

# vShield API Programming Guide

vShield 5.1.3

vShield App 5.1.3

vShield Edge 5.1.3

vShield Endpoint 5.1.3

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see <http://www.vmware.com/support/pubs>.

EN-000869-05

**vmware®**

You can find the most up-to-date technical documentation on the VMware Web site at:

<http://www.vmware.com/support/>

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

[docfeedback@vmware.com](mailto:docfeedback@vmware.com)

Copyright © 2010 - 2014 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

# Contents

About This Book	11
<b>1 Overview of VMware vShield</b>	<b>13</b>
vShield Components	13
vShield Manager	13
vShield App	13
vShield Edge	14
vShield Endpoint	14
vShield Data Security	14
Compatibility Between Different REST API Versions	14
REST API Version 2.0 in vShield 5.0	14
Multitenancy	15
An Introduction to REST API for vShield Users	15
How REST Works	15
Using the vShield REST API	16
Ports Required for vShield REST API	16
About the REST API	16
RESTful Workflow Patterns	17
For More Information About REST	17
<b>2 vShield Manager Management</b>	<b>19</b>
Synchronizing vShield Manager with vCenter Server, SSO, and DNS	19
Querying vShield Manager Global Configuration	21
Resetting the Local Account Password	21
Add Security Profile	21
Get Security Profile	22
Get Password Hint Questions	22
Reset Password	22
Monitoring vShield Manager reachability	23
Working with vShield Manager Syslog Server Configuration	23
Configure vShield Manager Syslog Server	23
Get vShield Manager Syslog Server Configuration	23
Delete vShield Manager Syslog Server Configuration	23
Querying vShield Manager Logs	24
Get vShield Manager System Events	24
Get vShield Manager Audit Logs	24
Querying vShield Manager Tech Support Log	24
User Management	24
Get Information About a User	25
Create a Local User on vShield Manager	25
Update a Local User Account	26
Enable or Disable a User Account	26
Delete a User Account	26
Role Management	28
Get Role for a User	28
Get Role for a vShield Manager Roles	28
Add Role and Resources for a User	29
Change User Role	29

Get List of Possible Roles	30
Get List of Scoping Objects	30
Delete User Role	31
Creating IPset and MACset Containers	31
List IPsets Created on a Scope	31
Create an IPset on a Scope	31
Get Details of an IPset	32
Modify an Existing IPset	32
Delete an IPset	32
List MACsets Created on a Scope	33
Create a MACset on a Scope	33
Get Details of a MACset	33
Modify an Existing MACset	34
Delete a MACset	34
Security Group Scope and Members	34
List Security Groups Created on a Scope	34
Create Security Group on a Scope	35
Get Members for a Scope	35
Get Security Group Details	35
Modify a Security Group	36
Delete a Security Group	37
Add Member to Security Group	37
Delete Member from Security Group	37
Transport Set for Services	37
Working with Service Groups	37
List Service Groups on a Scope	37
Add Service Group to a Scope	38
Get Details of a Service Group	40
Modify Service Group Details	40
Delete Service Group from Scope	41
Working with Services	41
List Services on a Scope	41
Add Service to a Scope	41
Get Details of a Service	43
Modify Service Details	43
Delete Service from Scope	43
Working with the Members of a Service	44
Query Service Members	44
Add a Member to the Service	45
Delete a Member from the Service	45
Querying Object IDs	45
Query Datacenter MOID	45
Query Datacenter ID	45
Query Host ID	46
Query Portgroup ID	46

### 3 ESX Host Preparation for vShield App, vShield Endpoint, and vShield Data Security 47

Installing Licenses for vShield Edge, vShield App, and vShield Endpoint	47
Installing vShield App and vShield Endpoint Services on an ESX Host	47
Installing vShield Data Security	49
Upgrading vShield Data Security	49
Getting the Installation Status of vShield Services on an ESX Host	50
Uninstalling vShield Services from an ESX Host	50
Uninstalling vShield Data Security	50

<b>4</b>	<b>vShield Edge Installation and Upgrade</b>	<b>51</b>
	Installing a vShield Edge	51
	Running Queries on all vShield Edges	53
	Upgrading vShield Edge	55
	Deleting a vShield Edge	55
<b>5</b>	<b>vShield Edge Management</b>	<b>57</b>
	Running Queries on a Specific vShield Edge	58
	Query vShield Edge Details	58
	Query vShield Edge Summary	62
	Querying vShield Edge Status	64
	Working with Appliances	66
	Query Appliance Configuration	66
	Modify Appliance Configuration	67
	Change Appliance Size	67
	Manage an Appliance	67
	Query Appliance	68
	Modify Appliance	68
	Delete Appliance	69
	Working with Interfaces	69
	Add Interfaces	69
	Retrieve Interfaces for a vShield Edge	70
	Delete Interfaces	71
	Manage a vShield Interface	71
	Retrieve Interface with Specific Index	71
	Delete Interface Configuration	71
	Modify an Interface	71
	Query Interface Statistics	72
	Query Statistics for all Interfaces	72
	Query Statistics for Uplink Interfaces	73
	Query Statistics for Internal Interfaces	73
	Query Dashboard Statistics	74
	Configuring Edge Services	74
	Configure Firewall	75
	Add Firewall Configuration	75
	Query Firewall Configuration	76
	Delete Firewall Configuration	77
	Append Firewall Rules	78
	Add a Firewall Rule Above a Specific Rule	78
	Query Specific Rule	79
	Modify Firewall Rule	79
	Delete a Firewall Rule	80
	Manage Default Firewall Policy	80
	Query Firewall Statistics	81
	Query Firewall Statistics For a Rule	81
	Configure NAT	81
	Retrieve NAT Rules for a vShield Edge	82
	Delete all NAT Rules	83
	Add a NAT Rule above a Specific Rule	83
	Append NAT Rules	84
	Change a NAT Rule	84
	Delete a Rule	84
	Configure Routing	85

Configure Static and Default Routes	85
Query Static and Default Routes	85
Delete Static and Default Routes	86
Change Static Routes	86
Append Static Routes	86
Delete Static Routes	87
Configure Default Routes for vShield Edge	87
Delete Default Routes	87
Configure DNS Servers	87
Configure DNS	87
Retrieve DNS Configuration	88
Delete DNS Configuration	88
Retrieve DNS Statistics	89
Configure DHCP	89
Query DHCP Configuration	91
Delete DHCP Configuration	91
Retrieve DHCP Lease Information	92
Append IP Pool to DHCP Configuration	92
Append Static Binding to DHCP Configuration	92
Delete DHCP Pool	93
Delete DHCP Static Binding	93
Configure Certificates	93
Working with Certificates	93
Working with Certificate Signing Requests (CSRs)	94
Working with Certificate Revocation List (CRL)	95
Configure IPSEC VPN	96
Retrieve IPSec Configuration	97
Retrieve IPSec Statistics	98
Query Tunnel Traffic Statistics	99
Delete IPSec Configuration	100
Managing SSL VPN	100
Enable or Disable SSL VPN	100
Query SSL VPN Details	100
Manage Server Settings	100
Configure Private Networks	101
Configure Web Resource	103
Configure Users	105
Configure IP Pool	107
Configure Network Extension Client Parameters	110
Configure Network Extension Client Installation Package	110
Configure Portal Layouts	114
Configure Authentication Parameters	116
Configure SSL VPN Advanced Configuration	118
Working with Active Clients	119
Manage Logon and Logoff scripts	120
Reconfigure SSL VPN	122
Query SSL VPN Configuration	125
Delete SSL VPN Configuration	128
Query SSL VPN Statistics	128
Configure Load Balancer	129
Query Load Balancer Configuration	131
Query Statistics	132
Delete Load Balancer Configuration	133

Manage all Backend Pools	133
Manage all Virtual Servers	136
Retrieve Load Balancer Statistics	138
Enable Layer-4 Mode for Load Balancer	140
Configure High Availability (HA)	140
Retrieve High Availability Configuration	141
Delete High Availability Configuration	141
Force Syncing vShield Edge	141
Configuring Advanced Options for vShield Edge	141
Change AESNI Setting for a vShield Edge	141
Change FIPS Setting for a vShield Edge	142
Change Logging Level for vShield Appliance	142
Manage Auto Configuration Settings	142
Modify Auto Configuration Settings	142
Query Auto Configuration Settings	142
Change TCP Loose Setting	143
Replacing the Configuration of a vShield Edge	143
Redeploying vShield Edge Appliances	147
Managing CLI Credentials and Access	147
Change CLI Credentials	147
Change CLI Remote Access	147
Managing the Remote Syslog Server	148
Query Remote Syslog Server	148
Reconfigure Remote Syslog Server	148
Delete Remote Syslog Server	148
Debugging and Support	149
Query Technical Support Log	149
Query vShield Edge Service Statistics	149

## 6 Working with VXLAN Virtual Wires 153

Preparing for VXLAN Virtual Wires	153
Configuring Switches	154
Prepare Switch	154
Edit Teaming Policy	154
Query Configured Switches	154
Query Configured Switches on Datacenter	155
Query Specific Switch	155
Delete Switch	156
Working with Cluster Switch Mappings	156
Map a Cluster to a Switch	156
Synchronize hosts	156
Query all Cluster Mappings	157
Query Mappings by Switch	157
Query Specific Cluster	158
Delete Cluster Switch Mapping	158
Working with EAM Agencies	158
Install EAM Agency	159
Synchronize Agency State	159
Replace Agency Scope	159
Query Agency by Cluster	159
Query Agency Status	160
Query Agency ID for Cluster	160
Delete Agency	160
Uninstall Agency Status	160
Working with Segment IDs	160

Add a new Segment ID Range	160
Query all Segment ID Ranges	161
Query a Specific Segment ID Range	161
Update a Segment ID Range	162
Delete a Segment ID Range	162
Working with Multicast Address Ranges	162
Add a new Multicast Address Range	162
Query all Multicast Address Ranges	162
Get a Specific Multicast Address Range	163
Update a Multicast Address Range	163
Delete a Multicast Address Range	163
Working with Network Scopes	164
Create a Network Scope	164
Edit a Network Scope	164
Update Attributes on a Network Scope	164
Query existing Network Scopes	165
Query a Specific Network Scope	165
Delete a Network Scope	166
Working with Virtualized Networks	166
Create a VXLAN Virtual Wire	166
Query all VXLAN Virtual Wires on a Network Scope	166
Query all VXLAN Virtual Wires on all Network Scopes	167
Query a Specific VXLAN Virtual Wire	168
Delete a VXLAN Virtual Wire	168
Managing the VXLAN Virtual Wire UDP Port	168
Get UDP Port	168
Update UDP Port	168
Querying Allocated Resources	169
Testing Multicast Group Connectivity	169
Test Multicast Group Connectivity in a Network Scope	169
Test Multicast Group Connectivity in a VXLAN Virtual Wire	170
Performing Ping Test	170

## 7 vShield App Management 171

Modifying the State of a Datacenter	171
Retrieve Datacenter State	171
Modify Datacenter State	172
Configuring Firewall Rules for vCenter	172
Configuring the vShield App Firewall	172
Query Firewall Configuration	172
Add a Firewall Rule	178
Modify a Firewall Rule	180
Delete a Firewall Rule	182
Revert to Default Firewall Configuration	183
Configuring Fail-Safe Mode for vShield App Firewall	183
Configure Fail-Safe Mode for vShield App Firewall	183
Query Fail-Safe Mode Configuration for vShield App Firewall	184
Working with SpoofGuard	184
Get SpoofGuard Settings at Context Level	184
Replace SpoofGuard Settings	184
Get SpoofGuard IP Settings	185
Change SpoofGuard IP Settings	185
Working with Namespaces	186
Add Namespace in a Datacenter	186
Get Namespace Details	186



Delete a Namespace	186
Show Namespaces in a Datacenter	186
Getting Flow Statistic Details	187
Get Flow Statistics	187
Get Flow Meta-Data	189
Configure Addresses to be Ignored by Flow Parser	190
Query Addresses Ignored by Flow Parser	190
Excluding Virtual Machines from vShield App Protection	190
Add a Virtual Machine to the Exclusion List	190
Get Virtual Machine Exclusion List	190
Delete a Virtual Machine from Exclusion List	191
Configuring Syslog Service for a vShield App	191
Synchronizing vShield App	192
Querying vShield App Technical Support Log	192
Querying vShield App Status	193
Upgrading vShield App	193

## 8 vShield Endpoint Management 195

Overview of Solution Registration	195
Registering a Solution with vShield Endpoint Service	195
Register a Vendor	196
Register a Solution	196
Altitude of a Solution	196
IP Address and Port for a Solution	196
Activate a Solution	197
Querying Registration Status of vShield Endpoint	197
Get Vendor Registration	197
Get Solution Registration	197
Get IP Address of a Solution	198
Get Activation Status of a Solution	198
Querying Activated Security Virtual Machines for a Solution	198
Query Activated Security Virtual Machines	198
Query Activation Information	199
Unregistering a Solution with vShield Endpoint	199
Unregister a Vendor	199
Unregister a Solution	199
Unset IP Address	199
Deactivate a Solution	200
Status Codes and Error Schema	200
Return Status Codes	200
Error Schema	200

## 9 vShield Data Security Configuration 203

vShield Data Security User Roles	203
Defining a Data Security Policy	204
Query Regulations	204
Enable a Regulation	204
Query Classification Value	205
Configure a Customized Regex as a Classification Value	205
View the List of Excludable Areas	205
Exclude Areas from Policy Inspection	206
Specify Security Groups to be Scanned	207
Query Security Groups Being Scanned	207
Configure File Filters	208
Saving and Publishing Policies	209

Query Saved Policy	209
Query Published Policy	210
Publish the Updated Policy	210
Data Security Scanning	210
Start, Pause, Resume, or Stop a Scan Operation	211
Query Status for a Scan Operation	211
Querying Scan Results	211
Get List of Virtual Machines Being Scanned	211
Get Number of Virtual Machines Being Scanned	212
Get Summary Information about the Last Five Scans	213
Get Information for Virtual Machines Scanned During Previous Scan	213
Retrieve Information About Previous Scan Results	213
Get XML Representation of Policy Used for Previous Scan	213
Querying Violation Details	215
Get List of Violation Counts	215
Get List of Violating Files	216
Get List of Violating Files in CSV Format	217
Get Violations in Entire Inventory	217
	218
<b>10 Task Framework Management</b>	<b>219</b>
About Task Framework	219
Query Job Instances for Job ID	220
Query Latest Job Instances for Job ID	221
Block REST Thread	221
Query Job Instances by Criterion	221
<b>Appendix</b>	<b>223</b>
vShield Manager Global Configuration Schema	223
ESX Host Preparation and Uninstallation Schema	228
vShield App Schemas	229
vShield App Configuration Schema	229
vShield App Firewall Schema	229
vShield App SpoofGuard Schema	232
vShield App Namespace Schema	234
Error Message Schema	235

# About This Book

---

This manual, the *vShield API Programming Guide*, describes how to install, configure, monitor, and maintain the VMware® vShield™ system by using REST API requests. The information includes step-by-step configuration instructions and examples.

## Intended Audience

This manual is intended for anyone who wants to use REST API to install or use vShield in a VMware vSphere environment. The information in this manual is written for experienced system administrators who are familiar with virtual machine technology, virtualized datacenter operations, and REST APIs. This manual also assumes familiarity with vShield.

## VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation go to <http://www.vmware.com/support/pubs>.

## Document Feedback

VMware welcomes your suggestions for improving our documentation. If you have comments, send your feedback to [docfeedback@vmware.com](mailto:docfeedback@vmware.com).

## vShield Documentation

The following documents comprise the vShield documentation set:

- *vShield Administration Guide*
- *vShield Quick Start Guide*
- *vShield API Programming Guide*, this guide

## Technical Support and Education Resources

The following sections describe the technical support resources available to you. To access the current version of this book and other books, go to <http://www.vmware.com/support/pubs>.

### Online and Telephone Support

To use online support to submit technical support requests, view your product and contract information, and register your products, go to <http://www.vmware.com/support>.

Customers with appropriate support contracts should use telephone support for the fastest response on priority 1 issues. Go to [http://www.vmware.com/support/phone\\_support](http://www.vmware.com/support/phone_support).

## Support Offerings

To find out how VMware support offerings can help meet your business needs, go to <http://www.vmware.com/support/services>.

## VMware Professional Services

VMware Education Services courses offer extensive hands-on labs, case study examples, and course materials designed to be used as on-the-job reference tools. Courses are available onsite, in the classroom, and live online. For onsite pilot programs and implementation best practices, VMware Consulting Services provides offerings to help you assess, plan, build, and manage your virtual environment. To access information about education classes, certification programs, and consulting services, go to <http://www.vmware.com/services>.

# Overview of VMware vShield

---

VMware vShield™ is a suite of network edge and application-aware firewalls built for VMware vCenter Server integration. vShield inspects client-server communications and inter-virtual-machine communications to provide detailed traffic analytics and application-aware firewall protection. It is a critical security component to protect virtualized datacenters from attacks and misuse, and helps achieve compliance-mandated goals. This chapter includes the following topics:

- [“vShield Components”](#) on page 13
- [“Compatibility Between Different REST API Versions”](#) on page 14
- [“Ports Required for vShield REST API”](#) on page 16
- [“An Introduction to REST API for vShield Users”](#) on page 15

This guide assumes you have administrator access to the entire vShield system. If you are unable to access a screen or perform a particular task, consult your vShield administrator.

## vShield Components

vShield includes components and services essential for protecting virtual machines in a virtualized datacenter. vShield can be configured with a Web-based user interface, a command line interface (CLI), or a REST API.

To run vShield, you need one vShield Manager virtual appliance and at least one vShield App or vShield Edge virtual appliance. The vShield Manager virtual appliance can run on a different ESX host than the vShield App and vShield Edge virtual appliances.

### vShield Manager

vShield Manager is the centralized management component of vShield. You install it as a virtual appliance by deploying an OVA from the vSphere Client. Using vShield Manager’s user interface or vSphere Client plug-in, you can install, configure, and maintain vShield appliances. The vShield Manager user interface leverages the vSphere Web Services SDK to display tabs within the vSphere Client inventory panel. For details about the user interface, see the *vShield Administration Guide*.

### vShield App

A vShield App virtual appliance monitors all traffic into and out of an ESX host, and between virtual machines on the host. vShield App provides application-aware traffic analysis and stateful firewall protection, and it regulates traffic based on a set of rules, similar to an access control list (ACL).

As traffic passes through a vShield App, each session header is inspected to catalog the data. The vShield App creates a profile for each virtual machine detailing the operating system, applications, and ports used for network communication. Based on this information, the vShield App allows ephemeral port use by permitting dynamic protocols such as FTP or RPC to pass through, while maintaining lockdown on ports 1024 and higher. You cannot protect the ESX Service Console, ESXi direct console user interface (DCUI), or the VMkernel with vShield App because these components are not virtual machines.

---

**NOTE** vShield App and vApp are not the same thing. A vApp is a grouping of virtual machines in vSphere, for example a management appliance and a database appliance working together.

---

## vShield Edge

vShield Edge provides network edge security and gateway services to isolate a virtualized network, or virtual machines in a port group, vDS port group, or Cisco Nexus 1000V port group. You install a vShield Edge at a datacenter level and can add up to ten internal or uplink interfaces. The vShield Edge connects isolated, stub networks to shared (uplink) networks by providing common gateway services such as DHCP, VPN, NAT, and Load Balancing. Common deployments of vShield Edge include in the DMZ, VPN Extranets, and multi-tenant Cloud environments where the vShield Edge provides perimeter security for Virtual Datacenters (VDCs).

## vShield Endpoint

vShield Endpoint offloads antivirus and anti-malware agent processing to a dedicated secure virtual appliance delivered by VMware partners. Since the secure virtual appliance (unlike a guest virtual machine) doesn't go offline, it can continuously update antivirus signatures thereby giving uninterrupted protection to the virtual machines on the host. Also, new virtual machines (or existing virtual machines that went offline) are immediately protected with the most current antivirus signatures when they come online.

## vShield Data Security

vShield Data Security provides visibility into sensitive data stored within your organization's virtualized and cloud environments. Based on the violations reported by vShield Data Security, you can ensure that sensitive data is adequately protected and assess compliance with regulations around the world.

## Compatibility Between Different REST API Versions

Each release of the vShield REST API represents a new version of the REST API code with new and changed features. If you are running a previous version of vShield component software, you might not be able to use all of the features of the latest release of the vShield REST API.



**CAUTION** The REST APIs described in this document can change over time. At this point, vShield does not guarantee forward compatibility.

---

## REST API Version 2.0 in vShield 5.0

Release 5.0 of vShield introduces version 2.0 of the REST API. Many URLs changed from version 1.0 to 2.0.

You can determine the API version of a vShield component (such as Edge or App) with the following example REST calls. In the *GET* request syntax, <vsm-ip> represents the IP address or host name of vShield Manager.

### Example 1-1. Determine the API version of the vShield Manager or vShield Endpoint

---

GET https://<vsm-ip>/api/versions

```
<versions>
  <version value="2.1">
    <module name="VshieldAppGlobal" baseUri="/api/2.1/app" version="2.1"/>
    <module name="Flow" baseUri="/api/2.1/app/flow" version="2.1"/>
  </version>
  <version value="2.0">
    <module name="Dlp" baseUri="/api/2.0/dlp" version="2.0"/>
    <module name="Endpoint" baseUri="/api/2.0/endpointsecurity" version="2.0"/>
    <module name="MACSet" baseUri="/api/2.0/services/macset" version="2.0"/>
    <module name="SystemEvent" baseUri="/api/2.0/systemevent" version="2.0"/>
    <module name="AuditLog" baseUri="/api/2.0/auditlog" version="2.0"/>
    <module name="UserMgmt" baseUri="/api/2.0/services/usermgmt" version="2.0"/>
    <module name="Application" baseUri="/api/2.0/services/application" version="2.0"/>
    <module name="IPSet" baseUri="/api/2.0/services/ipset" version="2.0"/>
    <module name="SyslogServer" baseUri="/api/2.0/services/syslog/config" version="2.0"/>
    <module name="SecurityGroup" baseUri="/api/2.0/services/securitygroup" version="2.0"/>
  </version>
</versions>
```

```
</version>
</versions>
```

### Example 1-2. Determine the API version of a vShield App

```
GET https://<vsm-ip>/api/versions/app/<datacenter-id>
<versions>
  <version version="2.0">
    <module version="2.0" baseUri="/api/2.0/app" id="datacenter-21" name="app"/>
  </version>
</versions>
```

### Example 1-3. Determine the API version of a vShield Edge

```
GET https://<vsm-ip>/api/versions/edge/dvportgroup-63
<versions>
  <version version="2.0">
    <module version="2.0" baseUri="/api/2.0/networks" id="dvportgroup-63" name="edge"/>
  </version>
</versions>
```

The API version for vShield App is governed by the state of the datacenter in relation to a vShield component. If the datacenter state is in backwardCompatible mode, then it supports only version 1.0 REST calls. If the datacenter state is in regular mode, then it supports only 2.0 REST calls. These API versions are mutually exclusive – only one REST API version is supported at a time.

[Table 1-1](#) lists compatibility between different versions of the REST API, vShield Manager, and the vShield virtual appliances: vShield App, vShield Endpoint, and vShield Edge.

**Table 1-1. REST API Compatibility Matrix**

REST API Version	vShield Manager Version	vShield Appliance Version	Supported?
3.0	5.1	4.1	No
3.0	5.1	5.0	No
3.0	5.1	5.1	Yes
2.0	5.1	5.0	Yes
2.0	5.1	5.1	No

## Multitenancy

In vShield 5.0, the vShield App firewall configuration supports multitenancy. A single IP address can show up in multiple places in the network (different IP address namespaces) associated with different virtual machines. Only 2.0 REST APIs support multitenancy. In backward compatibility mode, vShield 5.0 supports the old APIs and does not enforce rules with awareness of multitenancy.

If you have written programs using 1.0 REST APIs, you should reconsider whether their design works as intended in the multitenancy scenario. If not, change your programs to use the API 2.0 calls.

## An Introduction to REST API for vShield Users

REST, an acronym for Representational State Transfer, is a term that has been widely employed to describe an architectural style characteristic of programs that rely on the inherent properties of hypermedia to create and modify the state of an object that is accessible at a URL.

### How REST Works

Once a URL of such an object is known to a client, the client can use an HTTP GET request to discover the properties of the object. These properties are typically communicated in a structured document with an HTTP Content-Type of XML or JSON, that provides a representation of the state of the object. In a RESTful workflow, documents (representations of object state) are passed back and forth (transferred) between a client and a

service with the explicit assumption that neither party need know anything about an entity other than what is presented in a single request or response. The URLs at which these documents are available are often “sticky,” in that they persist beyond the lifetime of the request or response that includes them. The other content of the documents is nominally valid until the expiration date noted in the HTTP Expires header.

---

**IMPORTANT** All vShield REST requests require authorization. The default vShield Manager login credentials are user admin password default. Unless you changed these, you can use the following basic authorization, where YWRtaW46ZGVmYXVsdA== is the Base 64 encoding of the default credentials admin:default.

Authorization: Basic YWRtaW46ZGVmYXVsdA==

---

## Using the vShield REST API

You have several choices for programming the vShield REST API: using Firefox, Chrome, or curl. To make XML responses more legible, you can copy and paste them into xmllcopyeditor or pspad.

### To use the REST API in Firefox

- 1 Locate the RESTClient Mozilla add-on, and add it to Firefox.
- 2 Click **Tools > REST Client** to start the add-on.
- 3 Click **Login** and enter the vShield login credentials, which then appear encoded in the Request Header.
- 4 Select a method such as GET, POST, or PUT, and type the URL of a REST API. You might be asked to accept or ignore the lack of SSL certificate. Click **Send**.

Response Header, Response Body, and Rendered HTML appear in the bottom window.

### To use the REST API in Chrome

- 1 Search the Web to find the Simple REST Client, and add it to Chrome.
- 2 Click its globe-like icon to start it in a tab.
- 3 The Simple REST Client provides no certificate-checking interface, so use another Chrome tab to accept or ignore the lack of SSL certificate.
- 4 Type the URL of a REST API, and select a method such as GET, POST, or PUT.
- 5 In the Headers field, type the basic authorization line, as in the Important note above. Click **Send**.

Status, Headers, and Data appear in the Response window.

### To use the REST API in curl

- 1 Install curl if not already installed.
- 2 In front of the REST URL, the -k option avoids certificate checking, and the -u option specifies credentials.

```
curl -k -u admin:default https://<vsm-ip>/api/2.0/services/usermgmt/user/admin
```

## Ports Required for vShield REST API

The vShield Manager requires port 443/TCP for REST API requests.

## About the REST API

REST APIs use HTTP requests (often sent by script or high-level language) as a way of making idempotent remote procedure calls that create, modify, or delete objects defined by the API. A REST API is defined by a collection of XML documents that represent the objects on which the API operates. The HTTP operations themselves are generic to all HTTP clients. To write a RESTful client, you should understand HTTP protocol and the semantics of standard HTML markup. For vShield REST API, you must know three things:

- The set of objects that the API supports, and what they represent. For example, what are vDC and Org?



- How the API represents these objects. For instance, what is the XML schema for the vShield Edge firewall rule set? What do the individual elements and attributes represent?
- How the client refers to an object on which it wants to operate. For example, what is a managed object ID?

To answer these questions, you look at vShield API resource schemas. These schemas define a number of XML types, many of which are extended by other types. The XML elements defined in these schemas, along with their attributes and composition rules (minimum and maximum number of elements or attributes, or the prescribed hierarchy with which elements can be nested) represent the data structures of vShield objects. A client can “read” an object by making an HTTP GET request to the object’s resource URL. A client can “write” (create or modify) an object with an HTTP PUT or POST request that includes a new or changed XML body document for the object. Usually a client can delete an object with an HTTP DELETE request.

This document presents example requests and responses, and provides reference information on the XML schemas that define the request and response bodies.

## RESTful Workflow Patterns

All RESTful workflows fall into a pattern that includes only two fundamental operations, which you repeat in this order for as long as necessary.

- Make an HTTP request (GET, PUT, POST, or DELETE). The target of this request is either a well-known URL (such as vShield Manager) or a link obtained from the response to a previous request. For example, a GET request to an Org URL returns links to vDC objects contained by the Org.
- Examine the response, which can be an XML document or an HTTP response code. If the response is an XML document, it may contain links or other information about the state of an object. If the response is an HTTP response code, it indicates whether the request succeeded or failed, and may be accompanied by a URL that points to a location from which additional information can be retrieved.

## For More Information About REST

For a comprehensive discussion of REST from both client and server perspectives, see *RESTful Web Services* by Leonard Richardson and Sam Ruby, published 2007 by O’Reilly Media.

There are also many sources of information about REST on the Web, including:

- <http://www.infoq.com/articles/rest-introduction>
- <http://www.infoq.com/articles/subbu-allamaraju-rest>
- <http://www.stucharlton.com/blog/archives/000141.html>



# vShield Manager Management

---

The vShield Manager requires communication with your vCenter Server and services such as DNS and NTP to provide details on your VMware Infrastructure inventory.

The chapter includes the following topics:

- [“Synchronizing vShield Manager with vCenter Server, SSO, and DNS”](#) on page 19
- [“Querying vShield Manager Global Configuration”](#) on page 21
- [“Resetting the Local Account Password”](#) on page 21
- [“Monitoring vShield Manager reachability”](#) on page 23
- [“Working with vShield Manager Syslog Server Configuration”](#) on page 23
- [“Querying vShield Manager Logs”](#) on page 24
- [“Querying vShield Manager Tech Support Log”](#) on page 24
- [“User Management”](#) on page 24
- [“Role Management”](#) on page 28
- [“Creating IPset and MACset Containers”](#) on page 31
- [“Security Group Scope and Members”](#) on page 34
- [“Transport Set for Services”](#) on page 37
- [“Querying Object IDs”](#) on page 45

---

**IMPORTANT** All vShield REST requests require authorization. See [“Using the vShield REST API”](#) on page 16 for details about basic authorization.

