PROMODAG STORELOG

Getting started

On-Premises
and
Hybrid environments

COPYRIGHTS

PROMODAG SA
8, rue Charles-Pathé
94300 VINCENNES
France

https://www.promodag.com

Rev- 1 - 11/2025

TABLE OF CONTENTS

Executive Summary

> FOR DECISION MAKERS
> Read: Executive Summary + Product Description.
> Time needed: 5 minutes.

The Problem:

Microsoft Exchange Online only retains message tracking logs for 90 days, creating compliance gaps and potential data loss for organizations subject to regulatory requirements or those needing long-term email audit trails. When critical email tracking data expires, forensic investigations become impossible and compliance violations can result in significant penalties.

The Solution:

Promodag StoreLog automatically retrieves and archives your Exchange message tracking data before it expires, storing it indefinitely in SQL databases for powerful analysis and reporting. This free utility saves organizations thousands in compliance costs, prevents data loss, and enables comprehensive email forensics—all without modifying your Exchange environment or requiring expensive third-party solutions.

Get Started in a couple of minutes

Ready to protect your message tracking data? Follow these 5 simple steps:

- **Create and authorize the app in Microsoft Entra ID** (5-10 min). Do it first, see "Certificate-Based Authentication to Exchange Online", on page 8,
- **Run the package** (2 min), see "Installing Promodag StoreLog", on page 11,
- **Create your database** (1 min), see "Initial Setup", on page 11,
- **Create your first Exchange Online tracking logs** (5-20 min depending on data volume), see "Retrieving Message Tracking Log files From an Exchange Online environment", on page 11 ,
- **Import data** (5-20 min depending on data volume), see "Importing Message Tracking Files", on page 12.

About This Guide

This guide is designed to provide a quick introduction to Promodag StoreLog for Microsoft Exchange, and it describes steps from getting started to querying the database.

For more details about specific features of Promodag StoreLog, please refer to the help file delivered with the application in the Help menu.

Introducing Promodag StoreLog

StoreLog is a free utility designed to help Exchange administrators retrieve, archive, and analyze message tracking data from both on-premises Exchange servers and Exchange Online (Office 365).

With Exchange Online's limitation of only retaining message tracking data for 90 days, StoreLog provides a crucial solution for organizations that need to preserve email tracking information for compliance, forensic analysis, or long-term reporting purposes.

Key Features

- Free to use - StoreLog is provided as freeware with no licensing costs or evaluation limitations
- Exchange Online integration - Automatically retrieves message tracking logs from Office 365 before they expire
- On-premises support - Works with Exchange Server 2010 through 2019
- SQL database storage - Imports tracking data into SQL Server for powerful querying and analysis
- Familiar log format - Generates message tracking files in the same format as on-premises Exchange servers
- Chronological organization - Sorts tracking events in proper time order, unlike native Exchange Online logs
- Long-term retention - Archive message tracking data indefinitely for compliance and analysis

Product Description

Who should use StoreLog?

- Exchange administrators managing hybrid or cloud-only environments
- IT professionals who need to retain email tracking data beyond Office 365's 90-day limit
- Organizations requiring forensic email analysis capabilities
- Companies with compliance requirements for email audit trails

What StoreLog does:

1. Connects to Exchange Online using secure certificate-based authentication
2. Retrieves message tracking data before it expires (90-day limit)
3. Generates daily message tracking log files in familiar Exchange format
4. Imports tracking data into SQL Server databases for analysis
5. Enables powerful SQL queries for email traffic analysis and forensic investigations
6. StoreLog is easy to install and configure, requiring no modifications to your Exchange environment. Once set up, it can be automated to regularly collect and archive your organization's email tracking data, ensuring you never lose valuable audit information.

Should you need a more advanced Exchange reporting tool, please download **Promodag Reports** from our website (http://www.promodag.com).

Chapter 1. Setting Up Your Environment

> **FOR IT ADMINISTRATORS**
> This chapter covers prerequisites and authentication setup. Essential for first-time setup.
> Time needed: 5-10 minutes.

1.1 Computer Requirements

1.1.1. Workstation hardware and software requirements

Computer requirements

Promodag StoreLog can be installed on a machine running a supported desktop or server operating system. It is not recommended to install it on a strategic element of your environment, for example a GC server or an Exchange server.

Hardware and software requirements

- Computer: A Core i3 Intel Processor with 4 GB of RAM or an equivalent Virtual Machine.
- Supported operating systems: A 64-bit version of Windows 10/Windows Server 2016 to Windows 11/Windows Server 2025. Core versions of Microsoft Windows Server are not supported.
- Database management system: Microsoft SQL Server Express LocalDB 2017 (delivered with the product) or Microsoft SQL Server 2012 to SQL Server 2025 (32 or 64-bit). Microsoft SQL Server Express database size is limited to 10 GB.

Network requirements

The computer running StoreLog does not need to be installed on an Exchange server or any strategic element of your environment. It can run on any workstation that meets the system requirements and has appropriate network connectivity.

Specific requirements for Exchange Online

Internet access

If your Exchange organization is Hybrid or full Office 365, the computer must have access to the Internet and the endpoints whose list is regularly updated by Microsoft must be reachable for customers using Office 365 plans, including Government Community Cloud (GCC).

