Priasoft – Migration Suite Setup

Background

The Priasoft Migration Suite for Exchange is a powerful and easy solution for Exchange-to-Exchange and Exchange-to-Office365 migrations. One of the first tasks prior to migration is the deployment and setup of one or more migration hosts. This document serves to provide concise instructions for successful setup of the software.

The PMSE uses several different protocols to communicate with your source and target environments, as follows:

- LDAP
  - Depending on options, the tools will attempt to read, write, and create objects in the source and target domains
  - Understanding permissions is critical to success and is nearly 90% of our support cases
- MAPI
  - This is an RPC based protocol. It is recommended to read about RPC here:
- Remote PowerShell
  - This uses WinRM which is pre-installed on Windows 7 and 2008 Server
- HTTP and HTTPS
  - WinRM uses this as well as the Priasoft tools. Our tools report anonymous statistics, migration errors, and licensing details to our Azure based backend. You can opt-out of this, but is generally discouraged.
- Windows Networking (UNC files paths, RPC, etc.)

The migration host needs to be able to communicate using these protocols without hindrance. Any blocks in these protocols will likely cause migration failures.

Requirements & Recommendations

There are several requirements and recommendations to consider to successfully migrate mailboxes using the PMSE.

Host Requirements

Hardware Minimum

Priasoft recommends configuring a machine with at least 4 GB of RAM and 4 CPUs (cores or processors) and a modern hard disk with at least 40 GB of free space. Although the software technically can run with less, it will likely increase the overall time to migrate.

The migration software is not disk intensive, but does use local disk for temporary storage during the migration. For performance considerations, an increase in RAM and CPU count always yields good results.

Physical vs. Virtual machines

Priasoft does not have a requirement for physical or virtual machines. Many customers successfully migrate on virtual machines. However, for cases where the speed of the migration is important, physical machines will out-perform a VM.

Note that if you do choose to use a VM, the following guidelines should be followed:

- Dedicate the network adapter in the VM to a physical network adapter, if possible; otherwise provide some level of isolation such that the VM's adapter will have 100% access to the physical layer.
- Dedicate matching physical RAM to the VM. Some VM solutions allow an 'on demand' memory model in which physical RAM is reallocated based on need. This hinders performance of the migration software inside the VM.
- Configure the VM with closely matched physical CPU to virtual CPU assignments and set the migration VM to have 100% utilization of the physical CPU(s).
    - Note that if you are concerned about performance, you will be better off making a physical machine with fewer CPUs than a VM with many.
    - In current VM solutions, a multi-processor VM doesn't have a concept of a 'multi-core' CPU. A VM configured with 4 CPUs is emulating a physical machine with 4 distinct CPUs (versus modern single CPUs with 4 cores). This means that if the physical architecture is 2 2-core CPUs, all 4 virtual CPUs will run on ONE of the 2 physical CPUs.
    - VM configuration is proving to be as much of an art as a technology and depends on the use and purpose of the VM. Default settings are often less than ideal for a migration host
- Do not duplicate a VM after you have installed licenses on the host.

In either case (physical/virtual), increasing RAM and CPU count allows for more mailboxes to migrate simultaneously. Higher migration concurrency equates to a shorter the overall duration of the migration.

Operating System and Core Components

The migration host must be Win8.1, Win10, Win11, Server2012R2, Server 2016, or Server 2019.

The migration host should have the latest patches and updates from Microsoft prior to installing the software and has the following additional software requirements for all versions of Exchange, including Office365:

- Microsoft .NET Framework 3.5.1 (and latest service packs)
- Microsoft .NET Framework 4.7.2 (or later) (and latest service packs)
- Microsoft Outlook
    - MUST BE 32bit
    - MUST have all current patches and updates applied.
    - Any of these versions can be used as long as Exchange allows: 2010, 2013, 2016, 2019, Office 365
        - Outlook 2010 cannot communicate with Office 365
        - Outlook 2013 will lose Office 365 support in April 2023
        - Outlook 2016 cannot communicate with Exchange 2003
        - Outlook 2019 cannot communicate with Exchange 2007
    - Office 365 migrations (source or target) require Outlook 2013 or later and will use Modern Authentication.
        - Priasoft recommends excluding the accounts used from participating in Multi-Factor Authentication.
    - The Outlook versions above are requirements ***for the migration host only***, not for end-users.

We also recommend downloading the very useful MFCMAPI tool to use when troubleshooting MAPI issues and to gain access to migrated mailboxes without needing to roll back the changes. You can download the tool here: http://mfcmapi.codeplex.com

Domain Membership

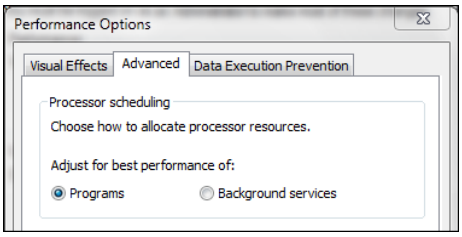
For on-premises destinations, the migration host must be a member of the target domain where the Exchange Servers are located.
For Office 365 destinations, the migration host must be a member of the source domain where the Exchange servers are located.
This is a logical requirement. In most cases it is preferable to have the migration host(s) physically located in the source data-center for performance reasons (there are many operations in the migration that are 'non-data' operations and having those occur local to the source reduces the overall time of the migration).
This is equally true for Office 365 migrations. If migrating from an Office 365 tenant as either cloud-to-ground or cloud-to-cloud, performance will be better if the migration host can be hosted in an Azure Virtual Machine.

Note: If the migration host will physically exist in an IP network that is different than the target you must configure your target environment's AD Sites/Subnets to include this remote network. Many of Microsoft's tools and APIs require proper AD site configurations. A common scenario that exhibits this need is when the source environment is connected to the target by a WAN or VPN. Many times the source environment is separate from the target and does not have IP subnets listed in the target's AD. Review this Microsoft article for more detailed information: Understanding Sites and Subnets (TECHNET)

Recommended Configuration Changes

The migration host should be treated as a dedicated and stand-alone computer specific to the migration. It is better to use the term "appliance" than "server" when referring to the migration host as such classification may make it easier to deploy in tightly controlled environments and change control patterns. Adding other roles, services, or software packages can destabilize the host, interfere with the Priasoft tools, or hinder performance. The following is a list of recommended configuration settings for the host to ensure its consistency throughout the migration.

- Treat each migration host as a purpose-built appliance in your data-center versus a user desktop.
    - However, avoid 'over securing' this machine as such a practice will likely create issues and/or bottlenecks
    - Create the host from a default install of the OS. Avoid using 'standard' images as those often have settings that are counter to performance and usability of the migration.
- Turn off User Account Control (UAC).
- Exclude from Group Policy
    - This is recommended because a computer policy can implement things like firewalls and anti-virus software that can interfere with the migration. Furthermore, group policy objects are often managed without consideration to specific machines with specific purposes. We have seen many cases where migrations execute successfully, but midway through the process, issues occur because of a change to a group policy.
- Disable virus scanners on the migration host
- Disable automatic updates
    - Most commonly, the Microsoft Windows Update service
    - Less commonly, 3rd party updaters
    - Note that even on windows server 2008, windows update is enabled by default
    - You don't want this machine to automatically reboot in the middle of a migration!
- Remove all cached credentials
    - Cached credentials override other credentials you may use and can cause unexpected results.
    - If cached credentials are needed, Priasoft Support will guide you thru the setup and use of such.
    - Cached credentials can be reviewed by running this command from
      Start -> Run: **rundll32.exe keymgr.dll, KRShowKeyMgr**

- Set windows performance to 'Programs' with regards to process scheduling (FYI: Windows Server defaults to 'Background services')
  - 

- Install the Priasoft products on a local drive (versus some network drive).

