Active Directory	Target Domain controllers	88, 389, 445, 3268	TCP (all) UDP (88, 389)

* Port 445 only needs to be open to the Source Domain Controller during Directory Sync Pro for Active Directory Profile creation

Directory Sync Pro for Active Directory Profile with Create Only or Create/Update Matching Option

Source	Target	Ports	Protocol
Directory Sync Pro for Active Directory	Source Domain controllers	88, 389, 445*, 3268	TCP (all) UDP (88, 389)
Directory Sync Pro for Active Directory	Target Domain controllers	88, 139, 389, 445, 3268	TCP (all) UDP (88, 389)

* Port 445 only needs to be open to the Source Domain Controller during Directory Sync Pro for Active Directory Profile creation

Directory Sync Pro for Active Directory Profile with Synchronize Passwords selected

Source	Target	Ports	Protocol
Directory Sync Pro for Active Directory	Source or Target Domain controllers	88, 139, 389, 445, 3268	TCP (all) UDP (88, 389)

Directory Sync Pro for Active Directory Profile with SID History Synchronization selected

Source	Target	Ports	Protocol
Directory Sync Pro for Active Directory	Source or Target Domain controllers	88, 135, 137, 139, 389, 445, 3268 and 49152-65535	TCP (all) UDP (88, 389)
Directory Sync Pro for Active Directory	Source or Target Domain controllers	88, 135, 137, 139, 389, 445, 3268 and 1024-5000	TCP (all) UDP (88, 389)
Target GC	Source PDC	135, 138, 389, 445, 1027	TCP (all)

Section 4. Migrator Pro for Active Directory Prerequisites

4.1 Migrator Pro for Active Directory Basic Installation Requirements

The Migrator Pro for Active Directory suite consists of Directory Sync Pro and Migrator Pro for Active Directory software packages. Both packages will require access to Microsoft SQL Server.

Single Server Installation Requirements

Supported Operating Systems	<ul style="list-style-type: none"> Windows Server 2016 Windows Server 2019 Windows Server 2022
SQL Server Requirements	<ul style="list-style-type: none"> SQL Server 2012 SP2 Express 64-bit, 2014, 2016, 2017, 2019, or 2022 SQL Server 2012 SP2 Express 64-bit Express is supported up to 5000 objects SQL Management Studio must be installed SQL Server Native Client 11 (Typically installed with the Directory Sync Pro and Migrator Pro for Active Directory Installation Wizard if necessary) SQL must be configured to permit mixed authentication, and one local SQL authentication account must be created for Migrator Pro for Active Directory and Directory Sync Pro for Active Directory to share.
Minimum Hardware Requirements	<ul style="list-style-type: none"> 2 CPU/vCPU 6GB RAM 10 GB disk space, inclusive of the SQL install requirements
Additional Components	<ul style="list-style-type: none"> If your server is not internet connected, you will be required to install the following components prior to installing Migrator Pro for Active Directory: <ul style="list-style-type: none"> .NET Framework 4.8 or newer Visual C++ 2013 Redistributable – BOTH the x64 and x86 versions must be installed, regardless of the fact that the Windows Operating system is 64-bit

If you are planning to have a long-term co-existence (1 year+), we recommend using the following formula to determine if you should use a full edition of SQL Server with our products. This formula assumes High / Verbose logging turned on for all profiles = worst case scenario.

Formula: (Expected months of co-existence x Users) x Profiles = N

If calculated N >= 12000 then we recommend full edition of SQL Server.

- Low example: 3 months x 300 users x 1 profile = 900
- Medium example: 6 months x 1000 users x 2 profiles = 12000
- High example: 12 months x 3000 users x 5 profiles = 180,000
- Extreme example: 14 months x 6000 users x 7 profiles = 588,000

Multi-Server Installation Requirements

Migrator Pro for Active Directory is scalable and supports segregating components and can be installed in a multi-server configuration to support larger or complex environments.

If required in larger installations, remote SQL Servers may be used for the primary database and the logging database. Additionally, the primary database and the logging database can be segregated onto separate SQL Server instances.

Each of the following roles/functions may be separated onto different servers as required in advanced configurations:

- Directory Sync Pro for Active Directory/Migrator Pro for Active Directory Administrative Web Interface
- Migrator Pro for Active Directory Web Service
- Directory Sync Pro for Active Directory Databases

When installed independently, the components require the following resources:

Supported Operating Systems	<ul style="list-style-type: none">• Windows Server 2016• Windows Server 2019• Windows Server 2022
Migrator Pro for Active Directory Split Role Minimum Hardware Requirements	<ul style="list-style-type: none">• 1 CPU/vCPU• 2GB RAM• 1 GB disk space
Directory Sync Pro for Active Directory Hardware Requirements	<ul style="list-style-type: none">• 2 CPU/vCPU• 4GB RAM• 5 GB disk space
SQL Server	<ul style="list-style-type: none">• SQL Server 2012 SP2 Express 64-bit, 2014, 2016, 2017, 2019, 2022• SQL must be configured to permit mixed authentication, and one local SQL authentication account must be created for Migrator Pro for Active Directory and Directory Sync Pro for Active Directory to share.• SQL Management Studio must be installed• Express editions of SQL Server are supported as long as the express installation includes SQL Management Studio
Additional Components	<ul style="list-style-type: none">• If your server is not internet connected, you will be required to install the following components prior to installing Migrator Pro for Active Directory:<ul style="list-style-type: none">◦ .NET Framework 4.8 or newer

- [Visual C++ 2013 Redistributable](#) – BOTH the x64 and x86 versions must be installed, regardless of the fact that the Windows Operating system is 64-bit

Report Server Requirements

SQL Server Requirements

- SQL Server 2012 SP2, 2014, 2017, 2019, or 2022
- Configured for Native Mode
- Review the *Installing and Configuring SQL Reporting Services* topic in the Migrator Pro for Active Directory documentation for more information.
-

4.2 Workstation and Member Server System Requirements

Supported Operating Systems

- Windows 10
- Windows 11
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

PowerShell Requirements

- All client operating systems must have at least PowerShell 2.0 installed.

.NET Framework Requirements

- All operating systems must have [.NET Framework 4.8](#) or newer installed.
- The “client” installation of the .NET Framework (before 4.5) is not sufficient and must be upgraded to the full .NET Framework.

4.3 Admin Agent Device Requirements

Operating System Requirements

- 64-bit operating systems only
- Windows PowerShell 4.0
- WMF 4.0 support

Supported Operating Systems

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

Additional Requirements

- Port Requirement: 80, 443
- Software Requirement: .NET Framework 4.7.2
- PowerShell Active Directory Module (only required if you want to run PowerShell scripts against Active Directory).

4.4 Networking Requirements

Domain Controller Access

For most scenarios, Migrator Pro for Active Directory requires access to at least one read/write domain controller in each source and target Active Directory domain. For fault tolerance, at least two domain controllers in each source and target domain is recommended.

If SID History will be synchronized, any domain controller listed in the Target DCs tab within a Directory Sync Pro for Active Directory profile will require access to the domain controller holding the PDC Emulator Active Directory FSMO role in the source. Keep in mind that even if the domain controller holding the PDC Emulator Active Directory FSMO role is not listed in the Source DCs tab, any SID History migration attempts will require a DC in the target to communicate with the PDC Emulator domain controller. For this reason, it is a best practice to ensure that all domain controllers specified on the Target DCs screen within a Directory Sync Pro for Active Directory profile have the appropriate networks access to communicate with the source domain controller holding the PDC Emulator Active Directory FSMO role before a SID History migration is attempted.

In limited scenarios, it is possible that Migrator Pro for Active Directory will not be responsible for creating or updating any accounts in the source or the target domains. In this scenario, Migrator Pro for Active Directory can be configured to communicate with Read Only Domain Controllers (RODCs).

Network/Firewall Requirements

Migrator Pro for Active Directory requires 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	135, 137, 389, 445, 1024-5000 (TCP) 389 (UDP)
Migrator Pro for Active Directory Server	Source and Target Domain Controllers	135, 137, 389, 445, 49152-65535 (TCP) 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) 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

4.5 SSL Certificate Requirements

Migrator Pro for Active Directory does not require HTTPS (HTTP with SSL), and can operate using HTTP. However, it is strongly recommended to implement Migrator Pro for Active Directory using HTTPS to secure communications between the devices to be migrated and the Migrator Pro for Active Directory Server. In order to activate HTTPS on the IIS component in Windows, the Migrator Pro for Active Directory system will require that a SSL certificate is present.

An SSL Certificate is not provided as part of the installation. For the most secure installation, purchasing an SSL Certificate from a Windows supported 3rd party provider is recommended.

In scenarios where this is not possible, self-signed SSL Certificate can be generated in Windows following these directions: [https://technet.microsoft.com/en-us/library/cc753127\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc753127(v=ws.10).aspx)

If using a self-signed certificate, it should be noted that Migrator Pro for Active Directory's agent component would utilize the operating system's certificate trust list. Due to the security nature of Active Directory migrations, there is no method of implementing an override and forcing the agent to use an untrusted certificate. If a self-signed certificate is used, that certificate will need to be added to the trusted root certificate list for all computer objects to be migrated. This can be accomplished via group policy: [https://technet.microsoft.com/en-us/library/cc738131\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc738131(v=ws.10).aspx)

4.6 Service Account Requirements

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.

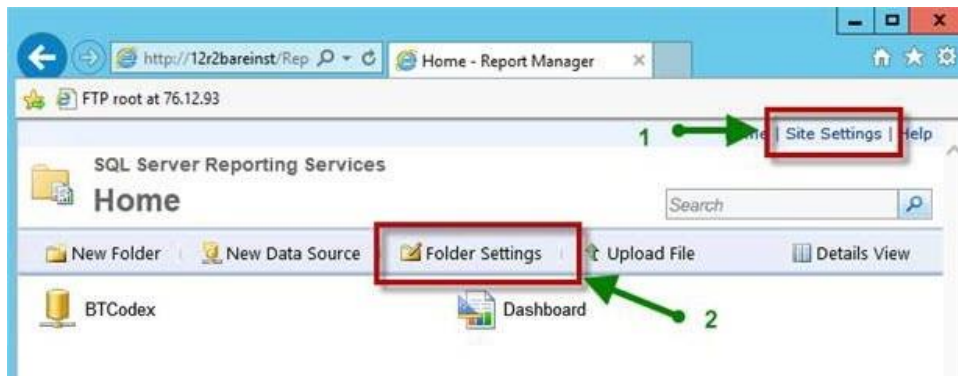
- One service account with administrative rights on the target domain(s)
 - If administrative rights cannot be granted, the service account requires the following rights:
 - The ability to create and modify user objects in the desired OUs in the target Active Directory environment.
 - Read Permissions to the configuration container in Active Directory
 - User credentials with the delegated migrateSIDHistory extended right.
- A service account in each source and target domain with the ability to modify computer objects and add computers to the domain.