---

## Synchronizing vShield Manager with vCenter Server, SSO, and DNS

You can synchronize the vShield Manager with the vCenter Server, add DNS servers to the vShield Manager for IP address and hostname resolution, configure time, and zone and add an NTP server. Synchronizing with vCenter Server enables the vShield Manager user interface to display your VMware Infrastructure inventory, and requires its IP address (or URL) and administrator login credentials. For the vcInfo schema, and the dnsInfo schema, see [“vShield Manager Global Configuration Schema”](#) on page 223.

**Example 2-1.** Synchronize the vShield Manager with vCenter server and SSO and identify DNS services

---

Request:

POST https://<vsm-ip>/api/2.0/global/config

Request Body:

```
<vsmGlobalConfig xmlns="vmware.vshield.edge.2.0">
```

```

<ssoInfo>
  <lookupServiceUrl>https://<SSO IP or Host name>:7444/lookupservice/sdk</lookupServiceUrl>
  <ssoAdminUserName>admin@System-Domain</ssoAdminUserName>
  <ssoAdminPassword></ssoAdminPassword>
</ssoInfo>
<vcInfo>
  <ipAddress>VC_IP</ipAddress>
  <userName>admin</userName>
  <password></password>
</vcInfo>
<dnsInfo>
  <primaryDns>10.112.192.1</primaryDns>
  <secondaryDns>10.112.192.2</secondaryDns>
</dnsInfo>
</vsmGlobalConfig>

```

---

Specifying DNS information is optional. You can synchronize vShield Manager with just vCenter Server.

### Example 2-2. Synchronize the vShield Manager with vCenter server and SSO

---

Request:

POST https://<vsm-ip>/api/2.0/global/config

Request Body:

```

<vsmGlobalConfig xmlns="vmware.vshield.edge.2.0">
  <ssoInfo>
    <lookupServiceUrl>https://<SSO IP or Host name>:7444/lookupservice/sdk</lookupServiceUrl>
    <ssoAdminUserName>admin@System-Domain</ssoAdminUserName>
    <ssoAdminPassword></ssoAdminPassword>
  </ssoInfo>
  <vcInfo>
    <ipAddress>VC_IP</ipAddress>
    <userName>admin</userName>
    <password></password>
  </vcInfo>
</vsmGlobalConfig>

```

---

### Example 2-3. Synchronize the vShield Manager with vCenter Server

---

Request:

POST https://<vsm-ip>/api/2.0/global/config

Request Body:

```

<vsmGlobalConfig xmlns="vmware.vshield.edge.2.0">
  <vcInfo>
    <ipAddress>10.112.196.22</ipAddress>
    <userName>administrator</userName>
    <password>123</password>
  </vcInfo>
</vsmGlobalConfig>

```

---

### Example 2-4. Configure NTP server

---

Request:

POST https://<vsm-ip>/api/2.0/global/config

Request Body:

```

<vsmGlobalConfig xmlns="vmware.vshield.edge.2.0">
  <timeInfo>
    <ntpServer>10.112.196.2</ntpServer>
  </timeInfo>
</vsmGlobalConfig>

```

```
</timeInfo>
</vsmGlobalConfig>
```

---

## Querying vShield Manager Global Configuration

You can query the current vCenter, SSO, DNS, and time/zone or NTP server configuration for the vShield Manager.

### Example 2-5. Get vShield Manager configuration

---

Request:

GET https://<vsm-ip>/api/2.0/global/config

Response Body:

```
<vsmGlobalConfig xmlns="vmware.vshield.edge.2.0">
  <ssoInfo>
    <vsmSolutionName>VSM_SOLUTION_963bf981-02c7-4037-bb86-763b7ff2fa8b</vsmSolutionName>
    <lookupServiceUrl>https://<SSO IP or host name>:7444/lookupservice/sdk</lookupServiceUrl>
  </ssoInfo>
  <vcInfo>
    <ipAddress><VC IP></ipAddress>
    <userName>root</userName>
  </vcInfo>
  <dnsInfo>
    <primaryDns>10.112.0.1</primaryDns>
    <secondaryDns>10.112.0.2</secondaryDns>
  </dnsInfo>
  <timeInfo>
    <clock>2012-10-16 13:17:27</clock>
    <ntpServer>time.vmware.com</ntpServer>
    <zone>GMT</zone>
  </timeInfo>
</vsmGlobalConfig>
```

---

## Resetting the Local Account Password

You can specify up to two pairs of hint questions and answers, which are saved as your security profile. You can reset your password by providing a hint question and answer along with a new password.

### Add Security Profile

You can specify up to two pairs of hint questions and answers.

### Example 2-6. Add security profile

---

Request:

PUT https://<vsm-ip>/api/2.0/services/usermgmt/securityprofile

Request Body:

```
<securityProfile>
  <passwordHintQuestionAnswer>
    <question></question>
    <answer></answer>
  </passwordHintQuestionAnswer>
  ...
  <passwordHintQuestionAnswer>
    <question></question>
    <answer></answer>
```

```

    </passwordHintQuestionAnswer>
  </securityProfile>

```

---

## Get Security Profile

You can retrieve the hint questions and answers for the logged in user.

### Example 2-7. Get security profile

---

Request:

GET https://<vsm-ip>/api/2.0/services/usermgmt/securityprofile

Response Body:

```

<?xml version="1.0" encoding="UTF-8"?>
<securityProfile>
  <passwordHintQuestionAnswer>
    <question>q1</question>
    <answer>a1</answer>
  </passwordHintQuestionAnswer>
</securityProfile>

```

---

## Get Password Hint Questions

You can retrieve the hint questions.

### Example 2-8. Get password hint questions

---

Request:

GET https://<vsm-ip>/api/2.0/services/usermgmt/passwordhint/userId

Response Body:

```

<?xml version="1.0" encoding="UTF-8"?>
<securityProfile>
  <passwordHintQuestionAnswer>
    <question>q1</question>
  </passwordHintQuestionAnswer>
</securityProfile>

```

---

## Reset Password

You can reset the password for a user by specifying the hint questions and answers for verification along with a new password.

**IMPORTANT** This URL does not require an authorization header. Hint questions and answers are used here for verification.

### Example 2-9. Reset password

---

Request:

PUT https://<vsm-ip>/api/2.0/services/usermgmt/passwordhint/admin

Request Body:

```

<securityProfile>
  <newPassword>ca$hC0w</newPassword>
  <passwordHintQuestionAnswer>
    <question>q1</question>
    <answer>a1</answer>
  </passwordHintQuestionAnswer>

```

---

```
</securityProfile>
```

---

## Monitoring vShield Manager reachability

You can verify that the vShield Manager is reachable.

**Example 2-10.** Verify that the vShield Manager is reachable

---

Request:

```
GET https://<vsm-ip>/api/2.0/global/heartbeat
```

---

## Working with vShield Manager Syslog Server Configuration

You can configure vShield manager to send system events and audit logs to a syslog server, retrieve current configuration, or delete the current configuration.

### Configure vShield Manager Syslog Server

You can configure vShield Manager to send logs to a syslog server. If a syslog server configuration exists, this call updates the configuration.

**Example 2-11.** Configure vShield Manager syslog server

---

Request:

```
PUT https://<vsm-ip>/api/2.0/services/syslog/config
```

Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
  <syslogServerConfig>
    <serverInfo>10.112.200.100:1000</serverInfo>
  </syslogServerConfig>
```

---

### Get vShield Manager Syslog Server Configuration

You can get the vShield Manager syslog server configuration.

**Example 2-12.** Get vShield Manager syslog server configuration

---

Request:

```
GET https://<vsm-ip>/api/2.0/services/syslog/config
```

---

### Delete vShield Manager Syslog Server Configuration

You can delete the vShield Manager syslog server configuration.

**Example 2-13.** Delete vShield Manager syslog server configuration

---

Request:

```
DELETE https://<vsm-ip>/api/2.0/services/syslog/config
```

---

## Querying vShield Manager Logs

You can retrieve vShield Manager system event and audit logs.

### Get vShield Manager System Events

You can retrieve vShield Manager system events.

---

#### Example 2-14. Get vShield Manager system events

---

Request:

```
GET https://<vsm-ip>/api/2.0/systemevent?startIndex=0\&pageSize=10
```

---

Where

- start index is an optional parameter which specifies the starting point for retrieving the logs. If this parameter is not specified, logs are retrieved from the beginning.
- page size is an optional parameter that limits the maximum number of entries returned by the API. The default value for this parameter is 256 and the valid range is 1-1024.

### Get vShield Manager Audit Logs

You can get vShield Manager audit logs.

---

#### Example 2-15. Get vShield Manager audit logs

---

Request:

```
GET https://<vsm-ip>/api/2.0/logging/auditlog?startIndex=0\&pageSize=10
```

---

Where

- start index is an optional parameter which specifies the starting point for retrieving the logs. If this parameter is not specified, logs are retrieved from the beginning.
- page size is an optional parameter that limits the maximum number of entries returned by the API. The default value for this parameter is 256 and the valid range is 1-1024.

## Querying vShield Manager Tech Support Log

You can get the path to the diagnostic log file for the vShield Manager. You can then send the diagnostic log to technical support for assistance in troubleshooting an issue.

---

#### Example 2-16. Get Tech Support Log File Path for a vShield Manager

---

Request:

```
GET https://<vsm-ip>/api/2.0/global/techSupportLogs
```

---

The technical support log is placed in a file at the following path, however the REST API has no provision for downloading it, and wget and curl do not have permission to download it, either. You can retrieve the log with vShield Manager by clicking **Settings & Reports > Configuration > Support > [Log Download] Initiate**.

```
/tech_support_logs/vsm/vshield_mgr_support_<date_time>GMT.log.gz
```

## User Management

The authentication and authorization APIs include methods to manage users and roles.



## Get Information About a User

You can retrieve information about a user.

### Example 2-17. Get information about a user

---

Request:

GET https://<vsm-ip>/api/2.0/services/usermgmt/user/<userId>

Request Body:

```
<userInfo>
  <objectId></objectId>
  <type>
    <typeName></typeName>
  </type>
  <name></name>
  <revision></revision>
  <objectTypeName></objectTypeName>
  <userId></userId>
  <fullName></fullName>
  <email></email>
  <isLocal></isLocal>
  <isEnabled></isEnabled>
  <isGroup></isGroup>
  <hasGlobalObjectAccess></hasGlobalObjectAccess>
  <accessControlEntry>
    <role></role>
    <resource>
      <objectId></objectId>
      <type>
        <typeName></typeName>
      </type>
      <name></name>
      <revision></revision>
      <objectTypeName></objectTypeName>
      <scope>
        <id></id>
        <objectTypeName></objectTypeName>
        <name></name>
      </scope>
    </resource>
    ...
  </accessControlEntry>
</userInfo>
```

---

User information includes user name, full name, email address, whether local or not, whether enabled, resource objects, roles, and scope.

## Create a Local User on vShield Manager

You can create a local vShield Manager user.

### Example 2-18. Create a local user

---

Request Header:

POST https://<vsm-ip>/api/2.0/services/usermgmt/user/local

Request Body:

```
<userInfo>
  <userId>somebody</userId>
  <password>123</password>
  <fullName>Person Somebody</fullName>
  <email>ps@y.com</email>
```

```

    <accessControlEntry>
      <role>security_admin</role>
      <resource>
        <resourceId></resourceId>
        ...
      </resource>
    </accessControlEntry>
  </userInfo>

```

---

## Update a Local User Account

You can update a local user account including password. If a password is not provided, the existing password is retained. The `<userId>` variable in the request header should be same as the one specified in XML. The API returns updated information for the user.

### Example 2-19. Update a local user account

---

Request Header:

PUT `https://<vsm-ip>/api/2.0/services/usermgmt/user/local/<userId>`

Request Body:

```

<userInfo>
  <userId>somebody</userId>
  <password>123</password>
  <fullName>Person Somebody</fullName>
  <email>ps@y.com</email>
  <accessControlEntry>
    <role>security_admin</role>
    <resource>
      <resourceId>datacenter-312</resourceId>
      ...
    </resource>
  </accessControlEntry>
</userInfo>

```

---

## Enable or Disable a User Account

You can disable or enable a user account, either local user or vCenter user. When a user account is created, the account is enabled by default.

### Example 2-20. Enable or disable a user account

---

Request:

PUT `https://<vsm-ip>/api/2.0/services/usermgmt/user/<userId>/enablestate/<value>`

---

The `<value>` can be 0 (zero) to disable the account, or 1 (one) to enable the account.

This API returns “204 No Content” if successful.

## Delete a User Account

The first API removes a local user account, or removes the VSM role assignment for a vCenter user, without affecting the vCenter account. The second API removes a vCenter user’s roles but is not allowed for local users.

### Example 2-21. Delete a user account

---

Request:

DELETE https://<vsm-ip>/api/2.0/services/usermgmt/user/<userId>

---

**Example 2-22. Delete a user role**

---

Request:

DELETE https://<vsm-ip>/api/2.0/services/usermgmt/role/<userId>

---

Both APIs return “204 No Content” if successful.<sup>7</sup>

## Role Management

When assigning or retrieving the role for a user, you cannot use a backslash (\) in the user name (userID parameter). Instead of specifying Domain\user1 as the user name, say user1@Domain.

### Get Role for a User

You can retrieve information about the role assigned to this user.

#### Example 2-23. Get user role

---

Request:

GET https://<vsm-ip>/api/2.0/services/usermgmt/role/<userId>

Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<accessControlEntry>
  <role></role>
  <resource>
    <objectId></objectId>
    <type>
      <typeName></typeName>
    </type>
    <name></name>
    <revision></revision>
    <objectTypeName></objectTypeName>
    <scope>
      <id></id>
      <objectTypeName></objectTypeName>
      <name></name>
    </scope>
  </resource>
  <resource>...</resource>
  ...
  ...
</accessControlEntry>
```

---

Possible roles are super\_user, vshield\_admin, enterprise\_admin, security\_admin, and auditor.

### Get Role for a vShield Manager Roles

You can retrieve information about users who have been assigned a vShield Manager role (local users as well as vCenter users with the vShield Manager role).

#### Example 2-24. Get user role

---

Request:

GET https://<vsm-ip>/api/2.0/services/usermgmt/users/vsm

Response Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<users>
  <userInfo>
    <objectId></objectId>
    <type>
      <typeName></typeName>
    </type><name></name>
    <revision></revision>
    <objectTypeName></objectTypeName>
    <userId></userId>
    <fullname></fullname>
    <email></email>
```

```

<isLocal></isLocal>
<isEnabled></isEnabled>
<isGroup>false</isGroup>
<hasGlobalObjectAccess></hasGlobalObjectAccess>
<accessControlEntry>
  <role></role>
  <resource>
    <objectId></objectId>
    <type>
      <typeName></typeName>
    </type>
    <name></name>
    <revision></revision>
    <objectTypeName></objectTypeName>
    <scope>
      <id>group-d1</id>
      <objectTypeName></objectTypeName>
      <name></name>
    </scope>
  </resource>
</accessControlEntry>
</userInfo>
<userInfo>
  ...
</userInfo>
</users>

```

---

Possible roles are super\_user, vshield\_admin, enterprise\_admin, security\_admin, and auditor.

## Add Role and Resources for a User

You can add role and accessible resources for the specified user. It affects only vCenter users, not local users. For local vShield Manager users, it displays the error “400: User already present.”

You cannot use a backslash (\) in the user name (userId parameter). Instead of specifying Domain\user1 as the user name, say user1@Domain.

Set isGroup=true to assign a role to a group isGroup=false to assign a role to a user.

### Example 2-25. Update user role

---

Request Header:

POST https://<vsm-ip>/api/2.0/usermgmt/role/<userId>?isGroup=true|false

Request Body:

```

<accessControlEntry>
  <role>new_role</role>
  <resource>
    <resourceId>resource-num</resourceId>
    ...
  </resource>
</accessControlEntry>

```

---

This API returns “204 No Content” if successful.

## Change User Role

You can update the role assignment for a given user. The API returns an output representation specifying a new <accessControlEntry> for the user.

### Example 2-26. Change user role

---

Request Header:

PUT https://<vsm-ip>/api/2.0/services/usermgmt/role/<userId>

Request Body:

```
<accessControlEntry>
  <role>new_role</role>
  <resource>
    <resourceId>resource-num</resourceId>
    ...
  </resource>
</accessControlEntry>
```

---

Possible roles are super\_user, vshield\_admin, enterprise\_admin, security\_admin, and auditor.

## Get List of Possible Roles

You can retrieve the possible roles in vShield Manager.

### Example 2-27. Get possible roles

---

Request:

GET https://<vsm-ip>/api/2.0/services/usermgmt/roles

Response Body:

```
<list>
  <string></string>
  <string></string>
  ...
</list>
```

---

## Get List of Scoping Objects

You can retrieve a list of objects that can be used to define a user's access scope.

### Example 2-28. Get scoping objects

---

Request:

GET https://<vsm-ip>/api/2.0/services/usermgmt/scopingobjects

Response Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<scopingObjects>
  <object>
    <objectId></objectId>
    <type>
      <typeName></typeName>
    </type>
    <name></name>
    <revision></revision>
    <objectTypeName></objectTypeName>
    <scope>
      <id></id>
      <objectTypeName></objectTypeName>
      <name></name>
    </scope>
  </object>
  <object>
    <objectId></objectId>
    <type>
      <typeName></typeName>
    </type>
    <name></name>
```

```

    <revision></revision>
    <objectTypeName></objectTypeName>
    <scope>
      <id></id>
      <objectTypeName></objectTypeName>
      <name></name>
    </scope>
  </object>
  ...
  ...
</scopingObjects>

```

---

The scoping objects are usually managed object references or vCenter Server names of datacenters and folders.

## Delete User Role

You can delete the role assignment for the specified vCenter user. Once this role is deleted, the user is removed from vShield Manager.

You cannot delete the role for a local user.

### Example 2-29. Delete role

---

Request:

```
DELETE https://<vsm-ip>/api/2.0/usermgmt/role/<user Id>
```

---

## Creating IPset and MACset Containers

You can create vShield containers based on IP addresses and MAC addresses. These APIs control two types of resources: vShield Manager scope object (global root, datacenter, or portgroup) and the IPset or MACset addresses.

## List IPsets Created on a Scope

You can retrieve all the IPsets that were created on the specified scope.

### Example 2-30. List IPsets on a scope

---

Request:

```
GET https://<vsm-ip>/api/2.0/services/ipset/<scope-moref>
```

---

The <scope-moref> can be global root, or a datacenter or portgroup of the vCenter to which vShield Manager is connected.

## Create an IPset on a Scope

You can create a new IPset on the specified scope.

### Example 2-31. Create IPset on a scope

---

Request:

```
POST https://<vsm-ip>/api/2.0/services/ipset/<scope-moref>
```

Request Body Example:

```

<ipset>
  <objectId>IPSet-1</objectId>
  <type>

```

```

    <typeName>IPSet</typeName>
  </type>
  <description>Test Description</description>
  <name>Test IPSet</name>
  <inheritanceAllowed>true</inheritanceAllowed>
  <revision>2</revision>
  <objectTypeName>IPSet<objectTypeName>
  <value>10.112.201.8-10.112.201.14</value>
</ipset>

```

---

The <scope-moref> can be global root, or a datacenter or portgroup of the vCenter to which vShield Manager is connected. In the request body example, inheritance is allowed (inheritanceAllowed is set to true). A range of IP addresses on the 10.112 net is specified (201.8 to 201.14).

## Get Details of an IPset

You can retrieve details about an IPset.

### Example 2-32. Get details of an IPset

---

Request:

```
GET https://<vsm-ip>/api/2.0/services/ipset/<ipset-id>
```

---

The <ipset-id> is as returned by listing the IPset on a scope.

## Modify an Existing IPset

You can modify an existing IPset and retrieve details about the modified IPset.

### Example 2-33. Modify an IPset

---

Request:

```
PUT https://<vsm-ip>/api/2.0/services/ipset/<ipset-id>
```

Request Body Example:

```

<ipset>
  <objectId />
  <type>
    <typeName />
  </type>
  <description>
    New Description
  </description>
  <name>TestIPSet2</name>
  <revision>0</revision>
  <objectTypeName />
  <value>10.112.201.8-10.112.201.21</value>
</ipset>

```

---

The <ipset-id> is as returned by listing the IPset on a scope. In the request body example, the IP address range is doubled.

## Delete an IPset

You can delete an IPset. The trailing boolean flag indicates forced or unforced delete. With forced delete, the object is deleted even if used in other places such as firewall rules, causing invalid referrals. For unforced delete, the object is deleted only if it is not used by other configuration; otherwise the delete fails.



**Example 2-34. Delete an IPset**

---

Request:

DELETE https://<vsm-ip>/api/2.0/services/ipset/<ipset-id>?force=<true|false>

---

No input representation is needed. On success, this request returns 200 HTTP OK.

**List MACsets Created on a Scope**

You can retrieve all the MACsets that were created on the specified scope.

**Example 2-35. List MACsets on a scope**

---

Request:

GET https://<vsm-ip>/api/2.0/services/macset/<scope-moref>

---

The <scope-moref> can be global root, or a datacenter or portgroup of the vCenter to which vShield Manager is connected.

**Create a MACset on a Scope**

You can create a MACset on the specified scope. On success, the API returns a string identifier for the new MACset.

**Example 2-36. Create MACset on a scope**

---

Request:

POST https://<vsm-ip>/api/2.0/services/macset/<scope-moref>

Request Body Example:

```
<macset>
  <objectId />
  <type>
    <typeName />
  </type>
  <description>Some description</description>
  <name>TestMACSet1</name>
  <revision>0</revision>
  <objectTypeName />
  <value>22:33:44:55:66:77,00:11:22:33:44:55,aa:bb:cc:dd:ee:ff</value>
</macset>
```

---

The <scope-moref> can be global root, datacenter or portgroup of the vCenter to which vShield Manager is connected. In the request body example, a comma-separated list of MAC addresses is specified.

**Get Details of a MACset**

You can retrieve details about a MACset.

**Example 2-37. Get details of a MACset**

---

Request:

GET https://<vsm-ip>/api/2.0/services/macset/<macset-id>

---

The <MACset-id> is as returned by listing the MACset on a scope.

## Modify an Existing MACset

You can modify an existing MACset and retrieve details about the modified MACset.

### Example 2-38. Modify details of a MACsets

---

Request:

PUT https://<vsm-ip>/api/2.0/services/macset/<MACset-id>

Request Body:

```
<macset>
  <objectId />
  <type>
    <typeName />
  </type>
  <description>Some description</description>
  <name>TestMACSet1</name>
  <revision>1</revision>
  <objectTypeName />
  <value>22:33:44:55:66:77,00:11:22:33:44:55</value>
</macset>
```

---

The <MACset-id> is as returned by listing the MACset on a scope. In the request body example, one MAC address fewer is specified.

## Delete a MACset

You can delete a MACset. The trailing boolean flag indicates forced or unforced delete. With forced delete, the object is deleted even if used in other places such as firewall rules, causing invalid referrals. For unforced delete, the object is deleted only if it is not used by other configuration; otherwise the delete fails.

### Example 2-39. Delete a MACset

---

Request:

DELETE https://<vsm-ip>/api/2.0/services/macset/<macset-id>

---

No input representation is needed. On success, this request returns 200 HTTP OK.

## Security Group Scope and Members

APIs are available for two types of resources:

- Scope – This identifies a vShield Manager scope object, which can either be a vCenter datacenter or a PortGroup (standard or distributed virtual switch). Security groups can only be created on valid scopes.
- Members – The security group object contains members.

## List Security Groups Created on a Scope

You can retrieve all the security groups that have been created on a specific scope.

### Example 2-40. Get existing security groups

---

Request:

GET https://<vsm-ip>/api/2.0/services/securitygroup/scope/<scope-moref>

---

The <scope-moref> could be the managed object reference of a datacenter or port group.

## Create Security Group on a Scope

You can create a new security group on the specified scope. Inheritance is not allowed.

### Example 2-41. Create new security group

---

Request:

POST https://<vsm-ip>/api/2.0/services/securitygroup/<scope-moref>

Request Body:

```
POST https://10.24.128.128/api/2.0/services/securitygroup/datacenter-31
<?xml version="1.0" encoding="UTF-8" ?>
<securitygroup>
  <objectId />
  <type>
    <typeName />
  </type>
  <description>
    Some description 2
  </description>
  <name>
    TestSecurityGroup2
  </name>
  <revision>
    0
  </revision>
  <objectTypeName />
</securitygroup>
```

---

## Get Members for a Scope

You can retrieve a list of applicable member elements that can be added to security groups created on a particular scope. Because security group allows only specific type of container elements to be added, this list helps you determine all possible valid elements that can be added.

### Example 2-42. Get members for a security group scope

---

Request:

GET https://<vsm-ip>/api/2.0/services/securitygroup/scope/<scope-moref>/members/

---

Note that this API command requires a slash (/) at the end. The request returns a long output representation of member objects.

## Get Security Group Details

You can retrieve the details about a security group.

### Example 2-43. Get details of a security group

---

Request:

GET https://<vsm-ip>/api/2.0/services/securitygroup/<securitygroup-id>

Response Body:

```
<securitygroup>
  <objectId>securitygroup-1</objectId>
  <type>
    <typeName>SecurityGroup</typeName>
  </type>
  <name>sg-669123615</name>
  <revision>2</revision>
```

```

<objectTypeName>SecurityGroup</objectTypeName>
<scope>
  <id>datacenter-2</id>
  <objectTypeName>Datacenter</objectTypeName>
  <name>mydc</name>
</scope>
<inheritanceAllowed>false</inheritanceAllowed>
<member>
  <objectId>vm-427</objectId>
  <type>
    <typeName>VirtualMachine</typeName>
  </type>
  <name>myvm</name>
  <revision>10</revision>
  <objectTypeName>VirtualMachine</objectTypeName>
  <scope>
    <id>domain-c893</id>
    <objectTypeName>ClusterComputeResource</objectTypeName>
    <name>mycluster</name>
  </scope>
</member>
</securitygroup>

```

---

## Modify a Security Group

You can modify an existing security group.

### Example 2-44. Modify a security group

---

Request:

PUT https://<vsm-ip>/api/2.0/services/securitygroup/<securitygroup-id>

Request Body:

```

<?xml version="1.0" encoding="UTF-8"?>
<securitygroup>
  <objectId> securitygroup-1 </objectId>
  <type>
    <typeName> SecurityGroup </typeName>
  </type>
  <description> Some description </description>
  <name> TestSecurityGroup </name>
  <revision> 4 </revision>
  <objectTypeName> SecurityGroup </objectTypeName>
  <member>
    <objectId> vm-213 </objectId>
    <type>
      <typeName> VirtualMachine </typeName>
    </type>
    <name> View-XP1 </name>
    <revision> 4 </revision>
    <objectTypeName> VirtualMachine </objectTypeName>
  </member>
  <member>
    <objectId> vm-214 </objectId>
    <type>
      <typeName> VirtualMachine </typeName>
    </type>
    <name> View-XP2 </name>
    <revision> 4 </revision>
    <objectTypeName> VirtualMachine </objectTypeName>
  </member>
</securitygroup>

```

---

## Delete a Security Group

You can delete an existing security group. The `force=` flag indicates if the delete should be forced or unforced. With forced delete, the object is deleted even if used in other places such as firewall rules, causing invalid referrals. For unforced delete, the object is deleted only if it is not used by other configuration; otherwise the delete fails.

---

### Example 2-45. Delete a security group

---

Request:

```
DELETE https://<vsm-ip>/api/2.0/services/securitygroup/<securitygroup-id>?force=<true|false>
```

---

No input representation is needed. On success, this request returns 200 HTTP OK.

## Add Member to Security Group

You can add a new member to a security group.

---

### Example 2-46. Add a member to a security group

---

Request:

```
PUT https://<vsm-ip>/api/2.0/services/securitygroup/<securitygroup-id>/members/<member-moref>
```

---

No input representation is needed. On success, this request returns 200 HTTP OK.

## Delete Member from Security Group

This API removes a member from a security group.

---

### Example 2-47. Delete member from a security group

---

Request:

```
DELETE https://<vsm-ip>/api/2.0/services/securitygroup/<securitygroup-id>/members/<member-moref>
```

---

No input representation is needed. On success, this request returns 200 HTTP OK.

## Transport Set for Services

The vShield transport set APIs are used to manipulate services, and control two types of resources:

- Scope – identifies the scope of a vShield Manager object, which can be either a vSphere datacenter or a port group (legacy or dvPortgroup). Services can be created on valid scopes or at a global level.
- Services – This is the main service object itself.

## Working with Service Groups

### List Service Groups on a Scope

You can retrieve a list of service groups that have been created on the scope specified by managed object reference `<moref>`.

---

### Example 2-48. List service groups on a given scope

---

Request:

```
GET https://<vsm-ip>/api/2.0/services/applicationgroup/<scope-moref>
```

**Request Body:**

```

<?xml version="1.0" encoding="UTF-8"?>
<list>
  <applicationGroup>
    <objectId>applicationgroup-1</objectId>
    <type>
      <typeName>ApplicationGroup</typeName>
    </type>
    <name>testglobalAG</name>
    <description></description>
    <revision>2</revision>
    <objectTypeName>ApplicationGroup</objectTypeName>
    <scope>
      <id>globalroot-0</id>
      <objectTypeName>GlobalRoot</objectTypeName>
      <name>Global</name>
    </scope>
    <extendedAttributes />
    <inheritanceAllowed>false</inheritanceAllowed>
    <member>
      <objectId>application-37</objectId>
      <type>
        <typeName>Application</typeName>
      </type>
      <name>SMTP</name>
      <revision>3</revision>
      <objectTypeName>Application</objectTypeName>
      <scope>
        <id>globalroot-0</id>
        <objectTypeName>GlobalRoot</objectTypeName>
        <name>Global</name>
      </scope>
      <extendedAttributes />
    </member>
  </applicationGroup>
</list>

```

---

A non-existent scope results in a 400 Bad Request error.

