Deployment Guide

# MobileIron Sentry

## TABLE OF CONTENTS

# 1 INTRODUCTION

MobileIron Sentry is a component of a MobileIron deployment that interacts with your company's ActiveSync server, such as a Microsoft Exchange Server. The ActiveSync server allows employees to access to their email, contacts, calendar, tasks, and notes from their mobile devices. MobileIron Sentry, with input from the Virtual Smartphone Platform (VSP), protects the ActiveSync server from wrongful access from the devices.

MobileIron is an integrated Mobile Device Management (MDM) platform that covers device and data access management. MobileIron Sentry offers a standalone solution or a cloud service solution that can support all the major mobile operating systems, such as Blackberry, Symbian, and Windows. It supports both corporate-liable and individual-owned devices, offering true multi-OS management across the leading mobile OS platforms.

# 2 DEPLOYMENT GUIDE OVERVIEW

This deployment guide shows how to install and configure the A10 device with MobileIron Sentry servers. The Thunder and AX Series Application Delivery Controllers (ADCs) offers additional security, reliability, and optimization features, such as: HTTP Compression, SSL Offload, and HTTP Connection Reuse, which are discussed in this deployment guide.

# 3 DEPLOYMENT GUIDE PREREQUISITES

This MobileIron integration has the following prerequisites:

**A10 tested configuration**

- The A10 Networks AX Series ADC must be running ACOS version 2.6.x or higher (while the AX Series is referred to below a Thunder Series appliance can be used as well)
- MobileIron Sentry has been tested with A10 hardware and virtual appliances.
- MobileIron device requirements
    - MobileIron Sentry
    - Running CentOS 6.4 (Operating System)
    - Running Sentry version 4.5 (or higher)
    - Apache 2.2 HTTP Server ("Apache" and "httpd")
    - Microsoft Exchange 2008 (or higher)

- Client Access (tested)
    - All smart mobile devices have been tested and are supported (except Blackberry Z10)

***Note:*** *Generally, if the MobileIron Sentry Virtual IP (VIP) is accessed from an external client, the AX device is deployed in routed mode. If the MobileIron services are accessed internally, the AX device is deployed in one-arm mode. If the MobileIron applications are accessed from both internal and external clients, then the AX device must be deployed in one-arm mode.*

***Note:*** *For a list of additional deployment modes* that *the* A10 *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 from a Command Line Interface (CLI) or Graphical User Interface (GUI):

- CLI – The CLI is a 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 – This is a web-based interface in which you click buttons, menus and other graphical icons to access the configuration or management pages. From these pages, you can 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 ARCHITECTURE OVERVIEW

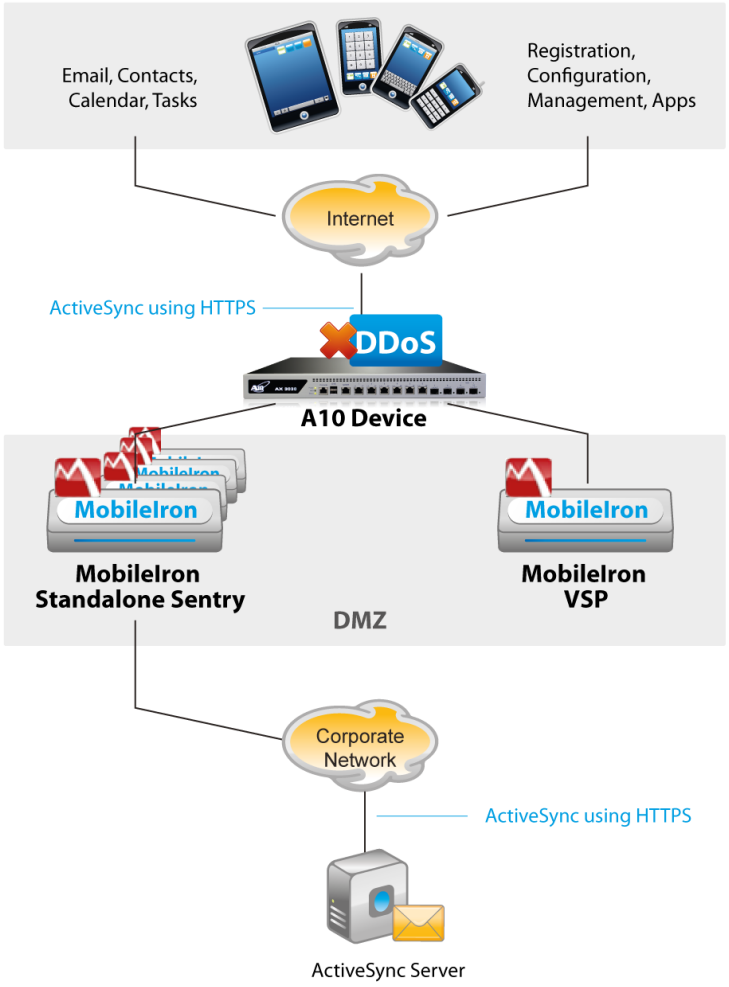


***Figure 5: Configuration overview***

# 6 BASIC CONFIGURATION

This section contains detailed instructions for installing the real servers, service group, virtual services, and virtual services in a basic MobileIron Sentry server.

You must configure HA health monitoring. If your network topology is based on “one-arm” deployment, and internal clients reside on the same subnet as the virtual server for the MobileIron Sentry server, then IP Source Network Address Translation (SNAT) also is required.