1.2 Microsoft Exchange Requirements

StoreLog supports Exchange Online (Office 365) as well as Microsoft Exchange Server from 2010 to 2019. It is possible to use the product in a mixed environment, with different versions of Exchange.

1.3 Certificate-Based Authentication to Exchange Online

1.3.1. Create the certificate and the Promodag StoreLog Application

Please follow these steps to create the Promodag StoreLog Application, the certificate, register them in Microsoft Entra ID and create a dedicated role group in Exchange Admin Center:

Prerequisites

The computer's operating system version must be greater than or equal to Windows 10/Windows Server 2016. Microsoft PowerShell 7 or higher is required.

The ExchangeOnlineManagement and Microsoft.Graph PowerShell modules should be installed on the computer. It they are not, please proceed with these steps:

1. Click ⊞ and search for PowerShell > Windows PowerShell 7 and run it as administrator.
2. Install the ExchangeOnlineManagement module: Install-Module ExchangeOn-lineManagement -Scope AllUsers

3. Install the Microsoft.Graph module: Install-Module Microsoft.Graph -Scope AllUsers

Create the certificate and application using the provided script

These steps will enable you to create a self-signed certificate, an application in Microsoft Entra ID to access your tenant, and a role group in Exchange Admin Center.

1. The script is delivered by default in the C:\Users\Public\Documents\Promodag\StoreLog\ dir-ectory but you can use it from a different location.

2. Run the script: ./CreateStorelogRBACApp.ps1
3. Enter certificate password at prompt and write it down.
4. The script will proceed, and you will be prompted to sign-in to Office 365 to create the role group and grant it the relevant permissions. Use a Global Administrator account.

5. A certificate valid for two years has now been created in the script directory with the name "StoreLogRBACAppCertificate.pfx". The application has been created in Microsoft Entra ID with the name "Promodag StoreLog RBAC Application", a role group with the name "Pro-modag StoreLog RBAC Role Group" has been created in Exchange Admin Center, a service principal object has been created for this new application and it has been added as a member of this new role group.

6. The script displays the summary information to be used in StoreLog: Application ID and cer-tificate path, plus a link (*Authorization URL*) to connect to Microsoft Entra ID and authorize

the newly created application. This information is then saved into a file in the current directory.

1.3.2. Authorize this new application in Microsoft Entra ID

Grant admin consent

1. Paste the URL displayed in a web browser to connect to Microsoft Entra ID. Sign in using a Global Administrator account. The Promodag StoreLog RBAC Application | API permissions page opens.

2. Click **Grant admin consent for <name of your Office 365 tenant>**.

3. Review the permissions granted to the application (see details of these permissions here: Required permissions)

Optional: You can delete the self-signed certificate and use your own if you prefer. To upload your own certificate, see the help file delivered with the application in the Help menu.

1.3.3. Apply "Promodag StoreLog RBAC Application" settings to StoreLog

Please make sure that you have retrieved the following information from the first step:

- Application ID,
- Certificate path,
- Certificate password.

1. In Promodag StoreLog, go to **Tools > Options**, Exchange Online Connection.
2. Enter the Application ID and Certificate password in the corresponding fields.
3. Enter the path to the .pfx certificate file in the corresponding field.

4. Click the Check validity link to verify the certificate expiration date.
5. Click the Check connection links to verify that StoreLog can connect to your tenant using the Microsoft Entra ID application and the certificate.

1.3.4. Create a custom StoreLog application manually

To create your own custom StoreLog app in Microsoft Entra ID, see the help file delivered with the application in the Help menu.

1.3.5. Edit or delete the a StoreLog Application, renew the certificate

To edit or delete your StoreLog app in Microsoft Entra ID or to renew its certificate, see the help file delivered with the application in the Help menu.

Chapter 2. Getting Started

> FOR QUICK SETUP
>
> Install the application, create Exchange Online message tracking files and import them.
> Time needed: 10-30 minutes.

2.1 Installing Promodag StoreLog

> Note: Please make sure that your workstation complies with all points listed in the "Computer Requirements", on page 7 before proceeding with the installation process.

2.1.1. Installing Promodag StoreLog

a. Go to http://www.promodag.com to download Promodag StoreLog.
b. Choose a temporary directory to store the installation package.
c. Click on the StoreLog60.exe icon from your temporary directory to start the installation process.

2.2 Initial Setup

2.2.1. Creating a New StoreLog Database

This is the very first step.

You may either click the icon in the toolbar, or use the *File > New database* option.

2.2.2. Gathering On-Premises Exchange servers

Once your database has been created, it is recommended that you gather On-premises Exchange servers, i.e. let Promodag StoreLog discover servers in your Exchange organization.

You may either click the icon in the toolbar, or use the *File > Gather On-premises Exchange Servers* option.

2.2.3. Retrieving Message Tracking Log files From an Exchange Online environment

Use the *Create Exchange Online Message Tracking Files* option in the file menu to query Office 365 and create your first message tracking files.

StoreLog will then query Exchange Online and generate one log per day, covering a period of 90 days at the most. The default directory for generated Message Tracking Log files is C:\Users\Public\Documents\Promodag\StoreLog\Office365MessageTracking\<Organization name> and the name format of these files is MSGTRKCyyyymmdd-1.log.

