



# Agency Cutover & Post Cutover Guide

Version 3  
July 19, 2011

Prepared by:  
Laura Parma, Implementation Manager

---

## Table of Contents

<a href="#">Introduction and Purpose</a> .....	<a href="#">2</a>
<a href="#">Background</a> .....	<a href="#">4</a>
<a href="#">Pilot Migration for Agencies</a> .....	<a href="#">5</a>
<a href="#">Before the Day of the Migration/Cutover</a> .....	<a href="#">6</a>
<a href="#">Day of Cutover/Migration</a> .....	<a href="#">8</a>
<a href="#">Post Cutover Tasks</a> .....	<a href="#">16</a>
<a href="#">Agency Help Desk /Service Cutover &amp; Post Cutover</a> .....	<a href="#">18</a>
<a href="#">Cutover &amp; Post Cutover Checklist: Migration Checklist</a> .....	<a href="#">19</a>

---

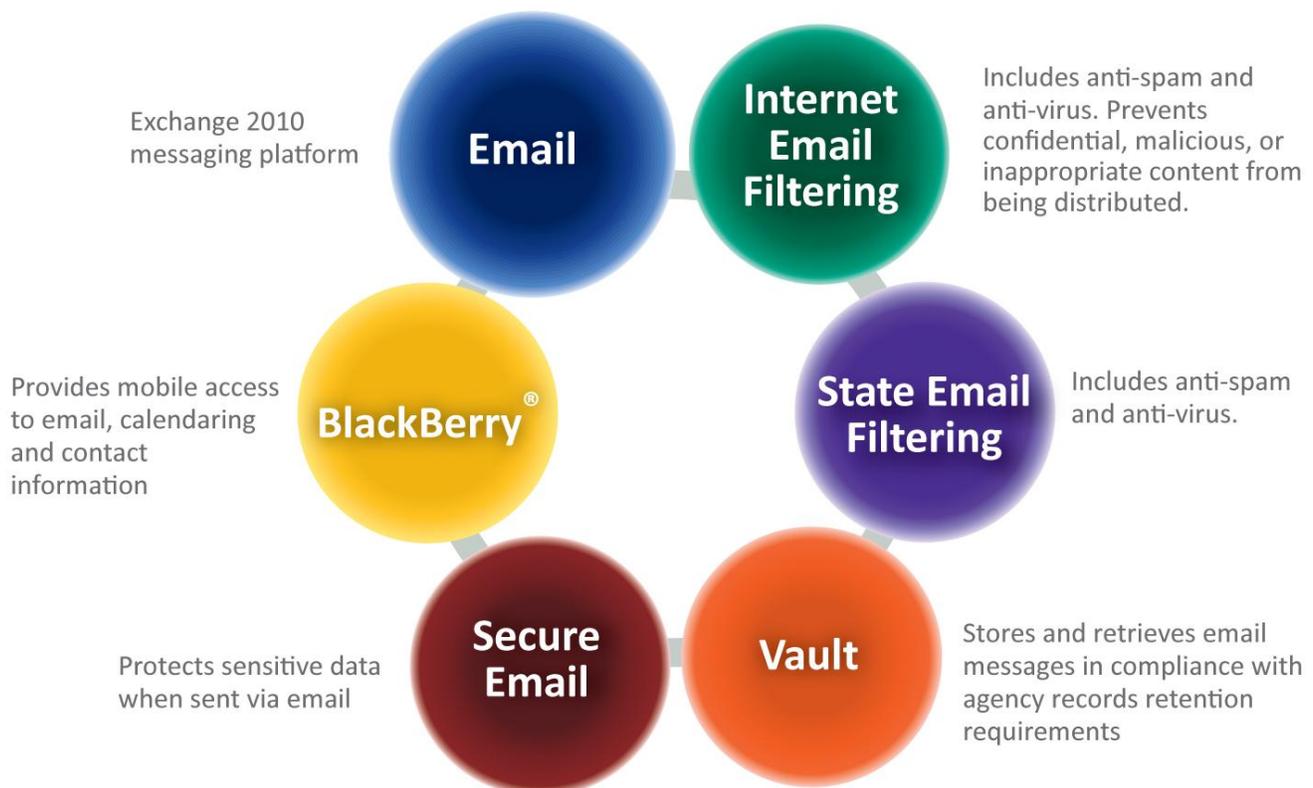
## Introduction and Purpose

The purpose of the **Agency Cutover & Post Cutover Guide** is to define the steps that agencies perform and DIS performs at the time of cutover and post cutover for the first phase of the Shared Services Email offering.