**Add Service Group to a Scope**

You can create a new service group on the specified scope.

**Example 2-49. Add a service group to a scope****Request:**

POST https://<vsm-ip>/api/2.0/services/applicationgroup/<scope-moref>

**Request Body:**

```

<application>
  <description>Some description</description>
  <name>TestApplication1</name>
  <revision>0</revision>
  <inheritanceAllowed>false</inheritanceAllowed>
</application>

```

---

For applicationProtocol, possible values are:

- TCP
- UDP
- ORACLE\_TNS
- FTP

- SUN\_RPC\_TCP
- SUN\_RPC\_UDP
- MS\_RPC\_TCP
- MS\_RPC\_UDP
- NBNS\_BROADCAST
- NBDG\_BROADCAST
- ICMP
- IGMP
- IPCOMP
- IPV6ROUTE
- IPV6FRAG
- IPV6ICMP
- IPV6NONXT
- IPV6OPTS
- RSVP
- GRE
- ESP
- AH
- L2TP
- SCTP
- IPV4
- ARP
- X25
- LLC
- FR\_ARP
- BPQ
- DEC
- DNA\_DL
- DNA\_RC
- DNA\_RT
- LAT
- DIAG
- CUST
- SCA
- TEB
- RAW\_FR
- RARP
- AARP
- ATALK
- IEEE\_802\_1Q
- IPX
- NETBEUI
- IPV6
- PPP
- ATMMPOA
- PPP\_DISC
- PPP\_SES
- ATMFATE
- LOOP

- L2\_OTHERS
- L3\_OTHERS

Only TCP and UDP support comma separated port numbers and dash separated port ranges. Other protocols support a single port number only.

On success, this call returns a string identifier for the newly created application, for instance Application-1. The location header in the reply contains the relative path of the created Application and can be used for further GET, PUT, and DELETE calls.

## Get Details of a Service Group

You can retrieve details about the service group specified by <applicationgroup-id> as returned by the call shown in [Example 2-54](#).

### Example 2-50. Retrieve details about a service group

---

Request:

```
GET https://<vsm-ip>/api/2.0/services/applicationgroup/<applicationgroup-id>
```

---

A non-existent application ID results in a 404 Not Found error.

## Modify Service Group Details

You can modify the name, description, applicationProtocol, or port value of a service group.

### Example 2-51. Modify service group

---

Request:

```
PUT https://<vsm-ip>/api/2.0/services/applicationgroup/<applicationgroup-id>
```

Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<applicationGroup>
  <objectId>applicationgroup-1</objectId>
  <type>
    <typeName>ApplicationGroup</typeName>
  </type>
  <name>testglobalAG-updated</name>
  <description>Updated with description</description>
  <revision>2</revision>
  <objectTypeName>ApplicationGroup</objectTypeName>
  <scope>
    <id>globalroot-0</id>
    <objectTypeName>GlobalRoot</objectTypeName>
    <name>Global</name>
  </scope>
  <extendedAttributes />
  <inheritanceAllowed>false</inheritanceAllowed>
  <member>
    <objectId>application-37</objectId>
    <type>
      <typeName>Application</typeName>
    </type>
    <name>SMTP</name>
    <revision>3</revision>
    <objectTypeName>Application</objectTypeName>
    <scope>
      <id>globalroot-0</id>
      <objectTypeName>GlobalRoot</objectTypeName>
      <name>Global</name>
    </scope>
  </member>
</applicationGroup>
```



```
</member>
</applicationGroup>
```

---

The call returns XML describing the modified service.

### Delete Service Group from Scope

You can delete a service group by specifying its <applicationgroup-id>. The force= flag indicates if the delete should be forced or unforced. For forced deletes, the object is deleted irrespective of its use in other places such as firewall rules, which invalidates other configurations referring to the deleted object. For unforced deletes, the object is deleted only if it is not being used by any other configuration. The default is unforced (false).

#### Example 2-52. Delete service group

---

Request:

```
DELETE https://<vsm-ip>/api/2.0/services/applicationgroup/<applicationgroup-id>?force=<true|false>
```

---

## Working with Services

### List Services on a Scope

You can retrieve a list of services that have been created on the scope specified by managed object reference <moref>.

#### Example 2-53. List services on a given scope

---

Request:

```
GET https://<vsm-ip>/api/2.0/services/application/scope/<moref>
```

---

A non-existent scope results in a 400 Bad Request error.

### Add Service to a Scope

You can create a new service on the specified scope.

#### Example 2-54. Add a service to a scope

---

Request:

```
POST https://<vsm-ip>/api/2.0/services/application/scope/<moref>
```

Request Body:

```
<application>
  <objectId>
  <type>
    <typeName/>
  </type>
  <description>Some description</description>
  <name>TestApplication1</name>
  <revision>0</revision>
  <objectTypeName/>
  <element>
    <applicationProtocol>UDP</applicationProtocol>
    <value>9,22-31,44</value>
  </element>
</application>
```

---

For applicationProtocol, possible values are:

- TCP
- UDP
- ORACLE\_TNS
- FTP
- SUN\_RPC\_TCP
- SUN\_RPC\_UDP
- MS\_RPC\_TCP
- MS\_RPC\_UDP
- NBNS\_BROADCAST
- NBDG\_BROADCAST
- ICMP
- IGMP
- IPCOMP
- IPV6ROUTE
- IPV6FRAG
- IPV6ICMP
- IPV6NONXT
- IPV6OPTS
- RSVP
- GRE
- ESP
- AH
- L2TP
- SCTP
- IPV4
- ARP
- X25
- LLC
- FR\_ARP
- BPQ
- DEC
- DNA\_DL
- DNA\_RC
- DNA\_RT
- LAT
- DIAG
- CUST
- SCA
- TEB
- RAW\_FR
- RARP
- AARP
- ATALK
- IEEE\_802\_1Q
- IPX
- NETBEUI
- IPV6
- PPP
- ATMMPOA

- PPP\_DISC
- PPP\_SES
- ATMFATE
- LOOP
- L2\_OTHERS
- L3\_OTHERS

Only TCP and UDP support comma separated port numbers and dash separated port ranges. Other protocols support a single port number only.

On success, this call returns a string identifier for the newly created application, for instance Application-1. The location header in the reply contains the relative path of the created Application and can be used for further GET, PUT, and DELETE calls.

### Get Details of a Service

You can retrieve details about the service specified by <applicationgroup-id> as returned by the call shown in [Example 2-54](#).

---

#### Example 2-55. Retrieve details about a service

Request:

```
GET https://<vsm-ip>/api/2.0/services/applicationgroup/<applicationgroup-id>
```

---

A non-existent application ID results in a 404 Not Found error.

### Modify Service Details

You can modify the name, description, applicationProtocol, or port value of a service.

---

#### Example 2-56. Modify application

Request:

```
PUT https://<vsm-ip>/api/2.0/services/applicationgroup/<applicationgroup-id>
```

Request Body:

```
<application>
  <objectId>Application-1</objectId>
  <type>
    <typeName>Application</typeName>
  </type>
  <description>Some description</description>
  <name>TestApplication</name>
  <revision>2</revision>
  <objectTypeName>Application</objectTypeName>
  <element>
    <applicationProtocol>TCP</applicationProtocol>
    <value>10,29-30,45</value>
  </element>
</application>
```

---

The call returns XML describing the modified service.

### Delete Service from Scope

You can delete a service by specifying its <applicationgroup-id>. The force= flag indicates if the delete should be forced or unforced. For forced deletes, the object is deleted irrespective of its use in other places such as firewall rules, which invalidates other configurations referring to the deleted object. For unforced deletes, the object is deleted only if it is not being used by any other configuration. The default is unforced (false).

**Example 2-57. Delete service**

---

Request:

DELETE https://&lt;vsm-ip&gt;/api/2.0/services/applicationgroup/&lt;applicationgroup-id&gt;?force=&lt;true|false&gt;

## Working with the Members of a Service

### Query Service Members

You can get a list of member elements that can be added to the service groups created on a particular scope. Since service group allows only either services or other service groups as members to be added, this helps you get a list of all possible valid elements that can be added to the service.

**Example 2-58. Retrieve member elements**

---

Request:

GET https://&lt;vsm-ip&gt;/api/2.0/services/applicationgroup/scope/&lt;scope-moref&gt;/members

Response Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<list>
  <basicinfo>
    <objectId>applicationgroup-3</objectId>
    <type>
      <typeName>ApplicationGroup</typeName>
    </type>
    <name>AGDC-1</name>
    <description>AG created in DC</description>
    <revision>1</revision>
    <objectTypeName>ApplicationGroup</objectTypeName>
    <scope>
      <id>datacenter-2</id>
      <objectTypeName>Datacenter</objectTypeName>
      <name>Datacenter</name>
    </scope>
    <extendedAttributes />
  </basicinfo>
  <basicinfo>
    <objectId>application-36</objectId>
    <type>
      <typeName>Application</typeName>
    </type>
    <name>ORACLE_TNS</name>
    <revision>2</revision>
    <objectTypeName>Application</objectTypeName>
    <scope>
      <id>globalroot-0</id>
      <objectTypeName>GlobalRoot</objectTypeName>
      <name>Global</name>
    </scope>
    <extendedAttributes />
  </basicinfo>
  <basicinfo>
    <objectId>application-37</objectId>
    <type>
      <typeName>Application</typeName>
    </type>
    <name>SMTP</name>
    <revision>3</revision>
    <objectTypeName>Application</objectTypeName>
    <scope>
      <id>globalroot-0</id>
      <objectTypeName>GlobalRoot</objectTypeName>
```

```

        <name>Global</name>
      </scope>
      <extendedAttributes />
    </basicinfo>
  </list>

```

---

### Add a Member to the Service

You can add a member to the service.

#### Example 2-59. Add member

---

Request:

```

PUT https://<vsm-ip>/api/2.0/services/applicationgroup/<applicationgroup-id>/members/
      <member-moref>

```

---

### Delete a Member from the Service

You can delete a member from the service.

#### Example 2-60. Add member

---

Request:

```

DELETE https://<vsm-ip>/api/2.0/services/applicationgroup/<applicationgroup-id>/members/
      <member-moref>

```

---

## Querying Object IDs

This section describes how to retrieve the IDs for the objects in your virtual inventory.

### Query Datacenter MOID

- 1 In a web browser, type the following:

```
http://<vCenter-IP>/mob
```

- 2 Click content.
- 3 Click on the rootFolder value.
- 4 Click on the childEntity value.

The datacenter MOID is displayed on top of the window.

### Query Datacenter ID

- 1 In a web browser, type the following:

```
http://<vCenter-IP>/mob
```

- 2 Click content.
- 3 Click on the rootFolder value.
- 4 Click on the childEntity value.

The datacenter value is the datacenter ID.

## Query Host ID

- 1 In a web browser, type the following:

`http://<vCenter-IP>/mob`

- 2 Click content.
- 3 Click on the rootFolder value.
- 4 Click on the childEntity value.
- 1 Click on the datacenter value.

The host value is the host ID.

## Query Portgroup ID

- 1 In a web browser, type the following:

`http://<vCenter-IP>/mob`

- 2 Click content.
- 3 Click on the rootFolder value.
- 4 Click on the childEntity value.
- 5 Click on the datacenter value.
- 6 Click on the host value.

The network property value is the portgroup ID.

# ESX Host Preparation for vShield App, vShield Endpoint, and vShield Data Security

# 3

You can extend the capabilities of vShield by adding the following services: vShield App, vShield Endpoint, and vShield Edge. You must prepare each ESX host in your environment for these services. The vShield Manager OVA file contains the drivers and files necessary to install all additional services.

This chapter includes the following topics:

- [“Installing Licenses for vShield Edge, vShield App, and vShield Endpoint”](#) on page 47
- [“Installing vShield App and vShield Endpoint Services on an ESX Host”](#) on page 47
- [“Installing vShield Data Security”](#) on page 49
- [“Upgrading vShield Data Security”](#) on page 49
- [“Getting the Installation Status of vShield Services on an ESX Host”](#) on page 50
- [“Uninstalling vShield Services from an ESX Host”](#) on page 50
- [“Uninstalling vShield Data Security”](#) on page 50

---

**IMPORTANT** All vShield REST requests require authorization. See [“Using the vShield REST API”](#) on page 16 for details about basic authorization.

---

## Installing Licenses for vShield Edge, vShield App, and vShield Endpoint

You must install licenses for vShield Edge, vShield App, and vShield Endpoint before installing these components. You can install these licenses by using the vSphere Client.

- 1 From a vSphere Client host that is connected to a vCenter Server system, select **Home > Licensing**.
- 2 For the report view, select **Asset**.
- 3 Right-click a vShield asset and select **Change license key**.
- 4 Select **Assign a new license key** and click **Enter Key**.
- 5 Enter the license key, enter an optional label for the key, and click **OK**.
- 6 Click **OK**.
- 7 Repeat these steps for each vShield component for which you have a license.

## Installing vShield App and vShield Endpoint Services on an ESX Host

To shorten the time to deployment, you can install vShield App and vShield Endpoint services on an ESX host by using a single REST call. You can do this by including `VszInstallParams` and `EpsecInstallParams` in the POST body.



**CAUTION** Do not install vShield App (or vShield Zones) on the ESX host where vCenter Server is running, otherwise vShield App could interfere with vSphere management traffic.

You must specify the host ID of the target ESX host to install all services.

See [“ESX Host Preparation and Uninstallation Schema”](#) on page 228.

---

**Example 3-1.** Install a vShield App and vShield Endpoint on an ESX host

---

Request

POST https://<vsm-ip>/api/1.0/vshield/<host-id>

Request Body

```
<VshieldConfiguration>
  <VszInstallParams>
    <DatastoreId>datastore-5035</DatastoreId>
    <ManagementPortSwitchId>network-4485</ManagementPortSwitchId>
    <MgmtInterface>
      <IpAddress>10.112.196.245</IpAddress>
      <NetworkMask>255.255.252.0</NetworkMask>
      <DefaultGw>10.112.199.253</DefaultGw>
    </MgmtInterface>
  </VszInstallParams>
  <EpsecInstallParams>true</EpsecInstallParams>
  <InstallAction>install</InstallAction>
</VshieldConfiguration>
```

---

ESX host preparation requires the following elements:

- **DatastoreId:** VC MOID of the datastore on which the vShield App service virtual machine files will be stored. For information on retrieving the datacenter ID, see [“Querying Object IDs”](#) on page 45.
- **ManagementPortSwitchId:** VC MOID of the port group that will host the management port of the vShield App.
- **MgmtInterface**
  - **IpAddress:** IP address to be assigned to the management port of the vShield App. This IP address must be able to communicate with the vShield Manager.
  - **NetworkMask:** Subnet mask associated with the IP address assigned to the management interface of the vShield App.
  - **DefaultGw:** IP address of the default gateway.

After installation of all components is complete, do the following:

- **vShield App:** At this point, vShield App installation is complete. Each vShield App inherits global firewall rules set in the vShield Manager. The default firewall rule set allows all traffic to pass. You must configure blocking rules to explicitly block traffic. To configure App Firewall rules, see [“Configuring Firewall Rules for vCenter”](#) on page 172.
- **vShield Endpoint:** To complete installation, see [“vShield Endpoint Management”](#) on page 195.

You can install a single service by identifying only that service in the POST body. In [Example 3-2](#), only vShield App is installed, as identified by inclusion of the VszInstallParams element only.

---

**Example 3-2.** Install a vShield App only

---

Request:

POST https://<vsm-ip>/api/1.0/vshield/<host-id>/vsz

Request Body:



```

<VshieldConfiguration>
  <VszInstallParams>
    <DatastoreId>datastore-5131</DatastoreId>
    <ManagementPortSwitchId>network-5134</ManagementPortSwitchId>
    <MgmtInterface>
      <IpAddress>10.112.196.245</IpAddress>
      <NetworkMask>255.255.252.0</NetworkMask>
      <DefaultGw>10.112.199.253</DefaultGw>
    </MgmtInterface>
  </VszInstallParams>
  <InstallAction>install</InstallAction>
</VshieldConfiguration>

```

---

## Installing vShield Data Security

You can install vShield Data Security on a host that has vShield Endpoint installed.

### Example 3-3. Install vShield Data Security on an ESX host

---

Request:

POST https://<vsm-ip>/api/1.0/vshield/<host-id>

Request Body:

```

<VshieldConfiguration>
  <VsdsInstallParams>
    <DatastoreId>datastore-5035</DatastoreId>
    <PortGroupId>network-12</PortGroupId>
    <MgmtInterface>
      <IpAddress>10.112.196.245</IpAddress>
      <NetworkMask>255.255.252.0</NetworkMask>
      <DefaultGw>10.112.199.253</DefaultGw>
    </MgmtInterface>
  </VsdsInstallParams>
  <InstallAction>install</InstallAction>
</VshieldConfiguration>

```

---

Where <host-id> is the MOID of the ESX host where vShield Data Security should be installed.

## Upgrading vShield Data Security

You can upgrade vShield Data Security on a host without having to provide configuration parameters.

### Example 3-4. Upgrade vShield Data Security on an ESX host

---

Request:

POST https://<vsm-ip>/api/1.0/vshield/<host-id>

Request Body:

```

<VshieldConfiguration>
  <VsdsInstallParams></VsdsInstallParams>
  <InstallAction>upgrade</InstallAction>
</VshieldConfiguration>

```

---

Where <host-id> is the MOID of the ESX host where vShield Data Security should be upgraded.

## Getting the Installation Status of vShield Services on an ESX Host

You can retrieve the installation or uninstallation status of vShield services on an ESX host to track progress as complete or not initiated. If neither of these operations is in progress, the response includes the list of installed services on the ESX host.

**Example 3-5.** Get vShield service installation status on an ESX host

---

Request:

GET https://<vsm-ip>/api/1.0/vshield/<host-id>

---

## Uninstalling vShield Services from an ESX Host

You must unregister SVMs before uninstalling vShield Endpoint from the ESX host.

**Example 3-6.** Uninstall vShield Endpoint

---

Request:

DELETE https://<vsm-ip>/api/1.0/vshield/<host-id>/epsec

---

**Example 3-7.** Uninstall a vShield App only

---

Request:

DELETE https://<vsm-ip>/api/1.0/vshield/<host-id>/vsz

---

## Uninstalling vShield Data Security

You can uninstall vShield Data Security on a host.

**Example 3-8.** Uninstall vShield Data Security

---

Request:

DELETE https://<vsm-ip>/api/1.0/vshield/<host-id>/vsds

---

Where <host-id> is the MOID of the ESX host where vShield Data Security should be deleted.

# vShield Edge Installation and Upgrade

# 4

After ESX host preparation is complete, you can secure internal networks by installing a vShield Edge.

For information on retrieving objects IDs, see [“Querying Object IDs”](#) on page 45.

This chapter includes the following topics:

- [“Installing a vShield Edge”](#) on page 51
- [“Running Queries on all vShield Edges”](#) on page 53
- [“Upgrading vShield Edge”](#) on page 55
- [“Deleting a vShield Edge”](#) on page 55

---

**IMPORTANT** All vShield REST requests require authorization. See [“Using the vShield REST API”](#) on page 16 for details about basic authorization.

---

## Installing a vShield Edge

You install a vShield Edge on a datacenter and can add up to ten internal or external interfaces. Each datacenter can have multiple vShield Edge instances.

The vShield Edge installation API copies the vShield Edge OVF from the vShield Manager to the specified datastore and deploys a vShield Edge on the given datacenter. After the vShield Edge is installed, the virtual machine powers on and initializes according to the given network configuration. If an appliance is added, it is deployed with the specified configuration.

Installing a vShield Edge instance adds a virtual machine to the vCenter Server inventory, which is mirrored in the vShield Manager user interface. You must specify an IP address for the management interface, and you may name the vShield Edge instance.

The configuration you specify when you install a vShield Edge is stored in the database. If an appliance is added, the configuration is applied to it and it is deployed.

**NOTE** Do not use hidden/system resource pool IDs as they are not supported on the UI.

### Example 4-1. Install a vShield Edge

---

Request:

POST https://<vsm-ip>/api/3.0/edges

Request Body:

```
<edge>
<datacenterMoid>datacenter-2</datacenterMoid>
<name>org1-edge</name>                                <!-- optional. Default is vShield-<edgeId>. Used as a vm name on VC appended by
               "-<haIndex>" -->
<description>Description for the edge gateway</description> <!-- optional -->
<tenant>org1</tenant>                                <!-- optional. Will be used in syslog messages -->
```

```

<fqdn>org1edge1</fqdn>                                <!-- optional. Default is vShield-<edgeId>. Used to set hostname on the vm.
                Appended by "-<haIndex>" -->
<vseLogLevel>info</vseLogLevel>                        <!-- optional. Default is info. Other possible values are EMERGENCY, ALERT,
                CRITICAL, ERROR, WARNING, NOTICE, DEBUG -->
<enableAesni>false</enableAesni>                       <!-- optional. Default is true -->
<enableFips>true</enableFips>                           <!-- optional. Default is false -->
<enableTcpLoose>false</enableTcpLoose>                 <!-- optional. Default is false -->
<appliances>
  <applianceSize>large</applianceSize>                 <!-- optional, Possible values are compact | large | XLarge. Default is compact
  -->
  <appliance>
    <resourcePoolId>resgroup-53</resourcePoolId>
    <datastoreId>datastore-29</datastoreId>
    <hostId>host-28</hostId>                            <!-- optional -->
    <vmFolderId>group-v38</vmFolderId>                 <!-- optional -->
    <customField>                                       <!-- optional -->
      <key>system.service.vmware.vsla.main01</key>
      <value>string</value>
    </customField>
    <cpuReservation>                                    <!-- optional -->
      <limit>2399</limit>
      <reservation>500</reservation>
      <shares>500</shares>
    </cpuReservation>
    <memoryReservation>                                <!-- optional -->
      <limit>5000</limit>
      <reservation>500</reservation>
      <shares>20480</shares>
    </memoryReservation>
  </appliance>
</appliances>
<vnics>
  <vnic>
    <index>0</index>
    <name>internal0</name>                              <!-- optional. Format of system default names is vNic0 ... vNic9 -->
    <type>INTERNAL</type>                              <!-- optional. Default is internal -->
    <portgroupId>network-114</portgroupId>
    <addressGroups>
      <addressGroup>                                    <!-- Vnic can be configured to have more than one addressGroup/subnets -->
        <primaryAddress>192.168.3.1</primaryAddress> <!-- This is mandatory for an addressGroup -->
        <secondaryAddresses>                            <!-- Optional. Should be used to add/defined other IPs used for NAT,
                LB, VPN, etc -->
          <ipAddress>192.168.3.2</ipAddress>
          <ipAddress>192.168.3.3</ipAddress>             <!-- Optional. This way multiple IP Addresses can be assigned
                to a vnic/interface -->
        </secondaryAddresses>
        <subnetMask>255.255.255.0</subnetMask>
      </addressGroup>
    </addressGroups>
    <macAddress>                                         <!-- optional. When not specified, macAddresses will be managed by vCenter
                Server-->
    <edgeVmHaIndex>0</edgeVmHaIndex>
    <value>00:50:56:01:03:23</value>
  </macAddress>
  <fenceParameter>                                     <!-- optional -->
    <key>ethernet0.filter1.param1</key>
    <value>1</value>
  </fenceParameter>
  <mtu>1500</mtu>                                       <!-- optional. Default is 1500 -->
  <enableProxyArp>true</enableProxyArp>               <!-- optional. Default is false -->
  <enableSendRedirects>true</enableSendRedirects>      <!-- optional. Default is true -->
  <isConnected>true</isConnected>                     <!-- optional. Default is false -->
  <inShapingPolicy>                                    <!-- optional -->
    <averageBandwidth>200000000</averageBandwidth>
    <peakBandwidth>200000000</peakBandwidth>
    <burstSize>0</burstSize>
    <enabled>true</enabled>
    <inherited>false</inherited>
  </inShapingPolicy>

```

```

        </inShapingPolicy>
    </outShapingPolicy>                                <!-- optional -->
        <averageBandwidth>400000000</averageBandwidth>
        <peakBandwidth>400000000</peakBandwidth>
        <burstSize>0</burstSize>
        <enabled>true</enabled>
        <inherited>>false</inherited>
    </outShapingPolicy>
</vnic>
</vnics>
<cliSettings>                                <!-- optional. Default user/pass is admin/default, and remoteAccess is false (i.e. disabled)
-->
    <userName>vmware123</userName>                <!-- When you change the userName, you are overwriting the current
userName. -->
    <password>mod-another!!123pass</password>        <!-- The password should be atleast 7 characters long, must be a mix of
alphabets, digits and special characters. Must contain at least 1 special character and 1 digit -->
    <remoteAccess>true</remoteAccess>                <!-- Indicates whether cli console access over ssh is enabled. Yu must open
relevant firewall rules to allow traffic on port 22. It is recommended to restrict ssh access to Edge cli to only
a limited ip addresses, so firewall rules must be opened cautiously. -->
</cliSettings>
<autoConfiguration>                            <!-- Optional. Default is enabled with rulePriority high -->
    <enabled>true</enabled>
    <rulePriority>high</rulePriority>                <!-- Optional. Default is high. Other possible value is low -->
</autoConfiguration>
</edge>

```

---

**IMPORTANT** The location header returns the edgeId of the installed vShield Edge. You must use this ID to configure and manage this vShield Edge instance.

## Running Queries on all vShield Edges

You can run several queries to get information on all vShield Edges in your environment.

Optional parameters are:

- pageSize – total number of vShield Edge instances to be listed on one page. Default pageSize is 256.
- startIndex – retrieve vShield Edge instances from the specified start index. Default startIndex is 0.
- sortOrderAscending – true for sort in ascending order and false for sort in descending order. Default is true which is ascending.
- sortBy – sort vShield Edge instances with the specified column name (supported columns are id, name, description, tenantId, and size). Default is id.

### Example 4-2. Querying vShield Edge Configurations

---

Get summary of all vShield Edge instances:

```
GET https://<vsm-ip>/api/3.0/edges/
```

Get summary of all vShield Edges with specified tenant:

```
GET https://<vsm-ip>/api/3.0/edges/?tenant=<tenantId>
```

Get summary of all vShield Edges which has one interface on specified port-group:

```
GET https://<vsm-ip>/api/3.0/edges/?pg=<pgModId>
```

Get summary of all vShield Edges which has the specified tenant and port-group:

```
GET https://<vsm-ip>/api/3.0/edges/?tenant=<tenant>&pg=<pgModId>
```

Get summary of all vShield Edges which are installed on the specified datacenter:

```
GET https://<vsm-ip>/api/3.0/edges/?datacenter=<datacenterMoid>
```

---

**Example 4-3. Query all vShield Edge instances**

---

Request:

GET https://&lt;vsm-ip&gt;/api/3.0/edges/

Response Body:

```

<edgeSummaries>
  <edgeSummary>
    <objectId>edge-29</objectId>
    <type>
      <typeName>Edge</typeName>
    </type>
    <name>test-name</name>
    <description>edge description</description>
    <revision>1</revision>
    <objectTypeName>Edge</objectTypeName>
    <id>edge-29</id>
    <state>deployed</state>
    <datacenterMoid>datacenter-2</datacenterMoid>
    <apiVersion>3.0</apiVersion>
    <recentJobInfo>
      <jobId>jobdata-15</jobId>
      <message>Configuring traffic shaping policy on disconnected vnic '0' is not allowed.</message>
      <status>FAILED</status>
    </recentJobInfo>
    <numberOfConnectedVnics>2</numberOfConnectedVnics>
    <appliancesSummary>
      <vmVersion>5.1.0</vmVersion>
      <applianceSize>compact</applianceSize>
      <fqdn>vShieldEdge-dvportgroup-30</fqdn>
      <numberOfDeployedVms>1</numberOfDeployedVms>
    </appliancesSummary>
    <featureCapabilities>
      <featureCapability>
        <service>firewall</service>
        <isLicensed>true</isLicensed>
        <maximumAllowedConfig>0</maximumAllowedConfig>
      </featureCapability>
      <featureCapability>
        <service>sslvpn</service>
        <isLicensed>true</isLicensed>
        <maximumAllowedConfig>0</maximumAllowedConfig>
      </featureCapability>
      <featureCapability>
        <service>dns</service>
        <isLicensed>true</isLicensed>
        <maximumAllowedConfig>0</maximumAllowedConfig>
      </featureCapability>
      <featureCapability>
        <service>staticRouting</service>
        <isLicensed>true</isLicensed>
        <maximumAllowedConfig>0</maximumAllowedConfig>
      </featureCapability>
      <featureCapability>
        <service>highAvailability</service>
        <isLicensed>true</isLicensed>
        <maximumAllowedConfig>0</maximumAllowedConfig>
      </featureCapability>
      <featureCapability>
        <service>syslog</service>
        <isLicensed>true</isLicensed>
        <maximumAllowedConfig>0</maximumAllowedConfig>
      </featureCapability>
      <featureCapability>
        <service>loadBalancer</service>
        <isLicensed>true</isLicensed>
        <maximumAllowedConfig>0</maximumAllowedConfig>
      </featureCapability>
    </featureCapabilities>
  </edgeSummary>
</edgeSummaries>

```

```

    </featureCapability>
    <featureCapability>
      <service>ipsec</service>
      <isLicensed>true</isLicensed>
      <maximumAllowedConfig>0</maximumAllowedConfig>
    </featureCapability>
    <featureCapability>
      <service>dhcp</service>
      <isLicensed>true</isLicensed>
      <maximumAllowedConfig>0</maximumAllowedConfig>
    </featureCapability>
    <featureCapability>
      <service>nat</service>
      <isLicensed>true</isLicensed>
      <maximumAllowedConfig>0</maximumAllowedConfig>
    </featureCapability>
    <timestamp>1332857004585</timestamp>
  </featureCapabilities>
</edgeSummary>
</edgeSummaries>

```

---

## Upgrading vShield Edge

Upgrades vShield Edge to version 5.1

### Example 4-4. Upgrade vShield Edge

---

Request:

POST https://<vsm-ip>/api/2.0/networks/<portGroupID>/edge/upgrade

---

**IMPORTANT** The location header returns the edgeId of the upgraded vShield Edge. You must use this ID to configure and manage this vShield Edge instance.