Networking Recommendations

- Leave IPv6 enabled
  - We have recently seen many customers uncheck the box for IPv6 on their network adapters. Unfortunately, it is not enough to uncheck the box. There is also a registry setting that must be employed and a reboot following such to properly disable IPv6. There is no harm to having IPv6 enabled on the migration host, and for simplicity we recommend leaving it enabled.
- Use a static IP
  - We have seen customers have migration problems due to changes in DHCP scopes which cause the migration computer to receive a new IP address and ultimately place them in a different AD site than before. It's best to avoid this situation by using a static IP.
- Use static DNS Suffixes
  - The migration computer should have static DNS suffixes added for each target and source domain.
  - List the source domain's DNS suffixes first, followed by the target domains. Be sure to include base domains if you have them (e.g. Exchange is in corp.company.com and there is an empty root of company.com; add both with the more specific domains at the top)
- Use static DNS servers
  - Ideally, the DNS servers used should be servers in the target forest that have forwarders to the source forest.
  - If your DNS servers do not have forwarders, you should add the DNS servers for your source forest in your IPv4 configuration
- Enable NetBIOS over TCP
  - MAPI (and some windows functions like SID to Username lookups) still uses RPC and NetBIOS to communicate.
- Disable local firewall software
- Disable (or remove, if possible) any virtual machine network adapters
  - These are usually seen on physical machines that have a VM solution installed locally (like VMware host)
  - If this host is itself a VM, you should only have a single network adapter
- When migrating to or from Office365, use Priasoft Endpoint Testing Tool to validate that GeoDNS is providing the nearest Microsoft endpoint.
  - Not using the nearest Microsoft endpoint will slow down the migration. Network latency (due to distance) is the biggest influencer to migration speed.
  - If the testing tool reports a better endpoint, a CNAME record should be created on the local DNS servers (host files should NOT be used).

Network Name Resolution

Priasoft's solutions (and many of Microsoft's APIs) rely on proper name resolution. The following 3 tests should be run on each migration hos t for each exchange server (CAS/HTS/MBX) and domain controllers in the source and target involved in the migration.

In addition, if the target is Exchange 2010, these tests should be run from each Exchange server as well. This is due to the fact that PowerShell commands are run locally on the Exchange server via Remote PowerShell (aka WinRM). The exchange servers must be able to resolve servers in the source environment.

1. **Nslookup** server_short_name
    a. Success should report the IP address(es) and the FQDN of the server
    b. Short name is important
    c. Failure typically means that DNS suffix is missing for the domain of the server
    d. Failure could also mean improper DNS setup – review DNS server (as seen from ipconfig /all)
2. **NBTSTAT** –a ip.address.returned.from.nslookup
    a. Success should show a NetBIOS name table with a '<00>GROUP' record matching the expected domain
    b. IP address is important to avoid 'cached' lookups
    c. IP address lookup also causes an RPC connectionto theIP which helps validatethatRPC communication is workingpr operly to thatspecific host
    d. Failure here typically means that NetBIOS is not enabled
        I. Not enabled on the migration computer OR
        II. Not enabled on the server – check both
    e. Failure can also mean an issuewith DNS (or WINS if installed and available)
    f. MAPIis an RPC based protocol and relies heavily on NetBIOS resolution
3. **Net view \\server_short_name** (this might fail with 'Access Denied' which is OK; any other error result is a problem).
    a. Success should show 'Shared resources at \\server_short_name' and a listing of shares (if any)
    b. This tests that Net BIOS resolution actually works
    c. This test also helps identify the server type:
        III. DCs will report a NETLOGON share
        IV. Mailbox Servers (NOTCAS/HTS) will show an Address Share
        V. CAS-only/HTS-only servers will show no shares (by default)
    d. Odd or unexpected results here can be indicative of an issue –contact us if you have an unexpected result

Access and Permissions

In order to migrate successfully, specific permissions to resources have to be configured. The Setup Tasks later in this document provide a detailed, step-by-step process for configuring permissions in the source and target environments.

There are 2 main categories of permissions that are covered by the Setup Tasks:

- Mailbox Content
- Active Directory

Mailbox Content Permissions

Access to mailbox content uses the aforementioned MAPI protocol (which is RPC based, even when using Outlook Anywhere). The nature of this type of connection is that authentication to resources (e.g. mailboxes) is based off of the currently logged in user (or matching Cached Credentials). Consider further that by design the migration of a mailbox is done by connecting to the source mailbox AND the target mailbox simultaneously. Priasoft circumvents issues in this pattern with exclusive technology that allows discrete in-line authentication per mailbox. This removes the necessity to have a trust or cached credentials (Windows Credential Manager) for accessing data. The Priasoft tools will prompt for MAPI credentials and will optionally allow for encrypted storage of these credentials for re-use.

Additionally, and differently than Outlook, Priasoft attempts to access a user's mailbox with a flag that requests "Admin Privileges" to the mailbox. In order to open a mailbox with this privilege, one must connect to a mailbox normally first, then "jump" to the requested mailbox with the "Admin" flag. Priasoft's approach to this is to connect to a System Mailbox (see Exchange Special Mailboxes) first, then "jump" to the user's mailbox from there. Every Exchange database has a corresponding System Mailbox. If the System Mailbox is missing, migrations from or to the mailbox's database will not succeed.

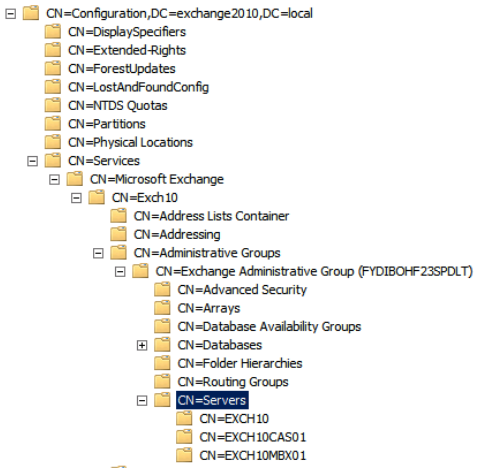
Accessing a mailbox using "Admin Privileges" allows the migration application to access ALL content of a user's mailbox, regardless of any folder-level security a user or other admin may have placed on a folder. This also provides a slight performance improvement over other operations since normal user checks are bypassed.

From a permissions standpoint this means that the account used to authenticate the logon must be able to logon and open System Mailboxes. It is for this reason that you cannot just apply permissions to end user mailboxes but must apply inheriting permissions in the Exchange system. Secondly, the ability to "jump" to another mailbox and request "Admin Privileges" also requires specific permissions.

The permissions that allow this behavior are, respectively, **Receive-As** (for mailbox access) and **Administer Information Store** (for jumping with Admin Privileges).