Once you have generated these log files you can:

- Automate this log generation process.
- Archive tracking logs for further processing.
- Open them in a text editor to search for a particular subject or recipient.
- Import them using StoreLog in an SQL server database, and then use standard SQL queries to produce simple reports.
- Import them using Promodag Reports, that supports Exchange Online.

2.2.4. Importing Message Tracking Files

This feature lets you import Exchange message tracking files into the database.

You can either

- Import message tracking files from a selection of servers, if you already have gathered On-premises Exchange servers from your organization (you may either click the icon in the toolbar, or use the **Import Message Tracking Files from a Selection of Servers** option).

- Or directly import message tracking files from a location (you may either click the icon in the toolbar, or use the **File > Import Message Tracking Files from a Location** option).

2.3 Scheduling and Automation

Once you have successfully retrieved and imported message tracking files, you can automate this process to run regularly. StoreLog operations can be scheduled using Windows Task Scheduler or automated through command-line parameters.

2.3.1. Automate the creation of Exchange Online message tracking files

To automatically create tracking files, use the **Schedule Exchange Online Message Tracking Files Creation** option in the **Tools** menu.
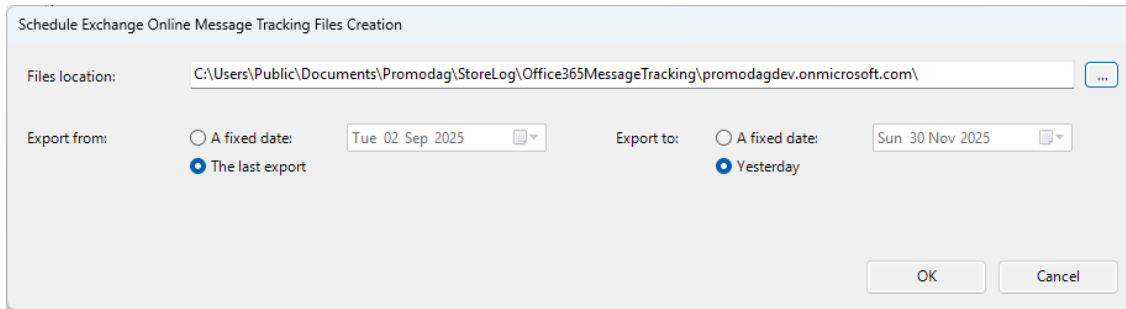
To create the default batch file in Promodag StoreLog, follow these steps:

1. Check default options and modify them if necessary. Click **OK**.
2. Open the C:\Users\Public\Documents\Promodag\StoreLog\6\Batches directory and verify that a StoreLog.prb has been created. Rename it if required.

To schedule the execution of this batch In Windows, follow these steps:

1. Open Task Scheduler by clicking the Start button, clicking Control Panel, clicking System and Security, clicking Administrative Tools, and then double-clicking Task Scheduler.
2. Click the Action menu, and then click **Create Basic Task**.
3. Type a name for the task and an optional description, and then click **Next**.
4. To select a schedule based on the calendar, click Daily, click Next; specify the schedule you want to use, and then click **Next**.
5. Click Start a program, and then click **Next**.
6. Click Browse and navigate to the installation directory of StoreLog, and select StoreLog.exe. The default installation directory of the program is: C:\Program Files\Promodag\StoreLog6.
7. In the 'Add arguments (optional)' field, enter the name of the batch as follows: /BatchFile-e=<batch name>.prb> and then click **Next**.
8. Click **Finish**.
9. Edit the new task and select the 'Run whether user is logged or not' radio button in the General tab.
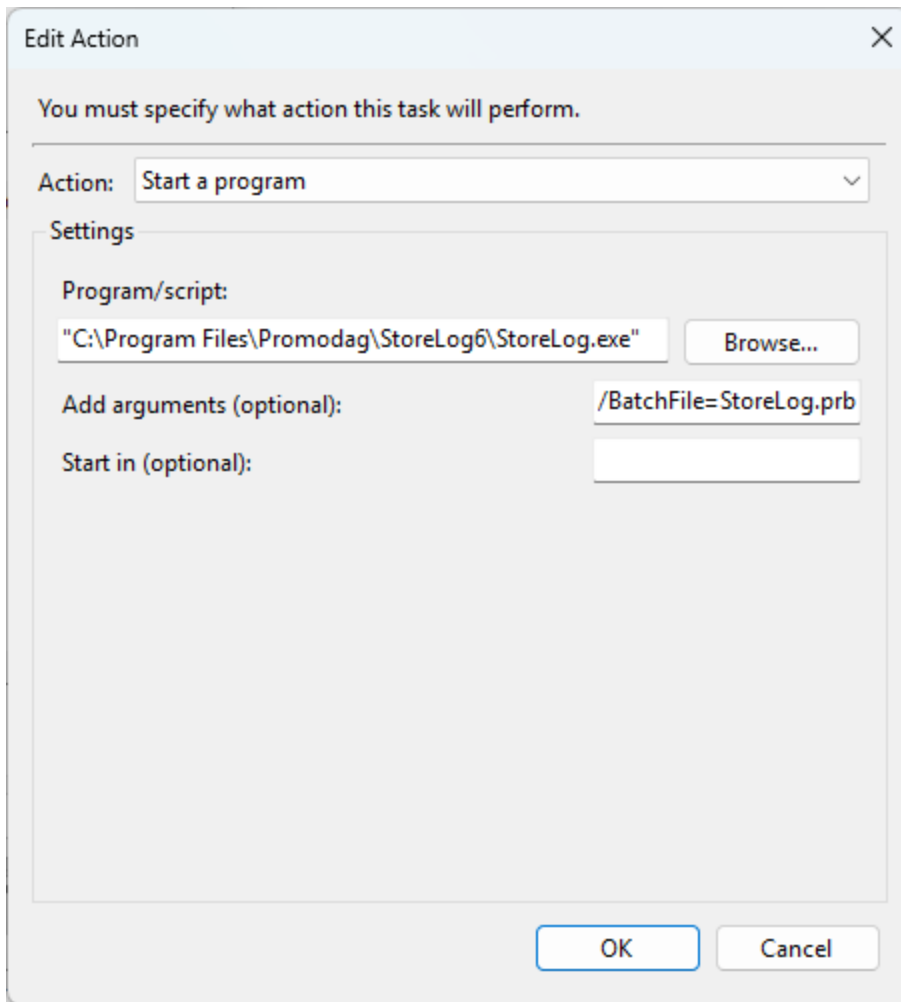
2.3.2. Automate the import of message tracking files