If vShield Edge in the previous release was installed using hidden/system resource pool IDs, the UI may show unusual behavior.

## Deleting a vShield Edge

You can delete a vShield Edge instance. Appliances associated with the vShield Edge instance are deleted as well.

### Example 4-5. Delete a vShield Edge

---

Request:

DELETE https://<vsm-ip>/api/3.0/edges/<edgeId>

---





# vShield Edge Management

---

You can manage vShield Edge services and firewall policies with the REST API. You can install Edge, post and delete configurations, and get status of various services.

**NOTE** Do not use hidden/system resource pool IDs as they are not supported on the UI.

This chapter includes the following topics:

- [“Running Queries on a Specific vShield Edge”](#) on page 58
- [“Working with Appliances”](#) on page 66
- [“Working with Interfaces”](#) on page 69
- [“Configuring Edge Services”](#) on page 74
  - [“Manage Auto Configuration Settings”](#) on page 142
  - [“Configure Firewall”](#) on page 75
  - [“Configure NAT”](#) on page 81
  - [“Configure Routing”](#) on page 85
  - [“Configure DNS Servers”](#) on page 87
  - [“Configure DHCP”](#) on page 89
  - [“Configure Certificates”](#) on page 93
  - [“Configure IPSEC VPN”](#) on page 96
  - [“Managing SSL VPN”](#) on page 100
  - [“Configure Load Balancer”](#) on page 129
  - [“Configure DNS Servers”](#) on page 87
  - [“Configure High Availability \(HA\)”](#) on page 140
- [“Force Syncing vShield Edge”](#) on page 141
- [“Configuring Advanced Options for vShield Edge”](#) on page 141
- [“Replacing the Configuration of a vShield Edge”](#) on page 143
- [“Redeploying vShield Edge Appliances”](#) on page 147
- [“Managing CLI Credentials and Access”](#) on page 147
- [“Debugging and Support”](#) on page 149

---

**IMPORTANT** All vShield REST requests require authorization. See [“Using the vShield REST API”](#) on page 16 for details about basic authorization.

---

## Running Queries on a Specific vShield Edge

You can retrieve the list of installed vShield instances filtered by datacenter or port group/tenant ID.

Retrieves summary of all vShield Edge instances in your inventory.

### Query vShield Edge Details

Retrieves the details of the specified vShield Edge.

#### Example 5-1. Query vShield Edge details

---

Request:

GET https://<vsm-ip>/api/3.0/edges/<edgeId>

Response Body:

```
<edge>
  <id>edge-79</id>
  <version>5</version>
  <description>testEdge</description>
  <status>deployed</status>
  <datacenterMoid>datacenter-2</datacenterMoid>
  <datacenterName>datacenterForEdge</datacenterName>
  <name>testEdge</name>
  <fqdn>testEdge</fqdn>
  <enableAesni>true</enableAesni>
  <enableFips>false</enableFips>
  <enableTcpLoose>false</enableTcpLoose>
  <vseLogLevel>info</vseLogLevel>
  <vnics>
    <vnic>
      <index>0</index>
      <name>uplink-vnic-network-2581</name>
      <type>uplink</type>
      <portgroupId>network-2581</portgroupId>
      <portgroupName>Mgmt</portgroupName>
      <addressGroups>
        <addressGroup>
          <primaryAddress>10.112.2.40</primaryAddress>
          <secondaryAddresses>
            <ipAddress>10.112.2.42</ipAddress>
          </secondaryAddresses>
          <subnetMask>255.255.254.0</subnetMask>
        </addressGroup>
      </addressGroups>
      <mtu>1500</mtu>
      <enableProxyArp>false</enableProxyArp>
      <enableSendRedirects>true</enableSendRedirects>
      <isConnected>true</isConnected>
    </vnic>
    ...
  </vnics>
  <appliances>
    <applianceSize>compact</applianceSize>
    <appliance>
      <highAvailabilityIndex>0</highAvailabilityIndex>
      <vcUuid>4208f392-1693-11db-6355-4affd859ef33</vcUuid>
      <vmId>vm-4021</vmId>
      <resourcePoolId>resgroup-2454</resourcePoolId>
      <resourcePoolName>Resources</resourcePoolName>
      <datastoreId>datastore-2457</datastoreId>
      <datastoreName>shahm-esx-storage</datastoreName>
      <hostId>host-2455</hostId>
      <hostName>10.112.196.160</hostName>
      <vmFolderId>group-v3</vmFolderId>
      <vmFolderName>vm</vmFolderName>
```

```

        <vmHostname>vShieldEdge-network-2264-0</vmHostname>
        <vmName>vShield-edge-79-0</vmName>
        <deployed>true</deployed>
        <<edgeId>>edge-79</edgeId>>
    </appliance>
</appliances>
<cliSettings>
    <remoteAccess>false</remoteAccess>
    <userName>admin</userName>
</cliSettings>
<features>
    <featureConfig/>
    <firewall>
        <version>1</version>
        <enabled>true</enabled>
        <defaultPolicy>
            <action>deny</action>
        </defaultPolicy>
        <loggingEnabled>false</loggingEnabled>
        <firewallRules>
            <firewallRule>
                <id>131078</id>
                <ruleTag>131078</ruleTag>
                <name>rule1</name>
                <ruleType>user</ruleType>
                <source>
                    <groupingObjectId>ipset-938</groupingObjectId>
                </source>
                <sourcePort>any</sourcePort>
                <destination/>
                <application>
                    <applicationId>application-666</applicationId>
                </application>
                <action>accept</action>
                <enabled>true</enabled>
                <loggingEnabled>false</loggingEnabled>
                <matchTranslated>false</matchTranslated>
            </firewallRule>
            ...
        </firewallRules>
    </firewall>
    <dns>
        <version>1</version>
        <enabled>false</enabled>
        <cacheSize>16</cacheSize>
        <listeners>
            <ipAddress>any</ipAddress>
        </listeners>
        <logging>
            <enable>false</enable>
            <logLevel>info</logLevel>
        </logging>
    </dns>
    <staticRouting>
        <version>1</version>
        <enabled>true</enabled>
        <defaultRoute>
            <vnid>0</vnid>
            <gatewayAddress>10.112.3.253</gatewayAddress>
            <description>defaultGw on the external interface</description>
        </defaultRoute>
        <staticRoutes>
            <route>
                <vnid>0</vnid>
                <network>192.168.30.0/24</network>
                <nextHop>10.112.2.41</nextHop>
                <type>user</type>
            </route>

```

```

...
</staticRoutes>
</staticRouting>
<highAvailability>
  <version>1</version>
  <enabled>>false</enabled>
  <declareDeadTime>6</declareDeadTime>
  <logging>
    <enable>>false</enable>
    <logLevel>info</logLevel>
  </logging>
</highAvailability>
<syslog>
  <version>1</version>
  <enabled>true</enabled>
  <protocol>udp</protocol>
  <serverAddresses>
    <ipAddress>1.1.1.1</ipAddress>
    <ipAddress>1.1.1.2</ipAddress>
  </serverAddresses>
</syslog>
<featureConfig/>
<loadBalancer>
  <version>1</version>
  <enabled>true</enabled>
  <accelerationEnabled>>false</accelerationEnabled>
  <virtualServer>
    <id>1</id>
    <name>listener1</name>
    <enabled>true</enabled>
    <ipAddress>10.112.2.42</ipAddress>
    <applicationProfile>
      <protocol>HTTP</protocol>
      <port>80</port>
    </applicationProfile>
    <logging>
      <enable>>false</enable>
      <logLevel>INFO</logLevel>
    </logging>
    <pool>
      <id>1</id>
    </pool>
  </virtualServer>
  ...
  <pool>
    <id>1</id>
    <name>pool1</name>
    <servicePort>
      <protocol>HTTP</protocol>
      <algorithm>IP_HASH</algorithm>
      <port>80</port>
      <healthCheckPort>80</healthCheckPort>
    </servicePort>
    <member>
      <ipAddress>192.168.10.7</ipAddress>
      <weight>1</weight>
      <servicePort>
        <protocol>HTTP</protocol>
        <port>80</port>
      </servicePort>
    </member>
  </pool>
  ...
</loadBalancer>
<ipsec>
  <version>1</version>
  <enabled>true</enabled>
  <logging>

```

```

        <enable>false</enable>
        <logLevel>info</logLevel>
    </logging>
    <sites>
        <site>
            <enabled>true</enabled>
            <name>site 1</name>
            <localId>10.112.2.40</localId>
            <localIp>10.112.2.40</localIp>
            <peerId>10.112.2.41</peerId>
            <peerIp>10.112.2.41</peerIp>
            <encryptionAlgorithm>aes256</encryptionAlgorithm>
            <mtu>1500</mtu>
            <enablePfs>true</enablePfs>
            <dhGroup>dh2</dhGroup>
            <localSubnets>
                <subnet>192.168.10.0/24</subnet>
            </localSubnets>
            <peerSubnets>
                <subnet>192.168.40.0/24</subnet>
            </peerSubnets>
            <psk>1234</psk>
            <authenticationMode>psk</authenticationMode>
        </site>
        ...
    </sites>
    <global>
        <caCertificates/>
        <crlCertificates/>
    </global>
</ipsec>
<dhcp>
    <version>1</version>
    <enabled>false</enabled>
    <staticBindings>
        <staticBinding>
            <autoConfigureDNS>true</autoConfigureDNS>
            <bindingId>binding-1</bindingId>
            <vmId>vm-2460</vmId>
            <vnicId>1</vnicId>
            <hostname>test</hostname>
            <ipAddress>192.168.10.6</ipAddress>
            <defaultGateway>192.168.10.1</defaultGateway>
            <leaseTime>86400</leaseTime>
        </staticBinding>
        ...
    </staticBindings>
    <ipPools>
        <ipPool>
            <autoConfigureDNS>true</autoConfigureDNS>
            <poolId>pool-1</poolId>
            <ipRange>192.168.10.2-192.168.10.5</ipRange>
            <defaultGateway>192.168.10.1</defaultGateway>
            <leaseTime>86400</leaseTime>
        </ipPool>
        ...
    </ipPools>
    <logging>
        <enable>false</enable>
        <logLevel>info</logLevel>
    </logging>
</dhcp>
<nat>
    <version>1</version>
    <enabled>true</enabled>
    <natRules>
        <natRule>
            <ruleId>196610</ruleId>

```

```

        <ruleTag>196610</ruleTag>
        <ruleType>user</ruleType>
        <action>dnat</action>
        <vnic>1</vnic>
        <originalAddress>10.112.196.162</originalAddress>
        <translatedAddress>192.168.10.3</translatedAddress>
        <loggingEnabled>>false</loggingEnabled>
        <enabled>>true</enabled>
        <protocol>tcp</protocol>
        <originalPort>80</originalPort>
        <translatedPort>80</translatedPort>
    </natRule>
    ...
</natRules>
</nat>
<featureConfig/>
</features>
<autoConfiguration>
    <enabled>true</enabled>
    <rulePriority>high</rulePriority>
</autoConfiguration>
</edge>

```

---

## Query vShield Edge Summary

Retrieves the summary of the specified vShield Edge and its connected interfaces.

### Example 5-2. Query vShield Edge summary

---

Request:

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/summary

Response Body:

```

<?xml version="1.0" encoding="UTF-8"?>
<edgeSummary>
    <objectId>edge-32</objectId>
    <type>
        <typeName>Edge</typeName>
    </type>
    <name>vShield-edge-32</name>
    <revision>16</revision>
    <objectTypeName>Edge</objectTypeName>
    <id>edge-32</id>
    <state>deployed</state>
    <datacenterMoid>datacenter-2</datacenterMoid>
    <datacenterName>Datacenter</datacenterName>
    <apiVersion>3.0</apiVersion>
    <numberOfConnectedVnics>2</numberOfConnectedVnics>
    <appliancesSummary>
        <vmVersion>5.1.0</vmVersion>
        <applianceSize>compact</applianceSize>
        <fqdn>vShield-edge-32</fqdn>
        <numberOfDeployedVms>1</numberOfDeployedVms>
        <activeVseHaIndex>0</activeVseHaIndex>
        <vmMoidOfActiveVse>vm-301</vmMoidOfActiveVse>
        <vmNameOfActiveVse>vShield-edge-32-0</vmNameOfActiveVse>
        <hostMoidOfActiveVse>host-159</hostMoidOfActiveVse>
        <hostNameOfActiveVse>10.20.114.8</hostNameOfActiveVse>
        <resourcePoolMoidOfActiveVse>resgroup-208</resourcePoolMoidOfActiveVse>
        <resourcePoolNameOfActiveVse>Resources</resourcePoolNameOfActiveVse>
        <dataStoreMoidOfActiveVse>datastore-160</dataStoreMoidOfActiveVse>
        <dataStoreNameOfActiveVse>storage1</dataStoreNameOfActiveVse>
        <statusFromVseUpdatedOn>1310625858000</statusFromVseUpdatedOn>
    </appliancesSummary>
    <featureCapabilities>

```

```

<timestamp>1337956125602</timestamp>
<featureCapability>
  <service>nat</service>
  <isSupported>true</isSupported>
  <configurationLimit>
    <key>MAX_RULES_PER_ACTION</key>
    <value>2048</value>
  </configurationLimit>
</featureCapability>
<featureCapability>
  <service>syslog</service>
  <isSupported>true</isSupported>
  <configurationLimit>
    <key>MAX_SERVER_IPS</key>
    <value>2</value>
  </configurationLimit>
</featureCapability>
<featureCapability>
  <service>staticRouting</service>
  <isSupported>true</isSupported>
  <configurationLimit>
    <key>MAX_ROUTES</key>
    <value>2048</value>
  </configurationLimit>
</featureCapability>
<featureCapability>
  <service>ipsec</service>
  <isSupported>true</isSupported>
  <configurationLimit>
    <key>MAX_TUNNELS</key>
    <value>64</value>
  </configurationLimit>
</featureCapability>
<featureCapability>
  <service>loadBalancer</service>
  <isSupported>true</isSupported>
  <configurationLimit>
    <key>MAX_POOLS</key>
    <value>10</value>
  </configurationLimit>
  <configurationLimit>
    <key>MAX_VIRTUAL_SERVERS</key>
    <value>10</value>
  </configurationLimit>
  <configurationLimit>
    <key>MAX_MEMBERS_IN_POOL</key>
    <value>32</value>
  </configurationLimit>
</featureCapability>
<featureCapability>
  <service>fw</service>
  <isSupported>true</isSupported>
  <configurationLimit>
    <key>MAX_RULES</key>
    <value>2048</value>
  </configurationLimit>
</featureCapability>
<featureCapability>
  <service>dns</service>
  <isSupported>true</isSupported>
  <configurationLimit>
    <key>MAX_SERVER_IPS</key>
    <value>2</value>
  </configurationLimit>
</featureCapability>
<featureCapability>
  <service>sslvpn</service>
  <isSupported>true</isSupported>

```

```

        <configurationLimit>
          <key>MAX_CONCURRENT_USERS</key>
          <value>25</value>
        </configurationLimit>
      </featureCapability>
    <featureCapability>
      <service>edge</service>
      <isSupported>true</isSupported>
      <configurationLimit>
        <key>MAX_APPLIANCES</key>
        <value>2</value>
      </configurationLimit>
      <configurationLimit>
        <key>MAX_VNICS</key>
        <value>10</value>
      </configurationLimit>
    </featureCapability>
    <featureCapability>
      <service>firewall</service>
      <isSupported>true</isSupported>
      <configurationLimit>
        <key>MAX_RULES</key>
        <value>2048</value>
      </configurationLimit>
    </featureCapability>
    <featureCapability>
      <service>dhcp</service>
      <isSupported>true</isSupported>
      <configurationLimit>
        <key>MAX_POOL_AND_BINDINGS</key>
        <value>2048</value>
      </configurationLimit>
    </featureCapability>
    <featureCapability>
      <service>highAvailability</service>
      <isSupported>true</isSupported>
      <configurationLimit>
        <key>MAX_MANAGEMENT_IPS</key>
        <value>2</value>
      </configurationLimit>
    </featureCapability>
  </featureCapabilities>
</edgeSummary>

```

---

## Querying vShield Edge Status

Retrieves the current status of the specified vShield Edge status and its features.

### Example 5-3. Get vShield Edge status

---

Get status of services on the vShield Edge appliance (by default getlatest=true and detailed=false):

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/status

Get detailed status of vShield per feature

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/status?detailed=true

Get latest available detailed status of vShield Edge from the database:

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/status?getlatest=false

Get latest available detailed status of vShield Edge per feature from the database:

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/status?getlatest=false&detailed=true

Get detailed live status of vShield Edge per feature:



GET https://<vsm-ip>/api/3.0/edges/<edgeId>/status?getlatest=true&detailed=true

Get latest available status of vShield Edge with aggregated summary per feature:

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/status?getlatest=false&detailed=false

#### Example 5-4. Get vShield Edge status

Request:

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/status

Response Body:

```
<edgeStatus>
  <timestamp>1343739873000</timestamp>
  <systemStatus>good</systemStatus>
  <activeVseHaIndex>0</activeVseHaIndex>
  <edgeStatus>GREEN</edgeStatus> <!-- {GREY,RED,YELLOW,GREEN}. GREY => unknown status. RED => None of
    appliance in serving state. YELLOW => Intermittent health check failures. If health check fails for 5
    consecutive times for all appliance (2 for HA else 1) then status will turn to RED. GREEN => Good -->
  <publishStatus>APPLIED</publishStatus> <!-- Applied or persisted i.e., not applied to vse yet-->
  <version>8</version> <!-- Current configuration version -->
  <edgeVmStatus>
    <edgeVmStatus>
      <edgeVMStatus>GREEN</edgeVMStatus> <!-- individual vm status -->
      <haState>active</haState> <!-- active / standby -->
      <index>0</index>
      <id>vm-358</id>
      <name>test2-0</name>
    </edgeVmStatus>
    <edgeVmStatus>
      <edgeVMStatus>GREEN</edgeVMStatus>
      <haState>active</haState>
      <index>1</index>
      <id>vm-362</id>
      <name>test2-1</name>
    </edgeVmStatus>
  </edgeVmStatus>
  <featureStatuses>
    <featureStatus>
      <service>loadBalancer</service>
      <configured>>false</configured>
      <serverStatus>down</serverStatus>
    </featureStatus>
    <featureStatus>
      <service>dhcp</service>
      <configured>true</configured>
      <publishStatus>Applied</publishStatus>
      <serverStatus>up</serverStatus>
    </featureStatus>
    <featureStatus>
      <service>sslvpn</service>
      <configured>>false</configured>
      <serverStatus>down</serverStatus>
    </featureStatus>
    <featureStatus>
      <service>syslog</service>
      <configured>>false</configured>
      <serverStatus>up</serverStatus>
    </featureStatus>
    <featureStatus>
      <service>nat</service>
      <configured>>false</configured>
    </featureStatus>
    <featureStatus>
      <service>dns</service>
      <configured>>false</configured>
```

```

        <serverStatus>down</serverStatus>
    </featureStatus>
    <featureStatus>
        <service>ipsec</service>
        <configured>>false</configured>
        <serverStatus>down</serverStatus>
    </featureStatus>
    <featureStatus>
        <service>firewall</service>
        <configured>>true</configured>
        <publishStatus>Applied</publishStatus>
    </featureStatus>
    <featureStatus>
        <service>staticRouting</service>
        <configured>>false</configured>
    </featureStatus>
    <featureStatus>
        <service>highAvailability</service>
        <configured>>true</configured>
        <publishStatus>Applied</publishStatus>
        <serverStatus>up</serverStatus>
    </featureStatus>
</featureStatuses>
</edgeStatus>

```

---

## Working with Appliances

You can manage the vShield Edge appliances with these REST calls.

**NOTE** Do not use hidden/system resource pool IDs as they are not supported on the UI.

### Query Appliance Configuration

Retrieves configuration of both appliances.

#### Example 5-5. Get appliance configuration

---

Request:

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/appliances

Request Body:

```

<appliances>
  <applianceSize>large</applianceSize>
  <appliance>
    <highAvailabilityIndex>0</highAvailabilityIndex>
    <resourcePoolId>resgroup-53</resourcePoolId>
    <datastoreId>datastore-29</datastoreId>
    <hostId>host-28</hostId>
    <vmFolderId>group-v38</vmFolderId>
    <customField>
      <key>system.service.vmware.vsla.main01</key>
      <value>string</value>
    </customField>
    <cpuReservation>
      <limit>2399</limit>
      <reservation>500</reservation>
      <shares>500</shares>
    </cpuReservation>
    <memoryReservation>
      <limit>5000</limit>
      <reservation>500</reservation>
      <shares>20480</shares>
    </memoryReservation>
  </appliance>
</appliances>

```

```

<appliance>
  <highAvailabilityIndex>1</highAvailabilityIndex>
  <resourcePoolId>resgroup-53</resourcePoolId>
  <datastoreId>datastore-29</datastoreId>
  <hostId>host-28</hostId>
  <vmFolderId>group-v38</vmFolderId>
  <customField>
    <key>system.service.vmware.vsla.main01</key>
    <value>string</value>
  </customField>
  <cpuReservation>
    <limit>2399</limit>
    <reservation>500</reservation>
    <shares>500</shares>
  </cpuReservation>
  <memoryReservation>
    <limit>5000</limit>
    <reservation>500</reservation>
    <shares>20480</shares>
  </memoryReservation>
</appliance>
</appliances>

```

---

## Modify Appliance Configuration

You can retrieve the configuration of both appliances by using the GET call in [Example 5-5](#) and replace the size, resource pool, datastore, and custom parameters of the appliances by using a PUT call. If there were two appliances earlier you PUT only one appliance, the other appliance is deleted.

### Example 5-6. Modify appliance configuration

---

Request:

PUT https://<vsm-ip>/api/3.0/edges/<edgeId>/appliances

Request Body:

```

<appliances>
  <applianceSize>COMPACT</applianceSize>
  <appliance>
    <resourcePoolId>resgroup-1610</resourcePoolId>
    <datastoreId>datastore-5288</datastoreId>
  </appliance>
  <appliance>
    <resourcePoolId>resgroup-1610</resourcePoolId>
    <datastoreId>datastore-5288</datastoreId>
  </appliance>
</appliances>

```

---

## Change Appliance Size

Changes the size of both appliances.

### Example 5-7. Change appliance size

---

Request:

POST https://<vsm-ip>/api/3.0/edges/<edgeId>/appliances/?size=compact|large|xlarge

---

## Manage an Appliance

You can manage an appliance by specifying its HA index.

## Query Appliance

Retrieves the configuration of the appliance with the specified `haIndex`.

### Example 5-8. Get configuration of appliance with specified `haIndex`

---

Request:

GET `https://<vsm-ip>/api/3.0/edges/<edgeId>/appliances/haIndex`

Response Body:

```
<appliance>
  <resourcePoolId>resgroup-53</resourcePoolId>
  <datastoreId>datastore-29</datastoreId>
  <hostId>host-28</hostId>
  <vmFolderId>group-v38</vmFolderId>
  <customField>
    <key>system.service.vmware.vsla.main01</key>
    <value>string</value>
  </customField>
  <cpuReservation>
    <limit>2399</limit>
    <reservation>500</reservation>
    <shares>500</shares>
  </cpuReservation>
  <memoryReservation>
    <limit>5000</limit>
    <reservation>500</reservation>
    <shares>20480</shares>
  </memoryReservation>
</appliance>
```

---

## Modify Appliance

Modifies the configuration of the appliance with the specified `haIndex`.

### Example 5-9. Modify configuration of appliance with specified `haIndex`

---

Request:

PUT `https://<vsm-ip>/api/3.0/edges/<edgeId>/appliances/haIndex`

Request Body:

```
<appliance>
  <resourcePoolId>resgroup-53</resourcePoolId>
  <datastoreId>datastore-29</datastoreId>
  <hostId>host-28</hostId>
  <vmFolderId>group-v38</vmFolderId>
  <customField>
    <key>system.service.vmware.vsla.main01</key>
    <value>string</value>
  </customField>
  <cpuReservation>
    <limit>2399</limit>
    <reservation>500</reservation>
    <shares>500</shares>
  </cpuReservation>
  <memoryReservation>
    <limit>5000</limit>
    <reservation>500</reservation>
    <shares>20480</shares>
  </memoryReservation>
</appliance>
```

---

## Delete Appliance

Deletes the appliance with the specified haIndex.

### Example 5-10. Delete appliance configuration

Request:

```
DELETE https://<vsm-ip>/api/3.0/edges/<edgeId>/appliances/haIndex
```

## Working with Interfaces

You can add up to ten internal or uplink interfaces to each vShield Edge instance. A vShield Edge must have at least one internal interface before it can be deployed.

### Add Interfaces

You can configure one or more interface for a vShield Edge. The specified configuration is stored in the database. If any appliance(s) is associated with this vShield Edge instance, the specified configuration is applied to the appliance as well.

### Example 5-11. Add an interface

Request:

```
POST https://<vsm-ip>/api/3.0/edges/<edgeId>/vnics/?action=patch
```

Request Body:

```
<vnics>
  <vnic>
    <index>0</index>
    <name>uplink-vnic-network-2581</name>
    <type>uplink</type>
    <portgroupId>network-2581</portgroupId>
    <mtu>1500</mtu>
    <enableProxyArp>>false</enableProxyArp>
    <enableSendRedirects>>true</enableSendRedirects>
    <isConnected>>true</isConnected>
    <inShapingPolicy>
      <!-- Optional. Can only be specified for an interface connected to a distributed
      portgroup -->
      <averageBandwidth>200000000</averageBandwidth>
      <peakBandwidth>200000000</peakBandwidth> <!-- Optional. Default is averageBandwidth.-->
      <burstSize>0</burstSize> <!-- Optional. Default is 0.-->
      <enabled>true</enabled> <!-- Optional. Default is true.-->
      <inherited>>false</inherited> <!-- Optional. Default is false.-->
    </inShapingPolicy>
    <outShapingPolicy>
      <!-- Optional. Can only be specified for an interface connected to a distributed
      portgroup -->
      <averageBandwidth>400000000</averageBandwidth>
      <peakBandwidth>400000000</peakBandwidth> <!-- Optional. Default is averageBandwidth.-->
      <burstSize>0</burstSize> <!-- Optional. Default is 0.-->
      <enabled>true</enabled> <!-- Optional. Default is true.-->
      <inherited>>false</inherited> <!-- Optional. Default is 0.-->
    </outShapingPolicy>
    <addressGroups>
      <addressGroup>
        <!-- Each addressGroup represents the IP addresses within the same subnet -->
        <primaryAddress>192.168.3.10</primaryAddress>
        <subnetMask>255.255.255.0</subnetMask>
      </addressGroup>
      <addressGroup>
        <primaryAddress>192.168.3.150</primaryAddress>
        <secondaryAddresses> <!-- Optional -->
          <ipAddress>192.168.3.151</ipAddress>
          <ipAddress>192.168.3.152</ipAddress>
```

```

        </secondaryAddresses>
        <subnetMask>255.255.254.0</subnetMask>
    </addressGroup>
</addressGroups>

</vnic>
<vnic>
...
</vnic>
</vnics>

```

---

where addressGroups contains IP addresses for the interface with each addressGroup representing the IP addresses within the same subnet. For each subnet, you can specify a primaryAddress (required), secondaryAddress (optional), and the subnetMask (required).

## Retrieve Interfaces for a vShield Edge

Retrieves all interfaces for the specified vShield Edge.

### Example 5-12. Retrieve all interfaces

---

Request:

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/vnics

Response Body:

```

<vnics>
  <vnic>
    <index>0</index>
    <name>uplink-vnic-network-2581</name>
    <type>uplink</type>
    <portgroupId>network-2581</portgroupId>
    <addressGroups>
      <addressGroup>
        <primaryAddress>10.112.2.40</primaryAddress>
        <secondaryAddresses>
          <ipAddress>10.112.2.42</ipAddress>
        </secondaryAddresses>
        <subnetMask>255.255.254.0</subnetMask>
      </addressGroup>
    </addressGroups>
    <mtu>1500</mtu>
    <enableProxyArp>false</enableProxyArp>
    <enableSendRedirects>true</enableSendRedirects>
    <isConnected>true</isConnected>
    <inShapingPolicy>
      <averageBandwidth>200000000</averageBandwidth>
      <peakBandwidth>200000000</peakBandwidth>
      <burstSize>0</burstSize>
      <enabled>true</enabled>
      <inherited>false</inherited>
    </inShapingPolicy>
    <outShapingPolicy>
      <averageBandwidth>400000000</averageBandwidth>
      <peakBandwidth>400000000</peakBandwidth>
      <burstSize>0</burstSize>
      <enabled>true</enabled>
      <inherited>false</inherited>
    </outShapingPolicy>
  </vnic>
  <vnic>
...
  </vnic>
</vnics>

```

---

## Delete Interfaces

Deletes one or more interfaces for a vShield Edge. Stores the specified configuration in database. If any appliance(s) are associated with this edge, disconnects and deletes the interface.

### Example 5-13. Delete interface

Request:

```
DELETE https://<vsm-ip>/api/3.0/edges/<edgeId>/vnics/?index=<vnicIndexId1>&index=<vnicIndexId2>
```

## Manage a vShield Interface

You can manage a specific vShield Edge interface.

### Retrieve Interface with Specific Index

Retrieves the interface with specified index for a vShield Edge.

### Example 5-14. Get interface with specific index

Request:

```
GET https://<vsm-ip>/api/3.0/edges/<edgeId>/vnics/index
```

### Delete Interface Configuration

Deletes the interface configuration and resets it to the factory default.

### Example 5-15. Delete interface configuration

Request:

```
DELETE https://<vsm-ip>/api/3.0/edges/<edgeId>/vnics/index
```

### Modify an Interface

Modifies the specified interface.

