SSL Orchestrator

Reference Guide

Version 14.0.0-4.0

Table of Contents

Document Overview

This document is a reference resource to assist in understanding SSL Orchestrator v4.0. It should be used in combination with standard BIG-IP TMSH and TMOS reference guides. This is not intended to describe how to setup SSL Orchestrator.

This guide is also not intended to cover how the components work, for more information on how the solution works and should be deployed, see the SSL Orchestrator v4.0 Architecture Guide.

Prior to architecting or implementing any SSL Orchestrator solutiom, you should be familiar with the contents of the SSL Orchestrator 4.0 Architecture Guide.

SSL Orchestrator Object Reference

This section covers the objects that are specific to SSL Orchestrator. These are iAppLX template objects.

Common Fields

Fields that are common to some or all of the below objects.

Name ***Required**	Each object has a name field. The name fields all start with "sslo" and contain a letter or string indicating what type of field it is. (detailed in each object below). Names are required and must be between x any y characters long and must only contain characters or numbers. Default: "sslo??_"
Description	Each object has a description field that can be used to provide additional information about the purpose of that object. These can often be seen in the object lists.
Strict Update	Default: True The strict update field is a Boolean (yes/no) field. Leaving it enabled will lock any objects that this object creates. Disabling it will allow those objects to be edited or deleted. If any managed objects are changed, they will automatically be set back to the state that SSL Orchestrator expects them to be on the next configuration edit. For more information, see the SSL Orchestrator v4.0 Architecture Guide.
IP Family	Default: IPv4 When present, this will allow entering IPv4, IPv6, or both IPv4 and IPv6 addresses in this form.

Common Fields for Service Objects:

The following fields that are in most of the service objects (each object will note the field and refer to this section for details.)

Port Remap

**Does not show for ICAP and Explicit HTTP Services*

Allows traffic being sent to the device to have the port number mapped to a specified port. The port will be reset on return from that device.

Options:

<checkbox>	*Default unchecked If Checked, will remap the port

Note:
Certain security devices will only work with specific ports, and in some cases security devices will not accept unencrypted traffic on port 443, this allows working around these limitations.

Remap Port To

**Only shows when Port Remap is selected*

Defines the port that traffic will be re-mapped to

**Defaults to port 80*

Service Down Action

Allows admin to define what should happen if all of the devices defined in the service are down.

Options:

Ignore	*Default
Reset	
Drop	

iRules

**Only shown for L2, L3, and HTTP Inline service.*

Allows attaching an iRule to the virtual server created for this.

Options:

iRule Selector	Can select multiple iRules.

Notes:
When developing iRules, keep in mind that the virtual server is not configured with client-side TCP profile, so rules requiring client TCP will not compile.

> **!** KNOWN ISSUE: in 14.0.0, the services will not allow you to add an iRules to the service without a workaround (See the SSLO v4.0 Architecture Guide use cases section.).

Object description table

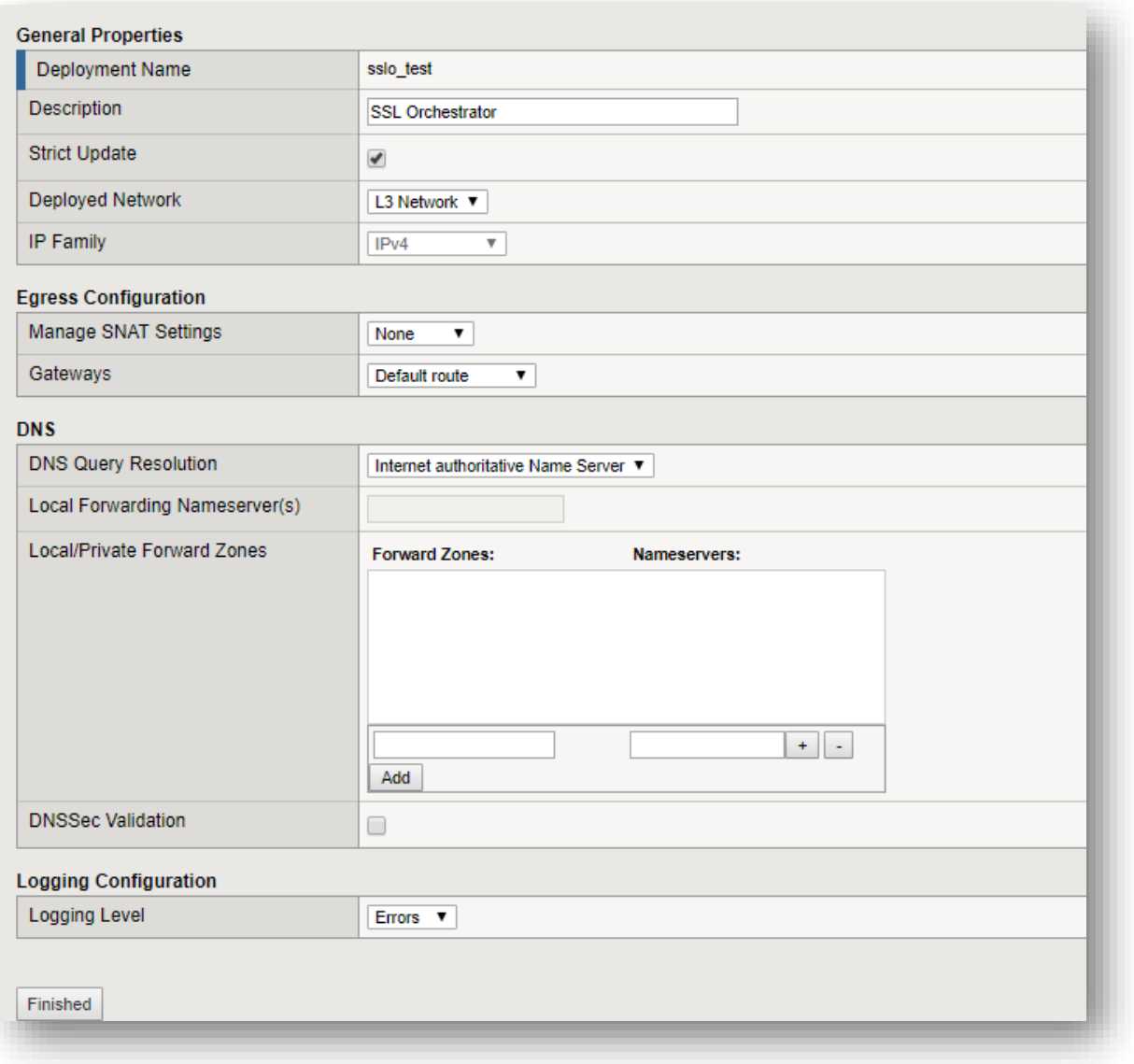
Each object below has an initial description table that provides information about how that object relates to other objects and is deployed.

SSLO Template Object	Explains which template object this object uses. This is helpful when trying to clear a specific type of object, or when troubleshooting a templating problem.
UI Location	Where in the interface this object is configured / created?
Linked from Objects	What objects will use this object once created?
Links to Objects	What objects this object uses? (note these may need to be created prior to creating this object).
Auto-created	Is this object automatically created by another?
Naming Prefix	What is the prefix added to the name when saving BIG-IP objects created by this object?

Base Configuration / Application Object

This is the base configuration for the SSL Orchestrator. This configures the basic options for getting traffic in and out of the system.

SSLO Template Object	Deployment
UI Location	GUI – SSL Orchestrator -> Deployment -> Deployment Settings
Linked from Objects	None
Links to Objects	None
Auto-created	No
Naming Prefix	sslo_



Fields

General Properties	
Deployment Name	This is the overall deployment name for the SSLO system.
Description	*See common fields
Strict Update	*See common fields

Deployed Network This field controls how SSLO is implemented in the network.

Options:

L2 Network	
L3 Network	*Default

Notes:
See the SSL Orchestrator v4.0 Architecture Guide for more information about the differences between L2 and L3 networks.

IP Family Handles selecting the IP family settings for the overall SSL Orchestrator.

Options:

IPv4	*Default
IPv6	
IPv4 & IPv6	

Notes:
Individual services can have different settings from the base settings. The system will try pass traffic using the same IP version through all services, however, if the service does not support the IP version that was received, it will convert it to the other version for that specific service, then back once it returns.

> **!** This field will be disabled once any rules have been created. To modify it you would have to remove any existing rules.

Egress Configuration

Manage SNAT Settings

Not available for Layer 2 Network Configurations

How SSLO should set the source address for traffic leaving SSLO to the destination.

Options:

None	*Default Use the original source address. Note in this case, the next hop device will need to correctly route any traffic back through the SSLO.
AutoMap	Traffic will be SNAT'ed using the self IP(s) defined on the outbound interfaces.
SNAT	Traffic will be sent to the destination. Note that you will have to define the SNAT addresses to use for this option.

Notes:
You should not use Automap in most production systems as there are only a limited number of available ports that can be used on Self IPs (See automap information in the BIG-IP documentation)

> **!** The SNAT setting will impact traffic going both inbound and outbound. This can cause problems for inbound traffic. (See the SSLO v4.0 Architecture Guide use cases section)

IPv(X) SNAT Addresses

**Shown when "SNAT" set in above field.*

Allows you to define a list of IPv4 or IPv6 addresses to use for SNAT.

Gateways

Not available for Layer 2 Network Configurations

Defines how traffic leaving SSLO will find its next hop router.

Options:

Default Route	*Default Uses normal BIG-IP default gateway to choose the interface to the next hop router.
Specific gateways	Allows specifying the addresses and ratios for the next hop router(s).

Notes:
Using "specific gateways" allows defining multiple paths for outbound traffic and creates a pool and gateway monitor.

IPvX Outbound Gateways

**Only shows when "Specific gateways" is selected in the "Gateways" field*

Allows defining the next hop gateways used for outbound traffic

Options List:

Ratio	Used for load balancing outbound gateways
Specific gateways	Defines the address for the next hop router.

Notes:
See the BIG-IP documentation on ratio load balancing for more information on how the ratio us used.

DNS

DNS Query Resolution

This solution uses DNS extensively. You can either permit the system to send DNS queries directly out to the Internet or specify one or more local forwarding nameservers to process all DNS queries from SSL Intercept.

Options:

Internet Authoritative Name Server	Allows defining multiple nameservers for different forwarding zones.
Local Forwarding Name Server	*Default Will use the same nameserver(s) for all lookups,

Notes:
Setting up multiple Authoritative name servers can be faster, but also requires TCP and UDP port 53 access to those servers.

Local Forwarding Nameserver(s)

**Shows when "Local Forwarding Name Server" is selected above.*

Allows defining the local nameserver(s) to use.

Local/Private Forward Zones

**Shows when "Internet Authoritative Name Server" is selected above.*

Allows defining multiple local and private forwarding zones and name servers.

Options List:

Forward Zone	A domain name zone that uses this nameserver.
Nameservers	A list of name servers to use for this zone.

Note:
When using forward zones, make sure to have a default zone (with an empty Forward Zone field) in the list for fallback.

DNSSec Validation

Will use DNSSec to validate all DNS addresses.

Checkbox:

Enabled	
Disabled	*Default

Note:
To use this option you will have to have DNSSec configured and active or traffic will fail silently.

Logging Configuration

Logging Level

Sets (or resets) the logging level for the SSLO specific functions.