The guide documents key activities to be coordinated by the Agency Implementation Coordinator in preparation for migration and following the migration to the Shared Services Email offering. The activities in the guide are summarized in the Agency Cutover & Post Cutover Checklist that will summarize completed activities, and the assertion that the agency has completed migration for phase one. The Agency Implementation Coordinator serves as the primary agency contact to the Shared Services Email Project (SSEP) and is responsible for coordinating the internal agency activities stated in the guide.

The Shared Services Email offering is summarized by the following diagram. Phase 1 migration includes the Email with Exchange 2010, Mail Filtering and BlackBerry® support.

# Shared Services Email Project Service Description



---

This guide documents the tasks for migration and post migration for agencies. These tasks are listed in each section and are summarized in the Agency Cutover Checklist & the Agency Post Cutover Checklist both included at the end of the guide. As you progress through the guide you will see prerequisite tasks that:

- Must be completed by your agency.
- Must be completed in coordination with DIS.

You can identify these tasks located throughout this document as they are marked by a specific icon. In addition each task will be numbered. The task number will appear to the right of the icon and is included for ease of reference. The table below identifies each icon, a sample task number, and relative description.

Icon	#	Task Description
	1	Tasks that must be Completed by the Agency.
	2	Tasks that must be Completed by DIS.

Agency Implementation Coordinators will interface with the Project Client Liaison to review any questions regarding this guide.

\*\*\*\*\*

---

## Background

On February 10, 2009, Governor Gregoire issued [Governor's Directive 09-02](#), directing state agencies to provide full assistance and support in the development and implementation of a shared services model. The Governor stated that, "Sharing administrative functions between agencies will allow you to focus on your core missions of providing essential services to Washingtonians. I expect that our new shared services approach and governance structure will capture the benefits of economies of scale in a way that ensures good customer service to the client agencies."

In response to adopting the shared services model and its governance, an email shared service project was identified, and approved by the Shared Services Executive Steering Committee, comprised of subset of agency Directors, and the Customer Advisory Board, comprised of state agency CIO's. The overall purpose to stand up a new email service is to optimize the value of IT by concentrating like email services from across state agencies to a central service to lower costs and improve service. The new email shared service was created through adoption of the Washington State Shared Services Model and identified as a learning experience to improve the shared services model.

This project meets the Governor's directive by providing a Shared Email Service. The outcomes from this effort reinforce the generally accepted benefits for a shared service which include:

- Drive cost and effort out of line and support services, including IT services
- Add value to line and support services
- Leverage existing agency resources, data and processes
- Avoid duplication
- Reduce risk
- Reduce time for problem resolution

\*\*\*\*\*

---

▲	1	Submit Agency Requested Pilot Migration and Agency Migration Schedule to Client Liaison. Group BlackBerry® Users to the Top of the List.
▲	2	Confirm Users have been Informed that their Mailboxes will be Migrated and that they should Contact the Agency Help Desk with any Issues or Questions. Remember to Communicate to Users the New Web Addresses for Outlook Web App (OWA). This should Include Communicating to End Users the Junk Mail Address: <a href="https://junkmail.wa.lc">https://junkmail.wa.lc</a>

### **Pilot Migration for Agencies**

It is assumed that each agency will have a small group of pilot users who serve as a pilot migration for their agency. The pilot size is approximately 5% of users. The pilot will provide a test for approximately a week to review the agency experience post migration. The pilot provides a method for validating the function of the cutover as well as the function of agency applications. Agency Implementation Coordinators will schedule and coordinate the actual pilot migration and agency migration schedule with their Project Client Liaison.

\*\*\*\*\*

---

## Before the Day of the Migration/Cutover

This section describes the activities that will take place for Exchange Mailboxes, Filtering readiness and BlackBerry® migration prior to the day of the migration/cutover.

This section outlines those tasks that must be completed during the transition from 2003 to 2010.

	<b>3</b>	<b>Disable Email Address Policies</b>
---	----------	---------------------------------------

### Disable Email Address Policies

In Exchange 2010, email address policies are enforced. For users with email addresses that do not match the proposed pattern, this can be problematic. So as to allow existing users to keep their current email addresses, policy enforcement will be disabled on all existing users. New users, created on Exchange 2010, will be subjected to the policy.

```
## Code to disable mailbox policies for existing users
Get-Mailbox <qualifiers as necessary> | Set-Mailbox -EmailAddressPolicyEnabled $False
```