4.7 SQL Server Reporting Services (SSRS) Account Requirements

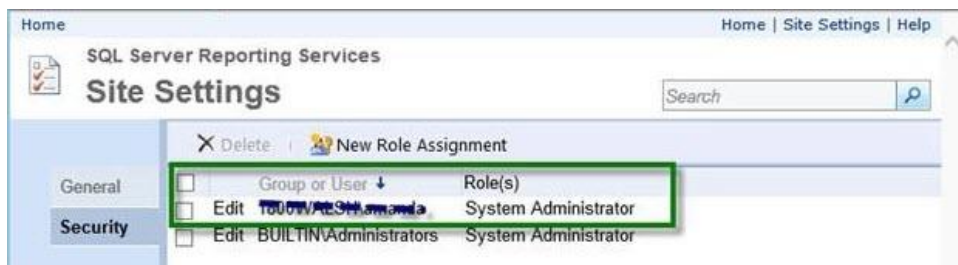
Migrator Pro for Active Directory's Reporting feature requires credentials in the following places:

- Content credential: Credential for accessing the report server content.

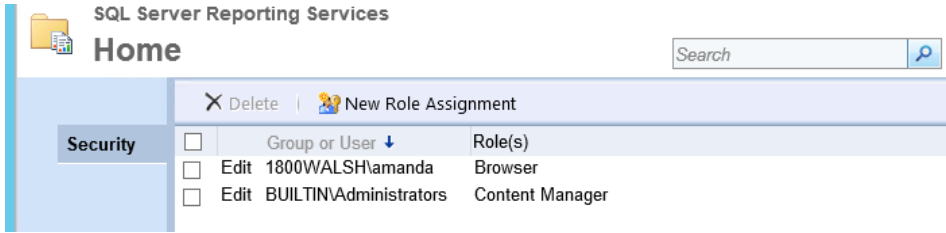
You must set the securities in two different places in the SSRS 'Report Manager' web interface (<http://<servername>/Reports>) to connect to the report server and upload reports from the installation program.



In the Site Settings, you MUST enable the 'System Administrator' role during installation. After installation is complete, you may change this user's role to 'System User' if desired.

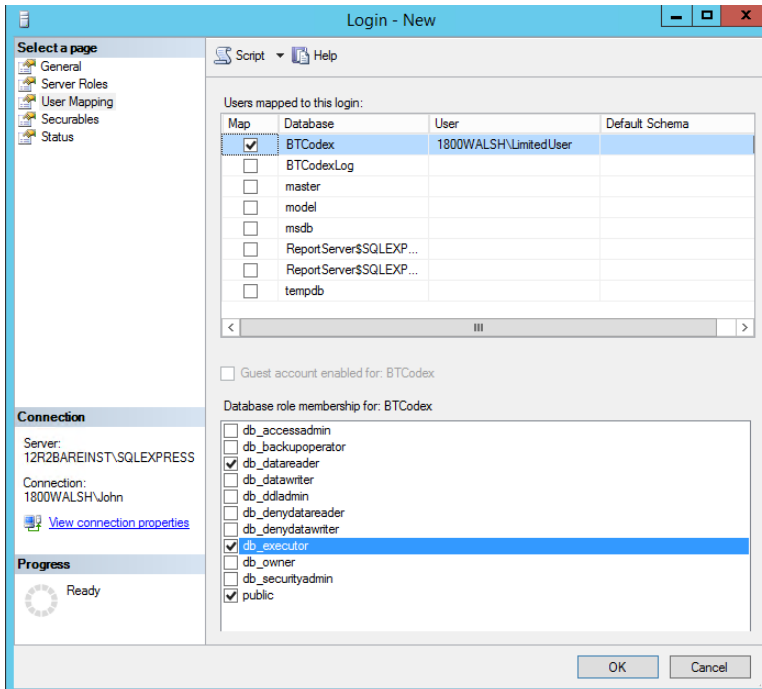


In the Folder Settings, you must add the same user with (at least) 'Browser' permission.

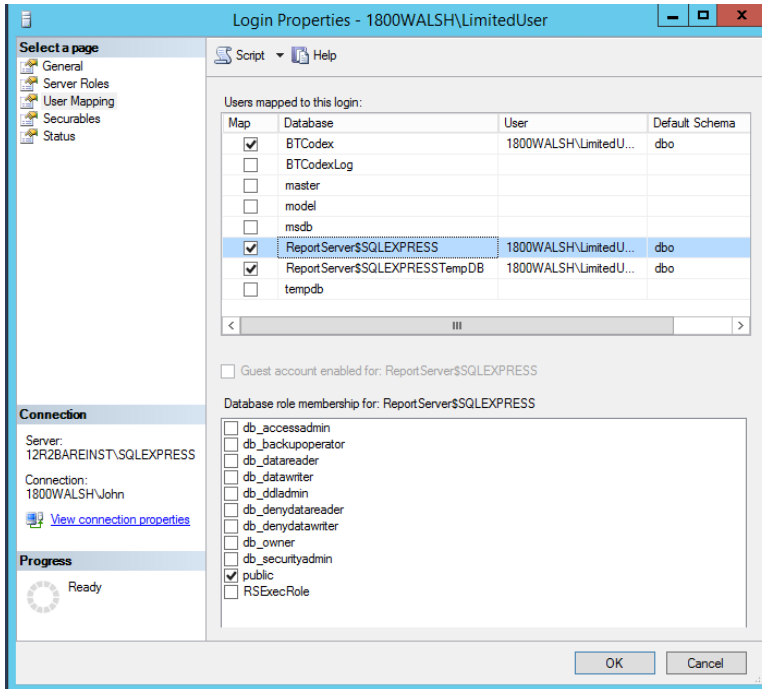


- Data Source Credential: The Data Source is used to access queries in the ADM database. These credentials and roles are set in the SQL server with SSMS

The user must have public, db_reader, and db_executor roles on the ADM database.



The user must have the public role on the report server and report server temp databases.



4.8 DNS SRV Record Requirement

In each source domain, a SRV DNS record must be created to enable autodiscover for Migrator Pro for Active Directory agents.

- To enable autodiscover when HTTPS is desired
 - Record Name: `_btadm._https.SourceDomainName.Local`
 - Weight and Priority: 0
 - Port Number: 443
- To enable autodiscover when HTTP is desired
 - Record Name: `_btadm._http.SourceDomainName.Local`
 - Weight and Priority: 0
 - Port Number: 80

4.9 Offline Domain Join (ODJ) Requirements

In order to successfully facilitate the new Cached Credentials job (which supports the Offline Domain Join feature) a one-way external trust must be configured from the source domain to the target domain.

The devices that the ODJ process is being run on must have network connectivity to BOTH the source and target environments at the same time in order to have the Cached Credentials function work properly.

Offline domain join files must be created prior to running the Offline Domain Join process. A full explanation of Microsoft's Djoin.exe utility and how to create these files can be found here:

<https://technet.microsoft.com/en-us/library/offline-domain-join-djoin-step-by-step%28v=ws.10%29.aspx>

Section 5. Requirements for Both Directory Sync Pro for Active Directory and Migrator Pro for Active Directory

5.1 Browser Requirements

Directory Sync Pro for Active Directory uses a browser-based user interface. We recommend using Edge, Chrome, or Firefox.

5.2 SID History and Password Synchronization Requirements

SID History Synchronization Requirements

Microsoft requires an administrative account in the source domain.

In order to support synchronization of SID History from the source to the target domains, Windows requires that a specific domain local group exists and that account auditing is enabled.

The source and target domains must not have the same NETBIOS name to allow the required trust between the two environments.

Communication between a Source PDC and the configured Target GC is required for SID History Migration to successfully complete. Please note, there are additional ports that must be open between the Source PDC and the configured Target GC as defined in Section 3. Directory Sync Pro for Active Directory Advanced Network Requirement's (Directory Sync Pro for Active Directory Profile with SID History Synchronization selected) of this document.

Preparing the Source and Target Domains

To prepare each source and target domain for SID History Synchronization, the following configuration steps must be completed:

- In the source domain, create a local group called SourceDomain\$\$\$, where SourceDomain is the NetBIOS name of your source domain. For example, if your domain's NetBIOS name is ADM, you must create a domain local group named ADM\$\$\$.



SID History synchronization will fail if members are added to this local group.

- Enable TCP/IP client support on the source domain PDC emulator:
 1. On the domain controller in the source domain that holds the PDC emulator operations master (also known as flexible single master operations or FSMO) role, click **Start**, and then click **Run**.
 2. In **Open**, type **regedit**, and then click **OK**.
 3. In Registry Editor, navigate to the following registry subkey:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA
 4. Modify the registry entry **TcpipClientSupport**, of data type **REG_DWORD**, by setting the value to 1.
 5. Close Registry Editor, and then restart the computer.

- Enable auditing in the target domain:
 1. Log on as an administrator to any domain controller in the target domain.
 2. Click **Start**, point to All Programs, point to Administrative Tools, and then click **Group Policy Management**.
 3. Navigate to the following node: Forest | Domains | Domain Name | Domain Controllers | Default Domain Controllers Policy
 4. Right-click **Default Domain Controllers Policy** and click **Edit**.
 5. In Group Policy Management Editor, in the console tree, navigate to the following node: Computer Configuration | Policies | Windows Settings | Security Settings | Local Policies | Audit Policy
 6. In the details pane, right-click **Audit account management**, and then click **Properties**.
 7. Click **Define these policy settings**, and then click **Success and Failure**.
 8. Click **Apply**, and then click **OK**.
 9. In the details pane, right-click **Audit directory service access** and then click **Properties**.
 10. Click **Define these policy settings** and then click **Success**.
 11. Click **Apply**, and then click **OK**.
 12. If the changes need to be immediately reflected on the domain controller, open an elevated command prompt and type *gpupdate /force*.
 13. Repeat the above steps in the source domain.



It may also be necessary to reboot the domain controller to have auditing take effect.

Even with group policy applied on the default domain controller for the domain audit, the server audit setting on the primary domain controller (PDC) may not be enabled. Please confirm this setting is enabled for the local security policy on the PDC server. If not enabled, use the local security policy to enable this setting.

