Quest

Migrator for Notes to SharePoint

Security Guide

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.

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

Migrator for Notes to SharePoint Security Guide
November 2022

Contents

Introduction

Migrator for Notes to SharePoint provides "Point and click" migration of Lotus Notes®, Lotus QuickPlace®/Quickr®, or Lotus Domino®.Doc documents to SharePoint Lists, Libraries, and InfoPath® Form Libraries. This simple but powerful tool makes it easy for technical or non-technical users to select data from a Lotus data source, define any desired data mapping rules, and write the data out to SharePoint. Information technology professionals can take advantage of the tool's many features to perform enterprise-level migration projects.

This document describes the security features of Migrator for Notes to SharePoint. This includes access control, protection of customer data, secure network communication, cryptographic standards, and more.

About Migrator for Notes to SharePoint

Migrator for Notes to SharePoint provides an easy-to-use, convenient way to migrate of Lotus Notes®, Lotus QuickPlace®/Quickr®, or Lotus Domino®.Doc documents to SharePoint Lists, Libraries. Migrator for Notes to SharePoint can quickly migrate your content into SharePoint while preserving valuable user metadata. Migratorfor Notes to SharePoint product comes in three editions:

- **Migrator for Notes to SharePoint Console**
  The Migrator for Notes to SharePoint Console provides a higher-level view of your migration process than the Migrator for Notes to SharePoint Designer. Rather than focusing on designing and running one migration job for one Notes database, the Console looks across many databases (potentially all the databases in your organization) and helps you control the entire migration process.
- **Migrator for Notes to SharePoint Designer**
  The Migrator for Notes to SharePoint Designer allows you to manage complete Job Definitions, set tool options, and run migration jobs.
- **Migrator for Notes to SharePoint Services**
  Suitable for migrations between Lotus Notes®, Lotus QuickPlace®/Quickr®, or Lotus Domino®.Doc documents to and Sharepoint On-premises and also specified Folder and SQL Server.

Architecture Overview

The following scheme shows the key components of the Migrator for Notes to SharePoint configuration.