Options:

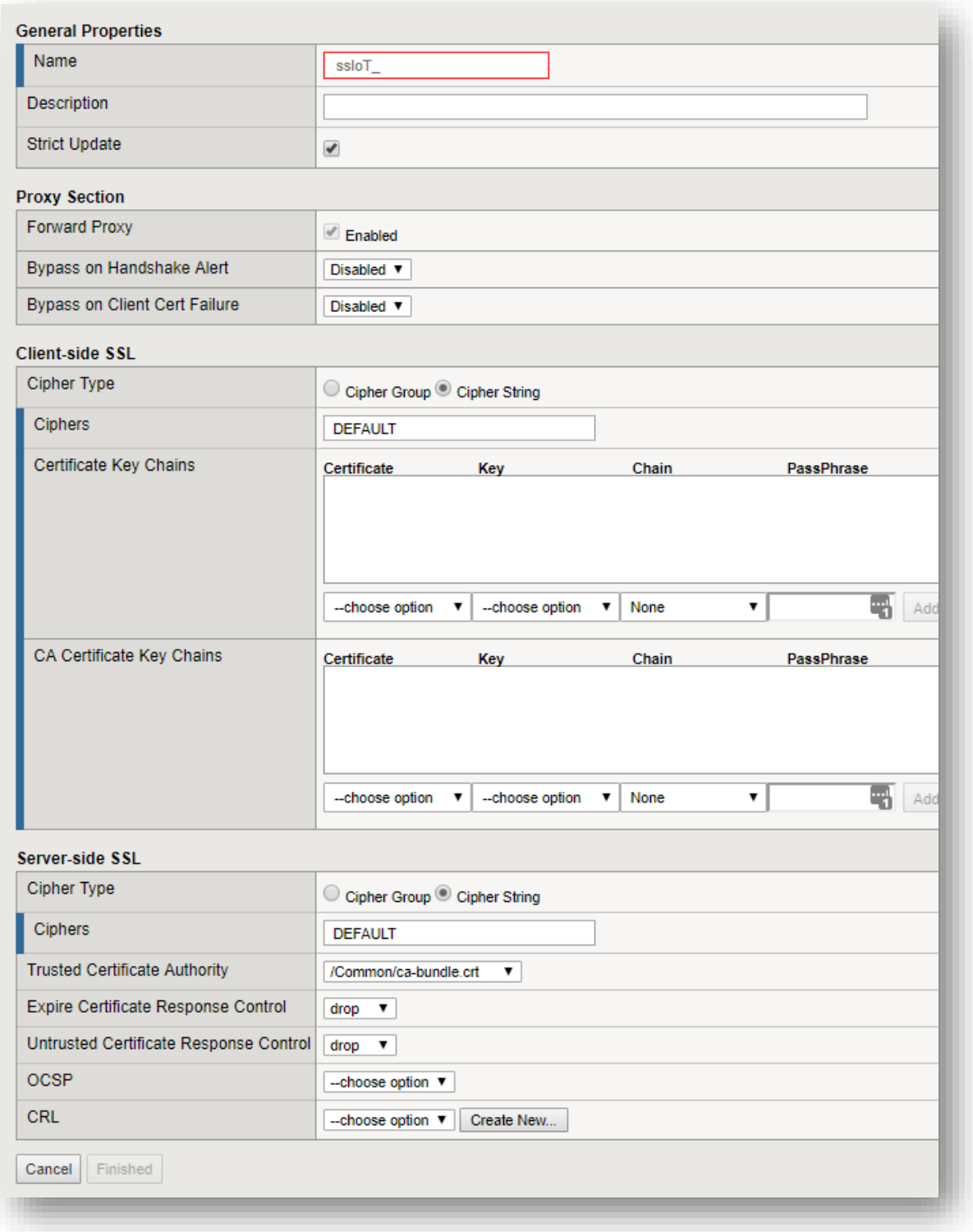
Errors	Sets all SSLO logging to ERROR level
Normal	*Default Sets all SSLO logging to NOTICE level
Debug	Sets all SSLO logging to DEBUG level

Notes:
If any SSLO logging option is changed in the SSL Orchestrator / Logs / Settings screen, changing this option will overwrite those changes.

SSL Setting Group Object

This object groups of SSL/TLS setting, and allows a single group of defined settings to be used in multiple other objects.

SSLO Template Object	SSL Template
UI Location	SSL Orchestrator / SSL Management / SSL Settings
Linked from Objects	**From Object Type** / **From Field Name** Inbound and outbound rules / SSL Settings
Links to Objects *(Note objects that must be created BEFORE creating this object if needed).*	**My Field Name** / **To Object Type** / **Can Create** Ciphers / Cipher Group / No Certificate / Certificate / No Key / Key / No Chain / Certificate / No Trusted Certificate Authority / Certificate / No OCSP / OCSP / No CRL / CRL / Yes
Manages Objects	Client and Server SSL Profiles
Auto-created	Yes – By all objects linked from.
Naming Pattern	ssloT_


General Properties
Name
ssloT_
Description
Strict Update
Proxy Section
Forward Proxy
Enabled
Bypass on Handshake Alert
Disabled
Bypass on Client Cert Failure
Disabled
Client-side SSL
Cipher Type
Cipher Group
Cipher String
Ciphers
DEFAULT
Certificate Key Chains
Certificate
Key
Chain
PassPhrase
--choose option
--choose option
None
CA Certificate Key Chains
Certificate
Key
Chain
PassPhrase
--choose option
--choose option
None
Server-side SSL
Cipher Type
Cipher Group
Cipher String
Ciphers
DEFAULT
Trusted Certificate Authority
/Common/ca-bundle.crt
Expire Certificate Response Control
drop
Untrusted Certificate Response Control
drop
OCSP
--choose option
CRL
--choose option
Create New...
Cancel
Finished

Fields

Proxy Section	
Forward Proxy	Specifies if this settings group is for a Forward Proxy **Checkbox Options:** Enabled – *Default Disabled **Notes:** This controls the forward / reverse proxy settings in the SSL Profile(s) created, as well as which fields are visible further down in this object.
Bypass on handshake alert **Only shown for forward proxy configurations.*	If an SSL Handshake error is received during the server-side handshake, should we bypass SSL Processing for all services. **Options:** Enabled Disabled – *Default **Notes:** On receiving a handshake_failure, protocol_version, or unsupported_extension alert message during the server-side SSL handshake. When this occurs, SSL traffic bypasses the BIG-IP system untouched, without decryption. This should be used with caution since it could be used by a knowledgeable attacker to bypass security scanning systems.
Bypass on Client Cert Failure **Only shown for forward proxy configurations.*	If a certificate error occurs during the server-side handshake, should we bypass SSL Processing for all services. **Options:** Enabled Disabled – *Default **Note:** This should be used with caution as it can introduce potential security holes in your system.
Client-Side SSL	

Cipher Type	Should we use a simple cipher string or a Cipher Group to select which ciphers to use for this? **Options:** <table><tr><td>Cipher Group</td><td></td></tr><tr><td>Cipher String</td><td>*Default</td></tr></table> **Note:** Cipher Groups can provide more flexibility in defining and maintaining ciphers. See the BIG-IP documentation on the configuration and use of Cipher Groups.
Ciphers	Allows selecting the ciphers used for client connections. This is either a string field to enter the cipher string, or a dropdown showing available cipher groups depending on the above setting. *Default (if String): “DEFAULT” **Notes:** Since SSLO does not currently support TLS 1.3, 1.3 ciphers should not be included in the Cipher Group For the list of ciphers used in the DEFAULT cipher set, see https://support.f5.com/csp/article/K54125331.

Certificate Key Chains

When setup as a forward proxy:
This is the example certificate that is used as a base when forging certificates. Normally this would not need to be changed, but if custom flags or settings are needed, this can be updated to reflect that, and each forged certificate will mirror this.

When setup as a reverse proxy:
This is the certificate used to send to the clients on connection. It should be one that the clients will trust, so if it is a custom certificate, then the root must be distributed to the clients, or it can be a commercial certificate based on one of the trusted certificate providers.

Options List:

Certificate	
Key	
Chain	
Passphrase	

Notes:
This allows multiple certificates; this ability is intended to add a second certificate for the purposes of supporting multiple encryption types (ECDSA and RSA). It is not intended to support multiple host certificates for the purposes of supporting SNI.
Normally the default certificate and key are selected for this field.

CA Certificate Key Chains

Only shows for Forward Proxy configurations.

This is the Certificate Authority certificate that is used to sign all forged certificates sent to the clients for transparent mode. This certificate must be distributed to all of the clients, otherwise they will get an "untrusted certificate" error.

Options List:

Certificate	
Key	
Chain	
Passphrase	

Notes:
This allows multiple certificates; however you can actually only add two certificates, with one of them for ECDSA encryption.
This certificate must be RSA based.
This certificate must also have at least the following flags set:

- Digital Signature key usage (digitalSignature)
- Certificate Signing key usage (keyCertSign)
- CA Basic Constraint set to TRUE

Server-Side SSL

<table>
<tr><td>Cipher Type</td><td>Same as Client-Side SSL Section</td></tr>
<tr><td>Ciphers</td><td>Same as Client-Side SSL Section</td></tr>
<tr><td>Trusted Certificate Authority</td><td>This allows setting the certificate bundle to be used for validating servers.

Options:<table><tr><td><list of certificates></td><td>*Default is the system CA-Bundle setup on initial setup.</td></tr></table></td></tr>
<tr><td>Expire Certificate Response Control</td><td>This allows configuring what should happen if an expired server certificate is received.

Options:<table><tr><td>Drop</td><td>*Default</td></tr><tr><td>Ignore</td><td></td></tr></table>Notes:
This should be used with caution, allowing expired certificates can have serious security implications.</td></tr>
<tr><td>Untrusted certificate response control</td><td>Allows configuring what should happen if a certificate is received that is not signed by a CA from the Trusted Certificate Authority list.

Options:<table><tr><td>Drop</td><td>*Default</td></tr><tr><td>Ignore</td><td></td></tr></table>Notes:
This should be used with caution, allowing expired certificates can have serious security implications.</td></tr>
<tr><td>OCSP</td><td>This allows configuring OCSP for validating server certificates.

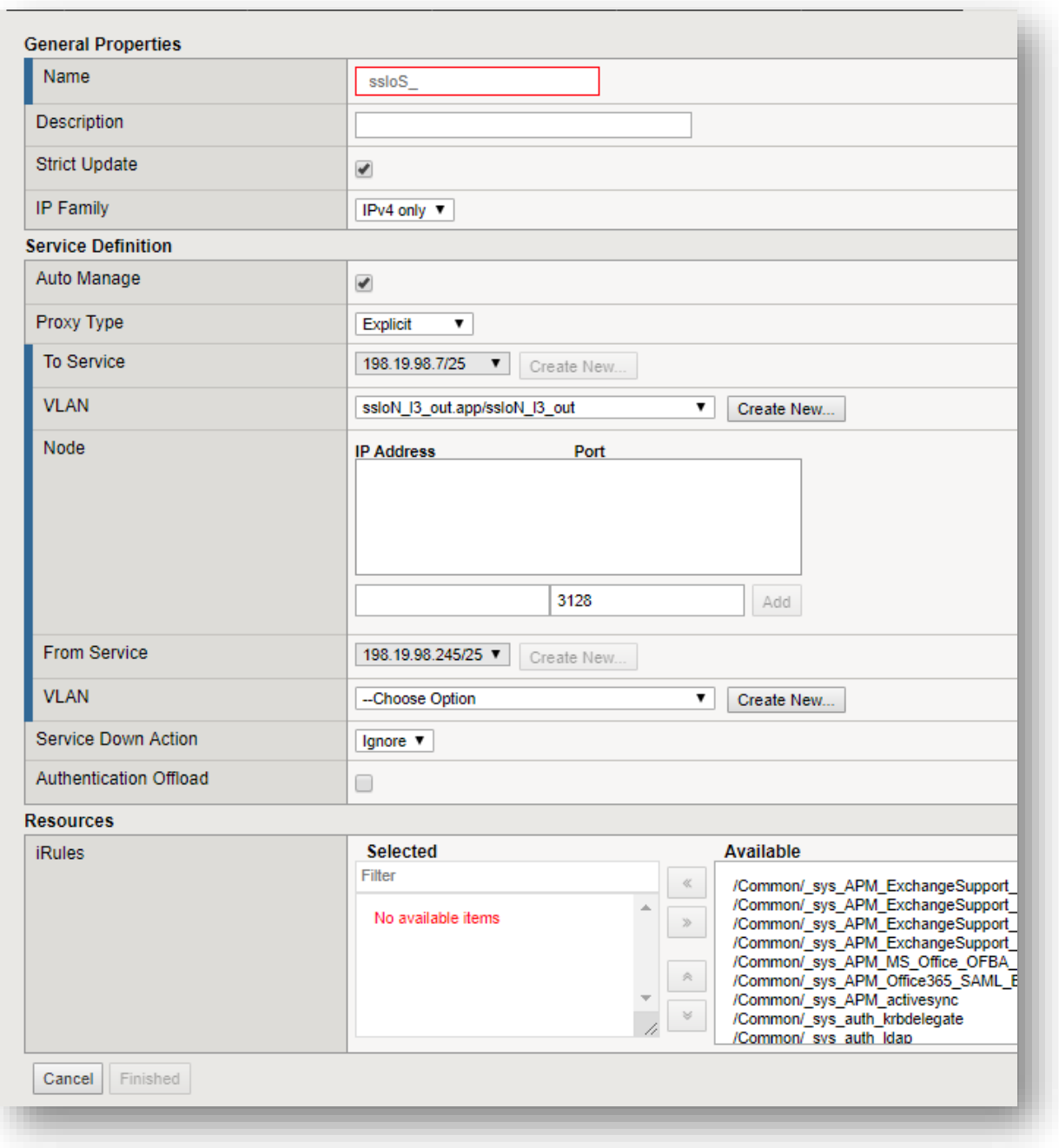
Options:<table><tr><td>-Chose Option</td><td>*Default</td></tr><tr><td><list of OCSP objects></td><td></td></tr></table>Notes:
OCSP objects must be already configured before selecting them.
See the LTM configuration guide for OCSP configuration</td></tr>
</table>

CRL	This allows configuring the BIG-IP to automatically retrieve and maintain CRLs for validating server certificates. **Options:** <table><tr><td>-Chose Option</td><td>*Default</td></tr><tr><td><list of CRL objects></td><td></td></tr></table> **Notes:** You have the ability to create CRL objects from here if needed. See the LTM configuration guide for CRL configuration

HTTP Service Objects

These objects are used to configure the HTTP Explicit and Transparent services.

