Deployment Guide

Microsoft IIS 7.0

TABLE OF CONTENTS

1 INTRODUCTION

Microsoft Internet Information Services (IIS) is a web server for Microsoft Windows Servers. IIS supports the HTTP, HTTPS, FTP, FTPS, SMTP and NNTP protocols. The IIS web server is purpose made for Microsoft Servers, and is the second most used server in the world, surpassed only by the Apache HTTP server.

2 DEPLOYMENT GUIDE OVERVIEW

The AX Series Application Delivery Controller (ADC) offers additional security, reliability and optimization. This guide shows how to install and configure the AX Series to optimize IIS. Step-by-step procedures are provided for configuring the A10 AX Series for Microsoft IIS 7.0.

3 DEPLOYMENT GUIDE PREREQUISITES

This deployment guide has the following prerequisites:

AX Series Requirement

The A10 Networks AX Series ADC must be running version 2.4.x or higher

Microsoft IIS Requirements

For IIS requirements please see http://www.microsoft.com/en-us/server-cloud/windows-server/internet-information-services-iis-overview.aspx.

Tested environment:

- IIS Server
  - ♦ Windows 2008 (64-bit) Enterprise Edition Server Operating System (OS)
  - ♦ Internet Information Service 7.0
- Client Access (tested)
  - ♦ Microsoft Internet Explorer Version 8.0
  - ♦ Google Chrome Version 10.0
  - ♦ Mozilla Firefox Version 8

Note: *Generally, if the Virtual IP (VIP) is accessed from an external client, the AX device would be deployed in a routed mode. If the IIS/web site services are accessed internally, the AX device would be* *deployed in one-arm mode. If the IIS web server applications are accessed from both internal and external clients, the AX device would be deployed in one-arm mode.*

Note: *For additional deployment modes the AX Series device can support, please visit the following URL:*

http://www.a10networks.com/products/axseries-load-balancing101.php

4 ACCESSING THE AX SERIES LOAD BALANCER

This section describes how to access the AX Series device. The AX device can be accessed either from a Command Line Interface (CLI) or Graphical User Interface (GUI):

- CLI – Text-based interface in which you type commands on a command line. You can access the CLI directly through the serial console or over the network using either of the following protocols:
  - ♦ Secure protocol – Secure Shell (SSH) version 2
  - ♦ Unsecure protocol – Telnet (if enabled)
- GUI – Web-based interface in which you click to access configuration or management pages and type or select values to configure or manage the device. You can access the GUI using the following protocol:
  - ♦ Secure protocol – Hypertext Transfer Protocol over Secure Socket Layer (HTTPS)

Note: *HTTP requests are redirected to HTTPS by default on the AX device.*

Default Access Information:

- Default Username: “admin”
- Default password: “a10”
- Default IP Address of the device: “172.31.31.31”

(For detailed information on how to access the AX Series device, refer to the *A10 Networks AX Series System Configuration and Administration Guide*.)

5 MICROSOFT IIS 7.0 RECOMMENDED INSTALLATION PROCEDURES

1. On a Windows Search Programs and Files window, type "server manager" to open the server manager interface.

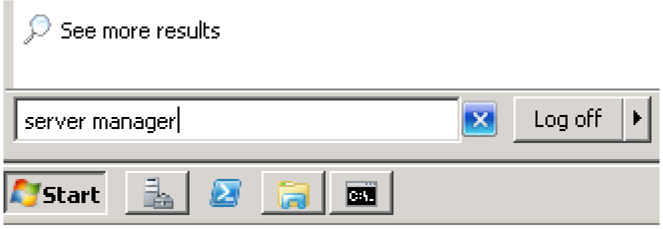
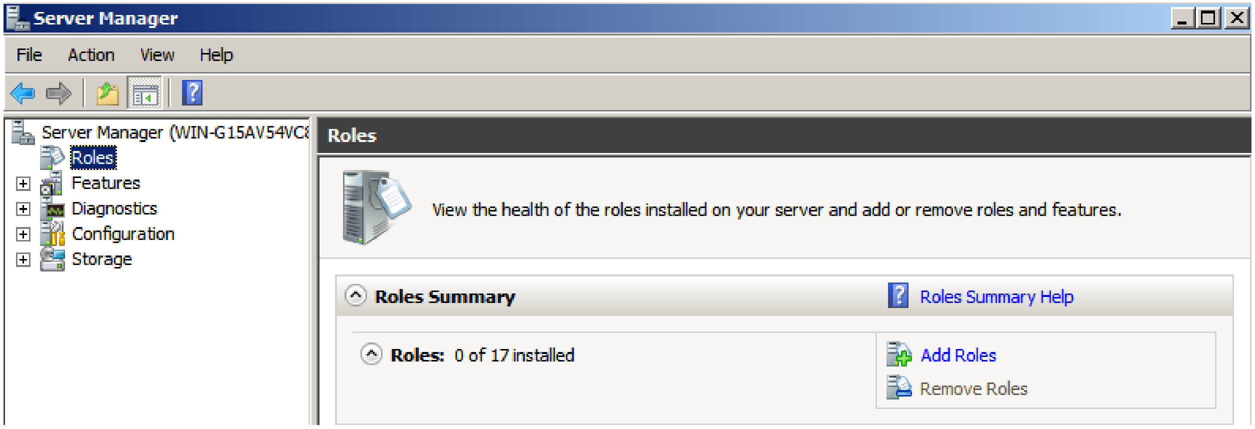


Figure 1: Server manager configuration

2. On the drop-down menu, select "Roles" and "Add Roles".

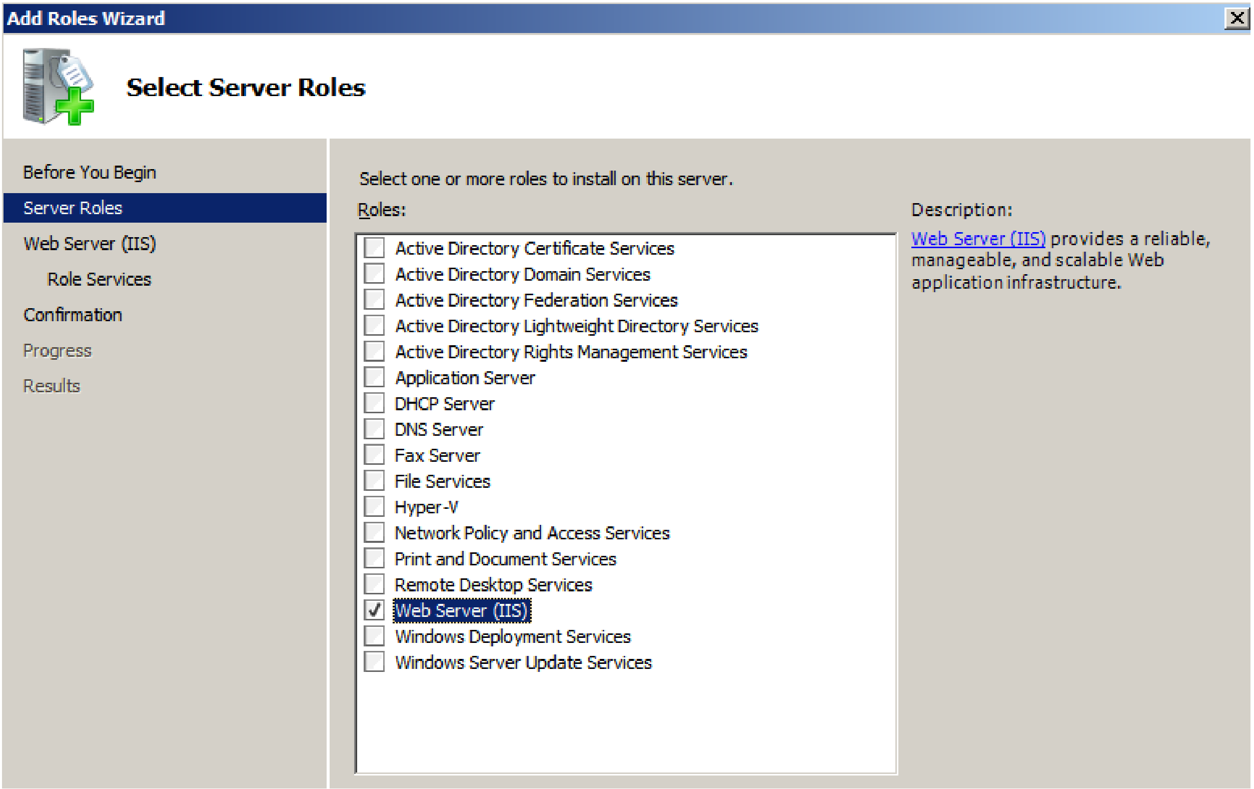


View the health of the roles installed on your server and add or remove roles and features.

Roles: 0 of 17 installed

Figure 2: Server role management

3. Select “Web Server (IIS)”.



Select one or more roles to install on this server.

Roles:

- □ Active Directory Certificate Services
- □ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Application Server
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- □ File Services
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Desktop Services
- ☑ Web Server (IIS)
- □ Windows Deployment Services
- □ Windows Server Update Services

Description:

Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

Figure 3: Server role selection

4. In the Confirm Installation Selections menu, select all the default configuration items and click to **Install** IIS to the server.

5. Once the installation is complete, verify its completion, open a browser, and navigate to http://localhost. If the web server responds, Microsoft IIS is now in working order. Install any additional servers and IIS servers for the application server pool.