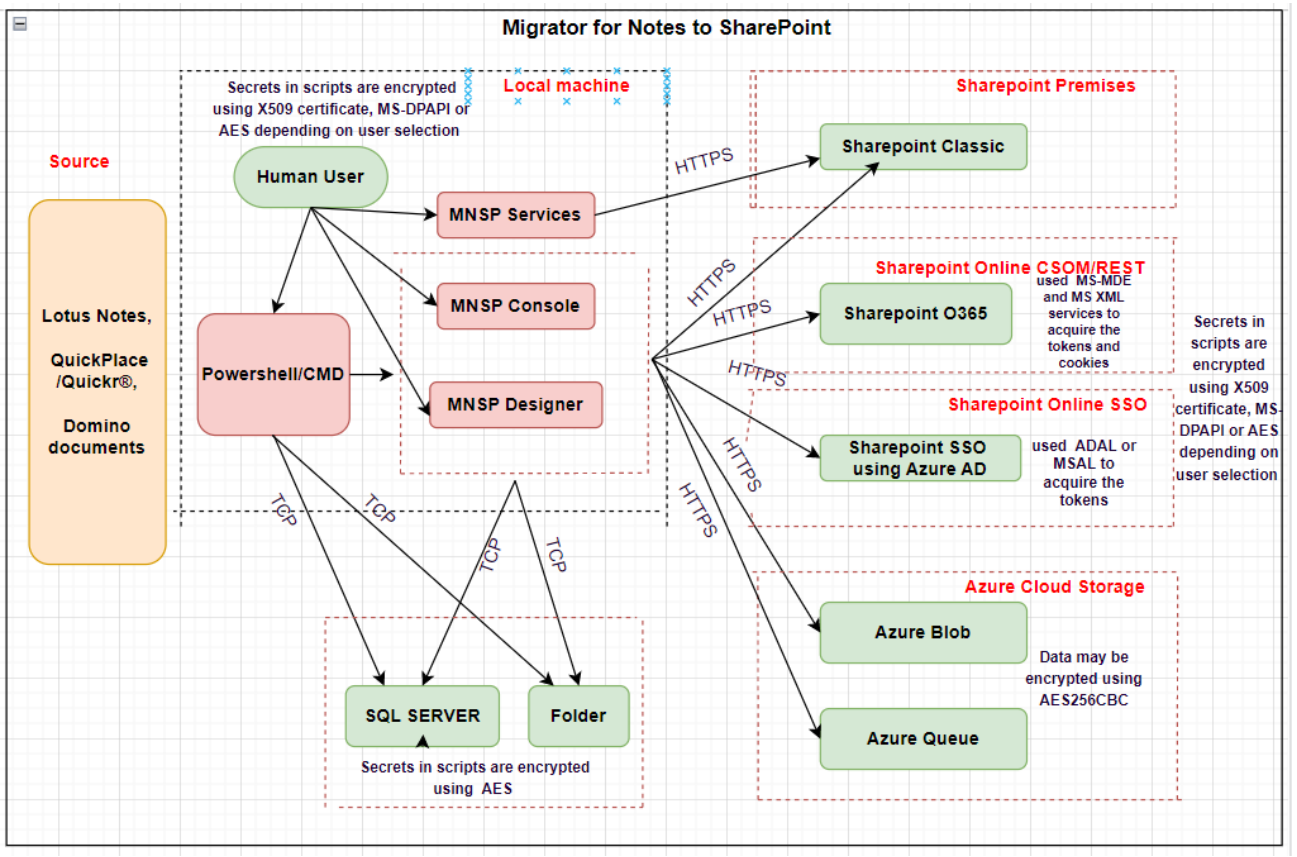


Figure 1: High-Level Architecture

Overview of Data Handled by Migrator for Notes to SharePoint

Migrator for Notes to SharePoint provides the following general features and components:

- Quickly and easily migrates Lotus Notes and Domino databases, Lotus QuickPlace/Quickr sites, or Lotus
- Domino.Doc cabinets
- Automatically maps Notes fields to SharePoint fields based on predefined rules
- Automatically detects when predefined Data Definitions can be applied (based on Notes template and
- SharePoint template used)
- Customizes Notes and SharePoint data access details as well as data mapping rules
- Saves customized Data Definitions for future use against other applications based on the same application
- template
- Provides command line mode for batch processing
- Provides detailed event logging
- Supports running migration jobs directly on your SharePoint server or sending extracted data to remote
- SharePoint servers from your desktop
- Allows bulk migration by IT professionals or ad-hoc migration by end users

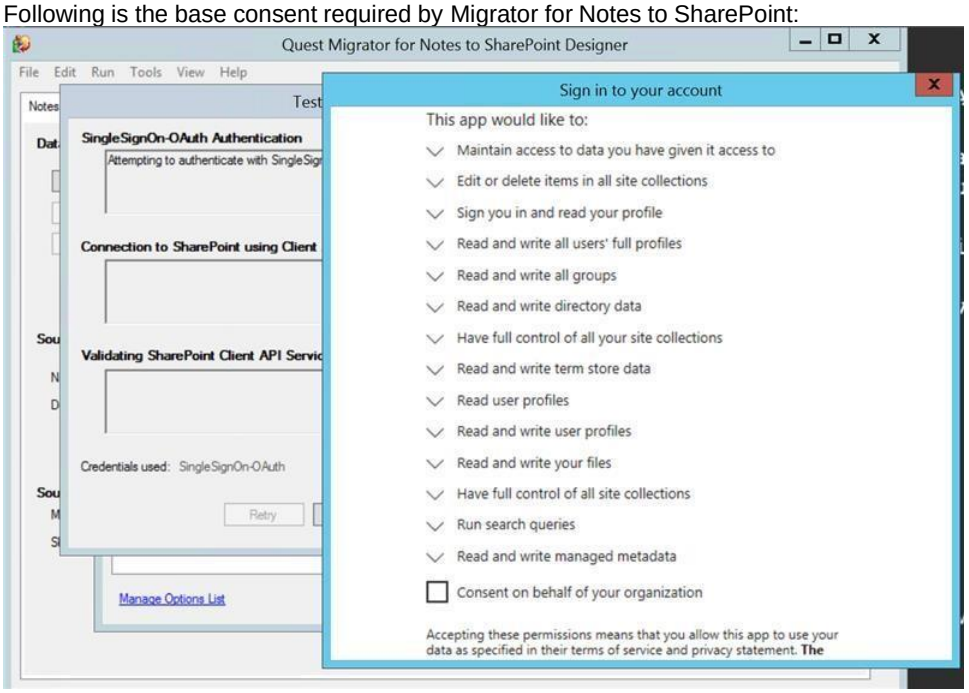
Admin Consent and Service Principals

Migrator for Notes to SharePoint can access the customer's Azure Active Directory and Office 365 tenancies. The customer grants that access using the Microsoft Admin Consent process, which will create a Service Principal in the customer's Azure Active Directory with minimum consents required by Migrator for Notes to SharePoint migration with SingleSignOn Authentication.

The Service Principal is created using Microsoft's OAuth certificate-based client credentials grant flow https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-oauth2-client-creds-grant-flow.

Customers can revoke Admin Consent at any time. See https://docs.microsoft.com/en-us/azure/activedirectory/manage-apps/delete-application-portal and https://docs.microsoft.com/en-us/skype-sdk/trustedapplication-api/docs/tenantadminconsent for details.