To automatically import message tracking files, use the **Schedule Message Trackin Data Import** option in the **Tools** menu.

The principle behind creating the default batch file (StoreLog.prb) and automation is identical to that described for creating tracking files. If you have already created your batch for creating message tracking files, StoreLog will simply modify it by adding the data import command.

2.3.3. Command line parameters

The syntax for running the StoreLog batch from the command line is identical to that used by a scheduled task:

"<Path to StoreLog.exe" /BatchFile=<Batch.prb>

Example: **"C:\Program Files\Promodag\StoreLog6\StoreLog.exe" /BatchFile-e=StoreLog.prb**

Chapter 3. Using StoreLog

FOR DATA ANALYSTS & COMPLIANCE TEAMS
Learn to query your archived data and create custom reports.
Time needed: 30 minutes + ongoing analysis.

3.1 Using the Database

You will have to use SQL Server management tools or any other third-party SQL query tool to exploit the data you have imported in your database.
Nevertheless, queries are easy to create, particularly if you use the graphical query designer tools delivered with SQL Server Management Studio to displays connections between tables (see "Database Schema Visualization", on page 20).

3.2 Common Use Cases

StoreLog's ability to archive message tracking data in SQL databases makes it valuable for several scenarios where long-term retention and querying of tracking logs is needed:

- **Compliance and data retention**

Organizations subject to regulatory requirements can use StoreLog to preserve message tracking data beyond Office 365's 90-day retention limit. By storing tracking logs in SQL databases, companies can maintain email audit trails for extended periods to meet compliance obligations and legal discovery requirements.

- **Forensic investigations**

When email-related incidents occur, StoreLog provides access to historical message tracking data that would otherwise be lost. Investigators can query the SQL database to trace message paths, identify senders and recipients, and establish communication timelines using standard SQL queries.

- **Long-term email flow analysis**

IT administrators can analyze email traffic patterns over extended periods by querying archived tracking data. This helps identify trends in email volume, track communication patterns between domains, and monitor the effectiveness of email routing configurations.

- **Custom reporting and analysis**

Organizations with specific reporting needs can leverage StoreLog's SQL database storage to create custom queries and reports. The familiar message tracking log format, combined with SQL's powerful querying capabilities, enables tailored analysis that meets unique business requirements.

- **Backup and archive strategy**

StoreLog serves as a backup solution for message tracking data, ensuring that critical email flow information is preserved even if Exchange Online logs are purged. This archived data can be essential for troubleshooting historical email delivery issues or reconstructing past communication events.

3.3 Getting Started with SQL Server Management Studio (For Non-Technical Users)

> FOR BUSINESS USERS & MANAGERS
> Simple steps to access your archived email data without technical expertise.
> Time needed: 10 minutes.

If you're not familiar with SQL Server Management Studio (SSMS), don't worry - you only need to know a few basics to query your StoreLog data.

3.3.1. Downloading and Installing SSMS

- Download SQL Server Management Studio from Microsoft's website (it's free)
- Install with default settings
- No special configuration needed.

3.3.2. Connecting to Your Database

- Open SSMS
- Click "Connect" → "Database Engine"
- Server name: your IT administrator will provide your with the SQL server name. If using a LocalDB database, simply enter **(localDB)\Promodag**.
- Authentication: Windows Authentication (default)
- Click **Connect**.

3.3.3. Finding Your Data

- In Object Explorer, expand "Databases"
- Look for your StoreLog database (usually named "StoreLog" or similar)
- Expand "Tables" to see your data tables.

3.3.4. Running Simple Queries

- Click "New Query" button
- Copy and paste queries from our "SQL Query Library", on page 28.
- Replace "@yourdomain.com" with your actual domain
- Click "Execute" (or press F5).