### Example 5-16. Modify interface

Request:

```
PUT https://<vsm-ip>/api/3.0/edges/<edgeId>/vnics/<index>
```

Response Body:

```
<vnic>
  <index>0</index>                                <!-- optional. System has default Names. format vNic0 ... vNic7 -->
  <name>uplink-vnic-network-2581</name>              <!-- optional. Default is internal>
  <type>uplink</type>
  <portgroupId>network-2581</portgroupId>           <!-- Possible values are portgroupIds or virtualWire-id. portgroupId
                                                    needs to be defined if isConnected=true -->
  <addressGroups>
    <addressGroup>                                  <!-- Vnic can be configured to have more than one addressGroup/subnets -->
      <primaryAddress>10.112.2.40</primaryAddress> <!-- This is mandatory for an addressGroup -->
      <secondaryAddresses><!-- Optional. Should be used to add/defined other IPs used for NAT, LB, VPN, etc -->
        <ipAddress>10.112.2.42</ipAddress>
      </secondaryAddresses>
      <subnetMask>255.255.254.0</subnetMask>
    </addressGroup>
  </addressGroups>
  <macAddress>                                       <!-- optional. When not specified, macAddresses will be managed by VC -->
```

```

    <edgeVmHaIndex>0</edgeVmHaIndex>
    <value>00:50:56:01:03:23</value>
  </macAddress>
  <fenceParameter>                                <!-- optional -->
    <key>ethernet0.filter1.param1</key>
    <value>1</value>
  </fenceParameter>
  <mtu>1500</mtu>                                <!-- Default is 1500.-->
  <enableProxyArp>false</enableProxyArp>          <!--Default is false.-->
  <enableSendRedirects>true</enableSendRedirects>  <!--Default is true.-->
  <isConnected>true</isConnected>                 <!--Default is false.-->
  <inShapingPolicy>                                <!-- optional -->
    <averageBandwidth>200000000</averageBandwidth>
    <peakBandwidth>200000000</peakBandwidth>
    <burstSize>0</burstSize>
    <enabled>true</enabled>
    <inherited>false</inherited>
  </inShapingPolicy>
  <outShapingPolicy>                                <!-- optional -->
    <averageBandwidth>400000000</averageBandwidth>
    <peakBandwidth>400000000</peakBandwidth>
    <burstSize>0</burstSize>
    <enabled>true</enabled>
    <inherited>false</inherited>
  </outShapingPolicy>
</vnic>

```

---

## Query Interface Statistics

### Query Statistics for all Interfaces

Retrieves statistics for all configured interfaces between the specified start and end times. When start and end time are not specified, all statistics since the vShield Edge deployed are displayed. When no end time is specified, the current vShield Manager time is set as endTime. Each record has the stats of 5 minutes granularity.

#### Example 5-17. Get interface statistics

---

Request:

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/statistics/interfaces

Request Body:

```

<statistics>
  <meta>
    <startTime>1336068000</startTime>  <!-- in seconds -->
    <endTime>1336100700</endTime>      <!-- in seconds -->
    <interval>300</interval>           <!-- 5 mins interval -->
  </meta>
  <data>
    <statistic>
      <vnic>0</vnic>
      <timestamp>1336068000</timestamp>
      <in>9.1914285714e+02</in>         <!-- Rx rate ( Kilobits per second - kbps ) -->
      <out>5.1402857143e+02</out>       <!-- Tx rate ( Kilobits per second - kbps ) -->
    </statistic>

    ...

    ...

    <statistic>
      <vnic>1</vnic>
      <timestamp>1336100700</timestamp>
      <in>9.2914285714e+02</in>
      <out>5.2402857143e+02</out>
    </statistic>

```



```

    </statistic>
  </data>
</statistics>

```

---

### Query Statistics for Uplink Interfaces

Retrieves statistics for all uplink interfaces between the specified start and end times. When start and end time are not specified, all statistics since the vShield Edge deployed are displayed. When no end time is specified, the current vShield Manager time is set as endTime. Each record has the stats of 5 minutes granularity.

#### Example 5-18. Get uplink interface statistics

---

Request:

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/statistics/interfaces/uplink

Request Body:

```

<statistics>
  <meta>
    <startTime>1336068000</startTime>    <!-- in seconds -->
    <endTime>1336100700</endTime>        <!-- in seconds -->
    <interval>300</interval>              <!-- 5 mins interval -->
  </meta>
  <data>
    <statistic>
      <vnic>0</vnic>
      <timestamp>1336068000</timestamp>
      <in>9.1914285714e+02</in>            <!-- Rx rate ( Kilobits per second - kbps ) -->
      <out>5.1402857143e+02</out>         <!-- Tx rate ( Kilobits per second - kbps ) -->
    </statistic>

    ...

    <statistic>
      <vnic>1</vnic>
      <timestamp>1336100700</timestamp>
      <in>9.2914285714e+02</in>
      <out>5.2402857143e+02</out>
    </statistic>
  </data>
</statistics>

```

---

### Query Statistics for Internal Interfaces

Retrieves statistics for all internal interfaces between the specified start and end times. When start and end time are not specified, all statistics since the vShield Edge deployed are displayed. When no end time is specified, the current vShield Manager time is set as endTime. Each record has the stats of 5 minutes granularity.

#### Example 5-19. Get internal interface statistics

---

Request:

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/statistics/interfaces/internal

Request Body:

```

<statistics>
  <meta>
    <startTime>1336068000</startTime>    <!-- in seconds -->
    <endTime>1336100700</endTime>        <!-- in seconds -->
    <interval>300</interval>              <!-- 5 mins interval -->
  </meta>

```

```

<data>
  <statistic>
    <vnic>0</vnic>
    <timestamp>1336068000</timestamp>
    <in>9.1914285714e+02</in>      <!-- Rx rate ( Kilobits per second - kbps ) -->
    <out>5.1402857143e+02</out>  <!-- Tx rate ( Kilobits per second - kbps ) -->
  </statistic>

  ...

  <statistic>
    <vnic>1</vnic>
    <timestamp>1336100700</timestamp>
    <in>9.2914285714e+02</in>
    <out>5.2402857143e+02</out>
  </statistic>
</data>
</statistics>

```

---

## Query Dashboard Statistics

Retrieves dashboard statistics between the specified start and end times. When start and end time are not specified, all statistics since the vShield Edge deployed are displayed. When no end time is specified, the current vShield Manager time is set as endTime. Each record has the stats of 5 minutes granularity.

### Example 5-20. Get interface statistics

---

Request:

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/statistics/dashboard/interface?interval=<range>

Request Body:

```

<dashboardstatistics>
  <meta>
    <startTime>1336068000</startTime>  <!-- in seconds -->
    <endTime>1336100700</endTime>      <!-- in seconds -->
    <interval>300</interval>           <!-- 5 mins interval -->
  </meta>
  <data>
    <interfaces>
      <vNic_0_in_pkt>
        <dashboardStatistic>
          <timestamp></timestamp>
          <value></value>
        </dashboardStatistic>
        <dashboardStatistic>
          <timestamp></timestamp>
          <value></value>
        </dashboardStatistic>
        ...
      </vNic_0_in_pkt>
      ...
    </interfaces>
  </data>
</dashboardstatistics>

```

---

## Configuring Edge Services

You configure Edge services such as NAT, Firewall, DHCP, static routing, load Balancer, and VPN.

---

**IMPORTANT** When you configure a vShield Edge service, the service is started on the appliance. If you do not want the service running, you must set `enabled=false`.

---

## Configure Firewall

The vShield Edge provides firewall protection for incoming and outgoing sessions. In addition to the default firewall policy, you can configure a set of rules to allow or deny traffic sessions to and from specific sources and destinations. You manage the default firewall policy and firewall rules together for each vShield Edge agent. You must specify both firewall rules and `defaultPolicy` together whenever modifying either of them, or else the one you do not specify will be deleted.

Firewall rules for a vShield Edge configured by using REST requests appear under the **Firewall** tab for the appropriate vShield Edge in the vShield Manager user interface and in the vSphere Client plug-in.

Rules can be defined using IPsets or services defined on the appropriate scope. Notes:

- You cannot enter a raw IP address or protocol-port/protocol-subtype as the source or destination of a rule. You must define an IPset or service. IPsets and services can be created on the following scoped:
  - vShield Edge - objects are available locally for that vShield Edge instance only
  - datacenter - objects are available to all vShield Edge instances on that datacenter

If the IPset or service is updated, the changes are applied to all vShield Edge instances using that IPset or service.

For information on creating an IPset, see [“Create an IPset on a Scope”](#) on page 31. For information on creating a service, see [“Add Service to a Scope”](#) on page 41.

- You can add multiple objects as the source or destination of a firewall rule.
- If you do not specify a `ruleTag` for a rule, vShield generates it automatically.
- Logging is disabled by default. To enable it, add `<enableLog> true` element within the `<rule>` section.

When `enabled=true`, vShield Edge pushes the rule to the appliance. When `enabled=false`, vShield Manager remembers the rule but does not push the rule to the appliance. By default, `enabled=true`. This is an optional parameter.

## Add Firewall Configuration

### Example 5-21. Add firewall configuration

---

PUT `https://<vsm-ip>/api/3.0/edges/<edgeId>/firewall/config`

Request Body:

```
<?xml version="1.0"?>
<firewall>
  <defaultPolicy>                                <-- Optional. default is deny -->
    <action>deny</action>
    <loggingEnabled>false</loggingEnabled>        <!-- Optional. Defaults to false -->
  </defaultPolicy>
  <firewallRules>
    <firewallRule>
      <ruleTag>1</ruleTag>                        <!-- Optional. Values should be 1-65536. If not specified, vShield Manager
                                                    generates a ruleId -->
      <name>rule1</name>                          <!-- Optional -->
      <source>                                     <!-- Optional. Default behaviour is like "any". ipsetId or predefined-vnicGroupIds can
                                                    be used -->
        <vnicGroupId>vnic-index-5</vnicGroupId>    <!-- Possible values are "vnic-index-[0-9]", "vse", "external" or
                                                    "internal". Can define multiple of these -->
        <groupingObjectId>ipset-128</groupingObjectId> <!-- Id of IPAddresses grouping Objects available to the edge.
                                                    Can define multiple of these -->
      </source>
      <sourcePort>80</sourcePort>                <!-- Optional. Default is "any". Possible inputs are : port, portRange, or
                                                    "any". Can define multiple of these -->
```

```

destination>                                <!-- Optional. Default behaviour is like "any". ipsetId or predefined-vnicGroupIds can
        be used -->
    <groupingObjectId>ipset-126</groupingObjectId> <!-- Id of IPAddresses grouping Objects available to the edge.
        Can define multiple of these -->
    <vnicGroupId>vnic-index-5</vnicGroupId>      <!-- Possible values are "vnic-index-[0-9]", "vse", "external" or
        "internal". Can define multiple of these -->
    <groupingObjectId>ipset-128</groupingObjectId> <!-- Id of IPAddresses grouping Objects available to the edge.
        Can define multiple of these -->
</destination>
<application>                                <!-- Optional. Default behaviour is like "any". applicationsetId or applicationgroupId
        can be used -->
    <applicationId>application-155</applicationId> <!-- Id of Service available to the edge. Can define multiple of these
        -->
</application>
<matchTranslated>true</matchTranslated>        <!-- Optional. Default behaviour is like "false" -->
<direction>in</direction>                    <!-- Optional. Default behaviour is like "any". Possible values are in|out -->
<action>accept</action>                      <!-- Mandatory. Possible values are accept|deny -->
<enabled>true</enabled>                      <!-- Optional. Default is true -->
<loggingEnabled>true</loggingEnabled>         <!-- Optional. Default is false -->
<description>comments</description>          <!-- Optional -->
</firewallRule>
<firewallRule>
...
</firewallRule>
.....
</firewallRules>
</firewall>

```

---

where the ruleId uniquely identifies a rule and must be specified for rules that are being updated.

If ruleTag is specified, the rules on vShield Edge are configured using this user input. Otherwise, vShield Edge is configured using the vShield Manager generated ruleIds.

VMware recommends that you avoid using the matchTranslated and direction tags from release 5.1 onwards.

## Query Firewall Configuration

Retrieves the firewall configuration for a vShield Edge.

### Example 5-22. Get firewall configuration

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/firewall/config

Response Body

```

<firewall>
  <version>1</version>
  <enabled>true</enabled>
  <defaultPolicy>
    <action>deny</action>
    <loggingEnabled>>false</loggingEnabled>
  </defaultPolicy>
  <firewallRules>
    <firewallRule>
      <id>131079</id>
      <ruleTag>131079</ruleTag>
      <name>firewall</name>
      <ruleType>internal_high</ruleType>
      <source>
        <vnicGroupId>vse</vnicGroupId>
      </source>
      <action>accept</action> <enabled>true</enabled>
      <loggingEnabled>>false</loggingEnabled>
      <description>firewall</description>
    </firewallRule>
    <firewallRule>
      ...
    </firewallRule>
  </firewallRules>
</firewall>

```

```

<firewallRule>
  ...
</firewallRule>
<firewallRule>
  <id>131077</id>
  <ruleTag>131077</ruleTag>
  <name>upgrade-network-2264-out</name>
  <ruleType>user</ruleType>
  <source>
    <groupingObjectId>ipset-940</groupingObjectId>
  </source>
  <sourcePort>8000</sourcePort>
  <destination>
    <groupingObjectId>ipset-941</groupingObjectId>
  </destination>
  <application>
    <applicationId>application-667</applicationId>
  </application>
  <action>deny</action>
  <direction>in</direction>
  <enabled>true</enabled>
  <loggingEnabled>>false</loggingEnabled>
  <matchTranslated>true</matchTranslated>
</firewallRule>
<firewallRule>
  <id>131078</id>
  <ruleTag>131078</ruleTag>
  <name>upgrade-network-2264-in</name>
  <ruleType>user</ruleType>
  <source>
    <groupingObjectId>ipset-938</groupingObjectId>
  </source>
  <sourcePort>any</sourcePort>
  <destination/>
  <application>
    <applicationId>application-666</applicationId>
  </application>
  <action>accept</action>
  <enabled>true</enabled>
  <loggingEnabled>>false</loggingEnabled>
  <matchTranslated>>false</matchTranslated>
</firewallRule>
<firewallRule>
  <id>131075</id>
  <ruleTag>131075</ruleTag>
  <name>default rule for ingress traffic</name>
  <ruleType>default_policy</ruleType>
  <action>deny</action>
  <enabled>true</enabled>
  <loggingEnabled>>false</loggingEnabled>
  <description>default rule for ingress traffic</description>
</firewallRule>
</firewallRules>
</firewall>

```

---

## Delete Firewall Configuration

When you delete a firewall configuration, all user-defined rules are deleted and the defaultPolicy is changed to deny. The autoPlumbed rules continue to exist.

### Example 5-23. Delete firewall configuration

```
DELETE https://<vsm-ip>/api/3.0/edges/<edgeId>/firewall/config
```

---

## Append Firewall Rules

Adds one or more rules below the existing rules in the rules table.

### Example 5-24. Add firewall rule

POST <https://vsm-ip>/api/3.0/edges/<edgeId>/firewall/config/rules>

Request Body:

```
<firewallRules>
  <firewallRule>
    <ruleTag>1</ruleTag>          <!-- Optional. Can be used to specify user controlled ids on vShield Edge. The
                                   inputs here should be 1-65536. If not specified, vShield Manager will generate ruleId -->
    <name>rule1</name>            <!-- Optional -->
    <source>                      <!-- Optional. Default behaviour is like "any". ipsetId or predefined-vnicGroupIds can
                                   be used -->
    <vnicGroupId>vnic-index-5</vnicGroupId> <!-- Possible values are "vnic-index-[0-9]", "vse", "external" or
                                   "internal". Can define multiple of these -->
    <groupingObjectId>ipset-128</groupingObjectId> <!-- Id of IPAddresses grouping Objects available to the edge.
                                   Can define multiple of these -->
  </source>
  <sourcePort>80</sourcePort>    <!-- Optional. Default is "any". Possible inputs are : port, portRange, or "any".
                                   Can define multiple of these -->
  <destination>                  <!-- Optional. Default behaviour is like "any". ipsetId or predefined-vnicGroupIds
                                   can be used -->
    <groupingObjectId>ipset-126</groupingObjectId> <!-- Id of IPAddresses grouping Objects available to the edge.
                                   Can define multiple of these -->
    <vnicGroupId>vnic-index-5</vnicGroupId> <!-- Possible values are "vnic-index-[0-9]", "vse", "external" or
                                   "internal". Can define multiple of these -->
    <groupingObjectId>ipset-128</groupingObjectId> <!-- Id of IPAddresses grouping Objects available to the edge.
                                   Can define multiple of these -->
  </destination>
  <application>                  <!-- Optional. Default behaviour is like "any". applicationsetId or applicationgroupId
                                   can be used -->
    <applicationId>application-155</applicationId> <!-- Id of Service available to the edge. Can define multiple of these
                                   -->
  </application>
  <matchTranslated>true</matchTranslated> <!-- Optional. Default behaviour is like "false" -->
  <direction>in</direction>        <!-- Optional. Default behaviour is like "any". Possible values are in/out -->
  <action>accept</action>          <!-- Mandatory. Possible values are accept|deny -->
  <enabled>true</enabled>          <!-- Optional. Defaults to true -->
  <loggingEnabled>true</loggingEnabled> <!-- Optional. Defaults to false -->
  <description>comments</description> <!-- Optional -->
</firewallRule>
<firewallRule>
...
</firewallRule>
</firewallRules>
```

### Add a Firewall Rule Above a Specific Rule

You can add a rule above a specific rule by indicating its ruleID. If no user-rules exist in the firewall rules table, you can specify ruleId=0. If you do not specify a ruleID or the specified ruleID does not exist, vShield Manager displays an error.

### Example 5-25. Add a rule above a specific rule

Request:

POST <https://vsm-ip>/api/3.0/edges/<edgeId>/firewall/config/rules?aboveRuleId=<ruleId>>

Request Body:

```
<firewallRule>
  <ruleTag>1</ruleTag>          <!-- Optional. This can be used to specify user controlled ids on VSE. The inputs
                                   here should be 1-65536. If not specified, VSM will generate ruleId -->
  <name>rule1</name>            <!-- Optional -->
```

```

<source>                                <!-- Optional. Default behaviour is like "any". ipsetId or predefined-vnicGroupIds can
    used -->
    <vnicGroupId>vnic-index-5</vnicGroupId>    <!-- Possible values are "vnic-index-[0-9]", "vse", "external" or
        "internal". Can define multiple of these -->
    <groupingObjectId>ipset-128</groupingObjectId>    <!-- Id of IPAddresses grouping Objects available to the edge. Can
        define multiple of these -->
</source>
<sourcePort>80</sourcePort>                <!-- Optional. Default is "any". Possible inputs are : port, portRange, or "any".
    Can define multiple of these -->
<destination>                                <!-- Optional. Default behaviour is like "any". ipsetId or predefined-vnicGroupIds can
    be used -->
    <groupingObjectId>ipset-126</groupingObjectId>    <!-- Id of IPAddresses grouping Objects available to the edge.
        Can define multiple of these -->
    <vnicGroupId>vnic-index-5</vnicGroupId>    <!-- Possible values are "vnic-index-[0-9]", "vse", "external" or
        "internal". Can define multiple of these -->
    <groupingObjectId>ipset-128</groupingObjectId>    <!-- Id of IPAddresses grouping Objects available to the edge.
        Can define multiple of these -->
</destination>
<application>                                <!-- Optional. Default behaviour is like "any". applicationsetId or applicationgroupId
    can be used -->
    <applicationId>application-155</applicationId>    <!-- Id of Service available to the edge. Can define multiple of
        these -->
</application>
<matchTranslated>true</matchTranslated>        <!-- Optional. Default behaviour is like "false" -->
<direction>in</direction>                    <!-- Optional. Default behaviour is like "any". Possible values are in|out -->
<action>accept</action>                        <!-- Mandatory. Possible values are accept|deny -->
<enabled>true</enabled>                        <!-- Optional. Defaults to true -->
<loggingEnabled>true</loggingEnabled>          <!-- Optional. Defaults to false -->
<description>comments</description>            <!-- Optional --> </firewallRule>
</firewallRule>

```

---

## Query Specific Rule

### Example 5-26. Retrieve specific rule

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/firewall/config/rules/<ruleId>

Response Body:

```

<firewallRule>
  <name>new rule</name>
  <source>
    <vnicGroupId>vnic-index-5</vnicGroupId>
  </source>
  <destination>
    <groupingObjectId>ipset-127</groupingObjectId>
  </destination>
  <action>accept</action>
  <enabled>true</enabled>
  <loggingEnabled>true</loggingEnabled>
  <description/>
</firewallRule>

```

---

## Modify Firewall Rule

You can modify a rule by specifying its rule ID.

### Example 5-27. .Update specific rule

PUT https://<vsm-ip>/api/3.0/edges/<edgeId>/firewall/config/rules/<ruleId>

Response Body:

```

<firewallRule>
  <ruleTag>1</ruleTag>    <!-- Optional. This can be used to specify user controlled ids on VSE. The inputs
    here should be 1-65536. If not specified, VSM will generate ruleId -->
  <name>rule1</name>      <!-- Optional -->

```

```

<source>                                <!-- Optional. Default behaviour is like "any". ipsetId or predefined-vnicGroupIds can
        be used -->
    <vnicGroupId>vnic-index-5</vnicGroupId>    <!-- Possible values are "vnic-index-[0-9]", "vse", "external" or
        "internal". Can define multiple of these -->
    <groupingObjectId>ipset-128</groupingObjectId>    <!-- Id of IPAddresses grouping Objects available to the edge. Can
        define multiple of these -->
</source>
<sourcePort>80</sourcePort>                <!-- Optional. Default is "any". Possible inputs are : port, portRange, or "any".
        Can define multiple of these -->
<destination>                                <!-- Optional. Default behaviour is like "any". ipsetId or predefined-vnicGroupIds can
        be used -->
    <groupingObjectId>ipset-126</groupingObjectId>    <!-- Id of IPAddresses grouping Objects available to the edge.
        Can define multiple of these -->
    <vnicGroupId>vnic-index-5</vnicGroupId>    <!-- Possible values are "vnic-index-[0-9]", "vse", "external" or
        "internal". Can define multiple of these -->
    <groupingObjectId>ipset-128</groupingObjectId>    <!-- Id of IPAddresses grouping Objects available to the edge.
        Can define multiple of these -->
</destination>
<application>                                <!-- Optional. Default behaviour is like "any". applicationsetId or applicationgroupId
        can be used -->
    <applicationId>application-155</applicationId>    <!-- Id of Service available to the edge. Can define multiple of
        these -->
</application>
<matchTranslated>true</matchTranslated>        <!-- Optional. Default behaviour is like "false" -->
<direction>in</direction>                    <!-- Optional. Default behaviour is like "any". Possible values are in|out -->
<action>accept</action>                        <!-- Mandatory. Possible values are accept|deny -->
<enabled>true</enabled>                        <!-- Optional. Defaults to true -->
<loggingEnabled>true</loggingEnabled>          <!-- Optional. Defaults to false -->
<description>comments</description>          <!-- Optional --> </firewallRule>
</firewallRule>

```

---

## Delete a Firewall Rule

Deletes the rule with the specified rule ID.

### Example 5-28. Delete firewall rule

Request Body;

DELETE https://<vsm-ip>/api/3.0/edges/<edgeId>/firewall/config/rules/<ruleId>

## Manage Default Firewall Policy

### Query Default Firewall Policy

Retrieves the default firewall policy for a vShield Edge.

### Example 5-29. Get default firewall policy

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/firewall/config/defaultpolicy

Response Body:

```

<?xml version="1.0" encoding="UTF-8"?>
<firewallDefaultPolicy>
    <action>DENY</action>
    <loggingEnabled>true</loggingEnabled>
</firewallDefaultPolicy>

```

---

### Change Default Firewall Policy

Sets default policy and enables or disables logging for the default policy. Enabling logging may affect performance.



**Example 5-30. Change default firewall policy**


---

PUT https://<vsm-ip>/api/3.0/edges/<edgeId>/firewall/config/defaultpolicy

Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<firewallDefaultPolicy>
  <action>ACCEPT</action>
  <loggingEnabled>true</loggingEnabled>
</firewallDefaultPolicy>
```

---

**Query Firewall Statistics**

Retrieves connections for the firewall configuration for the specified interval, which can be either 1-60 minutes, or a day, week, month, or year.

**Example 5-31. Retrieve firewall statistics**


---

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/statistics/dashboard/firewall?interval=<range>

Request Body:

```
<dashboardStatistics>
  <meta>
    <startTime>1336068000</startTime> <!-- in seconds -->
    <endTime>1336100700</endTime> <!-- in seconds -->
    <interval>300</interval> <!--range can be 1 - 60 minutes or oneDay|oneWeek|oneMonth|oneYear. Default is 60
    minutes -->
  </meta>
  <data>
    <firewall>
    </firewall>
  </data>
</dashboardStatistics>
```

---

**NOTE** For startTime and endTime, you must specify the Universal Time (UTC) shown on vShield Manager. Use the CLI command show clock to see the vShield Manager time.

**Query Firewall Statistics For a Rule****Example 5-32. Retrieve firewall statistics for a rule**


---

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/firewall/statistics/<ruleId>

Request Body:

```
<firewallRuleStats>
  <timestamp>1342317563</timestamp>
  <connectionCount>0</connectionCount>
  <packetCount>0</packetCount>
  <byteCount>0</byteCount>
</firewallRuleStats>
```

---

**Configure NAT**

The vShield Edge provides network address translation (NAT) service to protect the IP addresses of internal (private) networks from the public network. You can configure NAT rules to provide access to services running on privately addressed virtual machines. There are two types of NAT rules that can be configured: SNAT and DNAT. When you post a NAT configuration, all the rules (both SNAT and DNAT) must be posted together. Otherwise, only the posted rules are retained, and unposted rules are deleted.

All SNAT and DNAT rules configured by using REST requests appear under the **NAT** tab for the appropriate vShield Edge in the vShield Manager user interface and in the vSphere Client plug-in.

**Example 5-33. Configure SNAT and DNAT rules for a vShield Edge**

PUT https://<vsm-ip>/api/3.0/edges/<edgeId>/nat/config

```
<nat>
  <natRules>
    <natRule>
      <ruleTag>65537</ruleTag>      <!-- Optional. Can be used to specify user-controlled ids on VSE. Valid inputs
                                   65537-131072. If not specified, vShield manager will generate ruleId -->
      <action>dnat</action>
      <vnic>0</vnic>
      <originalAddress>10.112.196.116</originalAddress>
      <translatedAddress>172.16.1.10</translatedAddress>
      <loggingEnabled>true</loggingEnabled> <!-- Optional. Default is false -->
      <enabled>true</enabled>      <!-- Optional. Default is true -->
      <description>my comments</description> <!-- Optional -->
      <protocol>tcp</protocol>      <!-- Optional. Default is "any". This tag is not supported for SNAT rule -->
      <translatedPort>3389</translatedPort> <!-- Optional. Default is "any". This tag is not supported for SNAT rule -->
      <originalPort>3389</originalPort> <!-- Optional. Default is "any". This tag is not supported for SNAT rule -->
    </natRule>
    <natRule>
      <ruleTag>65538</ruleTag>      <!-- Optional. Can be used to specify user-controlled ids on VSE. Valid inputs
                                   65537-131072. If not specified, VSM will generate ruleId -->
      <action>snat</action>
      <vnic>1</vnic>
      <originalAddress>172.16.1.10</originalAddress>
      <translatedAddress>10.112.196.116</translatedAddress>
      <loggingEnabled>false</loggingEnabled> <!-- Optional. Default is "false" -->
      <enabled>true</enabled>      <!-- Optional. Default is "true" -->
      <description>no comments</description> <!-- Optional. Default is "any" -->
    </natRule>
  </natRules>
</nat>
```

For the data path to work, you need to add firewall rules to allow the required traffic for IP addresses and port per the NAT rules.

Rules:

- You must add <icmpType> if you configure icmp as the protocol.
- The originalAddress and translatedAddress elements can be entered in either of these methods:
  - <ipAddress> specified as a single IP address, a hyphen-separated IP address range (for example, 192.168.10.1-192.168.10.255) or a subnet in CIDR notation (198.168.10.1/24).
  - the keyword any
- The originalPort and translatedPort parameters can be entered in one of the following formats: the keyword any, the port number as an integer, or a range of port number, for example portX-portY.
- You can add multiple SNAT rules by entering multiple <type>snat</type> sections in the body.
- SNAT does not support port or protocol parameters.
- Logging is disabled by default. To enable logging, add an <enableLog> element set to true.

**Retrieve NAT Rules for a vShield Edge****Example 5-34. Configure SNAT and DNAT rules for a vShield Edge**

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/nat/config

Response Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<nat>
  <natRules>
    <natRule>
```

```

    <ruleTag>196609</ruleTag>
    <ruleId>196609</ruleId>
    <action>dnat</action>
    <vnic>0</vnic>
    <originalAddress>10.112.196.116</originalAddress>
    <translatedAddress>172.16.1.10</translatedAddress>
    <loggingEnabled>true</loggingEnabled>
    <enabled>true</enabled>
    <description>my comments</description>
    <protocol>tcp</protocol>
    <translatedPort>3389</translatedPort>
    <originalPort>3389</originalPort>
    <ruleType>user</ruleType>
  </natRule>
  <natRule>
    <ruleTag>196609</ruleTag>
    <ruleId>196609</ruleId>
    <action>snat</action>
    <vnic>1</vnic>
    <originalAddress>172.16.1.10</originalAddress>
    <translatedAddress>10.112.196.116</translatedAddress>
    <loggingEnabled>false</loggingEnabled>
    <enabled>true</enabled>
    <description>no comments</description>
    <protocol>any</protocol>
    <originalPort>any</originalPort>
    <translatedPort>any</translatedPort>
    <ruleType>user</ruleType>
  </natRule>
</natRules>
</nat>

```

---

## Delete all NAT Rules

Deletes all SNAT and DNAT rules for a vShield Edge. The auto plumbed rules continue to exist.

