

Agency Pre-Migration Tasks

This document is to be provided to the agency and will be reviewed during the Migration “Technical Kickoff” meeting between the ICS Technical Team and the agency.

Network:

Required Connectivity:

- [Open RPC port access to all workstations and servers.](#)
- [Direct Routed Network to ICS Domain](#)
- Enable all ports for ICS services IP address range (206.128 – 206.174) in agency firewall if one exists.
- Check MAPI, RPC connectivity at the agency
 - Complete this task by utilizing an ICS joined machine connected to the agency’s network and running the Outlook client (*do not use OWA as OWA is internet based and does not utilize MAPI or RPC*)

Servers:

Domain Controllers:

- [Determine Local Domain Controller Requirements](#)
- [Must be at 2003 Domain and Forest Functional Levels](#)
- Minimum OS of Windows 2000 SP4
- Establish Time Synchronization
- [Disable Windows Firewall](#)
- [Verify “Server Service” is running](#)
- [Must not contain file services](#)
- [Configure DNS and Suffix Settings for Target Domain](#) – add suffix search order to include target domain
- Identify Source Domain Controllers if reused for Target Domain

Exchange Servers:

- Rename server if its name is “Mail”
- Source Exchange running in Native Mode
- [Reduce Email Accounts to 200MB or Less](#)
- [Setup SMTP connectors](#)
- Create Target Domain recipient policies (QMM policy)
- [Disable Windows Firewall](#)
- Disable Circular Logging



- Create room and equipment resources in ICS
 - NOTE: Vista, Windows 7, or Server 2008 is required by the management console software.
- [Configure DNS and Suffix Settings for Target Domain](#) – add suffix search order to include target domain
- Record the AutoDiscover service for DNS for each email domain in both the internal and external DNS (NOTE: Free/Busy and offline address books are now web-based called “Exchange Web Services” these services rely on AutoDiscover internally to function)

SQL Servers:

- Minimum version SQL 7
- Rename Servers per Target Domain requirements
- [Disable Windows Firewall](#)
- [Configure DNS and Suffix Settings for Target Domain](#) – add suffix search order to include target domain

File Servers:

- Clean Up File Access Rights
- Verify no blocked permissions inheritance paths
- [Disable Windows Firewall](#)
- Rename Servers per Target Domain requirements
- [Verify “Server Service” is running](#)
- [Configure DNS and Suffix Settings for Target Domain](#) – add suffix search order to include target domain
- Verify remote registry service is running
- Permissions and File Shares – NTFS security, utilize custom built groups if using the default built-in groups create custom groups and move objects from the built-in groups into the custom groups.

Print Servers:

- Rename printers if such are to be published to the Active Directory
- [Configure DNS and Suffix Settings for Target Domain](#) – add suffix search order to include target domain

Active Directory:

Source Domain:

- Download and install the Management Console software (requires Vista, Windows 7 or server 2008). Include the Exchange Management console and the Remote Server Admin tool (RSAT)
 - Download and install ShellRunAs from Sys Internals
- Create a mail-enabled account “QMMSAD” with Domain Admin Rights
- Clean up unused and disabled accounts
- Identify administrative accounts – ensure admin accounts are located in the agency’s specific OU
- Clean up duplicate and disabled computer objects
- Clean up and prepare OU structure prior to migration
 - Rename Groups per Target Domain requirements
 - Create Service Accounts according to naming conventions in ICS
 - Upgrade groups to Universal Groups
- Upgrade Group Policy Management Console (GPMC export of Group Policies)
- [Set Group Policies to coincide with Target Doman Policies](#)
 - Match Password Policies
 - Match Enforcement Policies
 - [Disable Desktop Firewall](#)
 - Create GPO Migration Table
 - Backup GPOs
 - Create "Behave Like 2000" GPO setting
 - Create State Remote Registry setting for Vista
 - Create RPC state GPO to run
 - Create and apply Agency DNS search order GPO
 - Create Power Settings GPO (Preferences) – set to “Always On”
- If the default built-in groups have been used for setting permissions and Group Policy create new groups within the agency’s specific OU and associate the permissions and policies to these new groups.
- Verify there are no non-default settings implemented for Active Directory or Exchange.
- Review and streamline GPOs and permissions.