Validate Cross-Domain Verification

In order to receive the maximum benefit a trust should be in place. When a trust is present, it is necessary to ensure that the trust is properly configured to permit cross-domain verification. To do so, first identify if the trust between the source and target domain is an external trust or a forest trust. Next, following commands must be run from an administrative command prompt:

If the trust between the source and target is an external trust:

- From the source domain:
 - Netdom trust SourceDomain /domain: TargetDomain /quarantine:No /user: domainadministratorAcct /password: domainadminpwd
- From the target domain:
 - Netdom trust TargetDomain /domain: SourceDomain /quarantine:No /user: domainadministratorAcct /password: domainadminpwd

If the trust between the source and target is a forest trust:

- From the source domain:
 - Netdom trust SourceDomain /domain: TargetDomain /enablesIDHistory:Yes /user: domainadministratorAcct /password: domainadminpwd
- From the target domain:
 - Netdom trust TargetDomain /domain: SourceDomain /enablesIDHistory:Yes /user: domainadministratorAcct /password: domainadminpwd

Domain Controller Access

If SID History will be synchronized, any Domain Controller listed in the Target DCs tab within a Directory Sync Pro for Active Directory profile will require access to the Domain Controller holding the PDC Emulator Active Directory FSMO role in the source. Keep in mind that even if the Domain Controller holding the PDC Emulator Active Directory FSMO role is not listed in the Source DCs tab, any SID History migration attempts will require a DC in the target to communicate with the PDC Emulator domain controller. For this reason, it is a best practice to ensure that all Domain Controllers specified in the Target DCs tab within a Directory Sync Pro for Active Directory profile has the appropriate networks access to communicate with the source Domain Controller holding the PDC Emulator Active Directory FSMO role before a SID History migration is attempted.

Password Synchronization Requirements



The domain controller with the PDC Emulator FSMO role must not be configured to run LSASS as a protected service or the password sync will fail with an access denied error.

5.3 Password Requirements

Directory Sync Pro for Active Directory and Migrator Pro for Active Directory do not validate the password policies present within your domains. Verify that the password entered as the Default Password complies with the password policy of your target environment. Objects will fail to be created if the password violates that policy.

5.4 Internet Requirement for Online Help and Video Tutorials

An internet connection is required to access the online help system and video tutorials.

- Within the Directory Sync Pro for Active Directory/Migrator Pro for Active Directory interface, the online help system can be accessed by clicking “HELP” in the pull-down menu  and the video tutorials can be accessed by clicking the  icons found throughout the application. Relevant topics in the online help system can be found using the Search bar at top of the page or navigated to while viewing topics by clicking on a topic in the list on the left side of the page. Individual topics can be printed by using the browser’s Print function.
- Windows Server operating systems will need to have the Desktop Experience feature (or a video codec) installed to view the video tutorials.

Section 6. Installing Directory Sync Pro for Active Directory and Migrator Pro for Active Directory

The Directory Sync Pro for Active Directory and Migrator Pro for Active Directory installer can be used to install both Directory Sync Pro for Active Directory and Migrator Pro for Active Directory at the same time or individually. Migrator Pro for Active Directory should only be installed at the same time as Directory Sync Pro for Active Directory or if it has previously been installed on the same server.

This guide includes the steps for installing Directory Sync Pro for Active Directory and Migrator Pro for Active Directory at the same time. Installing Directory Sync Pro for Active Directory first and running the installer again to install the Migrator Pro for Active Directory components is another option.

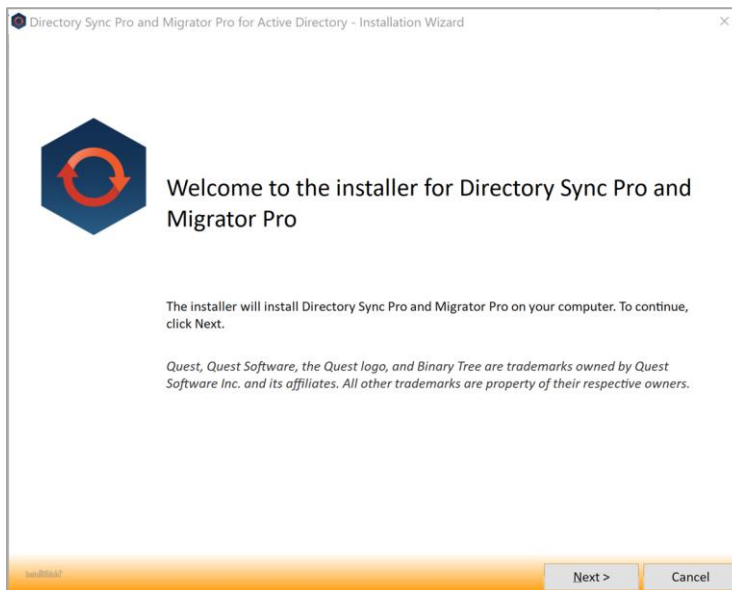
The installer creates a local group on the Directory Sync Pro for Active Directory server named BTDDirSyncPro and will add the currently logged in user to the group. Other users or a Domain group can be added to provide access to other users.



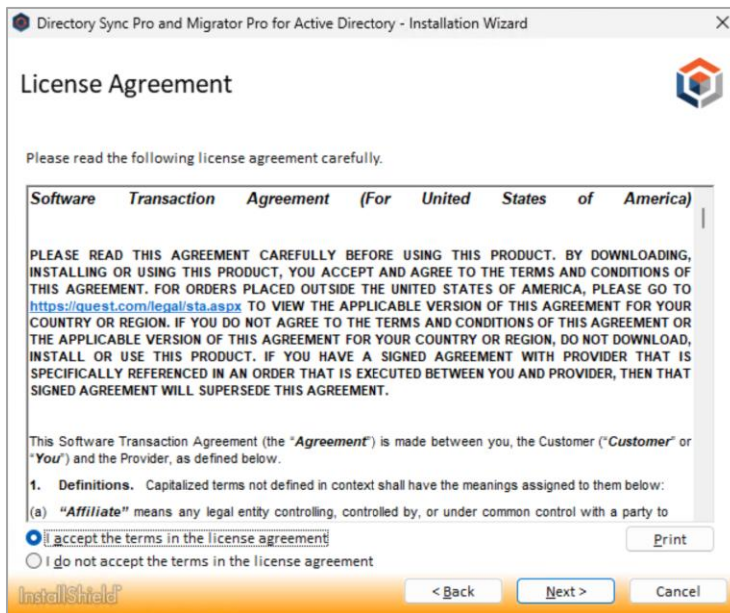
It is recommended to select “SQL Server Authentication” during the Directory Sync Pro for Active Directory/Migrator Pro for Active Directory server console installation if multiple people will be accessing the Directory Sync Pro for Active Directory/Migrator Pro for Active Directory web user interfaces. Otherwise, if “Windows Authentication” is chosen during installation, create a security group in AD and assign DB Owner rights to the Directory Sync Pro for Active Directory SQL databases and add all the users that need access to the console as members.

6.1 Installing Directory Sync Pro for Active Directory and Migrator Pro for Active Directory on a Windows Server

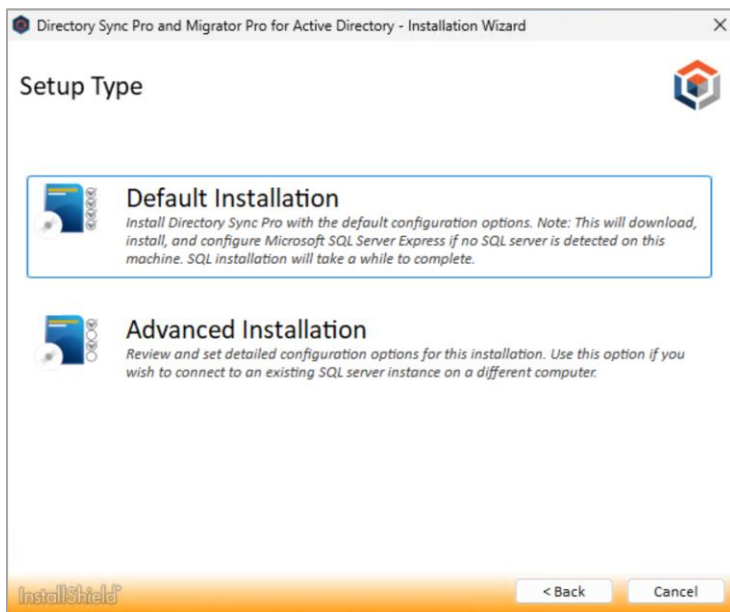
1. Download the installation package from the Quest Support site and save it on the Quest Windows Server.
2. Double-click the executable to begin installing Migrator Pro for Active Directory. The Welcome screen appears. Click **Next** to continue.



3. The License Agreement screen appears. To accept the terms of the license agreement and continue with the install, select “I accept the terms in the license agreement” and click **Next**.

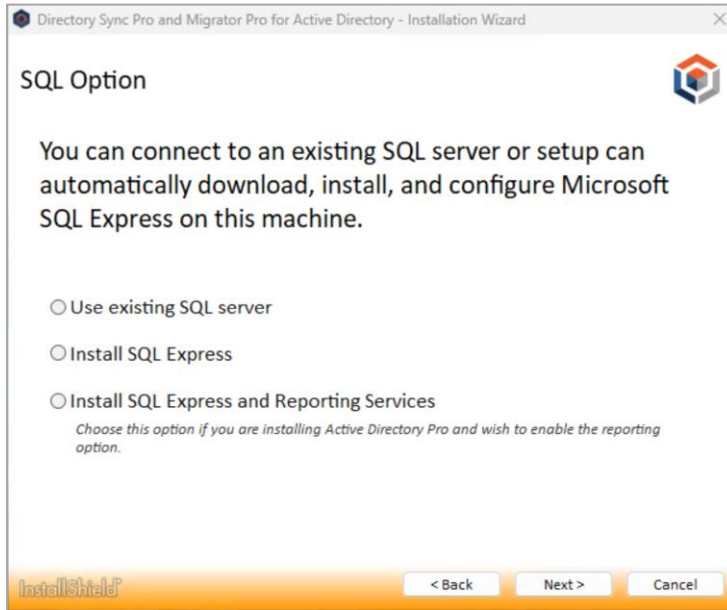


4. The Setup Type screen appears.



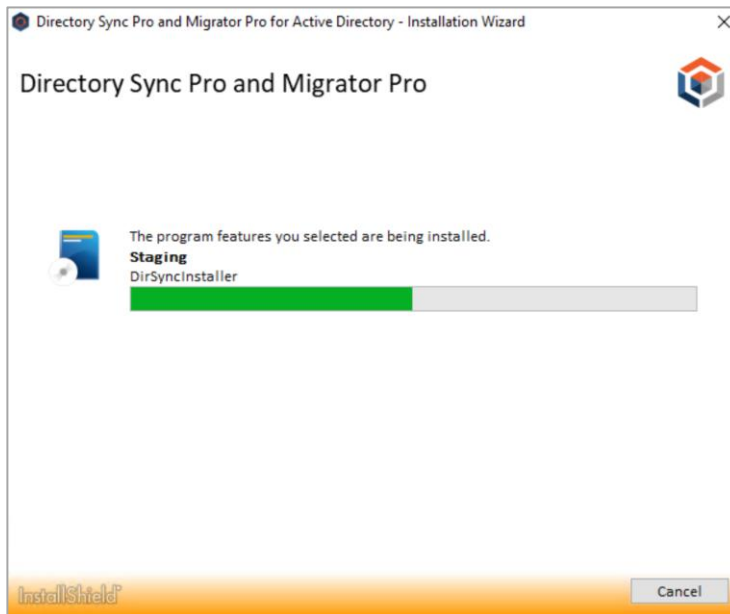
- Select **Default Installation** to install Directory Sync Pro for Active Directory and/or Migrator Pro for Active Directory with the default configuration options. A series of screens will appear while installing the needed databases and features. The Install Wizard Completed screen will appear when done.
- Select the **Advanced Installation** option to review and set the configuration options for the installation. The Install Wizard will continue to the next step.