### Example 5-35. Delete NAT rules

---

Request:

DELETE <https://<vsm-ip>/api/3.0/edges/<edgeId>/nat/config>

---

## Add a NAT Rule above a Specific Rule

Adds a NAT rule above the specified rule ID. If no NAT rules exist in the NAT rules table, you can specify ruleId=0. If you do not specify a ruleId or the specified ruleId does not exist, vShield Manager displays an error.

### Example 5-36. Add a NAT rule above a specific rule

---

POST <https://<vsm-ip>/api/3.0/edges/<edgeId>/nat/config/rules?aboveRuleId=<ruleId>>

Request Body:

```

<natRule>
  <action>dnat</action>
  <vnic>0</vnic>
  <originalAddress>10.112.196.116</originalAddress>
  <translatedAddress>172.16.1.10</translatedAddress>
  <loggingEnabled>true</loggingEnabled>
  <enabled>true</enabled>
  <description>my comments</description>
  <protocol>tcp</protocol>
  <translatedPort>3389</translatedPort>

```

```
<originalPort>3389</originalPort>
</natRule>
```

---

## Append NAT Rules

Appends one or more rules to the bottom of the NAT rules table.

### Example 5-37. Add NAT rules to the bottom of the rules table

---

POST https://<vsm-ip>/api/3.0/edges/<edgeId>/nat/config/rules

Response Body:

```
<natRules>
  <natRule>
    <action>dnat</action>
    <vnic>0</vnic>
    <originalAddress>10.112.196.116</originalAddress>
    <translatedAddress>172.16.1.10</translatedAddress>
    <loggingEnabled>true</loggingEnabled>
    <enabled>true</enabled>
    <description>my comments</description>
    <protocol>tcp</protocol>
    <translatedPort>3389</translatedPort>
    <originalPort>3389</originalPort>
  </natRule>
</natRules>
```

---

where vnic is the internal or uplink interface of the vShield Edge (0-9).

## Change a NAT Rule

Replaces the NAT rule with the specified rule ID.

### Example 5-38. Replaces a NAT rule

---

PUT https://<vsm-ip>/api/3.0/edges/<edgeId>/nat/config/rules/*ruleID*

Response Body:

```
<natRule>
  <action>dnat</action>
  <vnic>0</vnic>
  <originalAddress>10.112.196.116</originalAddress>
  <translatedAddress>172.16.1.10</translatedAddress>
  <loggingEnabled>true</loggingEnabled>
  <enabled>true</enabled>
  <description>my comments</description>
  <protocol>tcp</protocol>
  <translatedPort>3389</translatedPort>
  <originalPort>3389</originalPort>
</natRule>
```

---

where vnic is the internal or uplink interface of the vShield Edge (0-9).

## Delete a Rule

Deletes the rule with the specified rule ID.

### Example 5-39. Delete NAT rule

---

Request:

DELETE https://<vsm-ip>/api/3.0/edges/<edgeId>/nat/config/rules/*ruleID*

---

## Configure Routing

This uses the next-hop method for the outgoing interface. The vnic specifies the managed object ID of the network, attribute network designates the IP address range, and nextHop the static route.

### Configure Static and Default Routes

Use this call only for initial static route configuration. To make any changes thereafter, you must query the existing static route configuration and add new routes to the existing list and/or update the default route. If either the default route or the static routes is not present in the PUT call, it is deleted.

#### Example 5-40. Configure static and default route

PUT https://<vsm-ip>/api/3.0/edges/<edgeId>/routing/config

Request Body:

```
<staticRouting>
  <staticRoutes>
    <route>
      <vnic>0</vnic>
      <network>3.1.1.4/22</network>
      <nextHop>172.16.1.14</nextHop>
      <mtu>1500</mtu> <!-- Optional. Valid value:smaller than the MTU set on the interface. Default is MTU of the
                           interface on which this route is configured -->
    </route>
    <route>
      <vnic>1</vnic>
      <network>4.1.1.4/22</network>
      <nextHop>10.112.196.118</nextHop>
      <mtu>1500</mtu> <!-- Optional. Valid value:smaller than the MTU set on the interface. Default is MTU of the
                           interface on which this route is configured -->
    </route>
  </staticRoutes>
  <defaultRoute>
    <vnic>0</vnic>
    <gatewayAddress>172.16.1.12</gatewayAddress>
    <mtu>1500</mtu> <!-- Optional. Valid value:smaller than the MTU set on the interface. Default is MTU of the interface
                           on which this route is configured -->
  </defaultRoute>
</staticRouting>
```

### Query Static and Default Routes

#### Example 5-41. Retrieve static and default route

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/routing/config

Response Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<staticRouting>
  <staticRoutes>
    <route>
      <vnic>0</vnic>
      <network>3.1.1.4/22</network>
      <nextHop>172.16.1.14</nextHop>
      <mtu>1500</mtu> <!-- Optional. Valid value:smaller than the MTU set on the interface. Default is MTU of the
                           interface on which this route is configured -->
      <type>user</type>
    </route>
    <route>
      <vnic>1</vnic>
      <network>4.1.1.4/22</network>
      <nextHop>10.112.196.118</nextHop>
      <mtu>1500</mtu> <!-- Optional. Valid value:smaller than the MTU set on the interface. Default is MTU of the
                           interface on which this route is configured -->
    </route>
  </staticRoutes>
  <defaultRoute>
    <vnic>0</vnic>
    <gatewayAddress>172.16.1.12</gatewayAddress>
    <mtu>1500</mtu> <!-- Optional. Valid value:smaller than the MTU set on the interface. Default is MTU of the interface
                           on which this route is configured -->
  </defaultRoute>
</staticRouting>
```

```

        <type>user</type>
    </route>
</staticRoutes>
<defaultRoute>
    <vnic>0</vnic>
    <gatewayAddress>172.16.1.12</gatewayAddress>
    <mtu>1500</mtu> <!-- Optional. Valid value:smaller than the MTU set on the interface. Default is MTU of the interface
                                on which this route is configured -->
</defaultRoute>
</staticRouting>

```

---

## Delete Static and Default Routes

Deletes the routing configuration stored in the vShield Manager database and the default routes from the specified vShield Edge appliance.

### Example 5-42. Delete default route

Request

DELETE https://<vsm-ip>/api/3.0/edges/<edgeId>/routing/config

## Change Static Routes

Modifies static routes. The default route configuration does not change.

### Example 5-43. Modify static routes

PUT https://<vsm-ip>/api/3.0/edges/<edgeId>/routing/staticroutes

Request Body:

```

<staticRoutes>
  <route>
    <vnic>0</vnic>
    <network>3.1.1.4/22</network>
    <nextHop>172.16.1.14</nextHop>
    <mtu>1500</mtu> <!-- Optional. Valid value:smaller than the MTU set on the interface. Default is MTU of the
                                interface on which this route is configured -->
  </route>
  <route>
    <vnic>1</vnic>
    <network>4.1.1.4/22</network>
    <nextHop>10.112.196.118</nextHop>
    <mtu>1500</mtu> <!-- Optional. Valid value:smaller than the MTU set on the interface. Default is MTU of the
                                interface on which this route is configured -->
  </route>
</staticRoutes>
</staticRouting>

```

---

## Append Static Routes

Appends specified static routes to existing static routes.

### Example 5-44. Append static routes

Request

POST https://<vsm-ip>/api/3.0/edges/<edgeId>/routing/config/staticroutes

Request Body:

```

<staticRoutes>
  <route>
    <vnic>0</vnic>

```

```

    <network>3.1.1.4/22</network>
    <nextHop>172.16.1.14</nextHop>
    <mtu>1500</mtu>
  </route>
  <route>
    <vnic>1</vnic>
    <network>4.1.1.4/22</network>
    <nextHop>10.112.196.118</nextHop>
    <mtu>1500</mtu>
  </route>
</staticRoutes>

```

---

### Delete Static Routes

Deletes the static routing configuration stored in the vShield Manager database. Does not affect the default routes from the specified vShield Edge appliance.

#### Example 5-45. Delete static routes

---

Request

DELETE https://<vsm-ip>/api/3.0/edges/<edgeId>/routing/config/staticroutes

---

### Configure Default Routes for vShield Edge

The default route you configure does not affect the configured static routes on the vShield Edge.

#### Example 5-46. Configure default route

---

Request

PUT https://<vsm-ip>/api/3.0/edges/<edgeId>/routing/config/defaultroute

Request Body:

```

<defaultRoute>
  <vnic>0</vnic>
  <gatewayAddress>172.16.1.12</gatewayAddress>
  <mtu>1500</mtu>
</defaultRoute>

```

---

### Delete Default Routes

Deletes the default routes. Does not affect the static routes.

#### Example 5-47. Delete default route

---

Request

DELETE https://<vsm-ip>/api/3.0/edges/<edgeId>/routing/config/defaultroute

---

## Configure DNS Servers

You can configure external DNS servers to which vShield Edge can relay name resolution requests from clients. vShield Edge will relay client application requests to the DNS servers to fully resolve a network name and cache the response from the servers.

### Configure DNS

Updates the DNS server configuration. DNS server list allows two addresses – primary and secondary. The default cache size is 16 MB where the minimum can be 1 MB, and the maximum 8196 MB.

The default listeners is any, which means listen on all VSE interfaces. If provided, the listener's IP address must be assigned to an internal interface.

Logging is disabled by default.

#### Example 5-48. Configure DNS servers

---

Request:

PUT https://<vsm-ip>/api/3.0/edges/<edgeId>/dns/config

Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<dns>
  <enabled>true</enabled>          <!-- optional. default is true-->
  <dnsServers>
    <ipAddress>10.117.0.1</ipAddress> <!-- Max is 2 external dns server -->
  </dnsServers>
  <cacheSize>128</cacheSize>       <!-- optional. default is 16, max to 8192 -->
  <listeners>                      <!-- optiona. if provided, IPs must be defined on Edge interfaces. -->
    <ipAddress>192.168.100.1</ipAddress>
    <ipAddress>192.168.100.2</ipAddress>
  </listeners>
  <logging>                        <!-- optional. default is disabled. -->
    <logLevel>info</logLevel>      <!-- optional. default is "info" -->
    <enable>true</enable>          <!-- optional. default is "false" -->
  </logging>
</dns>
```

---

### Retrieve DNS Configuration

Gets details of DNS configuration, including the service status.

#### Example 5-49. Get DNS server configuration

---

Request:

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/dns/config

Response Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<dns>
  <enabled>true</enabled>
  <dnsServers>
    <ipAddress>10.117.0.1</ipAddress>
  </dnsServers>
  <cacheSize>128</cacheSize>
  <listeners>
    <ipAddress>192.168.100.1</ipAddress>
    <ipAddress>192.168.100.2</ipAddress>
  </listeners>
  <logging>
    <logLevel>info</logLevel>
    <enable>true</enable>
  </logging>
</dns>
```

---

### Delete DNS Configuration

Deletes DNS servers.

#### Example 5-50. Delete DNS servers

---

Request:



DELETE https://<vsm-ip>/api/3.0/edges/<edgeId>/dns/config

---

## Retrieve DNS Statistics

Gets DNS server statistics.

### Example 5-51. Get DNS server statistics

---

Request:

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/dns/statistics

Response Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<dns>
  <stats>
    <timeStamp>2011-10-10 12:12:12</timeStamp>
    <requests>
      <total>120000</total>
      <queries>110000</queries>
    </requests>
    <responses>
      <total>108000</total>
      <success>105000</success>
      <nrrset>1000</nrrset>
      <servFail>400</servFail>
      <formErr>300</formErr>
      <nxdomain>1000</nxdomain>
      <others>300</others>
    </responses>
    <cachedDBRRSet>15000</cachedDBRRSet>
  </stats>
</dns>
```

---

where

- requests.total indicates all the incoming requests to the DNS server, including DNS query and other types of request (e.g. transfer, updates)
- requests.queries indicates all the DNS queries the server received.
- responses.total indicates all responses the server returned to requests. It could be different from the requests.total because some requests could be rejected. total = success + nrrset + servFail + formErr + nxdomain + others
- responses.success indicates all the successful DNS answers.
- responses.nrrset indicates the count of no existent resource record set
- responses.servFail indicates the count of SERVFAIL answer
- responses.formErr indicates the count of format error answer
- responses.nxdomain indicates the count of no-suhc-domain answer
- responses.others indicates the count of other type of answers.

## Configure DHCP

vShield Edge provides DHCP service to bind assigned IP addresses to MAC addresses, helping to prevent MAC spoofing attacks. All virtual machines protected by a vShield Edge can obtain IP addresses dynamically from the vShield Edge DHCP service.

vShield Edge supports IP address pooling and one-to-one static IP address allocation based on the vCenter managed object ID (vmId) and interface ID (interfaceId) of the requesting client.

If either bindings or pools are not included in the PUT call, existing bindings or pools are deleted.

All DHCP settings configured by REST requests appear under the **vShield Edge > DHCP** tab for the appropriate vShield Edge in the vShield Manager user interface and in vSphere Client plug-in.

vShield Edge DHCP service adheres to the following rules:

- Listens on the vShield Edge internal interface (non-uplink interface) for DHCP discovery.
- As stated above, vmId specifies the vc-moref-id of the virtual machine, and vnicId specifies the index of the vNic for the requesting client. The hostname is an identification of the binding being created. This hostName is not pushed as the specified host name of the virtual machine.
- By default, all clients use the IP address of the internal interface of the vShield Edge as the default gateway address. To override it, specify defaultGateway per binding or per pool. The client's broadcast and subnetMask values are from the internal interface for the container network.
- leaseTime can be infinite, or a number of seconds. If not specified, the default lease time is 1 day.
- Logging is disabled by default.
- Setting the parameter enable=true starts the DHCP service while enable=false stops the service.
- Both staticBinding and ipPools must be part of the request body. Else, they will be deleted if configured earlier.

#### Example 5-52. Configure DHCP service

PUT https://<vsm-ip>/api/3.0/<edgeId>/dhcp/config

Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<dhcp>
  <enabled>true</enabled>                                <!-- optional, default is "true". -->
  <staticBindings>
    <staticBinding>
      <vmId>vm-111</vmId>                                <!-- required. the vm must be connected to the given vNic below. -->
      <vnicId>1</vnicId>                                  <!-- required. possible values 0 to 9 -->
      <hostname>abcd</hostname>                          <!-- optional. -->
      <ipAddress>192.168.4.2</ipAddress>                  <!-- required. the IP must belongs to one subnet of edge vNics, but
                                                           must NOT overlap any primary/secondary ips of defined explicitly in vNic. -->
      <defaultGateway>192.168.4.1</defaultGateway>        <!-- optional. default is the primary ip of the belonging
                                                           vNic.-->
      <domainName>eng.vmware.com</domainName>             <!-- optional. -->
      <primaryNameServer>192.168.4.1</primaryNameServer> <!-- optional. if autoConfigDNS=true, the dns
                                                           primary/secondary ips will be generated from DNS service(if configured). -->
      <secondaryNameServer>4.2.2.4</secondaryNameServer>
      <leaseTime>infinite</leaseTime>                    <!-- optional. in second, default is "86400". valid leaseTime is a valid
                                                           digit, or "infinite". -->
      <autoConfigureDNS>true</autoConfigureDNS>           <!-- optional. if autoConfigDNS=true, the dns
                                                           primary/secondary ips will be generated from DNS service(if configured). -->
    </staticBinding>
  </staticBindings>
  <ipPools>
    <ipPool>
      <ipRange>192.168.4.192-192.168.4.220</ipRange>    <!-- required. the ipRange must belongs to one of a subnet of
                                                           Edge vNics. And can NOT contains any ip that defined explicitly as vNic primary ip or
                                                           secondary ip. -->
      <defaultGateway>192.168.4.1</defaultGateway>        <!-- optional. default is the primary ip of the belonging
                                                           vNic.-->
      <domainName>eng.vmware.com</domainName>             <!-- optional. -->
      <primaryNameServer>192.168.4.1</primaryNameServer> <!-- optional. if autoConfigDNS=true, the dns
                                                           primary/secondary ips will be generated from DNS service(if configured). -->
      <secondaryNameServer>4.2.2.4</secondaryNameServer> <!-- optional. if autoConfigDNS=true, the dns
                                                           primary/secondary ips will be generated from DNS service(if configured). -->
      <leaseTime>3600</leaseTime>                        <!-- optional. in second, default is "86400". valid leaseTime is a valid
                                                           digit, or "infinite". -->
      <autoConfigureDNS>true</autoConfigureDNS>           <!-- optional. default is true. -->
    </ipPool>
  </ipPools>
</dhcp>
```

```

    </ipPools>
    <logging>                                <!-- optional. logging is disable by default. -->
        <enable>false</enable>                <!-- optional, default is false. -->
        <logLevel>info</logLevel>            <!-- optional, default is false. -->
    </logging>
</dhcp>

```

---

**NOTE** If the vShield Edge autoConfiguration flag and autoConfigureDNS is true, and the primaryNameServer or secondaryNameServer parameters are not specified, vShield Manager applies the DNS settings to the DHCP configuration.

## Query DHCP Configuration

Gets the DHCP configuration on a vShield Edge including IP pool and static binding assignments.

### Example 5-53. Get DHCP configuration

GET https://<vsm-ip>/api/3.0/<edgeId>/dhcp/config

Response Body:

```

<?xml version="1.0" encoding="UTF-8"?>
<dhcp>
    <enabled>true</enabled>
    <staticBindings>
        <staticBinding>
            <vmId>vm-111</vmId>
            <vnicId>1</vnicId>
            <hostname>abcd</hostname>
            <ipAddress>192.168.4.2</ipAddress>
            <defaultGateway>192.168.4.1</defaultGateway>
            <domainName>eng.vmware.com</domainName>
            <primaryNameServer>192.168.4.1</primaryNameServer>
            <secondaryNameServer>4.2.2.4</secondaryNameServer>
            <leaseTime>infinite</leaseTime>
            <autoConfigureDNS>true</autoConfigureDNS>
        </staticBinding>
    </staticBindings>
    <ipPools>
        <ipPool>
            <ipRange>192.168.4.192-192.168.4.220</ipRange>
            <defaultGateway>192.168.4.1</defaultGateway>
            <domainName>eng.vmware.com</domainName>
            <primaryNameServer>192.168.4.1</primaryNameServer>
            <secondaryNameServer>4.2.2.4</secondaryNameServer>
            <leaseTime>3600</leaseTime>
            <autoConfigureDNS>true</autoConfigureDNS>
        </ipPool>
    </ipPools>
    <logging>
        <enable>false</enable>
        <logLevel>info</logLevel>
    </logging>
</dhcp>

```

---

## Delete DHCP Configuration

Deletes the DHCP configuration and reverse the configuration back to factory defaults.

### Example 5-54. Delete DHCP configuration

Request:

DELETE https://<vsm-ip>/api/3.0/<edgeId>/dhcp/config

---

## Retrieve DHCP Lease Information

### Example 5-55. Get DHCP lease information

GET https://<vsm-ip>/api/3.0/<edgeId>/dhcp/leaseinfo

Response Body:

```
<dhcp>
  <timeStamp>1326950787</timeStamp>
  <dhcpLeaseInfo>
    <leaseInfo>
      <uid>\001\000PV\265\204\207</uid>
      <macAddress>00:50:56:b5:84:87</macAddress>
      <ipAddress>192.168.4.2</ipAddress>
      <clientHostname>vto-suse-dev</clientHostname>
      <bindingState>active</bindingState>
      <nextBindingState>free</nextBindingState>
      <cltt>4 2012/01/19 05:24:50</cltt>
      <starts>4 2012/01/19 05:24:50</starts>
      <ends>4 2012/01/19 17:24:50</ends>
      <hardwareType>ethernet</hardwareType>
    </leaseInfo>
  </dhcpLeaseInfo>
</dhcp>
```

## Append IP Pool to DHCP Configuration

Appends an IP pool to the DHCP configuration. Returns a pool ID within a Location HTTP header.

### Example 5-56. Add IP pool

POST https://<vsm-ip>/api/3.0/<edgeId>/dhcp/config/ippools

Response Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<ipPool>
  <ipRange>192.168.5.2-192.168.5.20</ipRange>
  <defaultGateway>192.168.5.1</defaultGateway>
  <domainName>eng.vmware.com</domainName>
  <primaryNameServer>1.2.3.4</primaryNameServer>
  <secondaryNameServer>4.3.2.1</secondaryNameServer>
  <leaseTime>3600</leaseTime>
  <autoConfigureDNS>true</autoConfigureDNS>
</ipPool>
```

## Append Static Binding to DHCP Configuration

Appends a static-binding to the DHCP configuration. A static-binding ID is returned within a Location HTTP header.

### Example 5-57. Add static binding

POST https://<vsm-ip>/api/3.0/<edgeId>/dhcp/config/bindings

Response Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<staticBinding>
  <vmId>vm-157</vmId>
  <vnicId>3</vnicId> <!-- possible values 0 to 9 -->
  <hostname>vShield-edge-2-0</hostname>
  <ipAddress>192.168.6.66</ipAddress>
  <defaultGateway>192.168.6.1</defaultGateway>
  <domainName>eng.vmware.com</domainName>
  <primaryNameServer>1.2.3.4</primaryNameServer>
```

```

    <secondaryNameServer>4.3.2.1</secondaryNameServer>
    <leaseTime>infinite</leaseTime>
    <autoConfigureDNS>true</autoConfigureDNS>
  </staticBinding>

```

---

### Delete DHCP Pool

Deletes a pool specified by pool-id.

#### Example 5-58. Delete DHCP pool

---

Request:

```
DELETE https://<vsm-ip>/api/3.0/edges/<edgeId>/dhcp/config/ippools/<poolId>
```

---

### Delete DHCP Static Binding

Deletes the static-binding specified by binding-id.

#### Example 5-59. Delete DHCP static binding

---

Request:

```
DELETE https://<vsm-ip>/api/3.0/edges/<edgeId>/dhcp/config/bindings/<bindingId>
```

---

## Configure Certificates

vShield Edge supports self-signed certificates, certificates signed by a Certification Authority (CA), and certificates generated and signed by a CA.

### Working with Certificates

Allows you to manage self signed certificates.

#### Create Certificate

Creates a single or multiple certificates.

#### Example 5-60. Create self signed certificate

---

Request:

```

POST https://<vsm-ip>/api/2.0/services/truststore/certificate/<scopeId>
<trustObject>
  <pemEncoding></pemEncoding>
  <privateKey></privateKey>
  <passphrase></passphrase>
</trustObject>

```

---

#### Create Certificate or Certificate Chain for CSR

Imports a certificate or a certificate chain against a certificate signing request.

#### Example 5-61. Create certificate for CSR

---

Request:

```
POST https://<vsm-ip>/api/2.0/services/truststore/certificate?csrId=<csrId>
```

Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
```

```

<trustObject>
  <pemEncoding></pemEncoding>
</trustObject>

```

---

### Query Certificates

Retrieves the certificate object for the specified certificate ID. If the certificate ID is a chain, multiple certificate objects are retrieved.

#### Example 5-62. Query specific certificate

---

Request:

```
GET https://<vsm-ip>/api/2.0/services/truststore/certificate/<certificateId>
```

---

#### Example 5-63. Query all certificates for a scope

---

Request:

```
GET https://<vsm-ip>/api/2.0/services/truststore/certificate/scope/<scopeId>
```

---

### Delete Certificate

Deletes the specified certificate.

#### Example 5-64. Delete certificate

---

Request:

```
DELETE https://<vsm-ip>/api/2.0/services/truststore/certificate/<certificateId>
```

---

## Working with Certificate Signing Requests (CSRs)

Allows you to manage CSRs.

### Create CSR

#### Example 5-65. Create CSR

---

Request:

```
POST https://<vsm-ip>/api/2.0/services/truststore/csr/<scopeId>
```

Request Body:

```

<csr>
  <subject>
    <attribute>
      <key>CN</key>
      <value>VSM</value>
    </attribute>
    <attribute>
      <key>O</key>
      <value>VMware</value>
    </attribute>
    <attribute>
      <key>OU</key>
      <value>IN</value>
    </attribute>
    <attribute>
      <key>C</key>
      <value>IN</value>
    </attribute>
  </subject>

```

```

    </subject>
    <algorithm>RSA</algorithm>
    <keySize>1024</keySize>
</csr>

```

---

### Create Self Signed Certificate for CSR

**Example 5-66.** Create self signed certificate for CSR

---

Request:

PUT https://<vsm-ip>/api/2.0/services/truststore/csr/<csrId>?noOfDays=<value>

---

### Query CSRs

Retrieves specified CSR or all CSRs for specified scope.

**Example 5-67.** Query specific CSR

---

GET https://<vsm-ip>/api/2.0/services/truststore/csr/<csrId>

---

**Example 5-68.** Query CSRs for specific scope

---

GET https://<vsm-ip>/api/2.0/services/truststore/csr/scope/<scopeId>

Request Body:

```

<csrs>
  <csr>
    ...
  </csr>
  <csr>
    ...
  </csr>
  ...
</csrs>

```

---

## Working with Certificate Revocation List (CRL)

Allows you to manage CRLs.

### Create a CRL

Creates a CRL on the specified scope.

**Example 5-69.** Create CRL

---

Request:

POST https://<vsm-ip>/api/2.0/services/truststore/crl/<scopId>

Request Body:

```

<trustObject>
  <pemEncoding></pemEncoding>
</trustObject>

```

---

### Query CRL

Retrieves all CRLs certificates for the specified certificate or scope.

**Example 5-70.** Query CRL

---

Retrieve certificate object for the specified certificate ID:

GET https://<vsm-ip>/api/2.0/services/truststore/crl/<crlId>

Retrieve all certificates for the specified scope:

GET https://<vsm-ip>/api/2.0/services/truststore/crl/scope/<scopeId>

---

### Delete CRL

Deletes the specified CRL.

#### Example 5-71. Delete CRL

---

Request:

DELETE https://<vsm-ip>/api/2.0/services/truststore/crl/<crlId>

---

## Configure IPSEC VPN

vShield Edge modules support site-to-site IPsec VPN between a vShield Edge instance and remote sites.

You must configure the required certificates at the vShield Edge scope. For information on configuring certificates, see [“Configure Certificates”](#) on page 93.