Name Services (DNS & WINS)

- Create DNS Forwarders to Target Domain
- [Add DNS Suffix Search order](#)
- Verify DNS resolution between Source and Target Domain
- Configure DHCP with DNS, and Suffix Settings
- Identify Back Office Servers (special cases, to be migrated as required):
 - SharePoint Servers
 - Live Communications Servers



- Project Servers

Establish Domain Trust (coordinate with ICS):

- Create 2 Way Forest Trust between agency Forest and ICS Forest
- Test NETDIAG and DCDIAG between Source and Target Domains

Workstations:

Desktops and Laptops:

- Workstations should be configured for DHCP
- Rename Workstations per Target Domain requirements (use 15 characters or less)
- [Disable Windows Firewall](#)
- Disable Windows and Personal Firewall (Such as Checkpoint)
- [Verify "Server Service" is running](#)
- Verify File and Print services are enabled
- [Vista Machines must have the "Remote Registry" Service](#) set to Auto Run
- Must be turned on and on the network to migrate
- Ensure all computers are connected through ONLY a wired Ethernet LAN connection before migration. Turn OFF wireless if the machine connects to a wireless network. Make sure the machine has only one connection to the network. We have discovered that computers whose sole network attachment is via a Wireless connection do not migrate easily.
- If able, set up Group Policy Preference Extensions to set "Always On" Power Scheme.
- Identify Offline File Synchronization Users and turn off synchronization
- Windows 2000 upgraded to XP must update secure pipe registry key to allow Local Service account "Read Access"
- Provide to agency End Users communications - email to users
- Install GPPE client side extensions for XP
- (ICS) Group Policy checks - (If a 3rd party tool such as: "Policy Maker" has been utilized - check for compatibility issues with ICS)

Known Migration occurrences:

- Web browser cookies may be lost
- Computers with files secured Encrypted File System (EFS) do not convert
- RPC over HTTP will always cause problems with Outlook Profile migrating, change to MAPI before migration if possible



- [Desktop may receive temporary profile after conversion](#) (NOTE: this may continue when several profiles are present, i.e. shared computers)
- Messenger Service is off – cannot send advanced notification when off
- Workstations with Static IP Addresses must be changed manually
- Desktop Profile lost (rare)
- Archiving Issues
- [PDA resynchronization](#)
- [Outlook Web Access \(OWA\)](#)
- [Migrating Exchange Resource Accounts](#)
- Machine names of over 15 characters causes issues as AD truncates longer names to 15 characters when creating the SID. The migration tool cannot match source machine names to target machine names.

Pre-Migration Certification:

- [Complete certification sign-off sheet](#)



Network

Open RPC port access to all workstations and servers.

The Quest Migration Manager agents are installed and updated from the Console (at ICS) over RPC and the agents transfer data directly between source and target servers over RPC as well, RPC traffic must be allowed over the routers separating the subnets.

Make sure that the following ports are open on workstations, servers, routers, and firewalls: **135 and 137–139**.

Direct Routed Network to ICS Domain

In order to for the Source agency systems to connect with the Target ICS domain, the core network must be directly routable. Source devices: workstations or servers behind indirect routing such as NAT or VPN tunnels will not function properly in within the ICS Domain.

Servers

Determine Local Domain Controller Requirements

Placement of Local ICS Domain controllers will be considered based on the criteria below. This information is taken from the ICS Active Directory Detailed Design Documentation.

Considerations for placing a Domain Controller

Physical Security: The domain controller contains information about the entire domain itself. Because of the global impact of this information if compromised, the domain information must be guarded closely. In an instance where a domain controller must be added to a remote location, it should be placed in a secured environment such as a physically locked room with controlled personnel access.

Data Availability: The Active Directory database located on the domain controller must be highly available. A domain controller should be located in a room with adequate air conditioning. The hardware which runs the domain controller must be redundant in its configuration. Redundant options should include multiple power supplies, battery backup, multiple network connections, and disk configurations which allow for continuance of domain controller function in case of disk failure.

Cost: A domain controller must meet or exceed Microsoft's recommended hardware specifications for running domain controller functions as well as anticipated user load. This additional hardware along with increased administration, maintenance, and proper security implementations, arrive at increased costs.

Platform: Windows Server 2008 will host Active Directory. In order to provide enhanced features of active directory, and a uniform Active Directory Functional Level, each domain controller placed in the domain must be installed as a Windows 2008 server running 64bit hardware.

Link Speed: Domain Controllers provide users with many functions. The primary function is that of authentication. If a user's access to a domain controller is provided over a slow link, the process of authenticating could take a very long time. The amount of time based on a predetermined threshold may determine whether to place a domain controller or not.

Link Availability: In the case of a link failure, users may not be able to authenticate directly with a domain controller until the link is brought back online. In this case, local workstation cached credentials will provide the user authentication to their workstation as well as local resources such as; printers and file services.

Site Location and Size: It is common practice to use a domain controller for each one thousand users in a domain. This can vary however, and is generally based on the size of the site and/or its number of connections required to pass through it for authentication. Close examination of the per site requirements according to size, connectivity, and throughput will further quantify the need for added domain controllers.