	<b>4</b>	<b>Set User Properties</b>
---	----------	----------------------------

### Set User Properties

At some point in the future, user mailboxes can be re-enabled for address policies if the address that will be enforced by the policy is consistent with their existing address. In addition to the display name attribute, the company attribute has been chosen to be a key field for address policy matches. The following code will modify the company attribute with each agency's agency code. Whatever you type within the quotes will appear on the company attribute.

```
## Set the users' company attribute to the agency code
Get-Mailbox <qualifiers as necessary> | Get-User | Set-User -company "AGY"
```



## 5 Change Address Lists and Address Policies to oPath

### Change Address Lists and Address Policies to oPath

In Exchange 2003, email addresses are stamped on user accounts by the Recipient Update Service (RUS). RUS uses a best effort approach to stamping addresses which has resulted in some inconsistency across the user base. In Exchange 2010, all email address policies are enforced and consistently implemented. However, Exchange 2010 requires policies to be written in the oPath syntax instead of the LDAP syntax used in Exchange 2003.

The approach for dealing with this change is to remove the 2003 policy object (that originated from the legacyExchangeDN attribute tied to the Exchange 5.5 site value) and replace it with an agency-specific oPath query. DIS will perform this task.

```
## Grab the policy object, put it in the pipeline and remove it
## These commands should be run per each policy object the agency supports
Get-EmailAddressPolicy -Identity "[Enter Address Policy Name]" | Remove-
EmailAddressPolicy

## Code to create a new email address policy for a sample agency
New-EmailAddressPolicy -name "AGY Users" -EnabledEmailAddressesTemplates
"SMTP:%rAa%rBb%rCc%rDd%rEe%rFf%rGg%rHh%rIi%rJj%rKk%rLl%rMm%rNn%rOo%rPp%rQq%rRr%rSs%rTt
%rUu%rVv%rWw%rXx%rYy%rZz%g.%rAa%rBb%rCc%rDd%rEe%rFf%rGg%rHh%rIi%rJj%rKk%rLl%rMm%rNn%rO
o%rPp%rQq%rRr%rSs%rTt%rUu%rVv%rWw%rXx%rYy%rZz%r'%s@agy.company.com","smtp:%m@agy.comp
any.com","X400:c=US;a= ;p=Company;o=Exchange;" -RecipientFilter (((RecipientType -EQ
'UserMailbox' -OR RecipientType -EQ 'MailUser') -AND (company -like 'AGY*' -OR
DisplayName -like '* (AGY)')) -OR ((RecipientType -EQ 'MailUniversalDistributionGroup'
-OR RecipientType -EQ 'MailNonUniversalGroup' -OR RecipientType -EQ
'MailUniversalSecurityGroup' -OR RecipientType -EQ 'DynamicDistributionGroup') -AND
(DisplayName -like 'AGY DL*' -OR DisplayName -like 'U-S-AGY*')) -OR (RecipientType -EQ
'PublicFolder' -AND DisplayName -like '* (AGY)'))
```

\*\*\*\*\*

---

## Day of Cutover/Migration

This section describes the activities that will take place for Exchange Mailboxes, Filtering readiness and BlackBerry® cutover/migration.

This section outlines those tasks that must be completed during the transition from 2003 to 2010.

### Migrate Journaling Functions to Exchange 2010

Users tied to journal mailbox databases in 2003 will need to follow the move procedures as defined in this section. In Exchange 2003, all users on a designated database will be journaled to a single mailbox on an alternate database (where the content is picked up by the vault or other archiving tool). The process in Exchange 2010 can be implemented identically to the 2003 environment or through journal rules if the agency has enterprise Client Access Licenses (CALs). All users on the designated journaled database should be moved together.

1. Before migrating the user, check the user's distribution group membership list. Change any distribution group expansion server to use Exchange 2010 if still using 2003 (this should be done as part of the pre-cutover work, but should be verified in larger organizations that process many changes a day).
2. Create new journaling rules on Exchange 2010 to emulate the desired effect of the 2003 journal procedures. In most cases, this will call for a rule to journal everything associated with the user. Journaling by rule requires an enterprise CAL. If standard journaling will be configured in Exchange 2010, the user will have to move to a designated database for which journaling is enabled.
3. Submit the new move request.
4. Exchange 2003 journaling will stop automatically once the user resides on the 2010 servers.
5. Ensure all content is vaulted from the 2003 journal mailbox before retiring the mailbox.



6

## Validate Naming Conventions for Directory Objects

### Validate Naming Conventions

The provided code sample is report code only. If exceptions are generated from the report, you will need to make the required changes.

