Quest®

Metalogix® Content Matrix

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

Metalogix® Content Matrix
Updated July 2023

Contents

Introduction **4**

About Metalogix® Content Matrix **5**

Architecture Overview **6**

Overview of Data Handled by Metalogix® Content Matrix **7**

Admin Consent and Service Principals **8**

Location of Customer Data **9**

Privacy and Protection of Customer Data **10**

- SharePoint Database Connections 10
- Azure Import Pipeline 10
- Distributed Migration 10
  - Jobs Database Credentials 10
- Backward Compatibility 11

Network Communications **12**

Authentication of Users and Services **13**

FIPS 140-2 Compliance **14**

Air Gap Compliance **15**

SDLC and SDL **16**

Customer Measures **17**

About Us **18**

- Technical Support Resources 18
- Contacting Quest 19

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 Metalogix® Content Matrix. This includes access control, protection of customer data, secure network communication, cryptographic standards and more.

2

About Metalogix® Content Matrix

Metalogix® Content Matrix is a Windows-based application that runs on a Windows server or client. It provides an easy to use, convenient way of moving SharePoint and Exchange content to SharePoint. With its familiar copy-and-paste style user interface, Metalogix® Content Matrix can quickly migrate your content into SharePoint, while preserving valuable user metadata. Metalogix® Content Matrix product comes in the following editions:

- **Metalogix® Content Matrix SharePoint Edition**

  Suitable for migrations between SharePoint servers, upgrading from one version of SharePoint to another, migrating to Office 365, or simply reorganizing SharePoint content.

- **Metalogix® Content Matrix Public Folder Edition**

  Suitable for migrating Exchange Public Folders or PST files to SharePoint.

Architecture Overview

The following scheme shows the key components of the Metalogix® Content Matrix configuration.

> NOTE: Metalogix® Content Matrix is a Windows-based desktop application and does not provide user or service management.