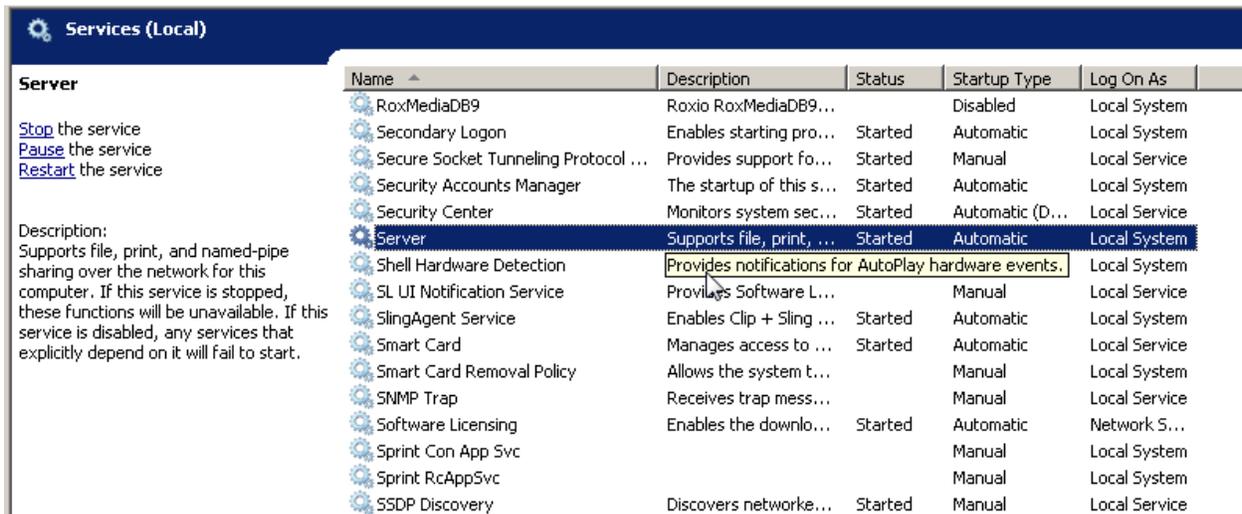
Must be at 2003 Domain and Forest Functional Levels

If the forest functional level in both source and target forests is set to Windows 2003 or higher, you can establish forest trust between the forest root domains.

Verify “Server Service” is running

Server service is automatically installed when you install the File and Printer Sharing service on the computer. Server service must be running on a computer in order for it to be updated from either Resource Updating Manager or the command-line updating tool VMover.exe.

If for some reason Server service is not allowed to run on the computers, you need to install or enable Server service temporarily, update the computers, and then disable or uninstall the service.



The screenshot shows the Windows Services console for 'Services (Local)'. The 'Server' service is highlighted in blue, indicating it is running. The service description is 'Supports file, print, and named-pipe sharing over the network for this computer. If this service is stopped, these functions will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.'