There are only 4 Active Directory object types in the Microsoft Exchange Configuration Hierarchy for which these 2 permissions can be applied:

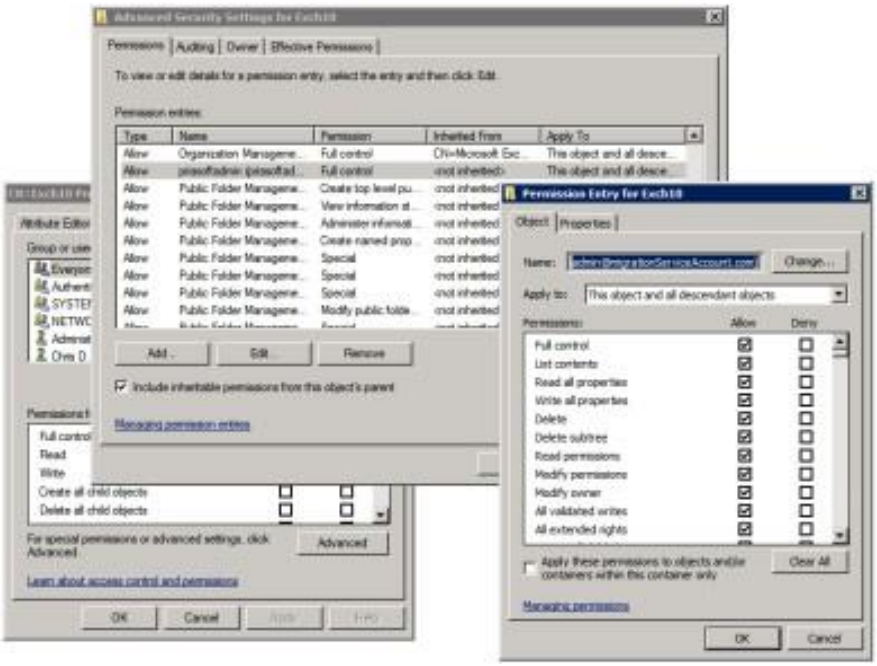
- The Exchange Organization object (LDAP object class: msExchOrganizationContainer)
  - This is the Top-Most object at which you can apply the required permissions.
  - It is recommended to apply permissions here and allow them to inherit to all sub objects so that changes to the environment (new database for instance) will automatically be accessible to the migration applications.
- An Administrative Group (LDAP object class: msExchAdminGroup)
  - Note that as of Exchange 2007, the ability to create multiple administrative groups was removed. There structural elements still exist and there is only a single admin group.
  - You will not see Administrative Groups except from an LDAP editor like ADSIEDIT in exchange 2007 or later
  - This object can inherit permissions from the Organization object.
- An Exchange Server (LDAP object class: msExchExchangeServer)
  - This object can inherit permissions from the Administrative Group or Organization object.
  - Note that Ex2010 and later do not have databases as children of a server. Applying permission at a server level will also require permissions at a database level.
- An Exchange Database (LDAP object class: msExchPrivateMDB)
  - Note that as of Exchange 2010, databases are no longer sub-objects under a server
  - This means that applying permissions at a server level will not inherit to a database and thus cannot be used effectively for permissions.



Typical Exchange 2010 Config Hierarchy

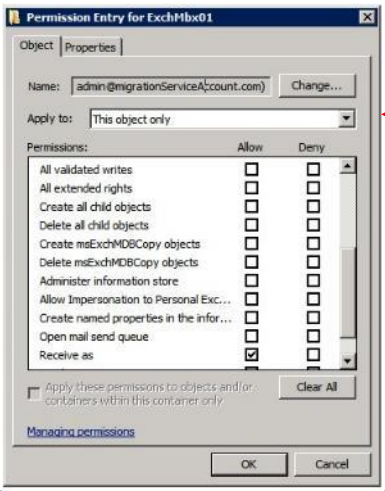
Given these 4 objects types, it should be understood the importance of AD permission inheritance and the effect of such. Priasoft has, over time, encountered environments in which inheritance is blocked at one or more locations in the Exchange object hierarchy (in the Configuration partition of AD). After applying permissions as outlined in the Setup Tasks below, you should validate that the applied permission have indeed inherited to the database(s) to which or from which you will migrate. It is an absolute requirement that the appropriate permissions be evidenced on the databases that will be involved in the migration. If, upon inspection, you find that the migration account is not listed on a database, you may have some level of permission inheritance being blocked by a parent (or parent's parent, etc.) container.

A common mistake that makes it appear as if there is blocked inheritance is when the specific account is not set to cascade down to sub-objects. Often (depending on the version and service pack of Windows) the default when adding a new account to the security of an object in AD is set to "This object only". After adding an account, you should review the account's inheritance from the "Advanced" options in the standard windows security dialog and ensure that an appropriate setting is chosen that causes the account (and it permissions) to flow down to all sub-objects.

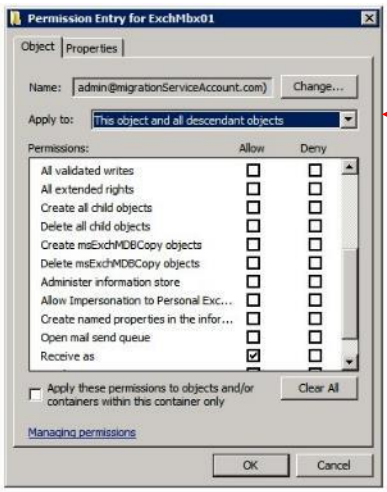


Notice the difference in the "Apply to:" option in the following two dialogs:

Incorrect "Apply To:"



Correct "Apply To:"



In order for the permissions given to admin@migrationServerAccount.com (as referenced in the above dialog) to be applied to the necessary databases (and mailboxes on the database), you must ensure that the correct "Apply to:" setting is used.

Lastly, please avoid setting permissions to the Exchange objects listed above using groups. Although from a technical standpoint such will work, there is increased risk of changes to the group for which you, as a migration admin or architect, may not receive notification or the chance to evaluate the impact. It is very important to note the fact that it only takes a single DENY permission on a group to cause migration problems; in Active Directory, DENY permissions override allow permissions, even if you explicitly assign an allow permission on an object. Furthermore, the DENY is true for ANY GROUP you are a member of, whether directly or indirectly (remember that groups can be members of other groups and so on).

Active Directory Permissions

In addition to mailbox content, Priasoft also handles the appropriate aspects for which Active Directory play a role. For instance, an AD user object has many properties that identify the mailbox database to which the user is associated and holds all the user's email addresses (including the primary SMTP address). The migrator will collect certain properties from the source AD user object and merge or copy them to the target AD user object. These operations provide the highest level of post-migration transparency to your end users.

Additionally, the migrator will make changes to objects in the source directory in order to remove that mailbox from use; this prevents a user from making changes to the mailbox after it's been migrated and prevents other from sending mail to the old mailbox. Also, based on an option, the migrator can create a forwarding object in the source directory to provide a consistent Address Book to those who have not migrated.

The migrator also needs permission to create a new container named Priasoft in the source and target directory. This container will be located in the Configuration partition of AD at the following path:

Configuration
Services
Microsoft Exchange
[Your Exchange Org Name]
Priasoft

This container provides a Read+Write location in AD for the Priasoft tools. This allows synchronization of configuration information between instances of Priasoft's tools and between instances running on multiple hosts.

As such, these require certain access to the source and target directory. Topically, the migrator and many of the other Priasoft tools require the following ability:

- LDAP Search operations, both against Domain Controllers and Global Catalogs
- Object binding, in order to read or write attributes
- Object creation ○ In the source AD, we may need to create Contacts to forward mail ○ In the target AD, we may need to create a new user account
- Object modification (related to object binding)
- Object deletion
    - In the source AD, during rollback, we attempt to delete the forwarding contact
    - In the target AD, we attempt to purge old Dry-Run objects

If you analyze these abilities, you can quickly see that we need READ, WRITE, CREATE, DELETE, and SEARCH permissions. As such, the easiest and most recognizable way to grant these permissions is by using an account that is a member of the Domain Admins (or Enterprise Admins for multi-domain forests) group. Often, and especially during a merger/acquisition consolidation, the initial reaction to this request is high resistance. The intent of this section of the document is to provide the necessary justification for this level of permission. It should also be noted that although the tools may use an account with high level permissions, none of Priasoft's tools provide a "backdoor" to any dangerous management routines (e.g. you cannot delete a user account using Priasoft's tools). Priasoft fully understands the importance of security and the risks associated with Domain Admin permissions which are why our migration tools do not provide AD or Exchange Management capabilities.