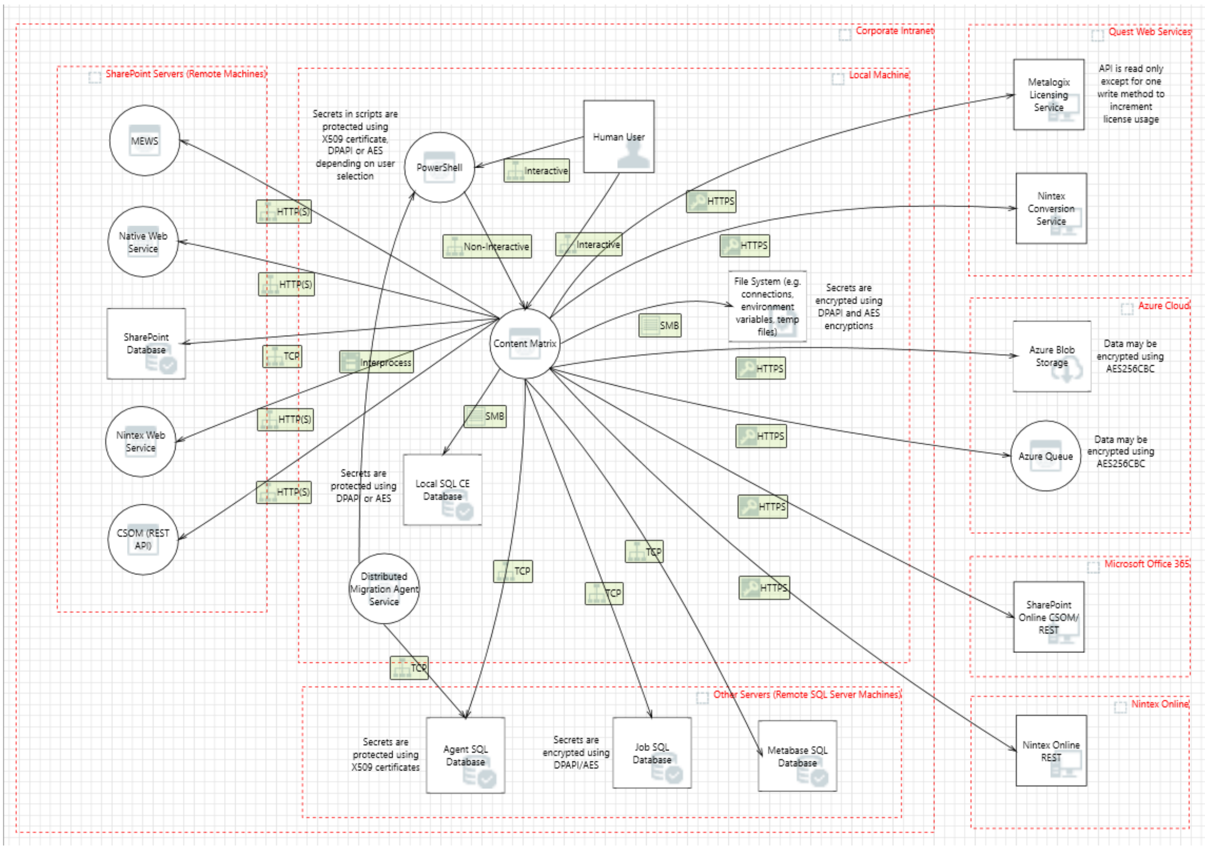

Corporate Intranet
SharePoint Servers (Remote Machines)
MEWS
Native Web Service
SharePoint Database
Nintex Web Service
CSOM (REST API)
Local Machine
Secrets in scripts are protected using X509 certificate, DPAPI or AES depending on user selection
PowerShell
Human User
Interactive
Non-Interactive
Interactive
HTTP(S)
HTTP(S)
TCP
Interprocess
HTTP(S)
HTTP(S)
Content Matrix
SMB
Secrets are protected using DPAPI or AES
Local SQL CE Database
Distributed Migration Agent Service
TCP
TCP
TCP
TCP
HTTPS
HTTPS
SMB
File System (e.g. connections, environment variables, temp files)
Secrets are encrypted using DPAPI and AES encryptions
HTTPS
HTTPS
HTTPS
HTTPS
Other Servers (Remote SQL Server Machines)
Secrets are protected using X509 certificates
Agent SQL Database
Secrets are encrypted using DPAPI/AES
Job SQL Database
Metabase SQL Database
Quest Web Services
Metalogix Licensing Service
API is read only except for one write method to increment license usage
Nintex Conversion Service
Azure Cloud
Azure Blob Storage
Data may be encrypted using AES256CBC
Azure Queue
Data may be encrypted using AES256CBC
Microsoft Office 365
SharePoint Online CSOM/ REST
Nintex Online
Nintex Online REST

Figure 1: High-Level Architecture

4

Overview of Data Handled by Metalogix® Content Matrix

Metalogix® Content Matrix manages the following types of customer data:

- Metalogix® Content Matrix works with SharePoint content and Exchange content. The content processed by the product is not persistently stored by the product. Some file content may be fetched and stored in file system encrypted for the period of migration.
- Some data from end-user SharePoint or Public Folder content can be stored by the product for troubleshooting purposes. This includes data to identify the items where some troubleshooting is required.
- The application stores administrative account name and password to perform migration operations. The data is stored in product database and is encrypted at rest.

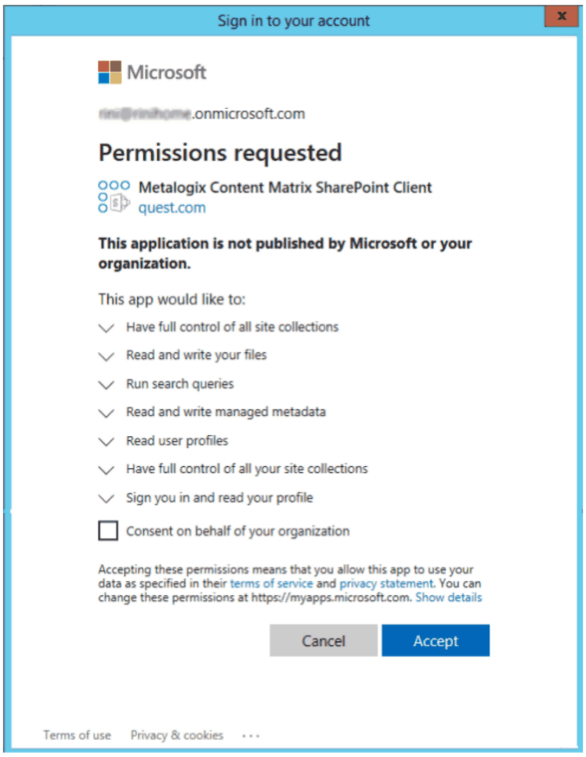
5

Admin Consent and Service Principals

Metalogix® Content Matrix 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 Metalogix® Content Matrix migration. 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 hhttps://docs.microsoft.com/en-us/azure/active-directory/manage-apps/delete-application-portal and https://docs.microsoft.com/en-us/skype-sdk/trusted-application-api/docs/tenantadminconsent for details.