Following is the base consent required by Migrator for Notes to SharePoint:



Location of Customer Data

- All computation is performed on the server(s) provided by the customer.
- In case of migration using the "Import API" option, binary contents of files are uploaded to Azure blob storage. Migrator for Notes to SharePoint can use either SPO-provided Azure container blob storage or customer-provided private Azure container blob storage.

Privacy and Protection of Customer Data

Encryption of secrets uses MS DPAPI (PBKDF2, AES).

Security-sensitive information like the password and OAuth tokens used in SharePoint connections are encrypted using Microsoft DPAPI (ProtectedData Class (System.Security.Cryptography) | Microsoft Docs).

Azure Import Pipeline

- When the Import Pipeline is used, security-sensitive information about azure blob storage SASS URL is stored with Microsoft DPAPI encryption.
- The files uploaded to Azure storage are encrypted with AesCryptoServiceProvider. (If private containers are used, this encryption is optional.)
- If Azure private containers are used with the Import Pipeline, the Azure storage connection string is encrypted with Microsoft DPAPI. (In the case of Distributed Migration, the Azure storage connection string is encrypted with the customer-provided X509 certificate.)

Distributed Migration

Passwords stored in the Distributed Database use customer-provided X509 certificates, which includes encryption. As noted above, if Azure private containers are used, the Azure storage connection string is also encrypted with the certificate.

Database Connection Credentials

Job database (SQL Server) connection credentials are encrypted with Microsoft DPAPI.

Network Communications

Source	Target		Port/Protocol
MNSP Console/Designer			
	SharePoint Server (remote machine)	Native Web Service	Native Web Service port (TCP)
		SharePoint DB	Default Protocol
	Azure Cloud	Azure Blob Storage	443 (TCP)
		Azure Queue	443 (TCP)
	Microsoft Office 365 (SPO CSOM)		443 (TCP)
	Single sign-on Authentication		443 (TCP)
PowerShell	MNSP Agents		135 (TCP) and dynamic ports (TCP)

Figure 2: List of protocols used and associated ports

.

Authentication of Users and Services

Migrator for Notes to SharePoint relies upon: -

- SharePoint servers using Quest import services
- SharePoint web services (Classic Mode Authentication)
- SharePoint web services (Forms-Based Authentication)
- Azure Active Directory authenticating via Office 365 OAuth Authentication
- SharePoint API services (Single Sign On -O Auth Authentication)

TLS Settings:

- Use TLS 1.2 - Select this check box to connect to SharePoint sites using the TLS 1.2 protocol in Settings link in Options

  Note: Microsoft Azure Active Directory (Azure AD) will soon stop supporting the following Transport Layer Security (TLS) protocols and ciphers: [**link**]
  - TLS 1.1
  - TLS 1.0
  - 3DES cipher suite (**TLS_RSA_WITH_3DES_EDE_CBC_SHA**)

FIPS 140-2 Compliance

Migrator for Notes to SharePoint cryptographic usage is based on FIPS 140-2 compliant cryptographic functions. Migrator for Notes to SharePoint makes use of FIPS 140-2 compliant encryption keys stored locally using Microsoft DPAPI]

Migrator for Notes to SharePoint has undergone a Quest internal Self-Affirmation process to confirm that all cryptographic usage relies exclusively on Third-Party FIPS 140-2 validated modules.

More information:

- Microsoft and FIPS: https://www.microsoft.com/en-us/trustcenter/compliance/fips
- Microsoft FIPS backgrounder: https://aka.ms/fips-backgrounder

SDLC and SDL

The Migrator for Notes to SharePoint team follows a strict Quality Assurance cycle.

- Access to source control and build systems is protected by domain security, meaning that only employees on Quest's corporate network have access to these systems. Therefore, once a Migrator for Notes to SharePoint technical resource leaves the company, this individual will no longer be able to access Migrator for Notes to SharePoint systems.
- All code is versioned in source control.
- All product code is reviewed by another developer before check-in.

In addition, the Migrator for Notes to SharePoint Development team follows a managed Security Development Lifecycle (SDL) which includes:

- MS-SDL best practices
- Threat modeling.
- OWASP guidelines.
- Regularly scheduled static code analysis is performed on regular basis.
- Regularly scheduled vulnerability scanning is performed on regular basis.

Segregated Development, Pre-Production, and Production environments. Customer data is not used in Development and Pre-Production environments. Migrator for Notes to SharePoint developers go through the same set of hiring processes and background checks as other Quest employees

Customer Measures

Migrator for Notes to SharePoint security features is only one part of a secure environment. Customers should follow their own security best practices when deploying Migrator for Notes to SharePoint within their environment.

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