riverbed

WHITE PAPER

Optimization in a Secure Windows Environment

A guide to the preparation, configuration and troubleshooting of Riverbed® Steelhead® appliances for Signed SMB and Encrypted MAPI

September 2013

OPTIMIZATION IN A SECURE WINDOWS ENVIRONMENT

Introduction

This guide is designed to help the reader create a plan and prepare for all the steps required to configure Riverbed® Steelhead® appliances to optimize in an environment where there are;

- Microsoft Windows Fileservers using Signed SMB, Signed SMB2 and Signed or Encrypted SMB3 for file sharing to Microsoft Windows clients
- Microsoft Exchange Servers providing an Encrypted MAPI communication to Microsoft Outlook clients
- Microsoft Web Servers requiring “per request” Kerberos authentication

Even though the majority of the configuration for these requirements need only be performed on the server-side Steelhead appliance, there are some settings which must also be performed on the client-side Steelhead appliance(s). It is therefore strongly advised to have all the Steelhead appliances operating with a minimum of Riverbed® Optimization System (RiOS®) v6.1.x but preferably RiOS v6.5.x or later. For any environment where there is a requirement for Kerberos authentication between the client and server, a minimum of RiOS v7.0 is needed. For any requirement where there is Signed SMB3 optimization, a minimum of RiOS v8.5 is needed.

As part of your preparation, reference should also be made to the most recent versions of the Riverbed Deployment Guide (both the “Appliance” and “Protocols” editions) and the Riverbed Steelhead Management Console User’s Guide. These manuals contain sections giving further detail and advice on design and configuration for Windows Domain Authentication as well as further explanation of Windows Domain architectures, trust relationships and the reasons for the use of Delegate User and Replication User accounts. These manuals are available for download via the Riverbed Technology support website (support.riverbed.com).

This document does not cover the settings required for optimization of Outlook Anywhere.

Structure of this Guide

This guide begins with a brief overview of the possible configuration options and is then organized into four main sections which explain the steps for configuration.
Section 1 is designed to cover all the configuration tasks needed when client-server authentication can be performed via delegation using a Delegate User account.
Section 2 covers all the configuration tasks, when the client-server authentication requires Kerberos from end to end.
Section 3 covers all the configuration tasks that enable the server-side Steelhead appliance to integrate with the Windows Active Directory (AD) environment and provide NTLM pass-through authentication.
The final section is a series of appendices that contain additional information which may be of use generally.
Therefore it is strongly recommended to read through the entire document including the appendices before starting the overall configuration.
Please note that this document includes screenshots of example configuration steps. While every attempt has been made to ensure accuracy, different versions of RiOS may have slightly different page layouts in the Management Console Graphical User Interface (GUI) to those shown in this guide.

What configuration options are available and how do I choose?

There are several components within a secure Windows environment and the combinations of these components often dictate what configuration options are available.
The main components that need to be considered are;

- Windows client operating system – for example: WinXP, Vista, Windows 7, Windows 8
- Windows domain level – for example: 2003, 2008, 2008-R2 native, mixed-mode
- Authentication mechanism – for example; NTLM only, Kerberos only, auto-negotiation NTLM or Kerberos
- RiOS version of client-side and server-side Steelhead

While the permutations of these components, and others, can lead to a number of configuration options, it is quite often the case that one of three basic configurations will stand out as the better choice.

Kerberos Constrained Delegation

Historically, the first option is to use a Delegate User account and authenticate using Kerberos Constrained Delegation. This option requires the most administrative effort on behalf of both the Steelhead appliance and Windows AD administrators. In the past, this option has been the most frequently used because it is suitable for a wide variety and combination of client and server OS versions. But following the release of RiOS v7.0 one or both of the next two options are recommended due to their simplicity.

Replication User

If the authentication mechanism is required to be Kerberos end to end between the clients and servers then the only option available is to configure the server-side Steelhead appliance to use a Replication User account. End to end Kerberos authentication is the default choice for Windows 7 or Windows 8 clients and Windows 2008 servers or later. But for backwards compatibility, it is quite often the case that clients and servers automatically negotiate to use either NTLM or Kerberos. Because of this reason, it is usually a good idea to configure a replication user and also have the server-side Steelhead appliance join the domain and integrate with Windows AD as described below.

Windows Active Directory Integrated Mode

Generally speaking if the Steelhead appliances are running RiOS v7.0 or later the easiest configuration is to have the server-side Steelhead appliance join the Windows Domain. Depending on the functional level of the Windows domain, the Steelhead appliance joins in one of two modes; Active Directory integrated Windows 2003, or Active Directory integrated Windows 2008. Once joined to the domain, the Steelhead appliance has sufficient privileges to be able to safely and securely communicate with the domain controllers[2]. This communication only occurs to determine the session key in use between the client and server for a connection of signed or encrypted traffic that is to be optimised. The authentication mechanism used in this case is NTLM and is generally described by Microsoft as “Pass-Through Authentication”. NTLM authentication is still the most prevalent authentication mechanism in use in production networks for reasons of backwards compatibility with older Windows clients and servers. If this option satisfies the authentication requirements there is no need to configure a replication user or delegation user.

If one of the above three options is suitable for your needs, then simply follow the guidelines provided in the relevant section.

Section 1 – Authentication via Kerberos Constrained Delegation
Section 2 – End to end Kerberos authentication
Section 3 – Integrating the server-side Steelhead with Active Directory

Remember that combinations of these three options may be possible. For example, it is possible to have the server-side Steelhead appliance integrate with AD and also be configured with a replication user account. In this way, the server-side Steelhead appliance would be able to work with both end-to-end Kerberos and NTLM authentication automatically choosing the correct method as needed. It is the combination of these two options which is strongly recommended since they cover the majority of deployment scenarios in production use today. To put it another way, sections 2 and 3 are most likely the ones you will need.

Automatic configuration

Starting with RiOS v8.5, there is the ability to configure a lot of the settings described in this document by using the Domain Auth “Easy Config” and “Auto Config” widgets. The Domain Auth Easy Config widget is a single point of configuration allowing the Steelhead appliance administrator to enter some Active Directory details along with desired optimization requirements. Then by pressing a button, the widget completes the join domain, customizes the delegate user or replication user account settings in AD and selects the correct Steelhead appliance optimization settings for relevant signed/encrypted SMB versions and encrypted MAPI.

It is still the Steelhead appliance administrator’s responsibility to decide which settings are required. The Domain Auth Easy Config widget will not automatically choose the correct settings, but once the settings are selected, the widget will do all the configuration tasks automatically. This can significantly reduce the number of manual tasks required thereby minimizing the potential for typographical errors. The Domain Auth Easy Config widget provides feedback in the form of an activity log as the tasks progress to completion.

[2] If you configure the Steelhead appliance to join with Windows 2003 mode or Windows 2008 mode, it does not provide any Windows domain controller functionality to any machines in the domain, does not respond to requests, does not advertise itself as a domain controller and does not register any SRV records. In addition, the Steelhead appliance does not perform any replication nor hold any AD objects. For more details, consult the relevant section of the Riverbed Deployment Guide – Protocols edition.

In each of the configuration sections (sections 1, 2 and 3) of this document, all the manual tasks are described. If you are planning to use the Domain Auth Easy Config widget, a few manual tasks are still needed to ensure the widget is successful. At the beginning of each section is a list of the tasks needed before using Domain Auth Easy Config.
For the reader who would like to take a quick look at the graphical interface of the widget, there is an example screenshot in the appendix of this document. Detailed information on how to use the widget is described in the Riverbed Steelhead Management Console User Guide for RiOS v8.5.

Section 1 – Authentication via Kerberos Constrained Delegation

Overview of required configuration tasks for authentication via delegation

There are a number of tasks to be performed and parameters to be configured. They are listed here;

1.1 Create a Delegate User account

1.2 Associate the Delegate User with CIFS/Exchange service(s) and enable delegation for the user

1.3 Configure Delegate User permissions to operate only with the chosen services

1.4 Join server-side Steelhead appliance to Windows Domain

1.5 Add Delegate User name to server-side Steelhead appliance configuration

1.6 Configure the Steelhead appliance to optimize Signed SMB and Encrypted MAPI

Some of these steps will require either administrator group level access to a Windows Domain controller or admin level access to a Riverbed Steelhead appliance. Therefore the appropriate personnel with the relevant access privileges will need to be on hand to perform the tasks. Administrator credentials are not stored on any Steelhead appliance. While these six steps are considered mandatory for the success of an install, there may be other steps required for particular requirements like, one-way trusts, alternative Organizational Units, password expiration, etc. Information on these additional items is to be found in the appendices of this document.

If you are planning to use the Domain Auth widgets, complete the following tasks first…..
1.1 – Create Delegate User account
1.4 – Join the server-side Steelhead appliance to the Windows Domain
1.5 – Add Delegate User name to server-side Steelhead appliance.
1.6 – Configuration of client-side and server-side Steelhead appliance(s) for signed SMB and encrypted MAPI.
DNS and NTP configuration as outlined in Table 1-4-1
Once the above tasks are successfully completed, use the “Configure Delegation Account” and “Add Delegation Servers” widgets. Using these two widgets will automatically complete tasks 1.2 and 1.3.

Performing the configuration tasks

1.1 - Create a Delegate User account

In the Windows Active Directory environment, (for example, using Windows administration tools on the Domain Controller) create a user in the same domain that the Exchange server, or File Server, is a member of.
Choose, *Active Directory Users and Computers* > *Domain Name* > *Users* and create the user (for example, with the name “delegate_rvbd”). Alternatively, you can select an existing user account.

Note: The same Delegate User account can be used for any Exchange servers and File servers in the domain.

Just like any other Windows resource, the server-side Steelhead appliance can only join one domain. If there are other application servers in other Windows Domains at the same location it is possible for the same Steelhead appliance to optimize traffic to/from these other servers. To enable this, a separate Delegate User will need to be created in each of the domains. All of the domains

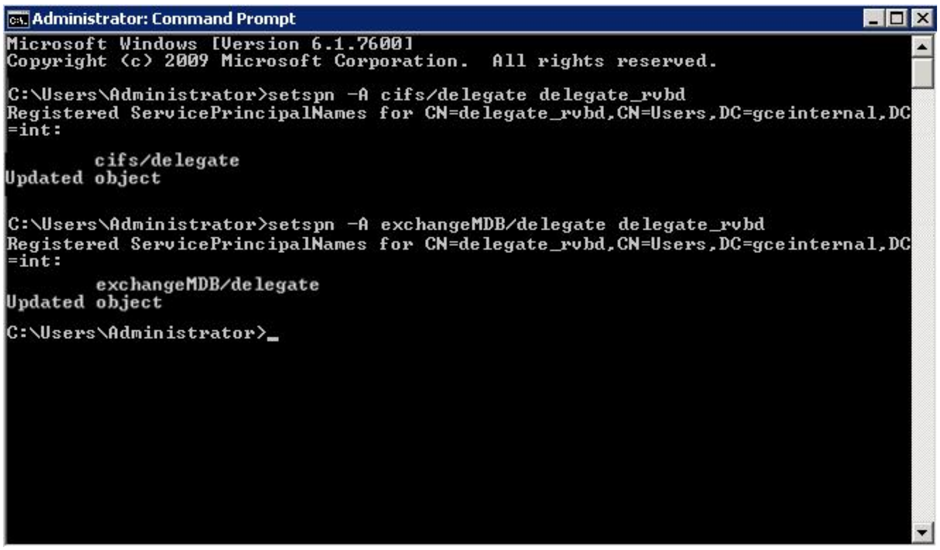
involved will need to be linked by 2-way, bi-directional trust relationships.
All of these Delegate Users will then be entered into the server-side Steelhead appliance configuration as part of this exercise.

1.2 - Associate the Delegate User with the CIFS or Exchange service and enable delegation for the user

Still on the Windows Domain Controller, create a Service Principal Name (SPN) for the delegate user using the *setspn.exe* command-line tool. Once the setspn command has been executed for the delegate user, it makes the “Delegation” configuration tab available in the user account properties. It is via this configuration tab that delegation is enabled for the delegate user. The Windows support tools must be installed on the Domain Controller in order for the setspn.exe utility to be available. The Windows Server 2003 SP1 Support Tools product CD includes this tool, or you can download it from the Microsoft Download Center. With Windows Server 2008 or later, the setspn.exe tool is installed by default.
To access the setspn.exe tool, open a command window (cmd) on the Domain Controller. Then use the following command syntax to add an SPN for the Delegate User

```
    C:\> setspn –A <service name>/delegate <delegate user name>
```

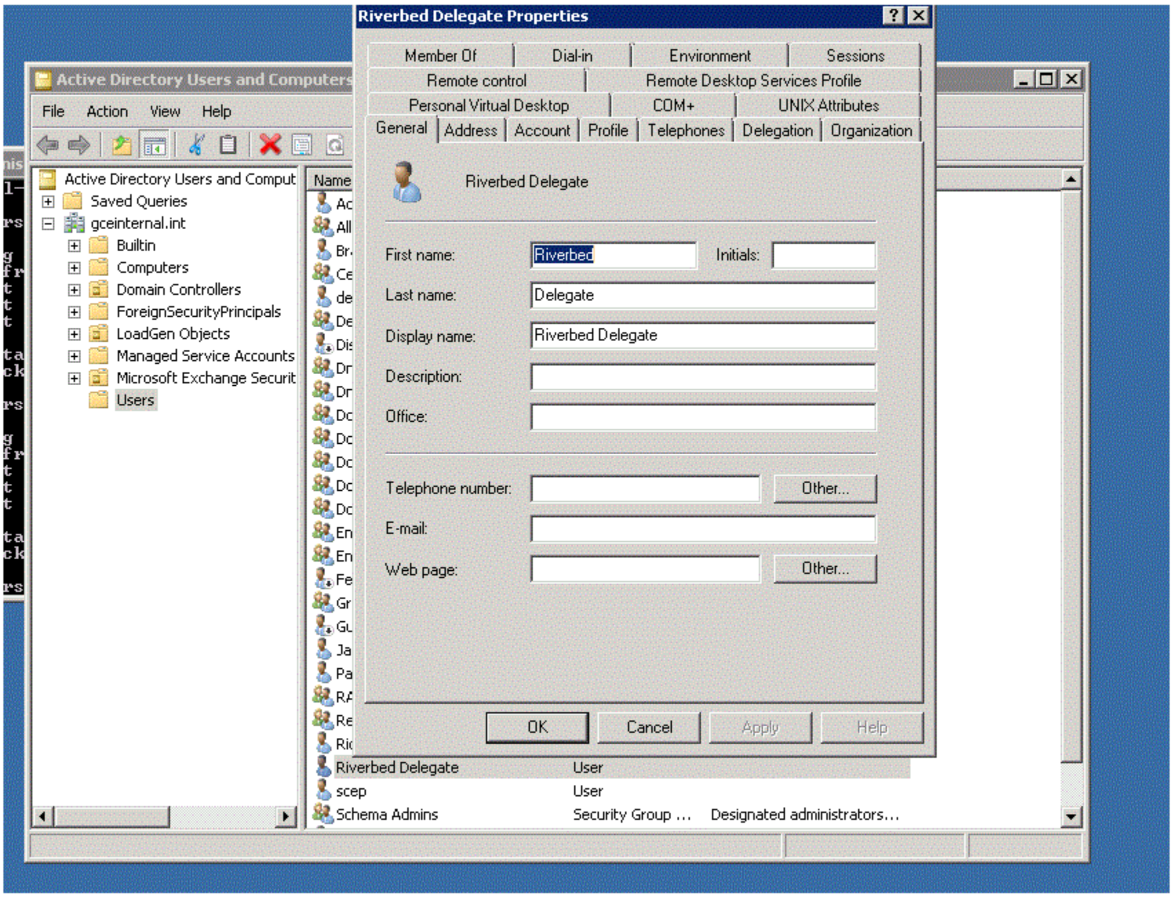
Where `<service name>` is either `cifs` for signed SMB, or `exchangeMDB` for encrypted MAPI, and `<delegate user name>` is the name of the Delegate User created in the previous step for example `delegate_rvbd.`
Figure 1-2-1 shows an example screenshot of running the setspn command for both types of service.



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>setspn -A cifs/delegate delegate_rvbd
Registered ServicePrincipalNames for CN=delegate_rvbd,CN=Users,DC=gceinternal,DC
=int:
        cifs/delegate
Updated object

C:\Users\Administrator>setspn -A exchangeMDB/delegate delegate_rvbd
Registered ServicePrincipalNames for CN=delegate_rvbd,CN=Users,DC=gceinternal,DC
=int:
        exchangeMDB/delegate
Updated object