The following PowerShell cmdlets can be used to identify objects in your directory that might create problems during the migration as they fall outside of state naming standards.

```
## Focus the administrative scope on the agency domain
Set-ADServerSettings -RecipientViewRoot "agy.wa.lcl"

## Get the DLs whose display names don't match the standard
Get-DistributionGroup | WHERE {$_.DisplayName -NotLike "AGY DL*" -AND $_.DisplayName -
NotLike "U-S-AGY*"}

## Check for DLs that are not universal in scope
Get-DistributionGroup | WHERE {$_.GroupType -NotLike "Universal*"}
```

	<b>7</b>	<b>Export Mailbox Dumpsters</b>
---	----------	---------------------------------

### Export Mailbox Dumpsters

If any users have been identified for preserving mailbox dumpster contents (which won't be migrated by default), they will need to have their 2003 mailboxes exported to a .pst file prior to migration. Be sure that the Exchange Trusted Subsystem has permissions on the server where .pst files will be created.

```
## To dump the contents of selected mailboxes...
New-MailboxExportRequest -mailbox [alias] -FilePath \\server\share\file.pst
```

	<b>8</b>	<b>Move Mailboxes (Validate that RPC/HTTP is Turned On at the Client)</b>
	<b>9</b>	<b>Confirm BlackBerry® Users have been informed to have Devices Powered On, Fully Charged, Within Coverage Area.</b>
	<b>10</b>	<b>DIS Migrate BlackBerry® Devices</b>

### Move the Mailboxes and Migrate BlackBerry® Devices

Each wave of the mailbox move process should be documented in its own CSV file. Users will be distributed across the available databases to maximize throughput and properly balance the load. Unlike previous versions where moves happened in real time, Exchange 2010 uses the Move Request feature, which queues the request for a background process. Note: The move request cmdlet is documented at the following address: <http://technet.microsoft.com/en-us/library/dd351123.aspx>. While this difference doesn't make the move process any slower, it does require a slightly different approach to managing the move process. BlackBerry® migrations need to also occur. Specifically, agencies will need to do the following:

1. Submit the initial move request using the New-MoveRequest cmdlet. The preferred approach for agencies deploying in waves is to import the CSV file for each wave into the PowerShell pipeline and submit the generic move request. Check the status of move requests. Note: Move requests and troubleshooting guidance is provided at <http://technet.microsoft.com/en-us/library/dd876924.aspx>
2. Failed move requests may require some changes to the code as documented below. Use the information at <http://technet.microsoft.com/en-us/library/dd638094.aspx> to troubleshoot failed mailbox moves. Some of the necessary code changes are documented below. DO NOT use additional parameters unless you are specifically troubleshooting an identified problem.
3. At the time that mailboxes are being moved, the associated BlackBerry® migrations need to occur. The following procedures should be followed as part of migrating mailboxes linked to BlackBerry® devices.
  - a. Reminder: Provide DIS with a list and schedule identifying which users mailboxes will be migrated on a specific date/time and specify which users are BlackBerry® users 30 days prior to the first scheduled migration date.
  - b. Recommend that all BlackBerry® users be migrated in 'groups' on specific date/times.

- 
- c. Customer agency needs to notify all BlackBerry® customers prior to BlackBerry® migration of 3 important items:
    - i. Devices must be powered on.
    - ii. Devices should be fully charged.
    - iii. Devices must be in coverage.

Note: The pre-migration items detailed above are required to ensure a successful BlackBerry® migration. If not, then the migration of the BlackBerry® device/user may fail. This would require coordinating another migration of that device/user with DIS, or reactivation of the device on the DIS 2010 BlackBerry® servers.

Note: It is highly recommended that you have a user with a BlackBerry® available to test and validate the BlackBerry® is functioning properly post migration.

If a BlackBerry® is not successfully migrated the night the user's mailbox moved, then:

- DIS will email agency BlackBerry® support staff immediately following a failed BlackBerry® migration identifying the user. BlackBerry® migration logs can usually identify the nature of the failure i.e. device out of coverage/powered off, etc..., and this information is provided to the agency support staff in the email.
  - Agency support staff have 2 options:
    - a. Take appropriate steps to ready device for migration and request that DIS attempt a 2<sup>nd</sup> migration of the impacted user.
    - b. Delete user from customer agency BES and then send a request to DIS to add a new user to the BlackBerry® service. Note: Please attach the BlackBerry® New/Cancel request form to your email to the DIS Service Desk [ServiceDesk@dis.wa.gov](mailto:ServiceDesk@dis.wa.gov) .
4. Remove mailbox move requests upon successful completion of the migration. You may delete requests sooner if desired, but all requests should be cleared at the end of the migration.

NOTE: If you want to use an automated approach to scheduling the mailbox moves, please coordinate that with your Implementation Coordinator.