Following is the base consent required by Metalogix® Content Matrix.



Sign in to your account

Microsoft

[redacted].onmicrosoft.com

Permissions requested

Metalogix Content Matrix SharePoint Client
quest.com

This application is not published by Microsoft or your organization.

This app would like to:

- Have full control of all site collections
- Read and write your files
- Run search queries
- Read and write managed metadata
- Read user profiles
- Have full control of all your site collections
- Sign you in and read your profile

□ Consent on behalf of your organization

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details

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 or file provided by the customer.
- In case of migration using "Import API" option, binary contents of files are uploaded to Azure blob storage. Metalogix® Content Matrix can use either SPO provided Azure container blob storage or customer provided private Azure container blob storage.

7

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 and Public Folder connections are encrypted using Microsoft DPAPI (ProtectedData Class (System.Security.Cryptography) | Microsoft Docs).

SharePoint Database Connections

When a SharePoint 2013 or later database connection is used as source, large file content is fetched and temporarily stored in file system before it is copied to the target. AesCryptoServiceProvider is used to encrypt this content.

Azure Import Pipeline

- When the Import Pipeline is used, security-sensitive information about Azure blob storage SAS 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.

Jobs Database Credentials

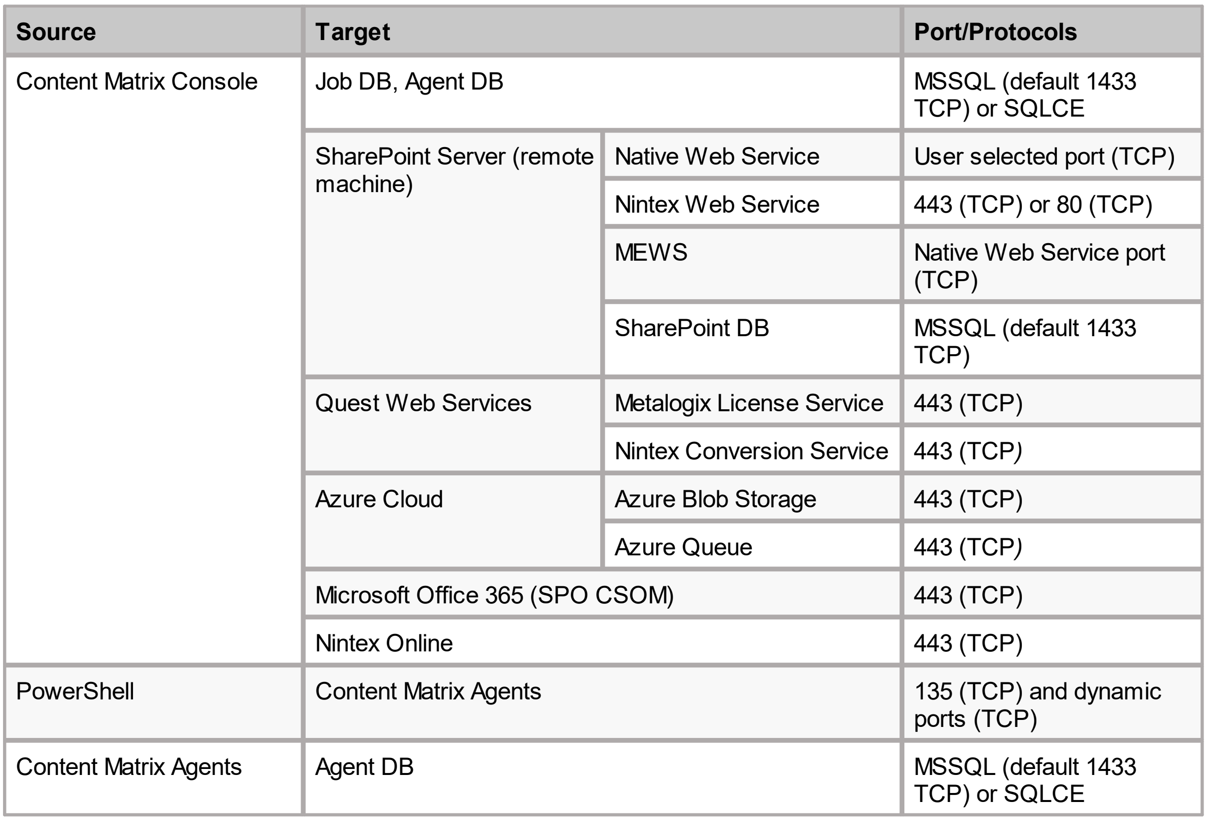
Job database (SQL Server) connection credentials are encrypted with Microsoft DPAPI.