***Note:*** *The Virtual Server is also known as the "Virtual IP" (or "VIP") that a client accesses during an initial request.*

# 7 HEALTH MONITOR CONFIGURATION

The AX Series can be configured to automatically initiate health status checks for real servers and service ports. Health checks are used to assure that all requests are sent to functional and available servers. If a server or a port does not respond appropriately to a health check, then the server is temporarily removed from the list of available servers until it starts responding appropriately to the health checks. At this point, the server is automatically added back to the list of available servers.

To configure a health check on the AX device:

1. Navigate to **Config Mode > SLB > Service**
2. Select **Add** from the **Health Monitor** drop-down list. In the **Name** field, enter "MISHC".
3. Select **Method** "HTTPS".
4. Click **OK**, and then proceed to the next section to configure the Service Group.

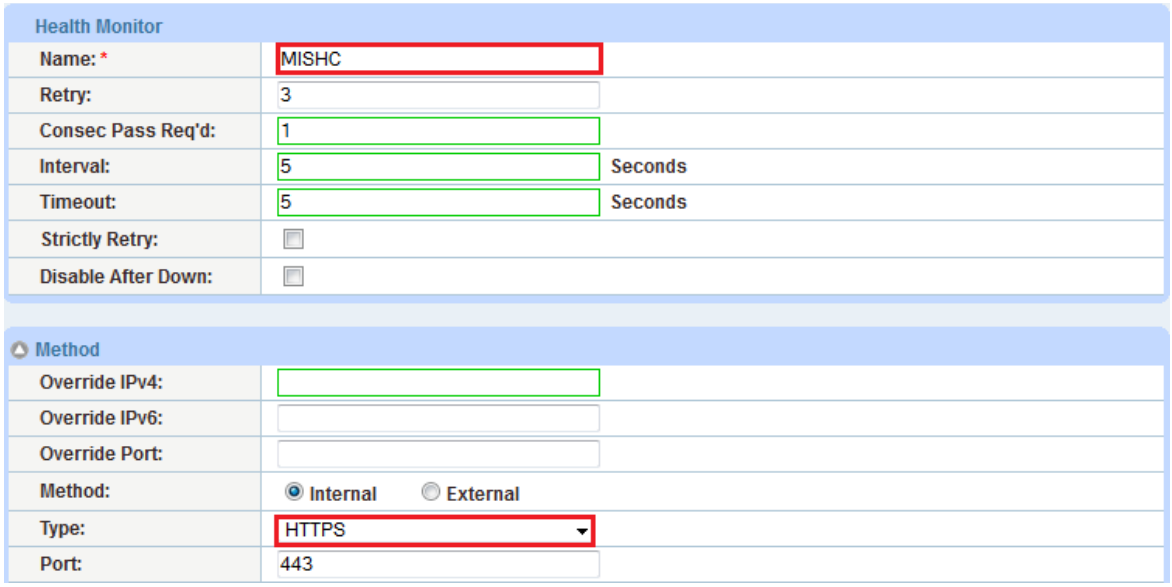


***Figure 6: Health monitor configuration***

# 8 SOURCE NAT CONFIGURATION

This section shows how to configure 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: 192.168.2.100), the client requests are “source NAT-ed”, which means that the AX device replaces the client’s source IP address with an address from a pool of source NAT addresses. SNAT is required when your network topology is based on “one-arm” mode deployment and if you have internal clients that reside on the same subnet as the VIP.

Follow the procedure below to configure the address pool used in Source NAT.

1. Navigate to **Config Mode> Service > IP Source NAT > IPv4 Pool**.
2. Click **Add**.
3. Enter the following:
   - **NAT:** “MISNATPOOL”
   - **Start IP Address:** “192.0.2.100”
   - **End IP Address:** “192.0.2.100”
   - **Netmask:** “255.255.255.0”

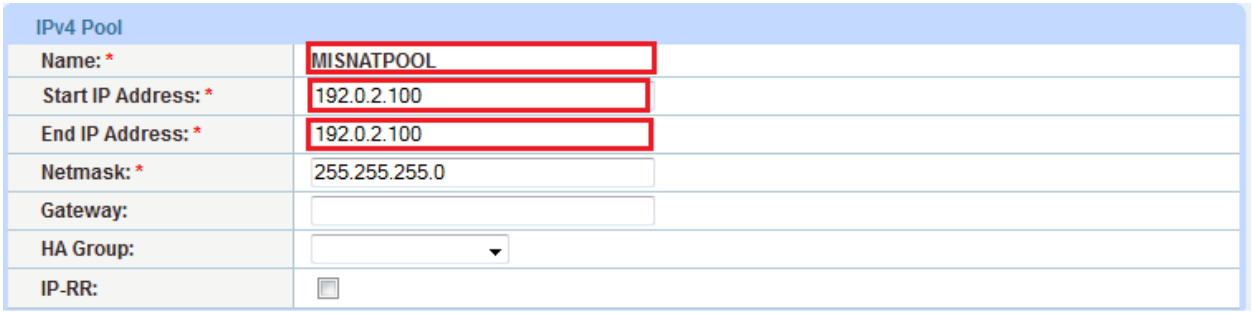


***Figure 7: Source NAT pool configuration***

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

***Note:*** *In the Virtual Service configuration section, you can apply the Source NAT pool to the VIP.*

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

# 9 SERVER CONFIGURATION

Follow the procedure below to configure the MobileIron Sentry on the AX Series.