3.3.5. Exporting Results

- Right-click on query results
- Choose "Save Results As..." → CSV format
- Save for reporting or analysis.

3.3.6. Common Questions

- What if I make a mistake?" - Queries only READ data, they won't change anything
- "Can I break something?" - No, you're only viewing data
- "What if I need help?" - Contact your IT administrator with specific questions

3.4 Using Data in SQL Server

Let us say that you recently received a number of spams whose subject contains the expression 'discount' or 'sales'. You have imported yesterday's message tracking files in a Promodag StoreLog database and you now need to find out which SMTP domains or specific addresses may need to be blocked.

3.4.1. Build queries using the Query Designer of SQL Server Management Studio

Search for external messages whose subject contains the string "Sales"

A simple query using, from the Events_365 table, the SenderAddress and Subject field containing the chain of characters 'sale' and the count of MessageId clearly shows which SMTP addresses sent those spams.

The Query Designer makes it easy to build:
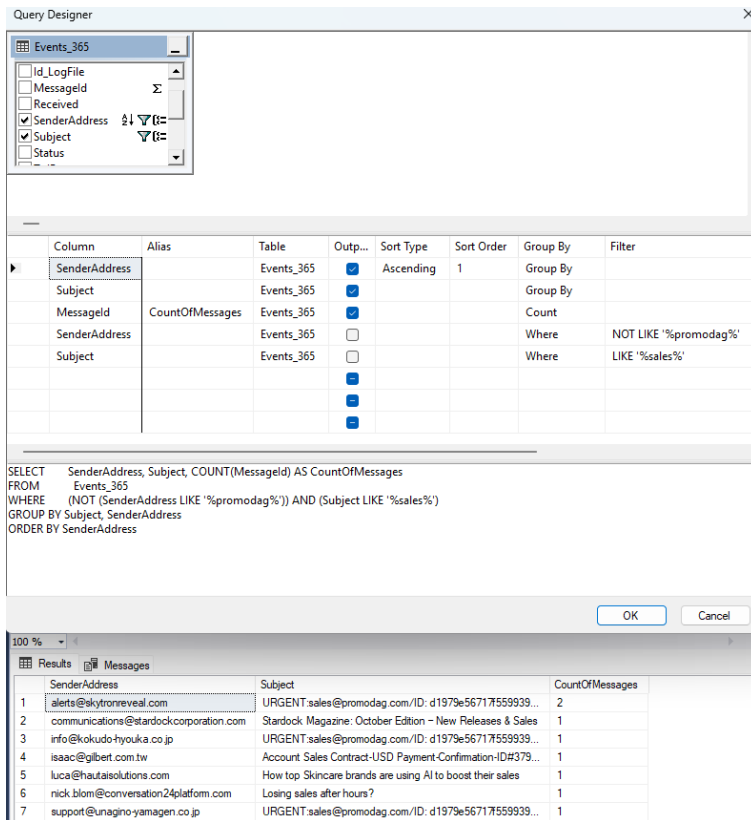
The SQL query itself is:

```
SELECT
SenderAddress,
Subject,
COUNT(MessageId) AS CountOfMessages
FROM [Events_365]
WHERE (NOT (SenderAddress LIKE '%promodag%'))
AND (Subject LIKE '%sales%')
GROUP BY Subject, SenderAddress
ORDER BY SenderAddress
```

Additional query examples

For more query examples, see "SQL Query Library", on page 28.

3.4.2. Database Schema Visualization

Here is StoreLog database structure as seen in SQL Server Management Studio.
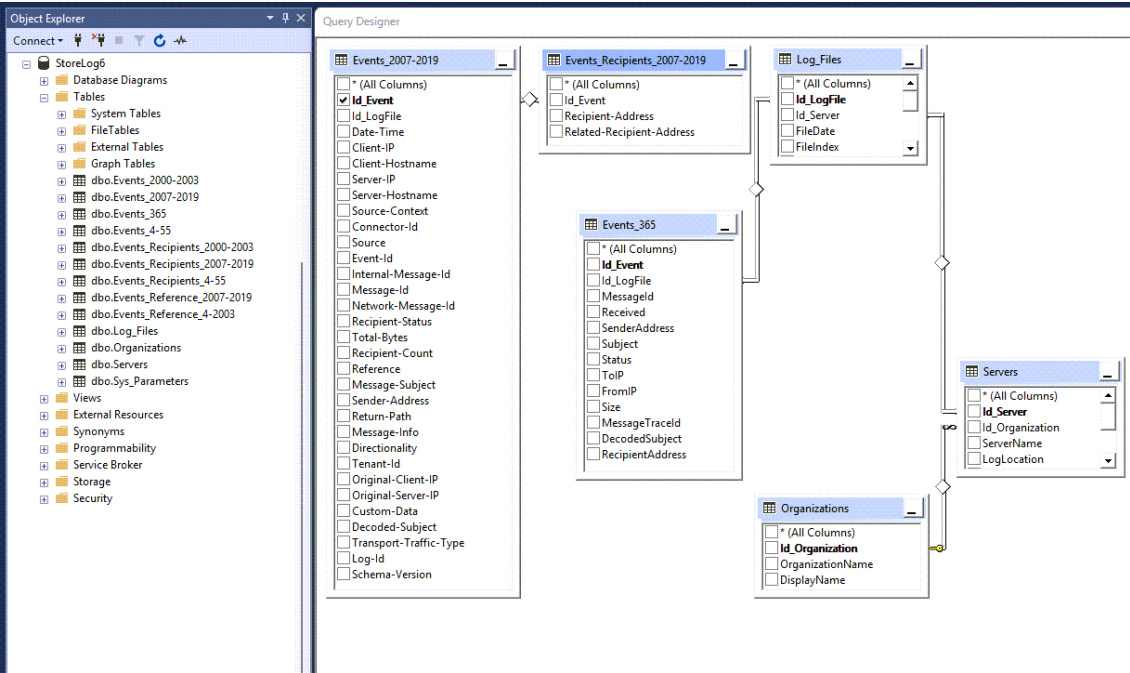
3.4.3. Database Reference

