CA.Mail to Office 365 Migration Process

Contents

Revision History

1 Introduction
  1.1 Terminology
  1.2 Migration Process Overview

2 Migration Requirements
  2.1 Identity Components
    2.1.1 Azure Active Directory Connect (AADConnect)
    2.1.2 Active Directory Federation Services (ADFS)
    2.1.3 Web Application Proxy Server (WAP) for ADFS
    2.1.4 Microsoft Exchange Server
  2.2 Identity Pre-requisites
    2.2.1 Identity Package
    2.2.2 Identity Remediation
    2.2.3 Attribute Merge
    2.2.4 Shared & Resource Mailboxes
    2.2.5 Distribution Groups
    2.2.6 State-Wide Global Address List (GAL)
    2.2.7 Migration Endpoint

2 Tenant-Specific Configurations
  2.1 Exchange Online Settings
    2.2.1 Mail-Flow
    2.2.2 Exchange Online Protection (EOP)
    2.2.3 Retention Policies
    2.2.4 Mobile Device Policies
    2.2.5 Public Folders

3 Appendix
  3.1 Roles and Responsibilities
## Revision History

<table>
<thead>
<tr>
<th>Author</th>
<th>Summary of changes</th>
<th>Date</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kyle Green</td>
<td>Initial Draft</td>
<td>10/4/16</td>
<td>0.1</td>
</tr>
<tr>
<td>Kyle Green</td>
<td>Second Draft</td>
<td>10/18/16</td>
<td>0.2</td>
</tr>
<tr>
<td>Clayton P. Cobb</td>
<td>Direct edits to new items</td>
<td>10/19/16</td>
<td>0.3</td>
</tr>
<tr>
<td>Clayton P. Cobb</td>
<td>Additional edits and Vendor text</td>
<td>10/20/16</td>
<td>0.4</td>
</tr>
<tr>
<td>Mark Eubanks</td>
<td>Additional edits</td>
<td>1/14/17</td>
<td>1.0</td>
</tr>
</tbody>
</table>
1 Introduction

The purpose of this document is to provide California state agencies, bureaus, commissions, departments, and offices (Customer) guidance on the migration of email services from CA.Mail to Office 365 Government Exchange Online. Certain steps within the process will be consistent across all Customers. However, many variances will occur in overall migration strategies, tenant-specific configurations, and Customer-specific prerequisites for migration readiness. It is mandatory that Customers work with a qualified and experienced Microsoft Cloud Partner to assist, educate, and plan for migration. Qualified partners must possess official Microsoft Competencies:

- Cloud Platform
- Cloud Productivity
- Enterprise Mobility Management

1.1 Terminology

**Customer:** Department, agency, bureau, commission, office, or other State of California entity that currently has email services and mailboxes provided under CA.Mail

**Vendor:** Qualified Microsoft Partner with the explicit competencies, skills, and experience to perform the necessary migration preparation and execution activities. Qualifications can be validated by CDT or Microsoft

**CA.Mail:** The current service hosting Customer email services

**Office 365 Government (O365):** This is the service Customers are migrating to

**Tenant:** Customer-specific, dedicated O365 environment

**Identity Components:** Server and application pre-requisites for advanced user management, authentication, state compliance policies, State-Wide Global Address List (GAL), and synchronizing on-premises Active Directory identities to O365. These components consist of:

1. On-Premises Active Directory
2. Azure Active Directory Connect (AADConnect) – for Directory Synchronization
   1. SQL Server for the State-Wide GAL
3. Active Directory Federation Services (ADFS)
4. Web Application Proxy Server(s) for ADFS
5. Microsoft Exchange 2016 server(s)

**Tenant-Specific Configurations:** Each Customer will be expected to address unique configurations based on Customer needs. These are typically policy-type settings within Exchange Online (e.g. Retention Policies, ActiveSync Policies, etc.).

1.2 Migration Process Overview

The migration process is comprised of the following high-level steps, which are more detailed in the document below:

1) Customer submits SR to CDT for “Migration Services”
2) CDT exports Customer data referred to as the “Identity Package”
3) Vendor aids Customer with identity pre-requisite tasks
4) Vendor and CDT configure synchronization for the Global Address List (GAL)
5) Vendor and Customer perform all tenant-specific work
6) Customer notifies CDT of migration readiness
7) CDT initiates mailbox migration move requests
8) Vendor completes move requests according to Customer’s schedule

The following high-level flowchart depicts this migration process from beginning to end:
2 Migration Requirements

2.1 Identity Components

Customers are expected to have already deployed the required servers, applications, and services for migration prerequisites, authentication, identity synchronization, and user management. All of these services combined are referred to as Customer's Identity Components. **It is critical that Customers design these components to have high-availability and geo-redundancy.** These components will be responsible for all user authentication to email, other O365 products, and any number of future third-party cloud products federated with Azure Active Directory (Azure AD). Due to the critical nature of these components, the majority of Customers are leveraging Microsoft Azure Government to achieve an optimal service-level agreement (SLA).