1. Navigate to **Config Mode > Service > SLB > Server**.
2. Click **Add** to add a new server.
3. Within the Server section, enter the following required information:
   - **Name:** "MIS1"
   - **IP address /Host:** "192.0.2.4"

   ***Note:*** *Enter additional servers if necessary.*

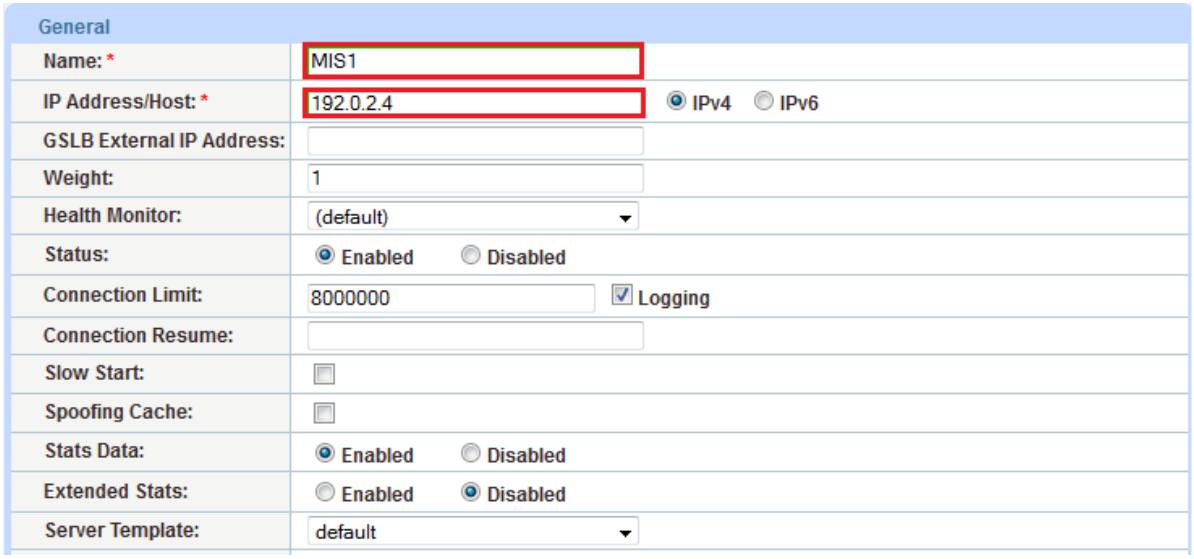


***Figure 8: Server configuration***

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**.

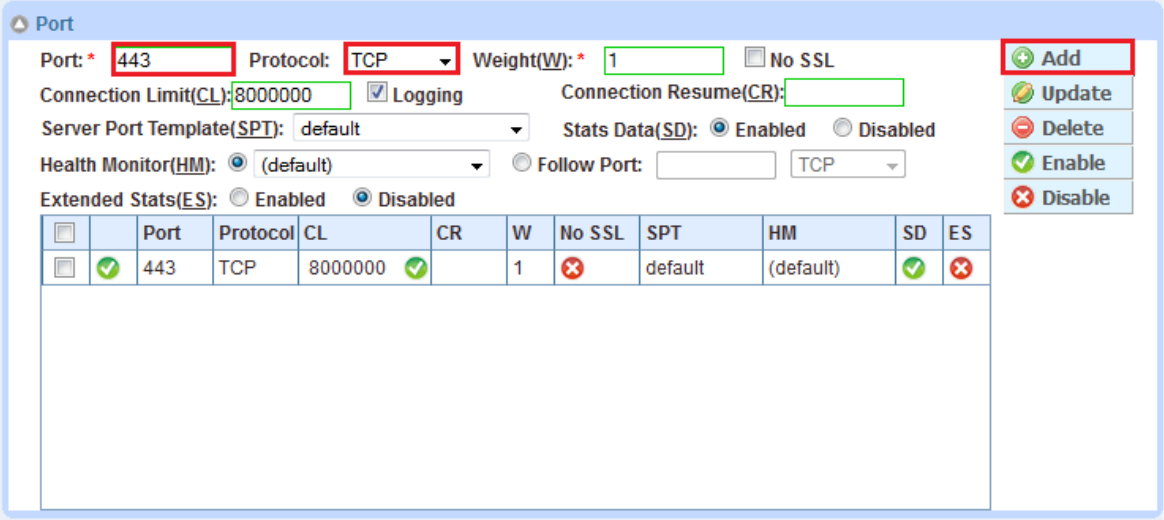


***Figure 9: Server port configuration***

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

## 10 SERVICE GROUP CONFIGURATION

Follow the procedure below to configure a service group.

1. Navigate to **Config Mode > Service > SLB > Service Group**.
2. Click **Add**.
3. Enter or select the following values:
   - **Name:** "MISGROUP"
   - **Type:** "TCP"
   - **Algorithm:** "Round Robin"
   - **Health Monitor:** "MISHC"
4. In the Server section, select a server from the Server drop-down list and enter "443" in the **Port** field.
5. Click **Add**. Repeat for each server.