As noted above, under the Mailbox Permissions section, you are welcome to experiment with more granular permissions, but note that Priasoft provides limited support for such and attempting to "over secure" the environment will likely cause project milestones to slip and increase the project length.

Setup

Priasoft has provided a setup wizard to configure service accounts to be used by the migration tools. The setup wizard is a detailed, guided tool that will explain each step and provide confirmation before continuing. The setup wizard is found after installing the Priasoft Migration Suite as a Start Menu shortcut with the name: Priasoft Migration Setup Utility

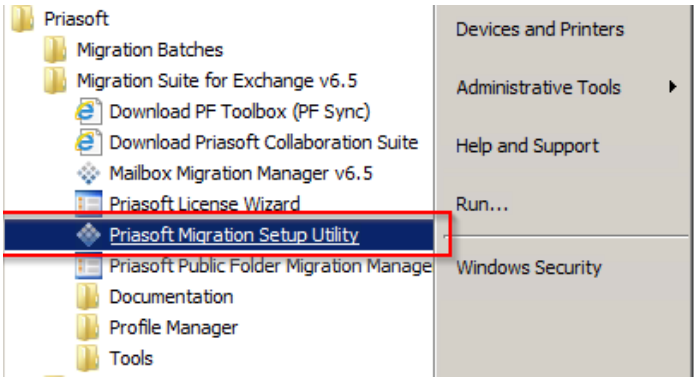
The use of this wizard provide many benefits, both for security protection and compatibility. While it is possible to configure the accounts manually, support is provided when the setup tool is used.

From a security point of view, the setup wizard provide the following advantages over manually built accounts:

- The accounts created are named using Domain specific details and thus could not be guessed by an attacker. This protects the service accounts from being re-used for means other than the intended purpose.
- The accounts are initially created in the built-in "Users" container in AD. The Users container is not an Organization Unit and as such is excluded from GPOs that are built to inherit down through a container structure. This protects the service accounts from accidentally being added or removed from groups, or permissions being adjusted by a GPO in such a way as to interfere with a migration.
- The passwords created are extremely complex and are calculated from Domain specific details, such that only someone already with sufficient access to the domain would even have a chance of determining the password. Furthermore, Priasoft is not able to reverse engineer the password without access to the domain. This level of security ensures that highly privileged service accounts cannot be used for alternate purposes and since no person will or can know the password, is actually more security than a manually built account.
- The setup wizard will request the use of a highly privileged account to be used during the setup, but NO ABILITY to save the credentials of this account is provided. This protects an enterprise by not caching credentials for a known admin account.
- The accounts created by the setup tool are stored in Priasoft encrypted credential store, on the migration host. The Priasoft tools can only use the data after successfully accessing the domain (in order to recalculate the service account password). As such, Priasoft's credential store is highly secure and provides enterprise level protections not seen in other tools:
    - The stored credentials can ONLY be used by Priasoft's tools. Other tools, like AD Users and Computers, Powershell, and scripts cannot use the Priasoft credential store.
    - Priasoft's tools, by design, do not provide any administration functions – neither purposely nor accidentally – and thus the credentials cannot be used in ways not intended. There are no abilities to delete or modify objects thru any dialog or scripting provide by the Priasoft Migration Suite.
    - The stored credentials can be copied from on migration host to another, however because the passwords and usernames of the accounts are domain specific, they cannot be used to access domains from which they were not configured. This removes a security hole found in other tools where a credential used in a test environment or other system is copied and pasted and reused in a production environment.
    - Administrators do NOT lose control over access to the environment. At any time an administrator can disable any if the Priasoft created service accounts to block access.
- The setup wizard, in addition to creating the service accounts required for migration, also sets proper permissions on Exchange databases, throttling policies (where appropriate), and Office 365 Tenants. The goal and purpose of the setup wizard is to ensure that all aspects of environment configuration are completed and validated thereby ensuring that the first execution of a migration does not face permissions or environmental configuration headaches.

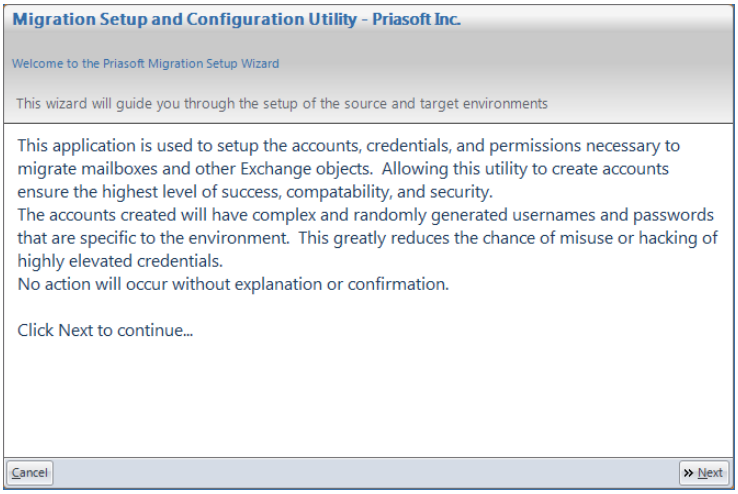
The Setup Wizard

1. Start Menu Item

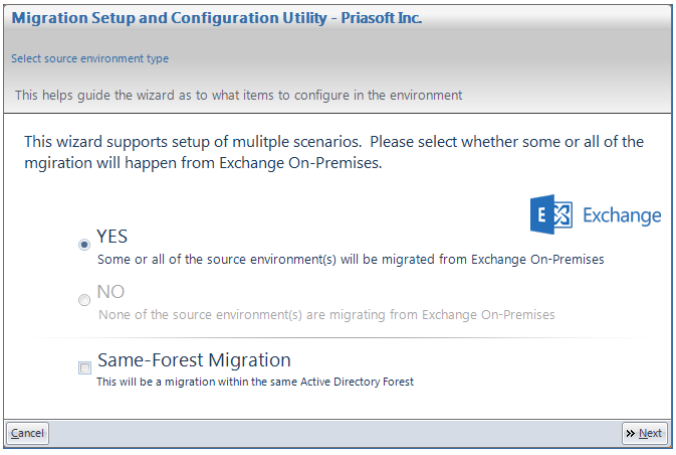


Source Environment Setup

1. Welcome Screen

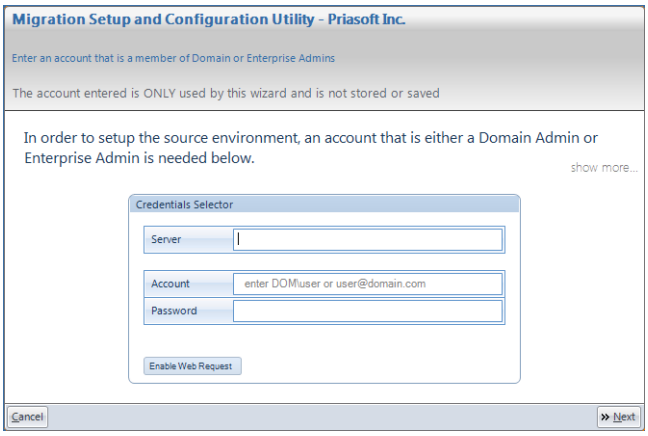


2. Source Version Selection



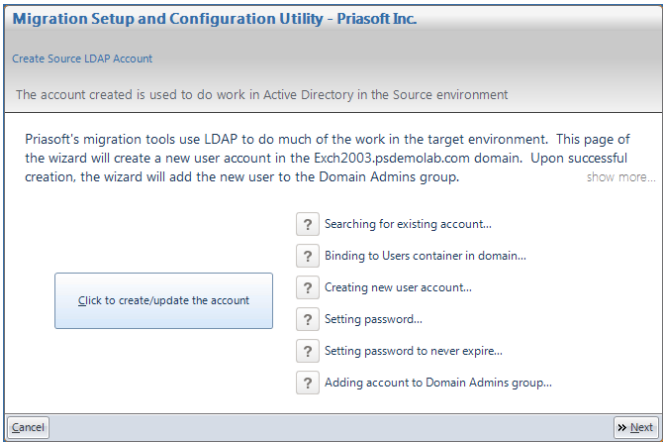
Note that “Same-Forest Migration” will cause the wizard to jump to “Target” configuration details. This is normal since a same-forest migration only has a single Active Directory environment. The services accounts created will be used for both the “source” and “target” in the Priasoft tools.