SSLO Template Object	Service Templates
UI Location	SSL Orchestrator / Services / HTTP Services
Linked from Objects	<table><tr><th>From Object Type</th><th>From Field Name</th></tr><tr><td>Per Request Policy Chain</td><td>Services</td></tr></table>
Links to Objects	<table><tr><th>My Field Name</th><th>To Object Type</th><th>Can Create</th></tr><tr><td>VLAN</td><td>SSLO Network Object</td><td>Yes</td></tr><tr><td>To/From Service</td><td>SSLO Network Object</td><td>Yes</td></tr><tr><td>iRules</td><td>iRules</td><td>No</td></tr></table>
Manages Objects	Virtual Servers, Pools, Monitors, Profiles
Auto-created	No
Naming Pattern	ssloS_



Fields

General Properties	
Name	*See common fields.
Description	*See common fields.
Strict Update	*See common fields.
IP Family	*See common fields.

Service Definition	
Auto Manage	Defines if this service should use address ranges pre-defined by SSLO. **Checkbox:** Enabled *Default Disabled **Notes:** If disabled, admins will need to define an address range and VLAN for this service. It is strongly recommended to leave this enabled and use the range as defined to minimize address range conflicts. See the SSLO v4.0 Architecture Guide security cases section
Proxy Type	Defines if the security devices operate as explicit or transparent. **Options:** Explicit *Default Transparent **Notes:** You cannot combine both explicit and transparent devices in the same service.
To/From Service **This is pre-selected, and disabled when "Auto Manage" is selected.*	When auto manage is disabled, this allows admins to configure the address range and VLAN used for the service. ! When auto manage is enabled, this is automatically created and is greyed out. The "To Service" field is used to define addresses and VLANs traffic going to the security device from the inside, and the "From service" field is used to define addresses and VLANs used for traffic going from the service to the BIG-IP. **Options:** <list of SSLO Network objects> The admin can create a new network object if the one they want is not available.

VLAN

**This is pre-selected, and disabled based on the VLAN in the network object when "Auto Manage" is disabled.*

When auto manage is enabled, this allows admins to configure the VLAN that should be used for the service traffic.

> **!** When auto manage is disabled, this is automatically filled in based on the VLAN defined in the network object in the "To/From Service" above and greyed out..

The "VLAN" field is used to define the VLAN for traffic going to or from the service device based on which address field it is near.

Options:

<list of defined VLANS>	The admin can create a new network object if the one they want is not available.

Node

Defines an address for each of the service devices in the service. Each HTTP service can have multiple service devices.

Options List:

IP Address	
Port	*Only shows for Explicit Services *Defaults to port 3128

Notes:
The address must be within the network range as defined by the To Service field, and it must be at least 2 addresses away from both the "to" and "from" service addresses.

Service Down Action

See common fields.

Authentication Offload

Allows the BIG-IP to handle authentication for clients, and to pass that authentication to the service devices.

Checkbox:

Enabled	
Disabled	*Default

Notes:
This option will not have any impact if APM is not licensed.
If APM is licensed and configured to authenticate users, this option will send the user ID to the HTTP proxy via the "X-Authenticated-User" header.
For an example of how to configure APM for authentication, See the SSLO v4.0 Architecture Guide use cases section)

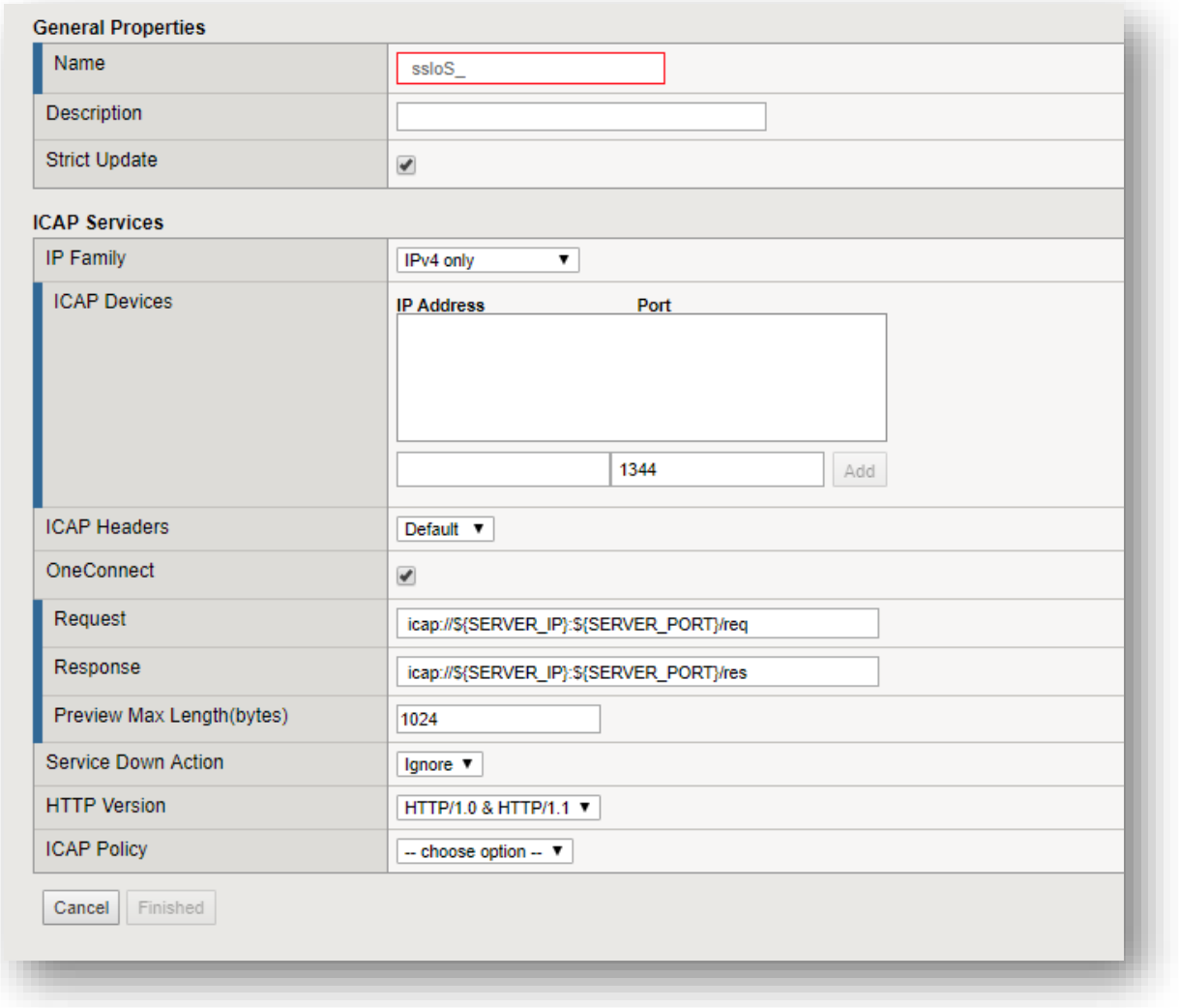
Resources

iRules	*See common fields

ICAP Service Objects

This object sets up an ICAP service.

SSLO Template Object	Services Template
UI Location	SSL Orchestrator / Services / HTTP Services
Linked from Objects	**From Object Type** / **From Field Name** Per Request Policy Chain / Services
Links to Objects	**My Field Name** / **To Object Type** / **Can Create** ICAP Policy / LTM CPM Policy / No
Manages Objects	Virtual Servers, Pools, Monitors, Profiles
Auto-created	No
Naming Pattern	ssloS_



Fields

General Properties	
Name	*See Common Fields
Description	*See Common Fields
Strict Update	*See Common Fields
ICAP Services	
IP Family	*See Common Fields

ICAP Devices

This is a list of the ICAP devices that we should send traffic to. You can configure multiple devices.

Options List:

IP Address	
Port	*Defaults to port 1344

Notes:
These servers will be load balanced using a simple round robin method.
The monitor for these uses a TCP monitor to the defined port.

ICAP Headers

This allows customizing the ICAP headers that are sent. Since some ICAP servers use these headers to differentiate the source of the traffic, this allows you to control them.

Options:

Default	*Default
Custom	

Notes:
See your ICAP systems documentation for the correct usage of these fields.

Host

Allows entering a custom host value.

Referrer

Allows entering a custom referrer value.

User Agent

Allows entering a custom user agent value.

From

Allows entering a custom from value.

One Connect

Should connections to the ICAP servers use OneConnect

Checkbox:

Enabled	*Default
Disabled	

Notes:
Some ICAP servers do not support multiple transactions per TCP connection, if this is the case this option should be disabled.

Request

What is the URL to send the ICAP request to for HTTP requests?

*Default: "`icap://${SERVER_IP}:${SERVER_PORT}/req`"

Notes:
The variables ${SERVER_IP} and ${SERVER_PORT} will be replaced with the server IP and port from the list of ICAP device.
See the ICAP server documentation for the correct value for this field.

Response

What is the URL to send the ICAP request to for HTTP responses?

*Default: "`icap://${SERVER_IP}:${SERVER_PORT}/res`"

Notes:
The variables ${SERVER_IP} and ${SERVER_PORT} will be replaced with the server IP and port from the above list.
See the ICAP server configuration for the correct value for this field.

Preview Max Length

This sets the number of bytes of the HTTP content that is sent to the ICAP server with the response. Setting this to 0 will send the entire content.

*Default: 1024

Notes:
Max for this is 51200 (or 50KB).
Depending on the ICAP server, this can cause significant overhead on the ICAP server if it is set to larger settings.
Setting this to anything other than 0 will cause the entire HTTP response to be cached until the ICAP server responds, which can add additional memory overhead to the BIG-IP system.
While in normal operation this is not expected to cause issues, in busy networks with large packet sizes it could fill up TCP buffers.

> **!** If TCP buffers are overflowing due to this, you could consider filtering the traffic that is going to ICAP using the ICAP policy field.

Service Down Action

*See Common Fields

HTTP Version

This allows the system to not send HTTP/1.0 traffic to the ICAP server.
Options:

HTTP/1.0 & HTTP 1.1	*Default
HTTP 1.1 only	

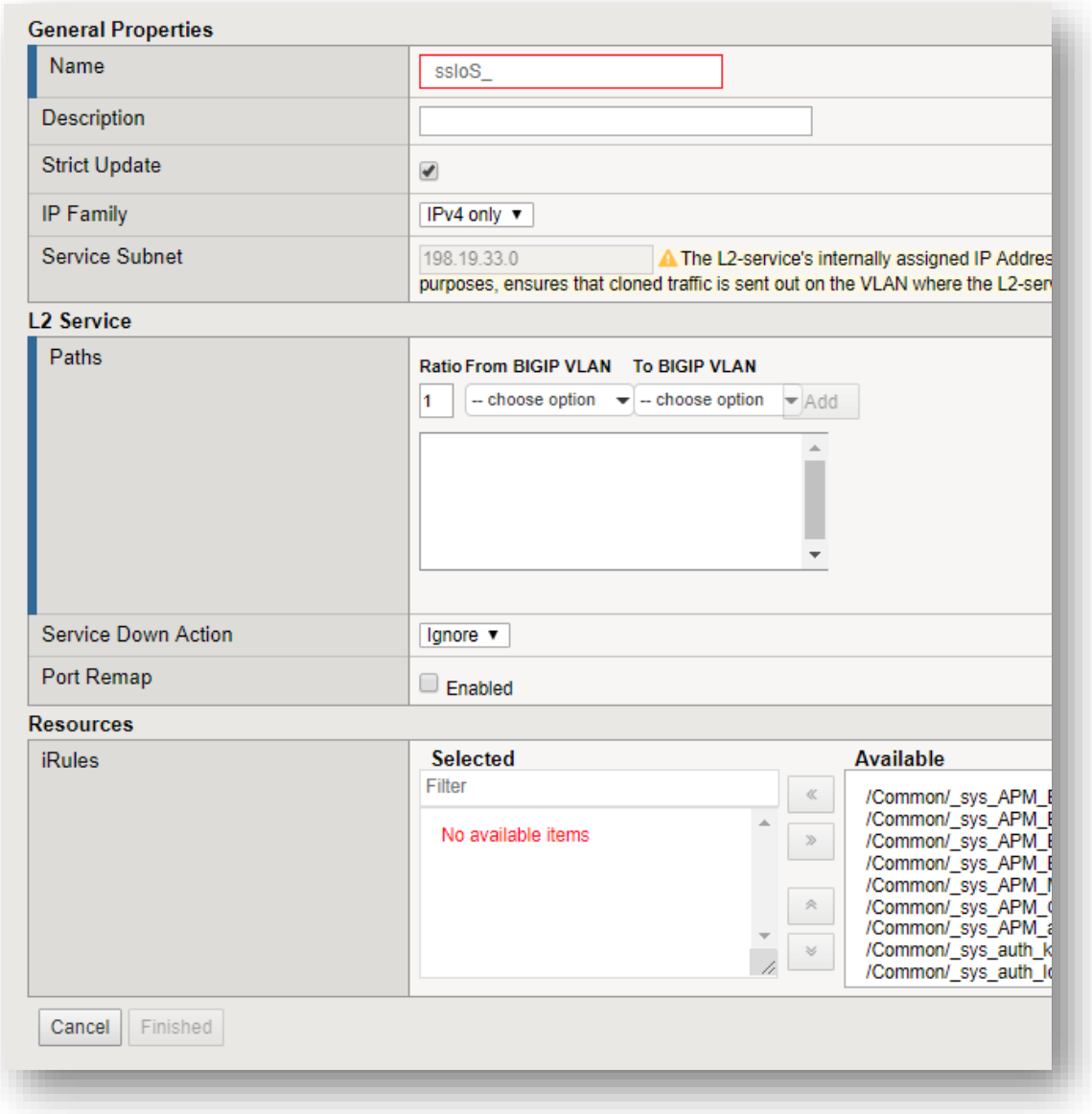
Notes:
Some ICAP servers cannot handle 1.0 traffic, this allows you to skip sending it to them.
If this is set to HTTP 1.1 Only and 1.0 traffic is received by the system it will simply bypass the ICAP service. It is not blocked or rejected. If you wish it to be blocked or rejected, add a rule to the VPE step to block it.

