MATRIX42
SMARTER WORKSPACE – BETTER LIFE

Silverback Mail Gateway
Installation Guide

Version 1.5

1. December 2015

Copyright © 2000 - 2014 Matrix42 AG

Contents

1. Introduction

This guide will help you deploy the Silverback and ActiveSync Silverback Mail Gateway. You can publish either Exchange ActiveSync or IBM Traveler using the Silverback Mail Gateway. This allows you to add multiple services to work together to spread the load of incoming devices across multiple 'nodes'.

If you need to enable Enterprise Certificate Authority on the SMG then it will be enabled for all services. Enterprise Certificate Authentication will stop Silverback from working if it is being published through the SMG.

2. Prerequisites

You need to make sure you have a Computer that is configured to be on the same network as the Silverback Mail Gateway. The configuration needs to be via Remote Desktop Protocol.

2.1. Account requirements and Permissions

To configure the Silverback Mail Gateway you will need to have an Administrative account. You will need to login using an admin account to do the necessary configuration.

2.2. Network and System Requirements

The Silverback Mail Gateway runs on Windows Server 2012. Install and patch a Windows 2012 server.

Incoming traffic

The Smartphones and tablets communicate via HTTPS (TCP Port 443), so this needs to be opened from the Internet to the Silverback Mail Gateway (SMG).

Outgoing traffic

Open the following outgoing traffic from the Silverback Mail Gateway:

- OSCP traffic: usually port http 80 (recommended by IT industry) to the destination OSCP endpoint, but also 443 in case of https
- CRL traffic: usually port http 80 (recommended by IT industry) to the destination CRL endpoint, but also 443 in case of https

2.3. SMG External DNS & SSL certificate

An external DNS address and correspondent SSL certificate is required for the incoming email client traffic from the internet, e.g. smg.customer_domain.com .

3. Initial Setup & Activation of your Silverback Mail Gateway

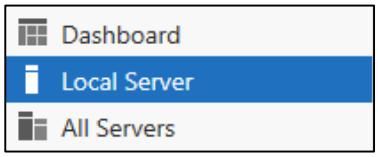
This will guide you through publishing Silverback and ActiveSync through the Matrix42 Silverback Mail Gateway.

3.1. Installing Internet Information Server

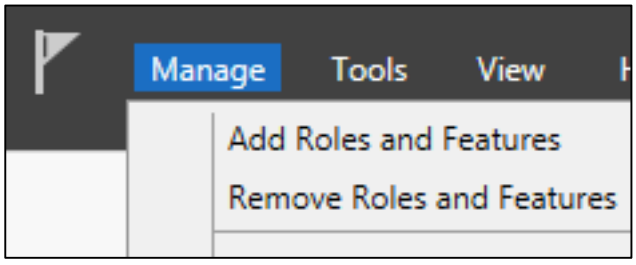
If you are competent at installing IIS and .NET 3.5.1, please skip to section 3.2

- Launch Server Manager

- Select ‘Local Server’ on the left hand navigation



- Click Manage and select ‘Add Roles and Features’

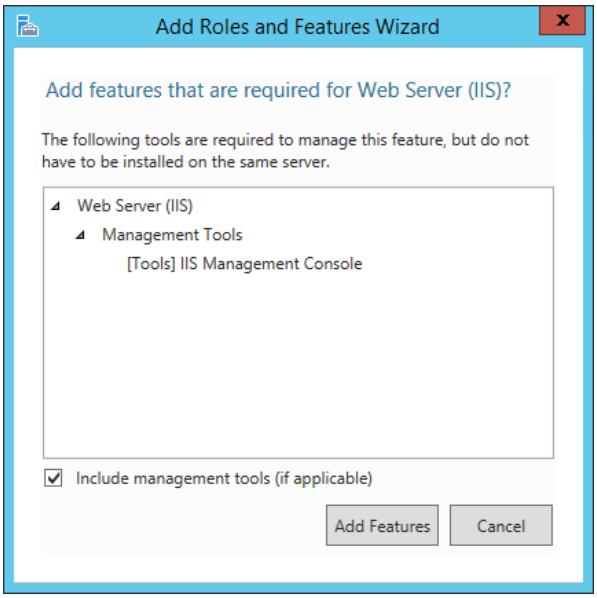


Silverback Mail Gateway

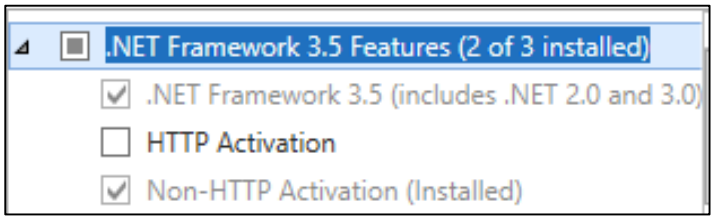
Click Next > Select Role-Based installation.
Click Next > Select your server
Click Next

- Tick ‘Web Server (IIS)

- Click ‘Add Feature’ > Click Next



- Select .Net Framework 3.5



- Click Next, Next, Next, Install

Silverback Mail Gateway

- To enable the required features run the following PowerShell :

```
Import-Module ServerManager
Add-WindowsFeature Web-Static-Content,Web-Default-Doc,Web-Dir-Browsing,Web-Net-Ext,Web-
Request-Monitor,Web-Http-Tracing,Web-Filtering,Web-Stat-Compression,Web-Mgmt-Console,NET-
Framework-Core,NET-Non-HTTP-Activ,NET-HTTP-Activation
```

- Check that it works:

```
Success Restart Needed Exit Code      Feature Result
 ------- -------------- ---------      --------------
 True    No             Success        {HTTP Activation, Application Development,...
```

- Hardening your SSL Stack: This is an optional step.

If you don't want your SSL stack hardened, then skip this step. If you have your own SSL hardening guide then apply it instead.

You may want to use the following hardening script. Download below script, open PowerShell ISE, and run the script in the PowerShell:

http://www.hass.de/content/setup-your-iis-ssl-perfect-forward-secrecy-and-tls-12

Alternatively you can download the script from the Matrix42 Knowledge Base and run it as administrator:
https://help.matrix42.com/03_Matrix42_Mobile/00_Silverback/Environmental_Configuration/SMG_IIS_SSL_Hardening_Powershell_Skript

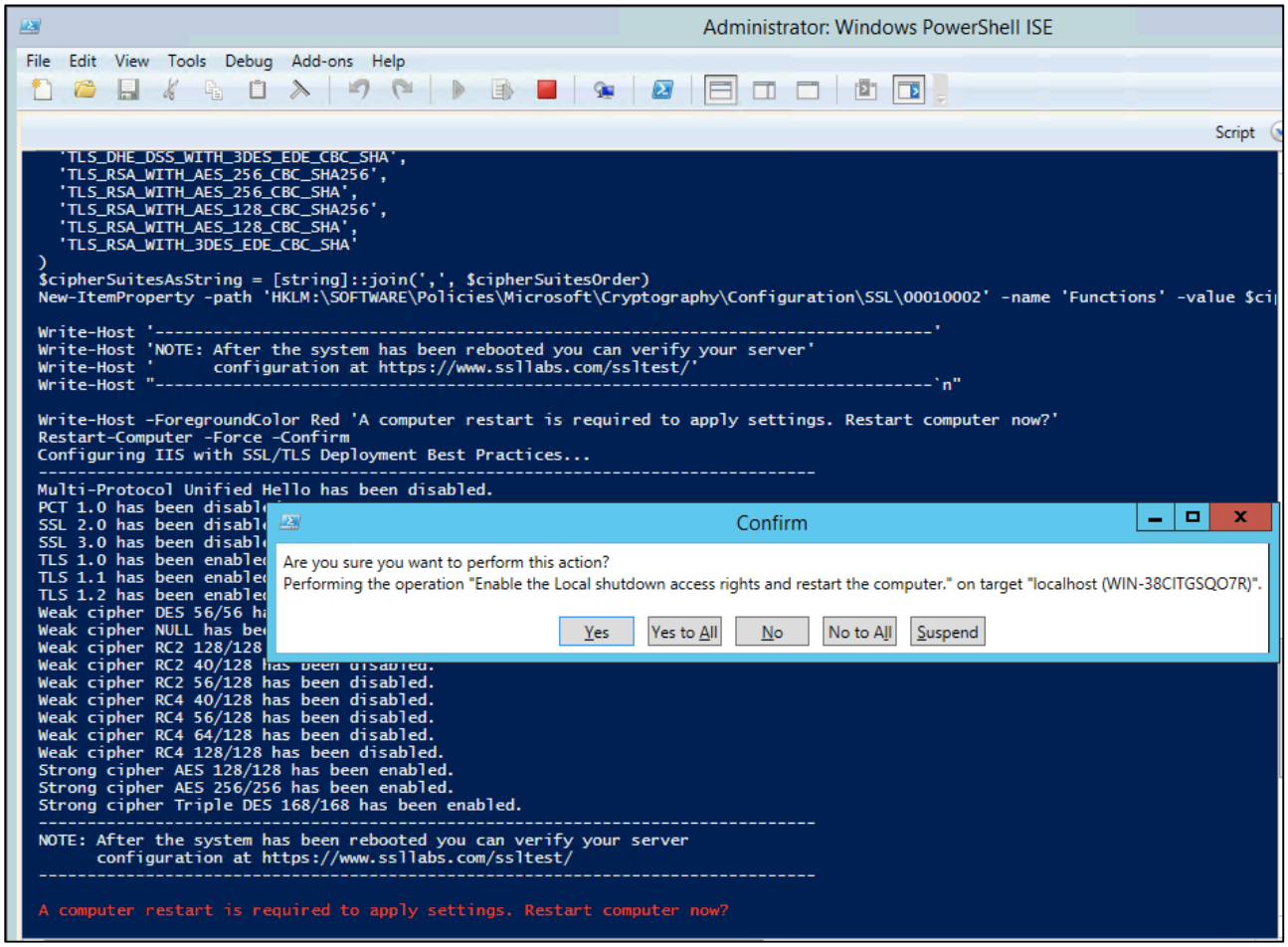
```
# Copyright 2014, Alexander Hass
# http://www.hass.de/content/setup-your-iis-ssl-perfect-forward-secrecy-and-tls-12
#
# Version 1.4
# - RC4 has been disabled.
# Version 1.3
# - MD5 has been disabled.
# Version 1.2
# - Re-factored code style and output
# Version 1.1
# - SSLv3 has been disabled. (Poodle attack protection)

Write-Host 'Configuring IIS with SSL/TLS Deployment Best Practices...'
Write-Host '------------------------------------------------------------------------------
---'

# Disable Multi-Protocol Unified Hello
. . . . .
```

Silverback Mail Gateway

- You will need to restart the computer, Click ‘Yes’ or ‘Yes to All’



Silverback Mail Gateway

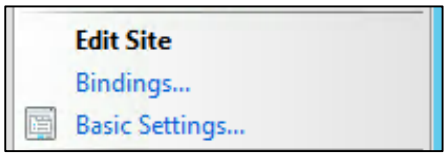
3.2. Import SSL Certificate and bind to the site

Devices must communicate over HTTPS and trust the server, to ensure the data in transit is encrypted; therefore the SSL Certificate on the web services that the devices access must be from a certificate authority trusted by the devices.