Backward Compatibility

- TDES is supported to decrypt data from version 9.2 or earlier. Beginning in Metalogix® Content Matrix version 9.3, Microsoft DPAPI is used to encrypt data.
- For Public Folder Edition, TDES is used to decrypt passwords for Exchange connections created in Metalogix® Content Matrix version 9.2 or earlier. Beginning in version 9.3, passwords are encrypted with Microsoft DPAPI.

8

Network Communications



Source	Target		Port/Protocols
Content Matrix Console	Job DB, Agent DB		MSSQL (default 1433 TCP) or SQLCE
	SharePoint Server (remote machine)	Native Web Service	User selected port (TCP)
		Nintex Web Service	443 (TCP) or 80 (TCP)
		MEWS	Native Web Service port (TCP)
		SharePoint DB	MSSQL (default 1433 TCP)
	Quest Web Services	Metalogix License Service	443 (TCP)
		Nintex Conversion Service	443 (TCP)
	Azure Cloud	Azure Blob Storage	443 (TCP)
		Azure Queue	443 (TCP)
	Microsoft Office 365 (SPO CSOM)		443 (TCP)
	Nintex Online		443 (TCP)
PowerShell	Content Matrix Agents		135 (TCP) and dynamic ports (TCP)
Content Matrix Agents	Agent DB		MSSQL (default 1433 TCP) or SQLCE

Figure 2: List of protocols used and associated ports

.

9

Authentication of Users and Services

Metalogix® Content Matrix relies upon

- Windows Authentication and Active Directory group membership to authenticate users
- Forms Based Authentication which authenticates through IIS
- Azure Active Directory authenticating via Office 365 OAuth Authentication
- Azure Active Directory authenticating via Office 365 Web Browser

10

FIPS 140-2 Compliance

Metalogix® Content Matrix cryptographic usage is based on FIPS 140-2 compliant cryptographic functions. Metalogix® Content Matrix makes use of FIPS 140-2 compliant encryption keys stored locally using Microsoft DPAPI.

Metalogix® Content Matrix 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

Air Gap Compliance

Metalogix® Content Matrix is Air Gap compliant.

What is Air Gap?

Air Gap is an architecture based on physical separation and trusted people. Its goal is to demonstrably protects all product builds and code delivery from potential mischievous employee or external actors, regardless of world location.

Air Gap Components

Air Gap consists of:

- A secure *facility* within Quest that contains the complete supply and assembly chain for all products in scope.
- *Limited access*: only select employees have access to review, accept, and transfer contributions into this environment.
- A *vetted secure build process* which entirely separates the Product Development from the Product Build.

12

SDLC and SDL

The Metalogix® Content Matrix 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, should an Metalogix® Content Matrix developer leave the company, this individual will no longer be able to access Metalogix® Content Matrix systems.
- All code is versioned in source control.
- All product code is reviewed by another developer before check in.

In addition, the Metalogix® Content Matrix Development team follows a managed Security Development Lifecycle (SDL) which includes:

- MS-SDL best practices
- Threat modelling.
- OWASP guidelines.
- Scheduled static code analysis is performed on a regular basis.
- Scheduled vulnerability scanning is performed on a regular basis.
- Development, Pre-Production, and Production environments are segregated. Customer data is not used in Development and Pre-Production environments.
- Metalogix® Content Matrix developers go through the same set of hiring processes and background checks as other Quest employees.

13

Customer Measures

Metalogix® Content Matrix security features are only one part of a secure environment. Customers should follow their own security best practices when deploying Metalogix® Content Matrix within their environment.

14

About Us

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com.

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

Contacting Quest

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