This section provides a complete technical reference for the StoreLog database schema. Whether you're writing custom queries, integrating with other systems, or simply need to understand how your data is organized, this reference will guide you through every table, column, and relationship.

How to Use

1. Use the **Table Overview** to understand which tables contain the data you need.
2. Reference **Detailed Table Structures** for exact column names and data types.
3. Check **Data Relationships** to understand how tables connect for JOIN queries.

Table overview

Table name	Environment	Purpose
Organizations	Both Environments	Organization/tenant information
Servers	Both Environments	Exchange servers and Office 365 tenants
Events_2007-2019	On-Premises Only	Message tracking events (sender info)
Events_Recipients_2007-2019	On-Premises Only	Message recipient information
Events_365	Exchange Online Only	Combined message tracking data
Log_Files	Both Environments	Log file metadata

Detailed table structures

Organizations (both environments)

Column name	Description
Id_Organization	Primary key identifier (internal use)
OrganizationName	Internal organization/tenant name
DisplayName	Human-readable organization/tenant display name

Servers (both environments)

Column name	Description
Id_Server	Primary key identifier (internal use)

Column name	Description
Id_Organization	Foreign key to Organizations table
ServerName	Exchange server name or "Office365Mes-sageTracking" for Office 365
LogLocation	Path to message tracking log files (On-Premises only)
NextFile	Next file to process
Selected	Whether server/tenant is selected for processing
ExchangeVersion	Version of Exchange Server or Office 365
LastGeneratedFile	Last processed log file

Events_2007-2019 (on-premises only - message information)

Column name	Description	Get-MessageTrackingLog equivalent
Id_Event	Primary key identifier (internal use)	-
Id_LogFile	Foreign key to Log_Files table	-
Date-Time	Event timestamp	Timestamp
Client-Ip	Client IP address	client-ip
Client-Hostname	Client hostname	client-hostname
Server-Ip	Server IP address	server-ip
Server-Hostname	Server hostname	server-hostname
Source-Context	Source context information	source-context
Connector-Id	Connector identifier	connector-id
Source	Message source	source
Event-Id	Event type identifier	event-id
Internal-Message-Id	Internal message identifier	internal-message-id
Message-Id	Message identifier	message-id
Network-Message-Id	Network message identifier	network-message-id
Recipient-Status	Recipient delivery status	recipient-status
Total-Bytes	Message size in bytes	total-bytes

Column name	Description	Get-MessageTrackingLog equivalent
Recipient-Count	Number of recipients	recipient-count
Reference	Reference information	reference
Message-Subject	Message subject (encoded)	message-subject
Sender-Address	Sender email address	sender-address
Return-Path	Return path address	return-path
Message-Info	Additional message information	message-info
Directionality	Message direction (inbound/outbound)	directionality
Tenant-Id	Tenant identifier	tenant-id
Original-Client-IP	Original client IP	original-client-ip
Original-Server-IP	Original server IP	original-server-ip
Custom-Data	Custom data field	custom-data
Decoded-Subject	Decoded message subject	-
Transport-Traffic-Type	Traffic type classification	transport-traffic-type
Log-Id	Log identifier	log-id
Schema-Version	Schema version	schema-version

Events_Recipients_2007-2019 (on-premises only - recipient information)

Column name	Description
Id_Event	Foreign key to Events_2007-2019 table
Recipient-Address	Recipient email address
Related-Recipient-Address	Related recipient address

Events_365 (Exchange Online only - combined data)

Column name	Description	Get-MessageTrace equivalent
Id_Event	Primary key identifier (internal use)	-
Id_LogFile	Foreign key to Log_Files table	-

Column name	Description	Get-MessageTrace equivalent
Organization	Office 365 organization name	Organization
MessageId	Unique message identifier	MessageId
Received	Message received timestamp	Received
SenderAddress	Sender email address	SenderAddress
RecipientAddress	Recipient email address	RecipientAddress
Subject	Message subject	Subject
Status	Message delivery status	Status
ToIP	Destination IP address	ToIP
FromIP	Source IP address	FromIP
Size	Message size in bytes	Size

Log_Files (both environments)

Column name	Description
Id_LogFile	Primary key identifier (internal use)
Id_Server	Foreign key to Servers table
Filename	Log file name
FirstLogEntry	Timestamp of first log entry
LastLogEntry	Timestamp of last log entry
DateProcessed	When the log file was processed
NumberOfEntries	Number of log entries processed