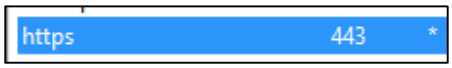
It's recommended that you purchase a Subject Alternate Name (SAN) or Wildcard certificate, e.g. ***.company.com**. This will ensure that devices will trust the server no matter what endpoint they connect to.

The certificate should be installed on the Silverback Mail Gateway and bound to the Silverback website.

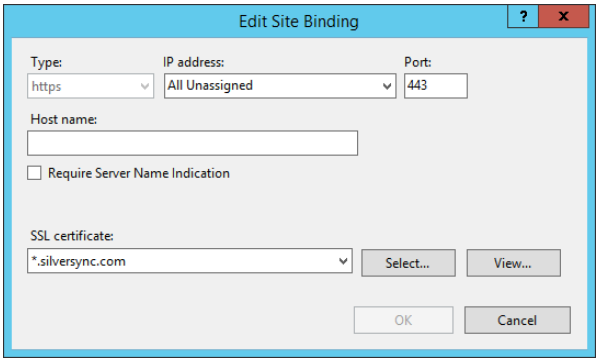
- Open IIS Manager and select the 'Default Web Site' and click 'Bindings'



- Select 'https 443' and click 'Edit…" :



- Select your certificate from the 'SSL Certificate' drop down and click OK.



- Close the IIS Management console

3.3. Install Application Request Routing

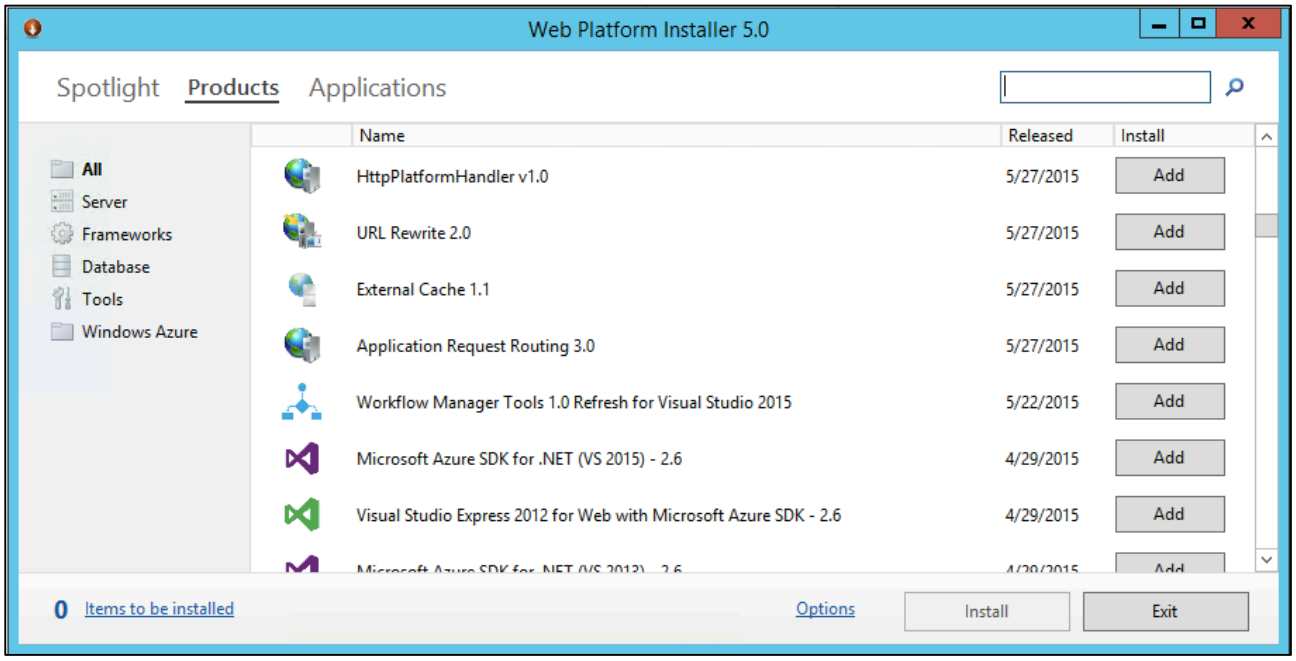
You need to Download and install the latest version on Application Request Routing. Several years ago, Microsoft introduced the **Web Platform Installer** (WebPI) mechanism, which makes it easy to manage installed components. It's used with many things, and is the preferred way to install ARR and all its components properly and easily.

3.3.1. Install ARR using Web Platform Installer

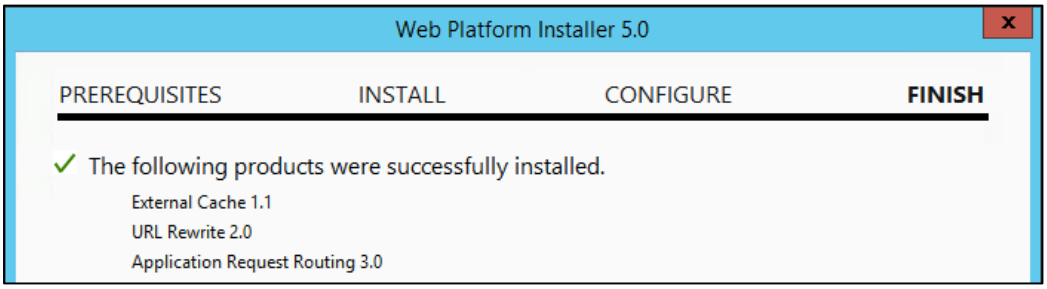
- Download and install the Web Platform Installer from here:

  http://www.microsoft.com/web/downloads/platform.aspx
  Once it installs, it will launch automatically.

- From the 'Products' section find 'Application Request Routing', click 'Add' and 'Install'.



- This will install ARR and all its dependencies. Exit WPI once is finishes.



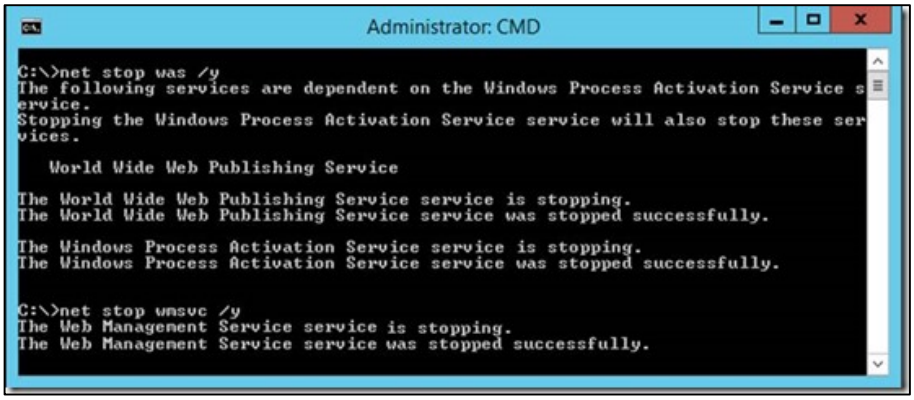
3.3.2. Install ARR Manually

Microsoft's Application Request Router (ARR) IIS Extension is a complex piece of software, which integrates with several other components to do its job. These components are URL Rewrite, Web Farm Framework and ARR's External Cache module. For things to work correctly, not only do you need all components, but they must also be installed in a specific order, which can be confusing.

Occasionally, though, you might find yourself in a situation where you still prefer to avoid using the WebPI installation option. If so, another option you have is installing it using the IExpress package, which includes all the components together.

Another option is to install the components by hand, which will require you to download the components separately. This is the procedure:

- Stop IIS first by typing **net stop was /y** and **net stop wmsvc /y** on an elevated command-line window:



- Download and install the URL Rewrite module.
  http://www.iis.net/downloads/microsoft/url-rewrite
- Download and install the Web Farm Framework module.
  http://www.iis.net/downloads/microsoft/web-farm-framework
- Download and install ARR itself.
  http://www.iis.net/downloads/microsoft/application-request-routing
- Download and install the External cache module.
  http://download.microsoft.com/download/3/4/1/3415F3F9-5698-44FE-A072-D4AF09728390/ExternalDiskCache_amd64_en-US.msi

Start the IIS services (or, simply reboot your server) and you should be good to go!

3.4. Publishing Silverback and ActiveSync using ARR

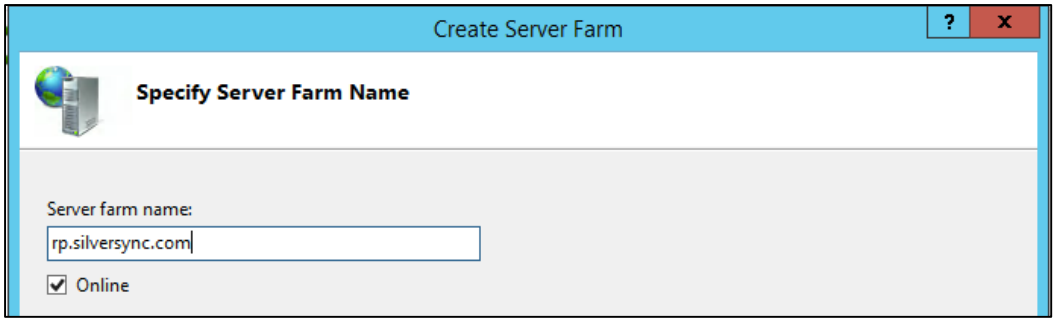
To publish Silverback and ActiveSync using Application Request Routing we need to create a server farms, implement health checking and configure URL Rewrite rules.

3.4.1. Create an Exchange ActiveSync or Traveler server Farm

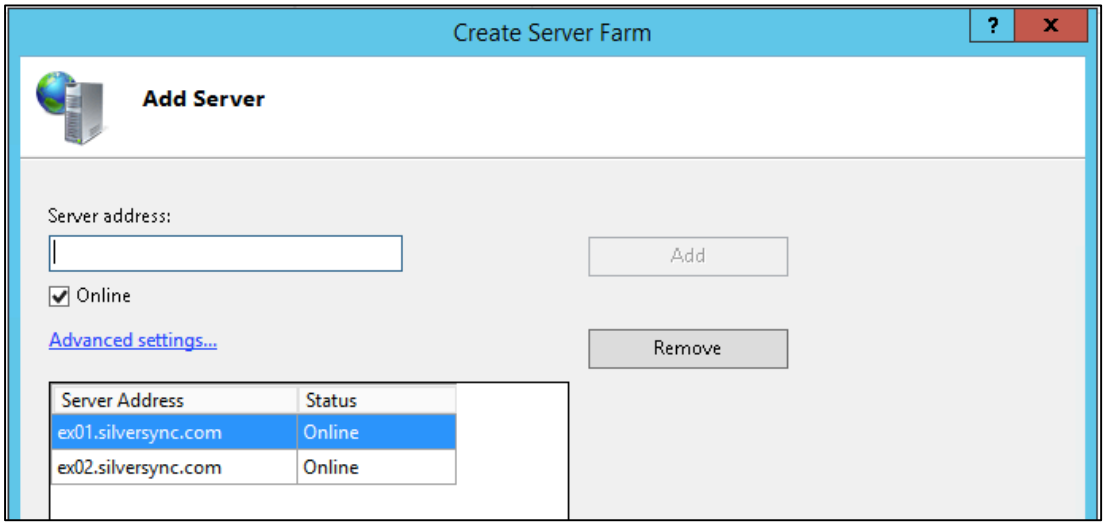
We need to create a server farm to publish Exchange ActiveSync or Domino Traveler.