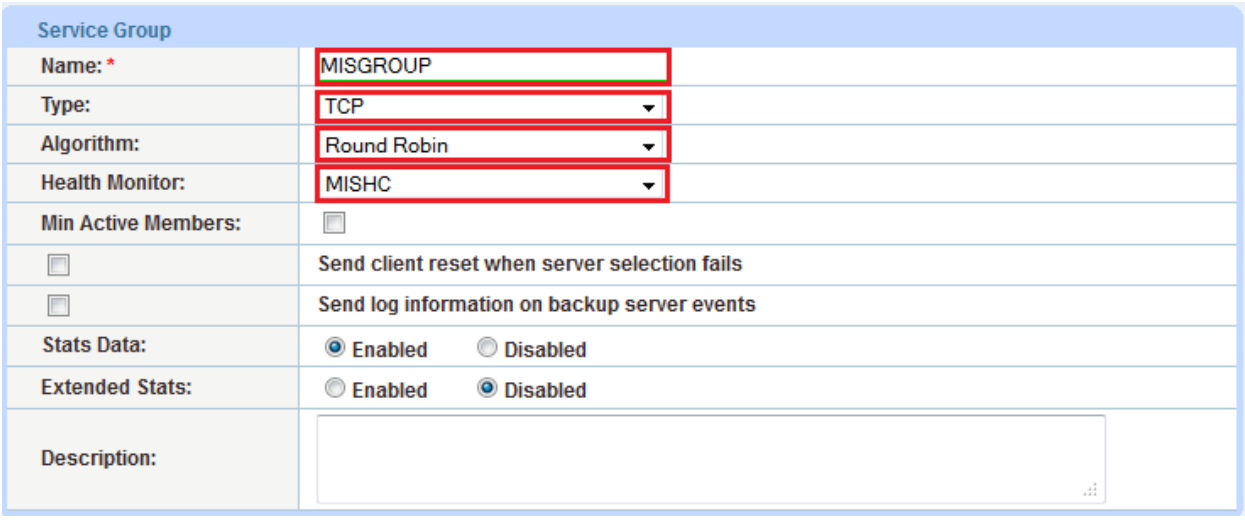


***Figure 10: Service group configuration***

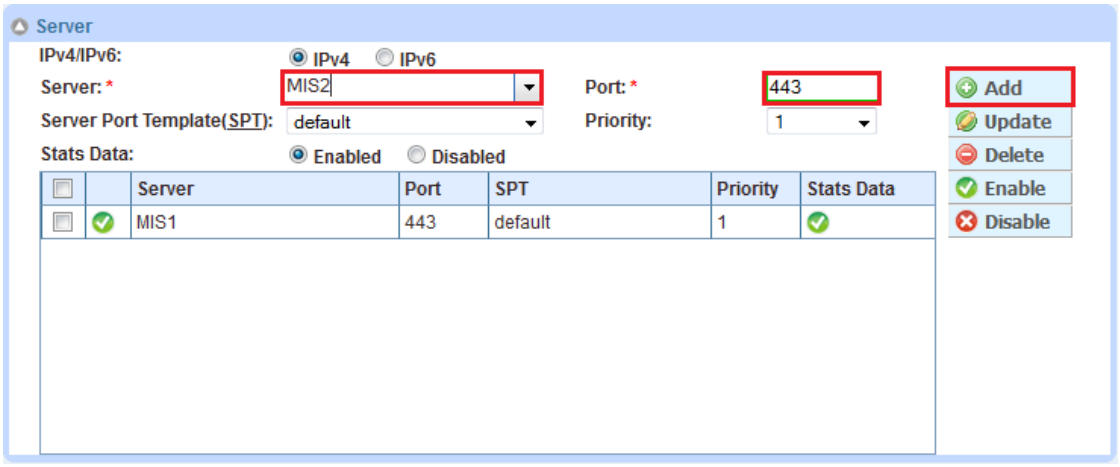


***Figure 11: Server configuration***

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

## 11 VIRTUAL SERVER CONFIGURATION

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

1. Navigate to **Config Mode > Service > SLB > Virtual Service**.
2. In the General section, enter the name of the VIP and its IP address:

- **Name:** "MISVIP"
- **IP Address:** "203.0.113.200"