5. The SQL Option screen appears. Select to use an existing SQL server or to install SQL Express and then click **Next**. If you choose to install SQL Express, a series of installation screens will appear while SQL Express is being installed.

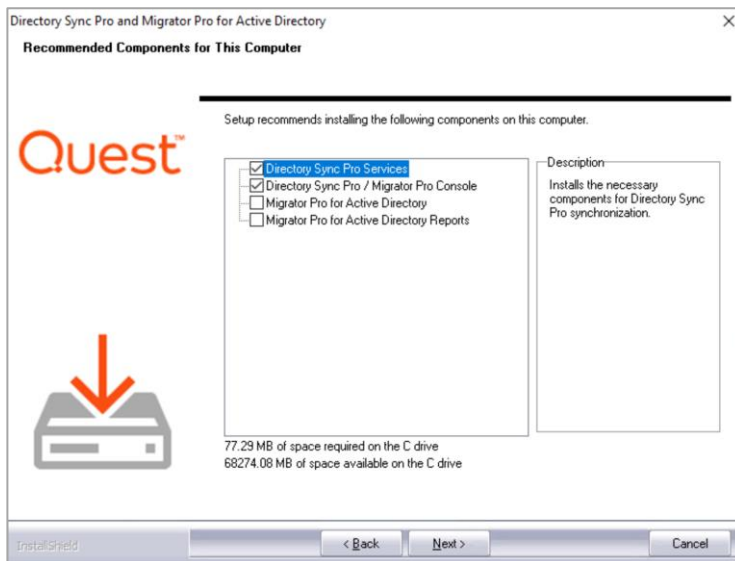


An existing SQL server must be used in STIG environments. SQL Express does not meet STIG requirements. Please see Appendix C. STIG Environments for more information.

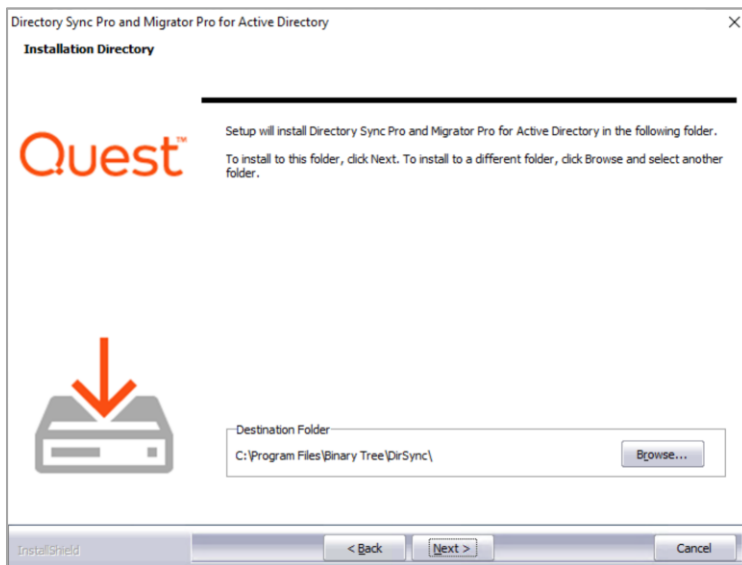
6. The Installation screen appears and will remain open. The Recommended Components screen will appear in a separate window. You will be prompted if there are applications using files that need to be updated by the installer.



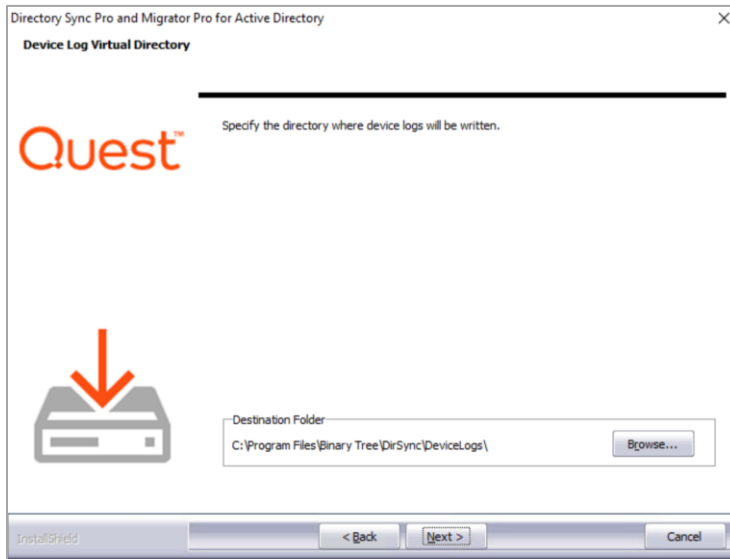
7. The Recommended Components for This Computer screen appears. By default, only the Directory Sync Pro for Active Directory components are selected. To install Migrator Pro for Active Directory, select the **Directory Sync Pro / Migrator Pro Console**, **Migrator Pro for Active Directory**, and (optionally) **Migrator Pro for Active Directory Reports** components and click **Next** to continue.



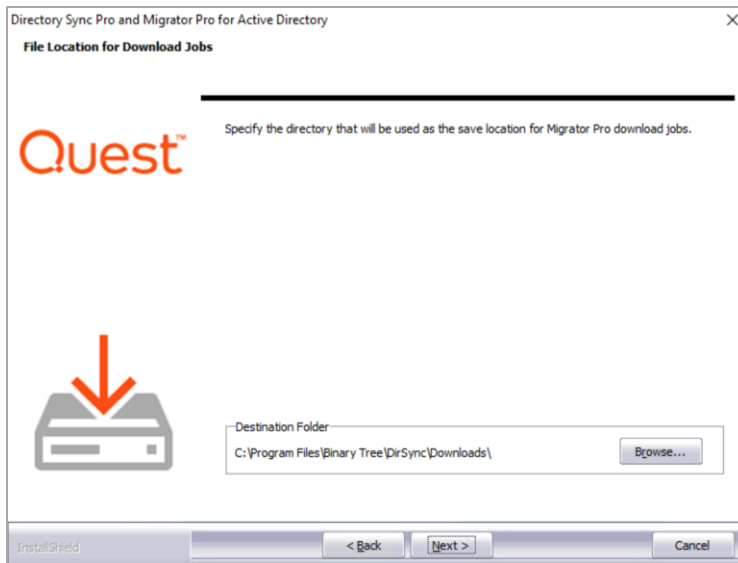
8. The Installation Directory screen appears. Both Directory Sync Pro for Active Directory and Migrator Pro for Active Directory are installed in the same directory. Click **Browse** to choose a different install location. Click **Next** to continue.



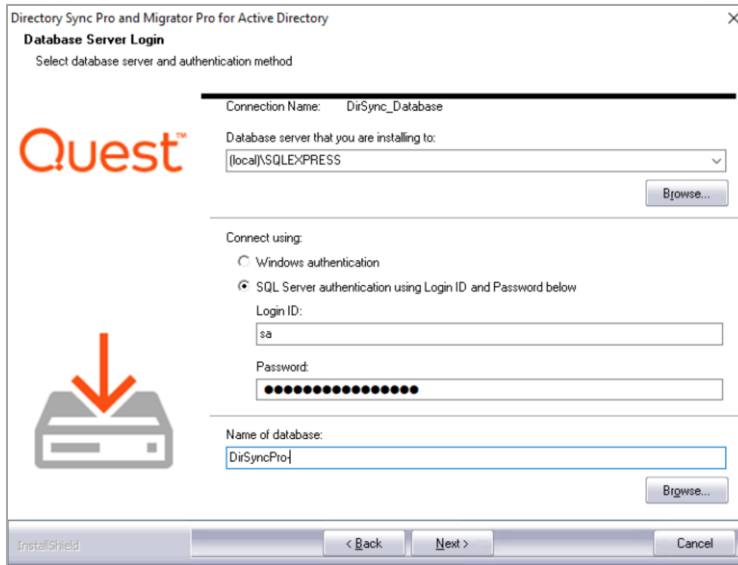
9. The Device Log Virtual Directory screen appears. Click **Browse** to choose a different location where device logs will be written. Click **Next** to continue.



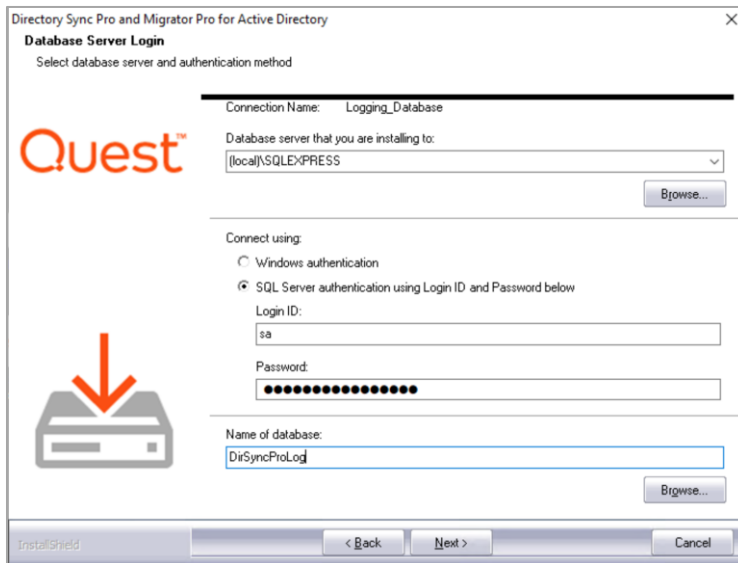
10. The File Location for Download Jobs screen appears. Click **Browse** to choose a different location where download jobs will be saved. Click **Next** to continue.