- Open IIS and click on **Server Farm**.
- Click 'Create Server Farm…' and give it a name as shown below.
  - This should be the internal URL of the ActiveSync / Traveler server.

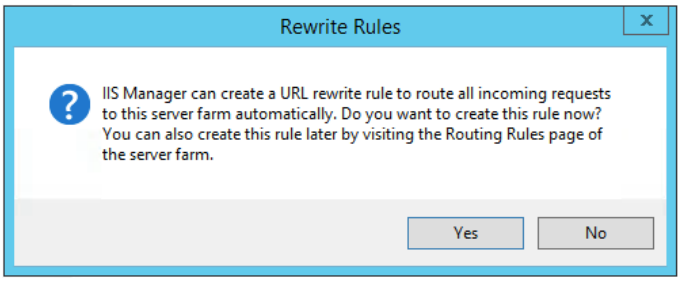
    This host name is used to build the URL re-writing rules so it must match the backend hostname. If the backend server is "Intranet" then the farm must be to.



- Click Next.
- On the **Add Server** page, add each of the Client Access servers and click **Finish**.
  - This should be the internal URL for the CAS servers.

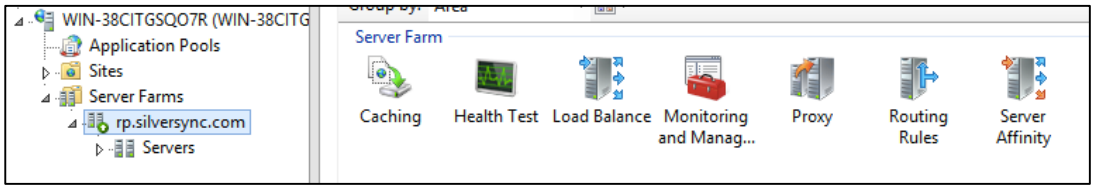


- Select **Yes** at the below prompt.



3.4.2. ActiveSync Server Farm Configuration Changes

Open the **Server Farm** settings node to make configuration changes.



- Select **Caching** and choose **Disable Disk Cache**.

- Select **Health Test**. This is used to make sure that a particular application is up and running:

In Exchange 2013 there is a new component called Managed Availability and it uses various checks to make sure that each of the protocols are up and running. We are going to leverage one of these checks to make sure that the service/protocol is available.

https://<fqdn>/<protocol>/HealthCheck.htm is the default web page present in Exchange 2013. These URL's are specific for each protocol and do not have to be created by the administrator.

Silverback Mail Gateway

- Configure the **Health Test.**

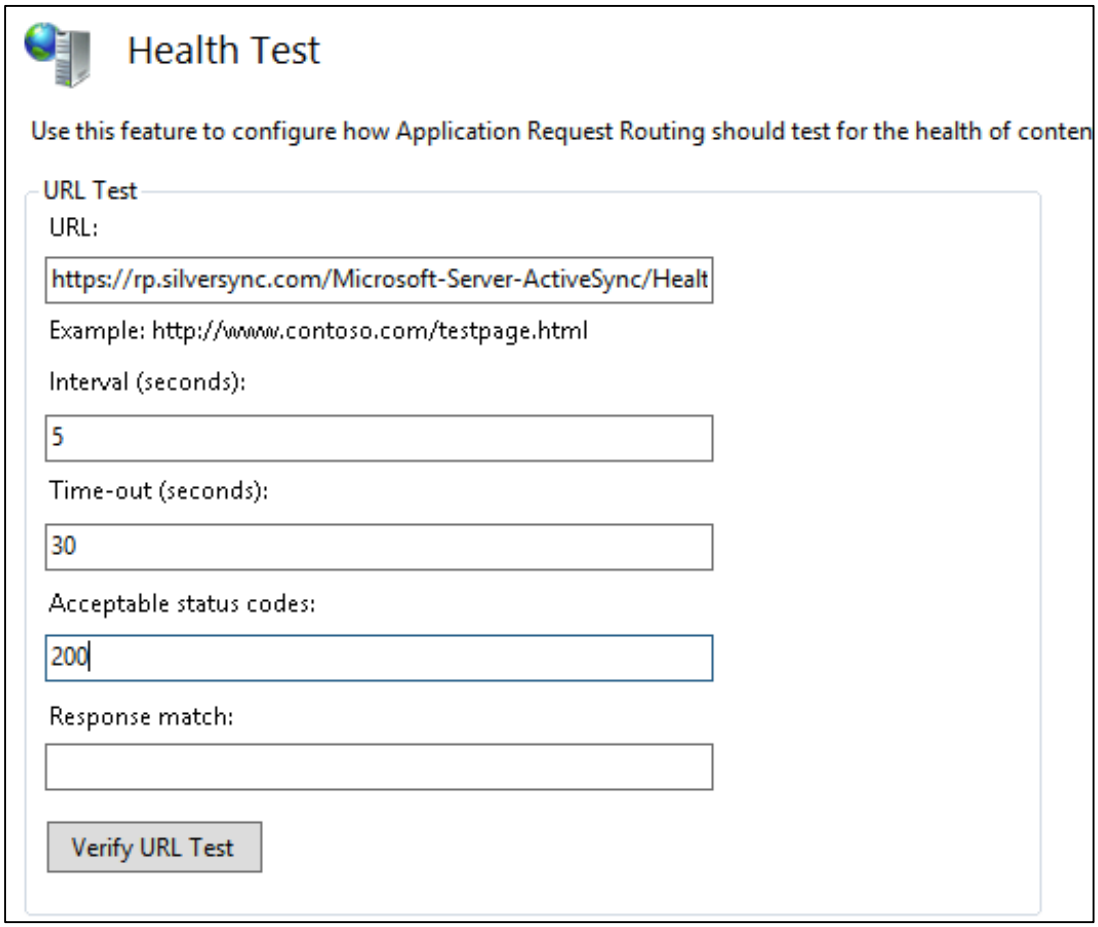
We are not rewriting the URL before the backend server receives the traffic so the host header in the traffic is still the external URL. We therefore need to test that the external URL works against the internal servers. You can amend this if you are an advanced user, but this is not covered in this guide. Configure with the following settings:

URL: https://rp.silversync.com/Microsoft-Server-ActiveSync/HealthCheck.htm

Interval: 5 seconds

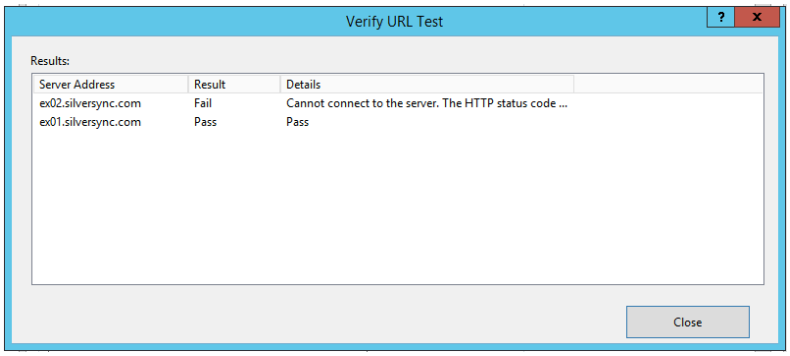
Time-Out: 30 seconds

Acceptable Status Code: 200



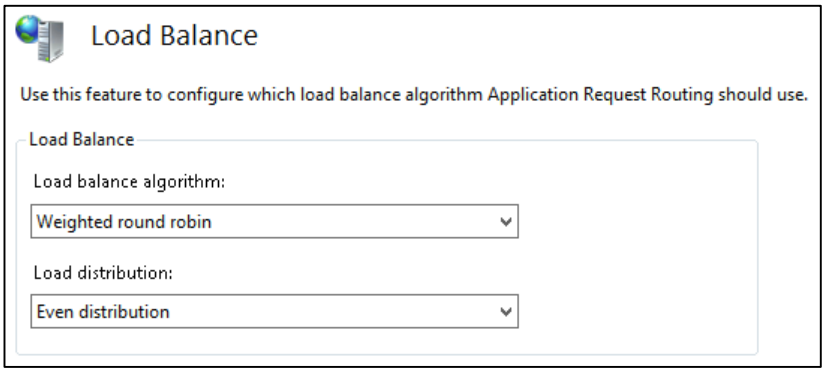
Silverback Mail Gateway

- Click Verify URL to Test, and they should pass.
  - This confirms the internal server is accessible.

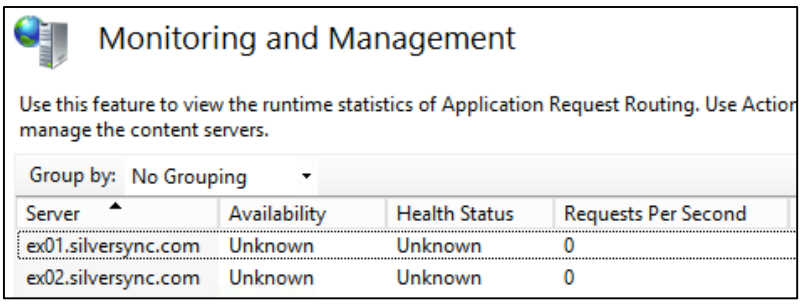


We shutdown ex02.silversync.com so you can see what an inaccessible server response looks like.

- Select **Load Balance** and choose **weighted round robin**. There are other options, but for this scenario, we find this to be simple and effective.

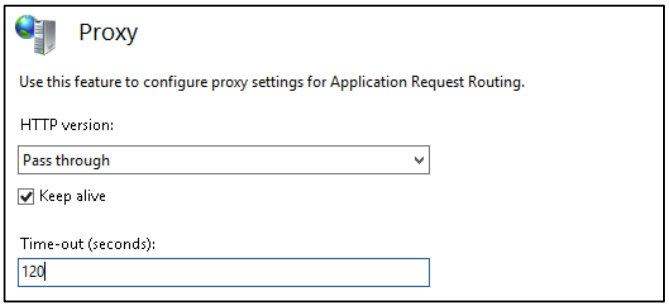


- Select **Monitoring and Management**. This shows the current state of the CAS servers that are part of this Server Farm. The Health Status is based on the output of the **Health Test** mentioned above.