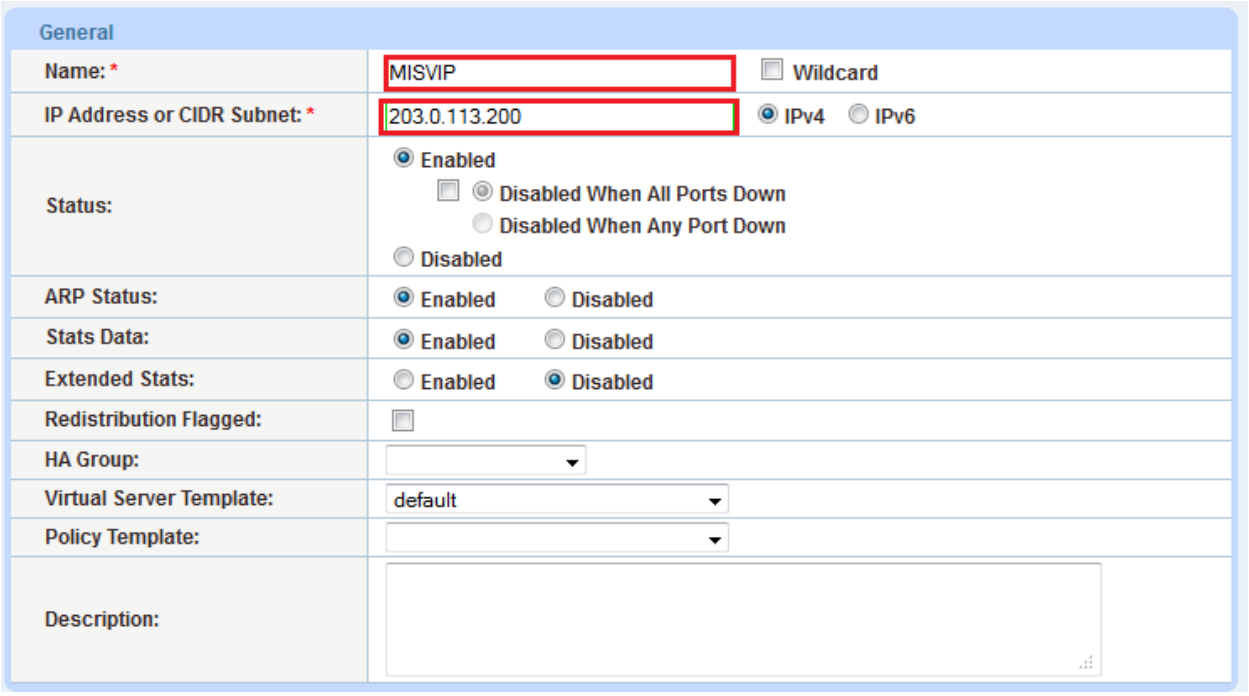


***Figure 12: Virtual server (VIP) configuration***

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

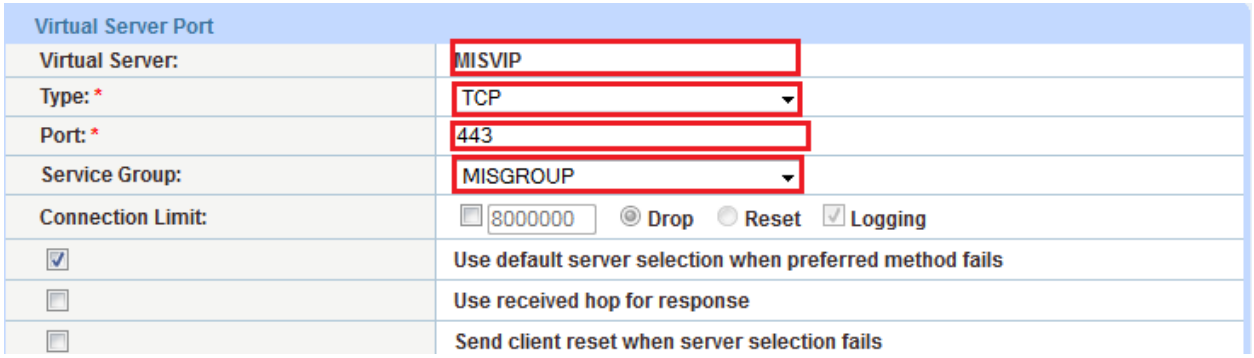


***Figure 13: Virtual-server port configuration***

4. Select the following values:

- **Virtual Server:** "TCP"

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

- Port: 443
- Address: MISVIP
- **Service Group:** "MISGROUP"

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

## 12 ADVANCED CONFIGURATION

This section contains the advanced configuration of the AX Series with MobileIron Sentry. The advanced configuration increases server performance with features such as SSL Offload, HTTP Connection Reuse, DDoS, and DNS Application Firewall.

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:*** *This section moves directly from the basic configuration into advanced configuration, based on the assumption that you already familiar with the basics of configuring the server, service group, virtual service, and virtual server.*

## 13 SSL OFFLOAD

SSL Offload mitigates the performance impact associated with encrypting and decrypting traffic on a web server. SSL Offload is a performance optimization feature that enables a server to offload the SSL traffic to the AX Series. Additionally, SSL Offloads provides ease of administration; only the ADC requires an SSL certificate, as opposed to each server.

To configure AX SSL Offload for the MobileIron Sentry server, navigate to the MobileIron virtual service on the AX device, and change the virtual service type from 443 (TCP) 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 "_203.0.113.200_TCP_443" service should be renamed “_203.0.113.200_HTTPS_443” when updating the virtual port from TCP to HTTPS service type.)*

*Note2: If you are using identity or device certificates do not configure SSL Offload as the Sentry needs the certificate to determine who the user is and there is no way to pass the certificate from the AX to the Sentry.*

