Ultimate Migrator Overview

Designed by Engineers for Engineers

The software has been built to automate the complete migration process from start to finish. No scripting required, with intelligent error handling and comprehensive reporting. This avoids the need to restart a migration from the beginning and so avoids duplicates. Software written from the Project Engineers perspective.

The architecture is designed to operate in a distributed environment. To achieve this, the application has been split into a number of key components, the **Central Application** and **Remote Agents**.

Central Application

A central administration console allows for the scheduling and management of the complete migration only - no messaging data is ever stored on the server or in its database. For enhanced security, the console can be set to require authentication and provide optional roles-based administration.

The *Central Application* is comprised of a number of distinct technologies:

- **Web Application** - presents the screens that permit the end-user to manage the application and initiate the discovery and ingestion functions. It can be installed on an existing archive server, but also be deployed onto a shared IIS or dedicated Windows server instance. The *Web Application* is linked to the *Remote Agents* by various web-services.

- **Scheduler Service** - A Windows service that hosts several scheduled tasks and is installed at the same time as the *Web Application*. Processes contained within this service allow functions such as regular status messages to be sent and data synchronisation to be performed.

- **Database** - The database contains the remote file list and history, as well as configuration settings that control how Ultimate Migrator operates

Remote Agents

The *Remote Agent* is a Windows service that can be deployed manually or automatically via, for example, Microsoft SCCM. One or more *Remote Agents* are installed into the Enterprise network which are configured to perform a selection of distinct roles using the *Central Application* console.

Remote Agents perform the heavy lifting by moving messages directly from the source to the destination in a single action. The messages are only ever held in memory before being saved to the destination and are never stored in intermediary locations temporarily. Security is at the heart of the software design.

- **Discovery** - Network bandwidth and infrastructure limitations are considered when deploying the *Remote Agents* for discovery purposes. The discovery process trawls the file system to identify PST files or interrogate source databases depending on the migration requirement.
  Where the *Remote Agent* cannot be installed onto the target server, it can be deployed onto a nearby server and configured for remote scanning.

- **Ingestion** – To optimise throughput and commence ingestion, one *Remote Agent* is installed directly onto each target archive server. Where that approach is not desirable or possible, then one dedicated machine per archive server can be utilised instead.
  Each *Remote Agent* server connects directly to the PST file location or source archive in order to retrieve and process the target items.

Security & Chain of Custody Considerations

Security of the data while en-route to its new destination is a key consideration of the software design. As such, the software has been entrusted to move messaging data between archive solutions on-premise and cloud-based, for governments, major banks and other heavily regulated industries around the world where compliance, security and chain of custody is paramount.

- The software is installed directly into the client infrastructure. There are no external or cloud based components so by default, no data ever leaves the boundaries of the client network.
- More often than not, client data centres are already heavily protected by firewall security, adding an additional layer of security.
- By sitting at a layer above the message we do not come into direct contact with the data and can thus guarantee that the data is passed between the source code and destination code in an unaltered state.
- With Enterprise Vault for example, the original archiving process adds a number of hidden attributes to the message that allows it to be tracked while still within the EV environment. When the message is copied to Exchange/Office 365, these identifiers are retained, so permitting continued tracking of the message post migration. Furthermore, all important pieces of information including the date originally sent, receive dates, senders, recipients, content and attachments remain unaltered, ensuring auditable compliance.
- Automation of the complete process from start to finish removes the risk of data tampering.
- Issues during the extraction are logged at the proprietary archive id level eg “savesetid” for EV; this provides the necessary information for auditing purposes.

All in all, the design of the software ensures that the migration process is straightforward, while ticking the compliance boxes at the same time.

Ultimate Migrator Connects to...

Source Files & Archives

- .PST files
- Journals
- Public Folders (Exchange, EV)
- Shortcuts
  (Exchange, File System, Public Folders)
- MSG, EML
  (File System, Zip Files, Encrypted Messages)
- MS Exchange
- O365
- Enterprise Vault
- EV.cloud
- Quest Archive Manager (QAM)
- EMC Source One
- HP (Autonomy, Zantas) EAS
- Global Relay
- Spam Experts
- Lotus Notes/Domino

Destination Platforms & Archives

- O365
  (Mailbox, Public Folder, Sharepoint, Teams, Groups)
- .PST
- File System
- Document Storage System
- FTPS supported systems
- Mimecast
- EV.cloud
- Cryoserver
- Solar Archive