#### Example 5-72. Configure IPSEC VPN

---

Request:

PUT https://<vsm-ip>/api/3.0/edges/<edgeId>/ipsec/config

Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<ipsec>
  <enabled>true</enabled> <!-- Optional, true by default -->
  <logging> <!-- optional. logging is disable by default. -->
    <logLevel>debug</logLevel> <!-- optional, default is info. -->
    <enable>true</enable> <!-- optional, default is false. -->
  </logging>
  <global>
    <psk>hello123</psk> <!-- Required only when peerIp is specified as any in siteConfig -->
    <serviceCertificate>certificate-4</serviceCertificate> <!-- Required when x.509 certificate mode is selected -->
    <caCertificates> <!-- Optional, CA list -->
      <caCertificate>certificate-3</caCertificate>
    </caCertificates>
    <crlCertificates> <!-- Optional, CRL list -->
      <crlCertificate>crl-1</crlCertificate>
    </crlCertificates>
  </global>
  <sites>
    <site>
      <enabled>true</enabled> <!-- Optional, true by default -->
      <name>VPN to edge-pa-1</name> <!-- Optional -->
      <description>psk VPN to edge-pa-1 192.168.11.0/24 == 192.168.1.0/24</description>
      <!-- Optional -->

      <localId>11.0.0.11</localId>
      <localIp>11.0.0.11</localIp>
      <peerId>11.0.0.1</peerId>
      <peerIp>any</peerIp> <!-- Can be a Ipv4Address such as 11.0.0.3 -->
      <encryptionAlgorithm>aes256</encryptionAlgorithm> <!-- Optional, default aes256 -->
      <authenticationMode>psk</authenticationMode> <!-- Possible values are psk and x.509 -->
      <!-- <psk>hello123</psk> --> <!-- Required if peerIp is not any -->
      <enablePfs>true</enablePfs> <!-- Optional, true by default -->
      <dhGroup>dh2</dhGroup> <!-- Optional, dh2 by default -->
      <localSubnets>
        <subnet>192.168.11.0/24</subnet>
      </localSubnets>
    </site>
  </sites>
</ipsec>
```



```

    <peerSubnets>
      <subnet>192.168.1.0/24</subnet>
    </peerSubnets>
  </site>
</sites>
<site>
  <name>VPN to edge-right</name>
  <description>certificate VPN to edge-right 192.168.22.0/24 == 192.168.2.0/24</description>
  <localId>11.0.0.12</localId>
  <localIp>11.0.0.12</localIp>
  <peerId>C=CN, ST=BJ, L=BJ, O=VMware, OU=DEV, CN=Right</peerId> <!-- Should be a DN if
    authenticationMode is x.509 -->
  <peerIp>11.0.0.2</peerIp>
  <encryptionAlgorithm>aes256</encryptionAlgorithm>
  <authenticationMode>x.509</authenticationMode>
  <enablePfs>true</enablePfs>
  <dhGroup>dh2</dhGroup>
  <localSubnets>
    <subnet>192.168.22.0/24</subnet>
  </localSubnets>
  <peerSubnets>
    <subnet>192.168.2.0/24</subnet>
  </peerSubnets>
</site>
</sites>
</ipsec>

```

---

## Retrieve IPSec Configuration

### Example 5-73. Get IPSec Configuration

---

Request:

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/ipsec/config

Response Body when IPSec is not configured:

```

<?xml version="1.0" encoding="UTF-8"?>
  <ipsec>
    <enabled>true</enabled>
    <logging>
      <enable>true</enable>
      <logLevel>debug</logLevel>
    </logging>
    <sites/> <!-- No site to site config present -->
  </ipsec>

```

Response Body when IPSec is configured for site-to-site:

```

<?xml version="1.0" encoding="UTF-8"?>
<ipsec>
  <enabled>true</enabled>
  <logging>
    <logLevel>debug</logLevel>
    <enable>true</enable>
  </logging>
  <global>
    <psk>hello123</psk>
    <serviceCertificate>certificate-4</serviceCertificate>
    <caCertificates> <!-- Optional, CA list -->
      <caCertificate>certificate-3</caCertificate>
    </caCertificates>
    <crlCertificates>
      <crlCertificate>crl-1</crlCertificate>
    </crlCertificates>
  </global>
  <sites>
    <site>

```

```

    <enabled>true</enabled>
    <name>VPN to edge-pa-1</name>
    <description>psk VPN to edge-pa-1 192.168.11.0/24 == 192.168.1.0/24</description>
    <localId>11.0.0.11</localId>
    <localIp>11.0.0.11</localIp>
    <peerId>11.0.0.1</peerId>
    <peerIp>any</peerIp>
    <encryptionAlgorithm>aes256</encryptionAlgorithm>
    <authenticationMode>psk</authenticationMode>
    <enablePfs>true</enablePfs>
    <dhGroup>dh2</dhGroup>
    <localSubnets>
      <subnet>192.168.11.0/24</subnet>
    </localSubnets>
    <peerSubnets>
      <subnet>192.168.1.0/24</subnet>
    </peerSubnets>
  </site>
</site>
  <name>VPN to edge-right</name>
  <description>certificate VPN to edge-right 192.168.22.0/24 == 192.168.2.0/24</description>
  <localId>11.0.0.12</localId>
  <localIp>11.0.0.12</localIp>
  <peerId>C=CN, ST=BJ, L=BJ, O=VMware, OU=DEV, CN=Right</peerId>
  <peerIp>11.0.0.2</peerIp>
  <encryptionAlgorithm>aes256</encryptionAlgorithm>
  <authenticationMode>x.509</authenticationMode>
  <enablePfs>true</enablePfs>
  <dhGroup>dh2</dhGroup>
  <localSubnets>
    <subnet>192.168.22.0/24</subnet>
  </localSubnets>
  <peerSubnets>
    <subnet>192.168.2.0/24</subnet>
  </peerSubnets>
</site>
</sites>
</ipsec>

```

---

## Retrieve IPSec Statistics

### Example 5-74. Get IPSEC statistics

---

Request:

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/ipsec/statistics

Response Body:

```

<?xml version="1.0" encoding="UTF-8"?>
<?xml version="1.0" encoding="UTF-8"?>
  <ipsecStatusAndStats>
    <siteStatistics>
      <ikeStatus>
        <channelStatus>up</channelStatus>
        <channelState>STATE_MAIN_I4 (ISAKMP SA established)</channelState>
        <lastInformationalMessage></lastInformationalMessage>
        <localIpAddress>10.0.0.12</localIpAddress>
        <peerId>11.0.0.12</peerId>
        <peerIpAddress>10.0.0.2</peerIpAddress>
      </ikeStatus>
    </siteStatistics>
    <tunnelStats>
      <tunnelStatus>up</tunnelStatus>
      <tunnelState>STATE_QUICK_I2 (sent QI2, IPsec SA established)</tunnelState>
      <lastInformationalMessage></lastInformationalMessage>
      <localSubnet>192.168.2.0/24</localSubnet>
      <peerSubnet>192.168.22.0/24</peerSubnet>
    </tunnelStats>
  </ipsecStatusAndStats>

```

```

        </tunnelStats>
    </siteStatistics>
    <siteStatistics>
        <ikeStatus>
            <channelStatus>up</channelStatus>
            <channelState>STATE_MAIN_I4 (ISAKMP SA established)</channelState>
            <lastInformationalMessage></lastInformationalMessage>
            <localIpAddress>10.0.0.11</localIpAddress>
            <peerId>11.0.0.11</peerId>
            <peerIpAddress>10.0.0.1</peerIpAddress>
        </ikeStatus>
        <tunnelStats>
            <tunnelStatus>up</tunnelStatus>
            <tunnelState>STATE_QUICK_I2 (sent QI2, IPsec SA established)</tunnelState>
            <lastInformationalMessage></lastInformationalMessage>
            <localSubnet>192.168.1.0/24</localSubnet>
            <peerSubnet>192.168.11.0/24</peerSubnet>
        </tunnelStats>
    </siteStatistics>
    <timeStamp>1325766138</timeStamp>
</ipsecStatusAndStats>

```

---

## Query Tunnel Traffic Statistics

Retrieves tunnel traffic statistics for the specified time interval. Default interval is 1 hour. Other possible values are 1-60 minutes | one day | one week | one month | one year.

### Example 5-75. Get tunnel traffic statistics

---

Request:

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/statistics/dashboard/ipsec?interval=<range>

Response Body:

```

<?xml version="1.0" encoding="UTF-8"?>
<dashboardStatistics>
    <meta>
        <startTime>1344809160</startTime>    <!-- in seconds -->
        <endTime>1344809460</endTime>    <!-- in seconds -->
        <interval>300</interval>
    </meta>
    <data>
        <ipsec>
            <ipsecTunnels>
                <dashboardStatistic>
                    <timestamp>1344809160</timestamp>
                    <value>0.0</value>
                </dashboardStatistic>
                <dashboardStatistic>
                    <timestamp>1344809460</timestamp>
                    <value>0.0</value>
                </dashboardStatistic>
            </ipsecTunnels>
            <ipsecBytesIn>
                <dashboardStatistic>
                    <timestamp>1344809160</timestamp>
                    <value>0.0</value>
                </dashboardStatistic>
                <dashboardStatistic>
                    <timestamp>1344809460</timestamp>
                    <value>0.0</value>
                </dashboardStatistic>
            </ipsecBytesIn>
            <ipsecBytesOut>
                <dashboardStatistic>
                    <timestamp>1344809160</timestamp>

```

```

        <value>0.0</value>
      </dashboardStatistic>
    <dashboardStatistic>
      <timestamp>1344809460</timestamp>
      <value>0.0</value>
    </dashboardStatistic>
  </ipsecBytesOut>
</ipsec>
</data>
</dashboardStatistics>

```

---

## Delete IPSec Configuration

Deletes the IPSEC configuration for the specified vShield Edge.

### Example 5-76. Delete IPSec

---

Request:

DELETE https://<vsm-ip>/api/3.0/edges/<edgeId>/ipsec/config/

---

## Managing SSL VPN

With SSL VPN-Plus, remote users can connect securely to private networks behind a vShield Edge gateway. Remote users can access servers and applications in the private networks.

### Enable or Disable SSL VPN

Enables or disables SSL VPN on the vShield Edge appliance.

### Example 5-77. Enable or disable SSL VPN

---

Request:

POST https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/?enableService=true|False

---

### Query SSL VPN Details

Retrieves SSL VPN details.

### Example 5-78. Get SSL VPN details

---

Request:

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/

---

## Manage Server Settings

### Apply Server Settings

Configures SSL VPN server on port 443 using the certificate named server-cert that is already uploaded on the vShield Edge appliance and the specified cipher.

### Example 5-79. Apply server settings

---

Request:

PUT https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/server/

Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<serverSettings>
  <ip>10.112.243.109</ip>          <!-- Ip of any of the external vnic -->
  <port>443</port>                <!-- optional. Default is 443 -->
  <!-- Certificate has to be generated using certificate REST API and id returned should be mentioned here-->
  <certificateId>certificate-1</certificateId> --> <!-- optional. -->
  <cipherList>                    <!-- Specify one of the below ciphers-->
    <cipher>RC4-MD5</cipher>|
    <cipher>AES128-SHA</cipher>|
    <cipher>AES256-SHA</cipher>|
    <cipher>DES-CBC3-SHA</cipher>
  </cipherList>
</serverSettings>
```

---

## Query Server Settings

Gets server settings.

### Example 5-80. Apply server settings

---

Request:

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/server/

Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<serverSettings>
  <ip>10.112.243.109</ip>
  <port>443</port>
  <certificateId>certificate-1</certificateId>
  <cipherList>
    <cipher>RC4-MD5</cipher>
  </cipherList>
</serverSettings>
```

---

## Configure Private Networks

### Add Private Network

Configures a private network that the administrator wants to expose to remote users over the SSL VPN tunnel.

### Example 5-81. Add private network

---

Request:

POST https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/client/networkextension/privatenetworks/

Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<privateNetwork>
  <description>This is a private network for UI-team</description>
  <network>192.168.1.0/24</network>
  <sendOverTunnel>                <!-- optional. -->
    <ports>20-40</ports>          <!-- optional. Default is 0-0 -->
    <optimize>>false</optimize>    <!-- optional. Default is true -->
  </sendOverTunnel>
  <enabled>true</enabled>         <!-- optional. Default is true-->
</privateNetwork>
```

---

### Modify Private Network

Modifies the specified private network in the SSL VPN service on vShield Edge.

**Example 5-82. Modify private network**

---

Request:

PUT https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/client/networkextension/privatenetworks/*privateNetworkID*

Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<privateNetwork>
  <description>This is a private network for UI-team</description>
  <network>192.168.1.0/24</network>
  <sendOverTunnel>
    <ports>20-40</ports>
    <optimize>>false</optimize>
  </sendOverTunnel>
  <enabled>true</enabled>
</privateNetwork>
```

---

**Query Specific Private Network**

Gets the specified private network profile in the SSL VPN instance on vShield Edge.

**Example 5-83. Query private network**

---

Request:

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/client/networkextension/privatenetworks/*privateNetworkID*

Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<privateNetwork>
  <description>This is a private network for UI-team</description>
  <network>192.168.1.0/24</network>
  <sendOverTunnel>
    <ports>20-40</ports>
    <optimize>>false</optimize>
  </sendOverTunnel>
  <enabled>true</enabled>
</privateNetwork>
```

---

**Query all Private Networks**

Gets all private network profiles in the SSL VPN instance on vShield Edge.

**Example 5-84. Query private network**

---

Request:

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/client/networkextension/privatenetworks/

Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<privateNetwork>
  <privateNetwork>
    <objectId>privatenetwork-1</objectId>
    <description>This is a private network for pune-qa-team</description>
    <network>192.168.1.0/24</network>
    <sendOverTunnel>
      <ports>10-20</ports>
      <optimize>true</optimize>
    </sendOverTunnel>
    <enabled>true</enabled>
  </privateNetwork>
```

---

```
</privateNetwork>
```

---

### Delete Private Network

Deletes the specified dynamic IP address configuration from the SSL VPN instance on vShield Edge.

#### Example 5-85. Delete private network

---

Request:

```
DELETE https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/client/networkextension/
        privatenetworks/<privatenetworkID>
```

---

### Delete all Private Network

Deletes all dynamic IP address configurations from the SSL VPN instance on VShield Edge.

#### Example 5-86. Delete private network

---

Request:

```
DELETE https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/client/networkextension/
        privatenetworks/
```

---

### Apply All Private Networks

Updates all private network configurations of vShield Edge with the given list of private network configurations. If the configuration is present, it is updated; if it is not present, a new private network configuration is created. Existing configurations not included in the REST call are deleted.

#### Example 5-87. Apply all private networks

---

Request:

```
PUT https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/client/networkextension/
        privatenetworks/
```

---

## Configure Web Resource

### Add Portal Web Resource

Adds a web access server that the remote user can connect to via a web browser.

#### Example 5-88. Add portal web resource

---

Request:

```
POST https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/webresources/
```

Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<webResource>
  <name>VMware</name>
  <url>http://www.vmware.com</url>
  <method name="POST">
    <data>username=stalin </data>
  </method>
  <description>Click here to visit the corporate intranet Homepage </description>
  <enabled>true</enabled>      <!--optional. Default is true-->
</webResource>
```

---

**Modify Portal Web Resource**

Modifies the specified web access server.

**Example 5-89. Modify portal web resource**

---

Request:

PUT https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/webresources/*ID*

Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<webResource>
  <name>VMware</name>
  <url>http://www.vmware.com</url>
  <method name="POST">
    <data>username=stalin </data>
  </method>
  <description>Click here to visit the corporate intranet Homepage </description>
  <enabled>true</enabled>      <!--optional. Default is true-->
</webResource>
```

---

**Query Portal Web Resource**

Gets the specified web access server.

**Example 5-90. Get specific portal web resource**

---

Request:

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/webresources/*ID*

Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<webResource>
  <name>VMware</name>
  <url>http://www.vmware.com</url>
  <method name="POST">
    <data>username=stalin </data>
  </method>
  <description>Click here to visit the corporate intranet Homepage </description>
  <enabled>true</enabled>      <!--optional. Default is true-->
</webResource>
```

---

**Query all Web Resources**

Gets all web resources on the SSL VPN instance.

**Example 5-91. Get portal web resource**

---

Request:

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/webresources/

Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<webResources>
  <webResource>
    <objectId>webresource-1</objectId>
    <name>VMware</name>
    <url>http://www.vmware.com</url>
    <method name="POST">
      <data>username=stalin </data>
    </method>
    <description>Click here to visit the corporate intranet Homepage </description>
```



```

        <enabled>true</enabled>
    </webResource>
</webResources>

```

---

### Delete Portal Web Resource

Deletes the specified web access server.

#### Example 5-92. Delete specific portal web resource

---

Request:

```
DELETE https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/webresources/ID
```

---

### Deletes all Web Resources

Deletes all web resources on the SSL VPN instance.

#### Example 5-93. Deletes all portal web resources

---

Request:

```
DELETE https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/webresources/
```

---

### Apply All Web Resources

Updates web resource configurations of vShield Edge with the given list of web resource configurations. If the configuration is present, it is updated; if it is not present, a new web resource configuration is created. Existing configurations not included in the REST call are deleted.

#### Example 5-94. Apply all private networks

---

Request:

```
PUT https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/client/networkextension/
    privatenetworks/
```

---

## Configure Users

### Add User

Adds a new portal user.

#### Example 5-95. Add a user

---

Request:

```
POST https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/auth/localserver/users/
```

Request Body:

```

<?xml version="1.0" encoding="UTF-8"?>
  <user>
    <userId>stalin</userId>
    <password>apple@123</password>
    <firstName>STALIN</firstName>
    <lastName>RAJAKILLI</lastName>
    <description>This user belong to vsm team</description>
    <disableUserAccount>>false</disableUserAccount>      <!--optional. Default is false-->
    <passwordNeverExpires>true</passwordNeverExpires>    <!--optional. Default is false-->
    <allowChangePassword>
      <changePasswordOnNextLogin>>false</changePasswordOnNextLogin> <!--optional. Default is false-->
    </allowChangePassword>
  </user>

```

---

```
</user>
```

---

## Modify User

Modifies the specified portal user.

### Example 5-96. Modify user

---

Request:

PUT https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/auth/localserver/users/

Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
  <user>
    <userId>stalin</userId>
    <password>apple@123</password>
    <firstName>STALIN</firstName>
    <lastName>RAJAKILLI</lastName>
    <description>This user belong to vsm team</description>
    <disableUserAccount>false</disableUserAccount>      <!--optional. Default is false-->
    <passwordNeverExpires>true</passwordNeverExpires>    <!--optional. Default is false-->
    <allowChangePassword>
      <changePasswordOnNextLogin>false</changePasswordOnNextLogin> <!--optional. Default is false-->
    </allowChangePassword>
  </user>
```

---

## Query User Details

Gets information about the specified user.

### Example 5-97. Query user

---

Request:

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/auth/localserver/users/*userID*

Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<users>
  <user>
    <userId>stalin</userId>
    <firstName>Bob</firstName>
    <lastName>Weber</lastName>
    <disableUserAccount>false</disableUserAccount>      <!--optional. Default is false-->
    <passwordNeverExpires>true</passwordNeverExpires>    <!--optional. Default is false-->
    <allowChangePassword>
      <changePasswordOnNextLogin>false</changePasswordOnNextLogin> <!--optional. Default is false-->
    </allowChangePassword>
  </user>
```

---

## Delete User

Deletes specified user.

### Example 5-98. Delete user

---

Request:

DELETE https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/auth/localserver/users/*userID*

---

### Delete all Users

Deletes all users on the specified SSL VPN instance.

#### Example 5-99. Delete all user

---

Request:

DELETE https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/auth/localserver/users/

---

### Apply all Users

Updates all users of vShield Edge with the given list of users. If the user is present, it is updated; if it is not present, a new user is created. Existing users not included in the REST call are deleted.

#### Example 5-100. Apply all users

---

Request:

PUT https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/auth/localusers/users/

Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<users>
  <user>
    <userId>stalin</userId>
    <password>apple@123</password>
    <firstName>Bob</firstName>
    <lastName>Weber</lastName>
    <description>This user belong to vsm team</description>
    <disableUserAccount>false</disableUserAccount>
    <passwordNeverExpires>true</passwordNeverExpires>
    <allowChangePassword>
      <changePasswordOnNextLogin>false</changePasswordOnNextLogin>
    </allowChangePassword>
  </user>
</users>
```

---

### Configure IP Pool

You can add, edit, or delete an IP pool.

#### Add IP Pool

Creates an IP pool that will be used to assign IP address to remote users.

#### Example 5-101. Add IP pool

---

Request:

POST https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/client/networkextension/ippools/

Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<ipAddressPool>
  <description>description</description>
  <ipRange>10.112.243.11-10.112.243.57</ipRange>
  <netmask>255.0.0.0</netmask>
  <gateway>192.168.1.1</gateway>
  <primaryDns>192.168.10.1</primaryDns>      <!--optional. -->
  <secondaryDns>4.2.2.2</secondaryDns>      <!--optional. -->
  <dnsSuffix></dnsSuffix>
  <winsServer>10.112.243.201</winsServer>
  <enabled>true</enabled>                    <!--optional. Default is true-->
</ipAddressPool>
```

---

```
</ipAddressPool>
```

---

### Modify IP Pool

Modifies the specified IP pool.

#### Example 5-102. Modify IP pool

---

Request:

PUT https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/client/networkextension/ippools/*ippoolID*

Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<ipAddressPool>
  <description>description</description>
  <ipRange>10.112.243.11-10.112.243.57</ipRange>
  <netmask>255.0.0.0</netmask>
  <gateway>192.168.1.1</gateway>
  <primaryDns>192.168.10.1</primaryDns>
  <secondaryDns>4.2.2.2</secondaryDns>
  <dnsSuffix></dnsSuffix>
  <winsServer>10.112.243.201</winsServer>
  <enabled>true</enabled>
</ipAddressPool>
```

---

### Query IP Pool

Gets details of the IP pool.

#### Example 5-103. Get IP pool

---

Request:

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/client/networkextension/ippools/*ippoolID*

Response Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<ipAddressPool>
  <objectId>ipPool-1</objectId>
  <description>description</description>
  <ipRange>10.112.243.11-10.112.243.57</ipRange>
  <netmask>255.0.0.0</netmask>
  <gateway>192.168.1.1</gateway>
  <primaryDns>192.168.10.1</primaryDns>      <!--optional. -->
  <secondaryDns>4.2.2.2</secondaryDns>      <!--optional. -->
  <dnsSuffix></dnsSuffix>
  <winsServer>10.112.243.201</winsServer>
  <enabled>true</enabled>                    <!--optional. Default is true-->
</ipAddressPool>
```

---

### Query all IP Pools

Gets all IP pools configured on the SSL VPN instance.

#### Example 5-104. Gets all IP pools

---

Request:

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/client/networkextension/ippools/

Response Body:

```
<?xml version="1.0" encoding="UTF-8"?>
```

```

<ipAddressPool>
  <objectId>ipPool-1</objectId>
  <description>description</description>
  <ipRange>10.112.243.11-10.112.243.57</ipRange>
  <netmask>255.0.0.0</netmask>
  <gateway>192.168.1.1</gateway>
  <primaryDns>192.168.10.1</primaryDns>    <!--optional. -->
  <secondaryDns>4.2.2.2</secondaryDns>    <!--optional. -->
  <dnsSuffix></dnsSuffix>
  <winsServer>10.112.243.201</winsServer>
  <enabled>true</enabled>                  <!--optional. Default is true-->
</ipAddressPool>

```

---

### Delete IP Pool

Deletes the specified IP pool.

#### Example 5-105. Delete IP pool

Request:

```
DELETE https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/client/networkextension/
      ippools/ippoolID
```

---

### Deletes all IP Pools

Deletes all IP pools on the SSL VPN instance.

#### Example 5-106. Deletes all IP pools

Request:

```
DELETE https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/client/networkextension/
      ippools/
```

---

### Apply all IP Pools

Updates all IP pools of vShield Edge with the given list of users. If the IP pool is present, it is updated; if it is not present, a new IP pool is created. Existing pools not included in the REST call are deleted.

#### Example 5-107. Apply IP pools

Request:

```
PUT https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/client/networkextension/ippools/
```

Request Body:

```

<?xml version="1.0" encoding="UTF-8"?>
<ipAddressPools>
  <ipAddressPool>
    <description>description</description>
    <ipRange>10.112.243.11-10.112.243.57</ipRange>
    <netmask>255.0.0.0</netmask>
    <gateway>192.168.1.1</gateway>
    <primaryDns>192.168.10.1</primaryDns>
    <secondaryDns>4.2.2.2</secondaryDns>
    <dnsSuffix></dnsSuffix>
    <winsServer>10.112.243.201</winsServer>
    <enabled>true</enabled>
  </ipAddressPool>
</ipAddressPools>

```

---

## Configure Network Extension Client Parameters

### Apply Client Configuration

Sets advanced parameters for full access client configurations – such as whether client should auto-reconnect in case of network failures or network unavailability, or whether the client should be uninstalled after logout.

#### Example 5-108. Apply IP pools

---

Request:

PUT https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/client/networkextension/clientconfig/

Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<clientConfiguration>
  <autoReconnect>true</autoReconnect>      <!--optional. Default is false-->
  <fullTunnel>                                <!--optional. Default Tunnel mode is SPLIT-->
  <excludeLocalSubnets>true</excludeLocalSubnets> <!--optional. Default is false-->
    <gatewayIp>10.112.243.11</gatewayIp>
  </fullTunnel>
  <upgradeNotification>>false</upgradeNotification> <!--optional. Default is false-->
</clientConfiguration>
```

### Get Client Configuration

Gets information about the specified client.

#### Example 5-109. Get client configuration

---

Request:

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/client/networkextension/clientconfig/

Response Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<clientConfiguration>
  <autoReconnect>true</autoReconnect> <!--optional. Default is false-->
  <tunnelConfiguration>
    <excludeLocalSubnets>true</excludeLocalSubnets> <!--optional. Default is false-->
    <gatewayIp>10.112.243.11</gatewayIp>
  </tunnelConfiguration>
  <upgradeNotification>>false</upgradeNotification> <!--optional. Default is false-->
</clientConfiguration>
```

---

## Configure Network Extension Client Installation Package

You can add, delete, or edit an installation package for the SSL client.

### Add Client Installation Package

Creates setup executables (installers) for full access network clients. These setup binaries are later downloaded by remote clients and installed on their systems. The primary parameters needed to configure this setup are - hostname of the gateway, and its port and a profile name which is shown to the user to identify this connection. Administrator can also set few other parameters such as whether to automatically start the application on windows login, hide the system tray icon etc.

#### Example 5-110. Add installation package

---

Request:

POST https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/client/networkextension/installpackages/

Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
```

```

<clientInstallPackage>
  <profileName>client</profileName>
  <gatewayList>
    <gateway>
      <hostName>10.112.243.123</hostName>
      <port>443</port> <!--optional. Default is 443-->
    </gateway>
  </gatewayList>
  <startClientOnLogon>>false</startClientOnLogon> <!--optional. Default is false-->
  <hideSystrayIcon>true</hideSystrayIcon> <!--optional. Default is false-->
  <rememberPassword>true</rememberPassword> <!--optional. Default is false-->
  <silentModeOperation>true</silentModeOperation> <!--optional. Default is false-->
  <silentModeInstallation>>false</silentModeInstallation> <!--optional. Default is false-->
  <hideNetworkAdaptor>>false</hideNetworkAdaptor> <!--optional. Default is false-->
  <createDesktopIcon>true</createDesktopIcon> <!--optional. Default is true-->
  <enforceServerSecurityCertValidation>>false</enforceServerSecurityCertValidation> <!--optional. Default is true-->
  <createLinuxClient>>false</createLinuxClient> <!--optional. Default is false-->
  <createMacClient>>false</createMacClient> <!--optional. Default is false-->
  <description>windows client</description>
  <enabled>true</enabled> <!--optional. Default is true-->
</clientInstallPackage>

```

---

### Modify Client Installation Package

Modifies the specified installation package.

#### Example 5-111. Modify installation package

---

Request:

```
PUT https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/client/networkextension/
installpackages/ID
```

Response Body:

```

<?xml version="1.0" encoding="UTF-8"?>
<clientInstallPackage>
  <profileName>client</profileName>
  <gatewayList>
    <gateway>
      <hostName>10.112.243.123</hostName>
      <port>443</port> <!--optional. Default is 443-->
    </gateway>
  </gatewayList>
  <startClientOnLogon>>false</startClientOnLogon> <!--optional. Default is false-->
  <hideSystrayIcon>true</hideSystrayIcon> <!--optional. Default is false-->
  <rememberPassword>true</rememberPassword> <!--optional. Default is false-->
  <silentModeOperation>true</silentModeOperation> <!--optional. Default is false-->
  <silentModeInstallation>>false</silentModeInstallation> <!--optional. Default is false-->
  <hideNetworkAdaptor>>false</hideNetworkAdaptor> <!--optional. Default is false-->
  <createDesktopIcon>true</createDesktopIcon> <!--optional. Default is true-->
  <enforceServerSecurityCertValidation>>false</enforceServerSecurityCertValidation> <!--optional.
    Default is true-->
  <createLinuxClient>>false</createLinuxClient> <!--optional. Default is false-->
  <createMacClient>>false</createMacClient> <!--optional. Default is false-->
  <description>windows client</description>
  <enabled>true</enabled> <!--optional. Default is true-->
</clientInstallPackage>

```

---

### Modify Client Installation Package

Modifies the specified installation package.

#### Example 5-112. Modify installation package

---

Request:

PUT https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/client/networkextension/  
installpackages/*ID*

#### Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<clientInstallPackage>
  <profileName>client</profileName>
  <gatewayList>
    <gateway>
      <hostName>10.112.243.123</hostName>
      <port>443</port> <!--optional. Default is 443-->
    </gateway>
  </gatewayList>
  <startClientOnLogon>false</startClientOnLogon>      <!--optional. Default is false-->
  <hideSystrayIcon>true</hideSystrayIcon>      <!--optional. Default is false-->
  <rememberPassword>true</rememberPassword>      <!--optional. Default is false-->
  <silentModeOperation>true</silentModeOperation>      <!--optional. Default is false-->
  <silentModeInstallation>false</silentModeInstallation>      <!--optional. Default is false-->
  <hideNetworkAdaptor>false</hideNetworkAdaptor>      <!--optional. Default is false-->
  <createDesktopIcon>true</createDesktopIcon>      <!--optional. Default is true-->
  <enforceServerSecurityCertValidation>false</enforceServerSecurityCertValidation>      <!--optional.
    Default is true-->
  <createLinuxClient>false</createLinuxClient>      <!--optional. Default is false-->
  <createMacClient>false</createMacClient>      <!--optional. Default is false-->
  <description>windows client</description>
  <enabled>true</enabled>      <!--optional. Default is true-->
</clientInstallPackage>
```

---

### Query Client Installation Package

Gets information about the specified installation package.

#### Example 5-113. Query installation package

#### Request:

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/client/networkextension/  
installpackages/*ID*

#### Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<clientInstallPackage>
  <objectId>clientinstallpackage-1</objectId>
  <profileName>client</profileName> <gatewayList>
  <gatewayList>
    <gateway>
      <hostName>10.112.243.123</hostName>
      <port>443</port> <!--optional. Default is 443-->
    </gateway>
  </gatewayList>
  <startClientOnLogon>false</startClientOnLogon>
  <hideSystrayIcon>true</hideSystrayIcon>
  <rememberPassword>true</rememberPassword>
  <silentModeOperation>true</silentModeOperation>
  <silentModeInstallation>false</silentModeInstallation>
  <hideNetworkAdaptor>false</hideNetworkAdaptor>
  <createDesktopIcon>true</createDesktopIcon>
  <enforceServerSecurityCertValidation>false</enforceServerSecurityCertValidation>
  <createLinuxClient>false</createLinuxClient>
  <createMacClient>false</createMacClient>
  <description>windows client</description>
  <enabled>true</enabled>
</clientInstallPackage>
```

---



**Query all Client Installation Packages**

Gets information about all installation packages.