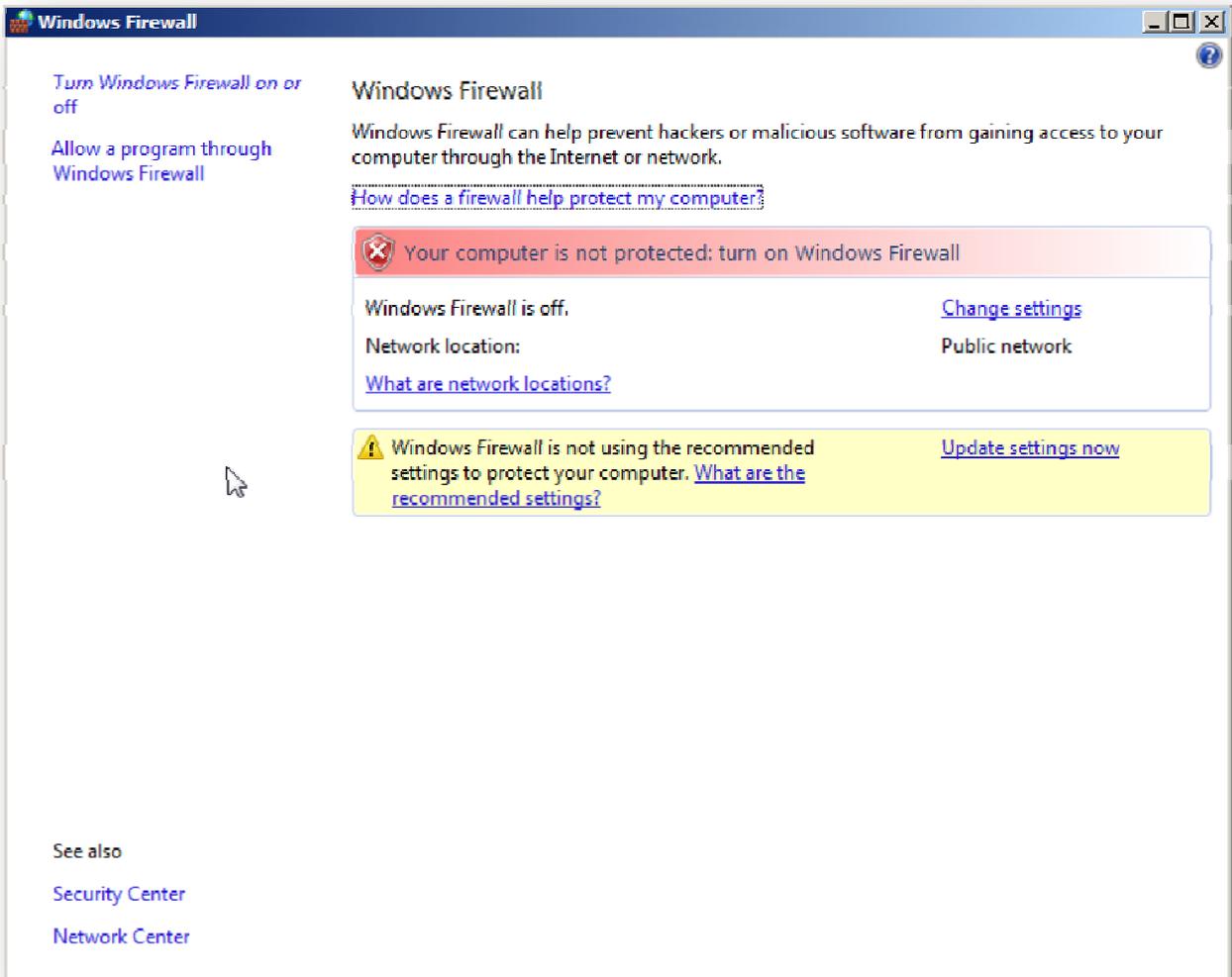
Name	Description	Status	Startup Type	Log On As
RoxMediaDB9	Roxio RoxMediaDB9...	Disabled	Local System	Local System
Secondary Logon	Enables starting pro...	Started	Automatic	Local System
Secure Socket Tunneling Protocol ...	Provides support fo...	Started	Manual	Local Service
Security Accounts Manager	The startup of this s...	Started	Automatic	Local System
Security Center	Monitors system sec...	Started	Automatic (D...	Local Service
Server	Supports file, print, ...	Started	Automatic	Local System
Shell Hardware Detection	Provides notifications for AutoPlay hardware events.			Local System
SL UI Notification Service	Provides Software L...		Manual	Local Service
SlingAgent Service	Enables Clip + Sling ...	Started	Automatic	Local System
Smart Card	Manages access to ...	Started	Automatic	Local Service
Smart Card Removal Policy	Allows the system t...		Manual	Local System
SNMP Trap	Receives trap mess...		Manual	Local Service
Software Licensing	Enables the downlo...	Started	Automatic	Network S...
Sprint Con App Svc			Manual	Local System
Sprint RcAppSvc			Manual	Local System
SSDP Discovery	Discovers networke...	Started	Manual	Local Service

Must not contain file services

Since Source Domain Controllers will not migrate to the new ICS domain. Because of this, resources located on Source Domain Controllers such as; “File Services” must be moved to a member server prior to migration. If the resources are not moved, they will not migrate.