The following code is the actual move request for mailboxes. It calls for the CSV created in previous steps and should match the variables you used (e.g. \$MB or \$alias). It is suggested that mailboxes start with a -BadItemLimit of 10. You may use the -WhatIf statement at the end for testing purposes. If the script fails, ensure you have proper credentials.

```
## Ensure your scope is proper for your agency (change "agy" to proper agency code)
set-adserversettings -recipientviewroot agy.wa.lcl

## Open the CSV file per wave and submit the mailbox move request

ForEach ($MB IN Import-CSV c:\path\file.csv) {

    ## The most basic Move Request - specify the DIS-hosted GC
    New-MoveRequest -Identity $MB.Name -DomainController agyGc01y2010.agy.wa.lcl

    ## Additional parameters to add if the basic move fails. These won't fix
    ## every problem, but should fix the majority of mailboxes.

    ## Add to the new-MoveRequest cmdlet when appropriate
    ## -BadItemLimit 10

    ## -BadItemLimit 100 -AcceptLargeDataLoss
    ## -AcceptLargeLoss is required for large number of bad items

    ## -IgnoreRuleLimitErrors #requires rebuilding client rules
}


```

The following commandlets will help you during and after the move request is made.

```
## To view the status of all move requests
get-moverequest

## To check on the status of move requests not complete
get-moverequest | where {$_.status -notlike "complete*"}

## To specifically seek move requests in a failed state
Get-MoveRequest | ?{$_.status -like "failed"}

## To verify that all mailboxes have been moved (this is an exceptions report)
get-mailbox | where {$_.RecipientTypeDetails -like "legacy*"}

## To generate a short real-time report on in process or complete move requests
Get-MoveRequest | Get-MoveRequestStatistics | ?{$_.status -notlike "failed"}


```

The following code generates a status report and automatically sends it to your administrator. Include the distribution list (DL) alias to the List in the "To Parameter of the send-mailmessage cmdlet." If you are sending to external recipients, the SmtplibServer that you specify must be configured to allow relay of the IP for the admin workstation on which you are running the Send-mailmessage cmdlet. If you are only sending to internal recipients, your Exchange 2003 server should work.

```
#####
## Save code as Send-MoveReport.ps1 ##
## Usage: .\send-moveReport.ps1 ##
## Parameters: None ##
## Author: Mark Dougherty ##
## Create Date: June 2010 ##
#####
## Make sure to scope for your agency
set-adserversettings -recipientviewroot AGY.wa.lcl

## Create a new variable and assign it to the output of the get-MoveRequestStatistics
cmdlet


```

```

$stats = Foreach ($mbx in Import-csv c:\path\file.csv) {
Get-MoveRequestStatistics -Identity $mbx.Name |
Format-Table alias,status,percentcomplete -AutoSize
}

## Push the output of stats to a string for use in the body of the email
$stats=$stats | out-string

## Send email message with report. Change the FROM and TO parameters. If you need
multiple
## recipients, separate with commas (no spaces between recipients)
send-mailmessage -from you@agy.wa.gov -to who@agy.wa.gov -Subject "Mailbox Move
Completion Report" -body $stats -smtpserver [hostname]

```



## 11 Enable Single Item Recovery

### Clean up the Mailbox – Enable Single Item Recovery

A number of property overrides may exist in the agency's 2003 environment that must be made consistent in the 2010 environment. These tasks must be completed during the move process. Ideally you would enable single item recovery immediately following a wave of mailbox moves. Optionally, you can enable single item recovery on all of your 2010 mailboxes without using an import file. Sample code is provided below:

```

## Import the same CSV file that was used to submit move requests
Foreach ($MB IN Import-CSV c:\path\file.csv) {

## For each mailbox returned, clean up and make settings consistent
Set-mailbox -identity $MB.name -SingleItemRecoveryEnabled:$true

}

##Option to set singleitemrecovery on all 2010 mailboxes
get-mailbox -RecipientTypeDetails usermailbox | set-mailbox -SingleItemRecoveryEnabled
$true

##Verify that all mailboxes have SingleItemRecoveryEnabled set to true
get-mailbox -RecipientTypeDetails usermailbox | ?{$_.SingleItemRecoveryEnabled -like
"false"}

## This code is run by DIS separately to set the mailbox quota to the db defaults
## It is not part of the mailbox cleanup process for agencies
Foreach ($MB IN Import-CSV c:\path\file.csv) {

Set-mailbox -identity $MB.name -UseDatabaseQuotaDefaults:$true

}

```

**Important:** Enabling Single Item Recovery ensures that deleted items are recoverable without using backup media. More information can be found at the following links:

[http://technet.microsoft.com/en-za/library/ee364755\(en-us\).aspx](http://technet.microsoft.com/en-za/library/ee364755(en-us).aspx)  
<http://blogs.technet.com/b/exchange/archive/2009/09/25/3408389.aspx>



### Disable Junk Mail Filtering for All Mailboxes

IronPort is used by the State of Washington as the message hygiene gateway for spam and viruses. Exchange 2010 also has hygiene functionality built-in. Because these two products handle spam differently, it is necessary to turn off the built-in features to provide users with a single repository for managing spam. This is accomplished by disabling junk mail features in both Outlook and Exchange (OWA). This change should be done at the end of your migration. Notify your users of the date of the change and let them know to begin using <http://junkmail.wa.lcl> to manage their junkmail and safe and blocked lists.

Update your agency's GPO for Outlook settings to ensure that junk mail filtering is disabled. To configure Outlook Junk E-mail Filter settings in Group Policy

1. In Group Policy, load the Office Outlook 2007 template (Outlk12.adm) and go to User Configuration\Administrative Templates\Microsoft Office Outlook 2007\Tools | Options...\Preferences\Junk E-mail.
2. Configure the following settings.
  - a. Hide Junk Mail UI = disabled
  - b. Junk E-mail protection level = Enabled
  - c. Select level = No Protection

More information about configuring Outlook settings for junk mail can be found at [http://technet.microsoft.com/en-us/library/cc179183\(office.12\).aspx](http://technet.microsoft.com/en-us/library/cc179183(office.12).aspx).

OWA junk mail settings must also be turned off so as not to conflict with the Ironport functionality. They are separate from the junk mail settings in the Outlook client. They can be set on a per mailbox basis.

```
#####
## Preferred Method  ##
#####

## Clear Junk Email Settings on all 2010 mailboxes
get-mailbox -RecipientTypeDetails usermailbox | Set-MailboxJunkEmailConfiguration -
Enabled $false -TrustedSendersAndDomains $null -BlockedSendersAndDomains $null

## Set OWAMailboxPolicy on all 2010 mailboxes
get-mailbox -RecipientTypeDetails usermailbox | Set-CASMailbox -OwaMailboxPolicy "OWA
NoJunk Mailbox Policy"

#####
## Code below is an alternate method using an input file #
#####

## disable the OWA junk mail filtering functionality (script uses
## the same csv file as mailbox moves). Be sure to rename the
## file before importing.

ForEach ($MB IN Import-CSV c:\path\file.csv) {

Set-MailboxJunkEmailConfiguration -Identity $mb.Name -Enabled $false -
TrustedSendersAndDomains $null -BlockedSendersAndDomains $null

## Sets an OWAMailboxPolicy that has JunkEmailEnabled set to false.
Set-CASMailbox $mb.name -OwaMailboxPolicy "OWA NoJunk Mailbox Policy"

}
```

---

If you receive the error noted below when running the Set-MailboxJunkEmailConfiguration cmdlet you can safely ignore it. This error is displayed for mailboxes that have never logged into OWA.

" The Junk E-Mail configuration couldn't be set. The user needs to sign in to Outlook Web App before they can modify their Safe Senders and Recipients or Blocked Senders lists."

More information about MailboxJunkEmailConfiguration cmdlet is located at <http://technet.microsoft.com/en-us/library/dd979780.aspx>

	13	<b>Agency End User Testing</b>
---	----	--------------------------------

### Agency End User Testing

Agency End User Testing information is available upon request. This information can be obtained by contacting your Project Client Liaison.

	14	<b>Validate Your Non-SMTP Agency Applications</b>
---	----	---

### Validation of Your Non-SMTP Agency Applications

Any application which has been updated by your agency to work with the Shared Service Email offering should have its integrated functionality validated post-migration to ensure that no new issues have occurred since your pre-migration testing. This validation should be the final step for publishing updated applications which integrate with the Shared Service Email offering.

Any applications which perform actions other than sending out emails via SMTP should have been discussed with your Project Client Liaison prior to migration and during you pre-cutover planning phase. It is assumed that you have updated your agency applications and have documented test plans to test these applications. It is also assumed that you have coordinated with your Project Client Liaison regarding applications that have integration with Exchange to confirm assumptions about integration with the Shared Services Email offering and any assumed security permissions beyond default configurations. Please refer to the ***Agency Application Integration Readiness Template*** for more information.