C:\Users\Administrator>_
```

Figure 1-2-1: setspn screenshot

1.2.1 Returning to the *Active Directory Users and Computers* > *Domain Name* > *Users* admin tool that was used in task 1.1, open the Properties for the user and select the “Delegation” tab



Riverbed Delegate Properties

Riverbed Delegate

First name: Riverbed Initials:

Last name: Delegate

Display name: Riverbed Delegate

Description:

Office:

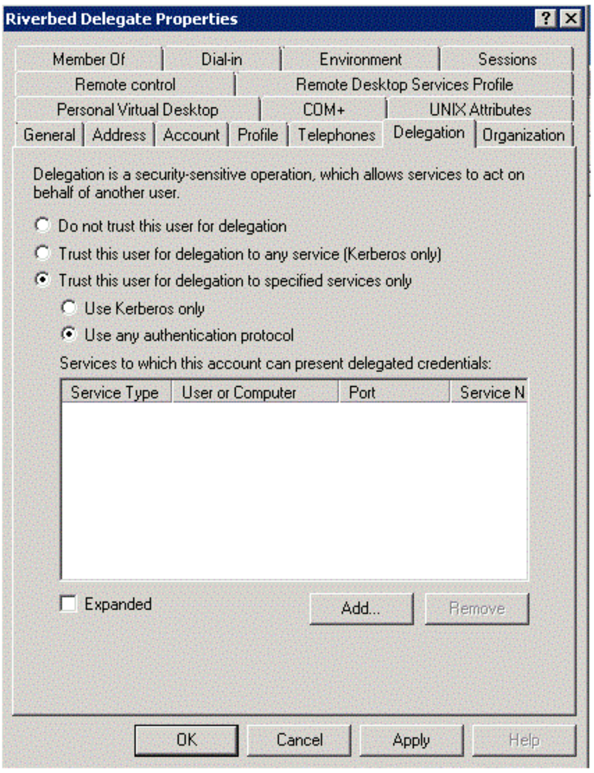
Telephone number:

E-mail:

Web page:

Riverbed Delegate	User	
scep	User	
Schema Admins	Security Group ...	Designated administrators...

Figure 1-2-2: Delegate User properties



Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this user for delegation
○ Trust this user for delegation to any service (Kerberos only)
● Trust this user for delegation to specified services only
○ Use Kerberos only
● Use any authentication protocol

Services to which this account can present delegated credentials:

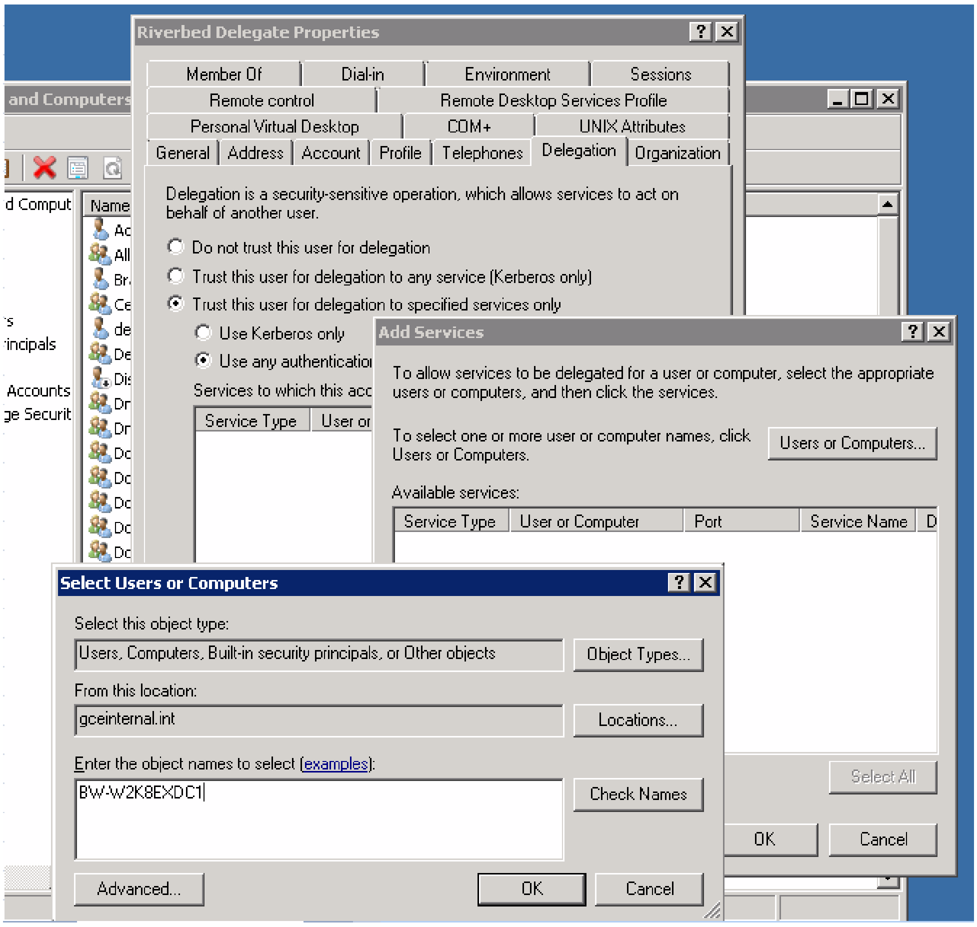
□ Expanded

Figure 1-2-3: Delegation tab

1.2.2 Enable the two settings; "Trust this user for delegation services to specified services only" and "Use any authentication protocol"

At this point the Delegate User is ready to be used. If the requirement is for "Manual Delegation", the Service field in the lower half of this Delegation tab needs to be populated with a list of all the signed SMB, signed SMB2, signed SMB3 and encrypted Exchange servers for this domain. This can be done using the "Add" button.
If Auto Delegation is to be used, this list does not need to be populated, however, due to the way that this Windows admin tool works, it is not possible to select "Apply" and "OK" to close this Properties tool without adding at least one service. Therefore the next steps must be performed at least once to add a service regardless of whether Manual or Auto delegation is to be used.

1.2.3 For Auto delegation, the easiest thing to do is choose any one of the servers. In this example, we will select a signed SMB (cifs) server called BW-W2K8EXDC1.



Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this user for delegation

○ Trust this user for delegation to any service (Kerberos only)

● Trust this user for delegation to specified services only

○ Use Kerberos only

● Use any authenticatio

Services to which this acc

To allow services to be delegated for a user or computer, select the appropriate users or computers, and then click the services.

To select one or more user or computer names, click Users or Computers.

Available services:

Service Type	User or Computer	Port	Service Name	D

Select this object type:
Users, Computers, Built-in security principals, or Other objects

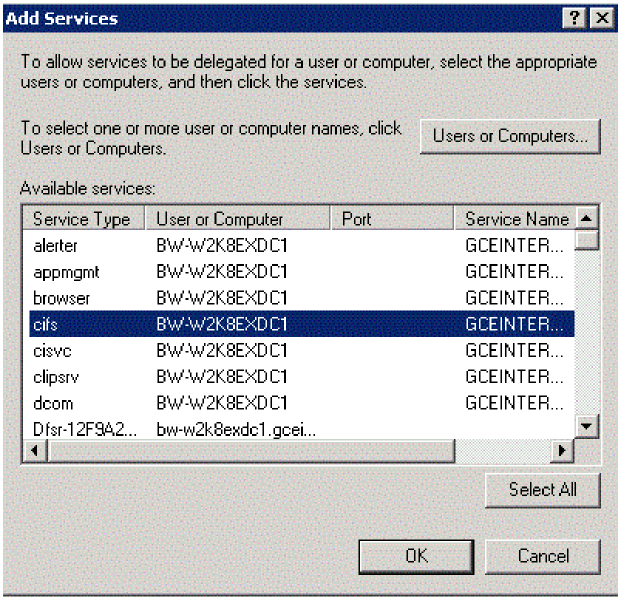
From this location:
gceinternal.int

Enter the object names to select (examples):
BW-W2K8EXDC1

Figure 1-2-4 Selecting server

1.2.4 As shown in Figure 1-2-4, select “Add” in the Delegation tab, then “Users or Computers”.

1.2.5 Enter the hostname of the server, in this example it is called BW_W2K8EXDC1



To allow services to be delegated for a user or computer, select the appropriate users or computers, and then click the services.

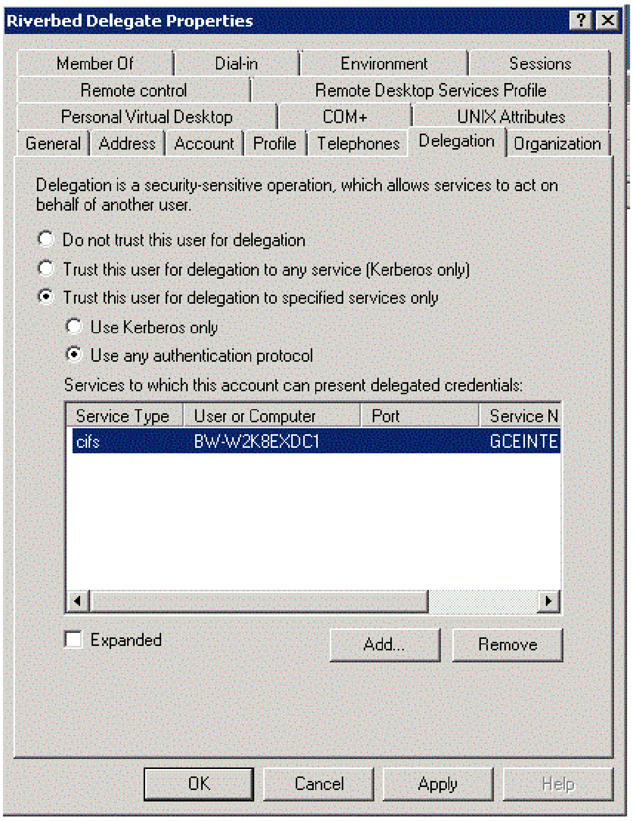
To select one or more user or computer names, click Users or Computers.

Available services:

Service Type	User or Computer	Port	Service Name
alerter	BW-W2K8EXDC1		GCEINTER...
appmgmt	BW-W2K8EXDC1		GCEINTER...
browser	BW-W2K8EXDC1		GCEINTER...
cifs	BW-W2K8EXDC1		GCEINTER...
cisvc	BW-W2K8EXDC1		GCEINTER...
clipsrv	BW-W2K8EXDC1		GCEINTER...
dcom	BW-W2K8EXDC1		GCEINTER...
Dfsr-12F9A2...	bw-w2k8exdc1.gcei...		

Figure 1-2-5: selecting “cifs” service

1.2.6 Select the “cifs” service (Figure 1-2-5), click OK, and the task is complete as shown in Figure 1-2-6.



Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this user for delegation
○ Trust this user for delegation to any service (Kerberos only)
● Trust this user for delegation to specified services only
○ Use Kerberos only
● Use any authentication protocol

Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service N
cifs	BW-W2K8EXDC1		GCEINTE

□ Expanded

Figure 1-2-6: Service added to Delegation tab

1.3 - Configure Delegate User permissions to automatically delegate only with the chosen services

Still on the Windows Domain Controller, use the Group Policy Management tool to add the Delegate user to the Group Policy Object (GPO) for the domain.

1.3.1 Navigate to *Start Menu* > *Administrative Tools* > *Group Policy Management Editor*

1.3.2 Navigate to the Domain Controllers Policy.

1.3.3 Open the Default Domain Controller Policy or your policy for the domain controllers.

1.3.4 Navigate down through *Computer Configuration* > *Policies* > *Windows Settings* > *Security Settings* > *Local Policies*

1.3.5 Select “User Rights Assignment”

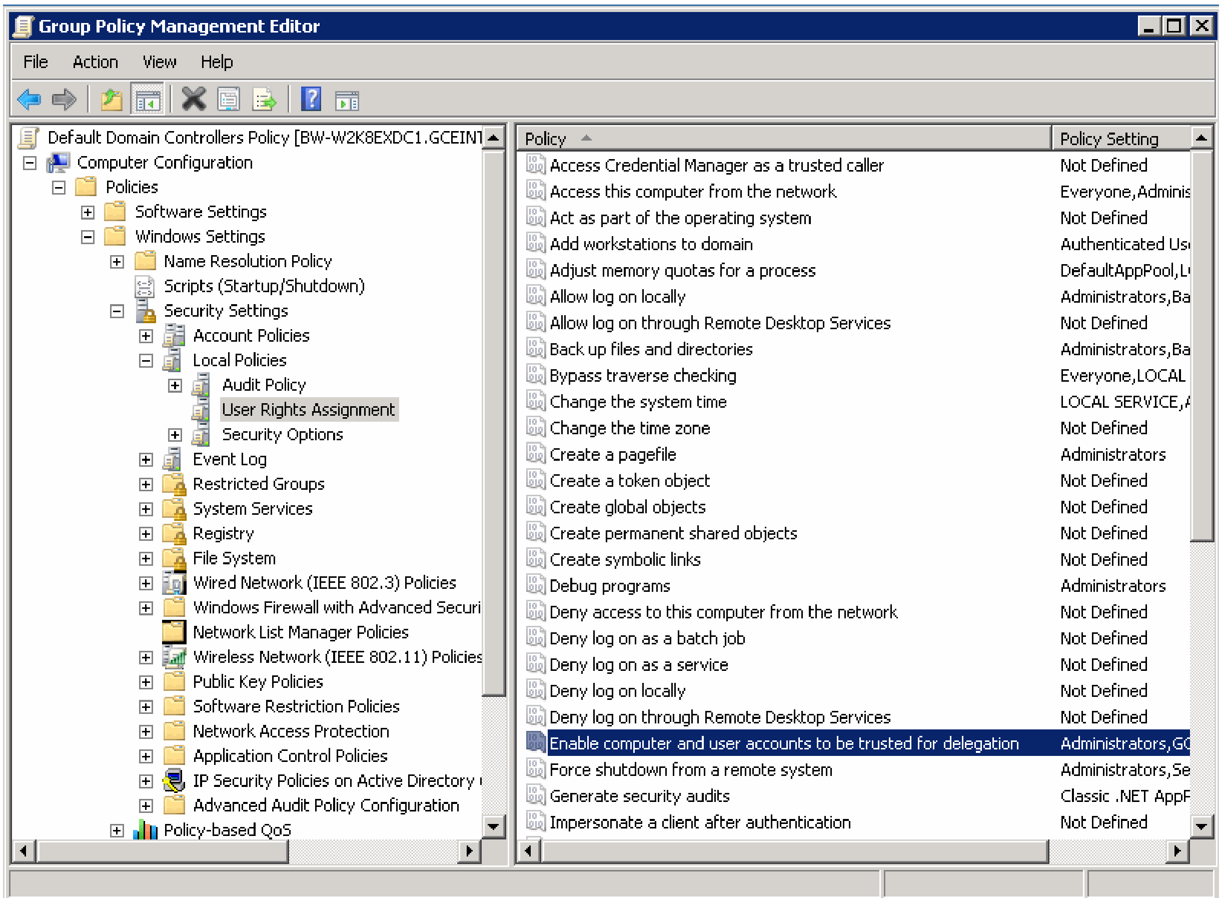
1.3.6 In the right-hand window, select and right-click on “Enable computer and user accounts to be trusted for delegation” to open the properties dialogue box.

1.3.7 In the *Security Policy Setting* tab, select “Add User or Group”

1.3.8 Enter the Delegate User name into the “User and group names” field.

1.3.9 Click “OK” out of the Group Policy Management tool.

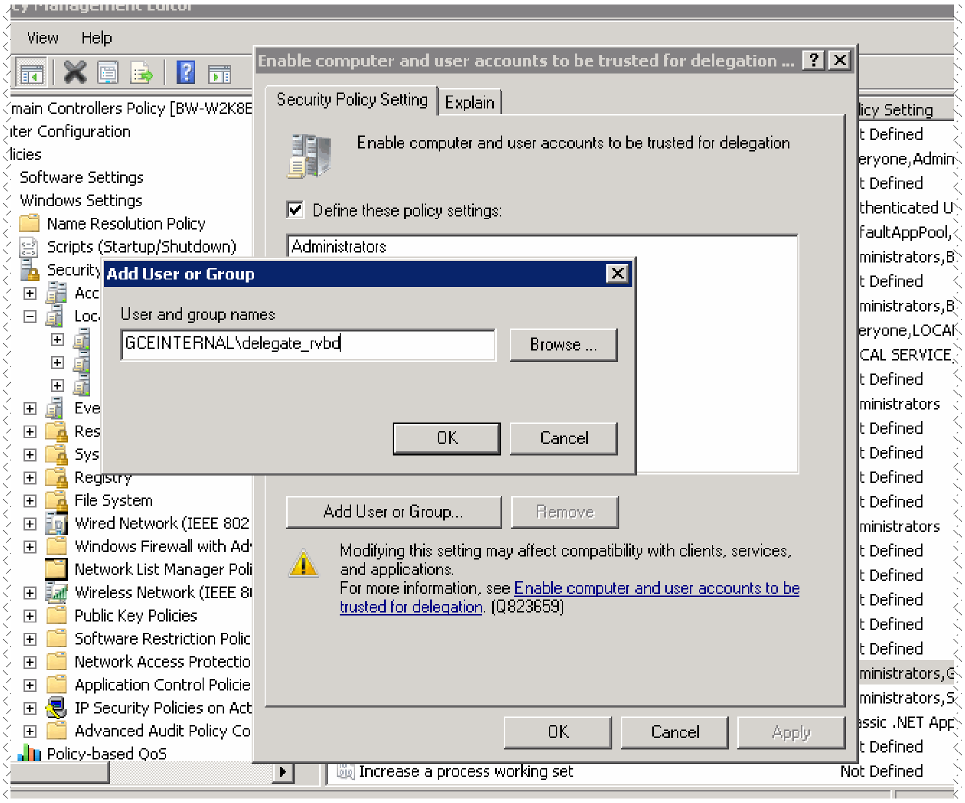
Figures 1-3-1, 1-3-2a and 1-3-2b below show an example series of screenshots for the above sequence of steps.



- Default Domain Controllers Policy [BW-W2K8EXDC1.GCEINT
  - Computer Configuration
    - Policies
      - Software Settings
      - Windows Settings
        - Name Resolution Policy
        - Scripts (Startup/Shutdown)
        - Security Settings
          - Account Policies
          - Local Policies
            - Audit Policy
            - User Rights Assignment
            - Security Options
          - Event Log
          - Restricted Groups
          - System Services
          - Registry
          - File System
          - Wired Network (IEEE 802.3) Policies
          - Windows Firewall with Advanced Securi
          - Network List Manager Policies
          - Wireless Network (IEEE 802.11) Policies
          - Public Key Policies
          - Software Restriction Policies
          - Network Access Protection
          - Application Control Policies
          - IP Security Policies on Active Directory (
          - Advanced Audit Policy Configuration
        - Policy-based QoS

Policy	Policy Setting
Access Credential Manager as a trusted caller	Not Defined
Access this computer from the network	Everyone,Adminis
Act as part of the operating system	Not Defined
Add workstations to domain	Authenticated Us
Adjust memory quotas for a process	DefaultAppPool,L
Allow log on locally	Administrators,Ba
Allow log on through Remote Desktop Services	Not Defined
Back up files and directories	Administrators,Ba
Bypass traverse checking	Everyone,LOCAL
Change the system time	LOCAL SERVICE,A
Change the time zone	Not Defined
Create a pagefile	Administrators
Create a token object	Not Defined
Create global objects	Not Defined
Create permanent shared objects	Not Defined
Create symbolic links	Not Defined
Debug programs	Administrators
Deny access to this computer from the network	Not Defined
Deny log on as a batch job	Not Defined
Deny log on as a service	Not Defined
Deny log on locally	Not Defined
Deny log on through Remote Desktop Services	Not Defined
Enable computer and user accounts to be trusted for delegation	Administrators,G
Force shutdown from a remote system	Administrators,Se
Generate security audits	Classic .NET AppP
Impersonate a client after authentication	Not Defined

Figure 1-3-1: Group Policy Management tool screenshot



Enable computer and user accounts to be trusted for delegation ...

Security Policy Setting | Explain

Enable computer and user accounts to be trusted for delegation

☑ Define these policy settings:

Administrators

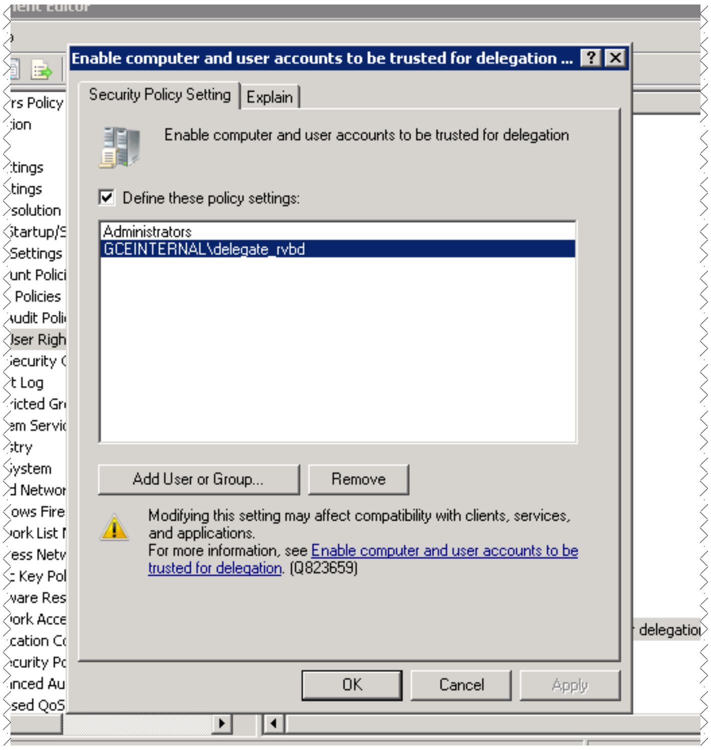
Add User or Group

User and group names

GCEINTERNAL\delegate_rvbd

Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Enable computer and user accounts to be trusted for delegation. (Q823659)

Figure 1-3-2a: Group Policy Management tool screenshots. “Add User”, in progress



Enable computer and user accounts to be trusted for delegation ...

Security Policy Setting | Explain

Enable computer and user accounts to be trusted for delegation

☑ Define these policy settings:

Administrators
GCEINTERNAL\delegate_rvbd

Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Enable computer and user accounts to be trusted for delegation. (Q823659)

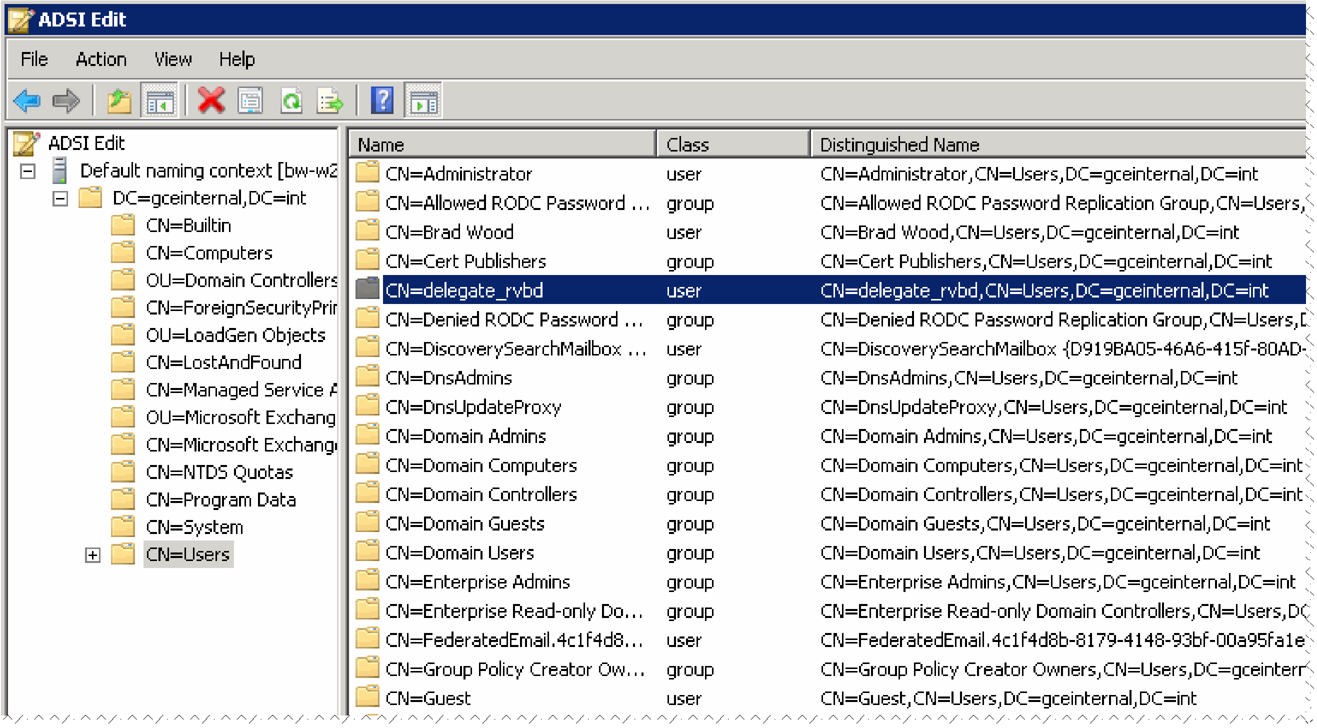
Figure 1-3-2b: Group Policy Management tool screenshots. “Add User”, completed

Continuing the Delegate User configuration, the Delegate User now needs to be granted “Allow” access to modify the Active Directory attribute msDS-AllowedToDelegateTo. Use the Active Directory Service Interfaces (ADSI) edit utility to achieve this.

1.3.1 Choose *Start* > *Run*, and open *adsiedit.msc*.
1.3.2 Select *Default naming context* > *Domain DN* > *CN=Users* > *CN=<Delegate User>*.
1.3.3 Right-click and go to *Properties* on CN=<Delegate User>.
1.3.4 Choose the *Security* tab, click *Advanced* and then click *Add*.
1.3.5 Type the delegate user name and click OK.
1.3.6 Click the *Properties* tab in the *Permission Entry* dialog box.
1.3.7 Add *Allow* access for:

- Read msDS-AllowedToDelegateTo
- Write msDS-AllowedToDelegateTo

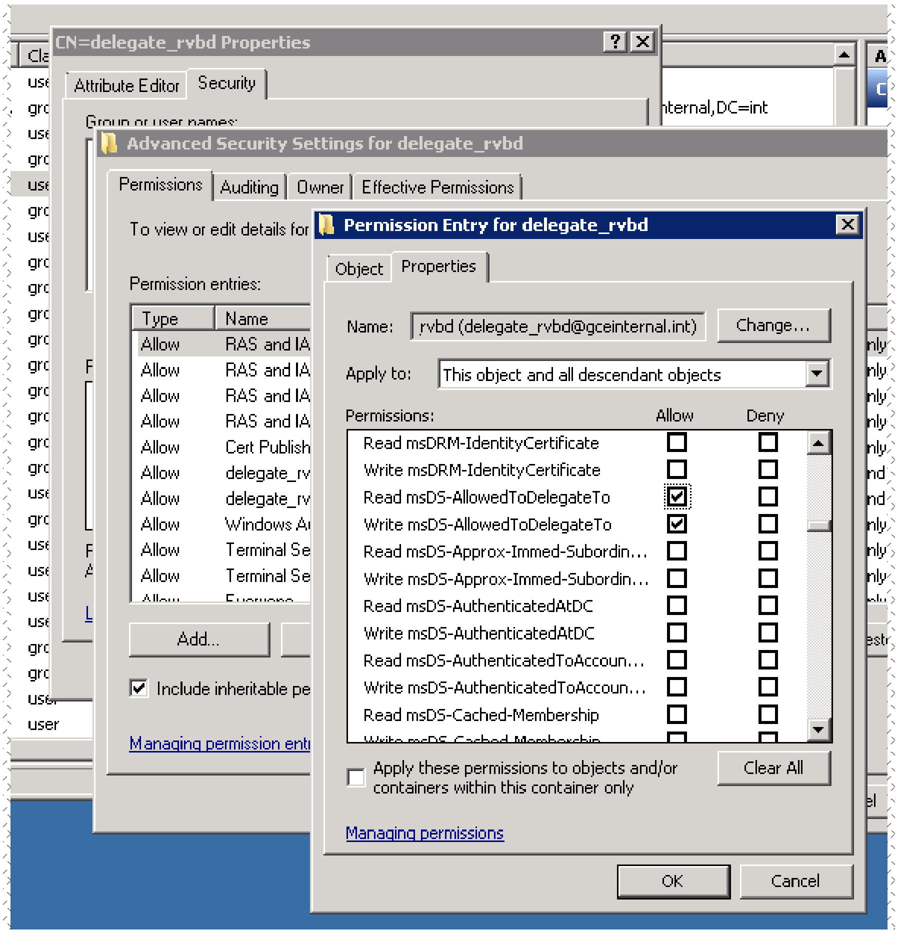
Figures 1-3-3 and 1-3-4 show an example series of screenshots for the above sequence of steps.



ADSI Edit
Default naming context [bw-w2
DC=gceinternal,DC=int
CN=Builtin
CN=Computers
OU=Domain Controllers
CN=ForeignSecurityPrir
OU=LoadGen Objects
CN=LostAndFound
CN=Managed Service A
OU=Microsoft Exchang
CN=Microsoft Exchang
CN=NTDS Quotas
CN=Program Data
CN=System
CN=Users

Name	Class	Distinguished Name
CN=Administrator	user	CN=Administrator,CN=Users,DC=gceinternal,DC=int
CN=Allowed RODC Password ...	group	CN=Allowed RODC Password Replication Group,CN=Users,
CN=Brad Wood	user	CN=Brad Wood,CN=Users,DC=gceinternal,DC=int
CN=Cert Publishers	group	CN=Cert Publishers,CN=Users,DC=gceinternal,DC=int
CN=delegate_rvbd	user	CN=delegate_rvbd,CN=Users,DC=gceinternal,DC=int
CN=Denied RODC Password ...	group	CN=Denied RODC Password Replication Group,CN=Users,D
CN=DiscoverySearchMailbox ...	user	CN=DiscoverySearchMailbox {D919BA05-46A6-415f-80AD-
CN=DnsAdmins	group	CN=DnsAdmins,CN=Users,DC=gceinternal,DC=int
CN=DnsUpdateProxy	group	CN=DnsUpdateProxy,CN=Users,DC=gceinternal,DC=int
CN=Domain Admins	group	CN=Domain Admins,CN=Users,DC=gceinternal,DC=int
CN=Domain Computers	group	CN=Domain Computers,CN=Users,DC=gceinternal,DC=int
CN=Domain Controllers	group	CN=Domain Controllers,CN=Users,DC=gceinternal,DC=int
CN=Domain Guests	group	CN=Domain Guests,CN=Users,DC=gceinternal,DC=int
CN=Domain Users	group	CN=Domain Users,CN=Users,DC=gceinternal,DC=int
CN=Enterprise Admins	group	CN=Enterprise Admins,CN=Users,DC=gceinternal,DC=int
CN=Enterprise Read-only Do...	group	CN=Enterprise Read-only Domain Controllers,CN=Users,DC
CN=FederatedEmail.4c1f4d8...	user	CN=FederatedEmail.4c1f4d8b-8179-4148-93bf-00a95fa1e
CN=Group Policy Creator Ow...	group	CN=Group Policy Creator Owners,CN=Users,DC=gceinterr
CN=Guest	user	CN=Guest,CN=Users,DC=gceinternal,DC=int

Figure 1-3-3: ADSI edit screenshot


CN=delegate_rvbd Properties
Attribute Editor
Security
Advanced Security Settings for delegate_rvbd
Permissions
Auditing
Owner
Effective Permissions
Add...
Managing permission entri

To view or edit details for

Permission entries:

Type	Name
Allow	RAS and IA
Allow	RAS and IA
Allow	RAS and IA
Allow	RAS and IA
Allow	Cert Publish
Allow	delegate_rv
Allow	delegate_rv
Allow	Windows A
Allow	Terminal Se
Allow	Terminal Se

☑ Include inheritable pe

Permission Entry for delegate_rvbd

Name: rvbd (delegate_rvbd@gceinternal.int)

Apply to: This object and all descendant objects

Permissions:

	Allow	Deny
Read msDRM-IdentityCertificate	☐	☐
Write msDRM-IdentityCertificate	☐	☐
Read msDS-AllowedToDelegateTo	☑	☐
Write msDS-AllowedToDelegateTo	☑	☐
Read msDS-Approx-Immed-Subordin...	☐	☐
Write msDS-Approx-Immed-Subordin...	☐	☐
Read msDS-AuthenticatedAtDC	☐	☐
Write msDS-AuthenticatedAtDC	☐	☐
Read msDS-AuthenticatedToAccoun...	☐	☐
Write msDS-AuthenticatedToAccoun...	☐	☐
Read msDS-Cached-Membership	☐	☐

☐ Apply these permissions to objects and/or containers within this container only

Figure 1-3-4: ADSI edit screenshot

If you need help troubleshooting, please also refer to the “Troubleshooting Delegate Users” section in the latest version of the Steelhead Management Console User’s Guide.

Note: Section 1.2 and section 1.3 above will need to be completed for each Delegate User created in each domain.

1.4 - Join the Server-side Steelhead appliance to the Windows Domain

When joining a Steelhead appliance to the Windows Domain, several prerequisites need to be configured to ensure smooth integration. The server-side Steelhead appliance must be able to successfully lookup its hostname in the DNS architecture. Ensure proper DNS entries are created in the DNS server(s) (only an "A record" is required) and the proper DNS servers are configured in the Steelhead appliance. The date and time of the server-side Steelhead appliance must be synchronized with the Windows Domain Controller. This is best accomplished by configuring the Steelhead to use the same NTP server as all the other servers in the domain. You must know the fully-qualified domain name. Table 1-4-1 is provided to collect this information for your environment.

Setting	Value	Step completed
DNS entry for Steelhead appliance		□
DNS server IP address(es)		□
NTP server IPs added to Steelhead configuration		□
Steelhead appliance Computer object created in Domain Controller		□
Fully-qualified Domain Name		

Table 1-4-1: Steelhead appliance prerequisites

Once the prerequisites are completed, join the server-side Steelhead to the AD domain.

To complete this step you will need a Windows user account with rights to join a host to the AD domain. NOTE: This account has nothing to do with the Delegate User account set up in the previous sections. The credentials of the account used to join the domain are not stored on any Steelhead appliance and are only used for the purposes of joining the Steelhead appliance to the domain.

1.4.1 On the server-side Steelhead(s) navigate to Configure > Networking > Windows Domain.

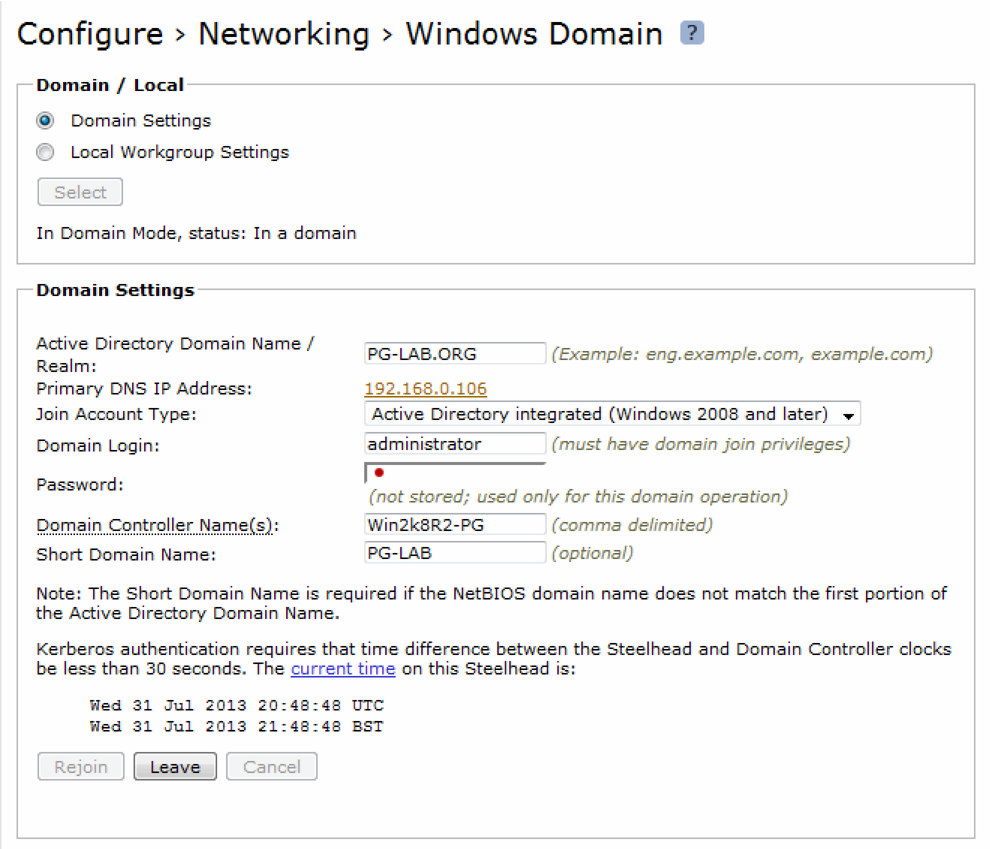
1.4.2 Enter the Active Directory Domain name, user id (of the user account with "Join Domain" privileges), password and optionally the DC name and Short Domain Name.

1.4.3 Select the Join Account Type. Depending on the version of RiOS running on the Steelhead appliance there may be several options available. When configuring for constrained delegation, any "join type" is suitable.

1.4.4 Next click the "Join" button at the bottom of the page and wait for feedback. If an error appears, take appropriate action.

1.4.5 Once successfully joined you will see the statement 'In Domain Mode, status: In a domain' in the top frame of the page.

Figure 1-4-1 shows a successful domain join.



Configure > Networking > Windows Domain ?

Domain / Local

● Domain Settings

○ Local Workgroup Settings

In Domain Mode, status: In a domain

Domain Settings

Active Directory Domain Name / Realm:	PG-LAB.ORG *(Example: eng.example.com, example.com)*
Primary DNS IP Address:	192.168.0.106
Join Account Type:	Active Directory integrated (Windows 2008 and later)
Domain Login:	administrator *(must have domain join privileges)*
Password:	*(not stored; used only for this domain operation)*
Domain Controller Name(s):	Win2k8R2-PG *(comma delimited)*
Short Domain Name:	PG-LAB *(optional)*

Note: The Short Domain Name is required if the NetBIOS domain name does not match the first portion of the Active Directory Domain Name.

Kerberos authentication requires that time difference between the Steelhead and Domain Controller clocks be less than 30 seconds. The current time on this Steelhead is:

```
Wed 31 Jul 2013 20:48:48 UTC
Wed 31 Jul 2013 21:48:48 BST
```

Figure 1-4-1: Example screenshot, Windows Domain page of Steelhead appliance GUI

Further details on joining a Windows Domain are available in the Steelhead Management Console User's Guide in the chapter *Configuring Network Integration Features*.
More recent versions of RiOS include tools to test the configuration settings and ensure a join is successful as well as a status log to show progress and any errors encountered during the join process.

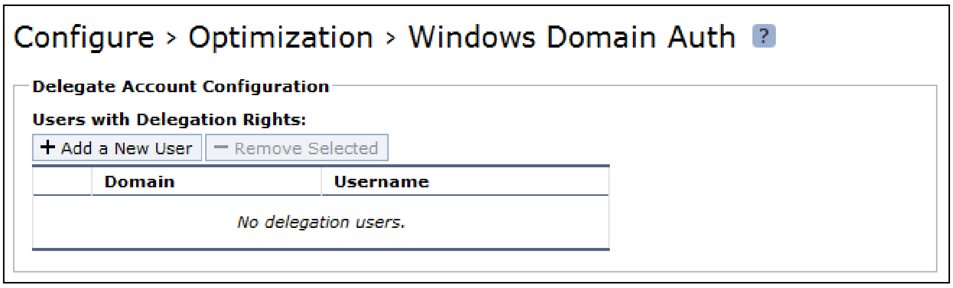
1.5 - Add the Delegate User to the server-side Steelhead appliance

----

NOTE: More recent versions of RiOS include both a collection of command line and graphical tools to help automate these remaining steps. Whether or not the tools are available on the Steelhead appliances you are configuring, the individual steps are shown here.

To add the delegate user to the server-side Steelhead you will need the AD domain name, delegate user name, and password for each delegate user that has been created in each domain. These should have already been created as described in sections 1.1, 1.2 and 1.3 above. Assuming the user(s) have been created, the following steps should then be performed.

1.5.1 On the server-side Steelhead(s) navigate to Configure > Optimization > Windows Domain Auth.



Configure > Optimization > Windows Domain Auth ?

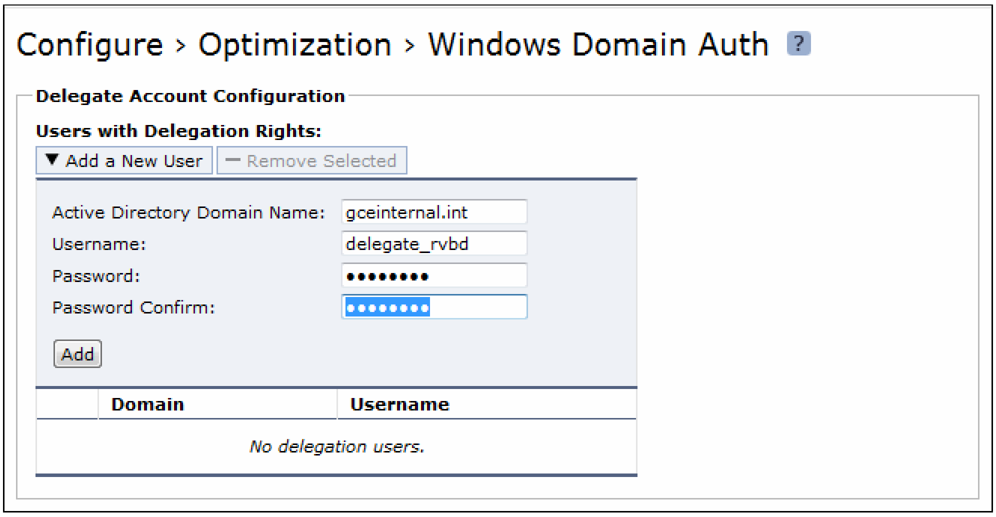
Delegate Account Configuration

Users with Delegation Rights:

Domain	Username
No delegation users.	

Figure 1-5-1: Windows Domain Auth page of Steelhead appliance GUI

1.5.2 Click the ‘Add a New User’ tab. Enter the AD domain, delegate user account name, and password.



Configure > Optimization > Windows Domain Auth ?

Delegate Account Configuration

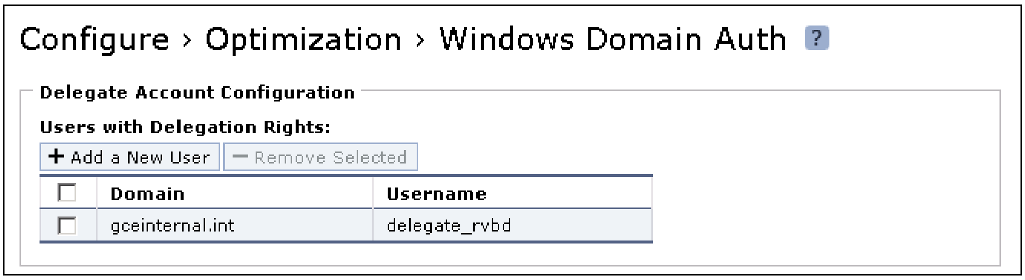
Users with Delegation Rights:

Active Directory Domain Name: gceinternal.int
Username: delegate_rvbd
Password: ••••••••
Password Confirm: ••••••••

Domain	Username
No delegation users.	

Figure 1-5-2: Add New Delegate User section on Windows Domain Auth page of Steelhead appliance GUI

1.5.3 Then click ‘Add’.



Configure > Optimization > Windows Domain Auth ?

Delegate Account Configuration

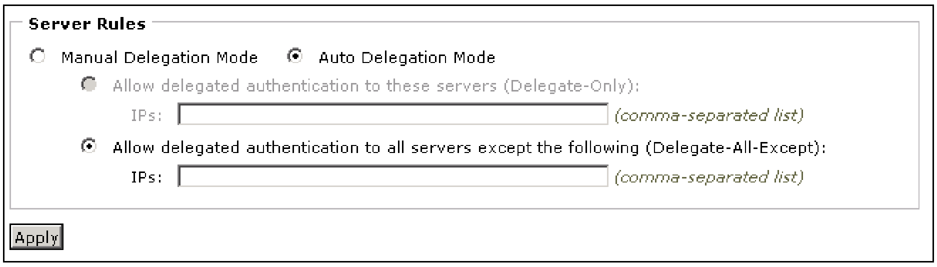
Users with Delegation Rights:

☐	Domain	Username
☐	gceinternal.int	delegate_rvbd

Figure 1-5-3: Add New Delegate User section on Windows Domain Auth page of Steelhead appliance GUI

1.5.4 Repeat steps 1.5.2 and 1.5.3 for each delegate user that has been created ensuring that the correct domain name is included in each case.

1.5.5 In the ‘Server Rules’ section, select the Auto Delegation Mode radio button and enter any server names that should not allow delegated authentication. This field can be left blank unless there is an explicit need to prevent the use of delegation to some servers.



Server Rules

○ Manual Delegation Mode ● Auto Delegation Mode

○ Allow delegated authentication to these servers (Delegate-Only):

IPs: *(comma-separated list)*

● Allow delegated authentication to all servers except the following (Delegate-All-Except):

IPs: *(comma-separated list)*

Figure 1-5-4: Delegation Mode setting on Windows Domain Auth page of Steelhead appliance GUI

1.5.6 Click the 'Apply' button.

1.6 - Configure the Steelhead appliance to optimize Signed SMB and Encrypted MAPI

1.6.1 - Configuration steps for Signed SMB, Signed SMB2 and Signed SMB3

1.6.1.1 On the server-side Steelhead appliance, navigate to Configure > Optimization > CIFS (SMB1).

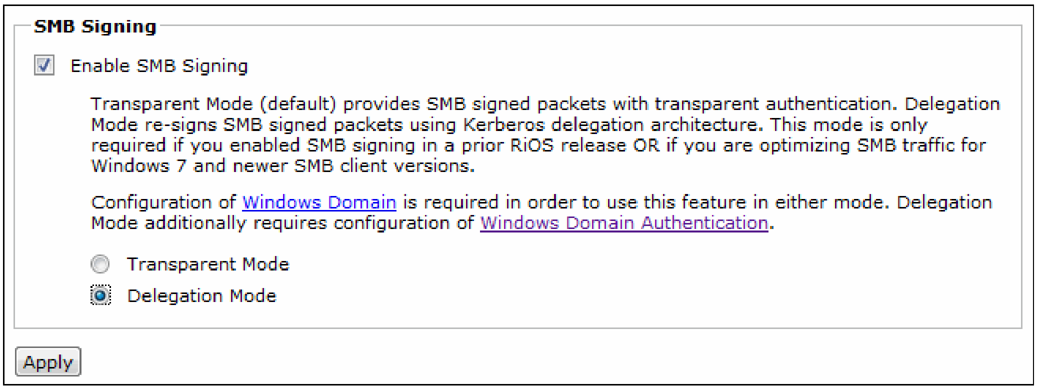
1.6.1.2 For RiOS versions prior to v6.5 if there are connections between Vista/Win7 clients and Windows 2008 R2 servers, select the 'Enable SMBv1 Backward Compatibility' check box. This will revert SMBv2 connections between Vista/Win7 clients and Windows 2008 R2 servers back to SMBv1 allowing the Steelhead appliances to provide full application layer acceleration for CIFS. This will provide a better experience for remote users compared to native SMBv2 without optimization.

Note: Consider upgrading to RiOS v6.5 for native optimization of SMB2. It is also worth noting that SMB2 provides extra security for signing as it uses HMAC SHA-256 instead of MD5.

1.6.1.3 If the Steelhead appliance is running RiOS v6.5 or later, there is a separate SMB2 configuration page located at Configure > Optimization > SMB2. With optimization for SMB2 enabled there is no need to select the "Backward Compatibility" option indicated in step 1.6.1.2 above. If the Steelhead is running RiOS v8.5 or later, there is the option to enable SMB3 optimization. This setting is included on the SMB2 configuration page of the GUI.

1.6.1.4 Under the SMB Signing, check the 'Enable SMB Signing' checkbox.

1.6.1.5 Next select the 'Delegation Mode' radio button.



SMB Signing

☑ Enable SMB Signing

Transparent Mode (default) provides SMB signed packets with transparent authentication. Delegation Mode re-signs SMB signed packets using Kerberos delegation architecture. This mode is only required if you enabled SMB signing in a prior RiOS release OR if you are optimizing SMB traffic for Windows 7 and newer SMB client versions.

Configuration of Windows Domain is required in order to use this feature in either mode. Delegation Mode additionally requires configuration of Windows Domain Authentication.

○ Transparent Mode

● Delegation Mode

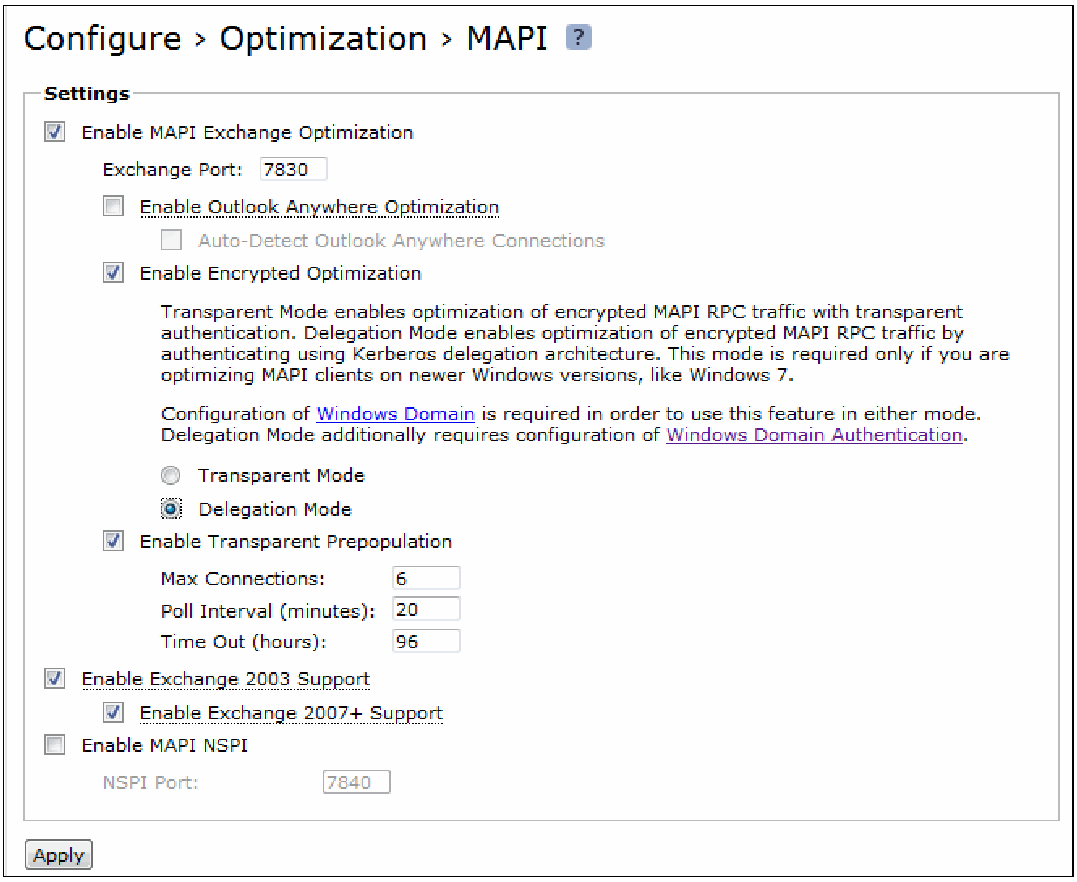
Figure 1.6.1-1: Enable SMB Signing section on CIFS Optimization page of Steelhead appliance GUI

1.6.1.6 Click the 'Apply' button.

1.6.1.7 No changes are needed on the client-side Steelhead appliance(s) unless SMB3 optimization is required. If SMB3 optimization is required, repeat steps 1.6.1.3 through to 1.6.1.6 on the client-side Steelhead appliance(s).

1.6.2 - Configuration steps for Encrypted MAPI

1.6.2.1 On all Steelhead appliances (client-side and server-side) navigate to Configure > Optimization > MAPI.



Configure > Optimization > MAPI

Settings

☑ Enable MAPI Exchange Optimization

Exchange Port: 7830

□ Enable Outlook Anywhere Optimization

□ Auto-Detect Outlook Anywhere Connections

☑ Enable Encrypted Optimization

Transparent Mode enables optimization of encrypted MAPI RPC traffic with transparent authentication. Delegation Mode enables optimization of encrypted MAPI RPC traffic by authenticating using Kerberos delegation architecture. This mode is required only if you are optimizing MAPI clients on newer Windows versions, like Windows 7.

Configuration of Windows Domain is required in order to use this feature in either mode. Delegation Mode additionally requires configuration of Windows Domain Authentication.

○ Transparent Mode

● Delegation Mode

☑ Enable Transparent Prepopulation

Max Connections: 6

Poll Interval (minutes): 20

Time Out (hours): 96

☑ Enable Exchange 2003 Support

☑ Enable Exchange 2007+ Support

□ Enable MAPI NSPI

NSPI Port: 7840

Figure 1.6.2-1: MAPI Optimization page of Steelhead appliance GUI

1.6.2.2 On Steelhead appliances running RiOS earlier than v6.5, select 'Enable MAPI Exchange 2000 Optimization' 'Enable MAPI Exchange 2003 Optimization' and 'Enable MAPI Exchange 2007+ Optimization' checkboxes.

NOTE: On Steelhead appliances running RiOS 7.0 or later, these individual checkboxes have been replaced with a single "Enable MAPI Exchange Optimization" checkbox.

1.6.2.3 Check the 'Enable Encrypted Optimization' checkbox.
1.6.2.4 Select the 'Delegation Mode' radio button.
1.6.2.5 Click the 'Apply' button.
1.6.2.6 Optionally you can configure secure peering between the client-side and server-side Steelhead appliances. Refer to Appendix A.4 of this document for outline guidance. For details, reference the Steelhead Management Console User's Guide section, *Configure Secure Peers*.

1.6.3 – Saving the configuration and restarting the Optimization Service

Finally, save the configuration and restart the optimization service. Do this by clicking 'Save' and 'Restart' in the navigation header. Or, proceed to the Configure > Configurations GUI page to save the configuration with a specific name and then restart the optimization service.

The integration with the Windows domain is now complete.

Once deployed successfully, monitor performance and health of the Steelhead appliance(s) to ensure proper optimization is occurring and full acceleration is being achieved for the appropriate clients and servers. Keep in mind AD and Windows administrators may make changes without notifying the networking team, so remain vigilant. Consider incorporating some of this configuration information into a Change Control Process that enables both the Windows Server Administration team and the Networking team to coordinate future updates and changes.

Appendix B in this document has some outline guidance for troubleshooting as well as pointers to other sources of help.

Section 2 – End to end Kerberos authentication

NOTE: A detailed overview of end to end Kerberos authentication involving Steelhead appliances is provided in the Riverbed Deployment Guide ("Protocols" edition).

Overview of required configuration tasks for end to end Kerberos authentication

There are a number of tasks to be performed and parameters to be configured. They are listed here;

2.1 Create a Replication User account

2.2 Configure the Replication User with limited privileges for replication

2.3 Optional - Configure Password Replication Policy (PRP) settings

2.4 Join server-side Steelhead appliance to Windows Domain

2.5 Add Replication User name to server-side Steelhead appliance configuration

2.6 Configure the Steelhead appliance to optimize Signed SMB Signed SMB2, Signed SMB3, HTTP and Encrypted MAPI

Some of these steps will require either administrator group level access to a Windows Domain controller or admin level access to a Riverbed Steelhead appliance. Therefore the appropriate personnel with the relevant access privileges will need to be on hand to perform the tasks. Administrator credentials are not stored on any Steelhead appliance. While these six steps are considered mandatory for the success of an install, there may be other steps required for particular requirements like, one-way trusts, alternative Organizational Units, password expiration, etc. Information on these additional items is to be found in the appendices of this document.

NOTE: End to end Kerberos authentication requires the Steelhead appliances to be running a minimum of RiOS v7.0.x
For signed SMB and signed SMB2 using Kerberos, only the server-side Steelhead appliance(s) need RiOS v7.0.x but both client-side and server-side Steelheads need this version if encrypted MAPI is in use with Kerberos. Full optimization of signed/encrypted SMB3 requires a minimum of RiOS v8.5 on both client-side and server-side Steelhead appliances.

If you are planning to use the Domain Auth Easy Config widget, complete the following tasks first…..

2.1 – Create a Replication User account,
2.5 – Add Replication User name to server-side Steelhead appliance.
DNS and NTP configuration as outlined in Table 2-4-1

The Domain Auth Easy Config widget will complete tasks 2.2, 2.4 and 2.6 with the exception of any client-side Steelhead appliance configuration. Any configuration on the client-side Steelhead appliance(s), for example enabling encrypted MAPI, will need to be done as a separate task.

Performing the configuration tasks

2.1 - Create a Replication User account

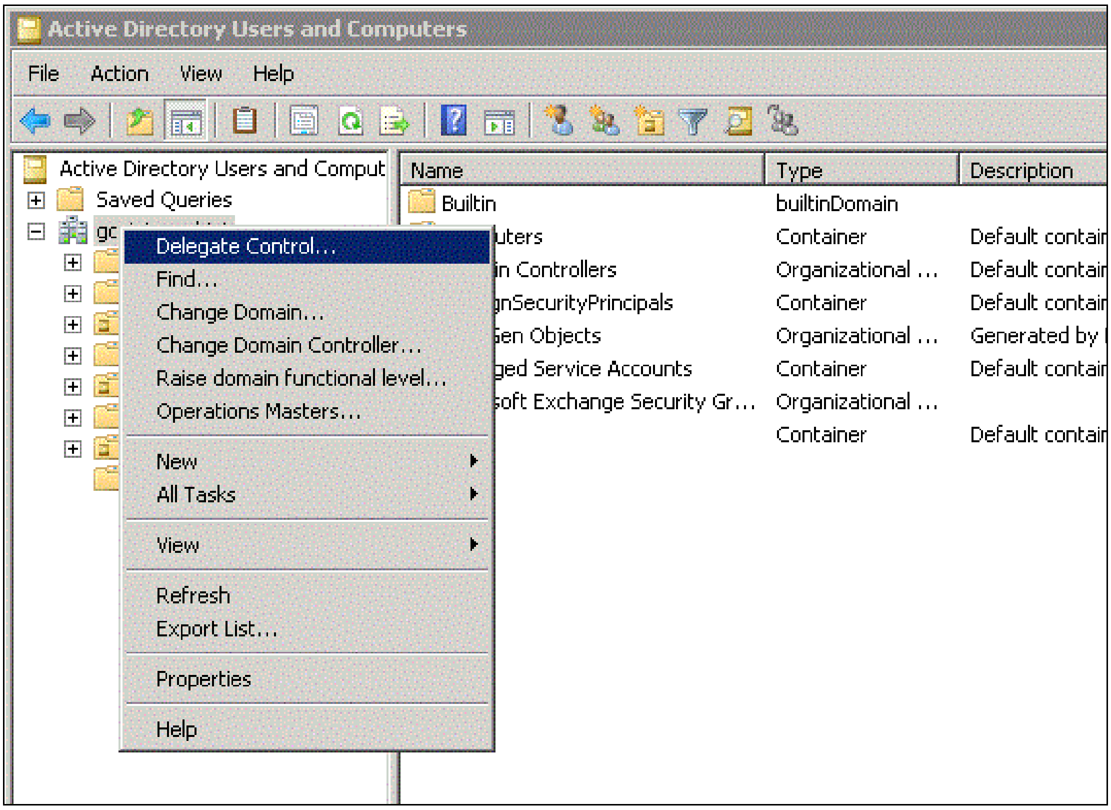
In the Windows Active Directory environment, (for example, using Windows administration tools on the Domain Controller) create a user in the same forest that the application server (Exchange, File-sharing, HTTP) is a member of.
Choose, *Active Directory Users and Computers* > *Domain Name* > *Users* and create the user (for example, with the name "replicate_rvbd"). Alternatively, you can select an existing user account.

Although the server-side Steelhead appliance will only be joining one domain, if there are other application servers in other Windows Domains at the same location which the same Steelhead appliance will be optimizing, then the same replication user account can be used across all domains. All of the domains involved will need to be linked by 2-way, bi-directional trust relationships or a suitable 1-way trust.

2.2 - Configure the Replication User with limited privileges for replication

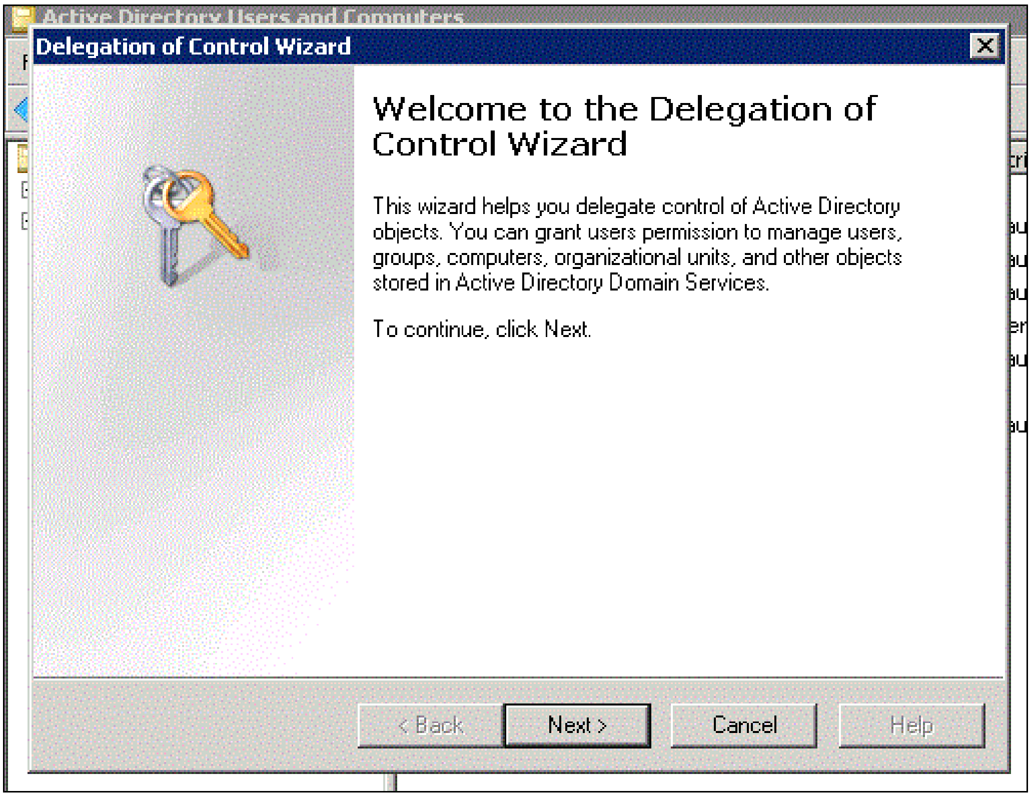
Once the replication user account has been created, it can then be assigned the limited privileges needed to perform replication. This task is performed on the Domain Controller using the "Delegation of Control Wizard". The steps are illustrated in this next section using example screenshots.

2.2.1 – On the Domain Controller, navigate to *Start Menu* > *Administrative Tools* > *Active Directory Users and Computers* then select the domain name where the replicate user account resides.
2.2.2 - "Right-click" on the domain name and select "Delegate Control". This launches the Delegation of Control Wizard.



Name	Type	Description
Builtin	builtinDomain	
uters	Container	Default contai
n Controllers	Organizational ...	Default contai
gnSecurityPrincipals	Container	Default contai
en Objects	Organizational ...	Generated by
ged Service Accounts	Container	Default contai
soft Exchange Security Gr...	Organizational ...	
	Container	Default contai

Figure 2-2-1: Delegate Control


Active Directory Users and Computers
Delegation of Control Wizard
< Back
Next >
Cancel
Help

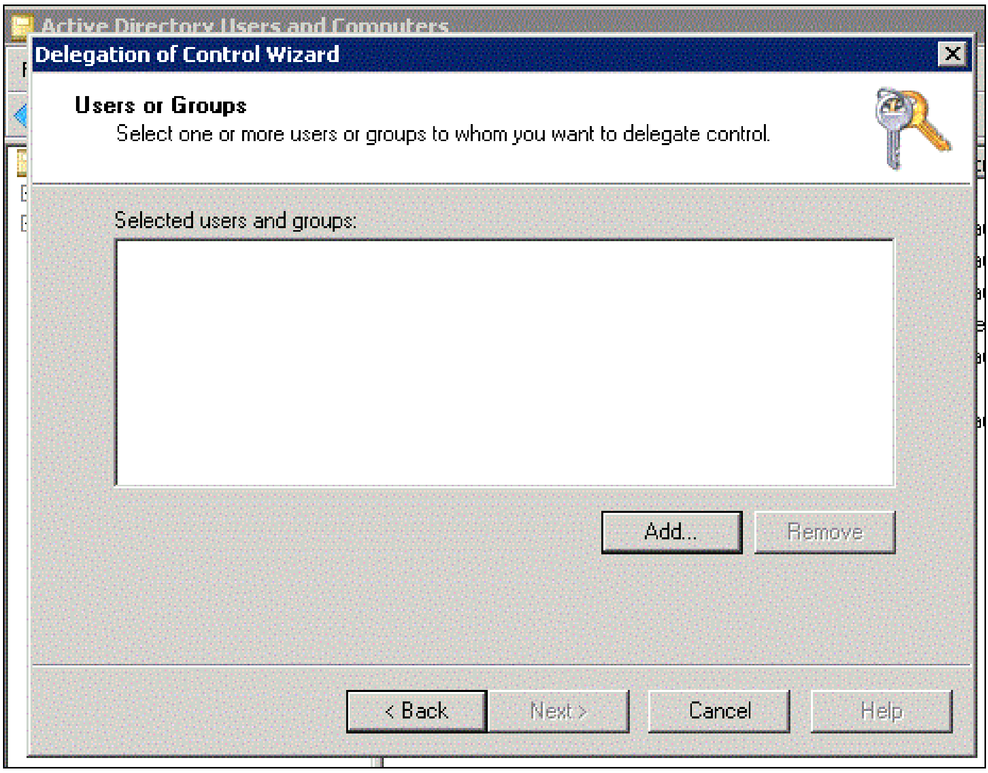
Welcome to the Delegation of Control Wizard

This wizard helps you delegate control of Active Directory objects. You can grant users permission to manage users, groups, computers, organizational units, and other objects stored in Active Directory Domain Services.

To continue, click Next.

Figure 2-2-2: Delegation of Control Wizard

2.2.3 – Click "Next" and "Add" to add the replication account user name as shown in the next three screenshots. Note that the example below includes the replication user account name "replicate_rvbd" in the domain "gceinternal.int". These values may be different for your specific configuration.



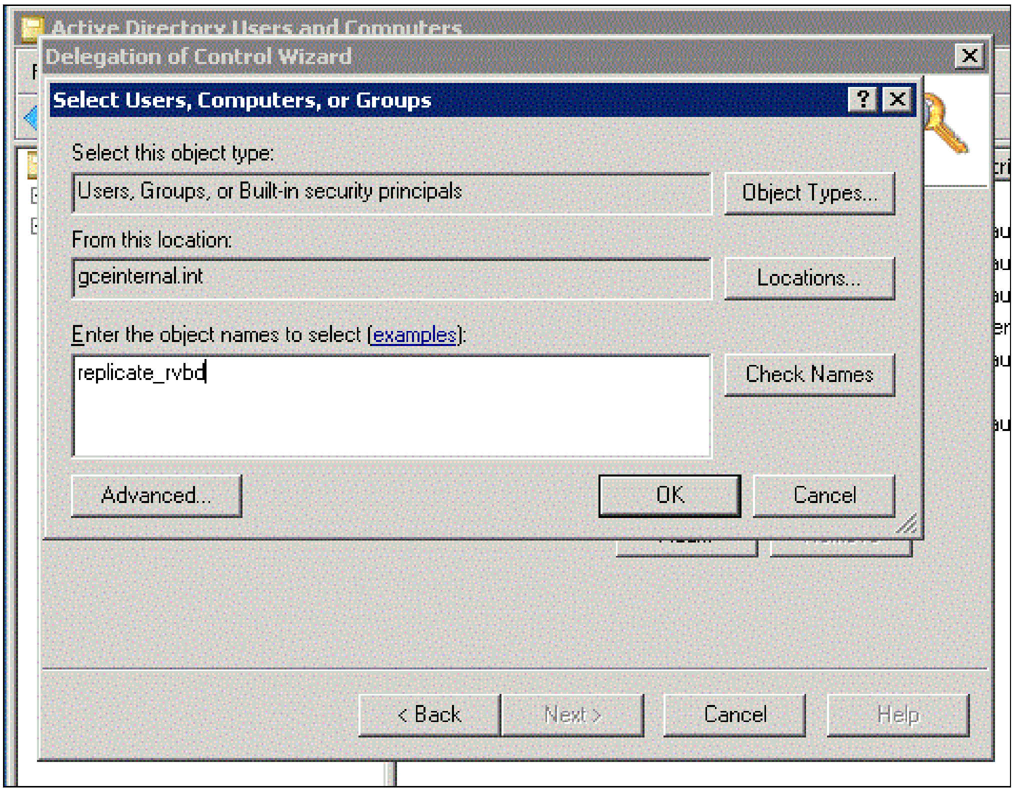
Delegation of Control Wizard

Users or Groups

Select one or more users or groups to whom you want to delegate control.

Selected users and groups:

Figure 2-2-3: Delegation of Control Wizard, Users or Groups



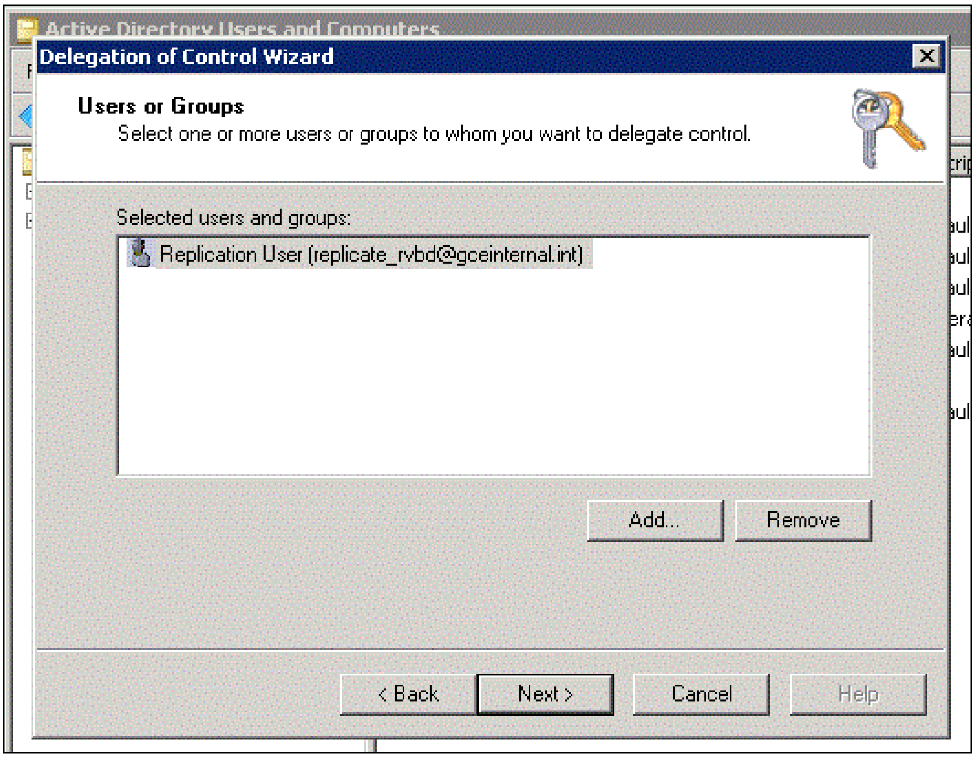
Select Users, Computers, or Groups

Select this object type:
Users, Groups, or Built-in security principals

From this location:
gceinternal.int

Enter the object names to select (examples):
replicate_rvbd

Figure 2-2-4: Delegation of Control Wizard, add replication user account


Active Directory Users and Computers
Delegation of Control Wizard

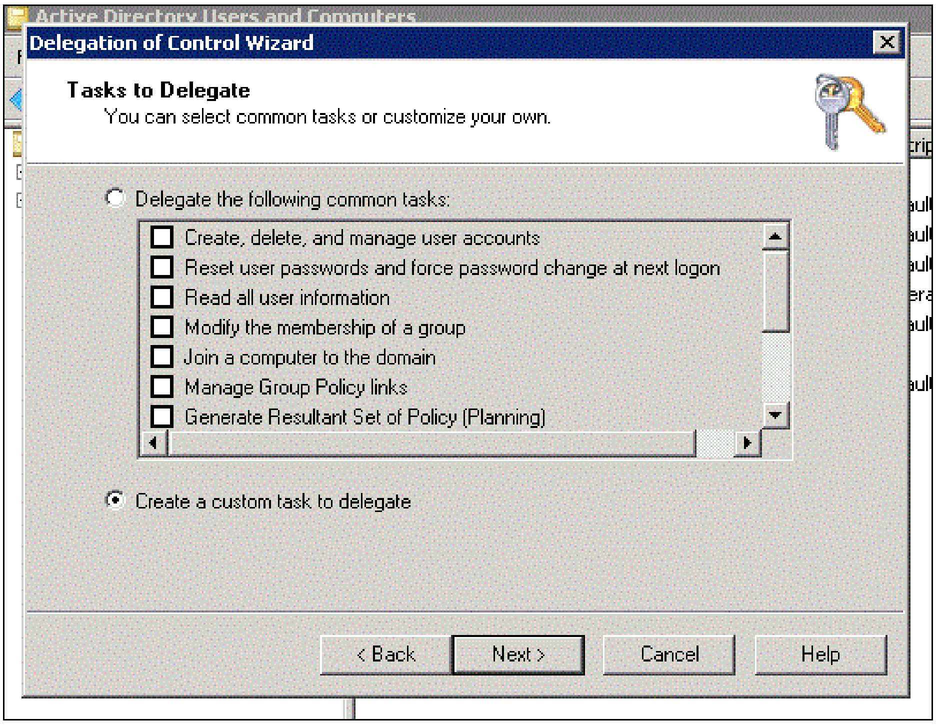
Users or Groups
Select one or more users or groups to whom you want to delegate control.

Selected users and groups:
Replication User (replicate_rvbd@gceinternal.int)

Add...
Remove
< Back
Next >
Cancel
Help

Figure 2-2-5: Delegation of Control Wizard, add replication user account

2.2.4 – Click “Next” to be able to configure the replication user account with the limited privileges needed to perform its task. Notice by default that the wizard offers a list of common tasks. These are too generic for the requirements of the replication user account and therefore as shown in figure 2-2-6 select “Create a custom task to delegate”.


Active Directory Users and Computers
Delegation of Control Wizard

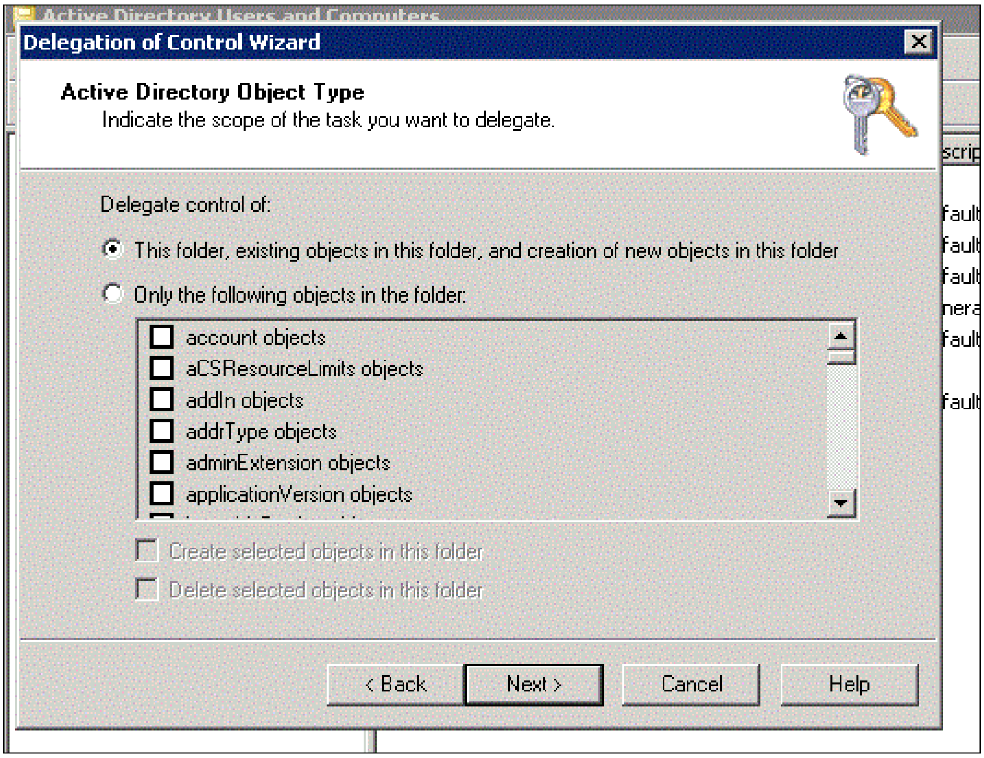
Tasks to Delegate
You can select common tasks or customize your own.

○ Delegate the following common tasks:
- □ Create, delete, and manage user accounts
- □ Reset user passwords and force password change at next logon
- □ Read all user information
- □ Modify the membership of a group
- □ Join a computer to the domain
- □ Manage Group Policy links
- □ Generate Resultant Set of Policy (Planning)

● Create a custom task to delegate

Figure 2-2-6: Delegation of Control Wizard, create custom task

2.2.5 – Click “Next” to be able to select the delegation control. Keep the default option; “Delegate control of: This folder, existing...”



Delegation of Control Wizard

Active Directory Object Type

Indicate the scope of the task you want to delegate.

Delegate control of:

● This folder, existing objects in this folder, and creation of new objects in this folder

○ Only the following objects in the folder:

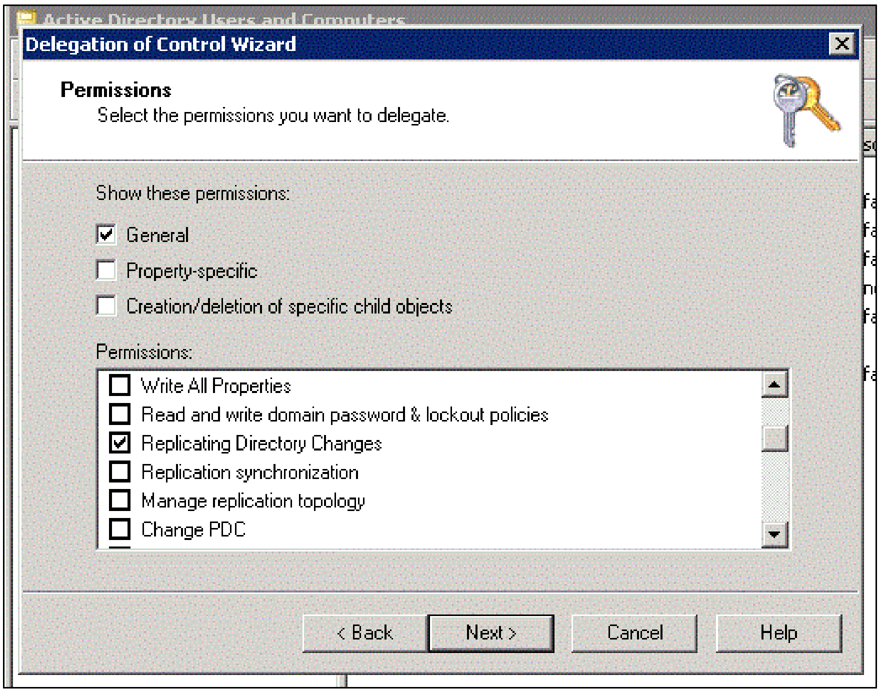
□ account objects
□ aCSResourceLimits objects
□ addIn objects
□ addrType objects
□ adminExtension objects
□ applicationVersion objects

□ Create selected objects in this folder

□ Delete selected objects in this folder

Figure 2-2-7: Delegation of Control Wizard, create custom task

2.2.6 – Click “Next” to select the delegation permissions. By default, the wizard shows the “General” permissions. Scroll down the “Permissions:” window and select “Replicating Directory Changes” and “Replicating Directory Changes All” as indicated in the next two screenshots, figures 2-2-8 and 2-2-9.



Delegation of Control Wizard

Permissions

Select the permissions you want to delegate.

Show these permissions:

☑ General

☐ Property-specific

☐ Creation/deletion of specific child objects

Permissions:

☐ Write All Properties

☐ Read and write domain password & lockout policies

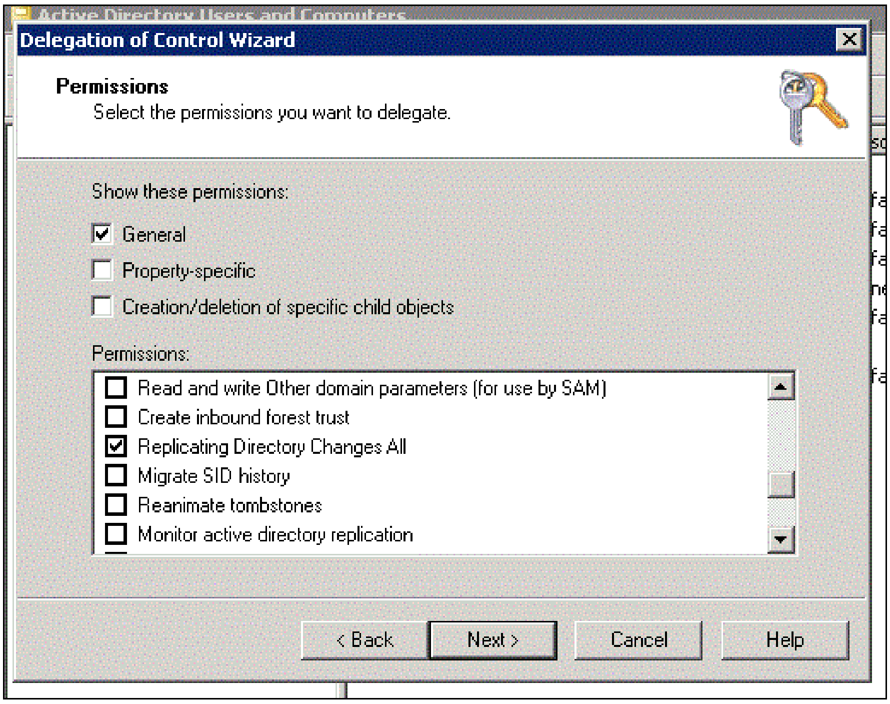
☑ Replicating Directory Changes

☐ Replication synchronization

☐ Manage replication topology

☐ Change PDC

Figure 2-2-8: Delegation of Control Wizard, permissions, Replicating Directory Changes



Delegation of Control Wizard

Permissions

Select the permissions you want to delegate.

Show these permissions:

☑ General

☐ Property-specific

☐ Creation/deletion of specific child objects

Permissions:

☐ Read and write Other domain parameters (for use by SAM)

☐ Create inbound forest trust

☑ Replicating Directory Changes All

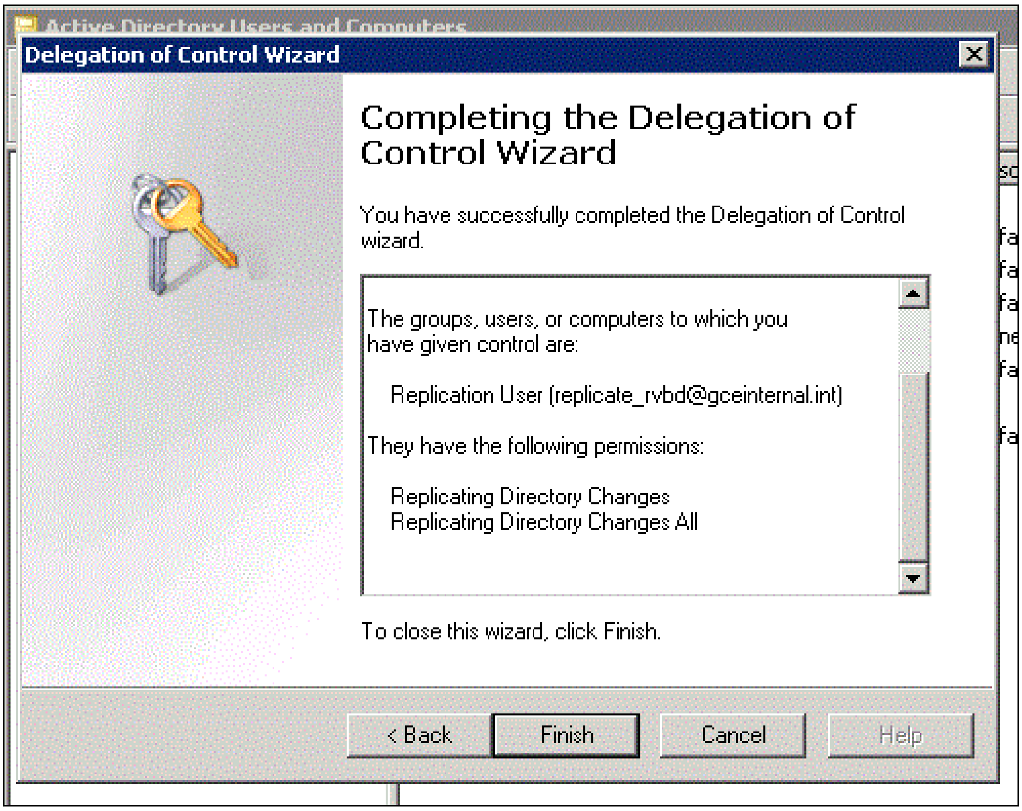
☐ Migrate SID history

☐ Reanimate tombstones

☐ Monitor active directory replication

Figure 2-2-9: Delegation of Control Wizard, permissions, Replicating Directory Changes All

2.2.7 – Click "Next" to complete the replication user account configuration and display a summary. The screenshot in figure 2-2-10 shows the final stage of the Delegation of Control Wizard. It displays the user account name and the permissions allocated to it. There should only be two permissions. This restricts the replication user to a very limited range of capability but is sufficient for the Steelhead appliance to perform its functions.


Active Directory Users and Computers
Delegation of Control Wizard
< Back
Finish
Cancel
Help

Completing the Delegation of Control Wizard

You have successfully completed the Delegation of Control wizard.

The groups, users, or computers to which you have given control are:

Replication User (replicate_rvbd@gceinternal.int)

They have the following permissions:

Replicating Directory Changes
Replicating Directory Changes All

To close this wizard, click Finish.

Figure 2-2-10: Delegation of Control Wizard, summary

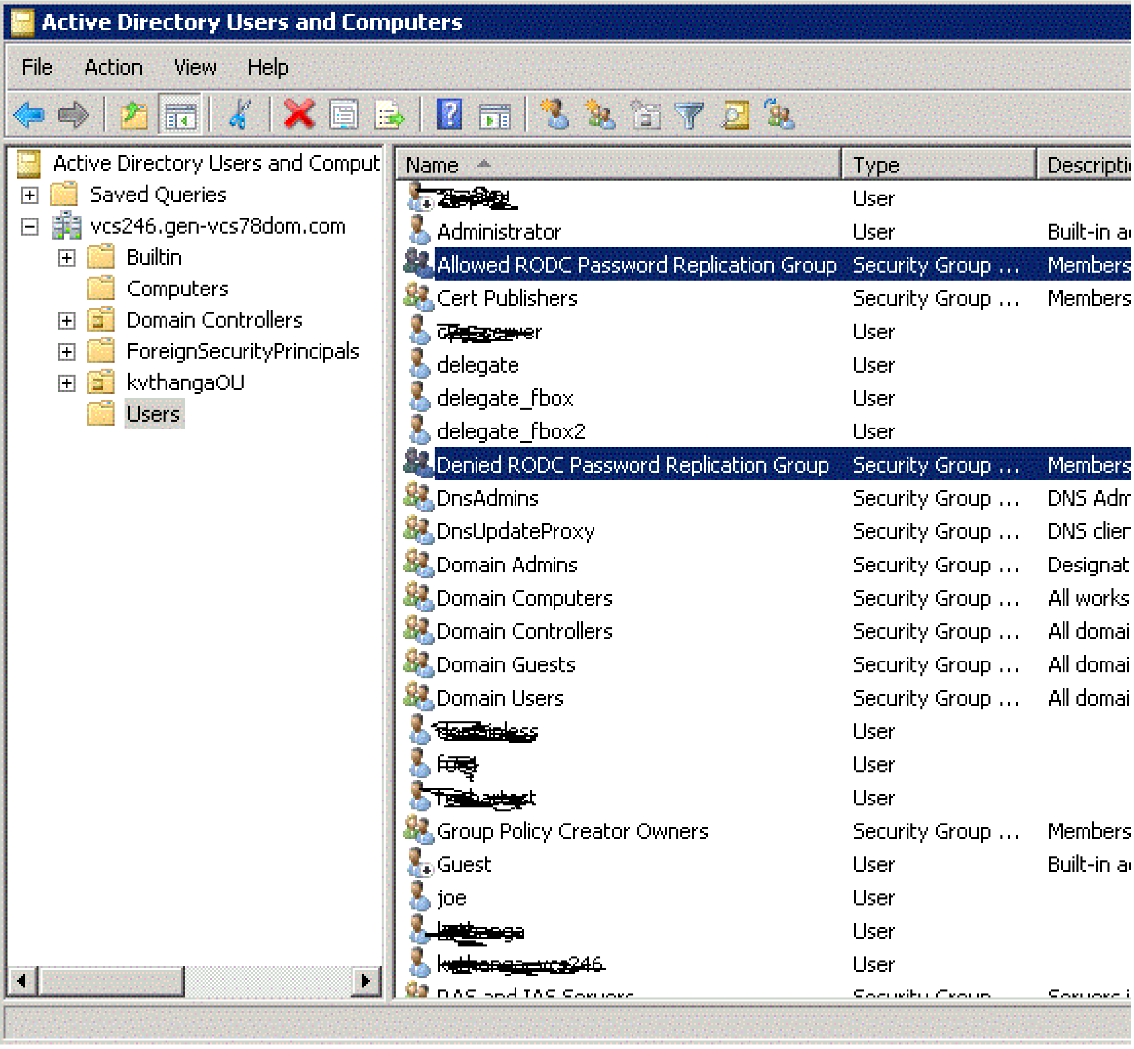
Notice in the above screenshot that the replication user account and domain name are for illustration purposes only. Your account name and domain will be different, but the permissions will be the same as shown here.

2.2.8 – Click “Finish” to close the wizard.

2.3 Optional - Configure Password Replication Policy (PRP) settings

Although the replication user account has a very restricted set of permissions, further limitations can be applied by making use of a Password Replication Policy (PRP). This type of policy is only available in Windows 2008 and 2008-R2 domains, it is not available with Windows 2003 domains.
Creating such a policy restricts the replication user so that it can only replicate for specified groups or users. While this may seem like a further security benefit, it does mean that the policy needs to be carefully managed and maintained. Therefore it can result in additional administrative overhead.

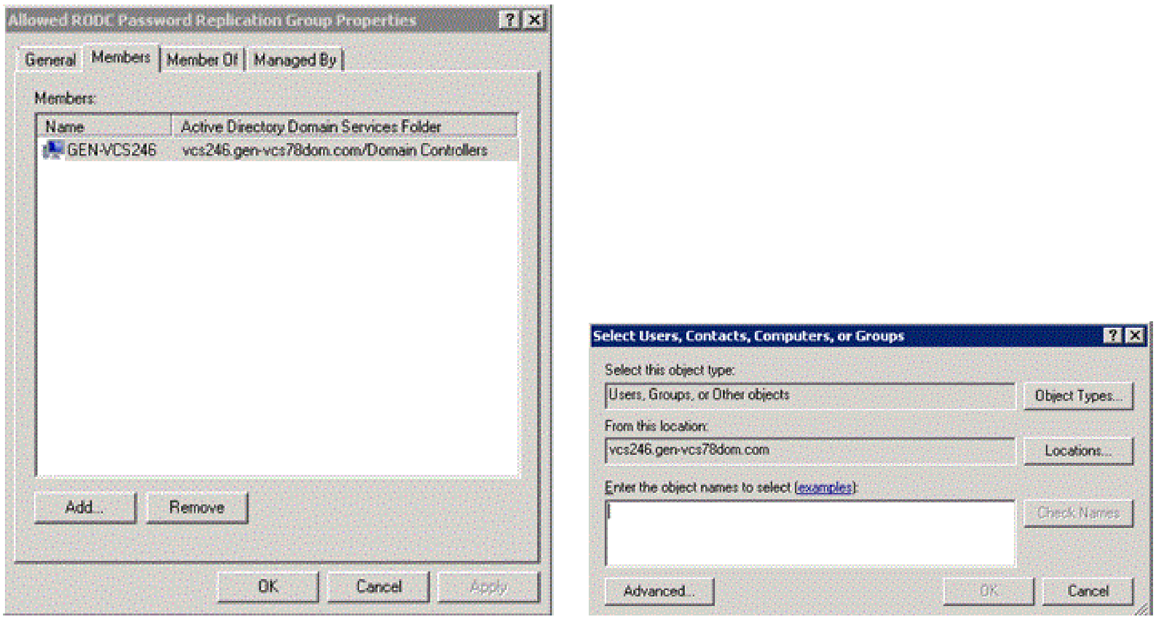
2.3.1 – On the Domain Controller, navigate to *Start Menu* > *Administrative Tools* > *Active Directory Users and Computers* then select the domain followed by “Users”. The right hand side shows the users and groups for the domain. In the list are two groups called “Allowed RODC Password Replication Group” and “Denied RODC Password Replication Group”. An example screenshot is shown in figure 2-3-1 with both groups highlighted to help illustrate.



Name	Type	Descripti
[redacted]	User	
Administrator	User	Built-in a
Allowed RODC Password Replication Group	Security Group ...	Members
Cert Publishers	Security Group ...	Members
[redacted]	User	
delegate	User	
delegate_fbox	User	
delegate_fbox2	User	
Denied RODC Password Replication Group	Security Group ...	Members
DnsAdmins	Security Group ...	DNS Adr
DnsUpdateProxy	Security Group ...	DNS clier
Domain Admins	Security Group ...	Designat
Domain Computers	Security Group ...	All works
Domain Controllers	Security Group ...	All domai
Domain Guests	Security Group ...	All domai
Domain Users	Security Group ...	All domai
[redacted]	User	
[redacted]	User	
[redacted]	User	
Group Policy Creator Owners	Security Group ...	Members
Guest	User	Built-in a
joe	User	
[redacted]	User	
[redacted]	User	
RAS and IAS Servers	Security Group	Servers i

Figure 2-3-1: PRP groups

2.3.2 – Depending on the type of PRP you wish to create, select either the “Allowed” or “Denied” group and right-click to open up the group properties.
Then click “Add” and enter in the user(s) or computer(s) that you wish to exclude or include. When you have completed the list click “OK” to complete the task.
See example screenshots in figure 2-3-2.



Members:

Name	Active Directory Domain Services Folder
GEN-VCS246	vcs246.gen-vcs78dom.com/Domain Controllers

Select this object type: Users, Groups, or Other objects

From this location: vcs246.gen-vcs78dom.com

Enter the object names to select (examples):

Figure 2-3-2: Add user/computer to PRP

2.4 - Join the Server-side Steelhead appliance to Windows Domain

When joining a Steelhead appliance to the Windows Domain, several prerequisites need to be configured to ensure smooth integration. The server-side Steelhead appliance must be able to successfully lookup its hostname in the DNS architecture. Ensure proper DNS entries are created in the DNS server(s) (only an "A record" is required) and the proper DNS servers are configured in the Steelhead appliance. The date and time of the server-side Steelhead appliance must be synchronized with the Windows Domain Controller. This is best accomplished by configuring the Steelhead to use the same NTP server as all the other servers in the domain. You must know the fully-qualified domain name. Table 2-3-1 is provided to collect this information for your environment.

Setting	Value	Step completed
DNS entry for Steelhead appliance		□
DNS server IP address(es)		□
NTP server IPs added to Steelhead configuration		□
Steelhead appliance Computer object created in Domain Controller		□
Fully-qualified Domain Name		

Table 2-4-1: Steelhead appliance prerequisites

Once the prerequisites are completed, join the server-side Steelhead to the AD domain.

To complete this step you will need a Windows user account with rights to join a host to the AD domain. NOTE: This account has nothing to do with the Replication User account set up in the previous sections. The credentials of the account used to join the domain are not stored on any Steelhead appliance and are only used for the purposes of joining the Steelhead appliance to the domain

2.4.1 On the server-side Steelhead(s) navigate to Configure > Networking > Windows Domain.
2.4.2 Enter the Active Directory Domain name, user id (of the user account with “Join Domain”

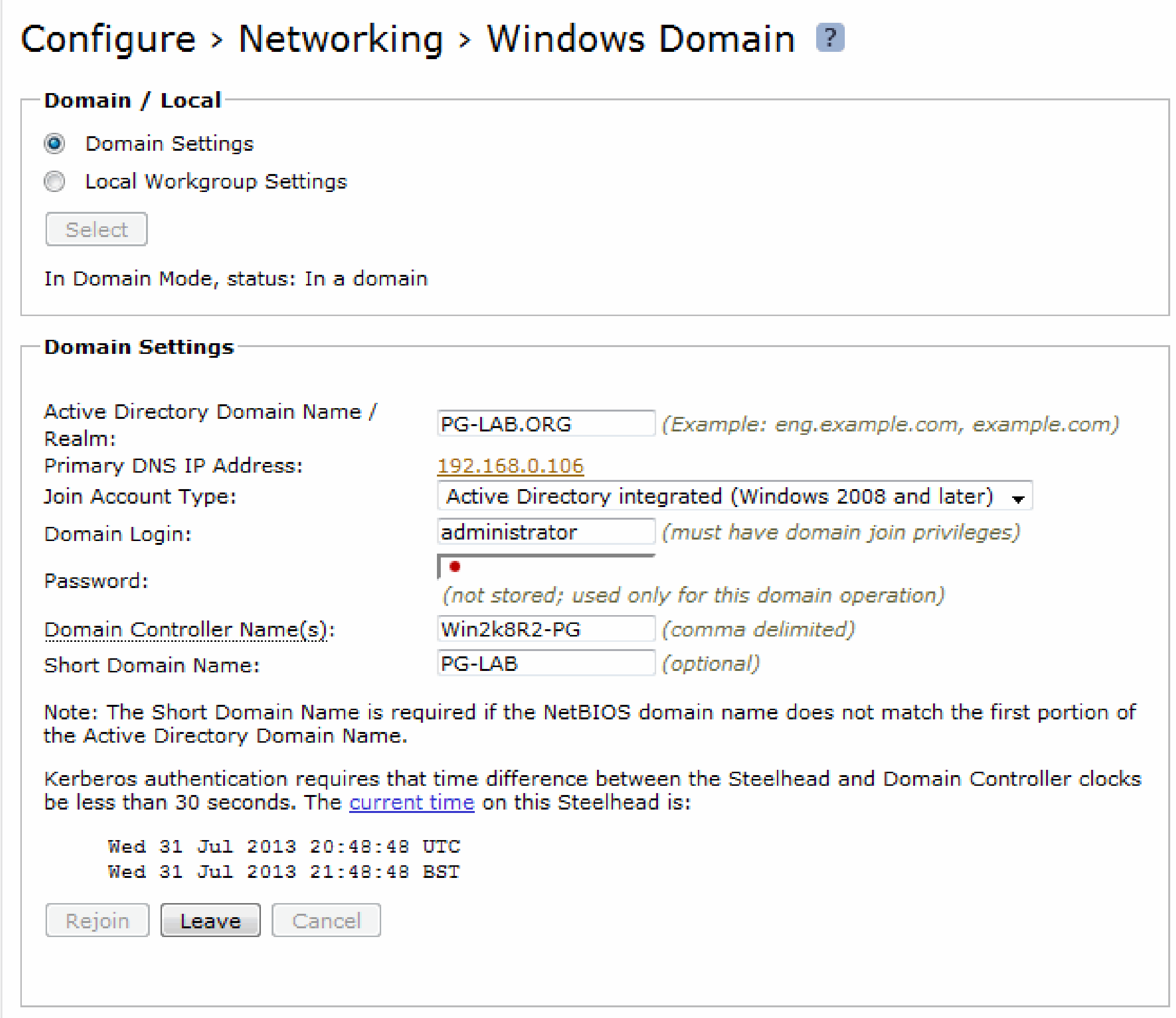
privileges), password and optionally the DC name and Short Domain Name.

2.4.3 Select the "Join Account Type" as either Workstation, Active Directory Integrated Windows 2003, or Active Directory Integrated Windows 2008. Whether you choose 2003 or 2008 mode depends on the domain functional level. If you choose "Workstation" it will not be possible to perform NTLM pass-through authentication.

2.4.4 Next click the "Join" button at the bottom of the page and wait for feedback. If an error appears, take appropriate action.

2.4.5 Once successfully joined you will see the statement 'In Domain Mode, status: In a domain' in the top frame of the page.

Figure 2-4-5 shows a successful domain join.



Configure > Networking > Windows Domain

Domain / Local

● Domain Settings

○ Local Workgroup Settings

In Domain Mode, status: In a domain

Domain Settings

Active Directory Domain Name / Realm:	PG-LAB.ORG (Example: eng.example.com, example.com)
Primary DNS IP Address:	192.168.0.106
Join Account Type:	Active Directory integrated (Windows 2008 and later)
Domain Login:	administrator (must have domain join privileges)
Password:	(not stored; used only for this domain operation)
Domain Controller Name(s):	Win2k8R2-PG (comma delimited)
Short Domain Name:	PG-LAB (optional)

Note: The Short Domain Name is required if the NetBIOS domain name does not match the first portion of the Active Directory Domain Name.

Kerberos authentication requires that time difference between the Steelhead and Domain Controller clocks be less than 30 seconds. The current time on this Steelhead is:

```
Wed 31 Jul 2013 20:48:48 UTC
Wed 31 Jul 2013 21:48:48 BST
```

Figure 2-4-5: Example screenshot, Windows Domain page of Steelhead appliance GUI

Further details on joining a Windows Domain are available in the Steelhead Management Console User's Guide in the chapter *Configuring Network Integration Features*.
More recent versions of RiOS include tools to test the configuration settings and ensure a join is successful as well as a status log to show progress and any errors encountered during the join process.

2.5 - Add the Replication User to the server-side Steelhead appliance

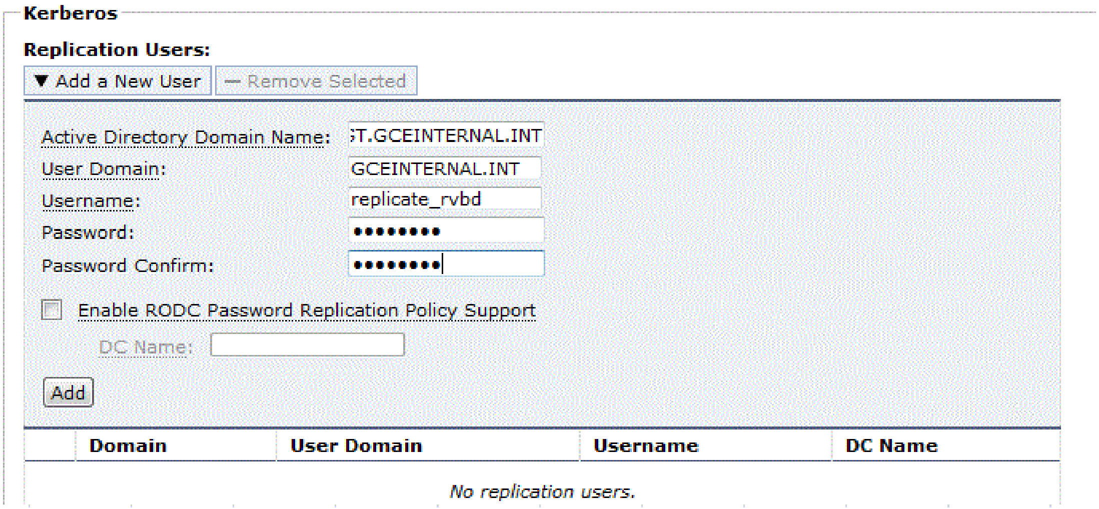
---

NOTE: More recent versions of RiOS include both a collection of command line and graphical tools to help automate these remaining steps. Whether or not the tools are available on the Steelhead appliances you are configuring, the individual steps are shown here.

To add the replication user to the server-side Steelhead you will need the AD domain name, replication user name, and password for the replication user that has been created. This should have already been created as described in sections 2.1 and 2.2 above. Assuming the user has been created, the following steps should then be performed.

2.5.1 On the server-side Steelhead(s) navigate to Configure > Optimization > Windows Domain Auth.

2.5.2 In the “Kerberos – Replication Users” section, click the ‘Add a New User’ tab. Enter the AD domain, User Domain, replication user account name, and password.



Active Directory Domain Name: ;T.GCEINTERNAL.INT
User Domain: GCEINTERNAL.INT
Username: replicate_rvbd
Password: ••••••••
Password Confirm: ••••••••

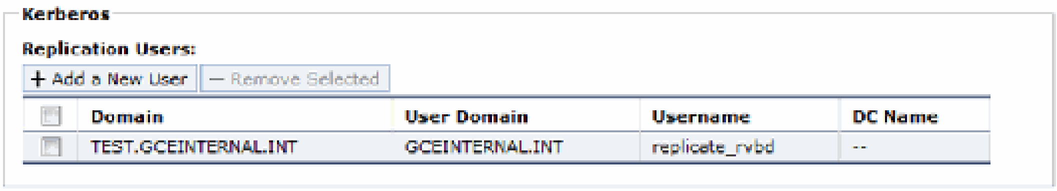
□ Enable RODC Password Replication Policy Support

DC Name:

	Domain	User Domain	Username	DC Name
	No replication users.			

Figure 2-5-2: Add New Replication User section on Windows Domain Auth page of Steelhead appliance GUI

2.5.3 Then click ‘Add’.The replication user name will be displayed.



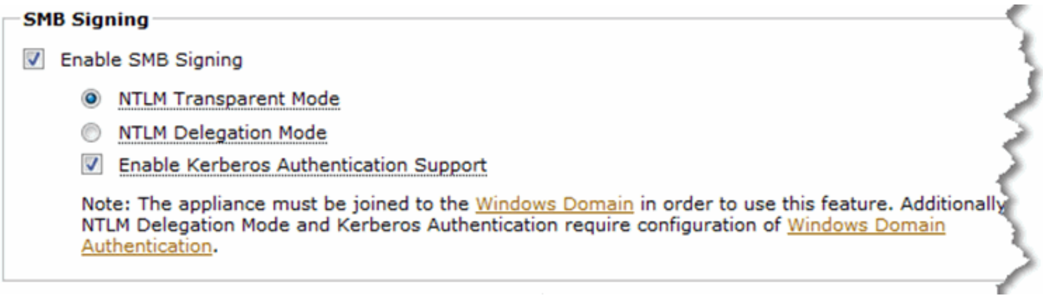
□	Domain	User Domain	Username	DC Name
□	TEST.GCEINTERNAL.INT	GCEINTERNAL.INT	replicate_rvbd	--

Figure 2-5-3: Add New Delegate User section on Windows Domain Auth page of Steelhead appliance GUI

2.6 - Configure the Steelhead appliance to optimize Secure Windows traffic

Configuration steps for Signed SMB, Signed SMB2 and Signed SMB3

2.6.1 On the server-side Steelhead navigate to Configure > Optimization > CIFS (SMB1).
2.6.2 Under the SMB Signing section, check the ‘Enable SMB Signing’ checkbox.
2.6.3 Next check the ‘Enable Kerberos Authentication’ checkbox.



SMB Signing

☑ Enable SMB Signing

● NTLM Transparent Mode

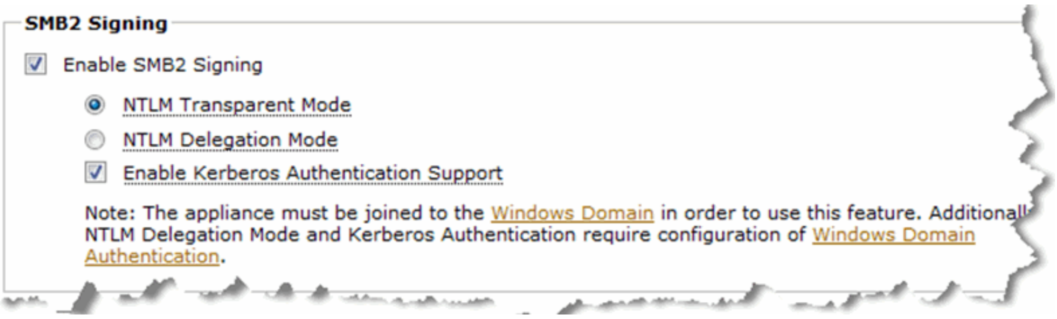
○ NTLM Delegation Mode

☑ Enable Kerberos Authentication Support

Note: The appliance must be joined to the Windows Domain in order to use this feature. Additionally NTLM Delegation Mode and Kerberos Authentication require configuration of Windows Domain Authentication.

Figure 2-6-3: Enable SMB Signing section on CIFS Optimization page of Steelhead appliance GUI

2.6.4 Click the 'Apply' button.
2.6.5 No changes are required on the client-side Steelhead appliances.
2.6.6 On the server-side Steelhead appliance navigate to Configure > Optimization > SMB2.
2.6.7 Under the SMB2 Signing section, check the 'Enable SMB2 Signing' checkbox. If your Steelhead appliance is running RiOS v8.5 then this checkbox will be labeled "Enable SMB2 and SMB3 Signing" and, so long as SMB3 optimization has been enabled, signed SMB3 will also be optimized.
2.6.8 Next check the 'Enable Kerberos Authentication' checkbox.



SMB2 Signing

☑ Enable SMB2 Signing

● NTLM Transparent Mode

○ NTLM Delegation Mode

☑ Enable Kerberos Authentication Support

Note: The appliance must be joined to the Windows Domain in order to use this feature. Additional NTLM Delegation Mode and Kerberos Authentication require configuration of Windows Domain Authentication.

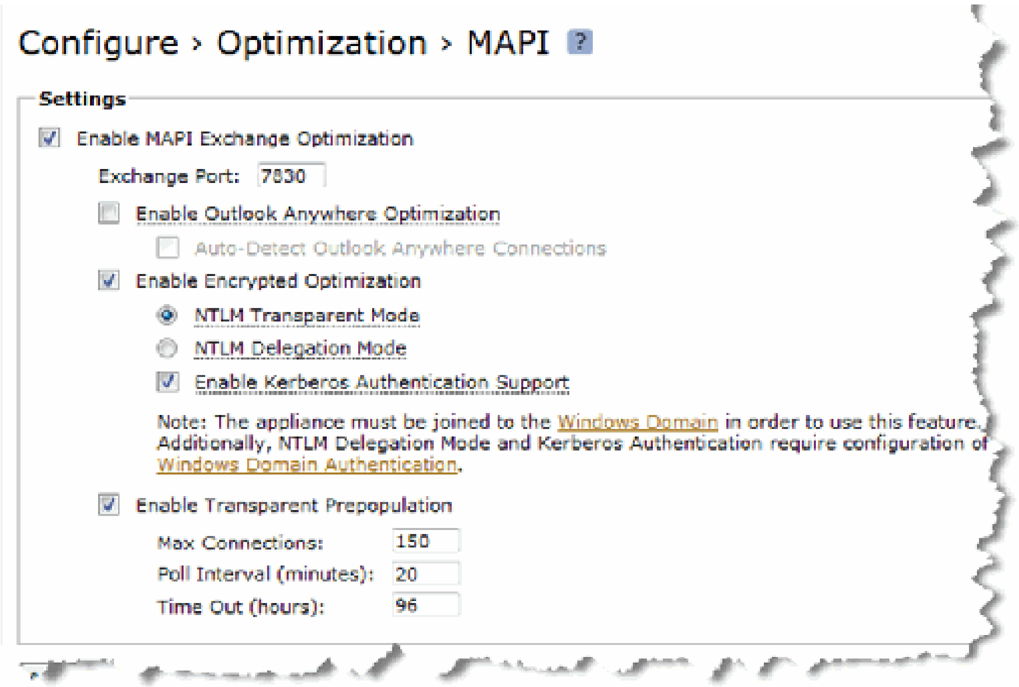
Figure 2-6-8: Enable SMB2 Signing section on SMB2 Optimization page of Steelhead appliance GUI

2.6.9 Click the 'Apply' button.
2.6.10 No changes are required on the client-side Steelhead appliances unless SMB3 optimization is required. If SMB3 optimization is required then repeat steps 2.3.5.6 through to 2.3.5.9 on the client-side Steelhead appliances.

Configuration steps for Encrypted MAPI

NOTE: For encrypted MAPI support, all Steelhead appliances must be running RiOS v7.0.0 or later and must be configured with the settings described here. The client-side Steelhead appliance does not need to join the Windows domain.

2.6.11 On all Steelhead appliances navigate to Configure > Optimization > MAPI.



Configure > Optimization > MAPI

Settings

☑ Enable MAPI Exchange Optimization

Exchange Port: 7830

□ Enable Outlook Anywhere Optimization

□ Auto-Detect Outlook Anywhere Connections

☑ Enable Encrypted Optimization

● NTLM Transparent Mode

○ NTLM Delegation Mode

☑ Enable Kerberos Authentication Support

Note: The appliance must be joined to the Windows Domain in order to use this feature. Additionally, NTLM Delegation Mode and Kerberos Authentication require configuration of Windows Domain Authentication.

☑ Enable Transparent Prepopulation

Max Connections: 150

Poll Interval (minutes): 20

Time Out (hours): 96

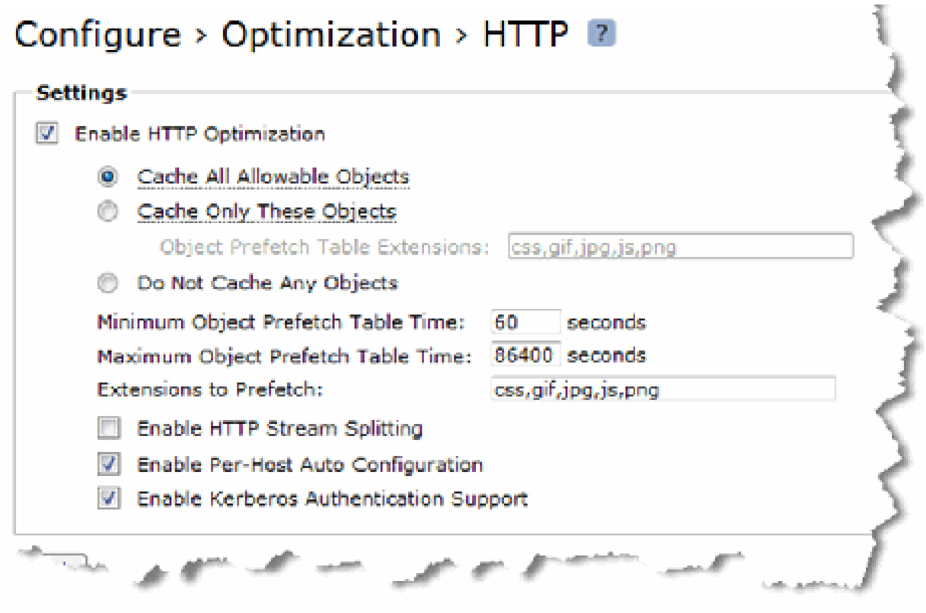
Figure 2-6-11: MAPI Optimization page of Steelhead appliance GUI

2.6.12 Check the ‘Enable Encrypted Optimization’ checkbox.
2.6.13 Check the ‘Enable Kerberos Authentication Support’ checkbox.
2.6.14 Click the ‘Apply’ button.

Configuration steps for HTTP

NOTE: For Kerberos Authentication with HTTP, all Steelhead appliances must be running RiOS v7.0.0 or later but only the server-side Steelhead appliance needs to be configured with the settings described here.

2.6.15 On the Steelhead appliance navigate to Configure > Optimization > HTTP



Configure > Optimization > HTTP

Settings

☑ Enable HTTP Optimization

● Cache All Allowable Objects

○ Cache Only These Objects

Object Prefetch Table Extensions: css,gif,jpg,js,png

○ Do Not Cache Any Objects

Minimum Object Prefetch Table Time: 60 seconds

Maximum Object Prefetch Table Time: 86400 seconds

Extensions to Prefetch: css,gif,jpg,js,png

□ Enable HTTP Stream Splitting

☑ Enable Per-Host Auto Configuration

☑ Enable Kerberos Authentication Support

Figure 2-6-15: HTTP Optimization page of Steelhead appliance GUI

2.6.16 Check the 'Enable Kerberos Authentication Support' checkbox.
2.6.17 Click the 'Apply' button.

Configuration steps for Secure Peering

2.6.18 Optionally you can also configure secure peering between the client-side and server-side Steelhead appliances. Refer to Appendix A.4 of this document for outline guidance. For more details, reference the Steelhead Management Console User's Guide section, *Configure Secure Peers*.

2.7 - Saving the configuration and restarting the Optimization Service

Finally, save the configuration and restart the optimization service. Do this by clicking 'Save' and 'Restart' in the GUI navigation header. Or, proceed to the Configure > Configurations GUI page to save the configuration with a specific name and then restart the optimization service.

The integration with the Windows domain is now complete.

Once deployed successfully, monitor performance and health of the Steelhead appliance(s) to ensure proper optimization is occurring and full acceleration is being achieved for the appropriate clients and servers. Keep in mind AD and Windows administrators may make changes without notifying the networking team so remain vigilant. Consider incorporating some of this configuration information into a Change Control Process that enables both the Windows Server Administration team and the Networking team to coordinate future updates and changes.

Appendix B in this document has some outline guidance for troubleshooting as well as pointers to other sources of help.

Section 3 – Configuring the server-side Steelhead with limited domain controller privileges

Overview of required configuration tasks for providing limited domain controller privileges

There are a number of tasks to be performed and parameters to be configured. They are listed here;

3.1 Join server-side Steelhead appliance to Windows Domain

3.2 Configure the Steelhead appliance to optimize Signed SMB and Encrypted MAPI

If you are planning to use the Domain Auth Easy Config widget, complete the following tasks first…..

DNS and NTP configuration as outlined in Table 3-1

The Domain Auth Easy Config widget will complete tasks 3.1 and 3.2 with the exception of any client-side Steelhead appliance configuration. Any configuration on the client-side Steelhead appliance(s), for example enabling encrypted MAPI, will need to be done as a separate task.

NOTE: If you have already completed the configuration tasks in Section 2 (End to end Kerberos authentication) and, when performing the join domain task, you joined as “Active Directory integrated” you do not need to complete any of the steps in this section.

3.1 - Join the Server-side Steelhead appliance to Windows Domain

When joining a Steelhead appliance to the Windows Domain, several prerequisites need to be configured to ensure smooth integration. The server-side Steelhead appliance must be able to successfully lookup its hostname in the DNS architecture. Ensure proper DNS entries are created in the DNS server(s) (only an "A record" is required) and the proper DNS servers are configured in the Steelhead appliance. The date and time of the server-side Steelhead appliance must be synchronized with the Windows Domain Controller. This is best accomplished by configuring the Steelhead to use the same NTP server as all the other servers in the domain. You must know the fully-qualified domain name. Table 3-1 is provided to collect this information for your environment.

Setting	Value	Step completed
DNS entry for Steelhead appliance		
DNS server IP address(es)		
NTP server IPs added to Steelhead configuration		
Fully-qualified Domain Name		
IP addresses or DNS names of Domain Controllers in the domain the Steelhead will join		
Domain functional level (2003, mixed or 2008)		

Table 3-1: Steelhead appliance prerequisites

Once the prerequisites are completed, join the server-side Steelhead to the AD domain.

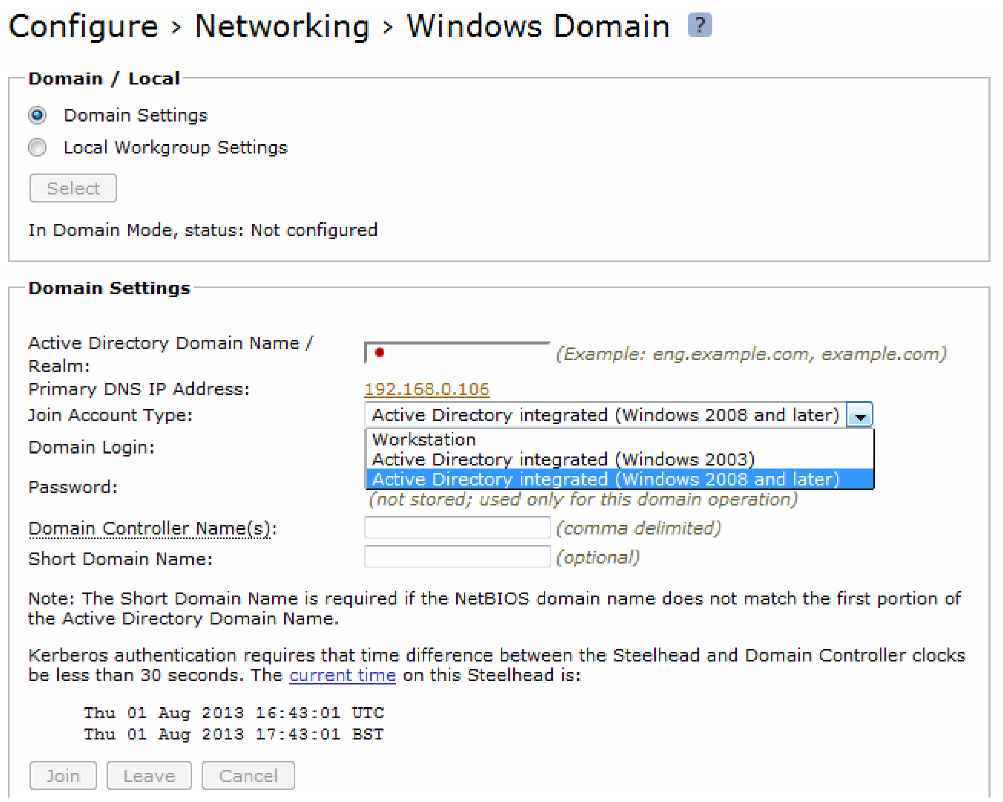
This task will require administrator level access (an account that is a member of the “Domain Admins” group, or a preconfigured account with sufficient privileges) to a Windows Domain controller and admin level access to the Riverbed Steelhead appliance. Therefore the appropriate personnel with the relevant access privileges will need to be on hand to perform the task. Administrator credentials are not stored on any Steelhead appliance. While this task is all that is needed to meet the basic requirements, there may be other steps to enable proper functionality with, for example; one-way trusts, organisational unit, password expiration, etc. Information on these additional items is to be found in the appendices of this document.
For more details on what capabilities the server-side Steelhead has when joined in this role, please consult the section at the

beginning of this guide entitled "*What configuration options are available and how do I choose?*".

3.1.1 On the server-side Steelhead(s) navigate to Configure > Networking > Windows Domain.

3.1.2 Enter the Active Directory Domain name, user id [for the user account with "Join Domain" Privileges] and its password.

3.1.3 Select the "Join Account Type" as either Active Directory Integrated Windows 2003, or Active Directory Integrated Windows 2008. Whether you choose 2003 or 2008 mode depends on the domain functional level . Figure 3.1.3 below shows an example screenshot.



Domain / Local

● Domain Settings
○ Local Workgroup Settings

In Domain Mode, status: Not configured

Domain Settings

Active Directory Domain Name / Realm: (Example: eng.example.com, example.com)
Primary DNS IP Address: 192.168.0.106
Join Account Type: Active Directory integrated (Windows 2008 and later)
Workstation
Active Directory integrated (Windows 2003)
Active Directory integrated (Windows 2008 and later)
Domain Login:
Password: (not stored; used only for this domain operation)
Domain Controller Name(s): (comma delimited)
Short Domain Name: (optional)

Note: The Short Domain Name is required if the NetBIOS domain name does not match the first portion of the Active Directory Domain Name.

Kerberos authentication requires that time difference between the Steelhead and Domain Controller clocks be less than 30 seconds. The current time on this Steelhead is:

```
Thu 01 Aug 2013 16:43:01 UTC
Thu 01 Aug 2013 17:43:01 BST
```

Figure 3-1-3: Example screenshot, Windows Domain page of Steelhead appliance GUI

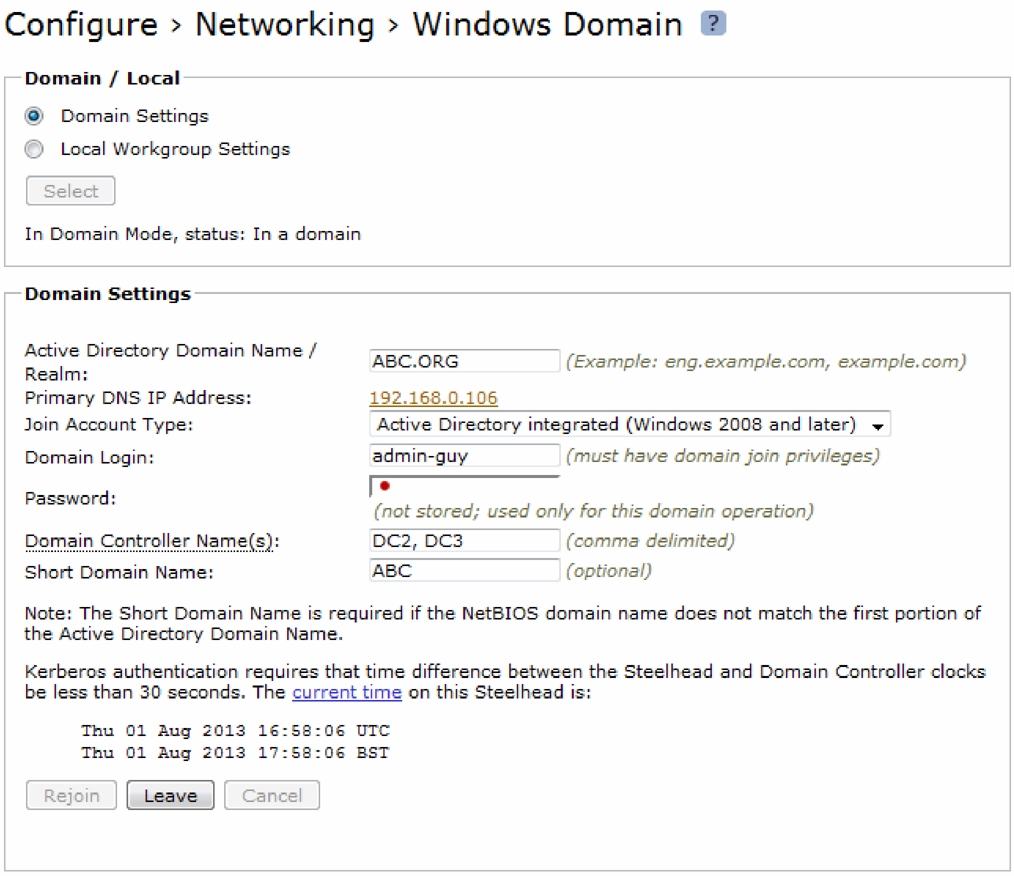
3.1.4 Enter the Domain Controller names or IP addresses of the nearest DCs. This ensures a quicker join especially in high latency networks. For 2008 or greater, and mixed domain types, the DCs must be the 2008(-R2) instances in the domain. When joining in 2008 mode it is strongly advised to provide one or more DCs in this field. If the domain is a mix of 2003 and 2008, then the Domain Controllers specified must be the 2008 type and not 2003 type.

NOTE: Although, the Steelhead will probably perform a successful join without having the domain controllers specified (a discovery is used), it is very strongly recommended that the correct details are entered in this field. Failure to do so can lead to intermittent but persistent authentication failures, especially in large domain structures.

3.1.5 Next click the "Join" button at the bottom of the page and wait for feedback. If an error appears, take appropriate action.

3.1.6 Once successfully joined you will see the statement 'In Domain Mode, status: In a domain' in the top frame of the page.

Figure 3-1-6 shows a successful domain join.



Configure > Networking > Windows Domain

Domain / Local

● Domain Settings

○ Local Workgroup Settings

In Domain Mode, status: In a domain

Domain Settings

Active Directory Domain Name / Realm: ABC.ORG (Example: eng.example.com, example.com)

Primary DNS IP Address: 192.168.0.106

Join Account Type: Active Directory integrated (Windows 2008 and later)

Domain Login: admin-guy (must have domain join privileges)

Password: (not stored; used only for this domain operation)

Domain Controller Name(s): DC2, DC3 (comma delimited)

Short Domain Name: ABC (optional)

Note: The Short Domain Name is required if the NetBIOS domain name does not match the first portion of the Active Directory Domain Name.

Kerberos authentication requires that time difference between the Steelhead and Domain Controller clocks be less than 30 seconds. The current time on this Steelhead is:

```
Thu 01 Aug 2013 16:58:06 UTC
Thu 01 Aug 2013 17:58:06 BST
```

Figure 3-1-6: Example screenshot, Windows Domain page of Steelhead appliance GUI

Further details on joining a Windows Domain are available in the Steelhead Management Console User's Guide in the chapter *Configuring Network Integration Features*.
More recent versions of RiOS include tools to test the configuration settings and ensure a join is successful as well as a status log to show progress and any errors encountered during the join process.

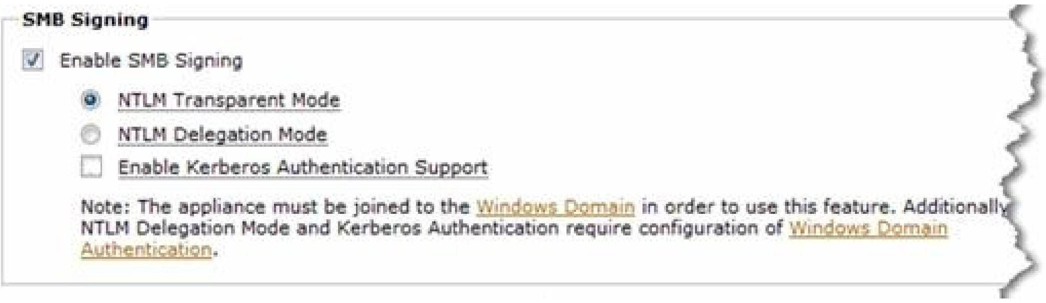
3.2 – Configure the Steelhead appliance to optimize Secure Windows traffic

---

NOTE: More recent versions of RiOS include both a collection of command line and graphical tools to help automate these remaining steps. Whether or not the tools are available on the Steelhead appliances you are configuring, the individual steps are shown here.

Configuration steps for Signed SMB and Signed SMB2

3.2.1 On the server-side Steelhead navigate to Configure > Optimization > CIFS (SMB1).
3.2.2 Under the SMB Signing section, check the 'Enable SMB Signing' checkbox
3.2.3 Ensure the 'NTLM Transparent Mode" option is selected



SMB Signing

☑ Enable SMB Signing

● NTLM Transparent Mode

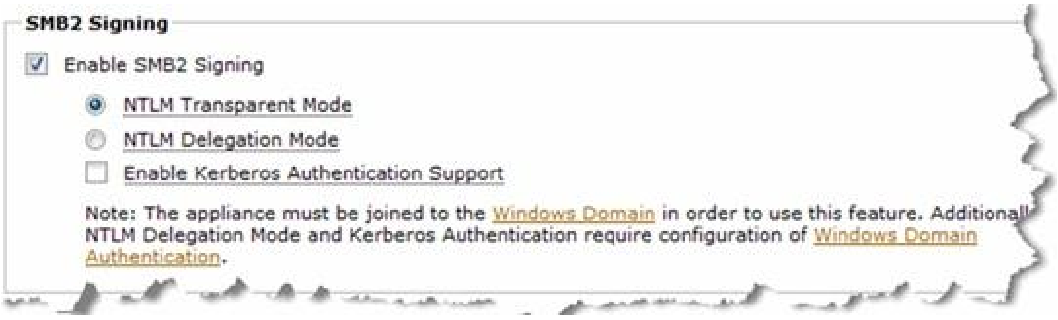
○ NTLM Delegation Mode

□ Enable Kerberos Authentication Support

Note: The appliance must be joined to the Windows Domain in order to use this feature. Additionally NTLM Delegation Mode and Kerberos Authentication require configuration of Windows Domain Authentication.

Figure 3-2-3: Enable SMB Signing section on CIFS Optimization page of Steelhead appliance GUI

3.2.4 Click the 'Apply' button.
3.2.5 No changes are required on the client-side Steelhead appliances.
3.2.6 On the server-side Steelhead appliance navigate to Configure > Optimization > SMB2
3.2.7 Under the SMB2 Signing section, check the 'Enable SMB2 Signing' checkbox. If your Steelhead appliance is running RiOS v8.5 then this checkbox will be labeled "Enable SMB2 and SMB3 Signing" and, so long as SMB3 optimization has been enabled, signed SMB3 will also be optimized.
3.2.8 Ensure the 'NTLM Transparent Mode" option is selected



SMB2 Signing

☑ Enable SMB2 Signing

● NTLM Transparent Mode

○ NTLM Delegation Mode

□ Enable Kerberos Authentication Support

Note: The appliance must be joined to the Windows Domain in order to use this feature. Additionall NTLM Delegation Mode and Kerberos Authentication require configuration of Windows Domain Authentication.

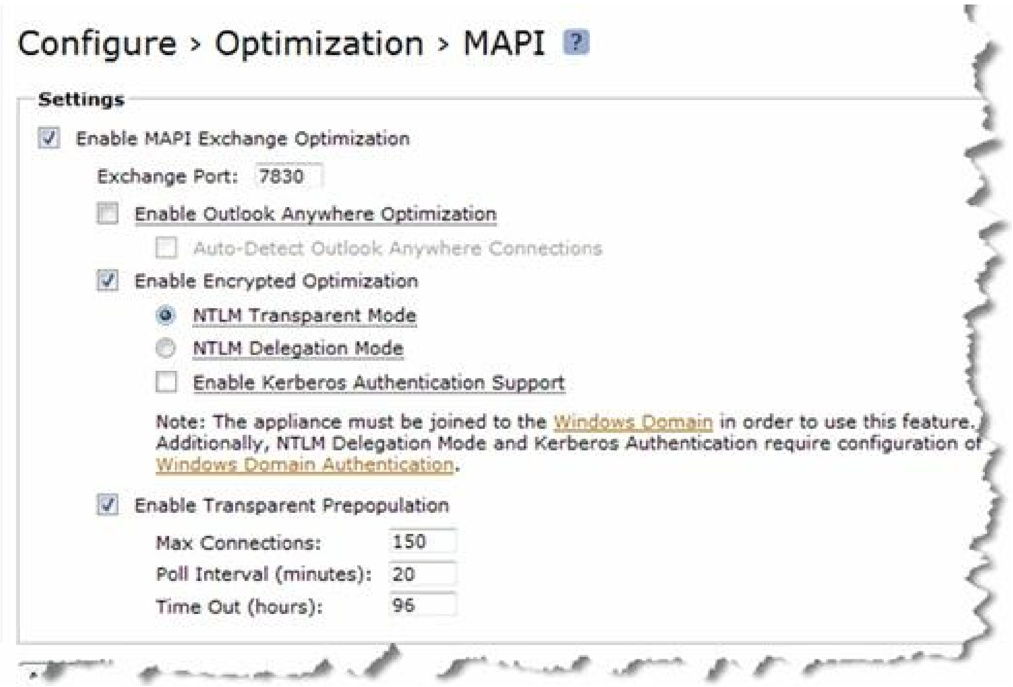
Figure 3-2-8: Enable SMB2 Signing section on SMB2 Optimization page of Steelhead appliance GUI

3.2.9 Click the 'Apply' button.
3.2.10 No changes are required on the client-side Steelhead appliances unless SMB3 optimization is required. If SMB3 optimization is required then repeat steps 3.2.6 through to 3.2.9 on the client-side Steelhead appliances..

Configuration steps for Encrypted MAPI

NOTE: For encrypted MAPI support, all Steelhead appliances must be running RiOS v7.0.0 or later and must be configured with the settings described here below. The client-side Steelhead appliance does not need to join the Windows domain.

3.2.11 On all Steelhead appliances navigate to Configure > Optimization > MAPI.



Configure > Optimization > MAPI

Settings

☑ Enable MAPI Exchange Optimization

Exchange Port: 7830

□ Enable Outlook Anywhere Optimization

□ Auto-Detect Outlook Anywhere Connections

☑ Enable Encrypted Optimization

● NTLM Transparent Mode

○ NTLM Delegation Mode

□ Enable Kerberos Authentication Support

Note: The appliance must be joined to the Windows Domain in order to use this feature. Additionally, NTLM Delegation Mode and Kerberos Authentication require configuration of Windows Domain Authentication.

☑ Enable Transparent Prepopulation

Max Connections: 150

Poll Interval (minutes): 20

Time Out (hours): 96

Figure 3-2-11: MAPI Optimization page of Steelhead appliance GUI

3.2.12 Check the ‘Enable Encrypted Optimization’ checkbox.
3.2.13 Click the ‘Apply’ button.

3.3 - Saving the configuration and restarting the Optimization Service

Finally, save the configuration and restart the optimization service. Do this by clicking ‘Save’ and ‘Restart’ in the GUI navigation header. Or, proceed to the Configure > Configurations GUI page to save the configuration with a specific name and then restart the optimization service.

The integration with the Windows domain is now complete.

Appendix A – Additional information and guidance

A.1 - Useful commands

There are some additional configuration tasks that can be performed on the server-side Steelhead appliance for specific requirements. In the majority of cases, the only way to perform these tasks is via the RiOS cli of the Steelhead appliance.

A.1.1 – Have the Steelhead appliance join the Windows Domain in a different Organizational Unit

When the server-side Steelhead is joined to the Windows Domain, it will automatically be placed the Organizational Unit (OU) called “Computers”. While this is standard behaviour for a Member Server when joining a Windows Domain, some Windows administrators prefer the Steelhead appliance to be placed into a different OU.
There are at least two ways to achieve this. The first one is simply to use an appropriate Windows admin tool, wizard or command, to “move” the server-side Steelhead appliance from the Computers OU to the desired OU. This can only be done after the server-side Steelhead appliance has joined the Windows Domain.
Another way is to have the server-side Steelhead appliance to join the domain and get placed directly into the desired OU as part of the join domain process. This can be achieved by using the RiOS command line to specify the required OU as part of the join domain command. The syntax is as follows;

```
# domain join domain-name <domain> login <username> password <********> org-unit <OU>
```

Where `<domain>` is the domain name for the Steelhead to join, `<username>` is the user with “joindomain” privileges, `<********>` is the user’s password and `<OU>` is the name of the Organisational Unit.

For example, the following command would have the Steelhead join the “RVBD.COM” domain and be placed into the “WAN-opt” Organisational Unit.