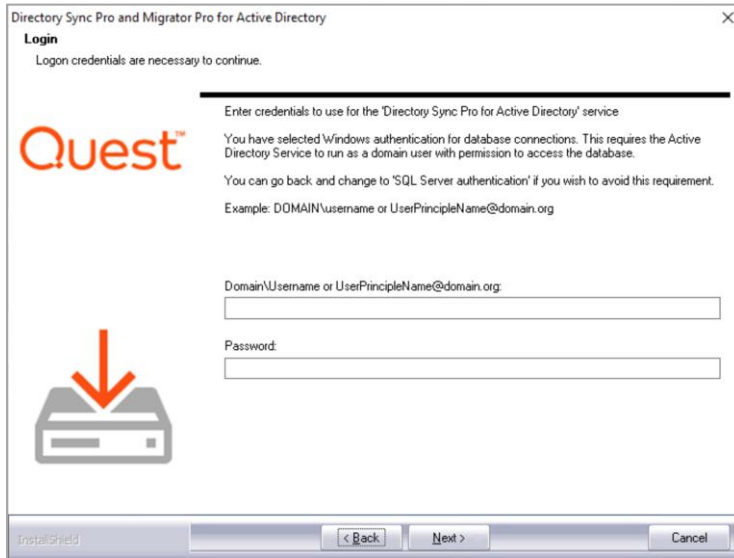
11. The Database Server Login screen appears. Enter the SQL Database Server location, credential information, and database name. Click **Next** to continue. If you choose to install SQL Server Express, the installer will populate the 'sa' account and default password. This password should be changed according to your organizations password complexity policy prior to configuring the product databases on the Database Server Login screen.



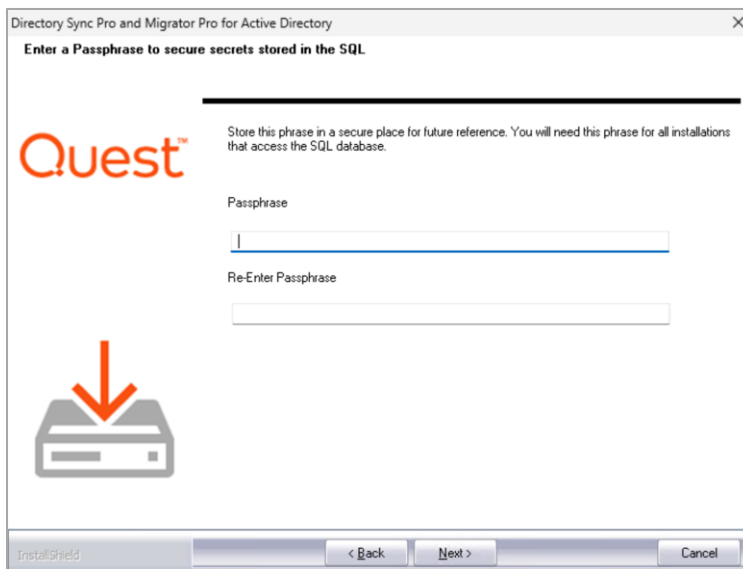
12. The Database Server Login screen appears again, this time for the logging database. Enter the SQL Database Server location for the logging database, credential information, and database name. Click **Next** to continue.



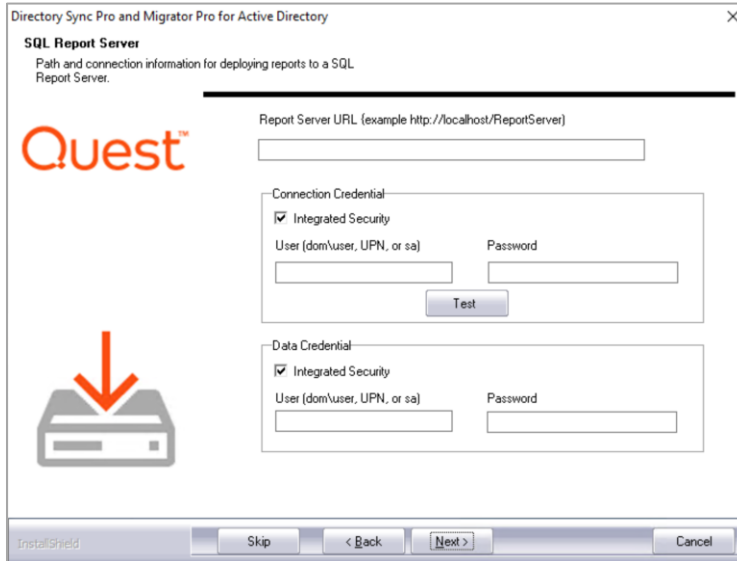
13. If you selected to connect using Windows Authentication on the previous screen, a screen to enter domain username and password appears. Enter the domain user in DOMAIN\username format and the password. Click **Next** to continue.



14. The SQL Passphrase screen appears if the passphrase was never entered on the current machine. The passphrase is required because once a database has been stamped with a passphrase, subsequent installs that reference the same database require the same passphrase. Enter the passphrase that was used during the initial installation of the SQL database. Click **Next** to continue.



15. If you selected to install the optional Reporting feature, the SQL Report Server screen appears. Enter the Report Server URL and select the appropriate Connection Credential and Data Credential options. Clicking the **Test** button to verify the SSRS connection credential is a best practice. See the Appendix of this document for information on verifying the Report Server URL. Click **Next** to continue. If SQL Server Reporting Services (SSRS) is not set up, click **Skip** and **OK** on the confirmation window.



The Connection Credential requires an account that has the Content Manager role and the System Administrator role defined on the SQL Server Reporting Server.

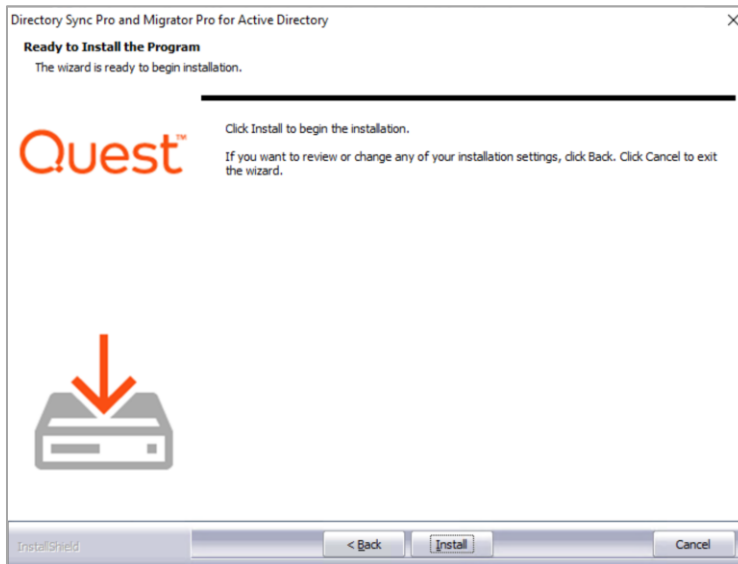
The Data Credential requires an account that has permission on the SQL Server Reporting Services database. These permissions are typically the database-level roles db_datareader and db_datawriter but should be verified by the SQL Server Reporting Services database administrator.

Reports will not appear in the Migrator Pro for Active Directory Console UI if the installation of the Reporting feature is skipped.

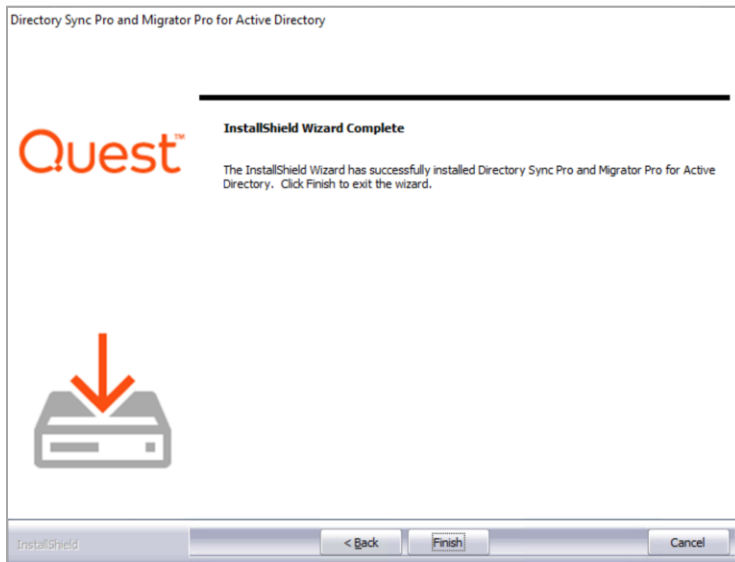
To install the Reporting feature at a later time, select to Modify the installation from the Programs and Features page in the Control Panel.

When an AD credential is used as the Data Credential on the SQL Report Server screen in the Migrator Pro for Active Directory installer, the Windows Credential check box is not checked. This will need to be changed manually in the DataSource in the Report Server after installation is completed.

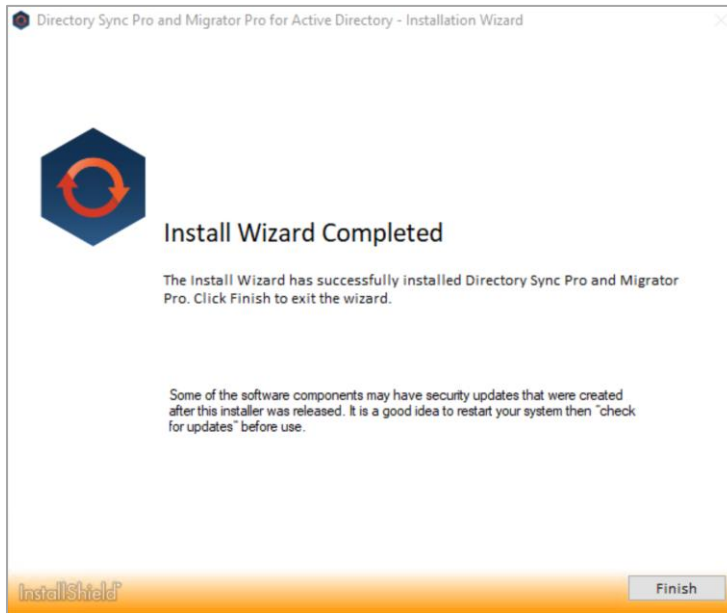
16. The Ready to Install screen appears. Click **Install** to begin the installation.



17. When the installation completes, the InstallShield Wizard Complete message appears. Click **Finish**.



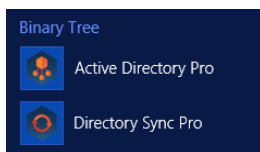
Also, click **Finish** on the Installation window.



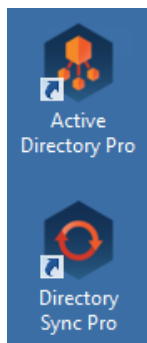
If upgrading from a previous version of Directory Sync Pro for Active Directory, you must delete the C:\Windows\BTPass folder from all domain controllers being used in the Directory Sync Pro for Active Directory profiles. A new version of BTPass will be pushed to the domain controllers on the next sync.

- The Apps screen or Start Menu is updated and the Migrator Pro for Active Directory and Directory Sync Pro for Active Directory icons are added to the desktop.