3. Source Environment Master Credentials



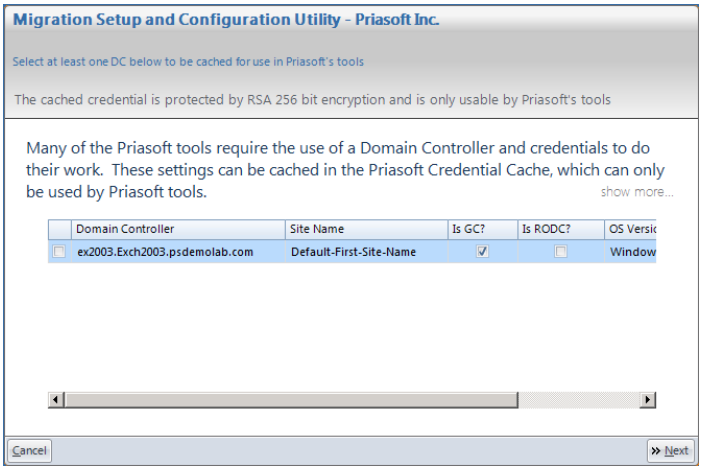
This page requires the use of a highly privileged account (Domain Admin) and is used to create the service accounts and to set the permissions on them. This account is not stored and cannot be saved in the Priasoft tools.
The “Enable Web Request” button will cause a dynamic web server (with a random port) to be created with which a remote administrator can pass the credentials back to the host without having to logon directly to the migration host. The credentials are sent back to the host using RSA 128bit encryption in order to protect the credential. This feature further enhances the security of the system since a key-logger or other tool would be unaware of the data coming in to the application. Once the credential is received, the web service is torn down and unavailable.

4. Create Source LDAP Account



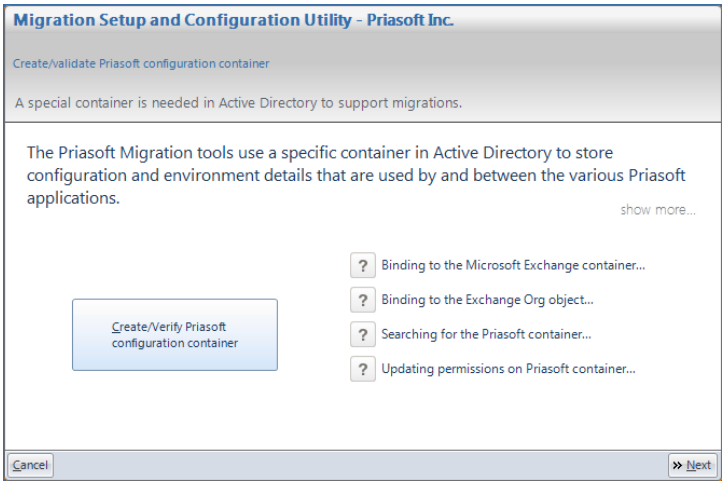
This page will create or update a domain specific account used for accessing and working with Active Directory objects. The account name will start with: PS-LDAP-SA. The characters after the prefix are data specific to the domain.

5. Domain Controller selection



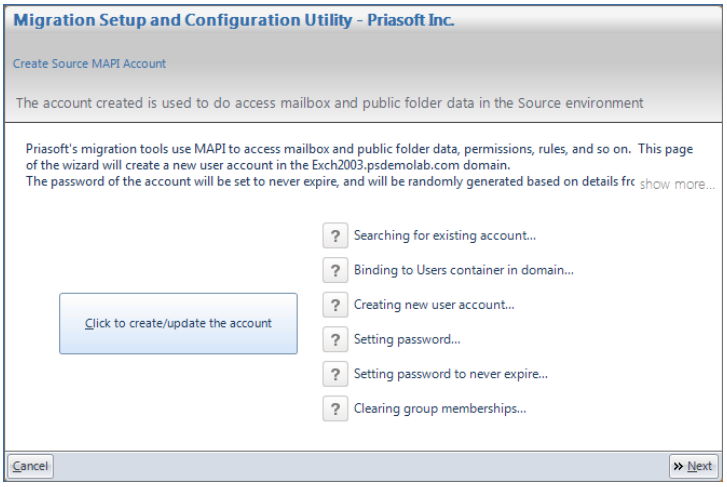
This page allows for the selection of one or more DCs to cache in the Priasoft credential store. When running other Priasoft tools, one can simply browse the credential store for the selected server(s) and select it for use.

6. Priasoft Configuration Container



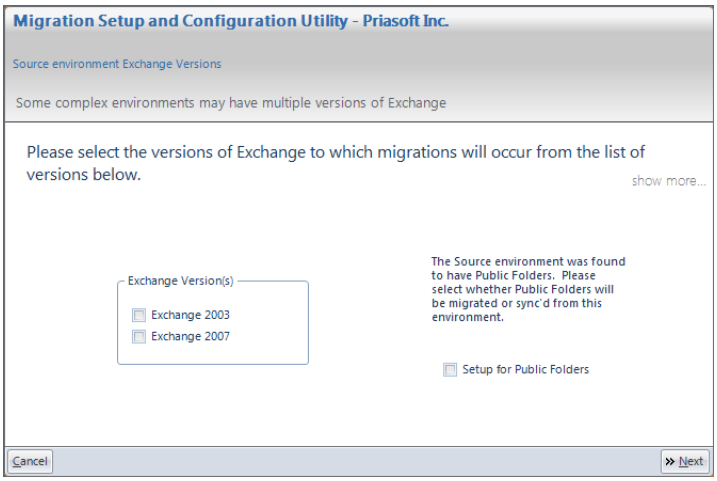
The Priasoft migration suite uses a container named “Priasoft” in AD to store configuration details used by Priasoft tools. The container is stored as a child of the Exchange Org object in the Configuration partition of AD. This is the only container for which the service accounts will have write access – all other objects in the Configuration partition are accessible only with read and search permissions.

7. Source MAPI Account



This page will create the service account used to access mailboxes and public folders in the source environment. The account name will be specific to the domain and its name will start with: PS-MAPI-SA.