```
# domain join domain-name RVBD.COM login Administrator password ****** org-unit WAN-opt
```

Note: Joining to a specific organizational unit when the server-side Steelhead is joined in “Active Directory integrated mode” is not supported.

A.1.2 - Support the Domain Controller request for password refresh on the Steelhead appliance Machine Account

Some Windows administrators require that Machine Accounts are refreshed at regular intervals, for example, every 30 days. By default the Steelhead appliance doesn’t have this setting enabled. To have the Steelhead appliance respond to the password refresh request, execute the following command via the RiOS cli on the Steelhead appliance;

```
# domain settings pwd-refresh-int <number of days>
```

Where `<number of days>` is the interval in days between password refresh requests.
For example, the following command would be suitable for a 30-day refresh interval;

```
# domain settings pwd-refresh-int 30
```

A.2 - Exchange clusters

A.2.1 - Single Exchange server

Before we look at what happens with Exchange clusters, it's important to first understand in simple terms what happens in a basic Exchange configuration when Steelheads are providing optimization.

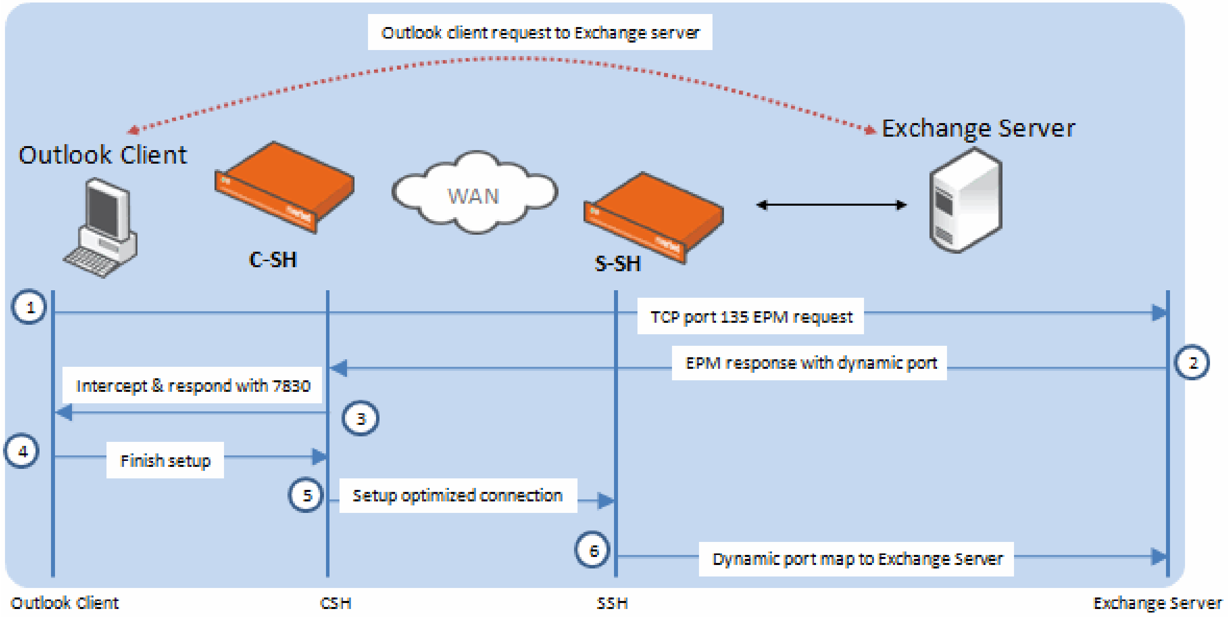

Outlook client request to Exchange server
Outlook Client
C-SH
WAN
S-SH
Exchange Server
1
TCP port 135 EPM request
EPM response with dynamic port
2
Intercept & respond with 7830
3
4
Finish setup
5
Setup optimized connection
6
Dynamic port map to Exchange Server
Outlook Client
CSH
SSH
Exchange Server

Figure A.2-1 Basic Exchange server configuration

Referring to figure A.2-1 we can see the initial connection setup between the Outlook client and the Exchange server when there are Steelhead appliances attempting to optimize the connection.

The five steps shown begin with the Outlook client sending a request to the Exchange server End Point Mapper (EPM) on well-known port 135.
The second step is the EPM response back to the client with a dynamic port number to use for the MAPI session. This reply is picked up by the C-SH (client-side Steelhead applaince). The C-SH remaps the dynamic port and responds to the client with port 7830. The client finishes the setup with the C-SH, the C-SH and S-SH (server-side Steelhead appliance) setup an optimized connection between themselves and finally, the S-SH talks to the Exchange server using the dynamic port that was supplied in the original EPM response.

This ensures the S-SH and C-SH can optimize the MAPI connection at the same time as maintaining transparency to the Exchange server (by using the dynamic port assigned for the client).
It's the job of the Steelhead appliance to maintain a list that includes the IP addresses and dynamic ports for each client and which Exchange servers are being used.

A.2.2 - Exchange cluster

With an Exchange cluster that comprises of multiple nodes the process is essentially the same as before except that the client initially sends the EPM request to the Exchange server cluster name. The EPM response to the client is supplied by one of the nodes in the cluster and includes the IP address of the node.

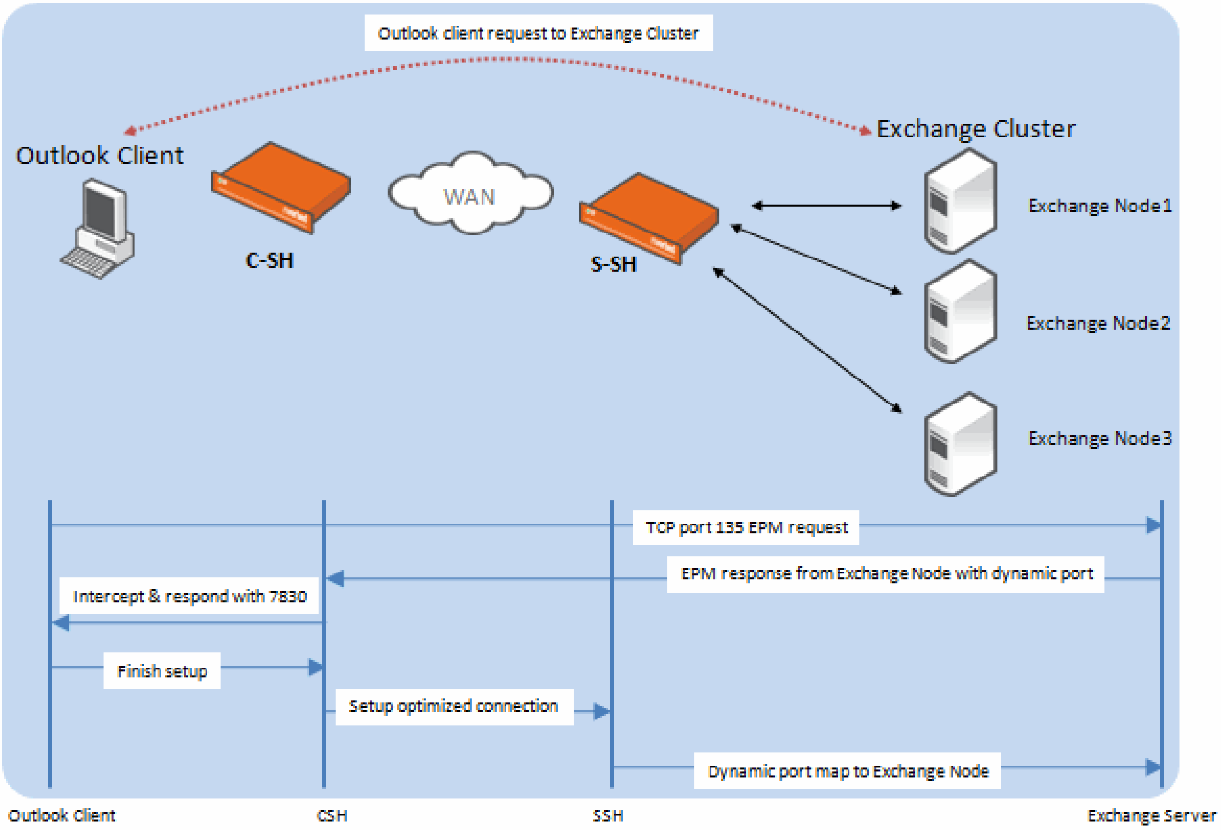

Outlook client request to Exchange Cluster
Outlook Client
C-SH
WAN
S-SH
Exchange Cluster
Exchange Node1
Exchange Node2
Exchange Node3
TCP port 135 EPM request
EPM response from Exchange Node with dynamic port
Intercept & respond with 7830
Finish setup
Setup optimized connection
Dynamic port map to Exchange Node
Outlook Client
CSH
SSH
Exchange Server

Figure A.2-2 Exchange cluster

Because of this, the S-SH is able to establish the server-side connection with the correct Exchange server node in the cluster. The same node in the cluster is used for the entire duration of the connection with the client. This Exchange node to client mapping is just the same as would occur in an un-optimized configuration. Once again, the Steelhead is able to maintain a list of the relevant MAPI connections between clients and server nodes.

For the server-side Steelhead appliance to correctly perform its optimization using the Delegate User account and the exchangeMDB SPN, it needs to be able to contact each node specifically rather than using the cluster name.

This requires that each node in the Exchange cluster is associated with the exchangeMDB Service Principal Name. Over time, as more capacity is required, more nodes are added to the cluster. But sometimes the configuration tasks may not be fully performed leaving some nodes in a cluster without have this setting configured. As a result, this can lead to Outlook users with an optimized connection occasionally being prompted for their account name and password when connecting to the Exchange cluster.

This is particularly relevant with Exchange clusters running Exchange 2003 and Exchange 2007.

Using the Windows command `setspn –L <node_name>` on the Domain Controller [in the domain where the Exchange server is located] will show a list of the SPNs for each node and whether exchangeMDB is included.

To add an SPN for a node of the Exchange cluster simply use the following command;

```
C:\> setspn –A exchangeMDB/<node_name> <node_name>
```

Where <node_name> is the name of the node in the Exchange cluster. For example, in an Exchange cluster of three nodes called exnode1, exnode2 and exnode3 the following commands are needed;

```
C:\> setspn –A exchangeMDB/exnode1 exnode1
C:\> setspn –A exchangeMDB/exnode2 exnode2
C:\> setspn –A exchangeMDB/exnode3 exnode3
```

Be careful to ensure that these commands are executed with the correct syntax using the same node name for each part of the command. Running the command incorrectly, for example " `setspn –A exchangeMDB/exnode1 exnode3` " will cause

the optimization of encrypted MAPI to fail.
If you suspect this is the case, refer to this useful KnowledgeBase article on the Riverbed support site. https://support.riverbed.com/kb/solution.htm?id=501A0000000cPLU&categoryName=Log+and+Error+Messages for further guidance.

A.2.3 - Exchange Cluster with Load-balancer

In a configuration where the Exchange server is behind a Load Balancer, the process is very similar to a standard Exchange cluster. The subtle difference is that the client, and therefore the server-side Steelhead appliance when there is an optimized connection, is communicating to the Exchange cluster through the Load Balancer. In this situation, the EPM response to the client contains the relevant server IP, but the client requests all begin with the same IP of the load balancer. Again, the Steelhead appliance tracks the EPM response to ensure the address mapping is correct.
The key thing in this situation is to ensure that each connection request can be uniquely identified and as such requires either Port or Full Transparency to be enabled for MAPI traffic, or, for MAPI port remapping to be disabled on the client side Steelhead appliance(s) using the CLI command:

```
no protocol mapi port-remap enable
```

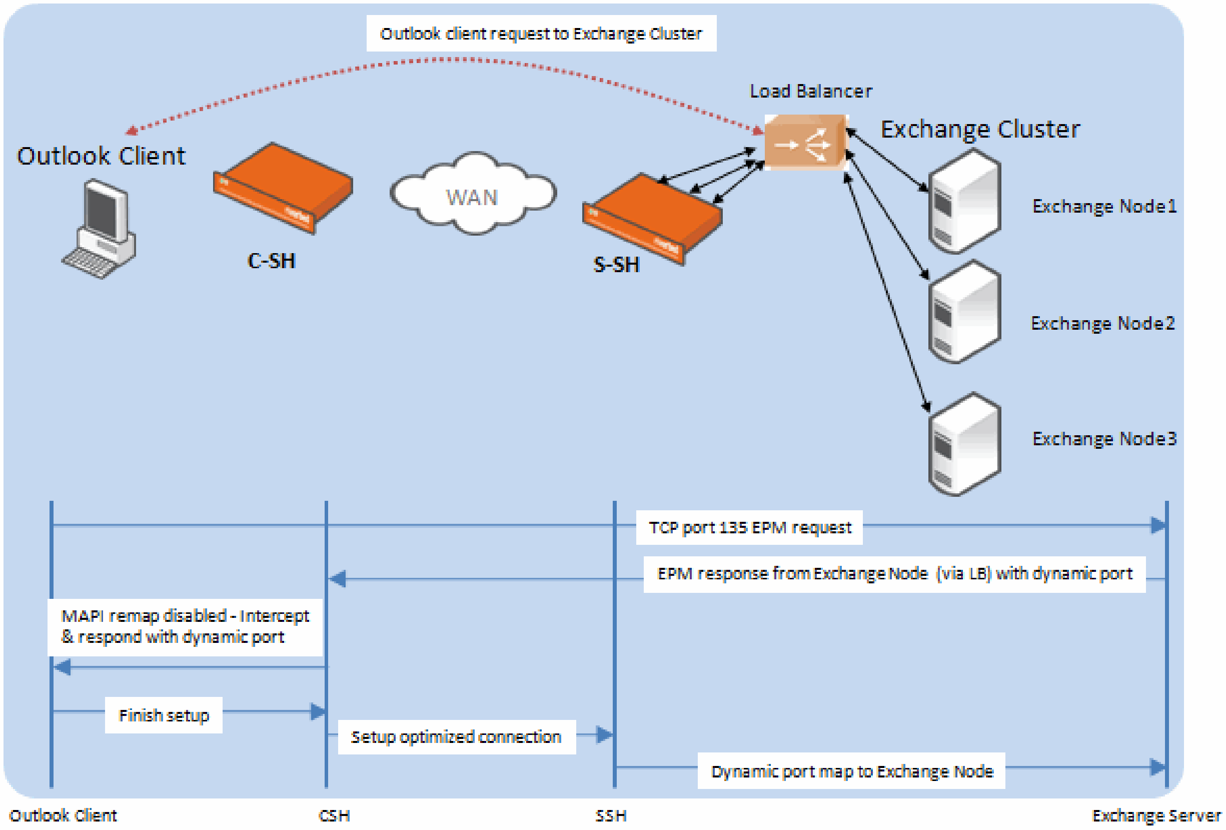

Outlook client request to Exchange Cluster
Load Balancer
Exchange Cluster
Outlook Client
C-SH
WAN
S-SH
Exchange Node1
Exchange Node2
Exchange Node3
TCP port 135 EPM request
EPM response from Exchange Node (via LB) with dynamic port
MAPI remap disabled - Intercept & respond with dynamic port
Finish setup
Setup optimized connection
Dynamic port map to Exchange Node
Outlook Client
CSH
SSH
Exchange Server

Figure A.2-3 Exchange cluster with Load Balancer

A.2.4 - Exchange 2010 architecture

Exchange 2010 takes the architecture of an Exchange server to a much more distributed design. Many of the functions that were handled by the Exchange server as a whole in previous versions of MS Exchange are now split across different “roles” within the Exchange 2010 Architecture. These roles may share the same physical hardware platform, but could also be distributed across multiple platforms for resiliency and scalability.
There are many roles and a complete high-level view in the form of a poster can be downloaded from this location: http://www.microsoft.com/download/en/details.aspx?id=5764

So the use of the name “Exchange Server” can now quite often mean a configuration that contains many separate components often running on separate server instances. For the purposes of this overview explanation we are just going to look at two roles within the Exchange Server, the Client Access Server Array and the Mailbox Server.

A.2.5 - Client Access Server Array

The Client Access Server (CAS) Array serves as a single point of contact for all client connections within an Active Directory location. Although called an “Array” and usually configured as two or more servers for resiliency and scalability, it can comprise of just a single server. The CAS Array does not provide load balancing itself, so a separate load balancing solution would be needed. This is quite often taken care of by installing Microsoft Network Load Balancer (NLB) on the CAS Array but could be provided by separate 3rd party load balancing products.

A.2.6 - Mailbox Server

The Mailbox server is simply the back-end server used for hosting Mailboxes and public folders. Any client requiring access to email messages located on the Mailbox server connects to the CAS Array and it is the service in the CAS Array which communicates with the Mailbox server.

A.2.7 - Basic architectures

As mentioned above, there are other functions in the Exchange 2010 architecture as well as the CAS Array and Mailbox server, but the following diagrams are to help illustrate the basic combinations of these two roles as part of an Exchange server.

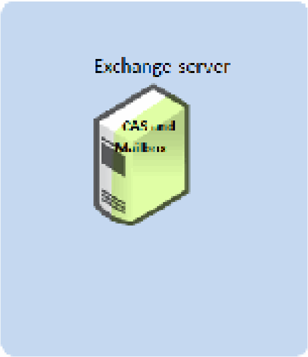


Figure A.2-4
CAS and Mailbox
sharing same hardware

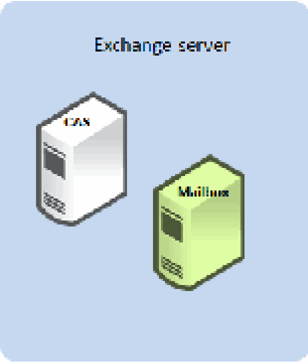


Figure A.2-5
CAS and Mailbox
using separate hardware

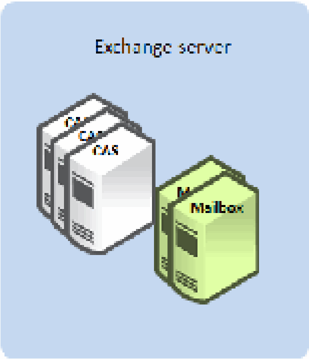


Figure A.2-6
Multiple CAS and Mailbox servers as part
of one Exchange 2010 server configuration

A.2.8 - Client to CAS Array communication

When an Outlook client tries to establish a connection to an Exchange 2010 server the request needs to go to the CAS Array. In the case that there are multiple servers in the Array, some form of load balancing is required.

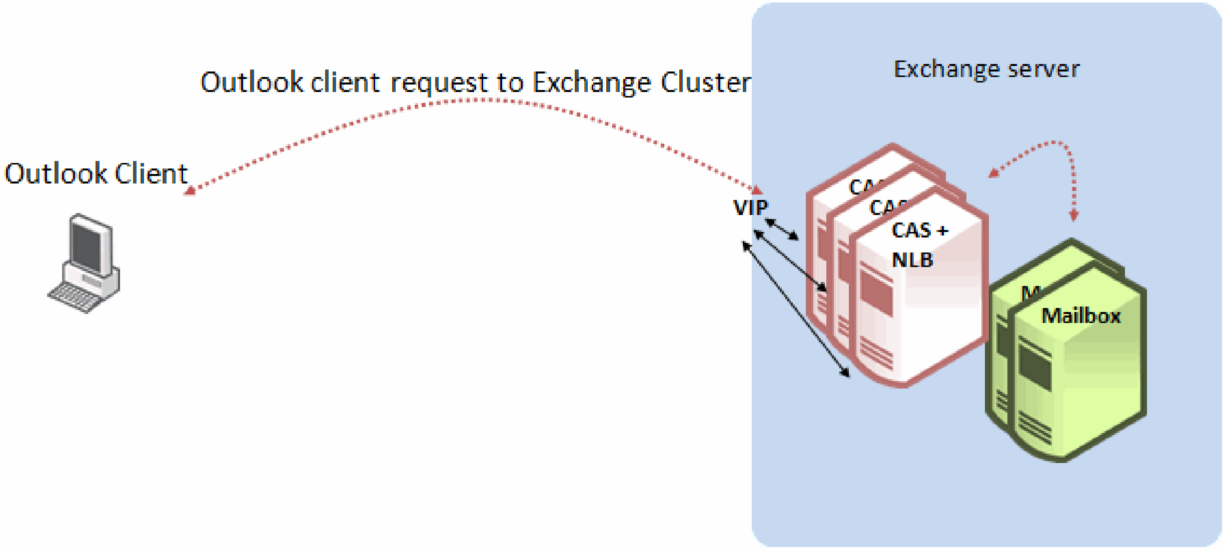


Figure A.2-7 Client EPM request to VIP of Exchange server CAS Array

For the purposes of illustration this example (shown in Figure A.2-7) makes use of Microsoft Network Load Balancer (NLB). NLB software is installed on all members of the CAS Array and one Virtual IP (VIP) is presented for clients. Clients open a connection to the VIP and send an EPM request which is responded to by one of the servers in the CAS Array.

Similarly, when Steelhead appliances are used to optimize MAPI traffic between the clients and Exchange server in this type of configuration, the server-side Steelhead appliance is communicating with the VIP and needs to ensure it keeps track of each individual EPM request per client and the CAS that responds. As described in section A.2.3 (Exchange Cluster with Load Balancer) this is achieved by the server-side Steelhead appliance tracking the IP address in the EPM response. Failure to do so can result in the Outlook client showing random and intermittent disconnection events with the Exchange server. Note that the server-side Steelhead appliance is not communicating with the Mailbox server(s), just the CAS.

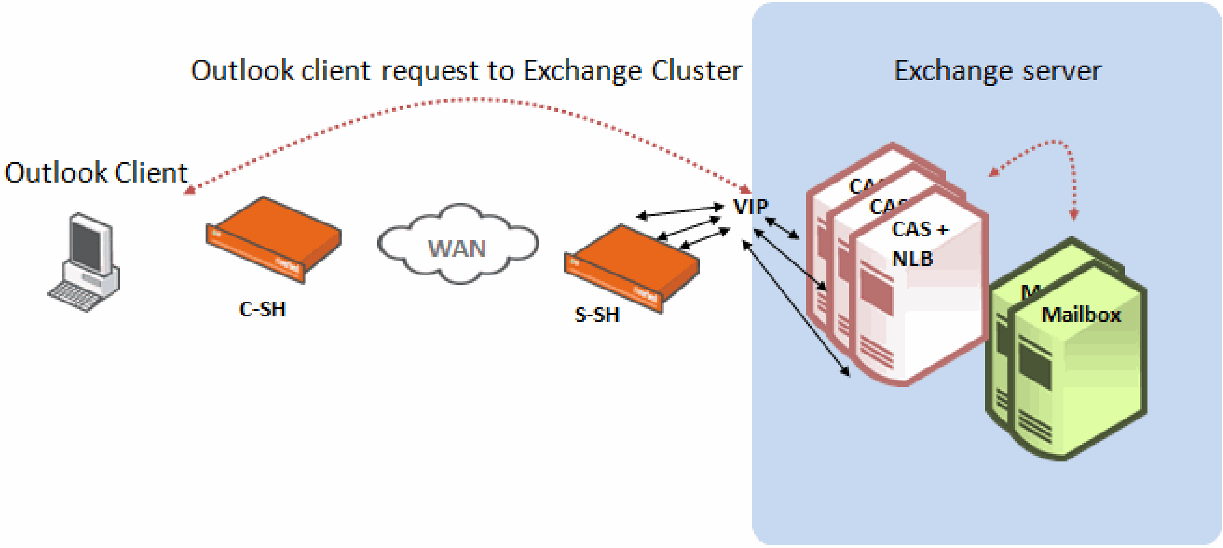


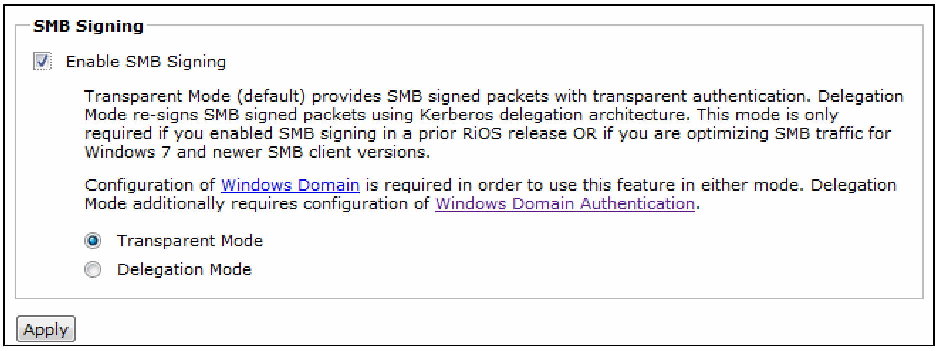
Figure A.2-8 Server-side Steelhead communication with VIP

Figure A.2-8 shows an example of an Exchange server with multiple CAS and Mailbox servers, with the Steelhead appliances providing optimization. Support for optimized connections in this type of configuration is included with later versions of RiOS starting with v6.1.4 and v6.5.1.
As previously mentioned, NLB is used as an example, but the principle is the same if other 3rd party load-balancers are used.

One final point on this type of deployment scenario. There is sometimes the question about optimizing traffic between the CAS array and the Mailbox server. Normally these two components are network connected via “LAN-latency” rather than across a WAN so the thought of optimizing the traffic using Steelhead appliances isn’t a factor. However, even if the CAS array and Mailbox server were separated by a WAN link, optimizing with Steelhead appliances is a configuration that is currently un-tested.

A.3 - Configurations for 1-way trust relationships

In some Windows domains there are only 1-way trusts between domains. This is usually due to a combination of security and management requirements configured by the Windows administrator. In this situation it is useful to know that the RiOS “Delegation Mode” is not supported. Instead, the server-side Steelhead appliance needs to be configured to use “Transparent Mode” for signed SMB, signed SMB2, signed SMB3 and encrypted MAPI. Kerberos authentication is also supported.
Simply set the radio button on the relevant optimization page of the Steelhead appliance GUI to “Transparent Mode”.
See example screenshots (figure A.3-1 and A.3-2) below.



SMB Signing

☑ Enable SMB Signing

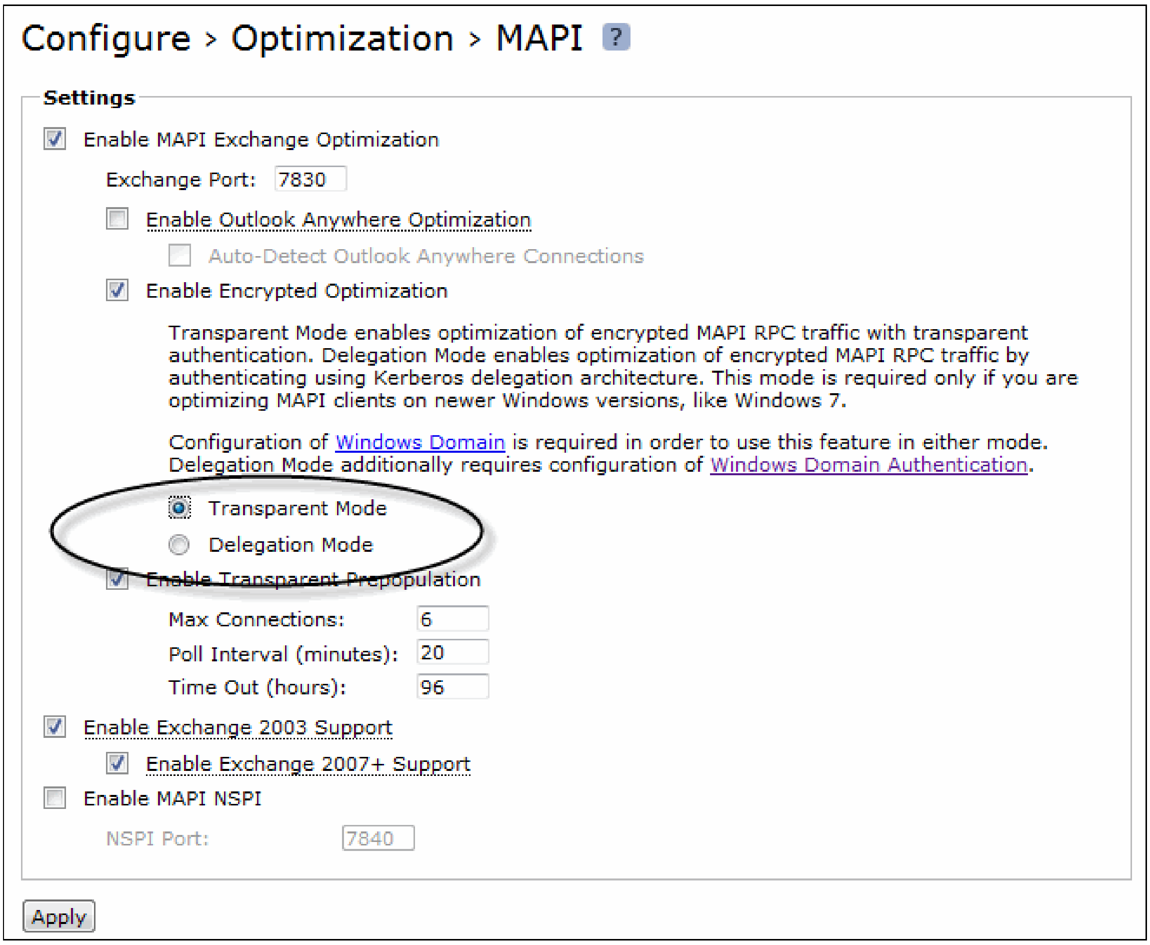
Transparent Mode (default) provides SMB signed packets with transparent authentication. Delegation Mode re-signs SMB signed packets using Kerberos delegation architecture. This mode is only required if you enabled SMB signing in a prior RiOS release OR if you are optimizing SMB traffic for Windows 7 and newer SMB client versions.

Configuration of Windows Domain is required in order to use this feature in either mode. Delegation Mode additionally requires configuration of Windows Domain Authentication.

● Transparent Mode

○ Delegation Mode

Figure A.3-1: Transparent Mode setting on SMB page of Steelhead appliance GUI



Configure > Optimization > MAPI

Settings

☑ Enable MAPI Exchange Optimization

Exchange Port: 7830

□ Enable Outlook Anywhere Optimization

□ Auto-Detect Outlook Anywhere Connections

☑ Enable Encrypted Optimization

Transparent Mode enables optimization of encrypted MAPI RPC traffic with transparent authentication. Delegation Mode enables optimization of encrypted MAPI RPC traffic by authenticating using Kerberos delegation architecture. This mode is required only if you are optimizing MAPI clients on newer Windows versions, like Windows 7.

Configuration of Windows Domain is required in order to use this feature in either mode. Delegation Mode additionally requires configuration of Windows Domain Authentication.

● Transparent Mode

○ Delegation Mode

☑ Enable Transparent Prepopulation

Max Connections: 6

Poll Interval (minutes): 20

Time Out (hours): 96

☑ Enable Exchange 2003 Support

☑ Enable Exchange 2007+ Support

□ Enable MAPI NSPI

NSPI Port: 7840

Figure A.3-2: Transparent Mode setting on MAPI page of Steelhead appliance GUI

When Transparent Mode is used, the server-side Steelhead appliance still needs to join a Windows Domain that has the 1-way trust to the Resource Domain where the server(s) are located. However, there is no need to create Delegate Users.

In addition to setting up Transparent Mode, the server-side Steelhead appliance needs to know the resource domain(s) that have the 1-way trust where the server(s) are located.
This setting is performed via the cli using the following command;