Apps screen:



Desktop icons:



Section 7. Upgrading Directory Sync Pro for Active Directory and Migrator Pro for Active Directory

Directory Sync Pro for Active Directory and Migrator Pro for Active Directory can be upgraded to a new version without uninstalling the existing version. The install wizard will detect the necessary changes and manage the upgrade.

7.1 Supported Upgrade Path

Upgrades are supported to the latest GA (Generally Available Release) from two GA versions prior. GA releases are listed on our website. If you are upgrading to a CSR (Customer Specific Release), please contact Support for clarification on whether the upgrade is supported.

If upgrading from a release older than two releases prior to the current GA, it is highly recommended that Support is contacted to discuss upgrade options for your specific environment. Some implementations which are more complex or have custom configurations may require a dedicated resource to assist in the upgrade process. If the upgrade goes beyond the scope of product support, this issue will be escalated to our Professional Services to assist at a billable rate.

Please contact Support if you have questions or need clarification on the Directory Synchronization upgrade process.

7.2 Upgrade Process

Directory Sync Pro for Active Directory and Migrator Pro for Active Directory can be upgraded to a new version without uninstalling the existing version. The installation wizard will detect the necessary changes and manage the upgrade.

Redeploying the Migrator Pro for Active Directory agents after upgrading is recommended in order to take advantage of new features in the new version of Migrator Pro for Active Directory.



Any customizations to the System actions in the ADM_Command and/or ADM_ActionCommand tables will be overwritten upon upgrade. If new custom actions are added through the user interface, those will not be lost during future upgrade.

The PowerShell commands that are installed and stored in the SQL database should not be modified as they may be lost during an upgrade.

Careful consideration should be taken when:

- Upgrading in a production environment
- Upgrading an older release of Directory Sync Pro for Active Directory to the latest release

Recommendations:

- Truncating the log or reducing the log size as much as possible before upgrading is recommended. This will reduce the amount of time needed to rebuild the log table index during the upgrade process.
- The examination of the Log SQL database during an upgrade may take longer than expected. Please allow the process to complete and the upgrade installation to proceed.

1. Download the installation package from the Support site and save it to the Quest Windows Server.

2. Run the executable file. The install wizard will appear and proceed through the standard installation steps.

NOTE !

You must delete the C:\Windows\BTPass folder from all domain controllers being used in the Directory Sync Pro for Active Directory profiles. A new version of BTPass will be pushed to the domain controllers on the next sync.

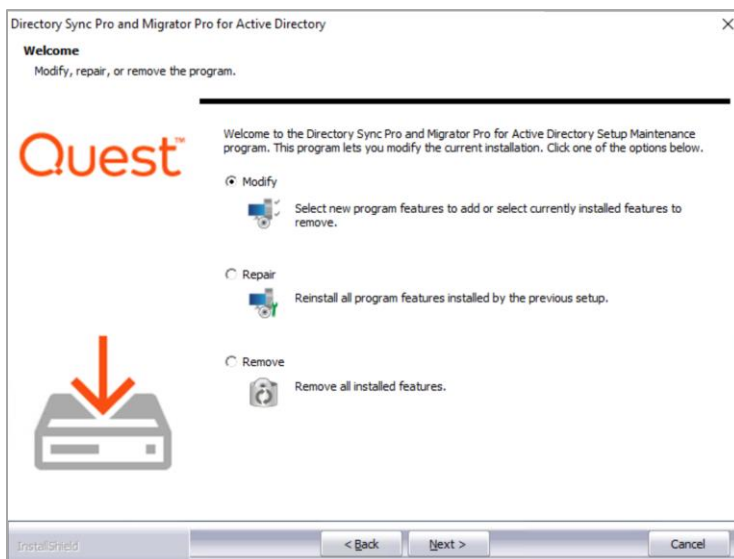
NOTE !

Mirroring should be stopped in the SQL environment prior to upgrading or installing.

Section 8. Modifying, Repairing and Uninstalling Directory Sync Pro for Active Directory and Migrator Pro for Active Directory

Directory Sync Pro for Active Directory and Migrator Pro for Active Directory can be modified, repaired, or uninstalled from the Programs and Features upgraded to a new version without uninstalling the existing version. The install wizard will detect the necessary changes and manage the upgrade.

1. Open Programs and Features by clicking the **Windows Start** button, clicking **Control Panel**, and clicking **Programs and Features**.
2. Select **Directory Sync Pro for Active Directory** or **Migrator Pro for Active Directory** from the list of programs and click **Change**.
3. The wizard screen appears displaying the following options. Select one of the following options and click **Next**:
 - **Modify** – use the Modify option to add and subtract components of Directory Sync Pro for Active Directory and/or Migrator Pro for Active Directory. This is useful if you wish to add or remove the Directory Sync Pro for Active Directory Console.
 - **Repair** – use the Repair option if Directory Sync Pro for Active Directory and/or Migrator Pro for Active Directory needs to be repaired due to corruption.
 - **Remove** – use the Remove option to uninstall Directory Sync Pro for Active Directory and/or Migrator Pro for Active Directory. You can also uninstall by clicking Uninstall on the Programs and Features page.



4. Proceed through the wizard until finished.

Section 9. Migrator Pro for Active Directory Agent Installation

9.1 Installing the Migrator Pro for Active Directory Agent on Devices

The Migrator Pro for Active Directory Agent is a key component of Active Directory migration. The agent contacts the Migrator Pro for Active Directory server at regular intervals, called polling, looking for jobs and tasks to perform.

Refer to the Requirements to verify all workstations and servers meet the requirements for agent installation.

Agent Installation

The agent can be installed using a GPO (Group Policy Object) or manually.

To install the agent with a GPO:

1. Right-click on the Migrator Pro for Active Directory Agent Installer MSI, point to **Share with**, and click on **specific people**.
2. Add a security group. The "authenticated users" group already includes all computers and is a good group to use. The group you add must have the shared Read permission and NTFS permission.
3. Click **Share**.
4. Click **Done**.
5. From the **Start** menu, point to **Administrative Tools** and click on **Group Policy Management**.
6. Right-click on the domain or OU you will be migrating and click on **Create a GPO in this domain, and link it here**.
7. In the New GPO dialog box, enter a **Name** for the GPO and click **OK**.
8. Click on the new GPO and click **OK**.
9. Right-click on the GPO and select **Edit**.
10. Open **Computer Configuration > Policies > Software Settings** and right-click on **Software Installation** and then point to **New** and click on **Package**.
11. In the **File Name** field, enter the UNC path to the MSI file and click **Open**.
12. Select the **Active Directory Pro Agent** and click **Open**.
13. In the Deploy Software window, select the **Assigned** deployment method and click **OK**.



The device must be rebooted for the applied group policy to complete the agent installation.

To verify the GPO:

1. Log on to a workstation within the scope of the GPO using administrator credentials.
2. From a command prompt on the workstation, run **gpresult -r**

3. The Computer Settings section will display the applied group policy.

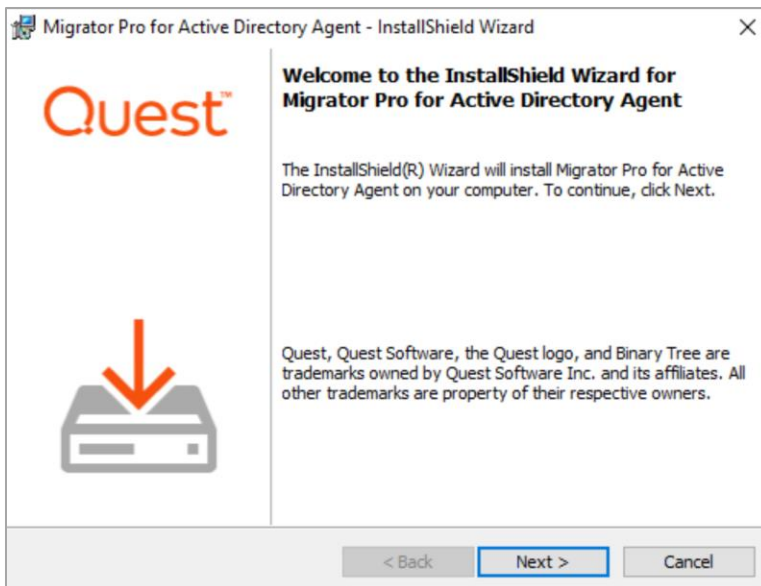


A newly applied group policy will not immediately be displayed.

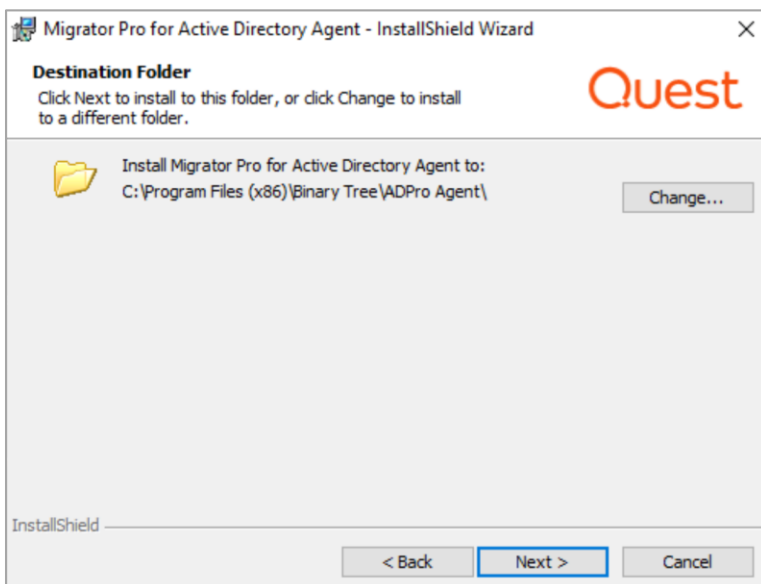
The Computer Settings section displays the applied group policy, but the agent installation is not completed until the device is rebooted.

To manually install the agent:

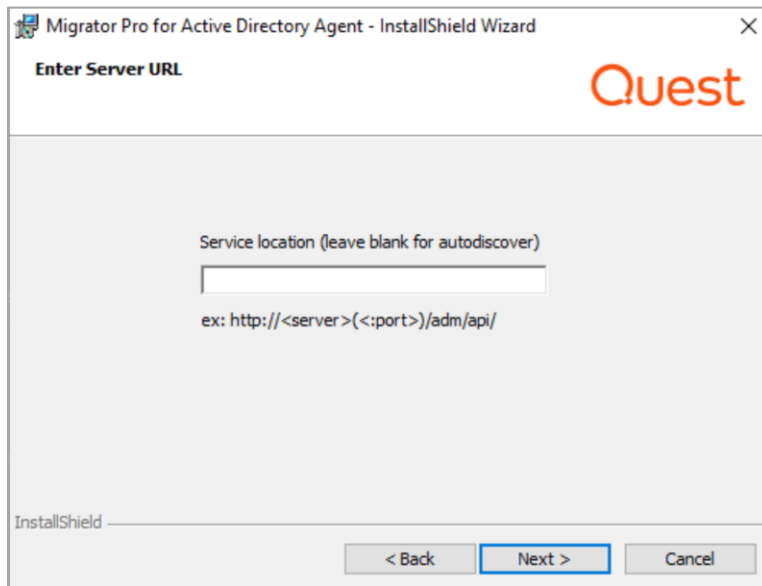
1. Copy the Active Directory Pro Agent Installer MSI file to each computer.
2. Double-click the file to open the installer.
3. On the Welcome screen, click **Next**.