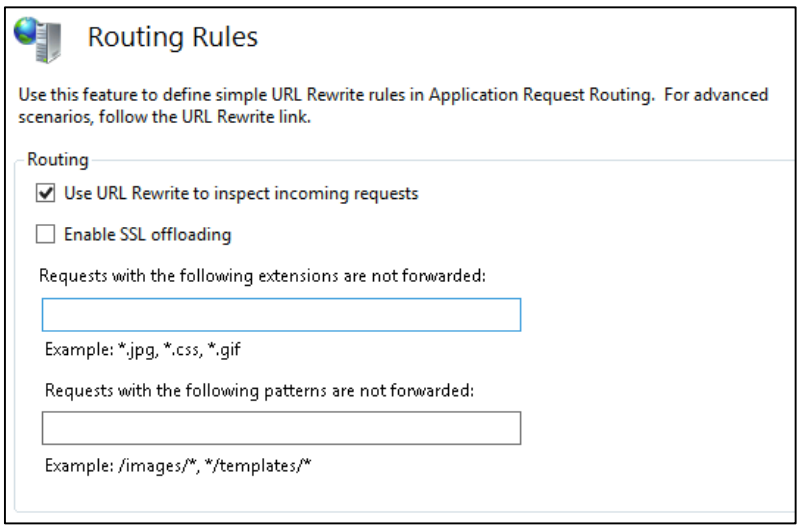


- Select **Proxy**. Change the below values. The actual value for these settings may need to be tweaked for your deployment, but these usually work well as a starting point.

Silverback Mail Gateway



- If you are using Exchange 2013 or SSL Re-encryption select **Routing Rules** and uncheck **Enable SSL Offloading.** If you are using SSL Offloading then check it.

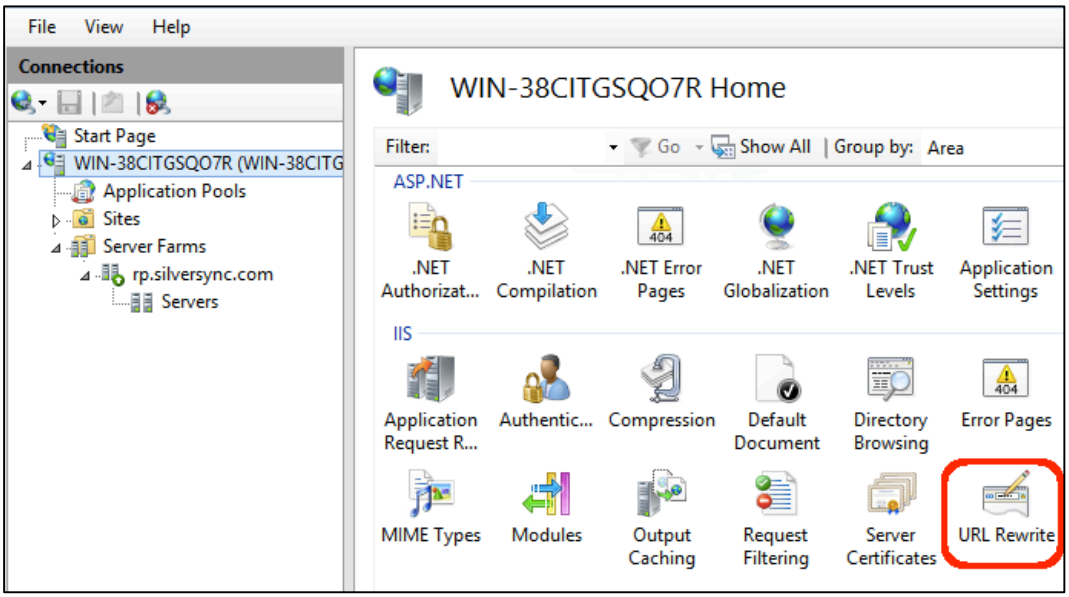


- Select **Server Affinity**. As long as you can get to a CAS server, you will be able to access your mailbox. No changes required.

Silverback Mail Gateway

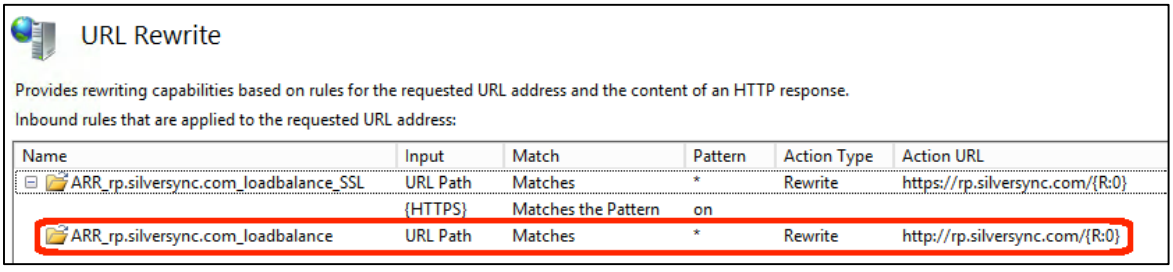
3.4.3. Create ActiveSync URL Rewrite Rules

- At the IIS Root and click on URL Rewrite.



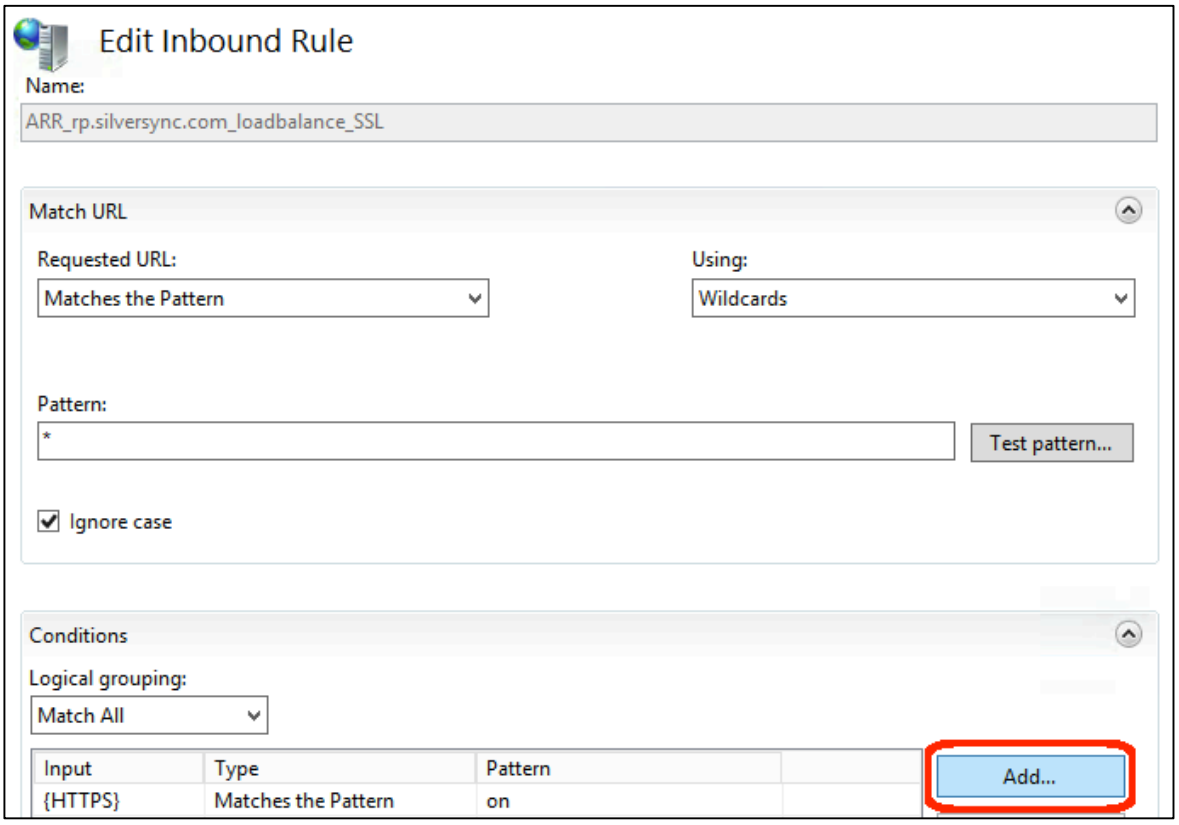
You should see two URL Rewrite rules already created.

- **Select** the HTTP rule and press Remove.

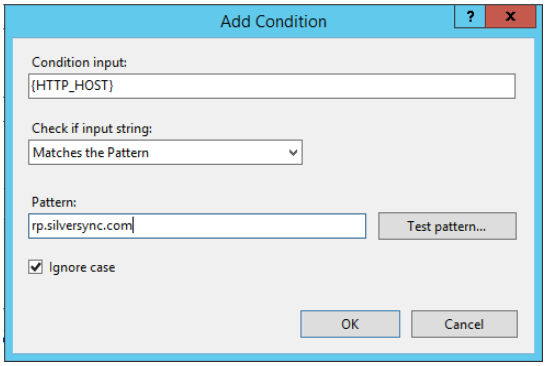


Silverback Mail Gateway

- Open the properties of the **SSL** rule. Under **Conditions** Click Add:



- Add a HTTP HOST for the external server FQDN, as below:



- Under **Action** make sure that you have the below options set i.e.: choose the appropriate Server Farm from the drop down menu.

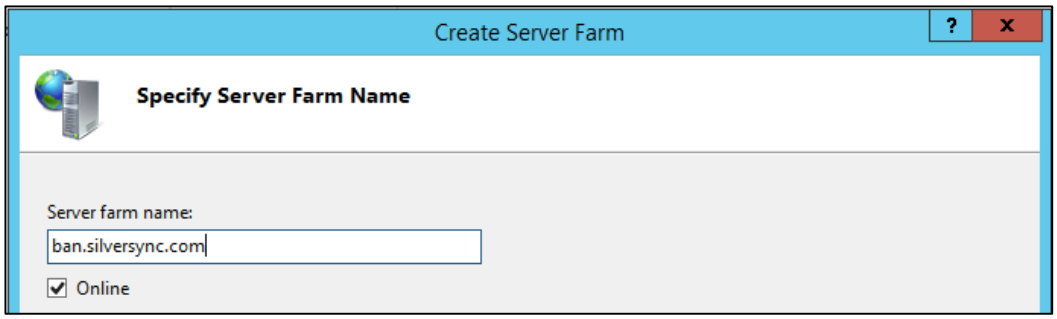
Note: Make sure the option “Stop processing of subsequent rules” is selected. This is to make sure that the validation process stops once the requested URL finds a match.

- **Repeat** the same steps for creating a Server Farm and URL Rewrite rule for Silverback.