ICAP Policy	This allows better control over which traffic is sent to the ICAP server. **Options:** <list of LTM Policies> **Notes:** Since many ICAP servers cannot handle significant quantities of traffic, this allows the admin to define more complex rules to see when traffic should be passed to the service and when it should be bypassed.

L2 Service Objects

This creates a layer 2 inline service.

SSLO Template Object	Service Templates		
UI Location	SSL Orchestrator / Services / L2 Services		
Linked from Objects	**From Object Type**	**From Field Name**	
	Per Request Policy Chain	Services	
Links to Objects	**My Field Name**	**To Object Type**	**Can Create**
	To/From VLAN	SSLO Network Object	Yes
	iRules	iRules	No
Manages Objects	Virtual Servers, Pools, Monitors, Profiles		
Auto-created	No		
Naming Pattern	ssloS_		



Fields

General Properties	
Name	*See Common Fields
Description	*See Common Fields
Strict Update	*See Common Fields
IP Family	*See Common Fields

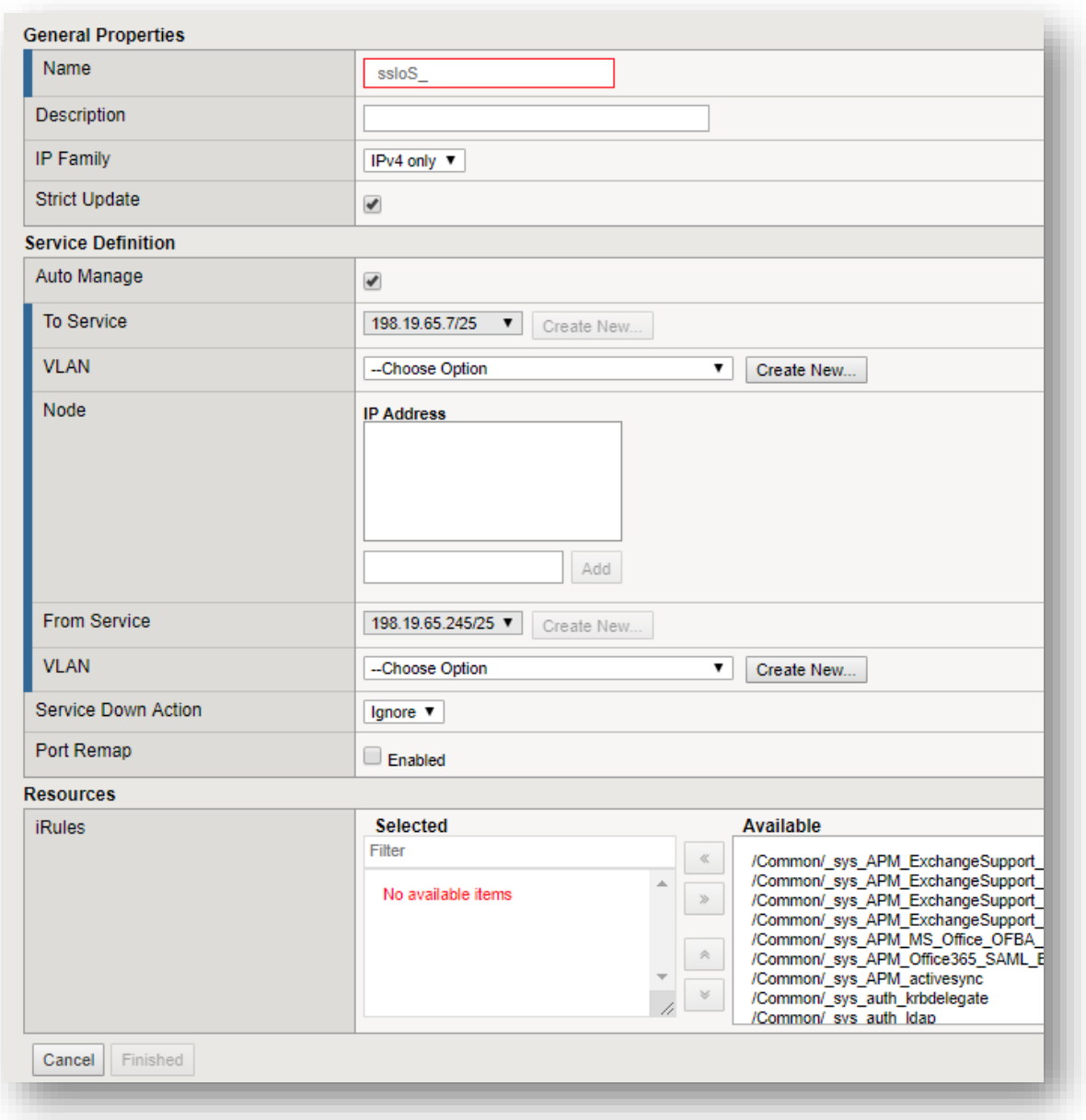
Service Subnet	Read-only field that shows the internally assigned address used for internal routing purposes. **Notes:** While you do not have to do anything with this information, you should insure that it is not included in any routable paths used elsewhere in the system as this would inhibit the internal routing process. ! This is not modifiable, so if the address is used in other locations, and you will either need to modify the routing so that it is not reachable from the SSL Orchestrator, or re-address the other network to de-conflict it with this one.
L2 Service	
Paths	Provides a list of paths (VLANS) for the system to follow to send traffic through the defined L2 devices. **Options List:** Ratio: *Default: 1 To/From BIG-IP VLAN: This is a selection of configured VLANS on the system, with the ability to add additional ones. **Notes:** See the SSL Orchestrator v4.0 Architecture Guide for information on how traffic flows through this type of device.
Service Down Action	*See Common Fields
Port Remap	*See Common Fields
Remap port to	*See Common Fields
Resources	
iRules	*See Common Fields

L3 Service Objects

This object creates a layer 3 service object

SSLO Template Object	Service Templates
UI Location	SSL Orchestrator / Services / L3 Services
Linked from Objects	**From Object Type**: Per Request Policy Chain **From Field Name**: Services

Links to Objects	**My Field Name**	**To Object Type**	**Can Create**
	VLAN	SSLO Network Object	Yes
	To/From Service	SSLO Network Object	Yes
	iRules	iRules	No
Manages Objects	Virtual Servers, Pools, Monitors, Profiles		
Auto-created	No		
Naming Pattern	ssloS_		



Fields

General Properties	
Name	*See Common Fields
Description	*See Common Fields
IP Family	*See Common Fields
Strict Update	*See Common Fields
Service Definition	
Auto Manage	Defines if this service should use address ranges pre-defined by SSLO. **Checkbox:** Enabled – *Default Disabled **Notes:** If disabled, admins will need to define an address range and VLAN for this service. It is strongly recommended to leave this enabled and use the range as defined to minimize address range conflicts. See SSL Orchestrator v4.0 Architecture Guide for more information.
To/From Service **This is pre-selected, and disabled when "Auto Manage" is selected.*	When auto manage is disabled, this allows admins to configure the address range and VLAN used for the service. ! When auto manage is enabled, this is automatically created and is greyed out. The "To Service" field is used to define addresses and VLANs traffic going to the security device from the inside, and the "From service" field is used to define addresses and VLANs used for traffic going from the service to the BIG-IP. **Options:** <list of SSLO Network objects> – The admin can create a new network object if the one they want is not available.

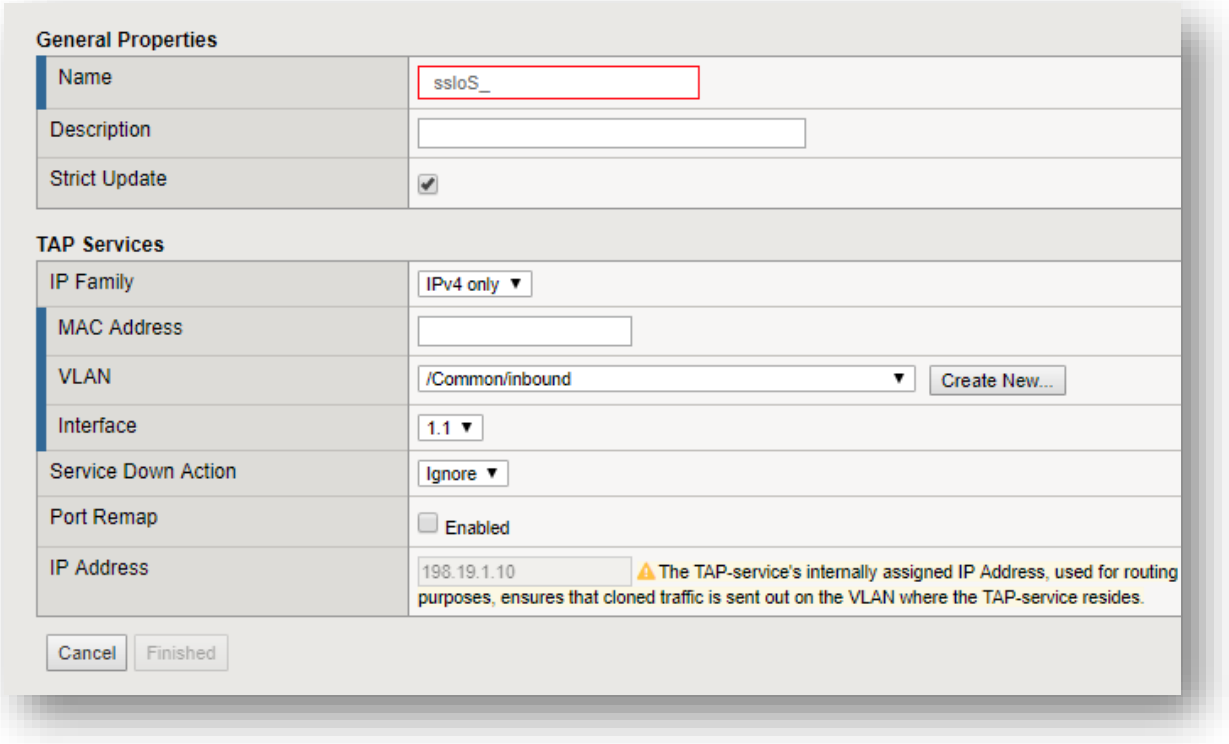
VLAN ***This is pre-selected, and disabled based on the VLAN in the network object when "Auto Manage" is disabled.***	When auto manage is enabled, this allows admins to configure the VLAN that should be used for the service traffic. **!** When auto manage is disabled, this is automatically filled in based on the VLAN defined in the network object in the "To/From Service" above and greyed out.. The "VLAN" field is used to define the VLAN for traffic going to or from the service device based on which address field it is near. **Options:** | <list of defined VLANS> | The admin can create a new network object if the one they want is not available. |
Node	Defines an address for each of the service devices in the service. Each L3 service can have multiple service devices. **Options List:** | IP Address | | **Notes:** The address must be within the network range as defined by the To Service field, and it must be at least 2 addresses away from both the to and from service addresses.
Service Down Action	*See common fields
Port Remap	*See common fields
Remap Port to	*See common fields
Resources	
iRules	*See Common Fields

TAP Service Objects

This allows you to create TAP Services, previously known as Read Only services.