	15	<b>Convert Agency FA mailboxes to Room Mailboxes</b>
---	----	--

### Convert Agency FA Mailboxes to Room Mailboxes

In Exchange 2010, the system recognizes resource mailboxes. It's actually an attribute of the mailbox that can be any of the following values:

- Regular
- Room
- Equipment
- Shared

Converting the mailbox to a non-regular (single user) mailbox is simple and can be handled using the following code.

```
## Converts mailbox with ConfRoom1 alias to a Room type mailbox
Set-Mailbox ConfRoom1 -Type Room
```

```
## Converts all facility mailboxes to a Room type mailbox
Get-mailbox "AGY FA *" | ?{$_RecipientTypeDetails -eq "UserMailbox"} | Set-Mailbox -
Type Room

## Or, if we have a separate list of just those requiring conversion
## assume a csv file format of Name,mbType

ForEach ($MB IN Import-CSV c:\path\file.csv) {

Set-Mailbox -Identity $MB.Name -Type $MB.mbType

}

```



## 16 Setup Calendar Processing and Auto-accept

### Setup Calendar Processing and Auto-accept

Configuring mailboxes to automatically accept meeting requests is built-in to Exchange 2010 (it required third party agents or the auto-accept agent in Exchange 2003). It can be configured from Outlook Web Application by end users for the resource mailboxes they control. However, it may also be desirable to have all resource mailboxes configured after the migration. The Resource Booking Attendant can accept or decline resource requests based upon policies that you create. If the Resource Booking Attendant is enabled, it uses the booking policies to determine if incoming requests will be accepted or declined. If the Resource Booking Attendant is disabled, the resource mailbox's delegate must accept or decline all requests. Prior to setting up the book agent, you will need to log into each facility mailbox and remove existing delegates that were established in the 2003 environment.

Depending on your specific needs, the following links can be used to understand the PowerShell cmdlets necessary to make bulk changes to resource mailboxes.

Calendar processing: <http://technet.microsoft.com/en-us/library/dd335046.aspx>

Auto-reply: <http://technet.microsoft.com/en-us/library/dd638217.aspx>

Automatic booking agent: <http://technet.microsoft.com/en-us/library/bb123495.aspx>

NOTE: If your agency requires the functionality provided by the Microsoft Auto Accept Agent (or third party equivalent), you will need to configure calendar processing immediately after the mailbox move to retain the functionality.

\*\*\*\*\*

---

## Post Cutover / Migration Tasks

	17	<b>SMTP Relay Migration</b>
---	----	-----------------------------

### SMTP Relay Migration

Agencies migrating to IronPort for inbound and outbound filtering will have the option to point applications and servers requiring SMTP relay to IronPort. The solution will allow for redundancy and throttling. It is important for agencies to identify their needs and migration paths internally.

This task does not need to be completed at the time of your migration. You can continue to use your existing infrastructure for relay until you are ready to switch. You should begin identifying your relay needs as soon as possible as you will be unable to decommission servers in your environment that support SMTP relay until you have pointed all devices and applications requiring relay to IronPort.

In order to place servers and applications into the allowed relay senders list, agencies will need to provide the following information:

Server Name:  
IP Address:  
Technical Contact:  
Potential for High Volume (Y/N):  
Function for Relay:  
Standby Server (Y/N):

Agencies may send requests to the DIS Service Desk when the service has been made available.

### Testing SMTP Applications

Any application which send out emails via SMTP should be tested after migration to the new SMTP Gateway. As stated above, this is not anticipated at the time of mailbox migration. Applications should be tested to ensure that they can send mail both internal to your organization and external to your organization. Any questions should be reviewed with your Client Liaison as you coordinate your SMTP Relay Migration.

	18	<b>Change/Create SPF Record</b>
---	----	---------------------------------

### Change / Create SPF Record

The Sender Policy Framework is a mechanism used to identify spam. Note: Sender Policy Framework syntax is documented at [http://www.openspf.org/SPF\\_Record\\_Syntax](http://www.openspf.org/SPF_Record_Syntax). **Error! Reference source not found.** is an adaptation of the information on that site. Each agency creates an SPF record in DNS that recipient organizations can query to determine whether a sending host is a valid host in the organization. The host can be internal or external and multiple mechanisms are available for use when writing the SPF record.

SPF works when the recipient host queries the sending domain's SPF record. The value returned by the DNS server is compared with the known properties (host name, IP address) of the sender and an appropriate action taken. SPF return values and actions are explained below.