If you have further questions on how to configure Microsoft IIS, visit the following web site for instructions:

http://support.microsoft.com/kb/323972

6 OPTIONAL: ISAPI CLIENT IP RETRIEVAL FILTER

The purpose of the ISAPI filter is to retrieve client IP addresses from HTTP headers that are inserted by a proxy server. This Dynamic Link Library (DLL) will be required to be installed within the IIS server. The DLL supports the following IIS environments:

- Windows 2000 Server or later
- IIS 5.0 or later
- Standalone DLL with no prerequisites for the DLL to work

The following HTTP headers are searched in the HTTP request. When there is a match, the matched HTTP headers are logged within the IIS logs. There are two sets of DLLs that are readily available: "A10-clientip-isapi.dll" for standard users; and, for high performance, "A10-fast-clientip-isapi.dll". Both DLLs can support a 32-bit or 64-bit OS.

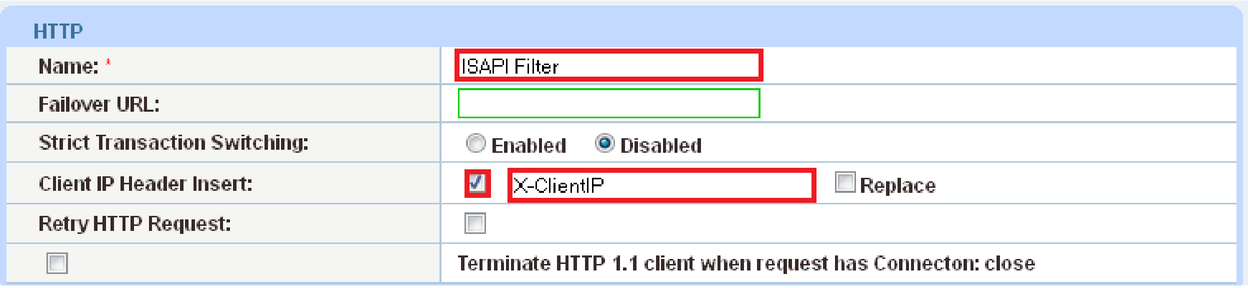
Sample Log:

```
2011-11-28 23:44:06 192.168.77.134 GET /upcase/upcase.htm - 80 -
22.2.2.22+22.12.31.22 dk-DLL-X-ClientIP 200 0 0 10342
```

Note: To obtain the ISAPI DLLs, please contact A10 Support.

To apply the ISAPI filter:

1. Navigate to **Config Mode > Service > Template > Application > HTTP**.
2. Enter the following:
   - ♦ **Name:** "ISAPI Filter"
   - ♦ **Client IP Header Insert:** Enter the required header. The following Client IP Header inserts are available:
     - o X-Forwarded-For
     - o X-ClientIP
     - o X-Client-IP
     - o Cip



HTTP

Name: *	ISAPI Filter
Failover URL:	
Strict Transaction Switching:	○ Enabled ● Disabled
Client IP Header Insert:	☑ X-ClientIP □ Replace
Retry HTTP Request:	□
□	Terminate HTTP 1.1 client when request has Connecton: close

Figure 4: ISAPI filter

Note: *You have the option to replace.*

3. Click **OK**, then click **Save** to save the configuration.

Note: *Make sure that you bind the HTTP template to the corresponding VIP.*

7 ARCHITECTURE OVERVIEW

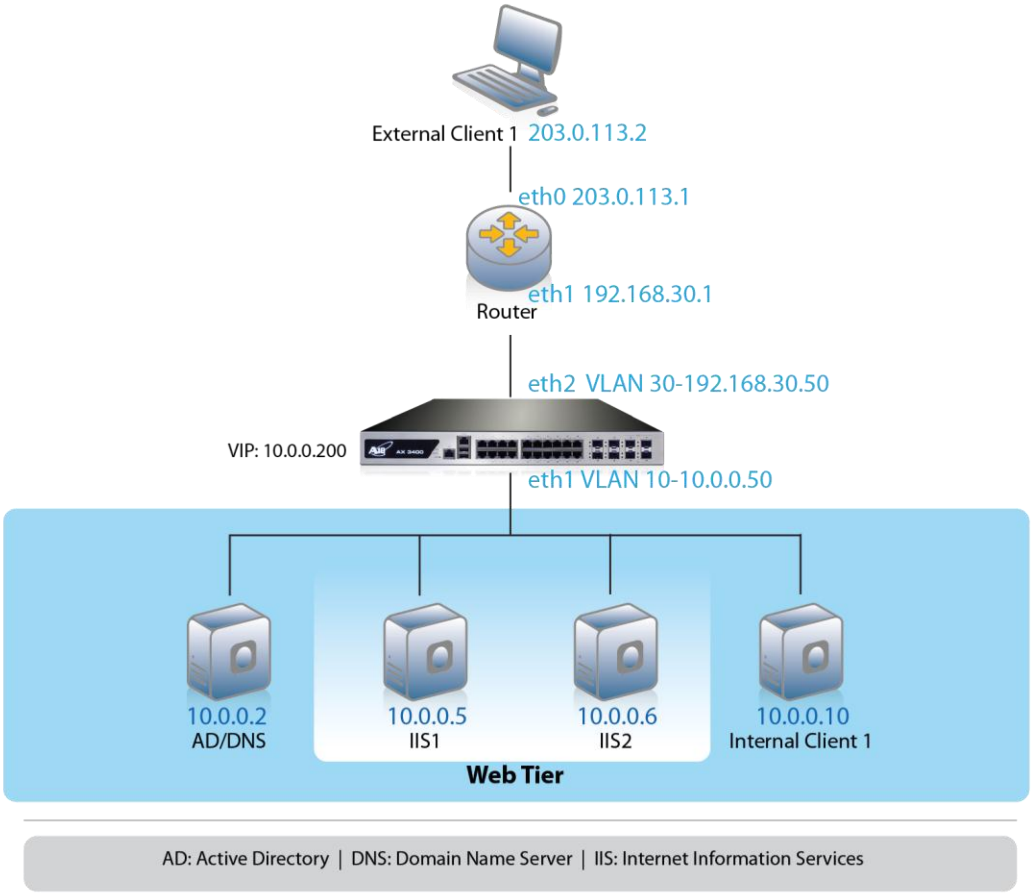


Figure 5: Configuration overview

Note: *In a typical network topology, the IIS servers are installed within the demilitarized zone (DMZ) and the AD/DNS server is deployed within the internal network.*

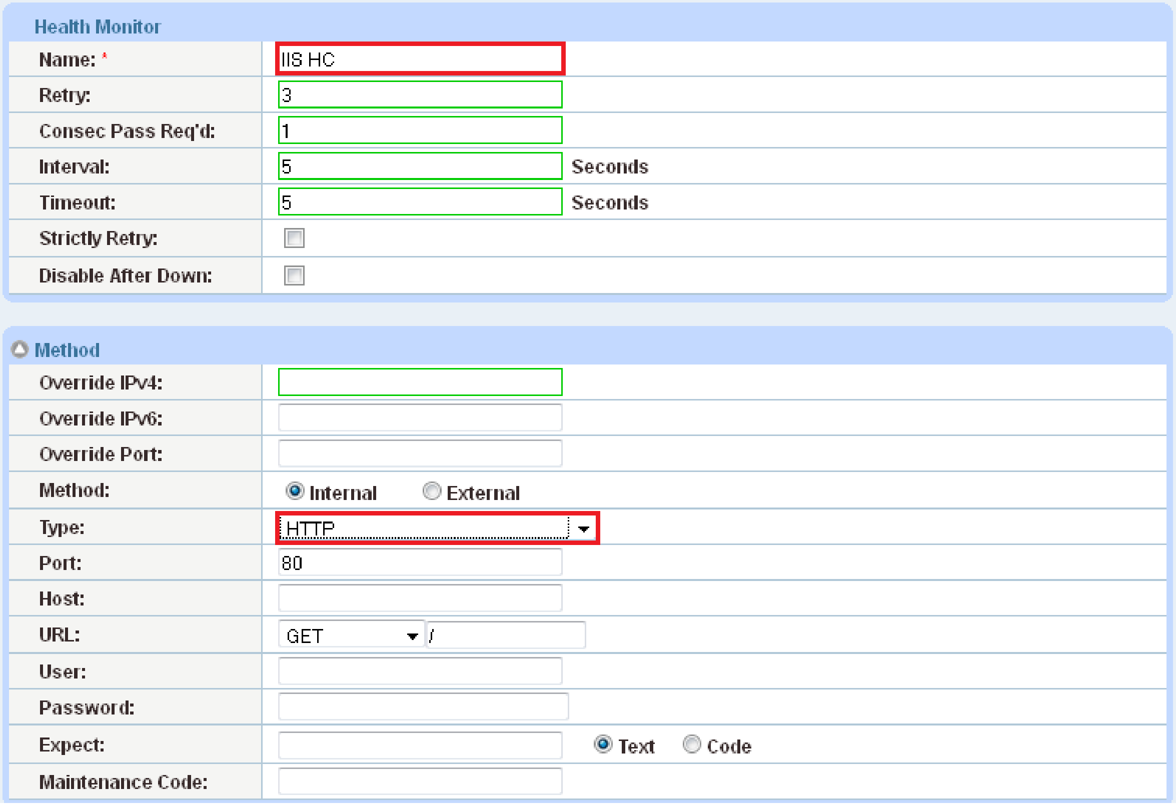
8 BASIC CONFIGURATION

This section explains how the AX Series is configured with Microsoft IIS servers. This section contains detailed instructions for installing the real servers, service group, and virtual services in a basic Microsoft IIS configuration. Before the basic configuration is created, health monitors and Source NAT must be configured.