SSLO Template Object	Service Templates
UI Location	SSL Orchestrator / Services / TAP Services
Linked from Objects	**From Object Type** | **From Field Name** Per Request Policy Chain | Services
Links to Objects	**My Field Name** | **To Object Type** | **Can Create** VLAN | SSLO Network Object | Yes iRules | iRules | No

Manages Objects	Virtual Servers, Pools, Monitors, Profiles
Auto-created	No
Naming Pattern	ssloS_



Fields

General Properties	
Name	*See Common Fields
Description	*See Common Fields
Strict Update	*See Common Fields
TAP Services	
IP Family	*See Common Fields
MAC Address	This is the MAC address of the TAP device that should receive the traffic. **Notes:** Traffic that is sent to TAP devices has the destination MAC overwritten with this MAC address.

VLAN	This is the VLAN that traffic is sent out on for the TAP device. **Options:** | <list of defined VLANS> | The admin can create a new network object if the one they want is not available. | **Notes:** While multiple TAP devices cannot be configured, you could have multiple devices on the target VLAN as long as they can monitor traffic and the network will forward the traffic to them.
Interface	Allows changing of the interface that traffic is sent on. **Option:** | <list if interfaces> | *Defaults to the interface that the VLAN is configure on in the above field. | **Notes:** This should not be changed unless you are sure that the TAP device is on a different interface from the default for the VLAN. This should be uncommon.
Service Down Action	*See common fields ! Since the TAP device is not monitored by default, this option does not do anything unless a monitor is added to the TAP device. (See the SSLO v4.0 Architecture Guide use cases section)
Port Remap	*See common fields
Remap Port to	*See common fields
Resources	
iRules	*See common fields

Network Objects

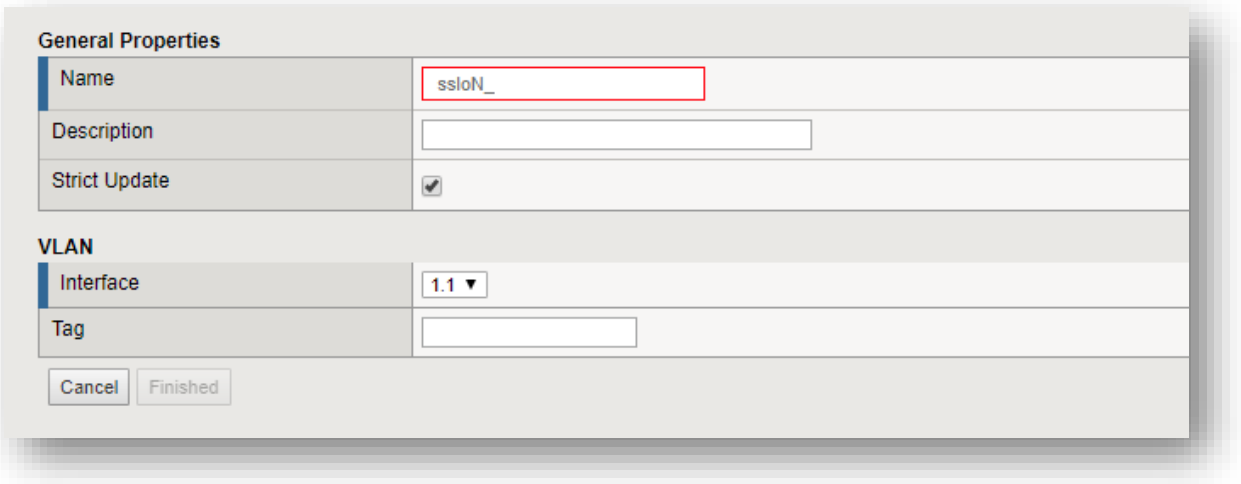
Network objects combine the Self-IP objects and the VLAN objects into a single SSLO template object. These are auto-created and depending on how they are created, you may see both the self IP information and VLAN information, or one or the other.

! Note that when creating these objects from other objects, the menu may only display the VLAN section, or the address section, depending on the needs of that object.

In general, you should not create or modify these directly, instead rely on the service template to do so.

SSLO Template Object	Network Template

UI Location	SSL Orchestrator / Network
Linked from Objects	**From Object Type** / **From Field Name** Service Objects / VLAN / Address
Links to Objects	**My Field Name** / **To Object Type** / **Can Create** VLAN / VLAN Objects / No Route Domain / Route Domain Objects. / No
Manages Objects	VLANs, Self IPs, Route Domains
Auto-created	Yes – By the service objects
Naming Pattern	ssloN_

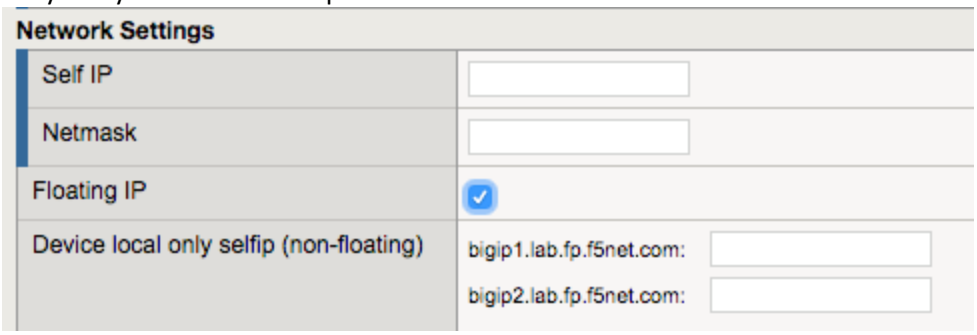


Fields

General Properties	
Name	*See Common Fields
Description	*See common Fields
Strict Update	*See common Fields
VLAN	
VLAN	Allows selection of the VLAN for the traffic. **Options:** <list of VLAN objects> – In layer 2 mode, only VWire VLANs will be shown
Network Setting	
Self IP	Allows setting the IP address for the traffic. **Notes:** This does not show up in network objects that were created simply to track VLAN usage.

Floating IP

Only on systems that are a part of a HA cluster.



This checkbox indicates that the above option is a Floating IP shared between all systems. (should be checked)

Device local only Self IP (non-floating)

Only on systems that are a part of a HA cluster.

This will have one box for each peer in the HA cluster. You enter the self IP for each device in these fields.

netmask

Allows setting the Network Mask for the traffic.

Notes:
You must use the full decimal (for IPv4) or hexadecimal (for IPv6) mask. Using the prefix length is not supported.
This does not show up in network objects that were created simply to track VLAN usage.

Route Domain

Allows setting the route domain for the traffic

Options:

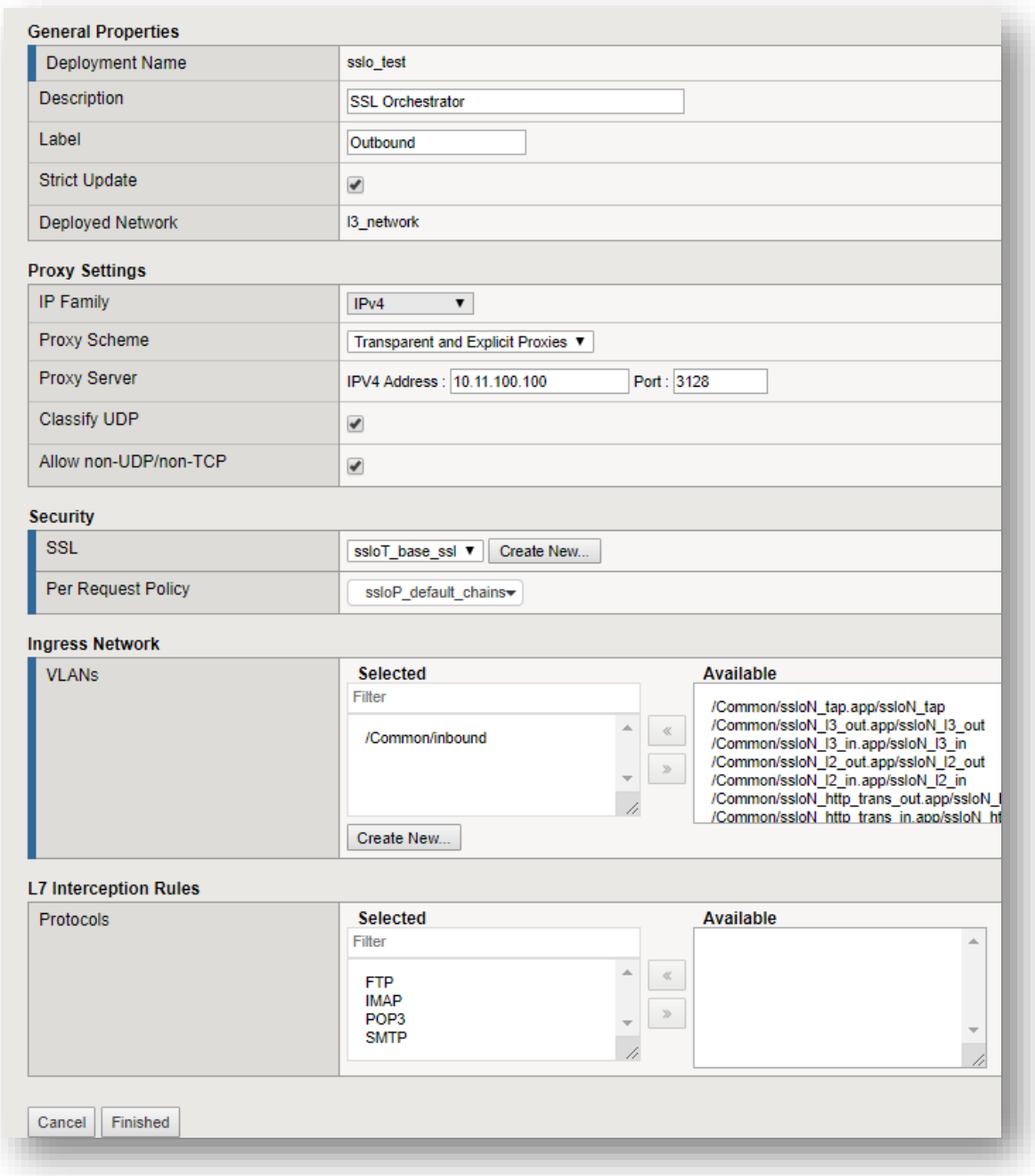
<list of route domain objects>	

Notes:
This does not show up in network objects that were created simply to track VLAN usage.

Default Outbound Rules

The default outbound rules object will create (and manage) the set of default outbound rules for the system. You can also create additional inbound and outbound rules, and you can edit the rules that are created by the default rules object. You should however be careful of editing the default rules since if you re-edit the default rules object, your previous edits will be overwritten.

SSLO Template Object	Policy Template
UI Location	SSL Orchestrator / Deployment / Interception Rules / Create/Edit Default Rules.
Linked from Objects	None
Links to Objects	**My Field Name** / **To Object Type** / **Can Create** SSL / SSLO SSL Setting Group / Yes Per Request Policy / SSLO Per Request Policy Chain / Yes VLANs / VLANs / Yes
Manages Objects	Access Policies / SSLO Rules / Per Request Policies
Auto-created	No
Naming Pattern	sslo_



Fields

General Properties	
Deployment Name	*Read only – Shows the SSLO deployment name
Description	*See common fields
Label	Allows a common label to be set for all default rules. This can help in sorting longer lists of rules.

Strict Update	*See Common Fields
Deployed Network	Read only - shows the current deployed network setting.
Proxy Settings	
IP Family	Shows the current setting from the deployment settings page.
Proxy Scheme	Defines which rules will be created. **Options:** Transparent Proxy – *Default Transparent and Explicit Proxies Explicit Proxy
Classify UDP ***Only shown when Explicit Proxy is selected above.**	Should we classify UDP traffic as well? **Checkbox:** Enabled – *Default Disabled **Notes:** If this is disabled, UDP traffic will be blocked from passing through the SSLO. In layer 2 network mode, this is Enabled and cannot be disabled.
Allow non-UDP / non-TCP **Only shown when transparent proxy is selected above*	Should non-UDP and non-TCP traffic be passed through the system. **Checkbox:** Enabled – *Default Disabled **Notes:** If disabled, traffic such as ICMP will be blocked from passing through the system. In layer 2 network mode, this is Enabled and cannot be disabled.
Proxy Server ***Only shown when Explicit Proxy is selected above.**	If Explicit Proxy is selected, what address and port should we listen on for outbound traffic? **Option Fields:** IPv4 Address Port
Security	

SSL

Allows you to select the specific SSL settings in use for the default rules created.