Data relationships and indexing

Primary relationships

- **Organizations → Servers:** One-to-many relationship via Id_Organization
- **Servers → Log_Files:** One-to-many relationship via Id_Server
- **Log_Files → Events_2007-2019:** One-to-many relationship via Id_LogFile
- **Log_Files → Events_365:** One-to-many relationship via Id_LogFile
- **Events_2007-2019 → Events_Recipients_2007-2019:** One-to-many relationship via Id_Event

Key indexes for performance

- **Events_2007-2019:** Indexes on Date-Time, Sender-Address, Message-Id, Internal-Message-Id
- **Events_Recipients_2007-2019:** Indexes on Id_Event, Recipient-Address
- **Events_365:** Indexes on Received, SenderAddress, RecipientAddress, MessageId
- **Log_Files:** Indexes on Id_Server, FirstLogEntry, LastLogEntry

Environment-specific considerations

On-Premises Exchange (2007-2019)

Message tracking data is stored in separate tables for events and recipients to normalize the data structure. Each message event can have multiple recipients, which are stored in the Events_Recipients_2007-2019 table.

Key characteristics:

- Detailed field mapping from Exchange message tracking logs
- Separate recipient tracking for multi-recipient messages
- Support for custom fields and extended properties
- File-based log processing with metadata tracking

Exchange Online (Office 365)

Message tracking data is stored in a single denormalized table (Events_365) that combines message and recipient information. This reflects the structure of data returned by the Get-MessageTrace PowerShell cmdlet.

Key characteristics:

- Simplified schema matching Office 365 API structure
- Combined message and recipient data in single records
- API-based data collection rather than file processing
- Organization-based multi-tenancy support

Data retention and archiving

The Promodag StoreLog database is designed to store historical message tracking data for compliance and analysis purposes. Consider implementing appropriate data retention policies based on your organization's requirements:

- **Short-term storage:** Recent data (last 30-90 days) for operational queries
- **Long-term archival:** Historical data for compliance and trend analysis
- **Partitioning strategy:** Consider date-based table partitioning for large datasets
- **Backup considerations:** Regular backups with appropriate retention schedules

Query optimization tips

Common query patterns

- **Date range queries:** Always include date/time filters to leverage indexes
- **Sender/recipient searches:** Use exact matches when possible for better performance
- **Message tracking:** Use Message-Id or Internal-Message-Id for precise lookups
- **Cross-environment queries:** Consider UNION queries when searching both on-premises and cloud data

Performance considerations

- Use appropriate WHERE clauses to limit result sets
- Consider using EXISTS instead of IN for subqueries
- Leverage covering indexes for frequently accessed columns
- Monitor query execution plans for optimization opportunities

3.4.4. SQL Query Library

This section provides a comprehensive collection of SQL queries organized by common use cases.

Remember to modify the variables in red according to your environment, for example @domain.com with your domain name, in the queries below.

Security and threat analysis

Identify potential phishing attempts

Detects messages with common phishing keywords (urgent, verify, suspended) from external domains, helping identify coordinated phishing campaigns.

SELECT [SenderAddress], [Subject], COUNT(*) AS MessageCount
FROM [Events_365]
WHERE ([Subject] LIKE '%urgent%' OR [Subject] LIKE '%verify%' OR [Subject] LIKE '%suspended%')
AND [SenderAddress] NOT LIKE '%@yourdomain.com'
GROUP BY [SenderAddress], [Subject]
HAVING COUNT(*) > 1
ORDER BY MessageCount DESC

Detect potential data exfiltration patterns

Identifies internal users sending unusually large volumes of data to external recipients, which may indicate unauthorized data transfers or compromised accounts.

SELECT [SenderAddress],
COUNT(*) AS MessageCount,
AVG(CAST([Size] AS BIGINT)) AS AvgMessageSize,
SUM(CAST([Size] AS BIGINT)) AS TotalDataSent,
MIN([Received]) AS FirstMessage,
MAX([Received]) AS LastMessage
FROM [Events_365]
WHERE [SenderAddress] LIKE '%@yourdomain.com'
AND [RecipientAddress] NOT LIKE '%@yourdomain.com'
AND [Size] > 5242880 -- Messages larger than 5MB
AND [Received] >= DATEADD(day, -7, GETDATE())
GROUP BY [SenderAddress]
HAVING COUNT(*) > 10 AND SUM(CAST([Size] AS BIGINT)) > 104857600 -- Total > 100MB
ORDER BY TotalDataSent DESC

Find messages from recently created domains (suspicious pattern)

Discovers domains that have sent multiple messages within a short timeframe, often indicating spam campaigns or malicious activity from newly registered domains.