Disable Windows Firewall

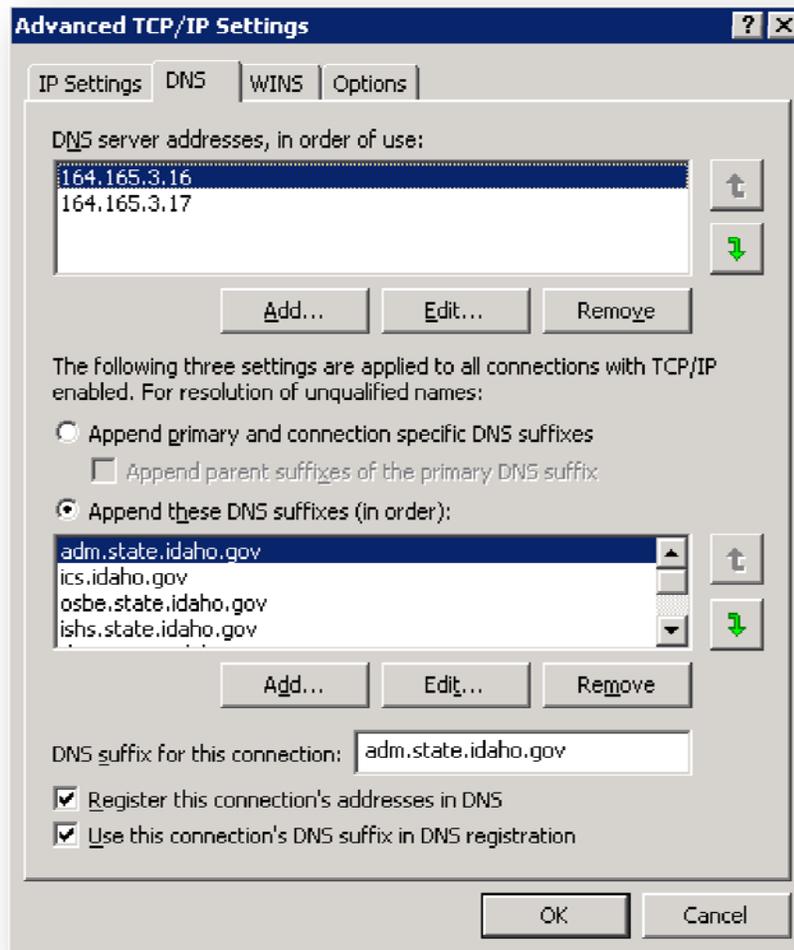
Workstations are updated from the Quest Console Server. The Resource Update Manger responsible for migrating the workstations require the Windows Firewall to be turned off.



Configure DNS and Suffix Settings for Target Domain

DNS forwarding information will be provided to each agency prior to migration. The information provided is to be added to the Source Domains existing DNS configuration.

DNS Suffix Settings need to be added to the TCP/IP properties of each node on the Source domain. This can be accomplished through Group Policy Settings established in the Source Domain prior to migration. ICS.IDAHO.GOV should be added to the DNS Suffix search order of each Source Domain Server and Workstation.



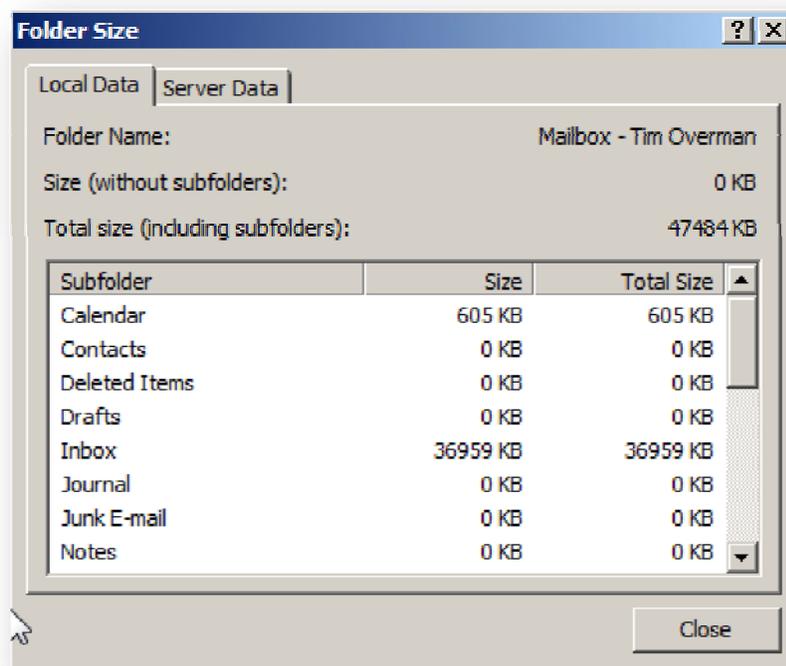
Exchange Servers:

Reduce Email Accounts to 200MB or Less

Source Exchange mailboxes must be less than 200MB in order to migrate to the ICS Exchange system. This requirement provides two benefits; first performance to the user mailbox is greatly increased. Second, the time to migrate each mailbox is decreased.

Users can locate the size of their mailbox in Outlook.