```
# protocol domain-auth oneway-trust dns-name <FQDN> netbios-name <NetBIOS>
```

Where <FQDN> is the Fully Qualified Domain Name of the delegation domain and <NetBIOS> is the NetBIOS name of the delegation domain.
The settings can be displayed using the command;

```
# show protocol domain-auth oneway-trust
```

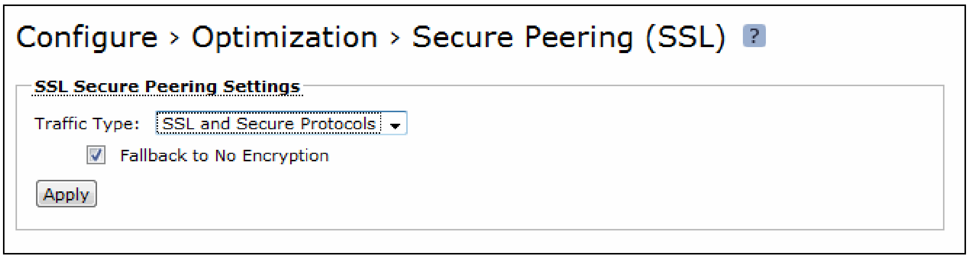
The only other requirement for a server-side Steelhead appliance running a RiOS version prior to v7.0 is that any Windows7 clients will need to have LmCompatibility level set to 2 or lower (this is via a registry setting). Additional details can be found at this location http://technet.microsoft.com/en-us/library/cc960646.aspx

For server-side Steelhead appliance(s) that are running RiOS v7.0 or later, the Steelhead appliance should join the Windows domain using “Active Directory Integrated Windows 2003 Mode” or Windows 2008 Mode (depending on the domain functional level). Although the resource domains with the one-way trusts still need to be added to the Steelhead appliance configuration, there is no need to make registry changes to Windows 7 clients.

A.4 – Secure Peering

It is usually advisable to ensure the optimized traffic [for signed SMB and/or encrypted MAPI] between the peer Steelhead appliances is sent via an encrypted connection. This can easily be achieved by configuring the “Secure Peering” feature on the Steelhead appliances.

To enable this feature, navigate to Configure > Optimization > Secure Peering (SSL).
Toggle Traffic type to *SSL and Secure Protocols* leaving the *Fallback to No Encryption* setting enabled. This will ensure that encrypted MAPI and/or signed SMB is always optimized even if there is no Secure Inner channel set up between the peer Steelhead appliances.
This setting will need to be enabled on both the client-side Steelhead and the server-side Steelhead.



Configure > Optimization > Secure Peering (SSL)

SSL Secure Peering Settings

Traffic Type: SSL and Secure Protocols

☑ Fallback to No Encryption

Figure A.4-1: Enabling Secure Peering

A.5 – Specifying Domain Controllers during a join domain process

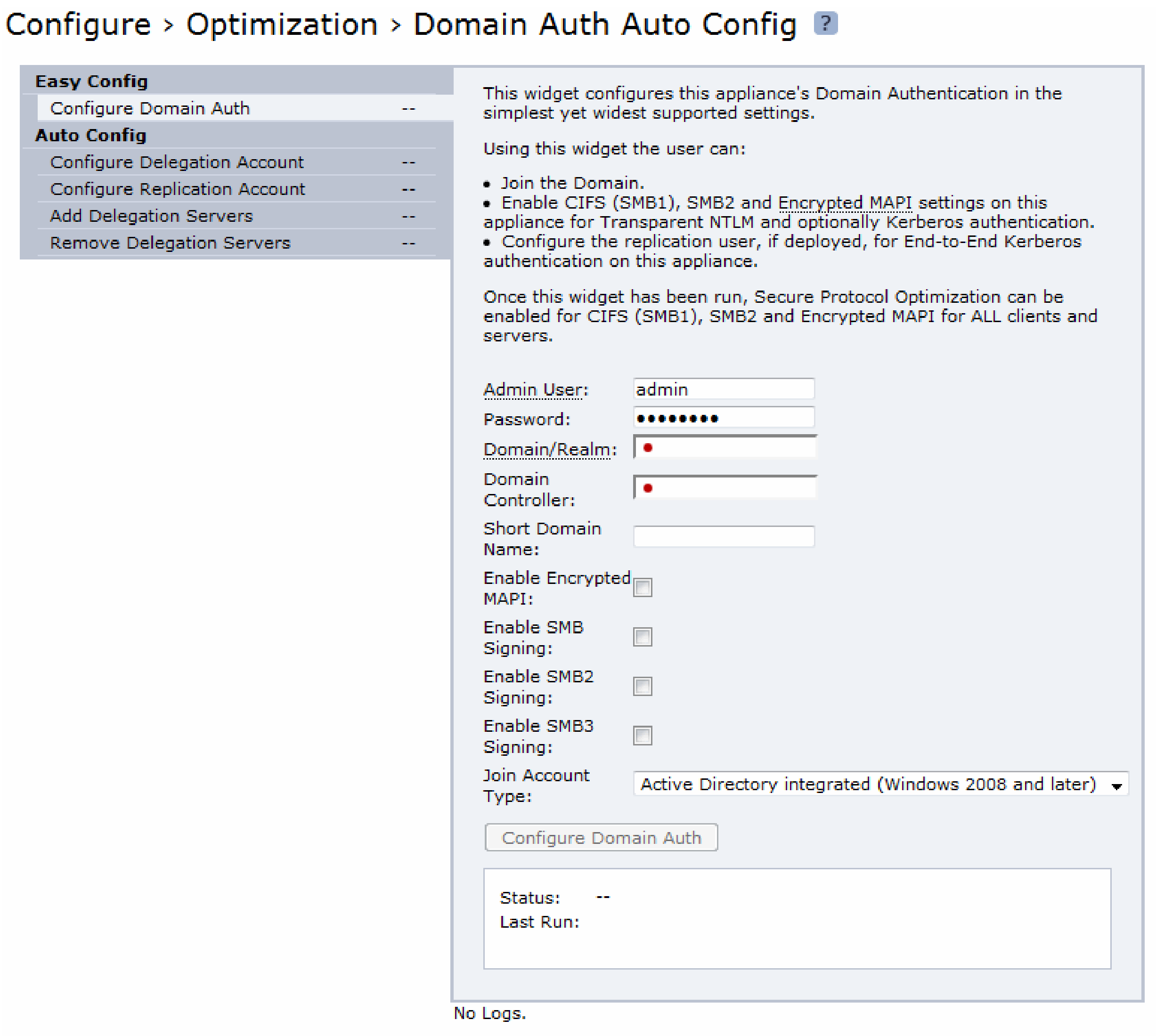
By default, when the server-side Steelhead appliance is joining a Windows Domain, it is not necessary to specify a domain controller (DC). The Steelhead appliance will automatically discover DCs and then select one to request the join.
If the DCs are geographically dispersed and the Steelhead appliance chooses a DC that is some distance away, this may cause delay in the communication between server-side Steelhead appliance and DC. But it is possible to “force” the Steelhead appliance to select a specific DC to communicate with that is nearby. This is done by simply including the IP address or DNS name of the DC in the “Domain Controllers Name” field of the Steelhead appliance GUI page for Windows Domain configuration.
NOTE: This is strongly advised when the Steelhead appliance is joining in Active Directory integrated mode. It is also strongly advised to specify at least two DCs [where possible] in order to provide an alternative.

A.6 – Joining the Steelhead appliance to the domain without using administrator privileges

In some cases, for security reasons, it is not possible to make use of an account with administrator privileges to enable the Steelhead appliance to join the domain. Within a Windows Active Directory environment it is possible to perform the domain join using a pre-created account. Full details and example screenshots are provided in the following knowledgebase article available on the Riverbed support site.
https://supportkb.riverbed.com/support/index?page=content&id=S18097

A.7 – Domain Auth Auto Config – Easy Config widget

As mentioned in several sections of this document, a lot of configuration can now be automated by using the Domain Auth Easy Config widget. The Domain Auth Easy Config widget does not choose the relevant settings but, once chosen by the Steelhead appliance administrator, the widget performs all the configuration tasks automatically. See the example screenshot below for an indication of the settings available.


Configure > Optimization > Domain Auth Auto Config ?
Easy Config
Configure Domain Auth --
Auto Config
Configure Delegation Account --
Configure Replication Account --
Add Delegation Servers --
Remove Delegation Servers --
Configure Domain Auth

This widget configures this appliance's Domain Authentication in the simplest yet widest supported settings.

Using this widget the user can:

- Join the Domain.
- Enable CIFS (SMB1), SMB2 and Encrypted MAPI settings on this appliance for Transparent NTLM and optionally Kerberos authentication.
- Configure the replication user, if deployed, for End-to-End Kerberos authentication on this appliance.

Once this widget has been run, Secure Protocol Optimization can be enabled for CIFS (SMB1), SMB2 and Encrypted MAPI for ALL clients and servers.

Admin User: admin
Password: ••••••••
Domain/Realm: ●
Domain Controller: ●
Short Domain Name:
Enable Encrypted MAPI: □
Enable SMB Signing: □
Enable SMB2 Signing: □
Enable SMB3 Signing: □
Join Account Type: Active Directory integrated (Windows 2008 and later)

Status: --
Last Run:

No Logs.

Figure A.6-1: Domain Auth Easy Config widget

As can be seen in *figure A.6-1* the Domain Auth Easy Config widget contains a number of fields. The first five are for Active Directory tasks (joining the domain, configuring replication user account).The next four are check-boxes for configuring the secure Windows settings on the Steelhead appliance. The last option is a “drop-down” to choose the desired domain join type.
Finally, below the button to actually tell the widget to perform the tasks, there is the status window and the feedback log which are dynamically updated as the widget proceeds through its tasks.
A full explanation of the settings and capabilities of this feature can be found in the Riverbed Steelhead Management Console Users Guide.

Appendix B – Troubleshooting

To confirm full acceleration of the signed SMB and encrypted MAPI applications use the Reports > Networking > Current Connections report in the Steelhead appliance GUI.
Confirm the application flow is optimized by verifying the ‘Established (Optimized)’ symbol (⏩) is present in the ‘Type’ column of the report. If in the ‘Notes’ column the triangular symbol is grey (△) no error is present and full acceleration is applied to the CIFS or MAPI session. This should be further confirmed by checking that the ‘Application’ column is stating “CIFS-SIGNED” or “MAPI-ENCRYPT”, and there should be some degree of data reduction indicated in the ‘Reduction’ column. See *Figure B-2* below for an example.

If there are authentication problems with signed SMB or encrypted MAPI traffic a ‘Protocol Error’ icon (⚠) is displayed in the far right hand column of the report and full acceleration is not applied. See *Figure B-1* below for an example.

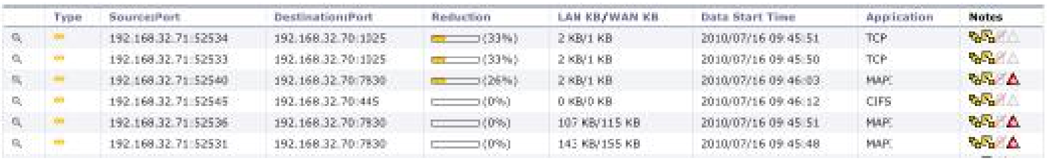
Confirm full acceleration for CIFS with signed SMB and encrypted MAPI:

1. On both Steelhead appliance(s) navigate to Reports > Networking > Current Connections.

2. In the regular expression filter, insert the test client’s IP address and click ‘Update Display.’

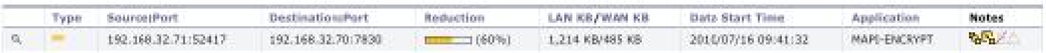
3. To test CIFS with signed SMB on the test client, map a network drive on the test server. To test encrypted MAPI open the Outlook client. It is helpful to move files or send emails during the testing to generate more connections.

4. While the application sessions are open go the Steelheads and update the Current Connections report. Confirm the application flow type is optimized, verify it is the proper host pair, verify it is the proper application and verify the Protocol Error icon’s color. If grey, it is fully accelerated. If red, a protocol error is present. If red, click the ‘details’ icon (🔍) for the connection to see if more information is available. *Figure B-1* shows an encrypted MAPI flow with a protocol error indicating the Steelhead was unable to decrypt the conversation. *Figure B-2* shows an encrypted MAPI flow that was properly optimized. One other item which indicates the MAPI flow was properly optimized is the designation of MAPI-ENCRYPT in the Application column.



	Type	Source:Port	Destination:Port	Reduction	LAN KB/WAN KB	Data Start Time	Application	Notes
🔍	⏩	192.168.32.71:52534	192.168.32.70:1025	(33%)	2 KB/1 KB	2010/07/16 09:45:51	TCP	△
🔍	⏩	192.168.32.71:52533	192.168.32.70:1025	(33%)	2 KB/1 KB	2010/07/16 09:45:50	TCP	△
🔍	⏩	192.168.32.71:52540	192.168.32.70:7830	(26%)	2 KB/1 KB	2010/07/16 09:46:03	MAPI	⚠
🔍	⏩	192.168.32.71:52545	192.168.32.70:445	(0%)	0 KB/0 KB	2010/07/16 09:46:12	CIFS	△
🔍	⏩	192.168.32.71:52536	192.168.32.70:7830	(0%)	107 KB/115 KB	2010/07/16 09:45:51	MAPI	⚠
🔍	⏩	192.168.32.71:52531	192.168.32.70:7830	(0%)	143 KB/155 KB	2010/07/16 09:45:48	MAPI	⚠

Figure B-1: Encrypted MAPI flows with protocol error

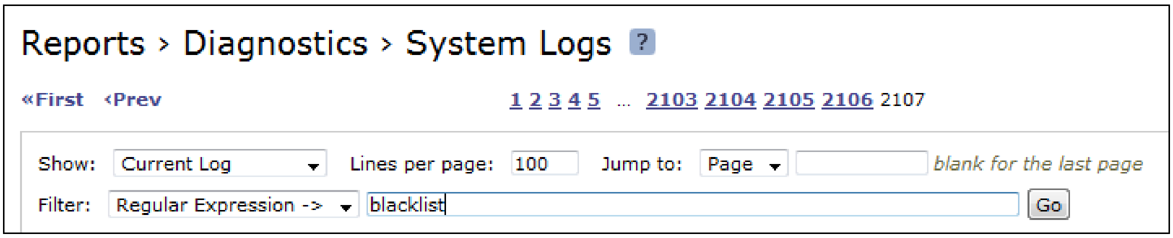


	Type	Source:Port	Destination:Port	Reduction	LAN KB/WAN KB	Data Start Time	Application	Notes
🔍	⏩	192.168.32.71:52417	192.168.32.70:7830	(60%)	1,214 KB/485 KB	2010/07/16 09:41:32	MAPI-ENCRYPT	△

Figure B-2: Encrypted MAPI flows properly optimized

5. If a protocol error is present and more details are not available in the ‘details’ view (🔍) of the connection you will need to look at the system logs for more information. Navigate to Reports > Diagnostics > System Logs. It is also worth changing the logging level to “INFO” for a period of time, but remember to restore the level to “NOTICE” once you have finished.

6. In the regular expression filter enter the test client IP address and click ‘Go’. You may also find it helpful to filter on keywords like; smb, cifs, cifs-auth, domain, krb or mapi.



Reports > Diagnostics > System Logs

«First ‹Prev 1 2 3 4 5 ... 2103 2104 2105 2106 2107

Show: Current Log Lines per page: 100 Jump to: Page blank for the last page

Filter: Regular Expression -> blacklist

Figure B-3: Steelhead System Logs Report

7. Be on the lookout for messages indicating authentication errors, servers or clients being “blacklisted”, etc. if there are any errors that cause clients or servers to become blacklisted, this can be confirmed by using the following cli commands….

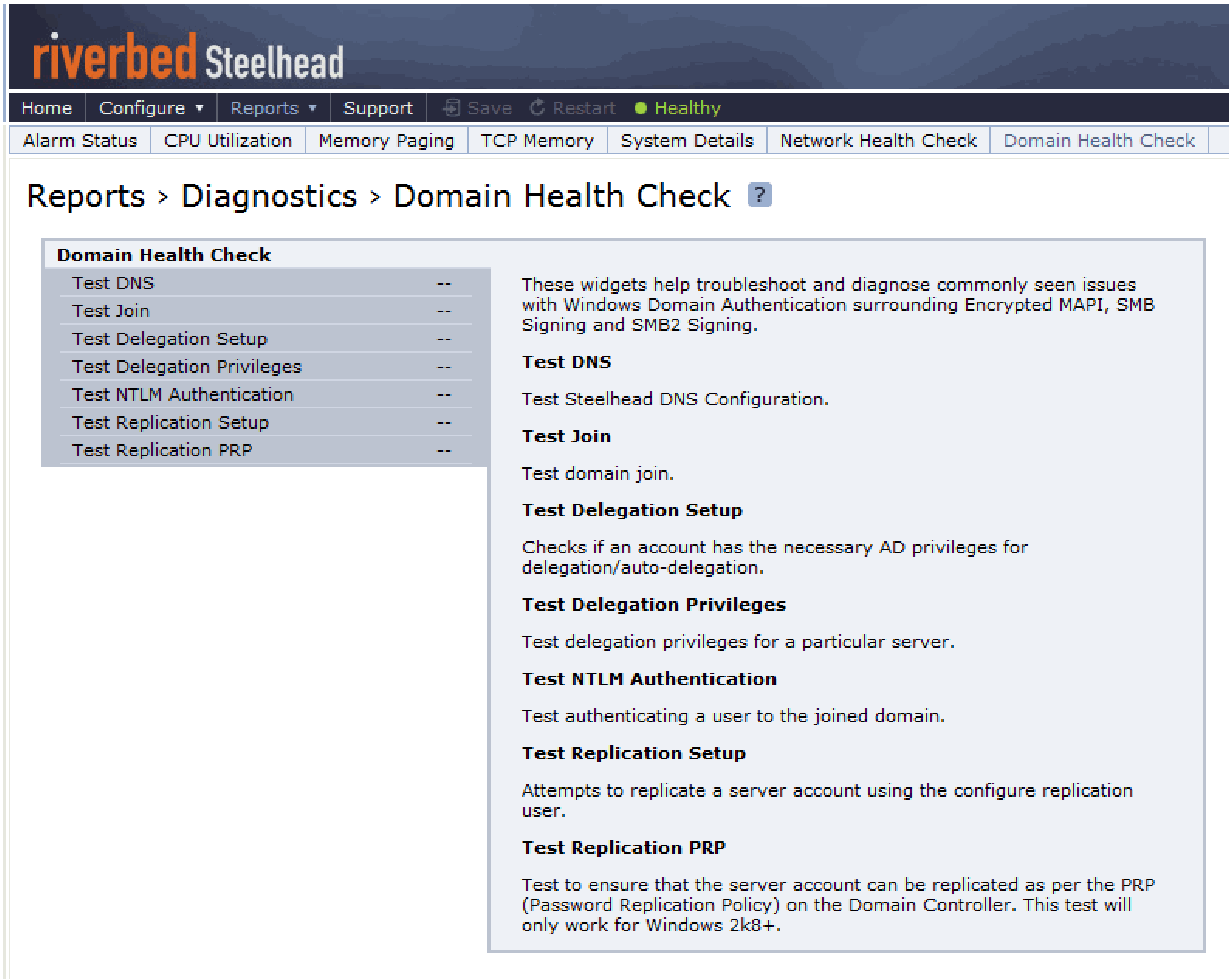
```
# show protocol cifs smb signing blacklist

# show protocol smb2 signing blacklist

# show protocol mapi encrypted blacklist
```

   These commands show the current entries on the blacklist for each of the three protocols. If you have SMB3 traffic being optimized, protocol errors will be entered into the SMB2 blacklist. This is because the SMB2 optimization feature in RiOS is also used to optimize SMB3 traffic. If the error causing the blacklist event is transient, the entry on the list will clear automatically after time. If the error is more persistent, or you wish to manually clear the blacklist, please make contact with Riverbed Support via the normal process to request help and guidance.

8. Analyze the findings and take appropriate action. If assistance is required search the Knowledge Base at (http://support.riverbed.com) and if you have a valid support contract, you could contact Riverbed Support (877-483-7233 or http://support.riverbed.com).

With RiOS v7.0 and later, there is a new feature known as Windows Domain Health Status. This feature comprises of several cli commands which can be used to test and display various settings and configurations on the server-side Steelhead. An overview is included in the latest version of the Riverbed Deployment Guide (“Protocols” edition) and full details of the commands and their syntax are provided in the latest version of the Riverbed Steelhead appliance cli manual.

With RiOS v8.5 and later the Windows Domain Health Status command have been brought out into the Steelhead appliance management console as a series of graphical tools.
An example screenshot of the Domain Health Check page is shown below.



Reports › Diagnostics › Domain Health Check ?

Domain Health Check	
Test DNS	--
Test Join	--
Test Delegation Setup	--
Test Delegation Privileges	--
Test NTLM Authentication	--
Test Replication Setup	--
Test Replication PRP	--

These widgets help troubleshoot and diagnose commonly seen issues with Windows Domain Authentication surrounding Encrypted MAPI, SMB Signing and SMB2 Signing.

Test DNS

Test Steelhead DNS Configuration.

Test Join

Test domain join.

Test Delegation Setup

Checks if an account has the necessary AD privileges for delegation/auto-delegation.

Test Delegation Privileges

Test delegation privileges for a particular server.

Test NTLM Authentication

Test authenticating a user to the joined domain.

Test Replication Setup

Attempts to replicate a server account using the configure replication user.

Test Replication PRP

Test to ensure that the server account can be replicated as per the PRP (Password Replication Policy) on the Domain Controller. This test will only work for Windows 2k8+.

Figure B-4: Domain Health Check page in Steelhead appliance Management Console

For more details on the use of the tests, consult the latest version of the Riverbed Steelhead Management Console Users Guide.

riverbed

Riverbed Technology, Inc.
199 Fremont Street
San Francisco, CA 94105
Tel: (415) 247-8800
www.riverbed.com

Riverbed Technology Ltd.
One Thames Valley
Wokingham Road, Level 2
Bracknell. RG42 1NG
United Kingdom
Tel: +44 1344 401900

Riverbed Technology Pte. Ltd.
391A Orchard Road #22-06/10
Ngee Ann City Tower A
Singapore 238873
Tel: +65 6508-7400

Riverbed Technology K.K.
Shiba-Koen Plaza Building 9F
3-6-9, Shiba, Minato-ku
Tokyo, Japan 105-0014
Tel: +81 3 5419 1990