9 HEALTH MONITOR CONFIGURATION

The AX series can automatically initiate health status checks for real servers and service ports. Health checks assure that all requests go to functional and available servers. If a server or a port does not respond appropriately to a health check, the server is temporarily removed from the list of available servers. Once the server is restored and starts responding appropriately to the health checks, the server is automatically added back to the list of available servers.

1. Navigate to **Config Mode > SLB > Server Port > Health Monitor**.
2. Select **Create** from the **Health Monitor** drop-down list.
3. In the **Name** field, enter “IIS HC”.
4. Select **Method** “HTTP”.
5. Click **OK**, then see the next section to continue with the Service Group configuration.



Health Monitor

Name: *	IIS HC	
Retry:	3	
Consec Pass Req'd:	1	
Interval:	5	Seconds
Timeout:	5	Seconds
Strictly Retry:	□	
Disable After Down:	□	

Method

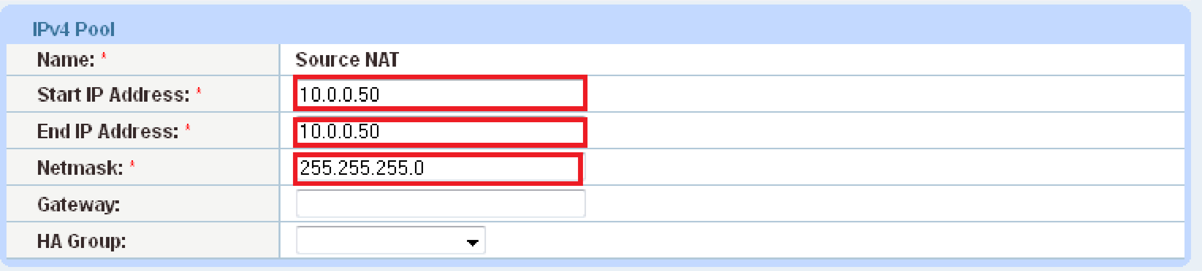
Override IPv4:		
Override IPv6:		
Override Port:		
Method:	● Internal ○ External	
Type:	HTTP	
Port:	80	
Host:		
URL:	GET /	
User:		
Password:		
Expect:		● Text ○ Code
Maintenance Code:		

Figure 6: Health monitor configuration

10 SOURCE NAT CONFIGURATION

This section configures the IP Address pool to be used for IP Source Network Address Translation (SNAT). When incoming traffic from a client accesses the VIP address (for example: 10.0.0.200), the client requests are "source NAT-ed", which means that the AX replaces the client's source IP address based on the configured address pool of the source NAT. SNAT is required when your network topology is based on "one-arm" deployment and if you have internal clients that reside on the same subnet as the VIP. The Source NAT template must be applied in the virtual server port for the NAT to take effect.

1. Navigate to **Config Mode> IP Source NAT > IPv4 Pool**.
2. Click **Add.**
3. Enter the following:
   - **NAT:** "Source NAT"
   - **Start IP Address:** "10.0.0.50"
   - **End IP Address:** "10.0.0.50"
   - **Netmask:** "255.255.255.0"



IPv4 Pool

Name: *	Source NAT
Start IP Address: *	10.0.0.50
End IP Address: *	10.0.0.50
Netmask: *	255.255.255.0
Gateway:	
HA Group:	

Figure 7: Source NAT pool configuration

4. Click **OK**, then click **Save** to save the configuration.

Note: *When you are in the Virtual Service configuration section, you can apply the "Source NAT" template that was created under the Source NAT Pool section.*

Note: *When using the AX device in a High Availability (HA) configuration, an HA Group must be selected. This will prevent duplicate IP addresses from occurring in the Source NAT Pool.*

11 SERVER CONFIGURATION

This section demonstrates how to configure the IIS web servers on the AX Series.

1. Navigate to **Config Mode > SLB > Server**.

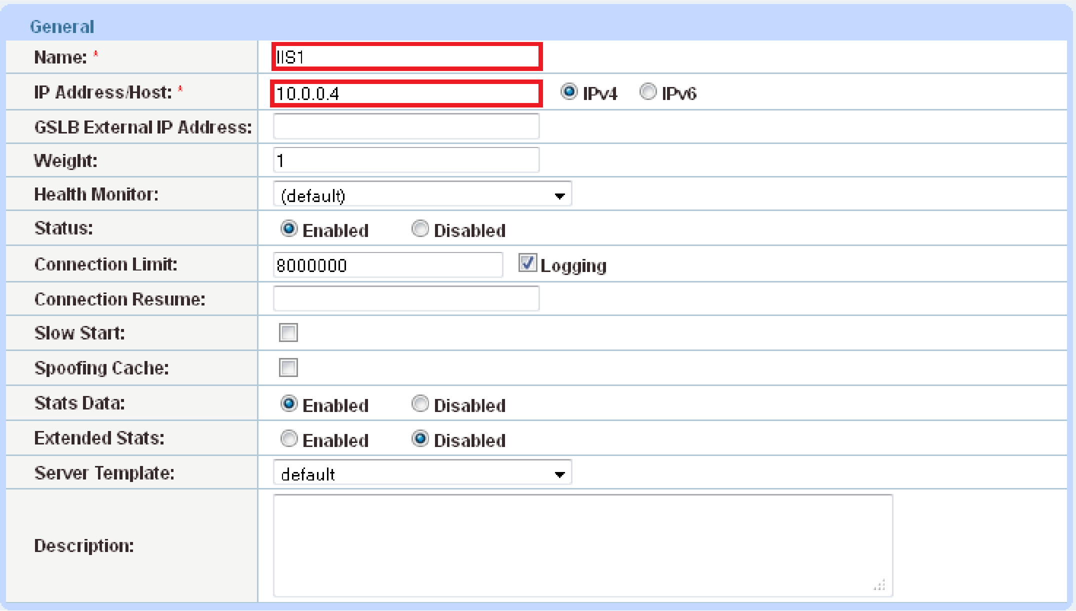
2. Click **Add** to add a new server.

3. Within the Server section, enter the following required information:

   - **Name:** "IIS1"

   - **IP address /Host:** "10.0.0.4"

   Note: *Enter additional servers if necessary.*



General

Name: *	IIS1
IP Address/Host: *	10.0.0.4 ● IPv4 ○ IPv6
GSLB External IP Address:	
Weight:	1
Health Monitor:	(default)
Status:	● Enabled ○ Disabled
Connection Limit:	8000000 ☑ Logging
Connection Resume:	
Slow Start:	□
Spoofing Cache:	□
Stats Data:	● Enabled ○ Disabled
Extended Stats:	○ Enabled ● Disabled
Server Template:	default
Description:	

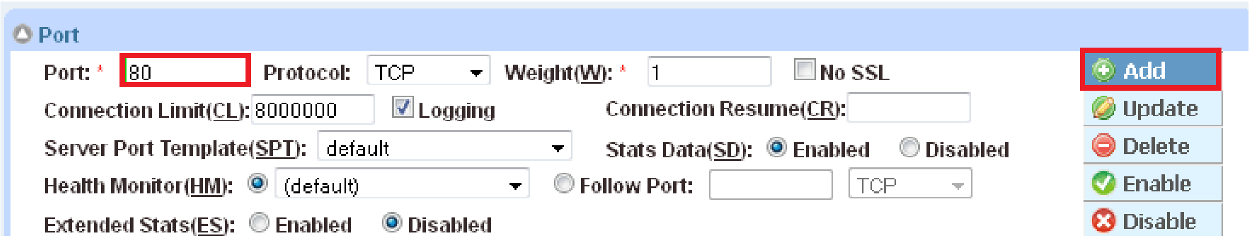
Figure 8: Server configuration

4. To add a port to the server configuration:

   a. Enter the port number in the **Port** field.

   b. Select the **Protocol**.

   c. Click **Add**.



Port

Port: * 80 Protocol: TCP Weight(W): * 1 □ No SSL

Connection Limit(CL): 8000000 ☑ Logging Connection Resume(CR):

Server Port Template(SPT): default Stats Data(SD): ● Enabled ○ Disabled

Health Monitor(HM): ● (default) ○ Follow Port: TCP

Extended Stats(ES): ○ Enabled ● Disabled

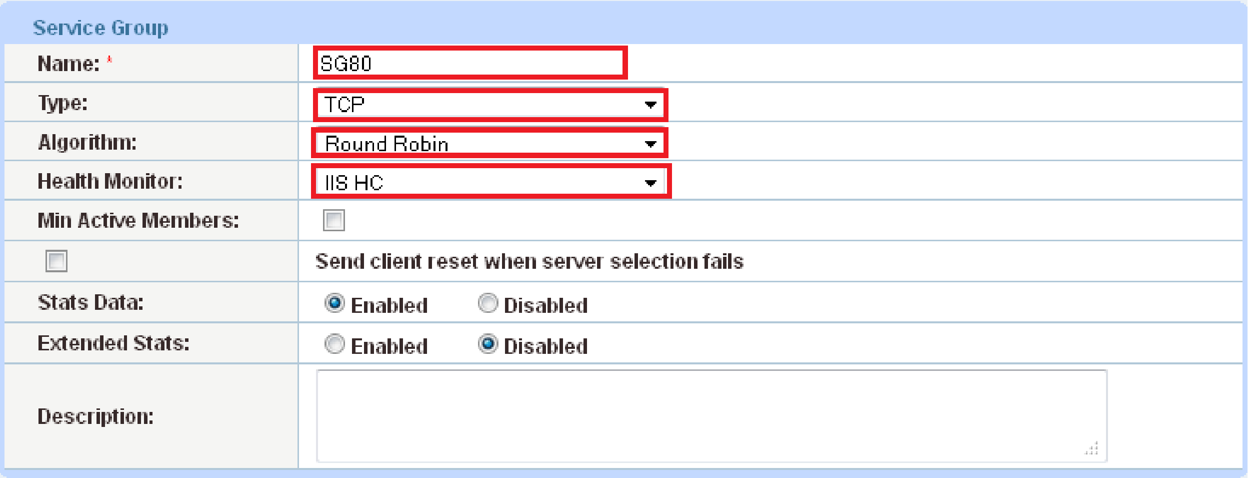
Figure 9: Server port configuration

5. Click **OK**, then click **Save** to save the configuration.

12 SERVICE GROUP CONFIGURATION

This section contains the basic configuration as to how to configure a service group.