3.4.4. Create a Silverback server Farm

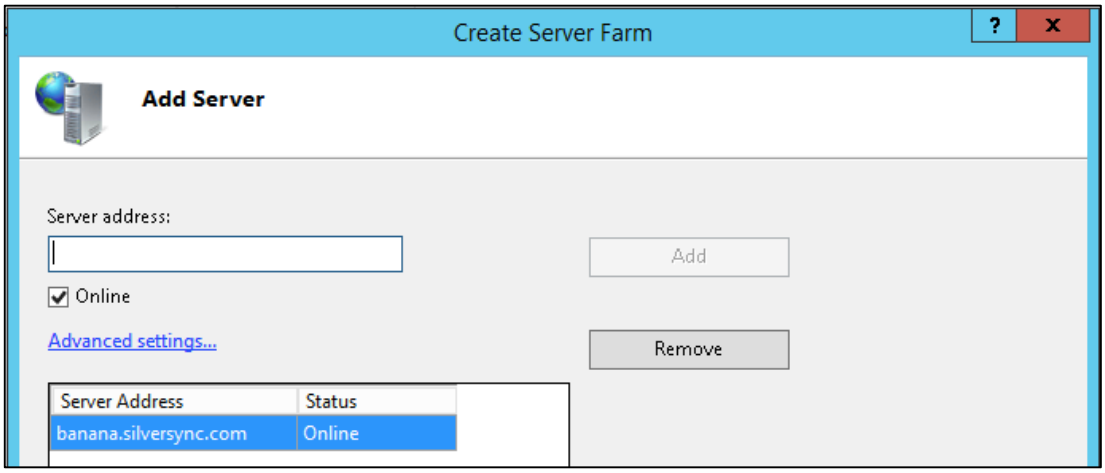
We need to create a server farm to publish Silverback.

- Open IIS and click on **Server Farm**.
- Click ‘Create Server Farm…’ and give it a name as shown below.

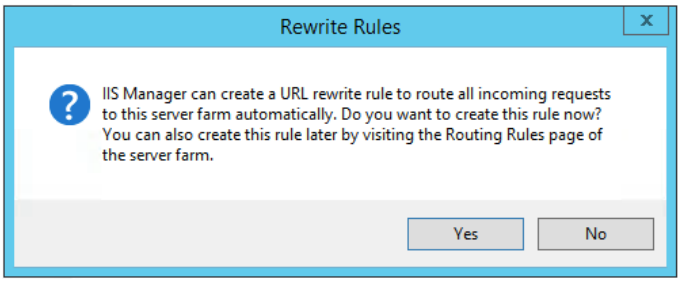


- Click Next.
- On the **Add Server** page, add each of the Silverback servers and click **Finish**.

Silverback Mail Gateway

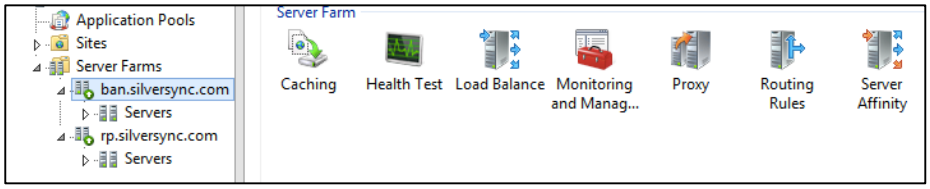


- Select **Yes** at the below prompt.



3.4.5. Silverback Server Farm Configuration Changes

Open the **Server Farm** settings node to make configuration changes.



- Select **Caching** and choose **Disable Disk Cache**.

Silverback Mail Gateway

- Select **Health Test**. This is used to make sure that a particular application is up and running:

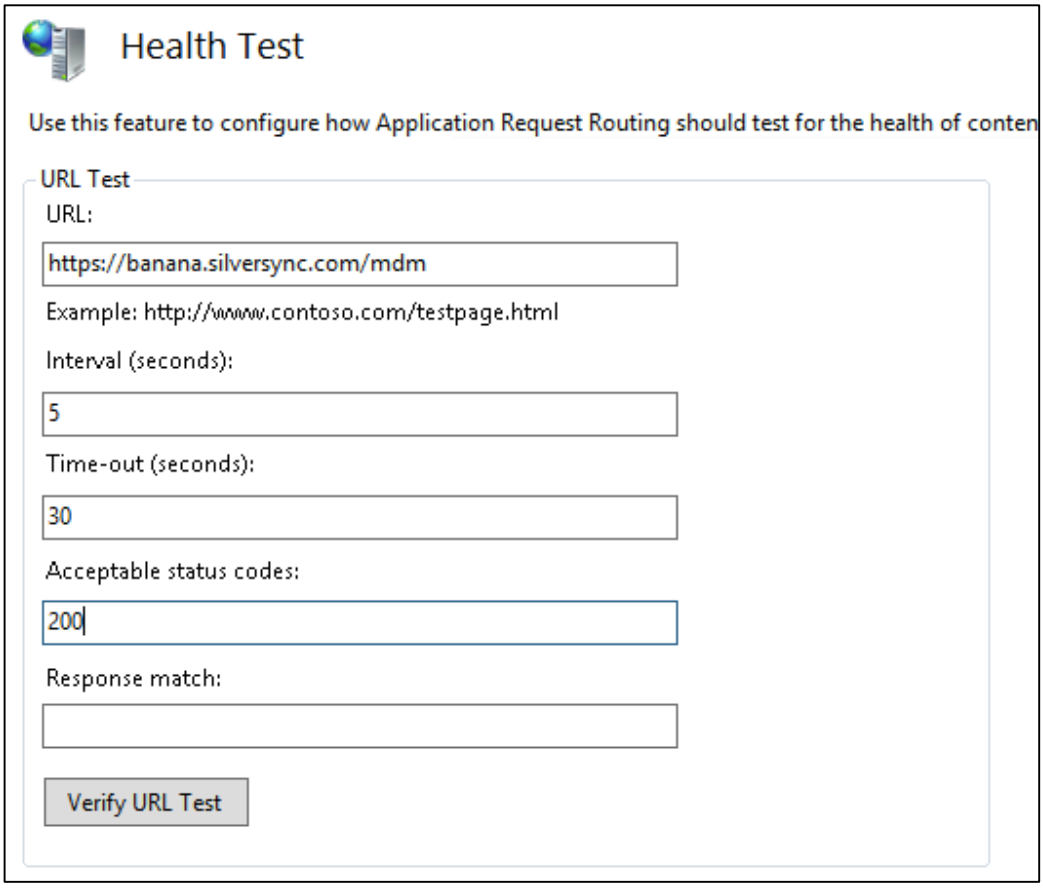
- Configure the **Health Test** with the following settings:

  URL: https://banana.silversync.com/mdm

  Interval: 5 seconds

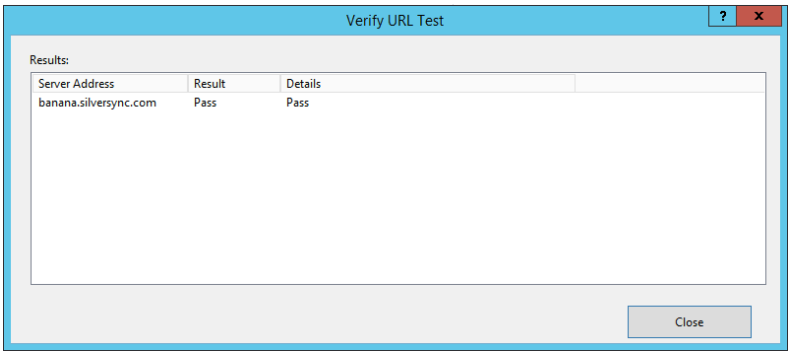
  Time-Out: 30 seconds

  Acceptable Status Code: 200

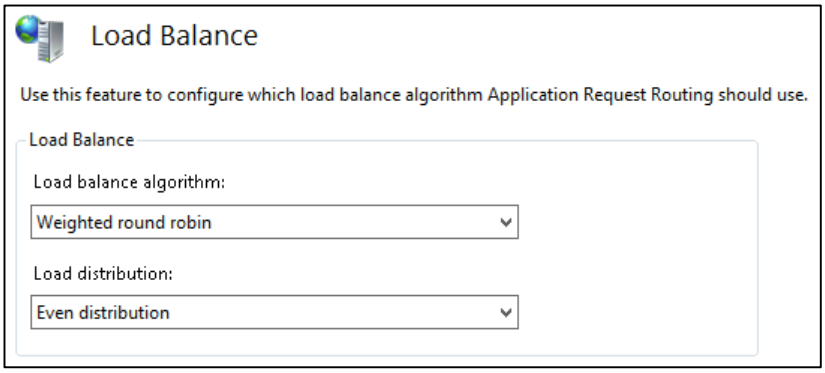


Silverback Mail Gateway

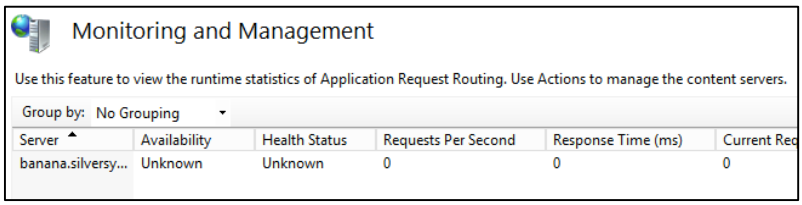
- Click Verify URL to Test, and they should pass.



- Select **Load Balance** and choose **weighted round robin**. There are other options, but for this scenario, we find this to be simple and effective.

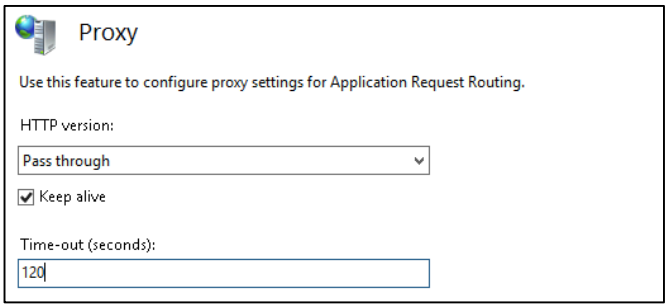


- Select **Monitoring and Management**. This shows the current state of the CAS servers that are part of this Server Farm. The Health Status is based on the output of the **Health Test** mentioned above.

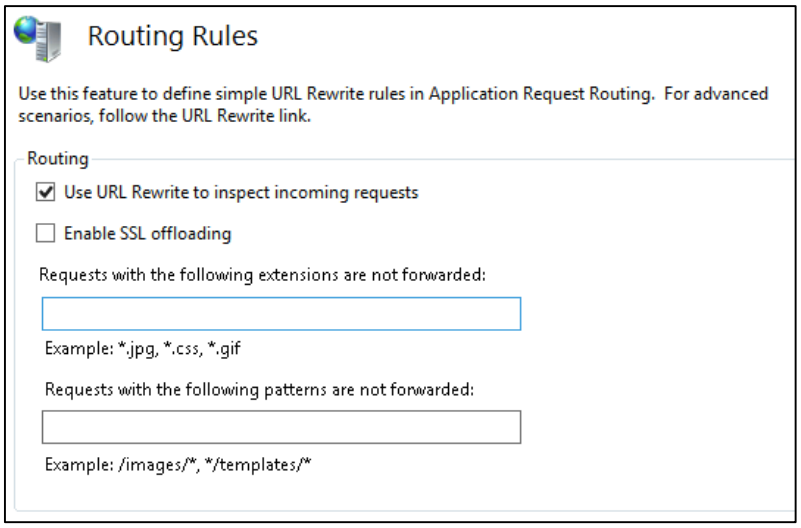


Silverback Mail Gateway

- Select **Proxy**. Change the below values. The actual value for these settings may need to be tweaked for your deployment, but these usually work well as a starting point.