An overview of component details is listed below. Customers are expected to adhere to State-mandated security policies to prevent users from accessing email using the Outlook desktop client from outside Customer’s network. ADFS is the official Microsoft solution to achieve this level of access control, and it is the State standard.

2.1.1 Azure Active Directory Connect (AADConnect)

AADConnect is a Microsoft application that resides on a single domain-joined server. Its purpose is to synchronize on-premises Active Directory users, groups, and contacts to Customer’s Azure AD Tenant. This allows users to access O365 and potentially thousands of Software-as-a-Service (SaaS) applications already federated with Azure AD while using the same on-premises credentials.

2.1.2 Active Directory Federation Services (ADFS)

ADFS is a role built-in to Windows Server 2012 R2, and this service provides single sign-on (SSO) capabilities for signing into O365. With ADFS, authentication to O365 is offloaded to Customer’s ADFS infrastructure, which is within Customer’s network. This is done through a relying party trust established between Customer’s ADFS farm and Azure AD.

2.1.3 Web Application Proxy Server (WAP) for ADFS

WAP is a role built-in to Windows Server 2012 R2, and the purpose of this role is to expose ADFS securely to the internet. WAP servers reside on non-domain joined servers; they also play a key role in controlling access from non-Customer networks.

2.1.4 Microsoft Exchange Server

Microsoft Exchange Server 2016 is a migration pre-requisite; this is due to the additional PowerShell cmdlets available for identity pre-work. Additionally, these servers are recommended by Microsoft for O365 customers to use for ongoing user management. The Exchange Admin Center provides administrators a friendlier interface for managing user attributes (e.g. email addresses, display name, etc.), which are then synchronized to O365 via AADConnect. The license for these servers is provided under the O365 licensing terms, but conditions apply. No email traffic or mailboxes may reside on these servers; they are for migration pre-work and user management only.

***Note: Exchange 2013 is also sufficient to meet migration prerequisites and provide the functionality for ongoing user management.***

2.2 Identity Pre-requisites

CA.Mail is built on an account/resource forest model where Customer users and groups reside in the on-premises Active Directory forest while “linked” user objects reside in the CA.Mail forest (RF01). This presents numerous challenges when Customer wants to remove dependencies on CA.Mail to simplify ongoing Active Directory integration with O365.

Before migrating email, Customer must also migrate a number of user attributes, distribution groups, and permissions from CA.Mail to Customer’s Active Directory or directly into O365. The end-state is Customer will only be synchronizing objects from on-premises Active Directory to the new O365 tenant while having no reliance on the CA.Mail directory going forward.

2.2.1 Identity Package

CDT will take responsibility of exporting what is being called the “Identity Package.” This package includes various exports of user attributes, distribution groups, distribution group members, mailbox permissions, mobile device policies, and other pertinent data. Customers and selected Vendors are expected to perform the necessary actions that are dependent on these data exports in the Identity Package.

2.2.2 Identity Remediation

Customers in all O365 migration scenarios are expected to do some level of Active Directory remediation before or after synchronizing identities using AADConnect. There are several tools for identifying issues before synchronization. AADConnect also produces error reports for synchronization failures. It is recommended that this remediation is done before synchronization and that Customer work with a Vendor for guidance.

2.2.3 Attribute Merge
The most prominent prerequisite for migrating email services from CA.Mail is the “Attribute Merge.” This term represents the action of exporting all Exchange user attributes from CA.Mail and ingesting them into Customer’s on-premises Active Directory forest. This is a requirement so that the user objects being synchronizing from Customer’s Active Directory forest to O365 have the required Exchange attributes that coincide with the CA.Mail mailbox. For instance, the “ExchangeGUID” is a unique identifier that ties a user account and a mailbox together. Without performing an Attribute Merge, the mailbox would fail to move due to a missing user account. This process is outlined in the diagram below:

### Attribute Merge Diagram

#### Attributes

The following attributes are required to “stage” user accounts in order to synchronize the required fields to initiate a mailbox migration:

- Name (name)
- DisplayName (displayname)
- SamAccountName (SamAccountName)
- WindowsEmailAddress (mail)
- PrimarySMTPAddress (from ProxyAddresses)
- LegacyExchangeDN (legacyExchangeDN)
- EmailAddresses (proxyaddresses)
- ExchangeGUID (msExchMailboxGUID)
- GrantSendOnBehalfTo (publicDelegates)
- ExternalEmailAddress (TargetAddress)