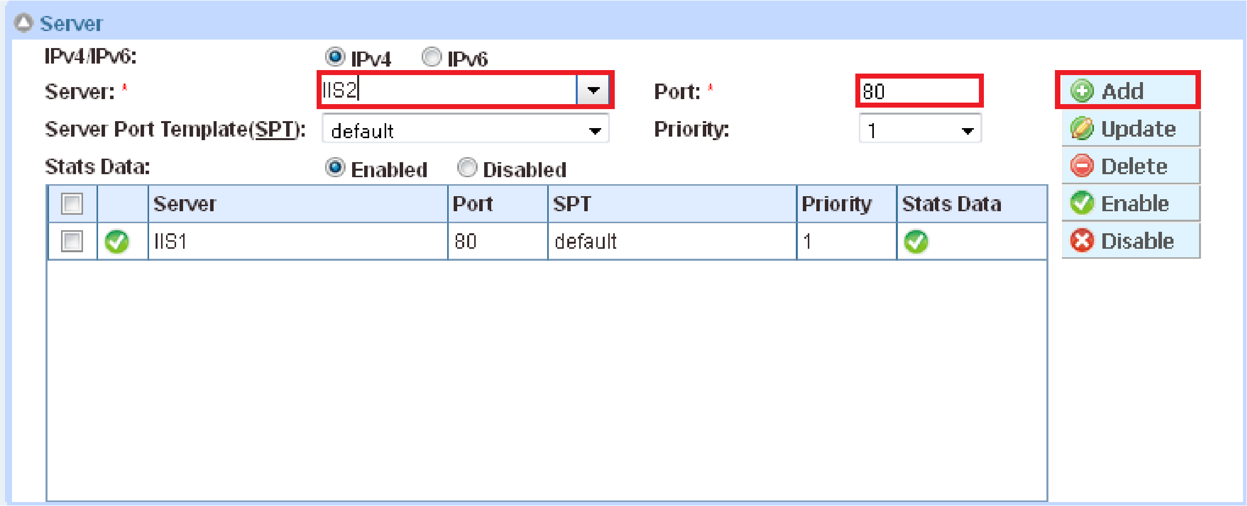
1. Navigate to **Config Mode > SLB > Service Group**.
2. Click **Add**.
3. Enter or select the following values:
   - **Name:** "SG80"
   - **Type:** "TCP"
   - **Algorithm:** "Round Robin"
   - **Health Monitor:** "IIS HC"
4. In the Server section, select a server from the Server drop-down list and enter "80" in the **Port** field.
5. Click **Add**. Repeat for each server.



Service Group

Name: *	SG80
Type:	TCP
Algorithm:	Round Robin
Health Monitor:	IIS HC
Min Active Members:	□
□	Send client reset when server selection fails
Stats Data:	● Enabled ○ Disabled
Extended Stats:	○ Enabled ● Disabled
Description:	

Figure 10: Service group configuration



Server

IPv4/IPv6: ● IPv4 ○ IPv6

Server: * IIS2 Port: * 80

Server Port Template(SPT): default Priority: 1

Stats Data: ● Enabled ○ Disabled

□		Server	Port	SPT	Priority	Stats Data
□	✓	IIS1	80	default	1	✓

Figure 11: Server configuration

6. Click **OK**, then click **Save** to save the configuration.

13 VIRTUAL SERVER CONFIGURATION

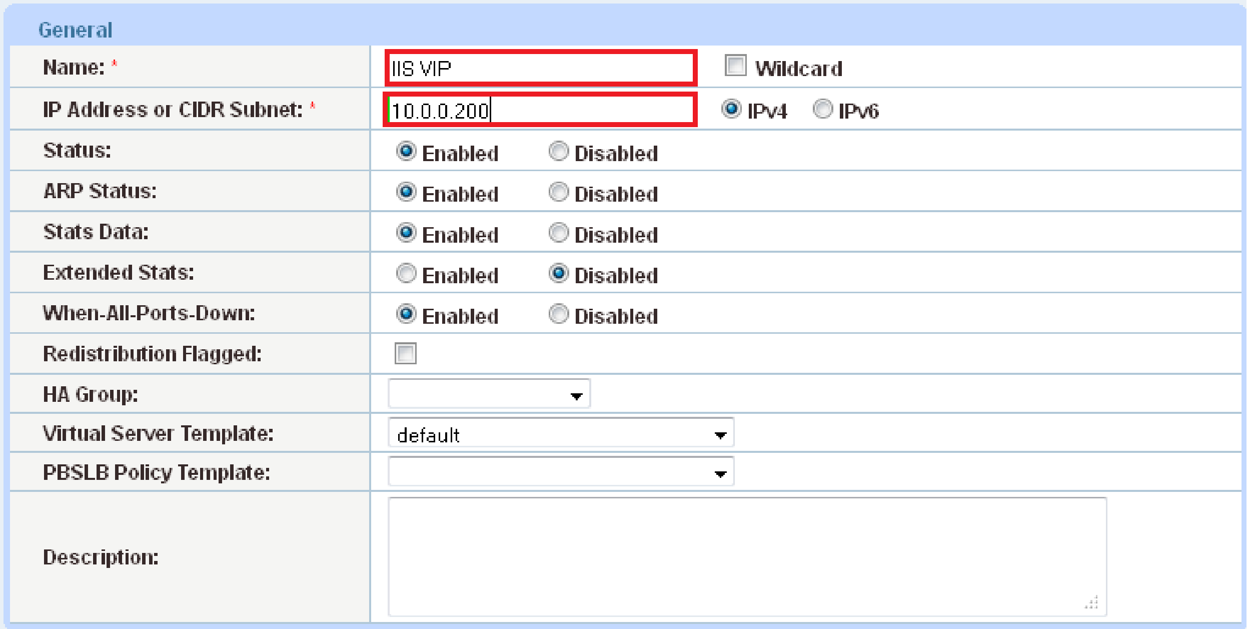
This section contains the basic configuration for a Virtual Server. The Virtual Server is also known as the "Virtual IP" ("VIP") that a client accesses during an initial request.

1. Navigate to **Config Mode > SLB > Virtual Service**.

2. In the General section, enter the name of the VIP and its IP Address:

   - **Name:** "IIS VIP"

   - **IP Address:** "10.0.0.200"

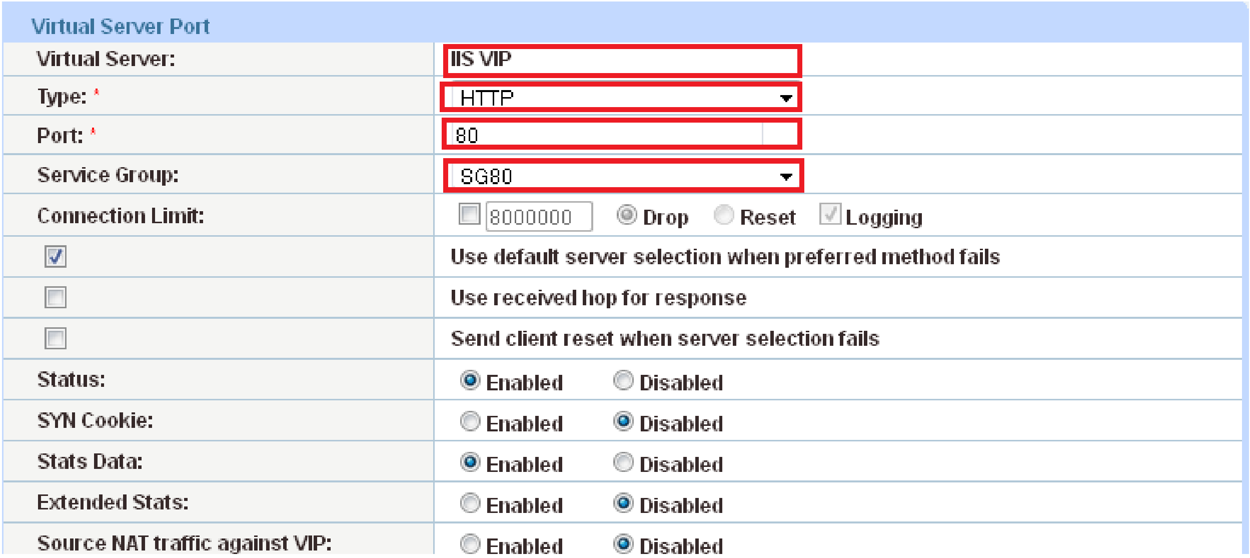


General

Name: *	IIS VIP	□ Wildcard
IP Address or CIDR Subnet: *	10.0.0.200	● IPv4 ○ IPv6
Status:	● Enabled ○ Disabled	
ARP Status:	● Enabled ○ Disabled	
Stats Data:	● Enabled ○ Disabled	
Extended Stats:	○ Enabled ● Disabled	
When-All-Ports-Down:	● Enabled ○ Disabled	
Redistribution Flagged:	□	
HA Group:		
Virtual Server Template:	default	
PBSLB Policy Template:		
Description:		