SELECT RIGHT([SenderAddress], LEN([SenderAddress]) - CHARINDEX('@', [SenderAddress])) AS Domain,
COUNT(*) AS MessageCount,

```
MIN([Received]) AS FirstSeen,
MAX([Received]) AS LastSeen
FROM [Events_365]
WHERE [SenderAddress] LIKE '%@%'
GROUP BY RIGHT([SenderAddress], LEN([SenderAddress]) - CHARINDEX('@', [SenderAddress]))
HAVING COUNT(*) > 10 AND DATEDIFF(day, MIN([Received]), MAX([Received])) < 7
ORDER BY MessageCount DESC
```

Email flow and performance analysis

Analyze email volume by domain

Provides a breakdown of message volume by sender domain, useful for identifying top communication partners and potential spam sources.

```
SELECT RIGHT([SenderAddress], LEN([SenderAddress]) - CHARINDEX('@', [SenderAddress])) AS Domain,
COUNT(*) AS MessageCount
FROM [Events_365]
WHERE [SenderAddress] LIKE '%@%'
GROUP BY RIGHT([SenderAddress], LEN([SenderAddress]) - CHARINDEX('@', [SenderAddress]))
ORDER BY MessageCount DESC
```

Analyze email traffic by hour of day

Shows email activity patterns throughout the day, helping optimize mail flow policies and identify unusual activity outside business hours.

```
SELECT DATEPART(hour, [Received]) AS HourOfDay,
COUNT(*) AS MessageCount
FROM [Events_365]
WHERE [Received] >= DATEADD(day, -7, GETDATE())
GROUP BY DATEPART(hour, [Received])
ORDER BY HourOfDay
```

Find top internal email senders

Lists the most active internal users by message count, useful for capacity planning and identifying users who may need additional training or monitoring.

```
SELECT [SenderAddress], COUNT(*) AS MessageCount
FROM [Events_365]
WHERE [SenderAddress] LIKE '%@yourdomain.com'
AND [RecipientAddress] LIKE '%@yourdomain.com'
AND [Received] >= DATEADD(day, -30, GETDATE())
GROUP BY [SenderAddress]
ORDER BY MessageCount DESC
```

Compliance and auditing

Find messages from a specific sender

29

Retrieves all messages from a particular email address, essential for investigations and compliance requests.

```
SELECT [Received], [SenderAddress], [RecipientAddress], [DecodedSubject]FROM [Events_365]
WHERE [SenderAddress] = 'user@domain.com'
ORDER BY [Received] DESC
```

Find all emails for a specific user (litigation hold)

Locates all messages where a user appears as either sender or recipient, critical for legal discovery and litigation hold requirements.

```
SELECT [Received], [SenderAddress], [RecipientAddress], [Subject], [MessageId]
FROM [Events_365]
WHERE [SenderAddress] = 'user@yourdomain.com' OR [RecipientAddress] = 'user@yourdomain.com'
ORDER BY [Received] DESC
```

Find large emails that might impact storage

Identifies messages exceeding size thresholds to help manage storage capacity and enforce email policies.

```
SELECT [SenderAddress], [RecipientAddress], [Subject], [Size], [Received]
FROM [Events_365]
WHERE [Size] > 10485760 -- 10MB
ORDER BY [Size] DESC
```

Hybrid environment queries

Compare on-premises vs cloud email volume

Provides a side-by-side comparison of message volumes between on-premises Exchange and Exchange Online environments, useful for migration planning and hybrid environment monitoring.

```
-- On-premises volume

SELECT 'On-Premises' AS Environment, COUNT(*) AS MessageCount
FROM [Events_2007-2019]
WHERE [Date-Time] >= DATEADD(day, -30, GETDATE())
UNION ALL
-- Cloud volume
SELECT 'Exchange Online' AS Environment, COUNT(*) AS MessageCount
FROM [Events_365]
WHERE [Received] >= DATEADD(day, -30, GETDATE())
```

This SQL query library provides essential tools for managing, analyzing, and securing your email environment using Promodag StoreLog data. These queries can be customized and combined to meet specific organizational needs, whether for security investigations, compliance reporting, or operational analysis.

Remember to:

- Always test queries on a subset of data first
- Use appropriate date ranges to optimize performance
- Consider creating views for frequently used queries
- Implement proper access controls when sharing query results
- For more advanced reporting capabilities, consider using Promodag Reports, which provides pre-built reports and visualizations for Exchange environments.

3.5 Next Steps

3.5.1. Immediate Actions

- **Verify automation** is running correctly (check scheduled tasks).
- **Test a few queries** from our "SQL Query Library", on page 28 to familiarize yourself.
- **Document your setup** for future reference and team members.

3.5.2. Ongoing Maintenance

- **Monitor disk space** as your database will grow over time. SQL Server Express LocalDB data-bases are limited to 10 GB.
- **Review certificate expiration dates** (renewed every 2 years).
- **Backup your database** regularly for disaster recovery.

3.5.3. Getting Help

- **Technical questions**: Refer to the complete help file (Help menu in StoreLog).
- **Advanced reporting**: Consider upgrading to Promodag Reports.
- **Community support**: While we don't provide direct support for this free tool, user feedback helps us improve future versions.

About Promodag

Email address	info@promodag.com
Postal address	8, rue Charles-Pathé 94300 VINCENNES France
Phone	+33 1 45 73 49 95 US Toll Free: +1 (844) 311-5003
Web site	https://www.promodag.com/

Note: This product has been released as freeware. We do not offer any support on Promodag StoreLog. However, we always welcome your suggestions and feedback. It will help us make it better in the future.

Index