- Select **Routing Rules** and uncheck **Enable SSL Offloading,** as it is not supported in Silverback.

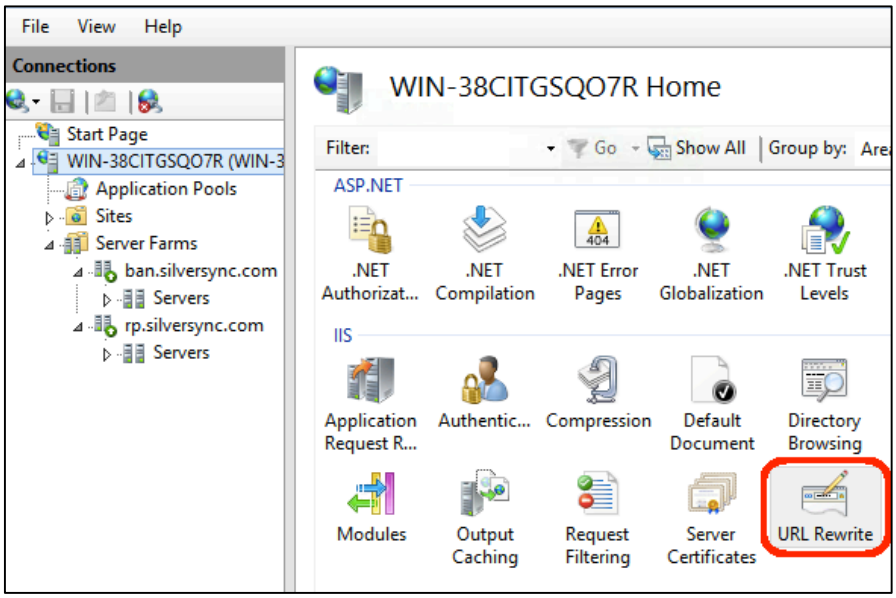


- Select **Server Affinity**. As long as you can get to a Silverback server, you will be able to access Silverback. No changes required.

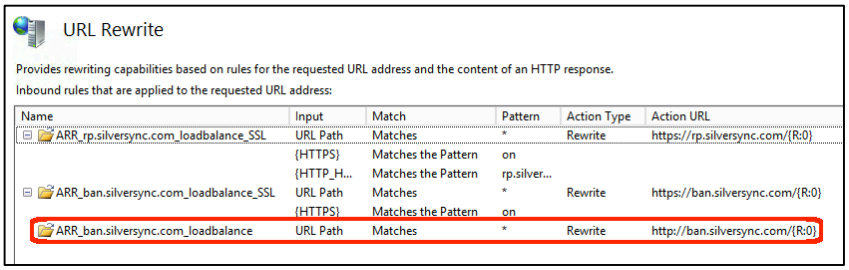
Silverback Mail Gateway

3.4.6. Create Silverback URL Rewrite Rules

- At the IIS Root and click on URL Rewrite.

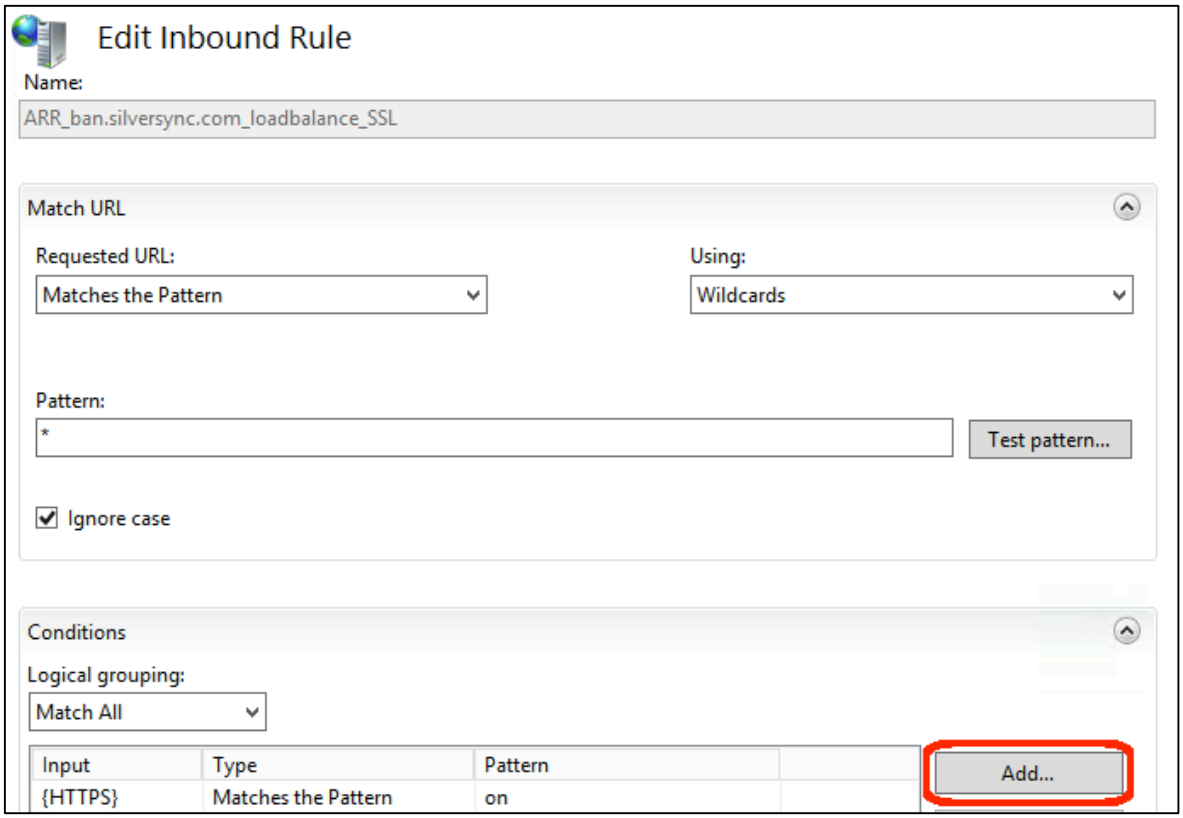


- **Select** the Silverback HTTP rule and press Remove.

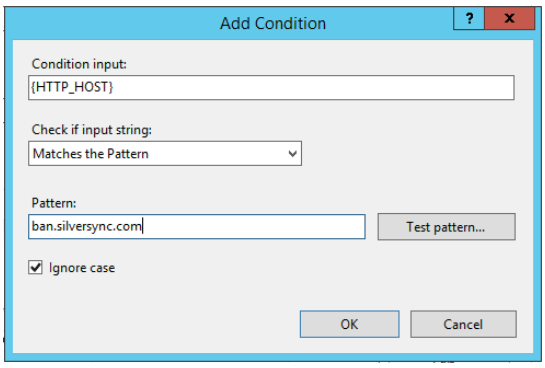


Silverback Mail Gateway

- Open the properties of the Silverback SSL rule. Under **Conditions** Click Add:

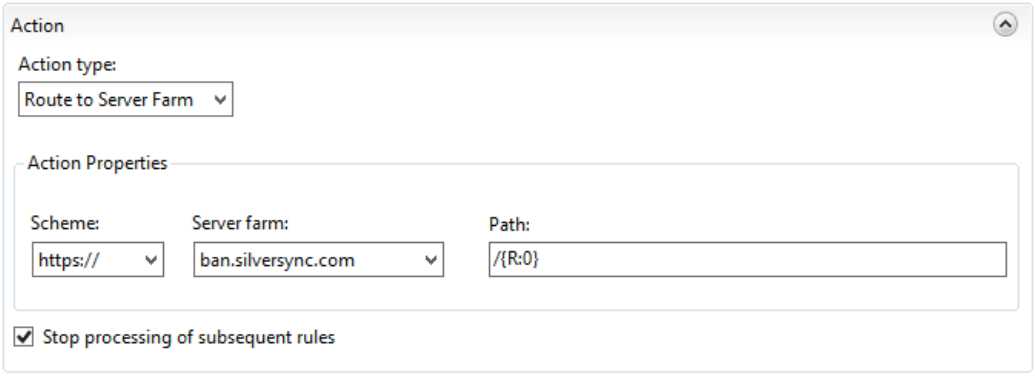


- Add a HTTP HOST for the external Silverback server FQDN, as below:



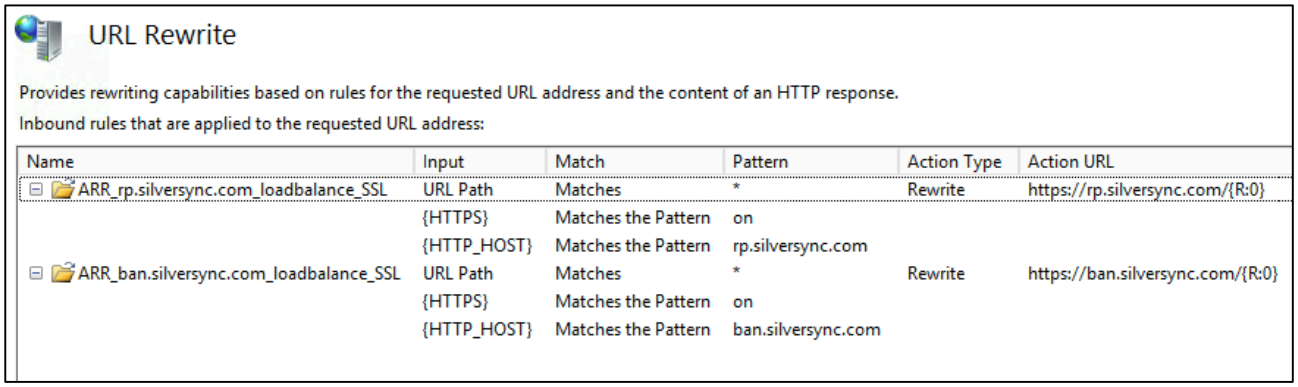
Silverback Mail Gateway

- Under **Action** make sure that you have the below options set. Choose the Silverback Server Farm from the drop down menu.



Note: Make sure the option “Stop processing of subsequent rules” is selected. This is to make sure that the validation process stops once the requested URL finds a match.