4. On the **Destination Folder** screen, click **Next**.



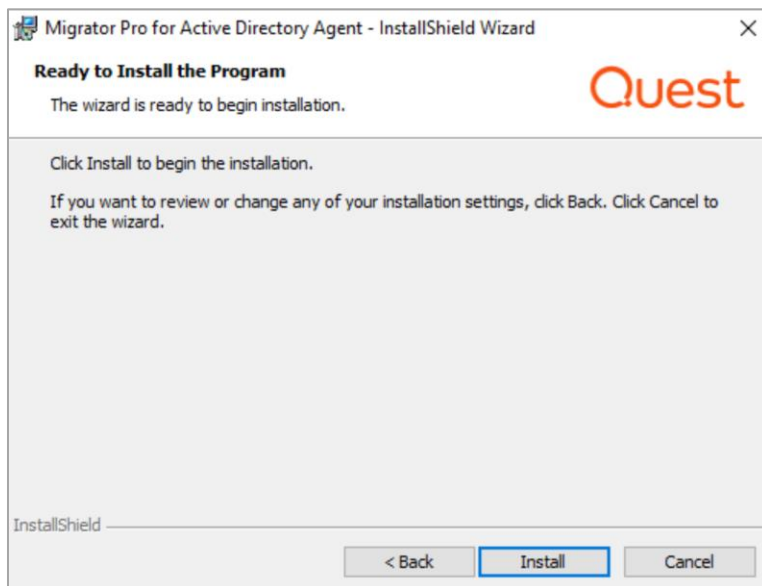
5. On the **Enter Server URL** screen, enter the FQDN of the server running the Migrator Pro for Active Directory service and click **Next**.



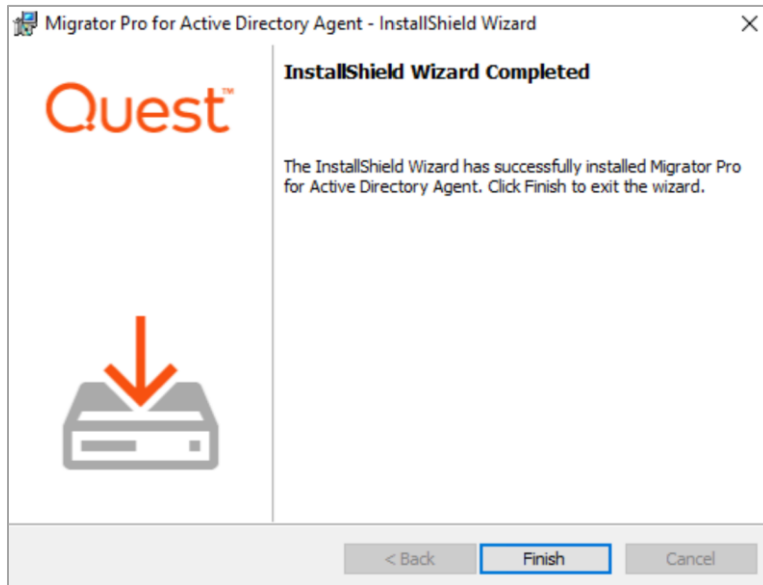
NOTE ! Leave this screen blank if an SRV record has been created. See [Creating SRV Records](#) below for more information.

If there is an SRV record found in the Domain, any entry manually entered during the agent install for the Server URI will be ignored.

6. On the **Ready to Install the Program** screen, click **Install**.



7. When the install completes, click **Finish**.



Refer to the Troubleshooting section to resolve common agent install issues.

Creating SRV Records

The Migrator Pro for Active Directory Agent uses DNS to "autodiscover" the Migrator Pro for Active Directory server. An SRV (service location) record must be created in DNS to point the clients to the correct server or servers.

To create an SRV record using DNS Manager:

1. In the DNS Manager, right-click on the DNS server and click on **Other New Records**.
2. In the Resource Record Type dialog, select the **Service Location (SRV)** type and click **Create Record**.
3. In the New Resource Record dialog, enter "_btadm" in the Service field.
4. Enter the following information for HTTP or HTTPS:
 - For HTTP:
Protocol: _http
Priority: 0
Weight: 0
Port Number: 80
Host offering the service: the FQDN of server running the Migrator Pro for Active Directory service.

- For HTTPS:

Protocol: _https

Priority: 0

Weight: 0

Port Number: 443

Host offering the service: the FQDN of server running the Migrator Pro for Active Directory service.



You can make SRV records using HTTP, HTTPS, or both protocols. Using HTTPS is suggested for increased security. If both protocols are used, the agent will always attempt to use HTTPS first.

5. Click **OK**.

Every client running the agent software must be able to resolve the DNS records.

To verify the clients can resolve the SRV DNS records:

1. Open a command prompt on the client machine.
2. Run **nslookup -q=srv _btadm._http.source.int** where "http" is the protocol: http or https, and "source.int" is the name of the source domain.

Section 10. Troubleshooting

10.1 Migrator Pro for Active Directory Agent Installation Troubleshooting

- **Problem:** The device registers but does not get discovered (Discovery Status remains blank in the Migrator Pro for Active Directory console).
Solution: Install PowerShell 2.0 or higher on the client. Operating systems earlier than Windows 7 do not natively include PowerShell.
- **Problem:** During manual installation, a "wizard interrupted" error appears.
Solution: Install .NET 4.7.2 or higher on the client and run the installer again.
- **Problem:** After a successful manual install, an "Unable to register" error appears in the Event Viewer.
Solution: Verify the path to the Migrator Pro for Active Directory server is correct and complete.
- **Problem:** After a successful manual install, an "Unable to auto-discover" error appears in the Event Viewer.
Solution: The SRV records are missing, incorrect, or unreachable. Verify SRV records are set up properly.

Appendix A: Configuring Directory Sync Pro for Active Directory in a Non-English Active Directory Environment

Directory Sync Pro for Active Directory refers to several system groups by their English names, which will not function properly when deploying in environments where non-English Active Directory is deployed. To resolve this, the mapping of these systems group names can be configured to accommodate non-English language deployments.

There are five new .config file values, representing the five system groups used by Directory Sync Pro for Active Directory: All Users, All Groups, All Rooms, Default Global Address List, and Deleted Objects. To localize a value, edit **BinaryTree.Dirsync.Exchange.exe.config** on the Exchange server and add the colored text below (the existing configuration is shown below in black), replacing the value with the equivalent value in the appropriate language.

```
<configuration>
  <configSections>
  </configSections>
<!--
  "ExchangeOrgCN" = The name of the Exchange Organization CN to use for the target AD. This is only used if
  it cannot be automatically detected.

  The names of the following AD objects can be localized.
  To use the localized versions, replace the string values below with the localized name.
  e.g. <add key="AllUsers" value="Tous les utilisateurs"/>
  e.g. <add key="DefaultGlobalAddressList" value="Liste d'adresses globale par défaut"/>

  "ReferralChasingOption"
  the available options for 'chase referrals' are:
  - None: Never chase the referred-to server. Setting this option prevents a client from contacting other servers in
  a referral process
  - Subordinate: Chase only subordinate referrals which are a subordinate naming context in a directory tree
  - External: Chase external referrals
  - All: Chase referrals of either the subordinate or external type
-->
<appSettings>
  <add key="ExchangeOrgCN" value="" />
  <add key="AllUsers" value="All Users" />
  <add key="AllContacts" value="All Contacts" />
  <add key="AllGroups" value="All Groups" />
  <add key="AllRooms" value="All Rooms" />
  <add key="DefaultGlobalAddressList" value="Default Global Address List" />
  <add key="DeletedObjects" value="Deleted Objects" />
```

Appendix B. Installing and Configuring SQL Server Reporting Services

Installing SQL Server Reporting Services



These instructions are for existing SQL Server installs where reporting services are being added.

Migrator Pro for Active Directory reporting is supported on SSRS 2012, 2014, or 2017.

1. Load the ISO into the DVD drive.
2. Open **My Computer**.
3. Double-click on the DVD drive to run the **SQL Server Installation Center** dialog.
4. Select **Installation** from the left.
5. Select **New installation or add features to an existing installation**.
6. Click the **OK** button on the Setup Support Rules page if everything passed.
7. Click the **Install** button on the SQL Setup Files page.
8. Click the **Next** button on the Setup Support Rules page if everything passed.
9. Select **Add features to an existing instance of SQL Server** (verify your instance is shown).
10. Click the **Next** button.
11. Check the **Reporting Services** box and click the **Next** button.
12. Click the **Next** button on **Installation Rules**.
13. Click the **Next** button on **Disk Space Requirements**.
14. Click in the **Account Name** field and select **NT AUTHORITY\NETWORK SERVICE**.
15. Click the **Next** button.
16. Click the **Next** button on the **Reporting Services Configuration to Install, but do not configure the report server** option.
17. Click the **Next** button.
18. Click the **Next** button on Installation Configuration Rules page if everything passed.
19. Click the **Install** button on the Ready to Install page.
20. If you have a green checkmark on the 'Complete' page, click the **Close** button.
21. Close the SQL Server Installation Center dialog.

Configuring SQL Server Reporting Services

1. Click **Start > All Programs > Microsoft SQL Server > Configuration Tools**.
2. Click on **Reporting Services Configuration Manager**.

3. Click the **Connect** button.
4. Select **Service Account** from the left.
 1. Verify Network Service is set for the built-in account.
5. Select **Database** from the left.
 1. Click the **Change Database** button.
 2. Verify 'Create a new report server database' is selected and click the **Next** button.
 3. Set your security type and click the **Next** button.
 4. Leave the defaults. Verify 'Report Server Mode' is set to 'Native' (Reporting will fail to work if not in Native Mode)
 5. Click the **Next** button.
 6. Click the **Next** button.
 7. Click the **Next** button and it will begin to configure the database.
 8. Click the **Finish** button.
6. Select **Web Service URL** from the left pane.
 1. Click the **Apply** button.
7. Select **Report Manager URL** from the left pane.
 1. Click the **Apply** button.
8. Click the **Exit** button.