Figure 12: Virtual server configuration

3. In the Port section, click **Add**.



Virtual Server Port

Virtual Server:	IIS VIP
Type: *	HTTP
Port: *	80
Service Group:	SG80
Connection Limit:	□ 8000000 ● Drop ○ Reset ☑ Logging
☑	Use default server selection when preferred method fails
□	Use received hop for response
□	Send client reset when server selection fails
Status:	● Enabled ○ Disabled
SYN Cookie:	○ Enabled ● Disabled
Stats Data:	● Enabled ○ Disabled
Extended Stats:	○ Enabled ● Disabled
Source NAT traffic against VIP:	○ Enabled ● Disabled

Figure 13: Virtual-server port configuration

4. Select the following values:

   - **Virtual Server:** “HTTP”

     Note: *The Port number will be pre-selected after selecting the protocol type.*

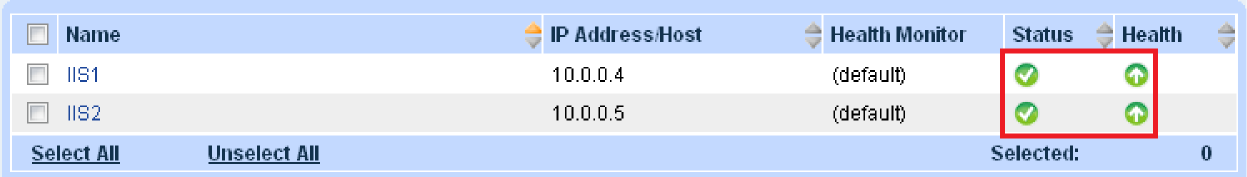
   - **Service Group:** "SG80"

5. Click **OK**, then click **Save** to save the configuration.

13.1 VALIDATING THE CONFIGURATION

This concludes the basic configuration of Microsoft Windows IIS 7.0 configuration. Using a client within the network, you can access the VIP with a browser and type the URL as http://10.0.0.200.

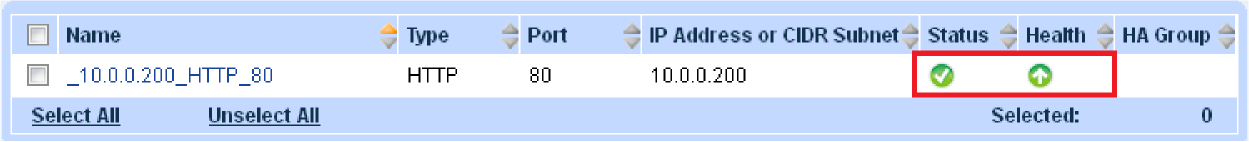
Within the AX GUI, you can validate that the IIS application is working and functional by navigating to the configuration lists for servers, virtual servers, and health monitors.



□	Name	IP Address/Host	Health Monitor	Status	Health
□	IIS1	10.0.0.4	(default)	✓	⬆
□	IIS2	10.0.0.5	(default)	✓	⬆

Select All Unselect All Selected: 0

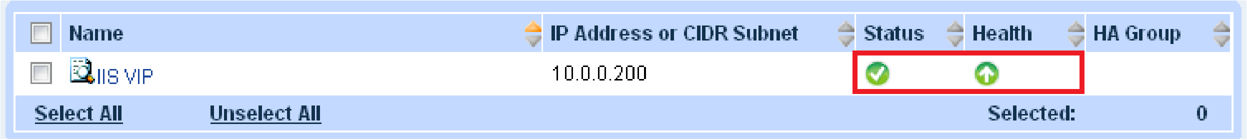
Figure 14: Server list



□	Name	Type	Port	IP Address or CIDR Subnet	Status	Health	HA Group
□	_10.0.0.200_HTTP_80	HTTP	80	10.0.0.200	✓	↑	

Select All Unselect All Selected: 0

Figure 15: Virtual service list



□	Name	IP Address or CIDR Subnet	Status	Health	HA Group
□	IIS VIP	10.0.0.200	✓	↑	

Select All Unselect All Selected: 0

Figure 16: Virtual server list

14 ADVANCED CONFIGURATION

This section contains the advanced configuration of the AX Series with Microsoft Windows IIS 7.0. The advanced configuration increases server performance with features such as SSL Offload, HTTP Compression, HTTP Connection Reuse, Cookie Persistence, and RAM Caching.

The first step in the advanced configuration is to predefine all the optimization and performance features in configuration templates. Once all the performance features are defined in the templates, you can bind the features to the VIP.

Note: *With the assumption that you already understand basic configuration of the server, service group, virtual service and virtual server, this section will move directly to advanced configuration with minimal changes from the basic configuration.*

15 SSL OFFLOAD

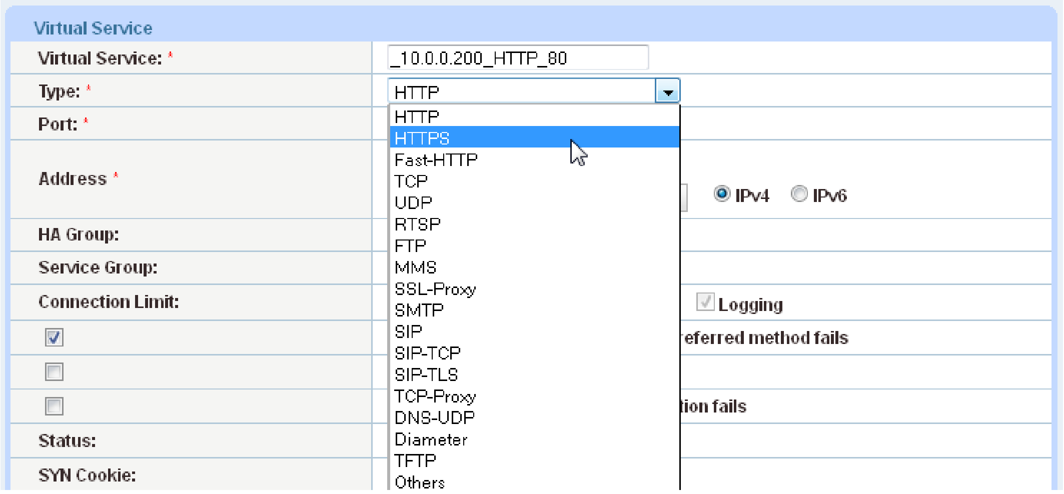
SSL Offload mitigates the impact of a web server application or web server farm from the burden of encrypting and decrypting SSL traffic sent via secure SSL. SSL Offload is a performance optimization that enables a server to offload the SSL traffic to the AX Series.

To configure AX SSL Offload with Microsoft IIS 7.0, navigate to the IIS application virtual service on the AX device, and change the virtual service type from 80 (HTTP) to 443 (HTTPS).

1. Navigate to **Config Mode > Service > SLB > Virtual Service**.
2. Click on the service name.
3. Select “HTTPS” from the **Port** drop-down list.

Note: *You also may want to change the name to correlate with the virtual port name. (As an example, the "_10.0.0.200_HTTP_80" service should be renamed “_10.0.0.200_HTTPS_443” if the virtual port is updated to use the HTTPS service type).*

Note: *Leave the port 80 configuration in the service group and server. SSL offload is configured as HTTPS (443) from the front end but is HTTP (80) to the backend servers/server pool.*



Virtual Service

Virtual Service: * _10.0.0.200_HTTP_80

Type: * HTTP

Port: *

Address * ● IPv4 ○ IPv6

HA Group:

Service Group:

Connection Limit: ☑ Logging

☑ referred method fails

☐

☐ tion fails

Status:

SYN Cookie:

Figure 17: Virtual service configuration

15.1 IMPORT OR GENERATE THE SERVER CERTIFICATE

Since the AX device will act as an HTTPS proxy for the Microsoft IIS web servers, the server certificate for each server must be imported onto or generated on the AX device.

There are two options to configure when installing an SSL template from the AX Series:

- **Option 1:** Generate a Self-Signed on the AX device.
- **Option 2:** Import an SSL Certificate and Key signed by a Certificate Authority (CA).

15.1.1OPTION 1: GENERATE A SELF-SIGNED CERTIFICATE

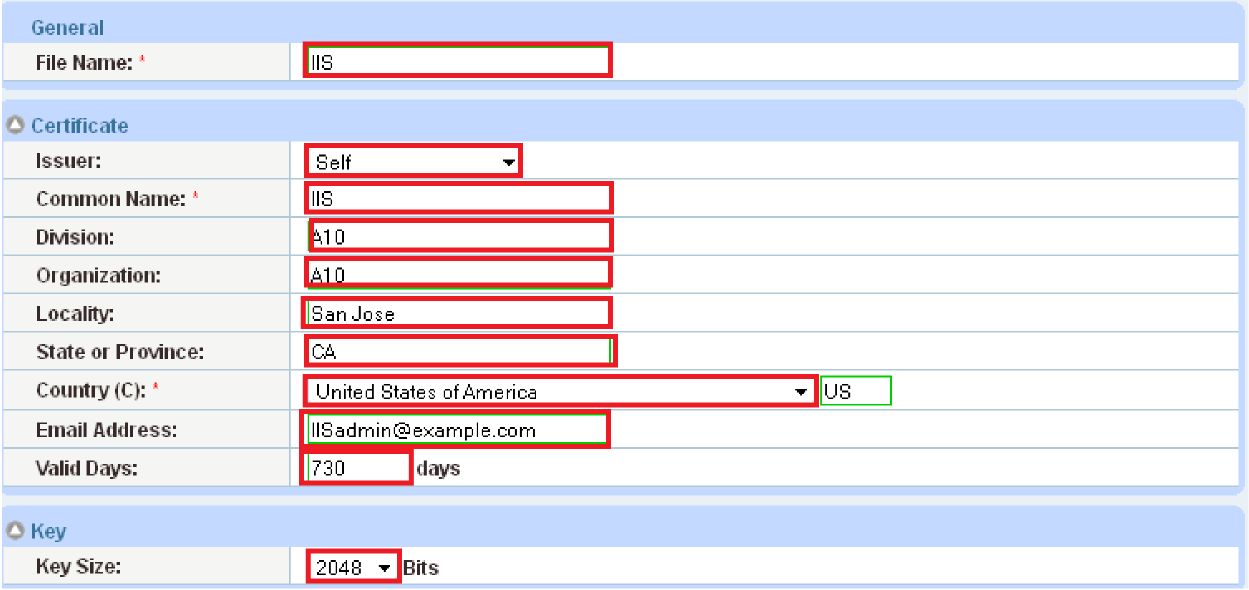
1. Navigate to **Config Mode > Service > SSL Management > Certificate**.
2. Click **Create**.
3. Enter the **File Name** of the certificate, “WS”.