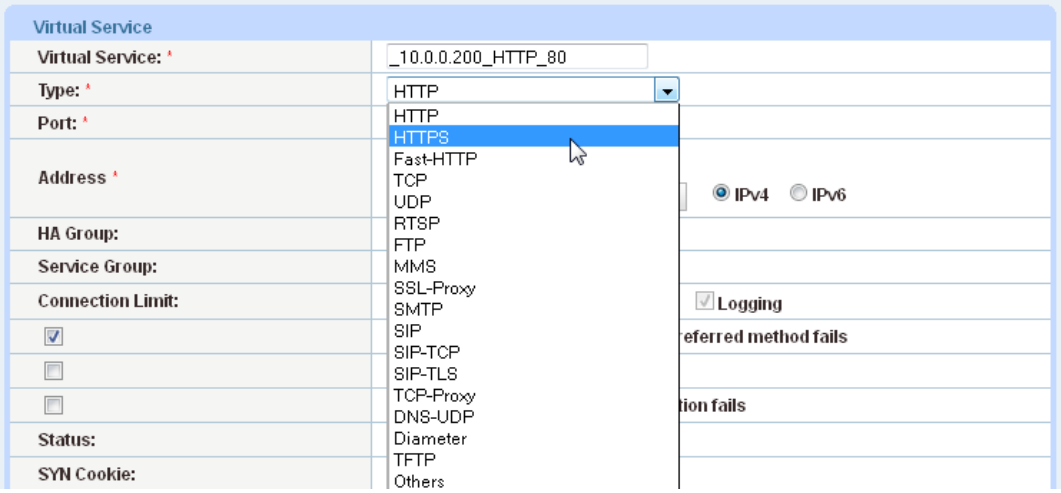


***Figure 17: Virtual service configuration***

## 13.1 IMPORT OR GENERATE THE SERVER CERTIFICATE

Since the AX device acts as an HTTPS proxy for the MobileIron Sentry servers, the AX device must have a certificate from each server.

There are two options that must be configured when installing an SSL template from the AX Series:

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

### 13.1.1 OPTION 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, “MISCERT”.
4. From the **Issuer** drop-down list, select “Self”.
5. Enter the following values:

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

***Note:*** *The AX Series supports 512-bit, 1028-bit, 2048-bit, and 4096-bit keys.*

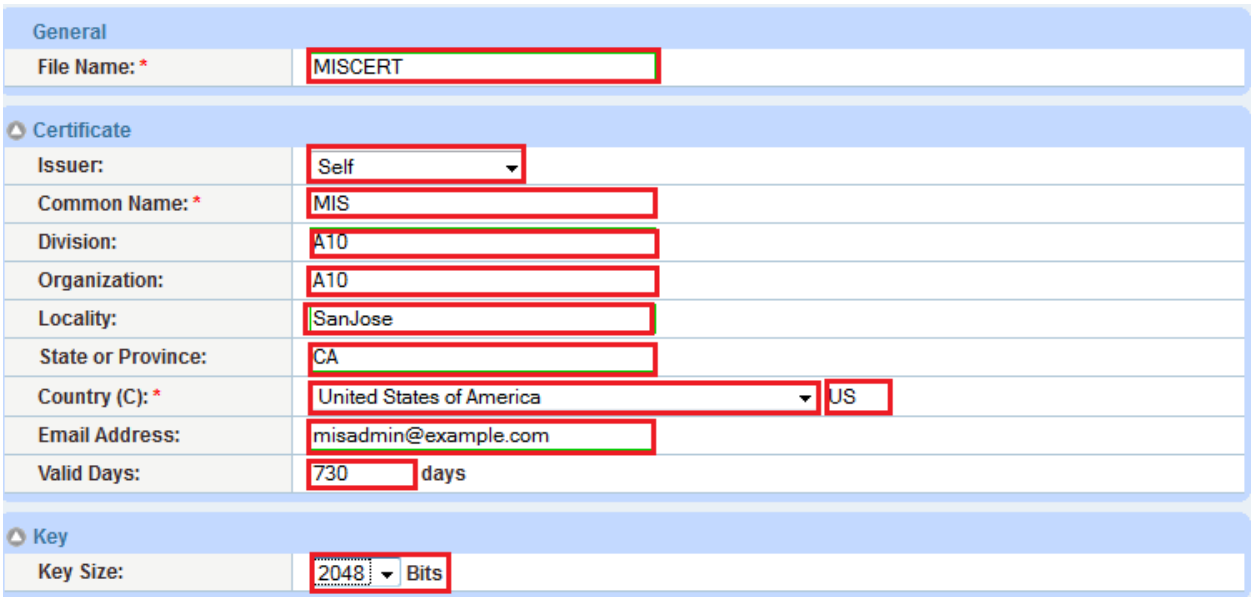


***Figure 18: Self-signed certificate configuration***

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

### 13.1.2 OPTION 2: IMPORT THE CERTIFICATE AND KEY

1. Navigate to **Config Mode > Service > SSL Management > Certificate**.
2. Click **Import**.
3. Enter the **Name**, “MISCERT”.
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.*

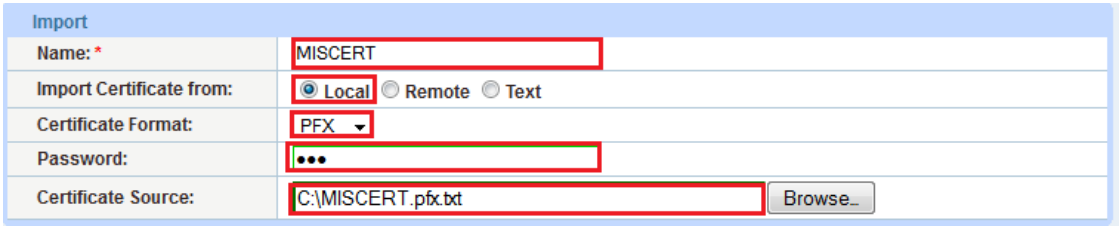


***Figure 19: SSL certificate import***

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

## 13.2 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-MIS”
   - **Certificate Name:** "MISCERT”
   - **Key Name:** “MISCERT”