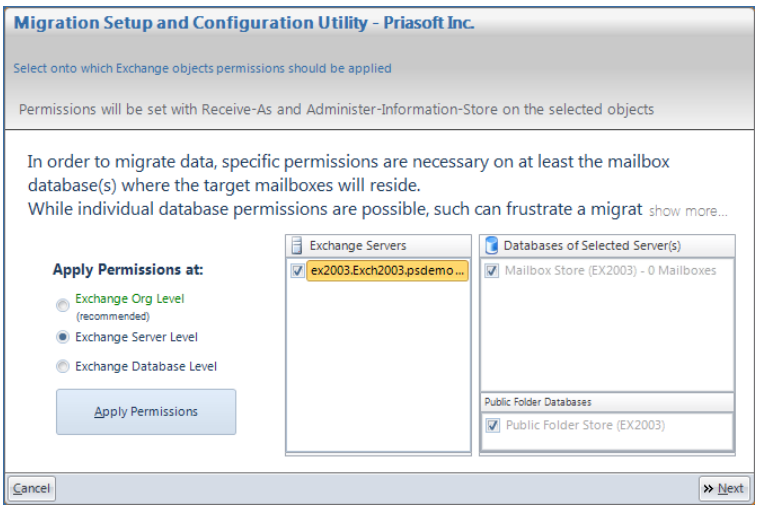
8. Source Exchange Versions



This page shows the versions of Exchange server found in Active Directory. One should select the versions of exchange from which mailboxes will be migrated. Additionally, if there are public folders to be migrated, that option should also be checked. The versions of exchange selected will determine which servers are shown on the next page for setting permissions.

NOTE: If the source version of Exchange selected is Exchange 2010 or higher, a page will be shown to configure throttling policies in the source so that the service accounts created are not limited in performance.

9. Source Exchange Permissions

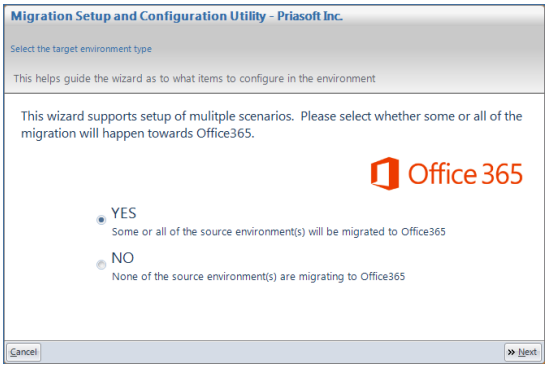


This page is used to configure the specific MAPI/Exchange permissions based on the version(s) selected on the previous page. It is possible to only set permissions on a single database, server, or the entire Exchange Organization. It is HIGHLY recommended to set the permissions at the Organization level so that if new servers or databases are added to the environment after setup, the permissions can automatically inherit from the Org. It is quite common to create a Dry-Run database after setup and if a setting other than Exchange Org Level is used, there may be a need to re-run the setup wizard to apply the permissions to the dry-run database.

Target Environment Setup

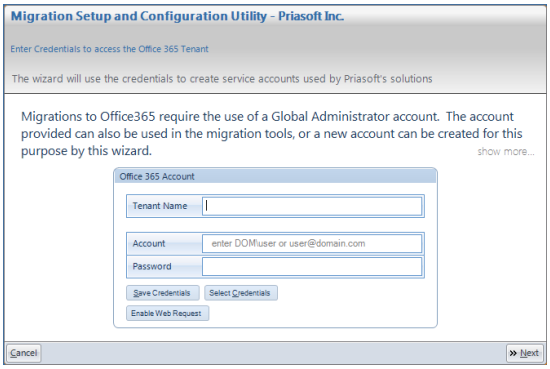
The setup wizard support both Office365 and On-Premises migration patterns, and even support cases where both may occur simultaneously (mergers and acquisitions may drive this pattern more than others).

10. Office365 Target Setup



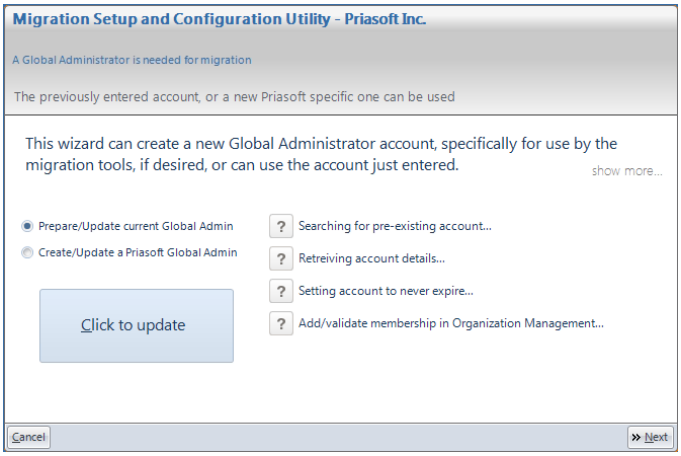
If the migration is not moving to Office365, when Next is click (after selecting “NO”), the wizard will jump to #14 below.

11. Office 365 Tenant Credentials



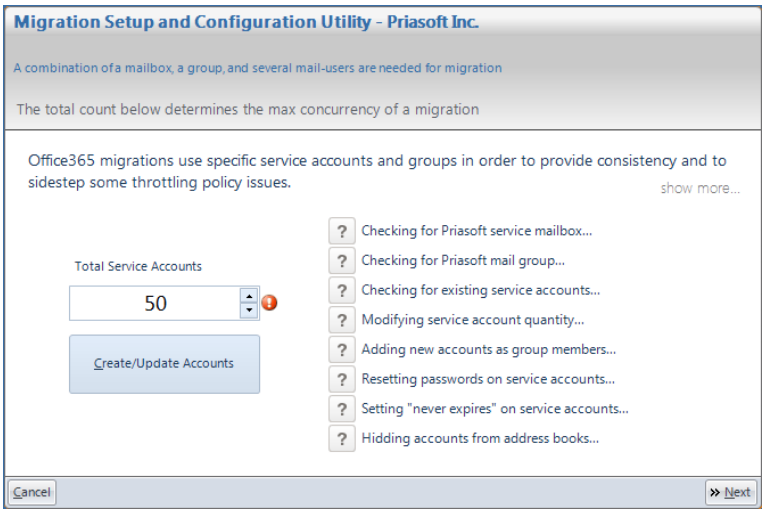
The credentials entered here should be a Global Administrator of the Tenant. The credential can be requested from a remote administrator using the “Enable Web Request” feature and the credentials provide can be saved in the Priasoft credential store. Note that clicking next will setup connections to Office365 and AzureAD via powershell and may take a few minutes to return.

12. Global Admin Selection/Creation



This page allows for the creation/update of a Global Admin account, or allows for the use/preparation of the GA account used in the previous page. In either case, validation of the account's status and assignments into proper roles are performed so that the account can be used for migrations.

13. Office 365 Migration Service Accounts



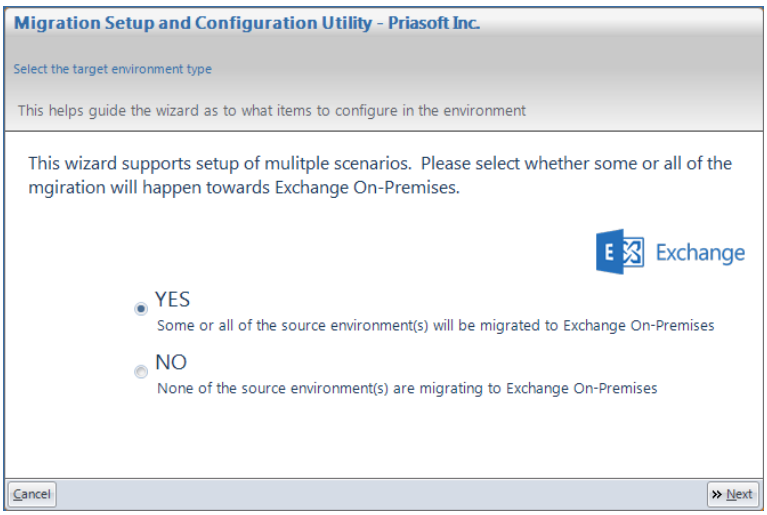
A unique and market leading feature of the Priasoft Migration Suite for Office365 is our ability to circumvent the built-in throttling that exists when attempting to push data to the cloud. This page of the wizard is used to pre-create several service accounts that are used for logging on to the Exchange Online services and accessing Office 365 mailboxes. With this approach, the tools can migrate many dozen mailboxes concurrently without being throttled – this is achieved because the throttling policies are attached to the logon token used to authenticate to a mailbox, not the mailbox itself.