Options:

<list of SSL setting groups>	Can also create new groups

Notes:
See the SSL Setting Groups object for more information.

Per Request Policy

Allows selection of the services to be in the service chain for the default rules.

Options:

<list of per-request policy – Chain objects>	Can create new objects

Notes:
See the Per Request Policy (Service Chain) object for more information.

Ingress Network

VLAN

Allows selection of one or more VLANS to listen on for outbound traffic.

Options:

<list of configured VLANS>	Multi-select list, can also create new VLANS from here. In layer 2 mode, only VWire VLANs will be shown

L7 Interception Rules

Protocols

**Only shown when transparent proxy is selected above*

Allows selection of specific Application protocols that will have a custom rule created for each selected protocol to handle STARTTLS encryption.

Multi-select List:

FTP	Incudes FTP and FTPS
IMAP	Includes IMAP over STARTTLS
POP3	Includes POP3 over STARTTLS
SMTP	Includes SMTP over STARTTLS

Notes:
See the SSL Orchestrator v4.0 Architecture Guide for more information on STARTTLS and how SSLO handles it.

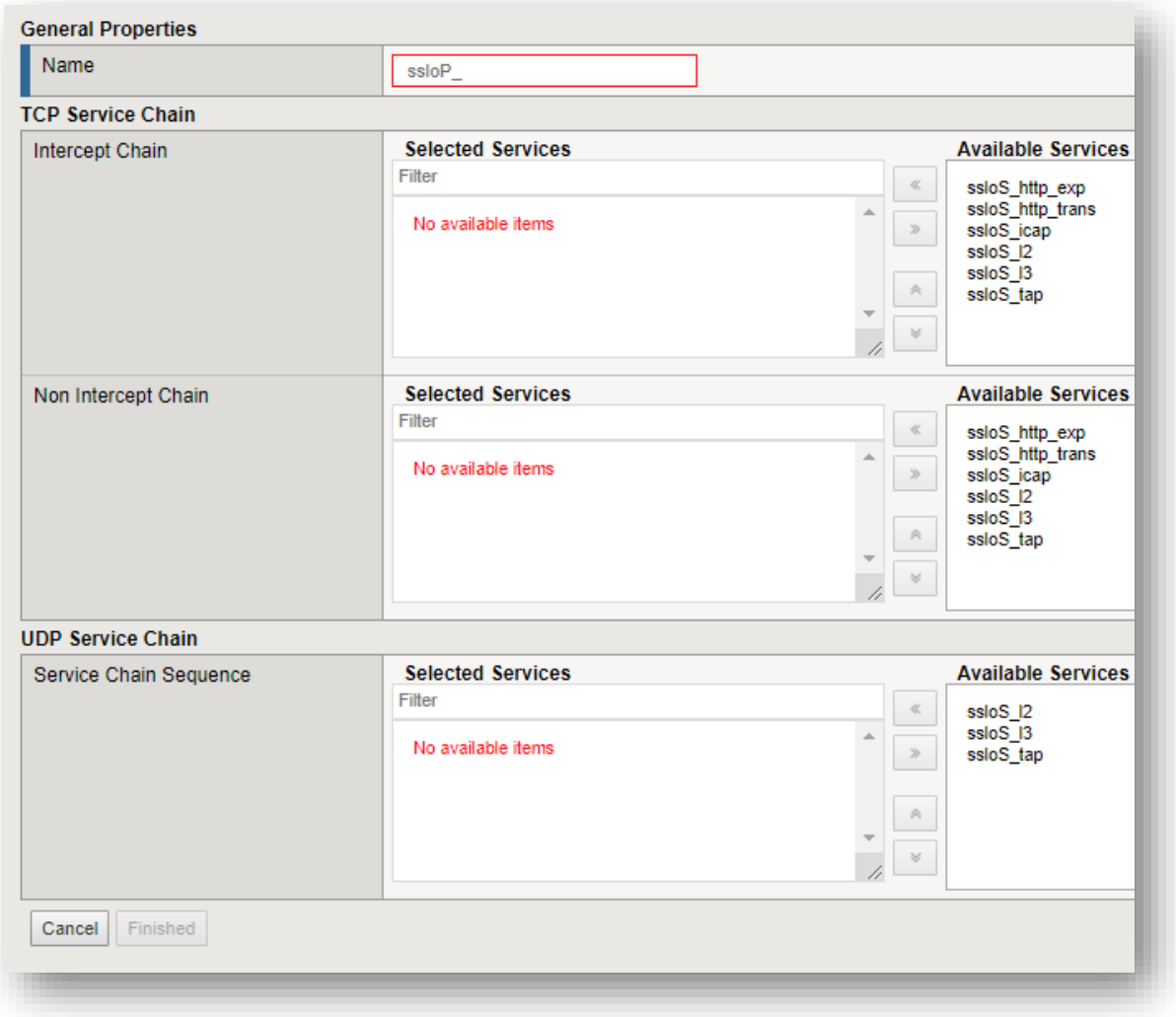
Per Request Policy (Chain Creation)

The SSLO per-request policy is officially a virtual policy editor policy, however when creating the rules, if you select “add” per-request policy, you are taken to a page that allows defining the chains. This then creates the VPE policy.

On this page, you can create up to three chains, one for UDP and two for TCP. You create them by selectin the service on the right side of the multi-select, then moving it to the left side. Once the service is on the left, it can be moved up and down to control the order in which the services are used.

This SSLO Per Request Policy will then create two APM per-request policies, one for TCP and one for UDP. That can be edited using the Visual Policy Editor.

SSLO Template Object	Policy Template
UI Location	SSL Orchestrator / Deployment / Policies / Per-Request Policy
Linked from Objects	**From Object Type** / **From Field Name** Access Policy / Per Request Policy
Links to Objects	None
Manages Objects	Access Policies
Auto-created	Yes – By Default Rules
Naming Pattern	ssloP_



Fields

TCP Service Chain	
Intercept Chain	This creates a chain called Service Chain Intercepted in the default TCP policy that is used by default.
Non-intercept chain	This creates a chain called Service Chain Not Intercepted in the default TCO policy that is not used by the default rules. See the SSLO v4.0 Architecture Guide use cases section for an example of how to use this chain.
UDP Service Chain	
Service Chain Sequence	This creates a service chain called Service Chain Intercepted in the default UDP policy

Inbound and Outbound Rules

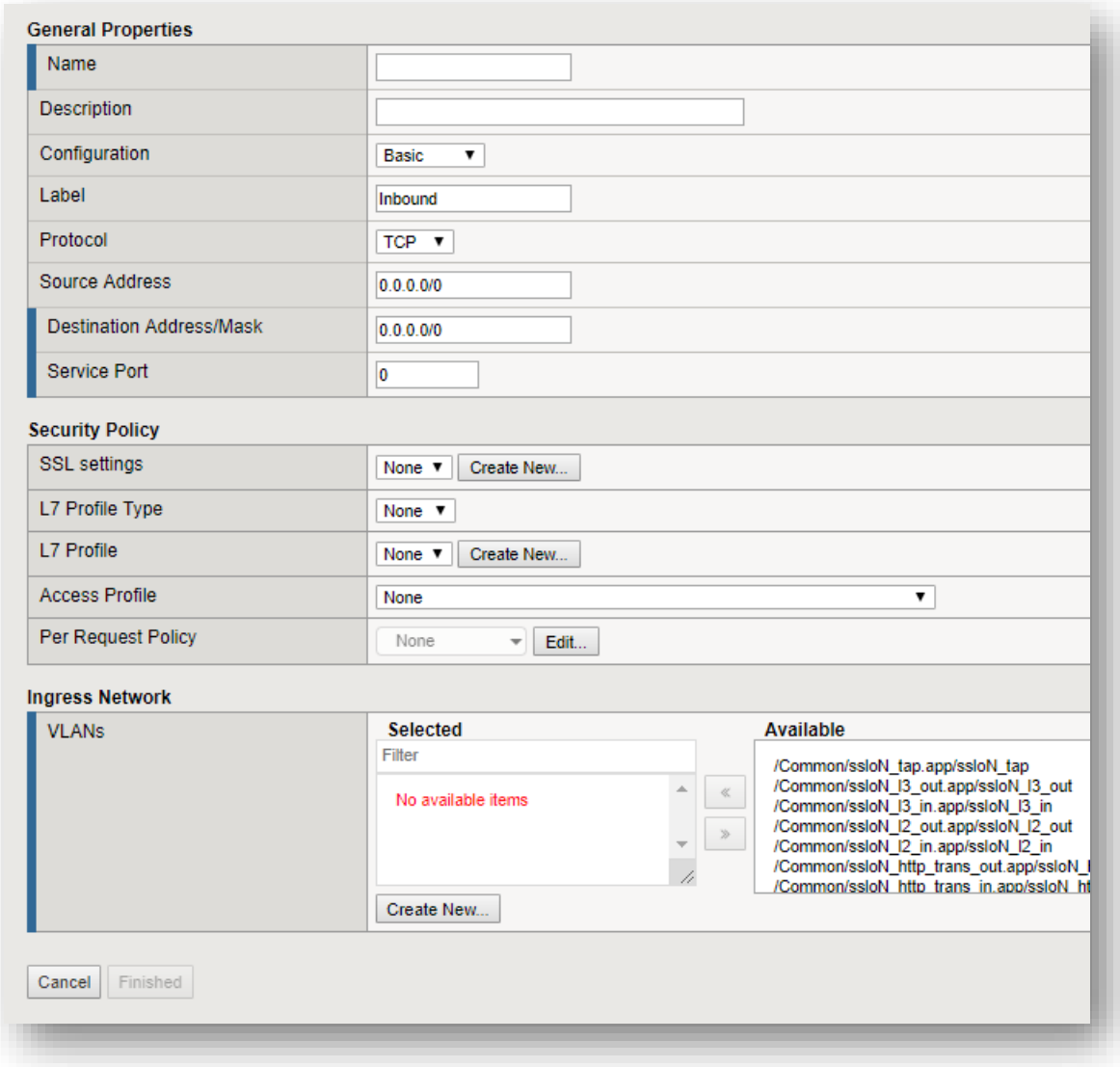
You can create additional inbound and outbound rules or edit existing ones. The rules define the listening virtual server as well as the policy that controls how the traffic is handled and forwarded.

Be aware that if you are editing default rules directly, any changes you make can be overwritten if the "edit default rules" button is used later.

Many of the fields here are the same as the default rules object, however the default rules object drives creating or editing multiple rules, whereas the inbound and outbound rules are editing a single rule.

> **!** By default, you can only have one outbound explicit proxy rule, and it must be created using the default rules option (See the SSLO v4.0 Architecture Guide use cases section.)

SSLO Template Object	Policy Template
UI Location	SSL Orchestrator / Deployment / Interception Rules
Linked from Objects	None
Links to Objects	**My Field Name** / **To Object Type** / **Can Create** SSL / SSLO SSL Setting Group / Yes Per Request Policy / SSLO Per Request Policy Chain / Yes VLANs / VLANs / Yes
Manages Objects	Access Policies / SSLO Rules / Per Request Policies
Auto-created	Yes (for default rules)
Naming Pattern	sslo_



Fields

General Properties	
Name	This is the name for the rule. Note it does **not** automatically start with "sslo_"
Description	*See common fields.

Configuration

Controls the display of advanced fields

Options:

Basic	*default
Advanced	Strongly suggest selecting “Advanced”

Notes:
You cannot change this field once the rule has been saved.

> ! We strongly suggest setting this to “Advanced” since this cannot be changed after the rule is created, which could require you to re-create this rule if you need an advanced option later.

Label

Provides for a label to be attached to the rule, this allows for better sorting of longer rule lists.

*Defaults to “inbound” or “outbound” depending on which rule type was selected.

Protocol

What protocol should the listener for this rule use?

Options:

TCP	*Default
UDP	
Other	

Notes:
“Other” would also include TCP or UDP if it is not otherwise defined in another rule.

Source Address

Source address and mask length

Notes:
Accept traffic originating from this address/mask.

Destination address / mask

**Required*

Destination address to listen on and mask.

Notes:
This is the address that the virtual server will listen on. You can use network addresses here as well. IF defining a single address, make sure to use a mask that indicates that (/32 for IPv4).

Service Port

Destination address to listen on and mask.

Notes: What TCP or UDP Port to listen to. You can enter “0” to listen to all ports.

VLAN

On Inbound rules this is in the "Ingress network" section.

Multi-selector for VLANs

Options:

<list of available VLANs>	Multi Select with ability to add VLAN. In layer 2 mode, only VWire VLANs will be shown

Security Policy

Client / Server TCP Profile

***Only shows when TCP is selected above**

In advanced fields

Which TCP profile should we use for client and server-side communications.

Options:

<list of TCP profiles>	Client Default: "/Common/f5-tcp-lan" Server Default: "/Common/f5-tcp-wan"

SSL Settings

*Only shows when TCP is selected above

*On outbound rules, only shows for transparent proxy

What SSL settings group should be used with this rule / listener.