- **Pass Phrase:** “example”
- **Confirm Pass Phrase:** “example”

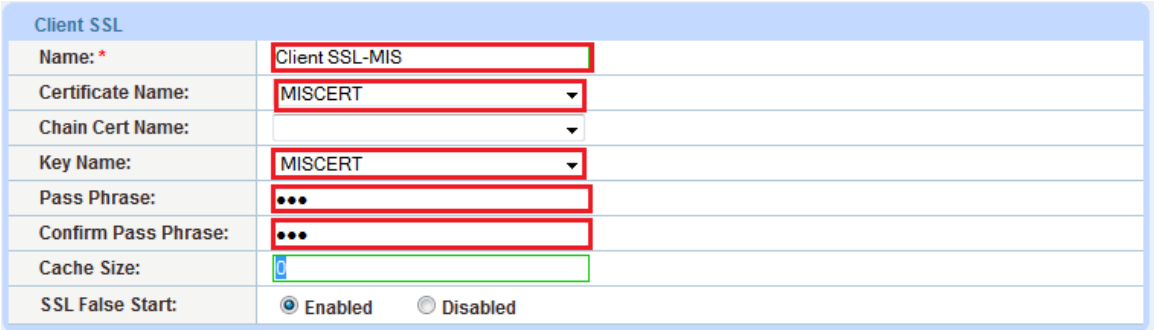


***Figure 20: Client SSL template***

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 > Service > 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.

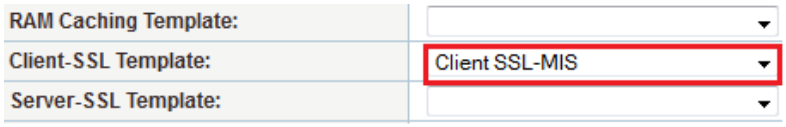


***Figure 21: Client SSL template selection***

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

## 14 TCP CONNECTION REUSE

1. Navigate to **Config Mode > Service > Template > Connection Reuse**.
2. Click **Add**.
3. Enter **Name**: “MISConnectionreuse”.

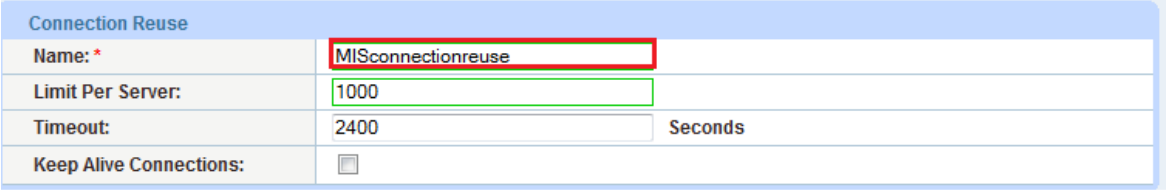


***Figure 25: TCP Connection Reuse template***

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

***Note:*** *For the best connection reuse results, these are the recommend MobileIron Sentry Apache HTTP web server settings in the Apache httpd.conf file.*

- KeepAlive – On
- MaxKeepAliveRequests – 0 or a high number such as 800+. The value 0 = unlimited.
- KeepAlive Timeout – high value, 250+
- MaxRequestsPerChild – 5000-10000

## 15 HTTP-TO-HTTPS REDIRECT

This section explains how to redirect MobileIron Sentry traffic that originates from HTTP (80) to HTTPS (443) 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. Navigate to **Config Mode > Service > aFleX**
2. Create the aFleX script.
3. Configure a VIP with virtual service HTTP (port 80).
4. Apply the aFleX script to the virtual port on the VIP.

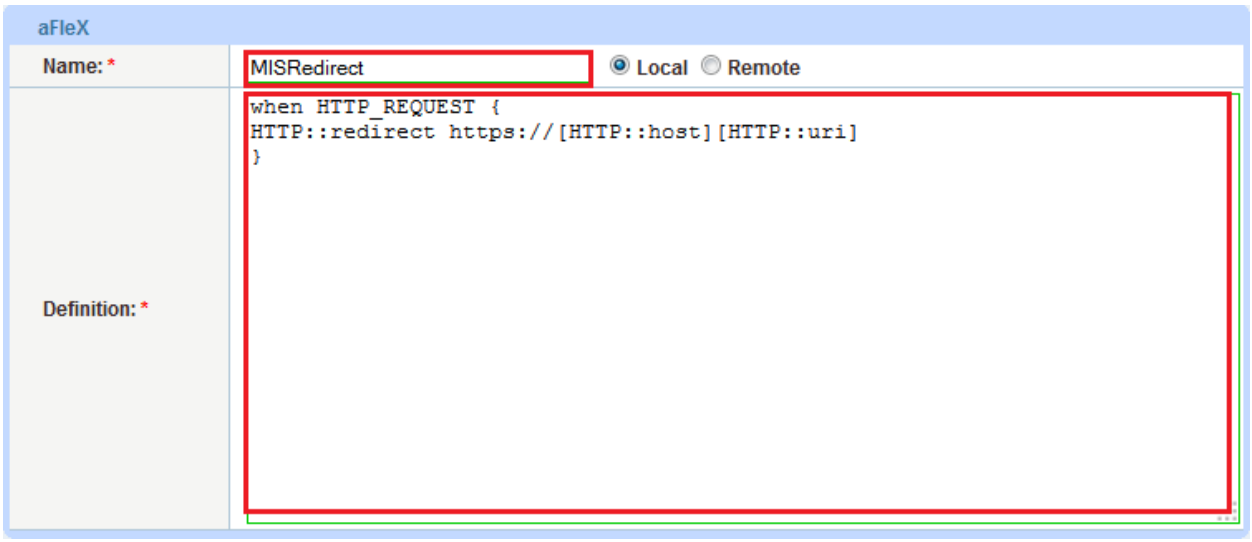


***Figure 27: Redirect script***

**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.*

## 16 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 > Service > SLB > Virtual Service**.
2. Click on the virtual service name.