4. From the **Issuer** drop-down list, select “Self”.

5. Enter the following values:

    - **Common Name:** “IIS”
    - **Division:** “A10”
    - **Organization:** “A10”
    - **Locality:** San Jose
    - **State or Province:** “CA”
    - **Country:** “USA”
    - **Email Address:** “IISadmin@example.com”
    - **Valid Days:** “730” (Default)
    - **Key Size (Bits):** “2048”

Note: *The AX Series can support 512-bit, 1028-bit, 2048-bit, and 4096-bit keys. The higher the bit size, the more CPU processing that will be required on the AX device.*



General

File Name: *	IIS

Certificate

Issuer:	Self
Common Name: *	IIS
Division:	A10
Organization:	A10
Locality:	San Jose
State or Province:	CA
Country (C): *	United States of America US
Email Address:	IISadmin@example.com
Valid Days:	730 days

Key

Key Size:	2048 Bits

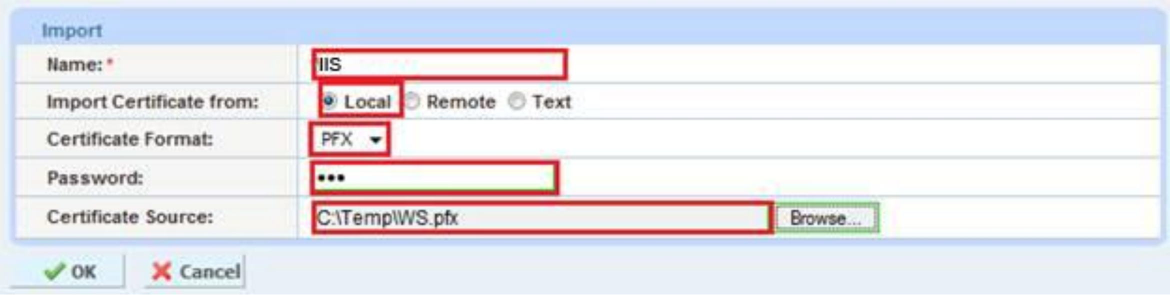
Figure 18: Self-signed certificate configuration

6. Click **OK**, then click **Save** to save the configuration.

15.1.2 OPTION 2: IMPORT THE CERTIFICATE AND KEY

1. Navigate to **Config Mode > Service > SSL Management > Certificate**.
2. Click **Import**.
3. Enter the **Name**, “IIS”.
4. Select “Local” or “Remote”, depending on the file location.
5. Enter the certificate **Password** (if applicable).
6. Enter or select file location and access settings.
7. Click **OK**.

Note: *If you are importing a CA-signed certificate for which you used the AX device to generate the CSR, you do not need to import the key. The key is automatically generated on the AX device when you generate the CSR.*



Import

Name: *	IIS
Import Certificate from:	● Local ○ Remote ○ Text
Certificate Format:	PFX
Password:	•••
Certificate Source:	C:\Temp\WS.pfx

Figure 19: SSL certificate import

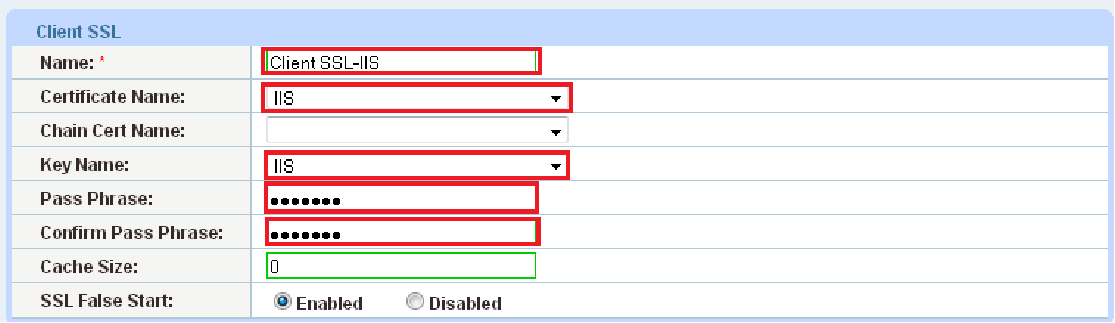
8. Click **OK**, then click **Save** to save the configuration.

16 CONFIGURE AND APPLY CLIENT SSL TEMPLATE

This section describes how to configure a client SSL template and apply it to the VIP.

1. Navigate to **Config Mode > Service > Template > SSL > Client SSL**.
2. Click **Add**.
3. Enter or select the following values:
   - **Name:** “Client SSL-IIS”
   - **Certificate Name:** “IIS”

- **Key Name:** “IIS”
- **Pass Phrase:** “example”
- **Confirm Pass Phrase:** “example”



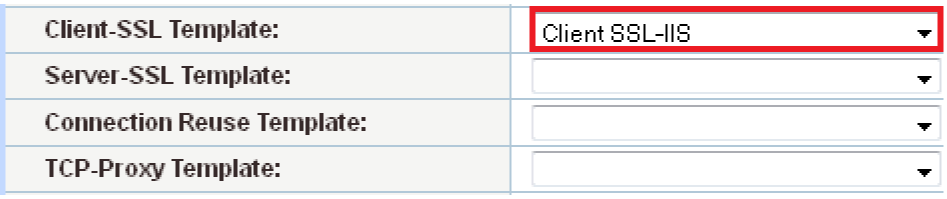
Client SSL

Name: *	Client SSL-IIS
Certificate Name:	IIS
Chain Cert Name:	
Key Name:	IIS
Pass Phrase:	•••••••
Confirm Pass Phrase:	•••••••
Cache Size:	0
SSL False Start:	● Enabled ○ Disabled

Figure 20: Client SSL template

Once the Client SSL template is completed, you must bind the template to the HTTPS VIP (port 443), as follows:

1. Navigate to **Config Mode > SLB > Virtual Server**.
2. Click on the virtual server name.
3. Select “443” and click **Edit**.
4. Apply the Client SSL template created by selecting it from the **Client-SSL Template** drop-down list.



Client-SSL Template:	Client SSL-IIS
Server-SSL Template:	
Connection Reuse Template:	
TCP-Proxy Template:	

Figure 21: Client SSL template selection

5. Click **OK**, then click **Save** to save the configuration.

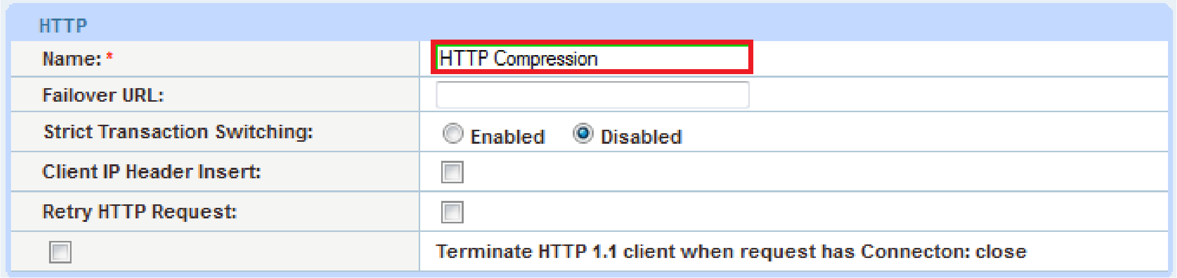
17 HTTP COMPRESSION

HTTP Compression is a bandwidth optimization feature that compresses the requested HTTP objects from a web server. If your web site uses lots of bandwidth, enabling HTTP Compression will provide faster transmission times between a client's browser and web servers. The purpose of compression is to transmit the requested data more efficiently and with faster response times to the client. HTTP Compression makes HTTP requests much faster by transmitting less data.

17.1 CREATE HTTP COMPRESSION TEMPLATE

1. Navigate to **Config Mode > Template > Application > HTTP**.
2. Click **Add**.
3. Enter a **Name**, "HTTP Compression".
4. Click **Compression** to display the compression configuration options.