### AttributeMerge-FromCAMail.PS1

The “AttributeMerge-FromCAMail.PS1” script provided by CDT can be used as a reference for how the “Attribute Merge” process can be accomplished. The script is provided as-is without warranty of any kind. The entire risk arising out of the use or performance of the sample and documentation remains with Customer. In no event shall CDT or its authors be liable for any...
2.2.4 Shared & Resource Mailboxes

Similar to the attribute merge mentioned above, Shared and Resource mailboxes represent another unique scenario that requires some level of Active Directory work. Due to Customers having the ability to create Shared and Resource mailboxes directly through ECAT without needing an on-premises user account, there is no way to migrate the mailbox to O365 without a synchronized account from Customer’s Active Directory forest. This dictates the requirement that Customer must create Active Directory account objects in Customer’s Active Directory forest to represent those mailboxes. An attribute merge must be performed for these new accounts after initial creation. This process is outlined in the diagram below:

Shared & Resource Mailbox Account Diagram

Create-o365SharedMailboxObject.ps1

The “Create-o365SharedMailboxObject.ps1” script provided by CDT can be used as a reference for how the Shared & Resource mailbox account creation process can be accomplished. The script is provided as-is without warranty of any kind. The entire risk arising out of the use or performance of the sample and documentation remains with Customer. In no event shall CDT or its authors be liable for any damages whatsoever due to the use of this script. It is merely a sample.

2.2.5 Distribution Groups

Distribution groups that were created in CA.Mail through ECAT need to be migrated to Customer’s Active Directory forest or directly into O365/Azure AD. The timing of this migration is critical and has dependencies on other tasks including the synchronization of the State-Wide GAL. There are also pros and cons between these distribution groups residing in AD versus O365/Azure AD. The most prominent consideration is that if the groups reside in AD and are being synchronized, users cannot manage them through Outlook. A Vendor can elaborate on the pros and cons and address the importance of timing.

Permissions

If a Customer has granted mailbox permissions (e.g. full access, send-as, etc.) using distribution groups that were created...
directly in CA.Mail through ECAT, mitigation must take place to preserve those permissions. Mailbox permissions are built around SIDs attached to users and groups. When migrating a distribution group to O365 by recreating it, a new SID is generated, making the permissions on the mailbox useless. Due to this, the permissions for these distribution groups must be re-applied after mailbox migrations have occurred. CDT will export permissions as part of the “Identity Package.”

Create-O365GroupsFromXMLs.ps1
The “Create-O365GroupsFromXMLs.ps1” script provided by CDT can be used as a reference for how the distribution group creation process can be accomplished. This script does not take permissions into account. The script is provided as-is without warranty of any kind. The entire risk arising out of the use or performance of the sample and documentation remains with Customer. In no event shall CDT or its authors be liable for any damages whatsoever due to the use of this script. It is merely a sample.

2.2.6 State-Wide Global Address List (GAL)
CDT has developed a new solution built in Microsoft Azure Government to provide Customers with an automated State-Wide GAL solution. This build was required, because the existing GAL goes away whenever a Customer moves out of CA.Mail or California Email Services (CES). This new solution uses an advanced configuration of the AADConnect application to synchronize contacts into Customer’s O365 tenants from all other State Customers. Technically, these contacts are required in order for migrated users to reply to old emails after migration, and they may also be a prerequisite for migrating distribution groups should those groups contain members from other State Customers.

2.2.7 Migration Endpoint
Within Exchange Online (EXO), a migration endpoint that can resolve the CA.Mail endpoint must be created. The credentials and URL needed to do this will be communicated to Customer by CDT during the migration project.
2 Tenant-Specific Configurations

In addition to the requirements to migrate mailboxes from CA.Mail to O365, Customer will have technical prerequisites that extend beyond what is documented above. These configurations are unique to each Customer and should be facilitated through a Vendor; below are some examples (non-exhaustive list).

2.1 Exchange Online Settings

2.2.1 Mail-Flow
Customer needs to carefully plan out how mail-flow will work during pilot migrations and after production migrations. Not every Customer will be the same, but the mail-flow must include the creation of Send and Receive connectors in Exchange Online.

CDT Example: CDT set up Send and Receive connectors for mail-flow to continue working between CA.Mail and pilot users in O365. At the time of the production migration “cutover,” which occurred in one iteration, CDT redirected mail-flow from being delivered to CA.Mail directly to Exchange Online.

2.2.1 Exchange Online Protection (EOP)
EOP is the anti-spam and anti-malware service included in Exchange Online. If a Customer is planning on routing mail-flow through EOP, it is highly-recommended to work with a Vendor to configure the product before routing mail-flow. These are the settings that will dictate what mail gets blocked or marked as spam or “junk.”