Options:

<list of SSLO SSL Setting Groups>	Can also create a new one.

Notes:
See SSL Settings Groups for more information.

L7 Profile Type

*Only shows with TCP or UDP set above.

*Only shows for outbound rules.

Does this rule handle any specific STARTTLS protocol?

Options:

HTTP	*Default
FTP	
IMAP	
POP3	
SMTP	

Notes:
This only indicates if STARTTLS support is required. The protocols will be supported in non STARTTLS modes without this option.
See the SSL Orchestrator v4.0 Architecture Guide for information on how this interacts with STARTTLS

L7 Profile

**Only shows with TCP or UDP set above.*

Select the specific L7 Profile to use for this rule / listener.

Options:

<dropdown of profiles>	Can also create a new profile. Only shows profiles that match the L7 Profile type selected above.

Note:
For explicit proxy rules, this should be set to the "sslo<system_name>-xp-http" L7 profile (or equivalent)

Explicit Proxy

**Only shows on outbound rules*

For outbound rules, should this rule / listener act as an explicit proxy

Checkbox:

Enabled	
Disabled	*Default

Note:
This field actually only changes the filter for the Access profile (below) and hides some of the fields. Actually, setting up the Explicit proxy is more dependent on the Access profile.
(See the SSLO v4.0 Architecture Guide use cases section for more information on setting up explicit proxies.)

Access Profile

**Only shows for TCP/UDP protocol rules)*

You select an Access Profile for use for this rule. Normally, you would select the one that was created for the default policies, which should be called "`ssloP_default_chains.app/ssloP_default_chains_accessProfile`" unless authentication or other per-session actions are needed.

Options:

<list of SSLO access profiles>	This will only display access profiles that are compatible with SSLO, which are of the following types: • SSL Orchestrator • SWG - Explicit

Note:
An access profile is required to be selected if traffic handling is to be performed. If this field is empty, traffic matching this rule will flow through SSLO without going to any service.
When Explicit proxy is selected, this field will only show SWG – Explicit profile types.

Per Request Policy

**Only shows for TCP/UDP protocol rules)*

**Only active after selecting the Access profile.*

This shows a list of the SSLO per-request policies. The per-request policy defines how the traffic will be sent to the various services defined in the policy.

Options:

<list of SSLO per-request policies>	You can create a new one from here using "new", or edit the policy in the visual policy editor using the "edit" button.

Notes:
The list is a list of the SSLO per-request policies, not Access per-request policies. (See SSL Orchestrator v4.0 Architecture Guide for more information)
A per-request policy is required to be selected if traffic handling is to be performed. If this field is empty, traffic matching this rule will flow through SSLO without going to any service.
The access profile field must be filled in before this field will be available.

Ingress Network

VLANs

**Only here for Inbound rules*

See above VLAN field definition.

Resources

iRules

**Advanced field*

Allows attaching an iRule to the rule.

Multi-Selector:

<list of available iRules>	

Notes:
The iRule is attached to the virtual server listener before it is sent along to the services.
For Explicit proxy rules, this should include "sslo_<name>-xp"
If authentication is being used as part of an explicit proxy, this should ALSO include "sslo_<name>-xp-auth".

Pool **Advanced Field*	Allows selecting a pool to send traffic to after processing instead of the defined gateway from the deployment settings page. **Options:** <list of available pools> **Notes:** This will override any settings from the deployment settings page.

SSLO Specific VPE Agents Reference

In the Visual Policy Editor (VPE), SSLO policies have access to a limited number of agents.

SSLO Usable Agents List:

Assignment	Pool Assign	Assign a Local Traffic Pool
	Variable Assign	Assign custom variables, configuration variables, or predefined session variables
Endpoint Security (Server Side)	Client IP Subnet Match	Create policy branch rules based on user's subnet
	Client Port Match	Create policy branch rules based on user's port
	Dynamic Date Time	Create branch rules based on day or time
	IP Geolocation Lookup	Determine an IP's geographic location
	IP Reputation Lookup	Check an IP's reputation
	Server IP Subnet Match	Create policy branch rules based on server's subnet
	Server Port Match	Create policy branch rules based on server's port
Classification	Application Filter	Assign a Filter to lookup Applications
	Application Lookup	Application Lookup
	Category Lookup	Category Lookup
	URL Branching	Simple branching rules based on the URL
	URL Filter Assign	Assign a Filter to lookup URLs
General Purpose	Empty	An Empty Agent for constructing custom Branch Rules
	HTTP Headers	Modify HTTP Headers
	IP Protocol Lookup	Determine IP Protocol
	iRule Event	Raises an iRule ACCESS_PER_REQUEST_ACTION_EVENT event for use with custom iRules
	L7 Protocol Lookup	L7 Protocol Lookup
	Logging	Log custom messages and session variables for reporting and troubleshooting
	SSL Bypass Set	SSL Bypass Set
	SSL Check	SSL Check
	SSL Intercept Set	SSL Intercept Set
	SSO Configuration Select	SSO Configuration Select
Traffic Management	Proxy Select	Proxy Select
	Service Connect	Service Connect
	Session Check	Session Check

SSLO Macros	Categorization	Macro call to Categorization
	SSL Intercept Policy	Macro call to SSL Intercept Policy
	Service Chain Not Intercepted	Macro call to Service Chain Not Intercepted
	IP Policy	Macro call to IP Policy
	Proxy Chaining(Connect)	Macro call to Proxy Chaining(Connect)
	Proxy Chaining(URI Rewrite)	Macro call to Proxy Chaining(URI Rewrite)

The following are references to specific VPE agents that are used in the default SSLO policy. These are also documented in APM documentation; however this document focuses on how the fields interact with SSLO. For information on the default configuration of these agents, and how they are used in SSLO, see the SSL Orchestrator v4.0 Architecture Guide.

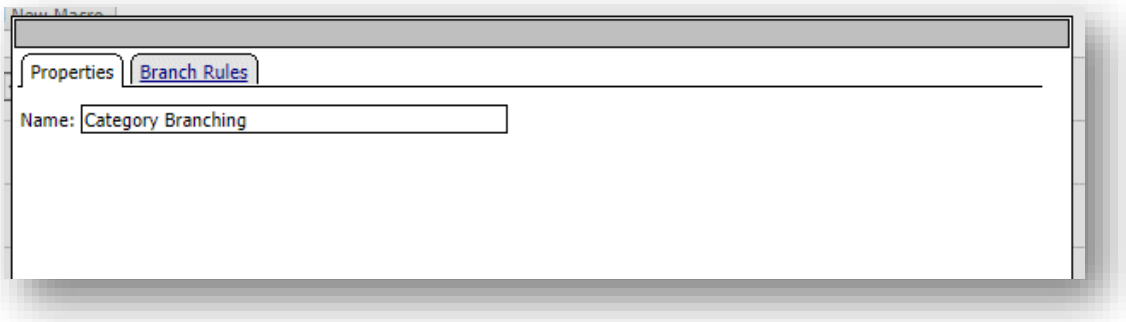
Empty Macro

The empty macro is used when there is a need to branch traffic based on criteria that can be determined in the branching tab, without further processing of the traffic.

Used in SSLO Macros:

- Categorization / SSL Check
- Categorization / L7 Protocol Lookup
- SSL Intercept Policy / Category Branching
- Proxy Chaining(Connect) / Lasthop Check
- Proxy Chaining(URI Rewrite) / Lasthop Check
- Proxy Chaining(URI Rewrite) / L7 Protocol Lookup

Example:



Fields

- None

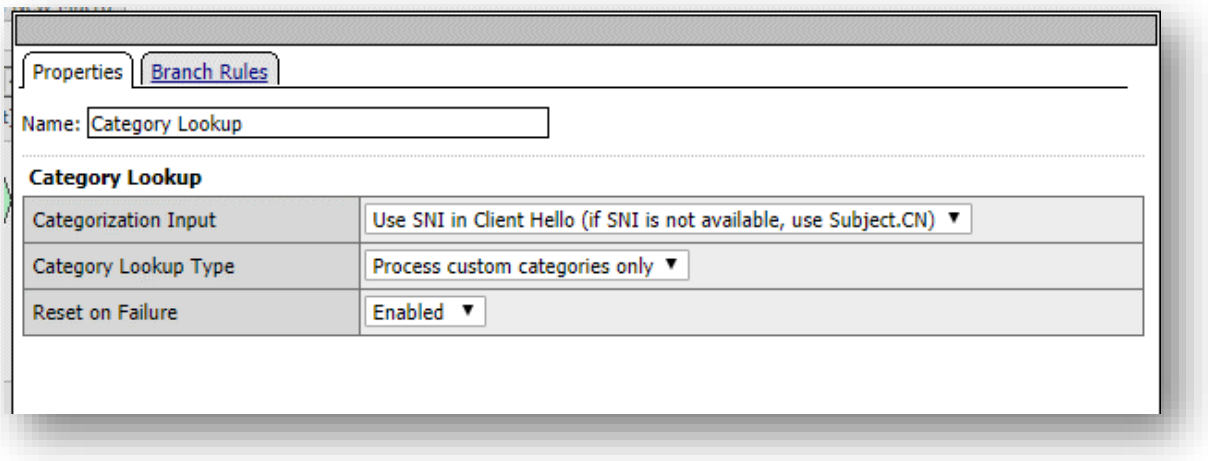
Category Lookup

This step is used to detect URL Categories and branch based on them.

Used in SSLO Macros:

- Categorization / Category Lookup (x2)

Example



Fields

Categorization Input

This field defines how to find the hostname used for the lookup.

Options:

Use SNI in Client Hello (if SNI not available, use subject.CN)	*Default This will use the host name found in the SNI (Server Name Indicator) field of the Client Hello request if available, otherwise it will use the subject.CN. This option requires a TLS connection. This provides the most accurate information as it is based on the TLS connection's request and is the hardest to forge. This will only match on the scheme and host portion of the URI. For example, "https://f5.com/mypage.html" would match https://f5.com/index.html, as well as https://f5.com/foobar.htm. Matching the URI and HTTP CONNECT will match the
Use subject.CN in server cert	This will use the information from the server certificate's subject.CN. This requires a TLS Connection. This cannot be determined before we receive the server certificate, so it will not work until after the connection has been mostly completed. This will only match on the scheme and host portion of the URI. For example, "https://f5.com/mypage.html" would match https://f5.com/index.html, as well as https://f5.com/foobar.htm.
Use HTTP URI (Cannot be used for SSL bypass decisions)	This will use the information in the HTTP header, it requires an HTTP connection, so it cannot be used for general SSL bypass decisions. This matches the entire URI, including path and page if present. For example, https://f5.com/mypage.htm would not match "https://f5.com/index.htm"
Use HTTP CONNECT hostname	This uses information in the HTTP Connect header, so it can be used for connections that are passing through an upstream proxy. This will only match the hostname, not including the scheme or path. For example, https://f5.com would also match "http://f5.com"

Category Lookup Type

This field controls URL filtering based on custom or standard categories.

Options:

Custom Categories First, then standard categories if not found	
Always process full list of custom and standard categories	
Process Standard categories only	
Process Custom categories only	

Note:
If URL Filtering or SWG is not licensed and provisioned, or "Use HTTP URI is selected in the categorization input field this field will only have the "Process Custom categories only" option.

Reset on failure

Traffic passing through his step that fails the lookup can either be reset or pass through.

Options:

Enabled	*Default
Disabled	

Notes:
This would be disabled when branching rules are used to further handle failed lookups.

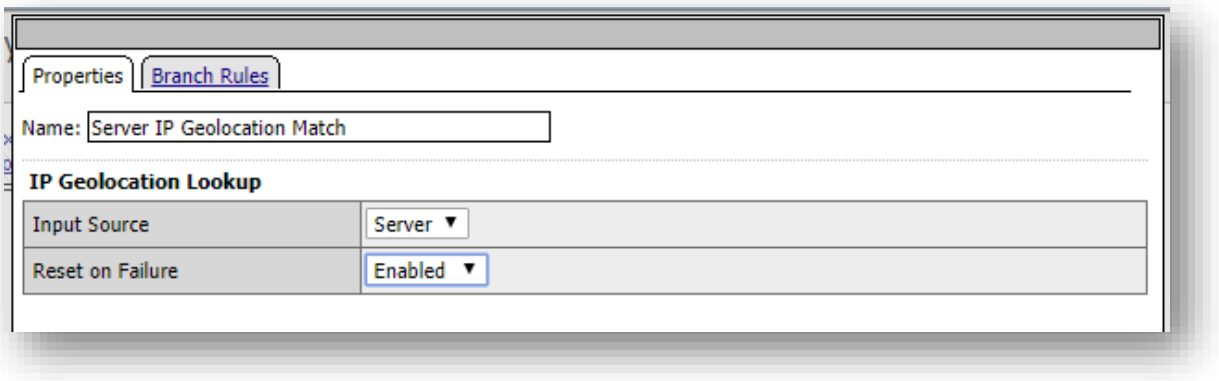
IP Geolocation Lookup

This step is used to check the geolocation code based on the IP address of the connection.