- Navigate to the URL Page again and it should look like this:



Name	Input	Match	Pattern	Action Type	Action URL
ARR_rp.silversync.com_loadbalance_SSL	URL Path	Matches	*	Rewrite	https://rp.silversync.com/{R:0}
	{HTTPS}	Matches the Pattern	on		
	{HTTP_HOST}	Matches the Pattern	rp.silversync.com		
ARR_ban.silversync.com_loadbalance_SSL	URL Path	Matches	*	Rewrite	https://ban.silversync.com/{R:0}
	{HTTPS}	Matches the Pattern	on		
	{HTTP_HOST}	Matches the Pattern	ban.silversync.com		

Silverback Mail Gateway

3.5. Solution Testing

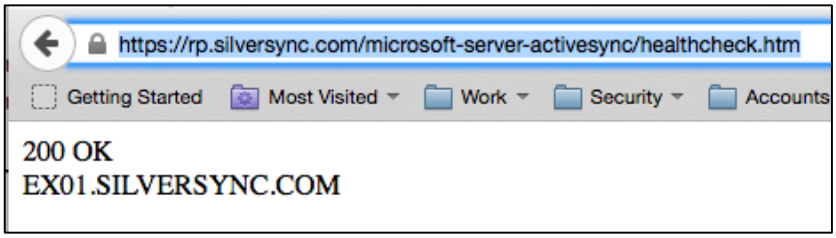
You should be able to navigate to Exchange ActiveSync / Traveler URL externally:

https://rp.silversync.com/microsoft-server-activesync/healthcheck.htm

or

https://rp.silversync.com/microsoft-server-activesync

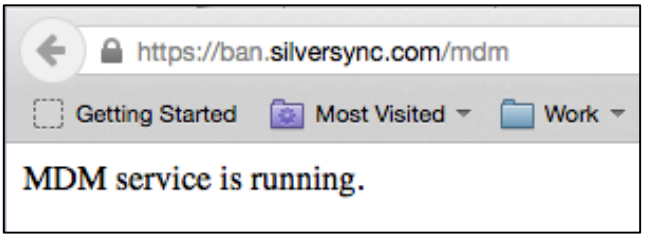
With Exchange ActiveSync you should get a response like this:



You should also be able to navigate to the Siverback URL externally:

https://ban.silversync.com/mdm

You should get a response like this:



3.6. Enterprise Certificate Authentication

You will need to create a client certificate to use as an enterprise client certificate. You can generate one from a certificate authority, or generate a single self-signed certificate. The self-signed certificate is the most secure option.

3.6.1. Create Enterprise Certificates

Use OPENSSL or suitable certificate generation tool to create a client certificate. The certificate must have the “Client Authentication” key usage. From a Windows Desktop or Server in an environment with a Microsoft Certificate Authority, the “certreq” tool can be used with the following steps:

3.6.1.1. Create the Certificate Request .inf File

Create a .inf file with a text editor with the following content (changing values to suite your environment) :

```
[NewRequest]
Subject = "CN=Silverback Certificate"
Exportable = TRUE
RequestType = CMC
KeyLength = 2048
Provider Type = 24

[RequestAttributes]
CertificateTemplate = "UserActiveSync"
SAN="upn=silverback.test@company.com&email=silverback.test@compa
ny.com"
```

Replace the Subject value with the desired certificate subject text, and in the RequestAttributes section, enter a template name, which the Certificate Authority will recognise as a User Certificate template.

For the SAN value, change the UPN and Email attributes to values, which will be recognisable in your environment. The value is not critical, but it should be clear to users looking at the certificate that its purpose is for the Silverback SMG.

3.6.1.2. Request the Certificate from the Certificate Authority

Execute the following commands to generate a certficiate:

```
certreq -new certificatereq.inf certificatereq.req
```

Replace certificatereq.inf with the name of the .inf file created in the previous step.

```
certreq -submit -config "certauth.company.com/Certificate
Authority" certficatereq.req certificate.cer
```

Replace "certauth.company.com/Certificate Authority" with the address and name of your certificate authority.

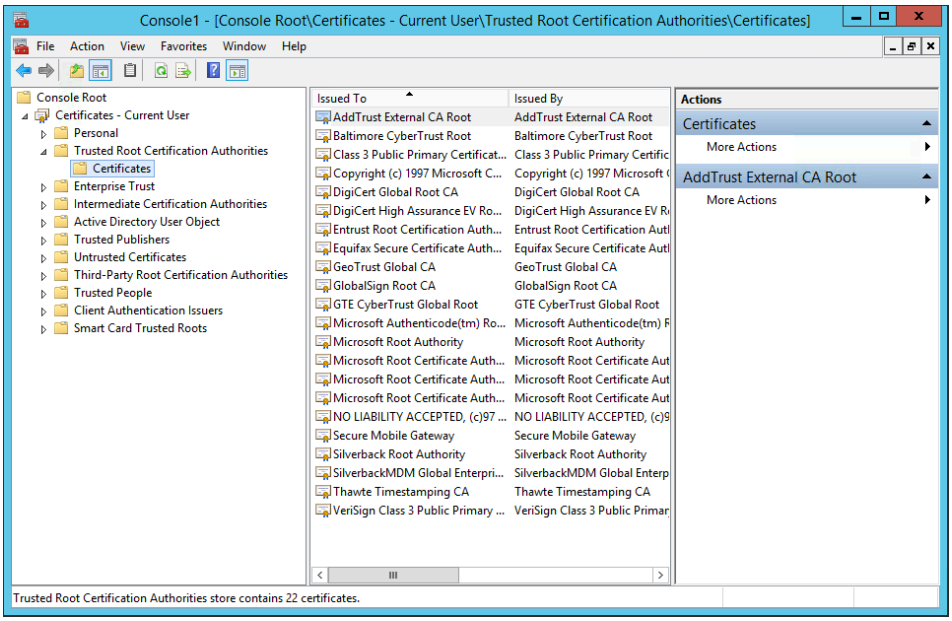
```
Certreq -accept certificate.cer
```

The above command completes the certificate request on the machine.

The certificate for Enterprise Certificate Authentication is now available on the machine. IF this was a separate machine to the SMG, export and copy the certificate to the SMG server.

3.6.2. Import Certificate Trust

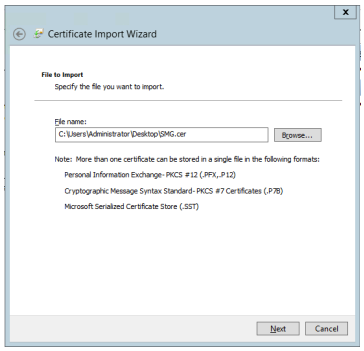
Open the Certificate Management Console on the SMG server:



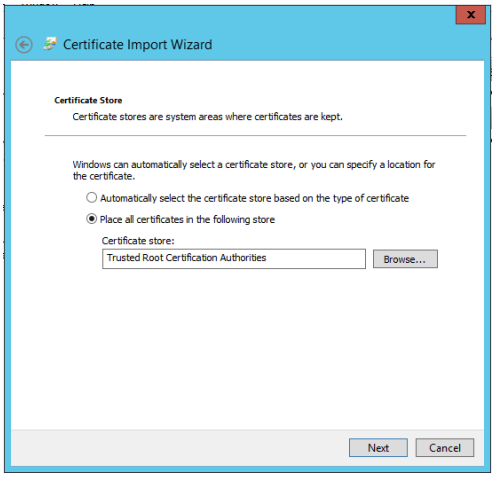
Right Click "Trusted Root Certificate Authorities\Certificates" and click "Import".

Silverback Mail Gateway

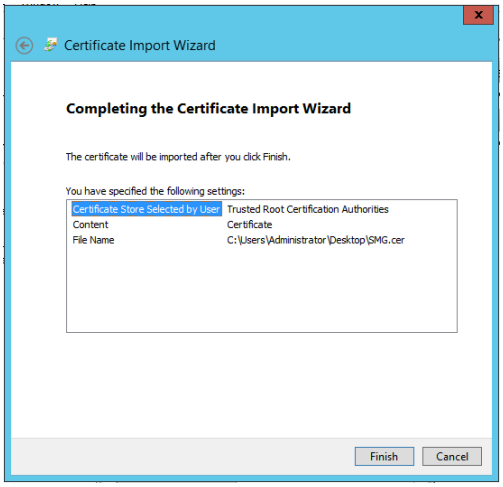
Select the SMG certificate:



Click Next:



Click Finish:



You will now have the enterprise certificate root correctly installed.

Silverback Mail Gateway

3.6.3. Client Certificate Authentication Registry Settings

It is recommended to backup the registry before making any modification to your registry.

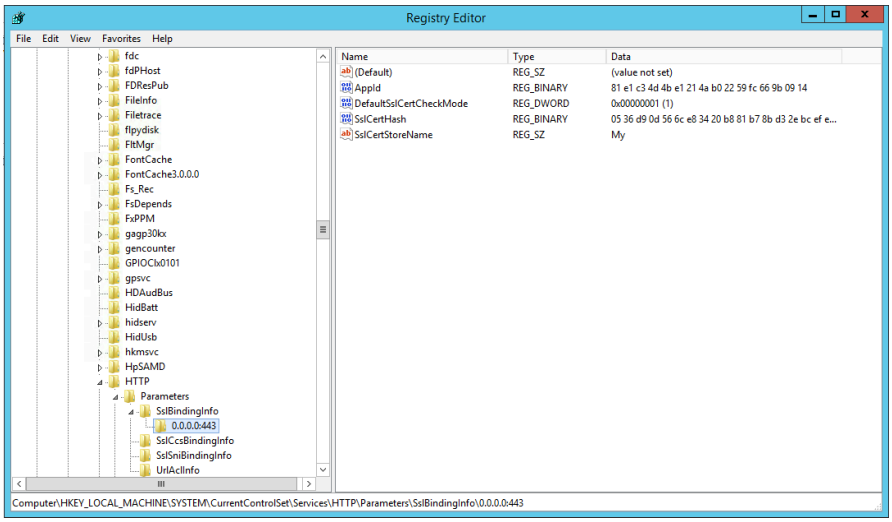
You need to apply these registry settings:

```
Windows Registry Editor Version 5.00


[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProvi
ders\SCHANNEL]
 "ClientAuthTrustMode"=dword:00000002
 "SendTrustedIssuerList"=dword:00000000


[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HTTP\Paramet
ers\SslBindingInfo\0.0.0.0:443]
 "DefaultSslCertCheckMode"=dword:00000001
```

You can copy this text and create the file “ARRSSL.reg” using it. Run the ARRSSL.reg file to import the registry settings. Check that the values have been set using regedit32.