Customer will also want to configure whether spam-marked email is delivered to the user’s “Junk” mail folder or sent to a hosted quarantine for email administrators to manage.

2.2.2 Retention Policies
Retention policies in Exchange Online must be configured. By default, all mail will be kept, and mail older than two (2) years will be sent to the user’s Online Archive (if created). CDT will export what Customer is currently using and provide it as part of the “Identity Package.”

2.2.3 Mobile Device Policies
Mobile device policies can be configured in Exchange Online or through Intune, which is part of the Microsoft Enterprise Mobility Suite (EMS). Customer may also be using a third-party mobile device management (MDM) solution, in which case there may be a need to integrate with O365. CDT will export data regarding mobile devices as part of the “Identity Package.”

2.2.4 Public Folders
Customers who use public folders should work with a Vendor to develop a preservation strategy. This may entail migration of public folder data and processes into other solutions (e.g. Shared Mailboxes, O365 Groups, etc.) or to modern public folders in Exchange Online. There is no official public folder migration method. The responsibility lies on Customer and Vendor to develop the plan and communicate the plan to CDT, if applicable.
### 3.1 Roles and Responsibilities

The following chart expands on the diagram in section 1.2:

<table>
<thead>
<tr>
<th>CDT</th>
<th>Department/Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Export “Identity Package”, consists of:</strong></td>
<td><strong>User Mail Attributes</strong></td>
</tr>
<tr>
<td>- Exchange User Attributes from CA.Mail</td>
<td>Ingest Exchange User Attributes from CA.Mail (attribute merge) to department’s AD forest, verify number and validity of Mail Enabled Users (MEUs)</td>
</tr>
<tr>
<td>- List of Shared/Resource Mailboxes (to create users in Customer’s forest)</td>
<td>- Add the “*.onmicrosoft.com” proxyaddress to every mailbox, can use the on-premises hybrid servers and an address policy</td>
</tr>
<tr>
<td>- Distribution Groups, Members, &amp; Owners</td>
<td></td>
</tr>
<tr>
<td>- Mailbox permissions for DGs &amp; Mailboxes</td>
<td></td>
</tr>
<tr>
<td>- List of Public Folders</td>
<td></td>
</tr>
<tr>
<td>- List of mobile devices</td>
<td></td>
</tr>
<tr>
<td><strong>Shared/Resource Accounts</strong></td>
<td><strong>Group Permissions</strong></td>
</tr>
<tr>
<td>Create user accounts in department’s AD forest to represent the shared/resource mailboxes in RF01</td>
<td>Mail-Enable all security groups used for mailbox permissions in department’s AD forest</td>
</tr>
<tr>
<td><strong>State-Wide GAL</strong></td>
<td><strong>Configure Exchange Online settings:</strong></td>
</tr>
<tr>
<td>Synchronize the State-Wide GAL, and all of department’s mail enabled users and groups</td>
<td>- MRM policies</td>
</tr>
<tr>
<td></td>
<td>- Compliance</td>
</tr>
<tr>
<td></td>
<td>- Mobile Device settings (ActiveSync)</td>
</tr>
<tr>
<td></td>
<td>- Mail-Flow Send &amp; Receive Connectors</td>
</tr>
<tr>
<td></td>
<td>- Migration Endpoint</td>
</tr>
<tr>
<td></td>
<td>- Etc.</td>
</tr>
<tr>
<td><strong>Configure Exchange Online Protection (EOP)</strong></td>
<td><strong>Define Migration Groups</strong></td>
</tr>
<tr>
<td>- Anti-Spam &amp; Anti-Malware settings</td>
<td>Compile CSV files for migration iterations (POC,</td>
</tr>
<tr>
<td>- Email Encryption (IRM)</td>
<td></td>
</tr>
<tr>
<td>- Transport Rules</td>
<td></td>
</tr>
<tr>
<td>- Etc.</td>
<td></td>
</tr>
<tr>
<td>Pilot, Production</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Create migration batches, create new move requests</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Monitor Move Requests</strong></td>
<td></td>
</tr>
<tr>
<td>Monitor health of move requests, remediate errors, complete or suspend move requests</td>
<td></td>
</tr>
<tr>
<td><strong>Perform post-migration O365 tasks:</strong></td>
<td></td>
</tr>
<tr>
<td>- License users</td>
<td></td>
</tr>
<tr>
<td>- Reapply permissions if needed</td>
<td></td>
</tr>
<tr>
<td>- Adjust mail-flow (MX Records?)</td>
<td></td>
</tr>
<tr>
<td>- Autodiscover</td>
<td></td>
</tr>
<tr>
<td>- Submit stragglers to CDT for follow-up migrations for missed mailboxes</td>
<td></td>
</tr>
</tbody>
</table>

End