The service accounts created are Mail-Enabled users in Exchange Online (but hidden from the GAL) and have a complex, calculated password for which part of it uses Tenant specific details. These service accounts do NOT consume licenses.

It is recommended to create 50 or more of these accounts early in the migration project because the actual use of them and recognition of existence by Exchange Online is not immediate – it can take many minutes between creation and valid use of the accounts.

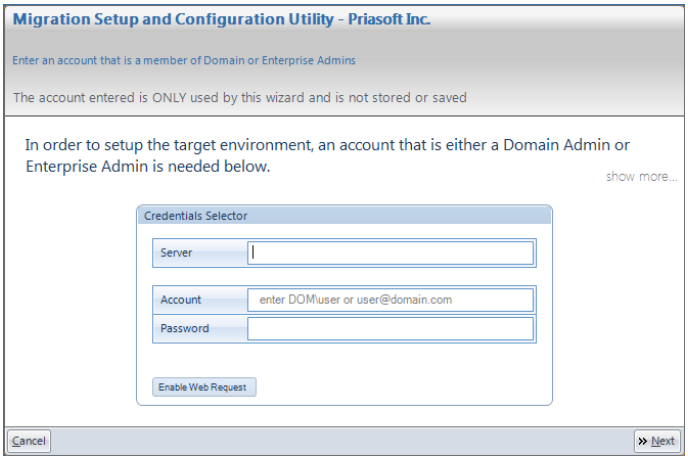
When building a batch for migration, a lower number can be used for concurrency but cannot exceed the number entered here. The number can be adjusted by re-running the setup wizard.

14. On-Premises Target Environment Setup



Note that if Office365 was not selected as a target environment option, the "NO" option on this page will be disabled.

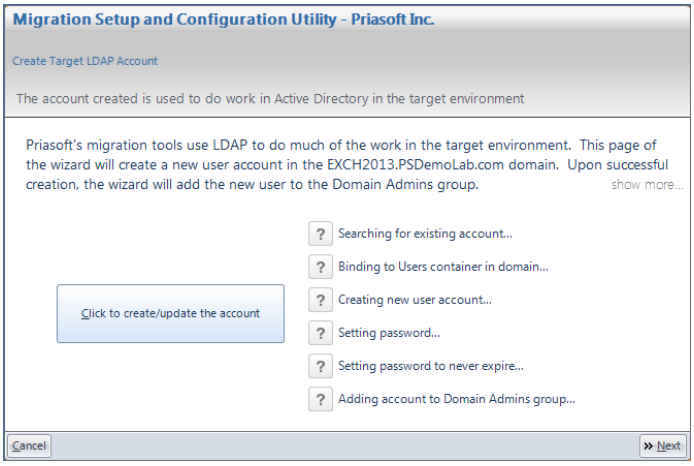
15. Target Environment Credentials



This page requires the use of a highly privileged account (Domain Admin) and is used to create the service accounts and to set the permissions on them. This account is not stored and cannot be saved in the Priasoft tools.

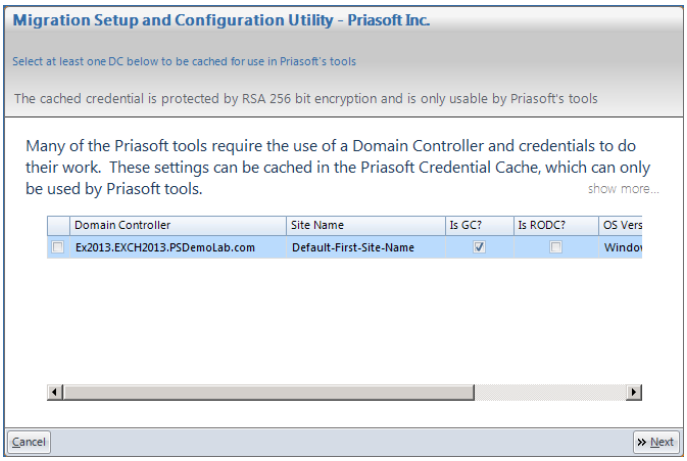
The "Enable Web Request" button will cause a dynamic web server (with a random port) to be created with which a remote administrator can pass the credentials back to the host without having to logon directly to the migration host. The credentials are sent back to the host using RSA 128bit encryption in order to protect the credential. This feature further enhances the security of the system since a key-logger or other tool would be unaware of the data coming in to the application. Once the credential is received, the web service is torn down and unavailable.

16. Create Target LDAP Account



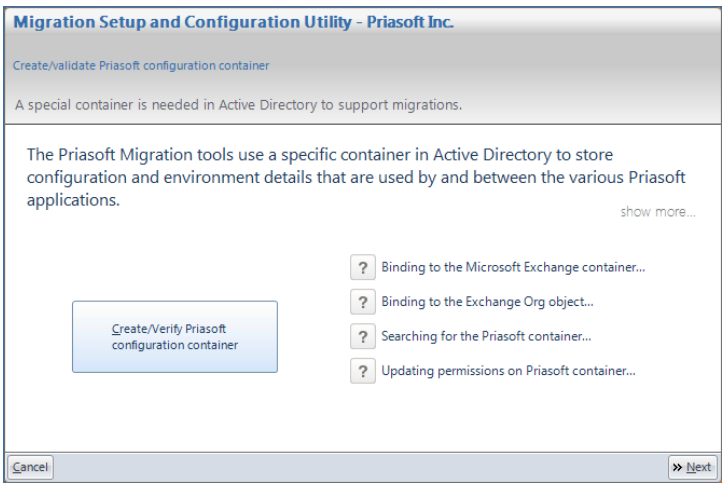
This page will create or update a domain specific account used for accessing and working with Active Directory objects. The account name will start with: PS-LDAP-SA. The characters after the prefix are data specific to the domain.

17. Domain Controller selection



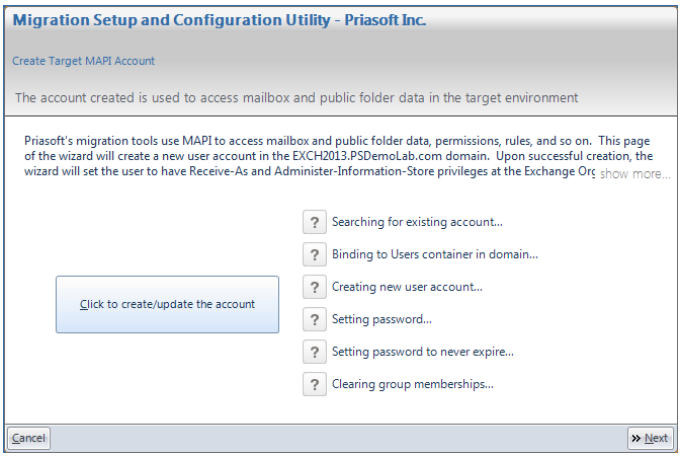
This page allows for the selection of one or more DCs to cache in the Priasoft credential store. When running other Priasoft tools, one can simply browse the credential store for the selected server(s) and select it for use.