Your Report URLs

Browseable URL

http://<servername>/Reports

Or

http://<servername>/Reports_InstanceName (if SQL Server is installed as an instance)

Web Service URL

http://<servername>/ReportServer

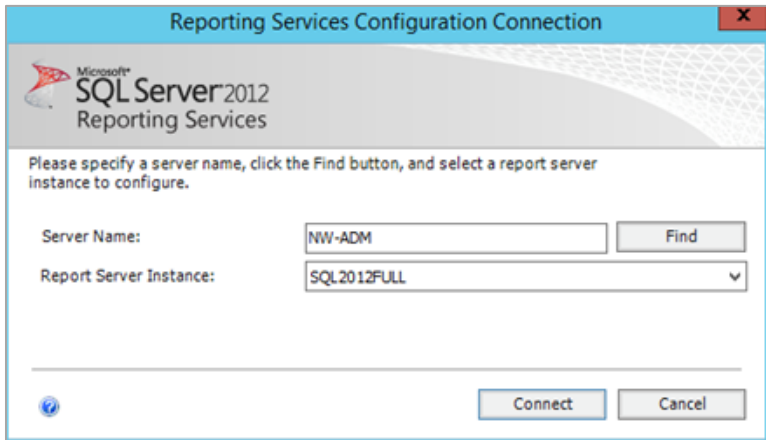
Or

http://<servername>/ReportServer_InstanceName (if SQL Server is installed as an instance)

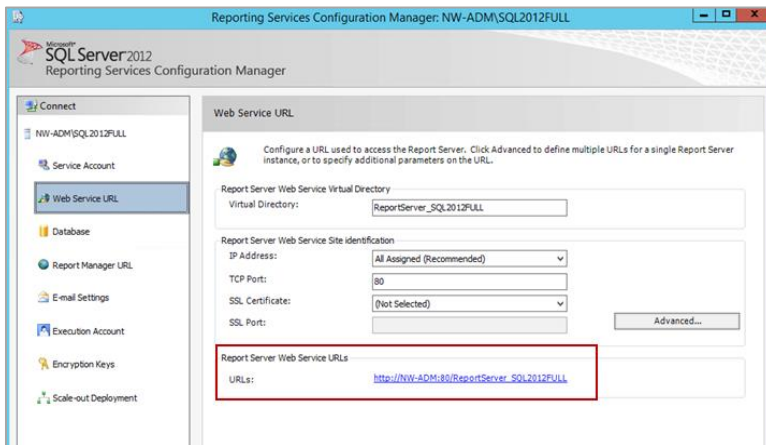
Verifying the Report Server URL

The Report Server URL is needed when installing the Reporting feature. Use the following steps to verify the correct URL to use.

1. Open Reporting Services Configuration Manager.
2. Provide the SQL Server Name and Report Server Instance name and click **Connect**.



3. In the left folder navigation, select **Web Service URL**.
4. The Report Server URL appears in the Report Server Web Service URLs section.



Appendix C. STIG Environments

Please note the following considerations for STIG environments.

SQL Express

The SQL Express option should not be chosen when installing Directory Sync Pro for Active Directory and Migrator Pro for Active Directory. SQL Express does not include the following settings or features needed for STIG environments:

- SQL Server must be monitored to discover unauthorized changes to stored procedures. (SQL Agents is not part of SQL Express) 41403, 41404, 41405

A dedicated SQL Server (full version) should be used.

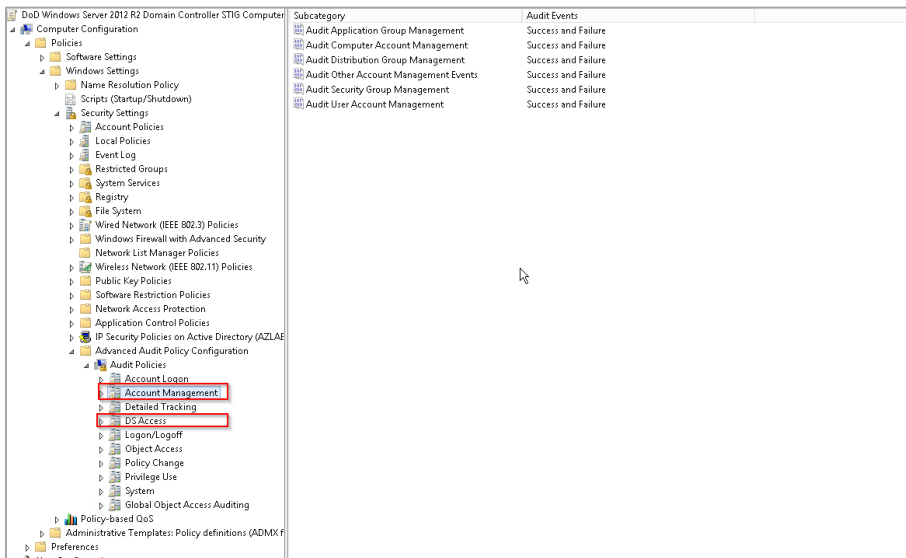
SID History

In order for SID History copy to function in a STIG environment, additional security setting changes are needed in GPO on the domain controller.

By default, Success and failure auditing of account management must be enabled for both source and target domains via local security policy or GPO. However, because “Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings” is enabled per STIG policy, additional audit policy settings must be configured for both source and target domains.

To configure the audit policy settings:

1. Navigate to the "Advanced Audit Configuration" settings in the Default Domain Controllers Policy (Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies).
2. Enable all the Subcategories of DS Access (Success) and Account Management (Success, Failure).



Additional Information

[Microsoft SQL Server 2012 Database Security Technical Implementation Guide \(stigviewer.com\)](#)

[Microsoft SQL Server 2012 Database Instance Security Technical Implementation Guide \(stigviewer.com\)](#)

[MS SQL Server 2016 Instance Security Technical Implementation Guide \(stigviewer.com\)](#)

[MS SQL Server 2016 Database Security Technical Implementation Guide \(stigviewer.com\)](#)

Appendix D. Deployment in FIPS Environment

Directory Sync Pro for Active Directory 20.11.2 can be successfully deployed in a FIPS environment by following the procedure described in this document.

The audience for this section is technical implementation consultants deploying Directory Sync Pro for Active Directory.

Cryptographic usage

Directory Sync Pro for Active Directory relies on the following Third-Party cryptographic libraries for its cryptographic needs.

Cryptographic usage	Cryptographic algorithm	Cryptographic parameters
Communication – Website User Interface	SSL TLS 1.2	
Communication – (SMB 3.x)	AES-128-CMAC, AES-128-GCM	
Communication – (SMB 2.1)	HMAC-SHA256	
Communication – (LDAP/Kerberos)	AES128_HMAC_SHA1, AES256_HMAC_SHA1	SESSION: Signing & Sealing
Communication – (Kerberos NTLM Authentication)	RC4_HMAC_MD5	
Symmetric encryption of bulk data	AES256 CBC Mode	KEY: 256-bit PBKDF2 (Constant) IV: 128-bit PBKDF2 (Constant)
Symmetric encryption of bulk data – Additional Entropy	RNG	64-bits (Random per encrypted value)
Symmetric encryption of secrets – (DPAPI) Configuration Parameters	AES256 CBC Mode	SCOPE: LocalMachine
Symmetric encryption of secrets – Additional Entropy	RNG	256-bits (Constant per node)
Hashing – (PBKDF2) Generation of encryption KEY/IV	HMACSHA1	HASH SIZE: 160-bit
Hashing – (DPAPI)	SHA512	HASH SIZE: 523-bit
Hashing – Attribute Change Detection	SHA256	HASH SIZE: 256-bit
Hashing – Legacy Attribute Change Detection	MD5	HASH SIZE: 128-bit

Background

To execute in a FIPS compliant mode, a Windows environment requires the Microsoft Policy “System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing” setting enabled.

Microsoft states that “This policy is only advisory to applications. Therefore, if you enable the policy, it does not make sure that all applications will comply”.

Directory Sync Pro for Active Directory leverages Microsoft’s CryptoAPI (CAPI) and CryptoAPI Next

Generation (CNG) for its cryptographic needs.

Microsoft Product Relationship with CNG and CAPI libraries is documented here:
<https://technet.microsoft.com/en-us/library/cc750357.aspx>

“Rather than validate individual components and products, Microsoft chooses to validate only the underlying cryptographic modules. Subsequently, many Windows components and Microsoft products are built to rely on the Cryptographic API: Next Generation (CNG) and legacy Cryptographic API (CAPI) FIPS 140 validated cryptographic modules. Windows components and Microsoft products use the documented application programming interfaces (APIs) for each of the modules to access various cryptographic services.

Prerequisites

External to Directory Sync Pro for Active Directory, the following server configurations are necessary to set up the environment for FIPS Mode.

1. Windows Server 2016 or later must be installed and up to date.
2. The following group policies must be enabled:
 - a. System Cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing.
 - i. Ensure this policy is enabled.
 - b. Network Security: Configure encryption types allowed for Kerberos.
 - i. Ensure the “AES128_HMAC_SHA1” and “AES256_HMAC_SHA1” values are selected.
 - ii. NOTE: Authentication of target accounts with synchronized passwords requires Kerberos encryption type “RC4_HMAC_MD5” to be allowed for participating devices.
3. Insecure SCHANNEL Server protocols must be disabled.
 - a. SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1
4. SSL certificate for Web Hosting issued by a trusted certificate authority.

Installation and operation

For environments with existing Directory Sync Pro for Active Directory installations, the installation must be upgraded to version 20.11 or later. If the existing installation is configured with fail-over nodes, each node must also be upgraded to version 20.11 or later.

For new installations, Directory Sync Pro for Active Directory 20.11 enforces all FIPS mode requirements, no additional steps are required.

WEBSITE SSL CERTIFICATE INSTALLATION

1. Ensure the certificate and CA certificate chain has been installed on the server.
2. Open Internet Information Services (IIS) Manager.
3. Expand the Sites node in the Connections pane.
4. Right-click the “DirSync” website node and choose “Edit Bindings...”.

- a. If the site has an “https” binding, select it and click “Edit...”
 - b. If the site does not have an “https” binding, click “Add...”
 - i. From the “Type” drop-down, select “https”.
 - c. From the “SSL certificate” drop-down, select the appropriate certificate.
 - d. Click OK.
 - e. Remove the “http” binding.
5. In the IIS Manager Features View pane, double-click “SSL Settings”.
 - a. Check the “Require SSL” checkbox and click “Apply” in the Actions pane.
 6. Validate the website can be accessed and the browser is indicating the certificate is valid and trusted.

References

[System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing](#)

[Network security: Configure encryption types for Kerberos](#)

[Windows Server SCHANNEL Protocol Settings](#)

[Internet Information Services \(IIS\) 7.0 Set Up SSL Certificates](#)

[Internet Information Services \(IIS\) 8.0 Centralized SSL Certificates](#)