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


***Figure 28: Applying features***

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

## 17 OTHER OPTIONAL FEATURES

The AX Series adds another security layer for load balanced servers and applications. Adding to an in-depth defense strategy, key protections are architected into A10 device hardware and software.

A10 provides high-performance detection and prevention against distributed denial-of-service (DDoS) and protocol attacks that can cripple servers and take down applications. Since the AX Series is placed between the routers and data center resources, it is ideally positioned to detect and stop attacks directed at any data center server or application. Using specialized ASICs in select models, A10 can continue to inspect, stop, and redirect all application traffic at network speeds.

1. To install a standard set og DDoS mitigation features, navigate to **Config Mode > Service > SLB > Global > DDoS Protection.**

2. Select all the checkboxes for the DDoS Protection features you would like to activate.

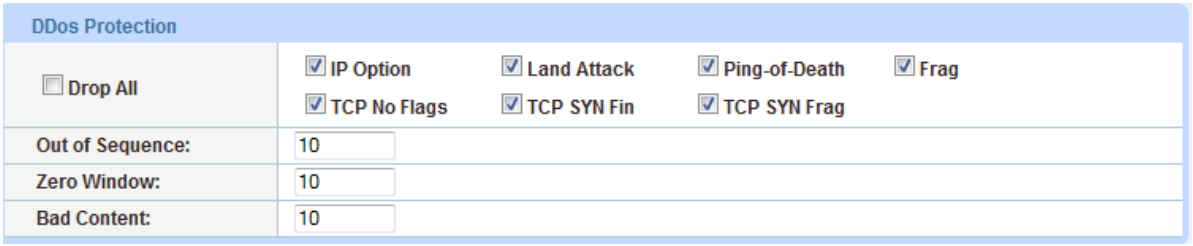


***Figure 29: DDoS Protection***

6. Click **OK** and then click **Save** to store your configuration changes.

For other DDoS protection mechanisms please refer to the standard Systems Configuration and Administration Guide.

## 18 SUMMARY AND CONCLUSION

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

- High availability for MobileIron servers helps prevent ActiveSync sessions failures, with no adverse impact on mobile access to applications.
- Seamless distribution of client traffic across multiple MobileIron servers for site scalability.
- Higher connection counts, faster end user responsiveness, and reduced MobileIron Sentry server CPU utilization by initiating SSL Offload, TCP Connection Reuse, and DDoS mitigation.
- Improved site performance and reliability to end users by deploying DDoS mitigation features from A10 Networks.

By using the AX Series Advanced Traffic Manager, significant benefits are achieved for all MobileIron Sentry ActiveSync 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:

```
hostname basmis
ip nat pool MISNATPOOL 192.0.2.100 192.0.2.100 netmask /24
health monitor MISHC
 method tcp
slb server MIS1 192.0.2.4
   port 443  tcp
slb server MIS2 192.0.2.5
   port 443  tcp
slb service-group MISGROUP tcp
```

```
    health-check MISHC
    member MIS1:443
    member MIS2:443
slb template connection-reuse MISconnectionreuse
slb virtual-server MISVIP 203.0.113.200
   port 443  tcp
      name _203.0.113.200_HTTPS_443
      source-nat pool MISNATPOOL
      service-group MISGROUP
```

## B. CLI COMMANDS FOR SAMPLE ADVANCED CONFIGURATION

```
hostname advmis
ip nat pool MISNATPOOL 192.0.2.100 192.0.2.100 netmask /24
health monitor MISHC
 method https
 ip anomaly-drop frag
 ip anomaly-drop ip-option
 ip anomaly-drop tcp-no-flag
 ip anomaly-drop tcp-syn-fin
 ip anomaly-drop tcp-syn-frag
 ip anomaly-drop ping-of-death
 ip anomaly-drop land-attack
slb server MIS1 192.0.2.4
   port 443  tcp
slb server MIS2 192.0.2.5
   port 443  tcp
```

```
slb service-group MISGROUP tcp

    health-check MISHC

    member MIS1:443

    member MIS2:443

slb template connection-reuse MISconnectionreuse

slb template tcp-proxy test

   receive-buffer 512000109

slb template client-ssl "Client SSL-MIS"

   cert MISCERT

   key MISCERT pass-phrase encrypted
XL6aAvKM5xQ8EIy41dsA5zwQjLjV2wDnPBCMuNXbAOc8EIy41dsA5zwQjLjV2wDn

slb virtual-server MISVIP 203.0.113.200

   port 443  https

      name _203.0.113.200_HTTPS_443

      source-nat pool MISNATPOOL

      service-group MISGROUP

      template client-ssl "Client SSL-MIS"

      template connection-reuse MISconnectionreuse
```