Return	Explanation	Action
Pass	The SPF record designates the host to be allowed to send	accept

Return	Explanation	Action
Fail	The SPF record has designated the host as NOT being allowed to send	reject
SoftFail	The SPF record has designated the host as NOT being allowed to send but is in transition	accept (mark)
Neutral	The SPF record specifies explicitly that nothing can be said about validity	accept
None	The domain does not have an SPF record or the SPF record does not evaluate to a result	accept
PermError	A permanent error has occurred (eg. badly formatted SPF record)	unspecified
TempError	A transient error has occurred	accept or reject

**Table 1 - SPF Record Return Values and Associated Actions**

Examples of possible SPF records are listed below.

```
## Allow only those machines in your agency's MX records; prohibit all others
agy.wa.gov. TXT "v=spf1 mx -all"

## Allow machines associated with MX record; neutral on all others
agy.wa.gov. TXT "v=spf1 mx ?all"

## All DIS subnet and all agency MX records; prohibit all others
agy.wa.gov. TXT "v=spf1 ip4:192.168.0.1/16 mx -all"
```

After reviewing openspf.org ([http://www.openspf.org/SPF\\_Record\\_Syntax](http://www.openspf.org/SPF_Record_Syntax)) and creating the correct spf record syntax for your organization, you will need to submit a request to DIS Service Desk to implement that change. As explained earlier this is a DNS change and will need to be implemented by the Security Perimeter Group at DIS.



19

Begin use of DIS Service Desk for Tier 2 Support Requirements.

## Agency Help Desk/Service Cutover & Post Cutover

The Agency Pre-Cutover Readiness Guide described the support that agency help desks would be providing to their end users. Should the user have an issue post cutover, it is assumed that they will contact their agency help desk for assistance. If the agency is unable to resolve the problem after completing Tier 1 troubleshooting steps, they will escalate to the DIS Service Desk. The DIS Service Desk, available 24x7, is the single point of contact for customer requests, problem reporting, escalation, and notification. Regardless of severity or impact, all incidents which fall outside of normal operating parameters will be reported and handled according to established procedures.

Phone: (360) 753-2454 or 1-800-241-7597

Email: [Servicedesk@dis.wa.gov](mailto:Servicedesk@dis.wa.gov)

When contacting the DIS Service Desk via phone please provide the *Service* and *Priority* of the issue:

- **Shared Service Email Offering;** Exchange 2010/email; Vault; Filtering, Secure Email issue
- Normal (immediate response not required)
- High (degradation of service, work stoppage, high impact to staff)
- **Note:** Recommend calling the DIS Service Desk for High Priority issues

When contacting the DIS Service Desk via email:

- Use the subject line in email to emphasize the *Service* and *Priority* of the issue

\*\*\*\*\*

## Cutover & Post Cutover Checklist: Migration Checklist

### Cutover: Migration Checklist

<i>Use this checklist to keep track of outstanding tasks that should be completed <b>prior</b> to the move</i>			
	1	Submit Agency Requested Pilot Migration and Agency Migration Schedule to Client Liaison. Group BlackBerry® Users to the Top of the List.	<input type="checkbox"/>
	2	Confirm Users have been Informed that their Mailboxes will be Migrated and that they should Contact the Agency Help Desk with any Issues or Questions. Remember to Communicate to Users the New Web Addresses for Outlook Web App (OWA). This should Include Communicating to End Users the Junk Mail Address: <a href="https://junkmail.wa.lcl">https://junkmail.wa.lcl</a>	<input type="checkbox"/>
	3	Disable Email Address Policies	<input type="checkbox"/>
	4	Set User Properties	<input type="checkbox"/>
	5	Change Address Lists and Address Policies to oPath	<input type="checkbox"/>
	6	Validate Naming Conventions for Directory Objects	<input type="checkbox"/>
	7	Export Mailbox Dumpsters	<input type="checkbox"/>
	8	Move Mailboxes (Validate that RPC/HTTP is Turned On at the Client)	<input type="checkbox"/>
	9	Confirm BlackBerry® Users have been informed to have Devices Powered On, Fully Charged, Within Coverage Area.	<input type="checkbox"/>
	10	DIS Migrate BlackBerry® Devices	<input type="checkbox"/>
	11	Enable Single Item Recovery	<input type="checkbox"/>
	12	Disable Junk Mail Filtering	<input type="checkbox"/>
	13	Agency End User Testing	<input type="checkbox"/>
	14	Validate Your Non-SMTP Agency Applications	<input type="checkbox"/>
	15	Convert Agency FA mailboxes to Room Mailboxes	<input type="checkbox"/>
	16	Setup Calendar Processing and Auto-accept	<input type="checkbox"/>

### Post Cutover / Migration Tasks

<i>Use this checklist to keep track of outstanding tasks that should be completed <b>after</b> the move</i>			
	17	SMTP Relay Migration	<input type="checkbox"/>
	18	Change/Create SPF Record	<input type="checkbox"/>
	19	Begin use of DIS Service Desk for Tier 2 Support Requirements.	<input type="checkbox"/>