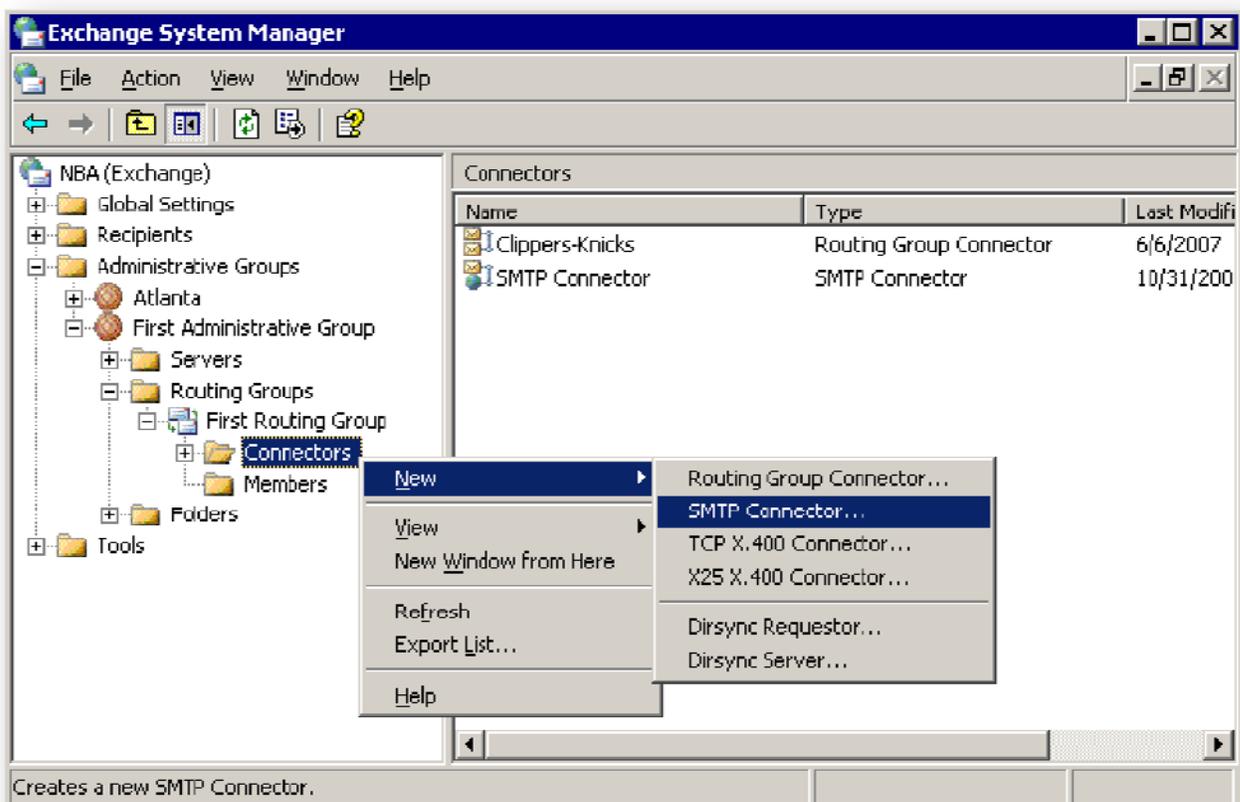
Right-Click on Users Mailbox > Properties > Click Folder Size Button



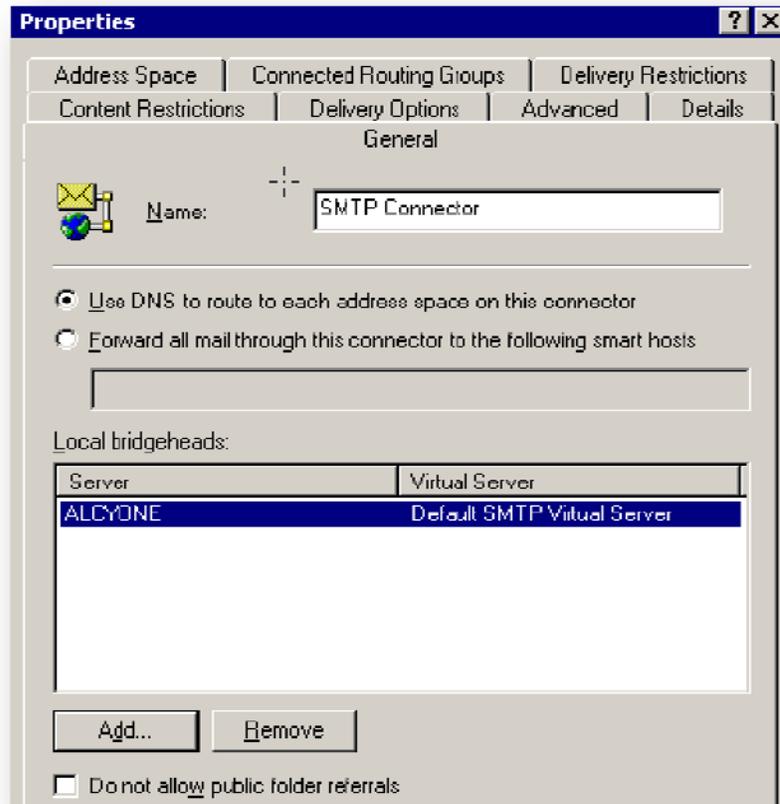
Setup SMTP connectors

Create SMTP connectors between the bridgehead servers of your source to the ICS Exchange organization by taking the following steps:

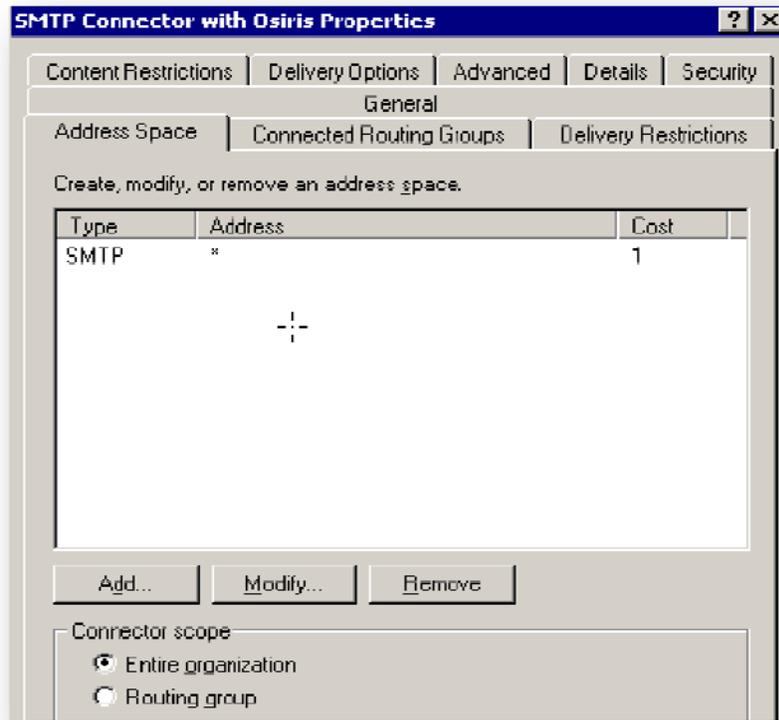
1. In Exchange 2003 System Manager, right-click the **Connectors** node, select **New**, and then select **SMTP Connector**.



2. Go to the **General** tab of the new connector's properties, and click the **Add** button to specify the name for the connector and local bridgehead server. Select the **Use DNS to route to each address space on this connector** option to use DNS to route mail to the address spaces specified for this connector.



3. When Migration Manager for Exchange is configured to use SMTP for mail redirection, mail is forwarded to additional SMTP addresses generated by the Directory Synchronization Agent and based on the address templates you provide when setting up the directory synchronization jobs. Go to the **Address Space** tab and click **Add...** Create the address "SOURCE.QMM" this is the address the migration uses to transfer mail to the ICS domain.