Note: *Compression is disabled by default. When compression is enabled, the compression options will have the default values shown in following example*:



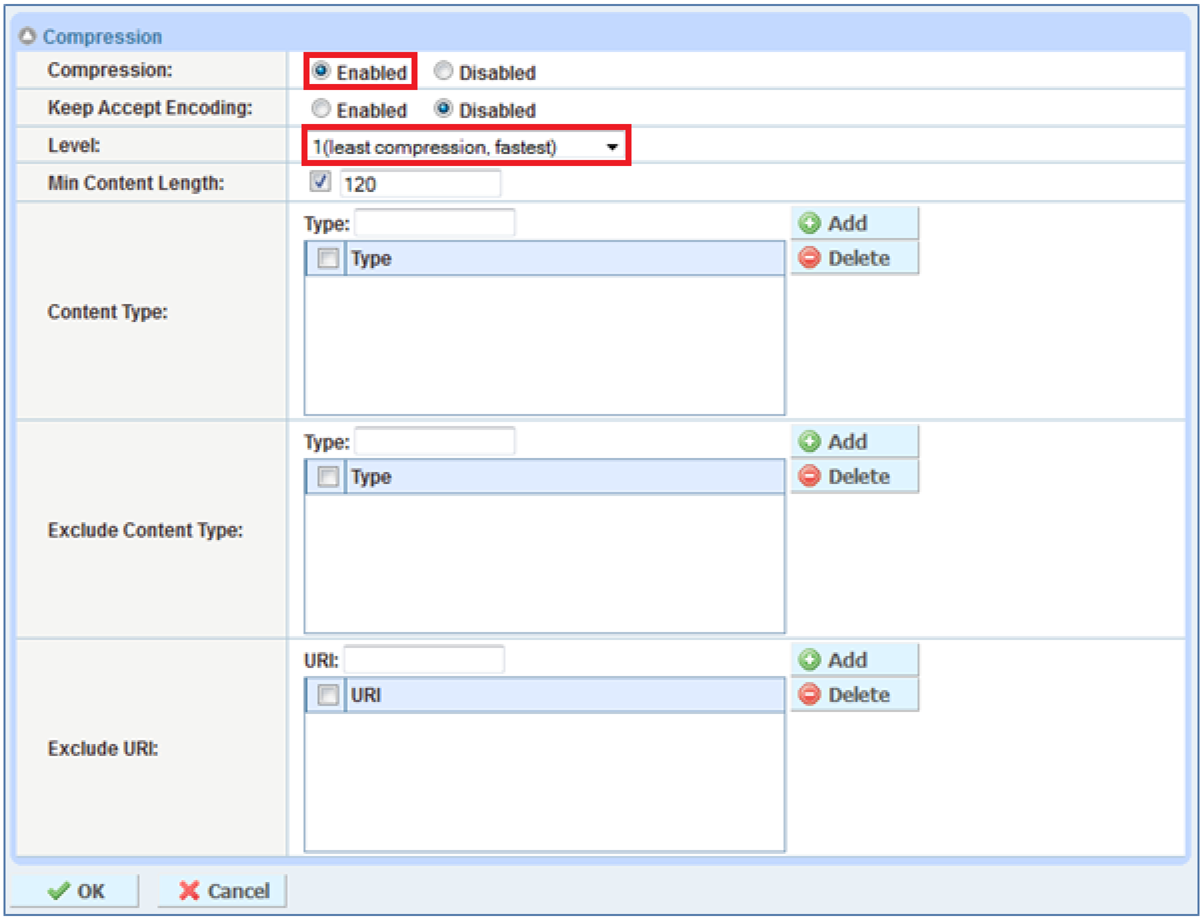
HTTP

Name: *	HTTP Compression
Failover URL:	
Strict Transaction Switching:	○ Enabled ● Disabled
Client IP Header Insert:	□
Retry HTTP Request:	□
□	Terminate HTTP 1.1 client when request has Connecton: close

Figure 22: HTTP Compression template

5. Select Enabled next to **Compression**.

Note: *The AX offers various compression levels, ranging from levels 1 to 9. Level 1 is the recommended compression setting.*



Compression

Compression:	● Enabled ○ Disabled
Keep Accept Encoding:	○ Enabled ● Disabled
Level:	1(least compression, fastest)
Min Content Length:	☑ 120
Content Type:	Type: □ Type
Exclude Content Type:	Type: □ Type
Exclude URI:	URI: □ URI

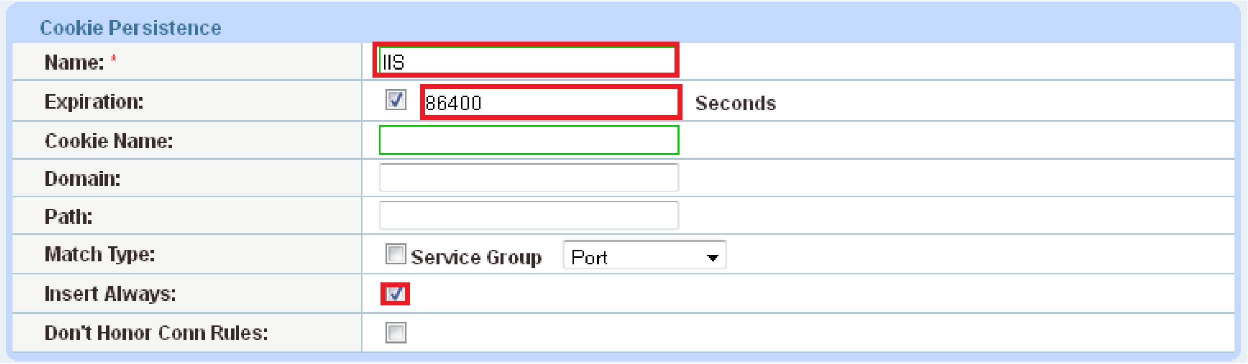
Figure 23: Compression configuration column

6. Click **OK**, then click **Save** to save the configuration.

18 COOKIE PERSISTENCE

To enable cookie persistence, the template must be created first, as follows:

1. Navigate to **Config mode > Service > Template > Cookie Persistence**.
2. Click **Add** to add a new cookie persistence template.
3. Enter the **Name**, "IIS".
4. Select the **Expiration** radio button and enter “86400” in the **Seconds** field.
5. Select the **Insert Always** checkbox.



Cookie Persistence

Name: *	IIS
Expiration:	☑ 86400 Seconds
Cookie Name:	
Domain:	
Path:	
Match Type:	□ Service Group Port
Insert Always:	☑
Don't Honor Conn Rules:	□

Figure 24: Cookie Persistence template

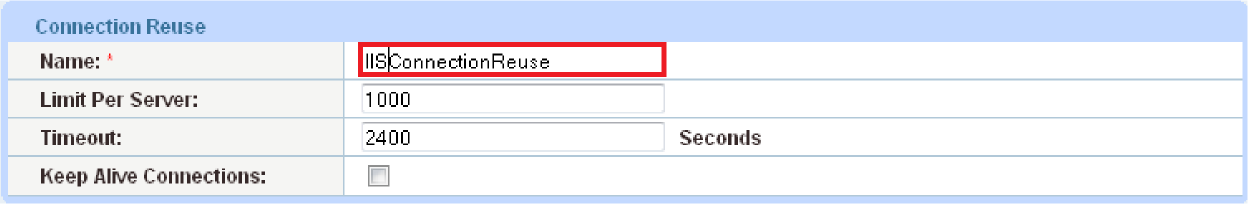
6. Click **OK**, then click **Save** to save the configuration.

19 TCP CONNECTION REUSE

1. Navigate to **Config Mode> Template > Connection Reuse**.

2. Click **Add**.

3. Enter **Name**: "IISConnectionReuse".



Connection Reuse

Name: *	IISConnectionReuse
Limit Per Server:	1000
Timeout:	2400 Seconds
Keep Alive Connections:	□

Figure 25: TCP Connection Reuse template

4. Click **OK**, then click **Save** to save the configuration.

20 RAM CACHING

Cacheable data is cached within the AX Series device, thus reducing overhead on the IIS web servers and increasing their capacity. RAM Caching reduces the number of connections and server requests that need to be processed.

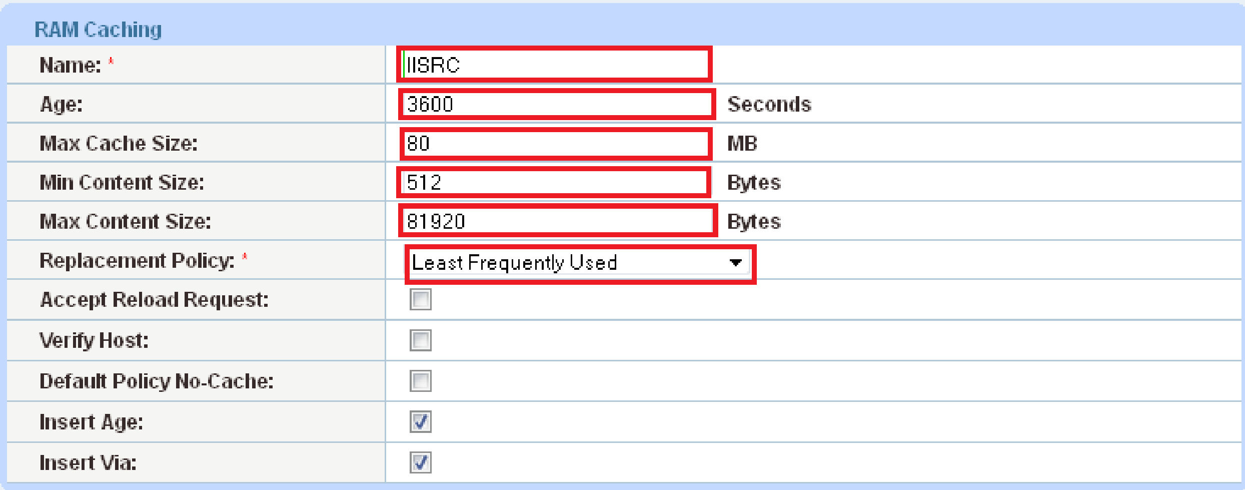
1. Navigate to **Config Mode > Service > Template > Application > RAM Caching**.