Used In:

- IP Policy / Server IP Geolocation Match

Example



Fields

Input Source

Determines which address to use for the lookup.

Options:

Client	
Server	*Default

Reset on failure

Traffic passing through his step that fails the lookup can either be reset, or can pass through.

Options:

Enabled	*Default Failed lookups will reset the connection
Disabled	

Notes:
This would be disabled when branching rules are used to further handle failed lookups.

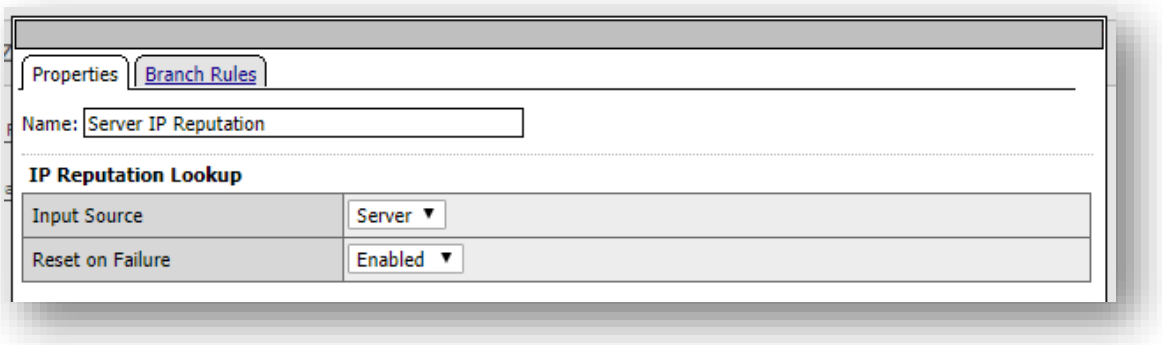
IP Reputation Lookup

This step is used to check the IP Reputation metadata based on the IP address of the connection.

Used in SSLO Macros:

- IP Policy / Server IP Reputation

Example:



Fields

Input Source

Determines which address to use for the lookup.

Options:

Client	
Server	*Default

Reset on failure

Traffic passing through his step that fails the lookup can either be reset, or can pass through.

Options:

Enabled	*Default
Disabled	

Notes:
This would be disabled when branching rules are used to further handle failed lookups.

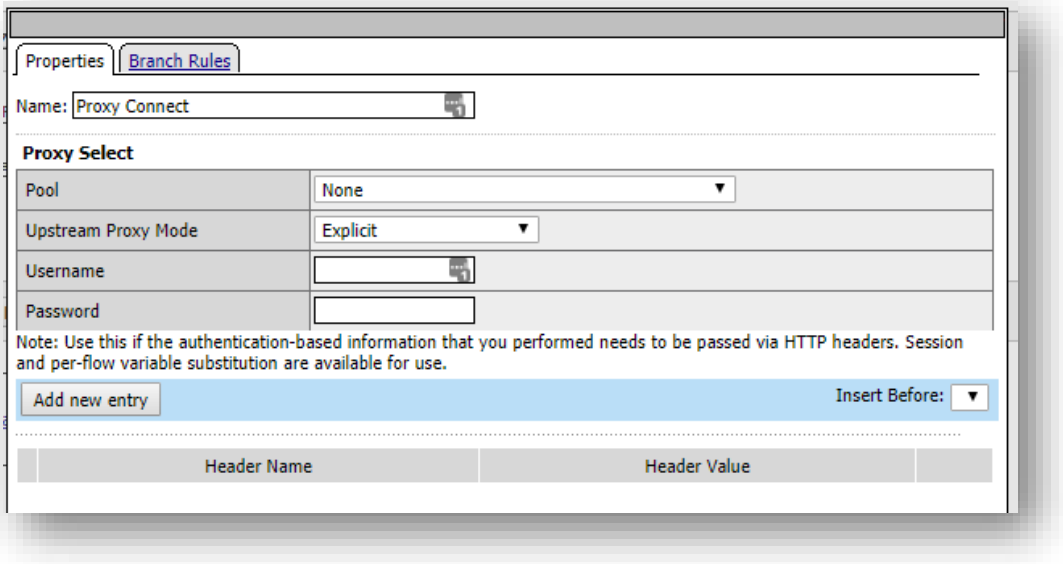
Proxy Select

This step will send the traffic to a specific explicit or transparent proxy, along with potentially re-writing HTTP header information as needed.

Used in SSLO Macros:

- Proxy Chaining(Connect) / Proxy Connect
- Proxy Chaining(URI Rewrite) / Proxy URI Rewrite

Example:



Fields

Pool
Required

Allows selecting of an existing pool of servers to send traffic to.

Options:

None	*Default
<list of pools>	

Notes:
For the purposes of SSLO, this should be pointed to the upstream explicit proxy or proxies.

Upstream Proxy Mode

Allows selection of the proxy mode of the upstream device

Options:

Explicit	*Default Sends traffic to an explicit upstream proxy. This will attach an HTTP Connect header to the traffic.
Transparent	Sends traffic to a transparent upstream proxy.
Explicit (no URI rewrite)	Will handle the need for some explicit proxy connections to setup the TCP connection prior to processing.

Notes:
In the "Service Chaining(Connect)" macro, this should be set to "Explicit(No URI rewrite)". (See the SSLO v4.0 Architecture Guide use cases section)

Username

Allows passing the username to be passed to the proxy.

Password

Allows setting the password to be passed to the proxy

Header Substitution List

Allows setting a list of HTTP headers that will be re-written when sending traffic to the proxy.

List Options:

Header Name	The HTTP header name to replace
Header Value	The value to replace it with

Notes:
This allows for session and per-flow variables in the replacement values, see APM documentation for more information on this.

SSL Bypass Set / SSL Intercept Set

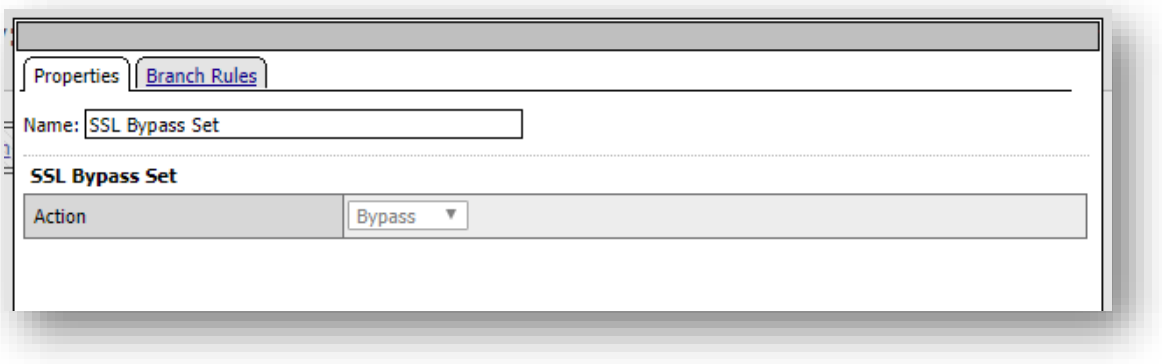
These steps are both the same base agent and appear as “SSL Bypass Set” in the details when used. These are used to control traffic decryption and encryption when passing through the service chain.

This macro is the point where the traffic is actually decrypted.

Used in SSLO Macros:

- SSL Intercept Policy / SSL Intercept Set

Example



Fields

Action

This controls if the traffic will be decrypted or not when passing through the step.

*Read only field

Options:

Intercept	*Default for SSL Intercept Set
Disabled	*Default for SSL Bypass Set

Notes:
The action is fixed for both agents, so you MUST use the correct agent for this step, you cannot change this field..

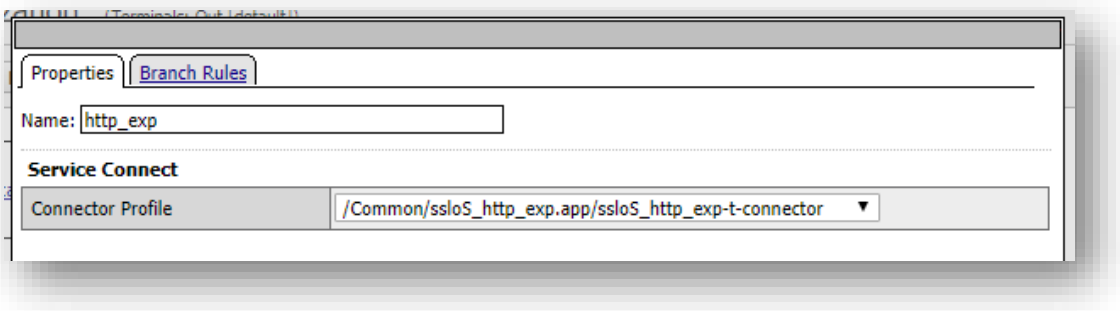
Service Connect

This object is used to pass the traffic through the specific services in the chain.

Used in SSLO Macro:

- Service Chain Intercepted / <all>
- Service Chain Not Intercepted / <all>

Example:



Fields

Connector Profile
**Required*

Traffic passing through this step will be forwarded to the specific connector profile devices

Options:

None	*Default
<list of connector profiles>	

Notes:
The connector profiles are used to handle the traffic going to and from the various services.

Legal Notices

Trademarks

AAM, Access Policy Manager, Advanced Client Authentication, Advanced Firewall Manager, Advanced Routing, AFM, APM, Application Acceleration Manager, Application Security Manager, Applications without Constraints, ARX, AskF5, ASM, BIG-IP, BIG-IP EDGE GATEWAY, BIG-IQ, BIG-IP iControl, Cloud Extender, CloudFucious, Cloud Manager, Clustered Multiprocessing, CMP, COHESION, Data Manager, DDoS Frontline, DDoS Hybrid Defender, DDoS SWAT, Defense.net, DevCentral, DevCentral [DESIGN], DNS Express, DSC, DSI, Edge Client, Edge Gateway, EDGE MOBILE, EDGE MOBILITY, EdgePortal, ELEVATE, EM, Enterprise Manager, ENGAGE, F5, F5 Agility, F5 iApps, F5[DESIGN], F5 Certified [DESIGN], F5 iControl, F5 LINK CONTROLLER, F5 Networks, F5SalesXchange [DESIGN], F5Synthesis, f5Synthesis, F5Synthesis[DESIGN], F5 TechXchange [DESIGN], F5 TMOS, Fast Application Proxy, Fast Cache, FCINCO, Global Traffic Manager, GTM, GUARDIAN, Herculon, iApps, IBR, Intelligent Browser Referencing, Intelligent Compression, IPv6 Gateway, iCall, iControl, iHealth, iQuery, iRules, iRules OnDemand, iSeries, iSession, L7 RateShaping, LC, Link Controller, Local Traffic Manager, LTM, LineRate Operating System, LineRate Point, LineRate Precision, LineRate Systems [DESIGN], LROS, LTM, Message Security Manager, MSM, OneConnect, Packet Velocity, PEM, Policy Enforcement Manager, Protocol Security Manager, PSM, Real Traffic Policy Builder, Ready Defense, SalesXchange, ScaleN, Signalling Delivery Controller, Silverline, Silverline Threat Intelligence, SDC, SSL Acceleration, SSL Everywhere, SSL Orchestrator, SDAC (except in Japan), StrongBox, SuperVIP, SYN Check, SYNTHESIS, TCP Express, TDR, TechXchange, TMOS, TotALL, Traffic Management Operating System, Traffix Systems, Traffix Systems (DESIGN), Transparent, Data Reduction, UNITY, VAULT, vCMP, VE F5 [DESIGN], Versafe, Versafe [DESIGN], VIPRION, Virtual Clustered Multiprocessing, WAF Express, WebSafe, We Make Apps Go [DESIGN], We Make Apps GO, and ZoneRunner, are trademarks or service marks of F5 Networks, Inc., in the U.S. and other countries, and may not be used without express written consent.

All other product and company names herein may be trademarks of their respective owners.

Patents

This product may be protected by one or more patents. See the F5 Patents page (https://www.f5.com/about/guidelines-policies/patents).

Notice

THE SOFTWARE, SCRIPTING, AND COMMAND EXAMPLES ARE PROVIDED “AS IS,” WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES, OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE, SCRIPTING AND COMMAND EXAMPLES, OR THE USE OR OTHER DEALINGS WITH THE SOFTWARE, SCRIPTING, AND COMMAND EXAMPLES.

Publication Date

This document was published in Sept 2018.

Copyright