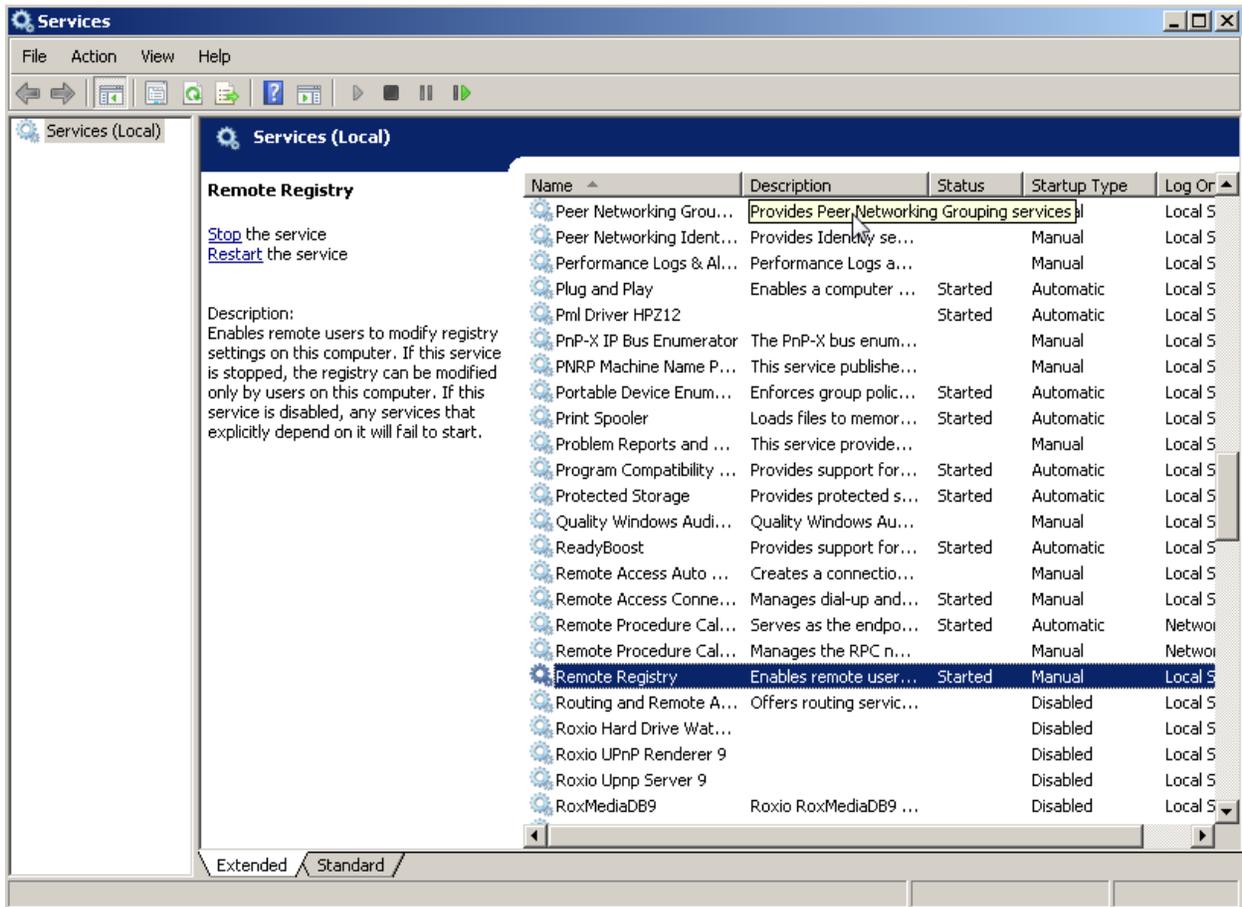


4. Configure other options if needed and click **OK**. This example shows the other options keeping their default values.

Set Group Policies to coincide with Target Doman Policies

Setting	Domain Policy
Account lockout duration	15 minutes
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	15 minutes

Vista Machines must have the “Remote Registry” Service turned on



Desktop may receive temporary profile after conversion

User's workstation has been processed using QMM RUM (Resource Updating Manager), but after a user logs on into the target domain, a new profile is created. Users simply need to restart their workstation to receive updated profile.

PDA resynchronization

Depending on the PDA in use for each environment, these devices may need to be resynchronized to the user's desktop or backend server. Example, Blackberry users will need to have their devices re-connected to the Blackberry Enterprise Server (BES) associated with the ICS Exchange System. As well, users who connect their PDA using Microsoft Active Sync will need to reconnect their device to the correct ICS Exchange addresses. Example, PDA re-points to OWA.ICS.IDAHO.GOV

Outlook Web Access (OWA)

The ICS Outlook Web Access location is new and must be communicated to the end users after their mailbox has been migrated. The new location for OWA is <https://owa.ics.idaho.gov>

This address will take the user to a new logon screen as shown below. The user should enter their user ID as follows. ICS\USER

Microsoft Office Outlook Web Access

Security ([show explanation](#))

This is a public or shared computer

This is a private computer

Use Outlook Web Access Light

I want to change my password after logging on

Domain\user name:

Password:

Connected to Microsoft Exchange
Secured by Microsoft Internet Security and Acceleration Server
© 2006 Microsoft Corporation. All rights reserved.



Migrating Exchange Resource Accounts

The shared resource functionality is greatly changed in the new 2007 Exchange environment. Source Exchange 2003 resources such as; meeting rooms, projectors, shared calendars, do not migrate directly to Exchange 2007. To facilitate the representation of previous Exchange 2003 resources, each shared resource will need to be identified and manually recreated in the Exchange 2007 system prior to the migration of mailbox accounts that dependant of them.



Certification of Agency Readiness

Agency Name _____

This certification signifies that the Department of Administration and the above named agency have completed all of the activities necessary to migrate to the State of Idaho Consolidated Messaging System.

	N/A	In Progress	Complete
Network			
Tasks 1-2			
Servers			
Domain Controllers			
Tasks 1-9			
Exchange Servers			
Tasks 1-6			
SQL Servers			
Tasks 1-3			
File Servers			
Tasks 1-4			
Print Servers			
Task 1			
Active Directory			

Source Domain			
Tasks 1-19			
Name Services			
Tasks 1-7			
Back Office Services			
Tasks 1-3			
Domain Trust (Coordinate with ICS)			
Tasks 1-3			
Workstations			
Desktops and Laptops			
Tasks 1-9			
End User Communications			
Understand and communicate known issues			
Tasks 1-9			

Sign Off:

ICS _____

Agency _____