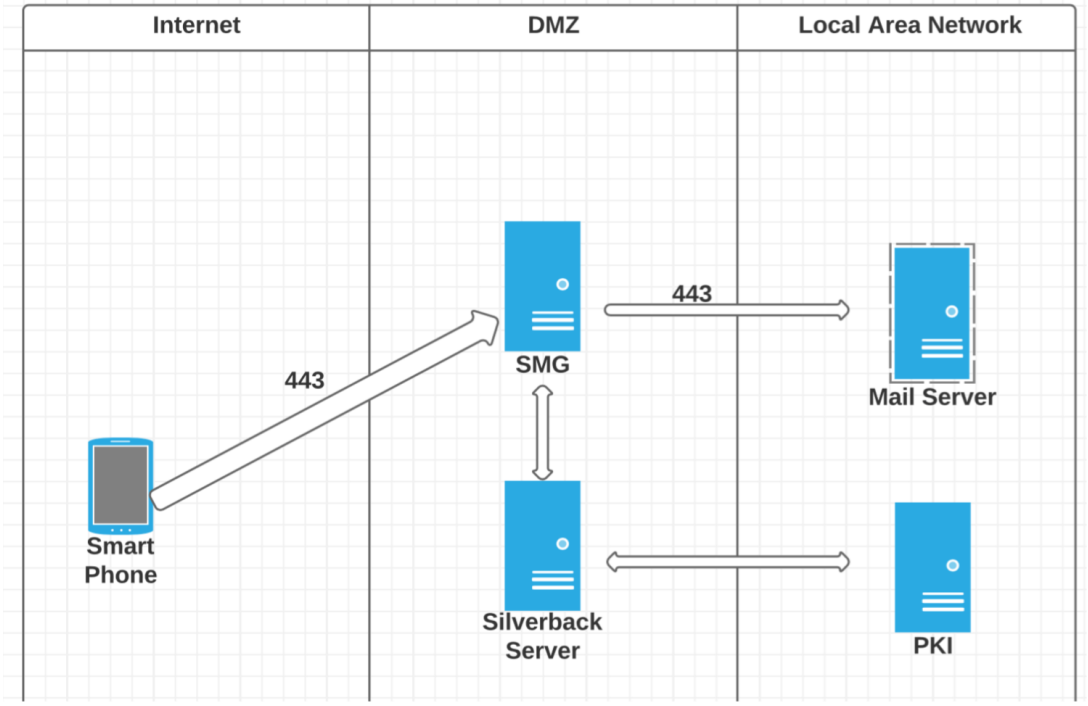


3.7. Blocking additional URL's

It is possible to create custom URL rewrite rules to block certain admin URL's from being published. You may want to block users from using this service to access Outlook Web Access, or the Silverback Admin Console.

3.8. User Based Certificate Authentication

You will need a PKI which creates user certificates and is connected to your Silverback server.



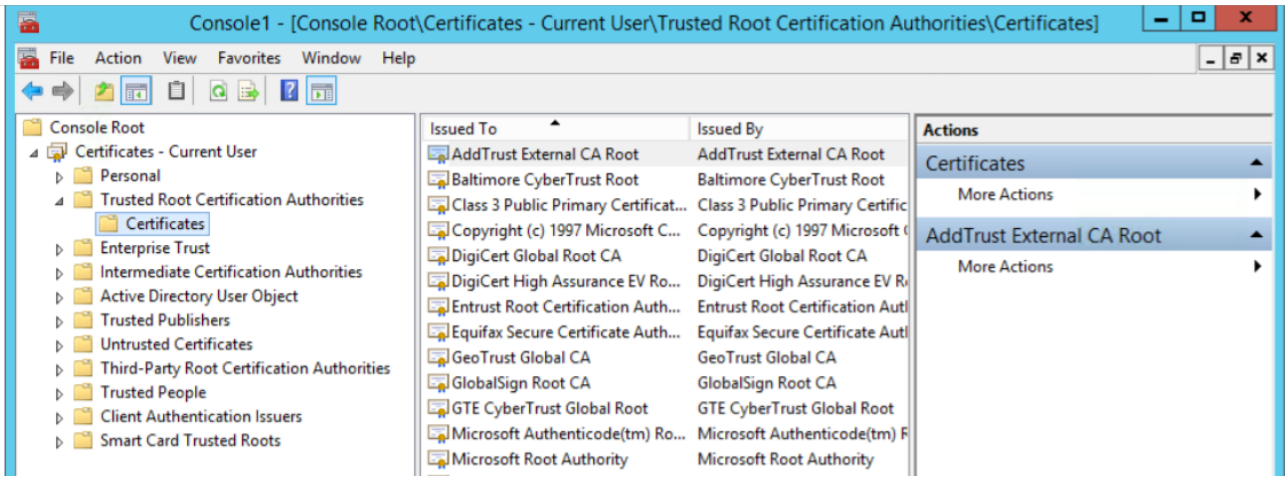
3.8.1. Import Certificate Trust

You have to import 2 certificates in the Certificate Store

1. **RootCaCertificate**

Silverback Mail Gateway

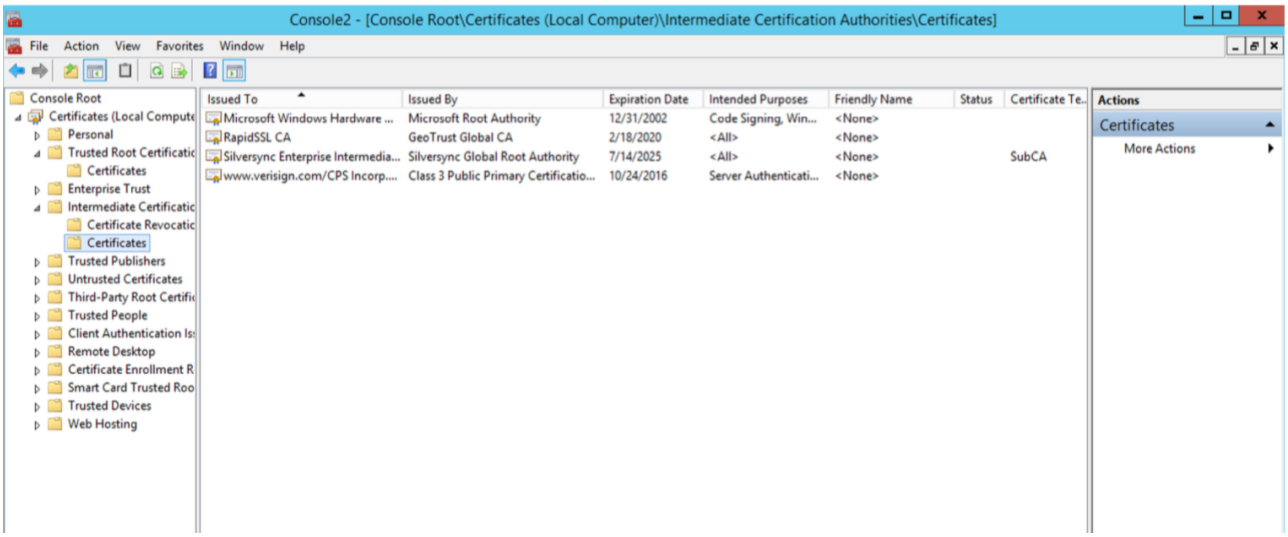
Open the Certificate Management Console on the SMG server:



Right Click “Trusted Root Certificate Authorities\Certificates” and click “Import”. Select the Root_CA certificate:

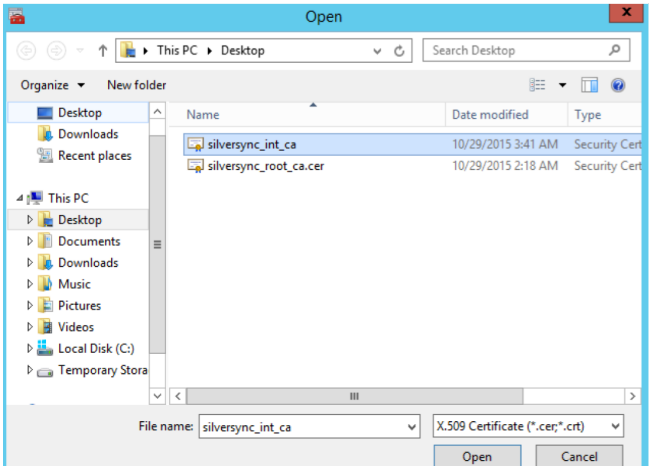
2. **IntermediateCertificate**

Right Click “Trusted Root Certificate Authorities\Certificates” and click “Import”

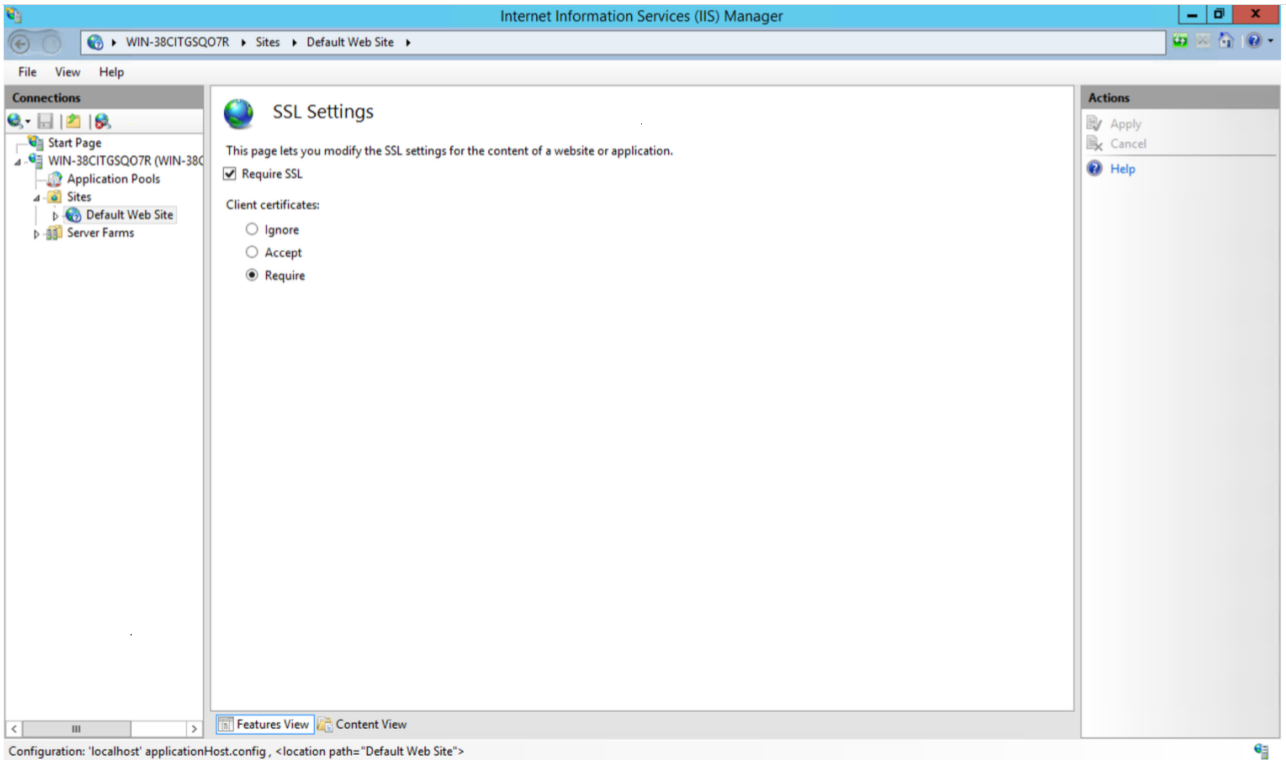


Silverback Mail Gateway

Select the Intermediate Certificate



Open the ISS Manager and go to Sites-> Default Web Site -> SSL Settings. Set the value to “ SSL Required”



Silverback Mail Gateway

Go to the Web Setting admin page of your Silverback Server

Go to the “General” Tab and change the Certificate Deployment from ‘Enterprise Certificate’ to ‘Individual Client’

Type the PKI string into the ‘Certificate Deployment’ field