18. Priasoft Configuration Container



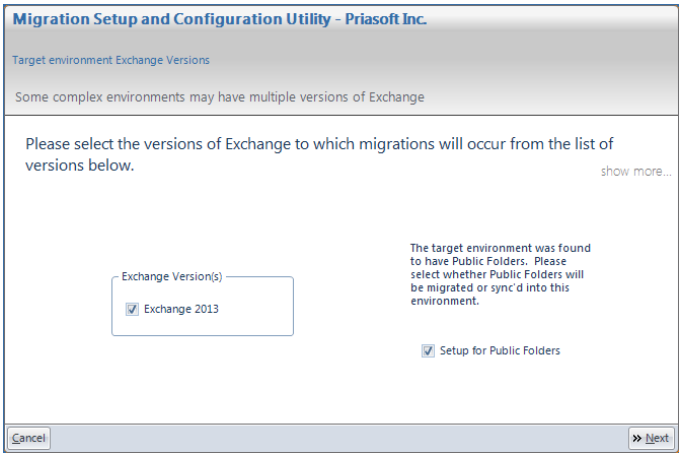
The Priasoft migration suite uses a container named “Priasoft” in AD to store configuration details used by Priasoft tools. The container is stored as a child of the Exchange Org object in the Configuration partition of AD. This is the only container for which the service accounts will have write access – all other objects in the Configuration partition are accessible only with read and search permissions.

19. Target MAPI Account



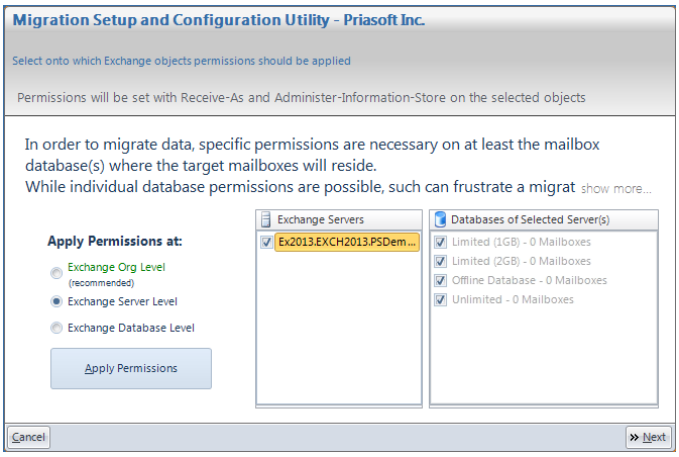
This page will create the service account used to access mailboxes and public folders in the source environment. The account name will be specific to the domain and its name will start with: PS-MAPI-SA.

20. Target Exchange Versions



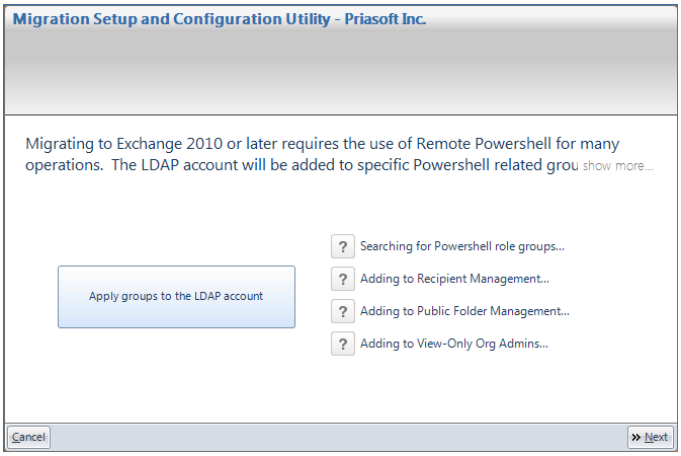
This page shows the versions of Exchange server found in Active Directory. One should select the versions of Exchange to which mailboxes will be migrated. Additionally, if there are public folders to be migrated and was selected in the source configuration pages, that option should also be checked. The versions of exchange selected will determine which servers are shown on the next page for setting permissions.

21. Target Exchange Permissions



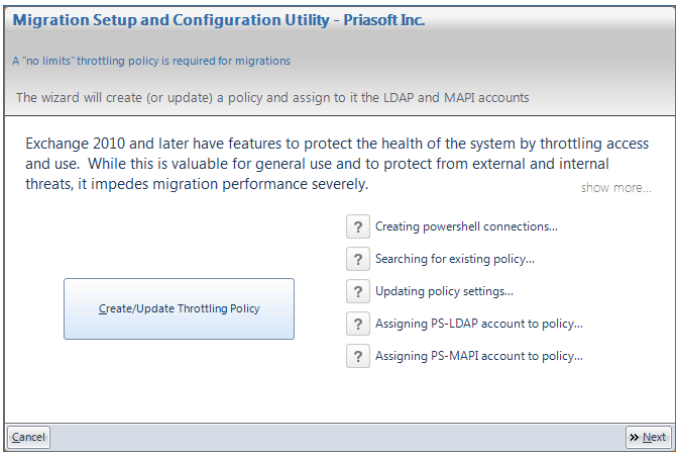
This page is used to configure the specific MAPI/Exchange permissions based on the version(s) selected on the previous page. It is possible to only set permissions on a single database, server, or the entire Exchange Organization. It is HIGHLY recommended to set the permissions at the Organization level so that if new servers or databases are added to the environment after setup, the permissions can automatically inherit from the Org. It is quite common to create a Dry-Run database after setup and if a setting other than Exchange Org Level is used, there may be a need to re-run the setup wizard to apply the permissions to the dry-run database.

22. Target Environment Powershell Setup



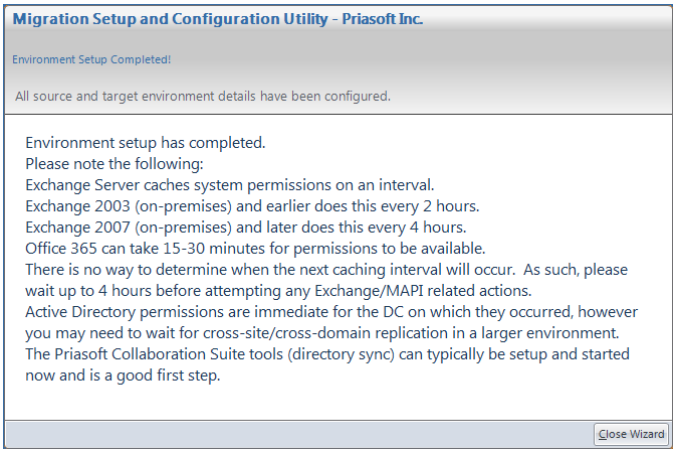
When migrating to Exchange 2007 or later, Exchange PowerShell is used for certain parts of the migration. In order to execute such commands, the service account (the LDAP account) must be a member of some key PowerShell Groups (Recipient Management, Public Folder Management, and View-Only Org Management) and must be "PowerShell Enabled". This page is not shown if the target environment is Exchange 2003 or earlier.

23. Target Environment Throttling Policy



When migrating to Exchange 2010 or higher, throttling policies exist that by default limit the number of mailboxes that can be migrated concurrently. This page will create a new throttling policy with the limits removed and will associate the service accounts (both LDAP and MAPI) with the policy. Without this step the concurrency would be limited to 18 or less mailboxes running concurrently.

24. Completion



The last page of the setup wizard. Note the information above and the requirement to wait several hours before attempting any migrations.