2. Click **Add**.

3. Enter or select the following values:

- **Name:** “IISRC”
- **Age:** 3600 seconds
- **Max Cache Size:** 80 MB
- **Min Content Size:** 512 Bytes
- **Max Content Size:** 81920 Bytes
- **Replacement Policy**: “Least Frequently Used”

Note: *The RAM Caching policy option is not required unless you have specific data that requires caching, no caching or invalidation. These policy options can be configured in the policy section of the RAM Caching template. For additional information on RAM caching policies, please refer to the AX Series Application Delivery and Server Load Balancing Guide.*



RAM Caching

Name: *	IISRC	
Age:	3600	Seconds
Max Cache Size:	80	MB
Min Content Size:	512	Bytes
Max Content Size:	81920	Bytes
Replacement Policy: *	Least Frequently Used	
Accept Reload Request:	□	
Verify Host:	□	
Default Policy No-Cache:	□	
Insert Age:	☑	
Insert Via:	☑	

Figure 26: RAM Caching template

4. Click **OK**, then click **Save** to save the configuration.

21 HTTP-TO-HTTPS REDIRECT

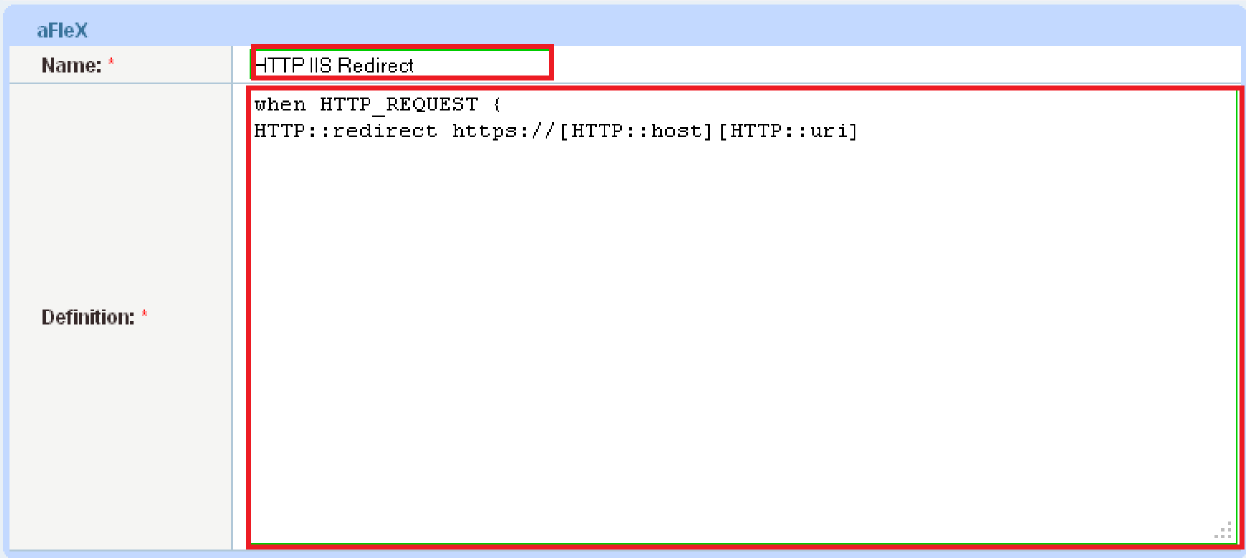
This section explains how to redirect IIS traffic that originates from HTTP to HTTPS using AX aFleX scripts. aFleX is based on a standard scripting language, TCL, and enables the AX device to perform Layer 7 deep-packet inspection (DPI). For examples of aFleX scripts, please refer to the following URL:

http://www.a10networks.com/products/axseries-aflex_advanced_scripting.php

As an example, one of the most commonly used aFleX scripts is the "HTTP redirect to HTTPS traffic" script. You can download additional aFleX script examples from the URL listed above.

To configure a transparent HTTPS redirect using aFleX:

1. Create the aFleX script.
2. Configure a VIP with virtual service HTTP (port 80).
3. Apply the aFleX script to the virtual port on the VIP.



Name: * HTTP IIS Redirect

Definition: *

```
when HTTP_REQUEST {
HTTP::redirect https://[HTTP::host][HTTP::uri]
```

Figure 27: Redirect script

Redirect Script Copy and Paste:

```
when HTTP_REQUEST {

HTTP::redirect https://[HTTP::host][HTTP::uri]

}
```

Note: *The aFleX script must be bound to virtual-server port 80.*

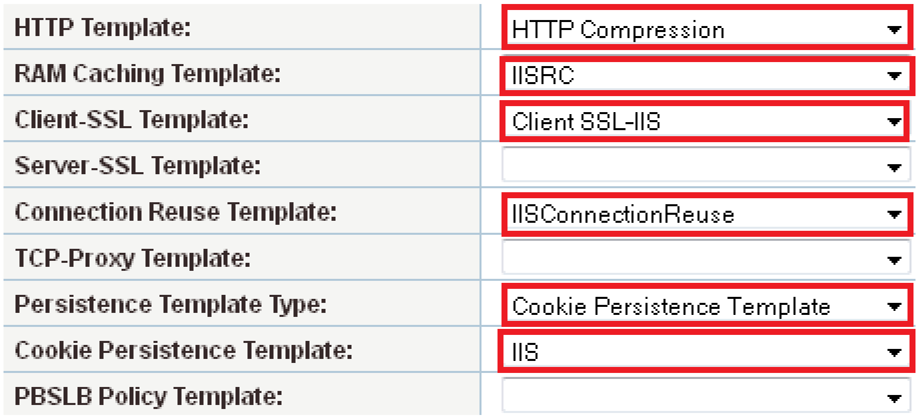
22 APPLY OPTIMIZATION AND ACCELERATION FEATURE TEMPLATES ON VIP

After configuring the optimization and acceleration features, you must bind them to the virtual port on the VIP to place them into effect.

1. Navigate to **Config Mode > SLB > Virtual Service**.

2. Click on the virtual service name.

3. Apply the features by selecting the templates from the applicable drop-down lists.



HTTP Template:	HTTP Compression
RAM Caching Template:	IISRC
Client-SSL Template:	Client SSL-IIS
Server-SSL Template:	
Connection Reuse Template:	IISConnectionReuse
TCP-Proxy Template:	
Persistence Template Type:	Cookie Persistence Template
Cookie Persistence Template:	IIS
PBSLB Policy Template:	

Figure 28: Applying features

4. Click **OK**, then click **Save** to save the configuration.

23 SUMMARY AND CONCLUSION

The sections above show how to deploy the AX device for optimization of Microsoft IIS web servers. By using the AX device to load balance a pool of IIS web servers, the following key advantages are achieved:

- High availability for IIS web servers to prevent web site failure, with no adverse impact on user access to applications

- Seamless distribution of client traffic across multiple IIS web servers for site scalability

- Higher connection counts, faster end user responsiveness, and reduced IIS server CPU utilization by initiating SSL Offload, HTTP Compression, RAM Caching and Connection Reuse

- Improved site performance and reliability to end users

By using the AX Series Advanced Traffic Manager, significant benefits are achieved for all Microsoft IIS web application users. For more information about AX Series products, please refer to the following URLs:

http://www.a10networks.com/products/axseries.php

http://www.a10networks.com/resources/solutionsheets.php

http:/www.a10networks.com/resources/casestudies.php

A. CLI COMMANDS FOR SAMPLE BASIC CONFIGURATION

The following sections show the CLI commands for implementing the sample configurations described above.

```
IISAX#show running-config

hostname IISAX

clock timezone Europe/Dublin

slb server IIS1 10.0.0.4

   port 80  tcp

slb server IIS2 10.0.0.5

   port 80  tcp

slb service-group SG80 tcp

    member IIS1:80

    member IIS2:80

slb virtual-server "IIS VIP" 10.0.0.200

   port 80  http

      name _10.0.0.200_HTTP_80

      source-nat pool "Source NAT"

      service-group SG80

end

IISAX#
```

B. CLI COMMANDS FOR SAMPLE ADVANCED CONFIGURATION

```
IISAX#show running-config

hostname IISAX

clock timezone Europe/Dublin

ip nat pool "Source NAT" 10.0.0.50 10.0.0.50 netmask /24

health monitor "IIS HC"

 method http

slb server IIS1 10.0.0.4

   port 80  tcp

slb server IIS2 10.0.0.5

   port 80  tcp

slb service-group SG80 tcp

    member IIS1:80

    member IIS2:80

slb template connection-reuse IISConnectionReuse

slb template cache IISRC

slb template http "HTTP Compression"

slb template client-ssl "Client SSL-IIS"

   cert IIS

   key IIS pass-phrase encrypted
KZlpUbp6Q888EIy41dsA5zwQjLjV2wDnPBCMuNXbAOc8EIy41dsA5zwQjLjV2wDn

slb template persist cookie IIS

   expire 86400

   insert-always

slb template persist source-ip srcip

slb virtual-server "IIS VIP" 10.0.0.200
```

```
   port 443  https
      name _10.0.0.200_HTTPS_443
      source-nat pool "Source NAT"
      service-group SG80
      template http "HTTP Compression"
      template cache IISRC
      template client-ssl "Client SSL-IIS"
      template http
      template connection-reuse IISConnectionReuse
      template persist cookie IIS
end
IISAX#
```