**Example 5-114.** Query all installation package

Request:

```
GET https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/client/networkextension/
installpackages/
```

Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<clientInstallPackages>
  <clientInstallPackage>
    <objectId>clientinstallpackage-1</objectId>
    <profileName>client</profileName> <gatewayList>
      <gateway>
        <hostName>10.112.243.123</hostName>
        <port>443</port>
      </gateway>
    </gatewayList>
    <startClientOnLogon>>false</startClientOnLogon>
    <hideSystrayIcon>true</hideSystrayIcon>
    <rememberPassword>true</rememberPassword>
    <silentModeOperation>true</silentModeOperation>
    <silentModeInstallation>>false</silentModeInstallation>
    <hideNetworkAdaptor>>false</hideNetworkAdaptor>
    <createDesktopIcon>true</createDesktopIcon>
    <enforceServerSecurityCertValidation>>false</enforceServerSecurityCertValidation>
    <createLinuxClient>>false</createLinuxClient>
    <createMacClient>>false</createMacClient>
    <description>windows client</description>
    <enabled>true</enabled>
  </clientInstallPackage>
</clientInstallPackages>
```

**Delete Client Installation Package**

Deletes the specified installation package.

**Example 5-115.** Delete installation package

Request:

```
DELETE https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/client/networkextension/
installpackages/ID
```

**Delete all Client Installation Packages**

Deletes all installation packages.

**Example 5-116.** Delete all installation packages

Request:

```
DELETE https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/client/networkextension/
installpackages/
```

## Apply all Installation Packages

Updates all installation packages on vShield Edge with the given list of installation packages. If the installation package is present, it is updated; if it is not present, a new installation package is created. Existing installation packages not included in the REST call are deleted.

### Example 5-117. Apply installation packages

---

Request:

PUT https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/client/networkextension/  
installpackages/

Request Body:

```
<clientInstallPackages>
  <clientInstallPackage>
    <objectId>clientinstallpackage-1</objectId>
    <profileName>client</profileName> <gatewayList>
    <gatewayList>
      <gateway>
        <hostName>10.112.243.123</hostName>
        <port>443</port>
      </gateway>
    </gatewayList>
    <startClientOnLogon>false</startClientOnLogon>
    <hideSystrayIcon>true</hideSystrayIcon>
    <rememberPassword>true</rememberPassword>
    <silentModeOperation>true</silentModeOperation>
    <silentModeInstallation>false</silentModeInstallation>
    <hideNetworkAdaptor>false</hideNetworkAdaptor>
    <createDesktopIcon>true</createDesktopIcon>
    <enforceServerSecurityCertValidation>false</enforceServerSecurityCertValidation>
    <createLinuxClient>false</createLinuxClient>
    <createMacClient>false</createMacClient>
    <description>windows client</description>
    <enabled>true</enabled>
  </clientInstallPackage>
</clientInstallPackage>
```

---

## Configure Portal Layouts

You can configure the web layout bound to the SSL VPN client.

### Upload Portal Logo

Uploads the portal logo from the given local path.

### Example 5-118. Upload portal logo

---

Request:

POST https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/layout/images/portallogo/

---

### Upload Phat Banner

Uploads the phat client banner from the given local path. The phat banner image must in the bmp format.

### Example 5-119. Upload phat banner

---

Request:

POST https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/layout/images/phatbanner/

---

**Upload Client Connected Icon**

Uploads the client connected icon from the given local path. The icon image must be of type ico.

**Example 5-120.** Upload client connected icon

Request:

POST https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/layout/images/connecticon/

**Upload Client Disconnected Icon**

Uploads the client disconnected icon from the given local path. The icon image must be of type ico.

**Example 5-121.** Upload client disconnected icon

Request:

POST https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/layout/images/disconnecticon/

**Upload Client Desktop Icon**

Uploads the client desktop icon from the given local path. The icon image must be of type ico.

**Example 5-122.** Upload client desktop icon

Request:

POST https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/layout/images/desktopicon/

**Upload Error Connected Icon**

Uploads the client error connected icon from the given local path. The icon image must be of type ico.

**Example 5-123.** Upload client desktop icon

Request:

POST https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/layout/images/erroricon/

**Apply Layout Configuration**

Sets the portal layout.

**Example 5-124.** Apply layout configuration

Request:

PUT https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/layout/images/

Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
  <layout>
    <!-- portal layout configuration-->
    <portalTitle>Pepsi Remote Access</portalTitle><!--optional. Default value is VMware -->
    <companyName>pepsi, Inc.</companyName><!--optional. Default value is VMware -->
    <!-- Portal Color Configuration-->
    <logoBackgroundColor>FFFFFF</logoBackgroundColor><!--optional. Default value is FFFFFFFF -->
    <titleColor>996600</titleColor><!--optional. Default value is 996600 -->
    <topFrameColor>000000</topFrameColor><!--optional. Default value is 000000 -->
    <menuBarColor>999999</menuBarColor><!--optional. Default value is 999999 -->
    <rowAlternativeColor>FFFFFF</rowAlternativeColor><!--optional. Default value is FFFFFFFF -->
    <bodyColor>FFFFFF</bodyColor><!--optional. Default value is FFFFFFFF -->
```

```
<rowColor>F5F5F5</rowColor><!--optional. Default value is F5F5F5 -->
</layout>
```

---

### Query Portal Layout

gets the portal layout configuration.

#### Example 5-125. Apply layout configuration

---

Request:

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/layout/

Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
  <layout>
    <!-- portal layout configuration-->
    <portalTitle>Pepsi Remote Access</portalTitle><!--optional. Default value is VMware -->
    <companyName>pepsi, Inc.</companyName><!--optional. Default value is VMware -->
    <!-- Portal Color Configuration-->
    <logoBackgroundColor>FFFFFF</logoBackgroundColor><!--optional. Default value is FFFFFFFF -->
    <titleColor>996600</titleColor><!--optional. Default value is 996600 -->
    <topFrameColor>000000</topFrameColor><!--optional. Default value is 000000 -->
    <menuBarColor>999999</menuBarColor><!--optional. Default value is 999999 -->
    <rowAlternativeColor>FFFFFF</rowAlternativeColor><!--optional. Default value is FFFFFFFF -->
    <bodyColor>FFFFFF</bodyColor><!--optional. Default value is FFFFFFFF -->
    <rowColor>F5F5F5</rowColor><!--optional. Default value is F5F5F5 -->
  </layout>
```

---

### Configure Authentication Parameters

You can add an external authentication server (AD, LDAP, Radius, or RSA) which is bound to the SSL gateway. All users in the bounded authenticated server will be authenticated.

#### Upload RSA Config File

Uploads the RSA configuration file to vShield Manager.

#### Example 5-126. Upload RSA config file

---

Request:

POST https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/auth/settings/rsaconfigfile/

---

### Apply Authentication Configuration

Sets authentication process for remote users. The administrator specifies whether username password based authentication should be enabled and the list and details of authentication servers such as active directory, ldap, radius etc. The administrator can also enable client certificate based authentication.

#### Example 5-127. Apply Authentication Configuration

---

Request:edgeId

PUT https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/auth/settings/

Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<authenticationConfig>
  <passwordAuthentication>
    <authenticationTimeout>1</authenticationTimeout>    <!--optional. Default value is 1 mins-->
    <!-- Only four auth servers can be part of authentication configuration including secondary auth server and can be of type
        AD,LDAP,RADIUS,LOCAL and RSA -->
```

```

<primaryAuthServers>
  <com.vmware.vshield.edge.sslvpn.dto.LdapAuthServerDto>
    <ip>1.1.1.1</ip>
    <port>90</port> <!--optional. Default value is 639 if ssl enabled or 389 for normal cfg-->
    <timeOut>20</timeOut> <!--optional. Default value is 10 secs-->
    <enableSsl>false</enableSsl> <!--optional. Default is false-->
    <searchBase>searchbasevalue</searchBase>
    <bindDomainName>binddnvalue</bindDomainName>
    <bindPassword>password</bindPassword> <!--optional.-->
    <loginAttributeName>cain</loginAttributeName> <!--optional. Default is sAMAccountName -->
    <searchFilter>found</searchFilter> <!--optional. Default is 'objectClass=*'-->
    <enabled>true</enabled> <!--optional. Default is ture-->
  </com.vmware.vshield.edge.sslvpn.dto.LdapAuthServerDto>
  <com.vmware.vshield.edge.sslvpn.dto.RadiusAuthServerDto>
    <ip>3.3.3.3</ip>
    <port>90</port> <!--optional. Default value is 1812-->
    <timeOut>20</timeOut> <!--optional. Default value is 10 secs-->
    <secret>struct9870</secret>
    <nasIp>1.1.1.9</nasIp> <!--optional. Default value is 0.0.0.0-->
    <retryCount>10</retryCount> <!--optional. Default value is 3-->
  </com.vmware.vshield.edge.sslvpn.dto.RadiusAuthServerDto>
  <com.vmware.vshield.edge.sslvpn.dto.LocalAuthServerDto>
    <!--Only one Local auth server can be part of authentication configuration -->
    <enabled>true</enabled>
    <passwordPolicy> <!-- optional. -->
      <minLength>1</minLength> <!--optional. Default value is 1-->
      <maxLength>1</maxLength> <!--optional. Default value is 63-->
      <minAlphabets>0</minAlphabets> <!--optional -->
      <minDigits>0</minDigits> <!--optional -->
      <minSpecialChar>1</minSpecialChar> <!--optional -->
      <allowUserIdWithinPassword>false</allowUserIdWithinPassword> <!-- optional. Default value is false -->
      <passwordLifeTime>20</passwordLifeTime> <!--optional. Default value is 30 days-->
      <expiryNotification>1</expiryNotification> <!--optional. Default value is 25 days-->
    </passwordPolicy>
    <accountLockoutPolicy> <!--optional -->
      <retryCount>3</retryCount> <!--optional. Default value is 3-->
      <retryDuration>3</retryDuration> <!--optional. Default value is 2 days -->
      <lockoutDuration>3</lockoutDuration> <!--optional. Default value is 2 days -->
    </accountLockoutPolicy>
  </com.vmware.vshield.edge.sslvpn.dto.LocalAuthServerDto>
  <!-- Only one RSA auth server can be configured. RSA configuration file has to be uploaded prior to config RSA
  auth server RSA timeOut is optional. Default value is 60 secs-->
  <com.vmware.vshield.edge.sslvpn.dto.RsaAuthServerDto>
    <timeOut>20</timeOut>
    <sourceIp>1.2.2.3</sourceIp>
  </com.vmware.vshield.edge.sslvpn.dto.RsaAuthServerDto> -->
</primaryAuthServers>
<secondaryAuthServer>
  <!--Any one of the auth server AD, LDAP, RSA, LOCAL or RADIUS can be sec auth server -->
  <com.vmware.vshield.edge.sslvpn.dto.AdAuthServerDto>
    <ip>1.1.1.1</ip>
    <port>90</port> <!--optional. Default value is 639 if ssl enabled or 389 for normal cfg-->
    <timeOut>20</timeOut> <!--optional. Default value is 10 secs-->
    <enableSsl>false</enableSsl> <!--optional. Default is false-->
    <searchBase>searchbasevalue</searchBase>
    <bindDomainName>binddnvalue</bindDomainName>
    <bindPassword>password</bindPassword> <!--optional. -->
    <loginAttributeName>cain</loginAttributeName> <!--optional. Default is sAMAccountName -->
    <searchFilter>found</searchFilter> <!--optional. Default is 'objectClass=*'-->
    <terminateSessionOnAuthFails>false</terminateSessionOnAuthFails> <!--optional. Default is false-->
    <enabled>true</enabled>
  </com.vmware.vshield.edge.sslvpn.dto.AdAuthServerDto>
</secondaryAuthServer>
</passwordAuthentication>
</authenticationConfig>

```

## Query Authentication Configuration

Gets information about the specified authentication server.

### Example 5-128. Apply Authentication Configuration

---

Request:

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/auth/settings/

Response Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<com.vmware.vshield.edge.sslvpn.dto.AuthenticationConfigurationDto>
  <passwordAuthentication>
    <authenticationTimeout>1</authenticationTimeout>
    <primaryAuthServers>
      <com.vmware.vshield.edge.sslvpn.dto.AdAuthServerDto>
        <ip>1.1.1.1</ip>
        <port>90</port>
        <timeOut>20</timeOut>
        <enableSsl>>false</enableSsl>
        <searchBase>searchbasevalue</searchBase>
        <bindDomainName>binddnvalue</bindDomainName>
        <bindPassword>password</bindPassword>
        <loginAttributeName>cain</loginAttributeName>
        <searchFilter>found</searchFilter>
        <enabled>true</enabled>
      </com.vmware.vshield.edge.sslvpn.dto.AdAuthServerDto>
    </primaryAuthServers>
    <secondaryAuthServer>
      <com.vmware.vshield.edge.sslvpn.dto.AdAuthServerDto>
        <ip>1.1.1.1</ip>
        <port>90</port>
        <timeOut>20</timeOut>
        <enableSsl>>false</enableSsl>
        <searchBase>searchbasevalue</searchBase>
        <bindDomainName>binddnvalue</bindDomainName>
        <bindPassword>password</bindPassword>
        <loginAttributeName>cain</loginAttributeName>
        <searchFilter>found</searchFilter>
        <terminateSessionOnAuthFails>>false</terminateSessionOnAuthFails>
        <enabled>true</enabled>
      </com.vmware.vshield.edge.sslvpn.dto.AdAuthServerDto>
    </secondaryAuthServer>
  </passwordAuthentication>
</authenticationConfig>
```

---

## Configure SSL VPN Advanced Configuration

### Apply advanced configuration

Applies advanced configuration.

### Example 5-129. Apply advanced configuration

---

Request:

PUT https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/advancedconfig/

Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<advancedConfig>
  <enableCompression>>false</enableCompression>      <!--optional. Default is false-->
  <forceVirtualKeyboard>>false</forceVirtualKeyboard>  <!--optional. Default is false-->
  <preventMultipleLogon>true</preventMultipleLogon>   <!--optional. Default is false-->
  <randomizeVirtualkeys>>false</randomizeVirtualkeys>  <!--optional. Default is false-->
```

```

<timeout>                                <!--optional. -->
  <forcedTimeout>16</forcedTimeout>      <!--optional. Value is in minute(s)-->
  <sessionIdleTimeout>10</sessionIdleTimeout> <!--optional. Default is 10 mins-->
</timeout>
<clientNotification></clientNotification>
<enablePublicUrlAccess>false</enablePublicUrlAccess> <!--optional. Default is false-->
<enableLogging>false</enableLogging>          <!--optional. Default is false-->
</advancedConfig>

```

---

## Query Advanced Configuration

Retrieves SSL VPN advanced configuration.

### Example 5-130. Query advanced configuration

Request:

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/advancedconfig/

Response Body:

```

<?xml version="1.0" encoding="UTF-8"?>
<advancedConfig>
  <enableCompression>false</enableCompression>    <!--optional. Default is false-->
  <forceVirtualKeyboard>false</forceVirtualKeyboard> <!--optional. Default is false-->
  <preventMultipleLogon>true</preventMultipleLogon>  <!--optional. Default is false-->
  <randomizeVirtualkeys>false</randomizeVirtualkeys> <!--optional. Default is false-->
  <timeout>                                <!--optional. -->
    <forcedTimeout>16</forcedTimeout>              <!--optional. Value is in minute(s)-->
    <sessionIdleTimeout>10</sessionIdleTimeout>      <!--optional. Default is 10 mins-->
  </timeout>
  <clientNotification></clientNotification>
  <enablePublicUrlAccess>false</enablePublicUrlAccess> <!--optional. Default is false-->
  <enableLogging>false</enableLogging>              <!--optional. Default is false-->
</advancedConfig>

```

---

## Working with Active Clients

You can retrieve a list of active clients for the SSL VPN session and disconnect a specific client.

### Query Active Clients

Retrieves a list of active clients for the SSL VPN session.

### Example 5-131. Query active clients

Request:

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/activesessions/

Response Body:

```

<?xml version="1.0" encoding="UTF-8"?>
<activeSessions>
  <activeSession>
    <sessionId>488382</sessionId>
    <sessionType>PHAT</sessionType>
    <userName>demo</userName>
    <startTime>2011-09-24-06:00</startTime>
    <upTime>101400</upTime>
    <idleTime>2</idleTime>
    <totalNonTcpBytesReceived>6576</totalNonTcpBytesReceived>
    <totalTcpBytesReceived>30816</totalTcpBytesReceived>
    <totalNonTcpBytesSent>0</totalNonTcpBytesSent>
    <totalTcpBytesSent>152722</totalTcpBytesSent>
    <clientInternalIp>1.0.192.10</clientInternalIp>
    <clientVirtualIP>192.168.27.20</clientVirtualIP>
  </activeSession>

```

```

    <clientExternalNatIp>10.112.243.227</clientExternalNatIp>
    <clientExternalNatPort>50498</clientExternalNatPort>
    <totalConnections>2</totalConnections>
    <totalActiveConnection>4</totalActiveConnection>
  </activeSession>
</activeSessions>

```

---

### Disconnect Active Client

Disconnects an active client.

#### Example 5-132. Disconnect active client

---

Request:

DELETE <https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/activesessions/sessionId>

---

### Manage Logon and Logoff scripts

You can bind a login or logoff script to the vShield Edge gateway.

#### Upload Script

You can add multiple login or logoff scripts. For example, you can bind a login script for starting Internet Explorer with gmail.com. When the remote user logs in to the SSL client, Internet Explorer opens up gmail.com.

The upload script returns a script file ID which is used to configure the file parameters.

#### Example 5-133. Upload script

---

Request:

POST <https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/script/file/>

---

#### Configure Script Parameters

Configures parameters associated with the uploaded script file.

#### Example 5-134. Add script parameters

---

Request:

POST <https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/script/>

Request Body:

```

<?xml version="1.0" encoding="UTF-8"?>
<logonLogoffScript>
  <scriptId>loginlogoffscriptfile-12</scriptId>  <!-- Script file id generated using upload script file REST API-->
  <type>BOTH</type>
  <description>Testing modify script</description>
  <enabled>>false</enabled>  <!--optional. Default is true -->
</logonLogoffScript>

```

---

#### Modify Script Configuration

Modifies the parameters associated with the specified script file ID.

#### Example 5-135. Modify script parameters

---

Request:



PUT https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/script/*scriptId*

Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<loginLogoffScript>
  <scriptId>loginlogoffscriptfile-12</scriptId>
  <type>BOTH</type>
  <description>Testing modify sscript</description>
  <enabled>>false</enabled>
</loginLogoffScript>
```

---

### Query Script Configuration

Retrieves parameters associated with the specified script file ID.

#### Example 5-136. Get script parameters

---

Request:

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/script/*scriptId*

Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<loginLogoffScript>
  <objectId>loginlogoffscript-1</objectId>
  <scriptId>loginlogoffscriptfile-12</scriptId>
  <type>BOTH</type>
  <description>Testing modify script</description>
  <scriptIdUri>https://<vsm-ip>/api/3.0/edges/<edge-id>/sslvpn/config/script/file/scriptId/
    scriptIdUri
  <enabled>>false</enabled>
</loginLogoffScript>
```

---

### Query All Script Configurations

Retrieves all script configurations for the specified vShield Edge.

#### Example 5-137. Get all script parameters

---

Request:

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/script/

Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<loginLogoffScript>
  <loginLogoffScript>
    <scriptId>loginlogoffscriptfile-12</scriptId>
    <type>BOTH</type>
    <description>Testing modify sscript</description>
    <enabled>>false</enabled>
  </loginLogoffScript>
</loginLogoffScript>
```

---

### Delete Script Configuration

Deletes the parameters associated with the specified script file ID.

#### Example 5-138. Delete script parameters

---

Request:

DELETE https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/script/scriptFileId

---

### Delete All Script Configurations

Deletes all script configurations for the specified vShield Edge.

#### Example 5-139. Delete script parameters

---

Request:

DELETE https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/script/

---

### Apply All Script Configurations

Updates all script configurations on the specified vShield Edge with the given list of configurations. If the configuration is present, it is updated; if it is not present, a new configuration is created. Existing configurations not included in the REST call are deleted.

#### Example 5-140. Apply script configurations

---

Request:

PUT https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/script/

Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<logonLogoffScript>
  <logonLogoffScript>
    <objectId>logonlogoffscript-1</objectId>
    <scriptId>logonlogoffscriptfile-12</scriptId>
    <type>BOTH</type>
    <enabled>>false</enabled>
    <description>This script will run on both login and logoff of phat client</description>
  </logonLogoffScript>
</logonLogoffScript>
```

---

### Reconfigure SSL VPN

Pushes the entire configurations of the SSL VPN to the specified vShield Edge.

#### Example 5-141. Reconfigure SSL VPN

---

Request:

PUT https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/

Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<sslvpnConfig>
  <enabled>true</enabled>
  <logging> <!-- optional . -->
    <enable>>false</enable>
    <logLevel>debug</logLevel>
  </logging>
  <serverSettings>
    <ip>10.112.243.109</ip>
    <port>443</port> <!--optional. Default is 443 -->
    <!-- Certificate has to be generated using certificate REST API and id returned should be mentioned here-->
    <!--<certificateId>certificate-1</certificateId> --> <!-- optional -->
    <cipherList> <!-- any one or more of the following ciphers can be part of configuration -->
      <cipher>RC4-MD5</cipher>
      <cipher>AES128-SHA</cipher>
      <cipher>AES256-SHA</cipher>
```

```

        <cipher>DES-CBC3-SHA</cipher>
    </cipherList>
</serverSettings>
<privateNetworks>
    <privateNetwork>
        <description>This is a private network for UI-team</description>
        <network>192.168.1.0/24</network>
        <sendOverTunnel>
            <ports>20-40</ports>                                <!-- optional. Default is 0-0 -->
            <optimize>>false</optimize>                            <!--optional. Default is true -->
        </sendOverTunnel>
        <enabled>>true</enabled>                                    <!--optional. Default is true-->
    </privateNetwork>
</privateNetworks>
<users>
    <user>
        <userId>stalin</userId>
        <password>apple@123</password>
        <firstName>STALIN</firstName>
        <lastName>RAJAKILLI</lastName>
        <description>This user belong to vsm team</description>
        <disableUserAccount>>false</disableUserAccount>            <!--optional. Default is false-->
        <passwordNeverExpires>>true</passwordNeverExpires>        <!--optional. Default is false-->
        <allowChangePassword>
            <changePasswordOnNextLogin>>false</changePasswordOnNextLogin>    <!--optional. Default is false-->
        </allowChangePassword>
    </user>
</users>
<ipAddressPools>
    <ipAddressPool>
        <description>description</description>
        <ipRange>10.112.243.11-10.112.243.57</ipRange>
        <netmask>255.0.0.0</netmask>
        <gateway>192.168.1.1</gateway>
        <primaryDns>192.168.10.1</primaryDns>
        <secondaryDns>4.2.2.2</secondaryDns>
        <dnsSuffix></dnsSuffix>
        <winsServer>10.112.243.201</winsServer>
        <enabled>>true</enabled>                                    <!--optional. Default is true-->
    </ipAddressPool>
</ipAddressPools>
<clientInstallPackages>
    <clientInstallPackage>
        <profileName>client</profileName>
        <gatewayList>
            <gateway>
                <hostName>10.112.243.123</hostName>
                <port>443</port>                                    <!--optional. Default is 443-->
            </gateway>
        </gatewayList>
        <!-- Optional Parameters-->
        <startClientOnLogon>>false</startClientOnLogon>            <!--optional. Default is false-->
        <hideSystrayIcon>true</hideSystrayIcon>                    <!--optional. Default is false-->
        <rememberPassword>true</rememberPassword>                <!--optional. Default is false-->
        <silentModeOperation>true</silentModeOperation>            <!--optional. Default is false-->
        <silentModeInstallation>>false</silentModeInstallation>    <!--optional. Default is false-->
        <hideNetworkAdaptor>false</hideNetworkAdaptor>            <!--optional. Default is false-->
        <createDesktopIcon>true</createDesktopIcon>                <!--optional. Default is true-->
        <enforceServerSecurityCertValidation>>false</enforceServerSecurityCertValidation>
                                                                    <!--optional. Default is true-->
        <createLinuxClient>false</createLinuxClient>                <!--optional. Default is false-->
        <createMacClient>false</createMacClient>                    <!--optional. Default is false-->
        <description>windows client</description>
        <enabled>true</enabled>                                    <!--optional. Default is true-->
    </clientInstallPackage>
</clientInstallPackages>
<webResources>
    <webResource>

```

```

    <name>VMware</name>
    <url>http://www.vmware.com</url>
    <method name="POST">
        <data>username=stalin </data>
    </method>
    <description>Click here to visit the corporate intranet Homepage </description>
    <enabled>true</enabled>                                <!--optional. Default is true-->
</webResource>
</webResources>
<clientConfiguration>
    <autoReconnect>true</autoReconnect>                    <!--optional. Default is false-->
    <fullTunnel><!--optional. Default Tunnel mode is SPLIT-->
        <excludeLocalSubnets>true</excludeLocalSubnets>    <!--optional. Default is false-->
        <gatewayIp>10.112.243.11</gatewayIp>
    </fullTunnel>
    <upgradeNotification>false</upgradeNotification>        <!--optional. Default is false-->
</clientConfiguration>
<advancedConfig>
    <enableCompression>false</enableCompression>            <!--optional. Default is false-->
    <forceVirtualKeyboard>false</forceVirtualKeyboard>        <!--optional. Default is false-->
    <preventMultipleLogon>true</preventMultipleLogon>          <!--optional. Default is false-->
    <randomizeVirtualkeys>false</randomizeVirtualkeys>         <!--optional. Default is false-->
    <timeout><!--optional. -->
        <forcedTimeout>16</forcedTimeout>                    <!--optional. -->
        <sessionIdleTimeout>10</sessionIdleTimeout>           <!--optional. Default value is 10 mins-->
    </timeout>
    <clientNotification></clientNotification>
    <enablePublicUrlAccess>false</enablePublicUrlAccess>      <!--optional. Default is false-->
    <enableLogging>false</enableLogging>                      <!--optional. Default is false-->
</advancedConfig>
<authenticationConfiguration>
    <passwordAuthentication>
        <authenticationTimeout>1</authenticationTimeout>      <!--optional. Default value is 1 mins-->
        <!-- Only four auth servers can be part of authentication configuration including secondary auth server
            and can be of
            type AD,LDAP,RADIUS,LOCAL and RSA -->
    </passwordAuthentication>
    <primaryAuthServers>
        <com.vmware.vshield.edge.sslvpn.dto.LdapAuthServerDto>
            <ip>1.1.1.1</ip>
            <port>90</port>                                    <!--optional. Default value is 639 if ssl enabled or 389 for
                normal cfg-->
            <timeOut>20</timeOut>                              <!--optional. Default value is 10 secs-->
            <enableSsl>false</enableSsl>                        <!--optional. Default is false-->
            <searchBase>searchbasevalue</searchBase>
            <bindDomainName>binddnvalue</bindDomainName>
            <bindPassword>password</bindPassword>              <!--optional.-->
            <loginAttributeName>cain</loginAttributeName>      <!--optional. Default is sAMAccountName
                -->
            <searchFilter>found</searchFilter>                  <!--optional. Default is 'objectClass=*'-->
            <enabled>true</enabled>                             <!--optional. Default is ture-->
        </com.vmware.vshield.edge.sslvpn.dto.LdapAuthServerDto>
        <com.vmware.vshield.edge.sslvpn.dto.RadiusAuthServerDto>
            <ip>3.3.3.3</ip>
            <port>90</port>                                    <!--optional. Default value is 1812-->
            <timeOut>20</timeOut>                              <!--optional. Default value is 10 secs-->
            <secret>struct9870</secret>
            <nasIp>1.1.1.9</nasIp>                              <!--optional. Default value is 0.0.0.0-->
            <retryCount>10</retryCount>                         <!--optional. Default value is 3-->
        </com.vmware.vshield.edge.sslvpn.dto.RadiusAuthServerDto>
        <com.vmware.vshield.edge.sslvpn.dto.LocalAuthServerDto>
            <!--Only one Local auth server can be part of authentication configuration
                -->
            <enabled>true</enabled>
            <passwordPolicy>                                    <!-- optional. -->
                <minLength>1</minLength>                        <!--optional. Default value is 1-->
                <maxLength>63</maxLength>                       <!--optional. Default value is 63-->
                <minAlphabets>0</minAlphabets>                  <!--optional -->
                <minDigits>0</minDigits>                         <!--optional -->
            </passwordPolicy>
        </com.vmware.vshield.edge.sslvpn.dto.LocalAuthServerDto>
    </primaryAuthServers>
</authenticationConfiguration>

```

```

        <minSpecialChar>1</minSpecialChar>                                <!--optional -->
        <allowUserIdWithinPassword>>false</allowUserIdWithinPassword> <!-- optional. Default value is false
        -->
        <passwordLifeTime>20</passwordLifeTime>                        <!--optional. Default value is 30 days-->
        <expiryNotification>1</expiryNotification>                    <!--optional. Default value is 25 days-->
    </passwordPolicy>
    <accountLockoutPolicy>                                              <!--optional -->
        <retryCount>3</retryCount>                                    <!--optional. Default value is 3-->
        <retryDuration>3</retryDuration>                              <!--optional. Default value is 2 days -->
        <lockoutDuration>3</lockoutDuration>                          <!--optional. Default value is 2 days -->
    </accountLockoutPolicy>
</com.vmware.vshield.edge.sslvpn.dto.LocalAuthServerDto>
    <!-- Only one RSA auth server can be configured.RSA configuration file
    has to be uploaded prior to config RSA auth server RSA timeOut is optional. Default value is 60
    secs -->
<!--com.vmware.vshield.edge.sslvpn.dto.RsaAuthServerDto>
<timeOut>20</timeOut>
<sourceIp>1.2.2.3</sourceIp>
</com.vmware.vshield.edge.sslvpn.dto.RsaAuthServerDto> -->
</primaryAuthServers>
<secondaryAuthServer>
<!--Any of one of the auth server AD, LDAP, RSA, LOCAL or RADIUS can be sec auth server -->
    <com.vmware.vshield.edge.sslvpn.dto.AdAuthServerDto>
        <ip>1.1.1.1</ip>
        <port>90</port>                                              <!--optional. Default value is 639 if ssl enabled or 389 for
                                normal cfg-->
        <timeOut>20</timeOut>                                          <!--optional. Default value is 10 secs-->
        <enableSsl>>false</enableSsl>                                  <!--optional. Default is false-->
        <searchBase>searchbasevalue</searchBase>
        <bindDomainName>binddnvalue</bindDomainName>
        <bindPassword>password</bindPassword>                        <!--optional. -->
        <loginAttributeName>cain</loginAttributeName>                <!--optional. Default is sAMAccountName
                                -->
        <searchFilter>found</searchFilter>                            <!--optional. Default is 'objectClass=*'-->
        <terminateSessionOnAuthFails>>false</terminateSessionOnAuthFails>
                                <!--optional. Default is false-->
        <enabled>>true</enabled>
    </com.vmware.vshield.edge.sslvpn.dto.AdAuthServerDto>
</secondaryAuthServer>
</passwordAuthentication>
</authenticationConfiguration>
</sslvpnConfig>

```

## Query SSL VPN Configuration

Retrieves the SSL VPN configurations of the specified vShield Edge.

### Example 5-142. Query SSL VPN Configuration

Request:

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/

Response Body:

```

<?xml version="1.0" encoding="UTF-8"?>
<sslvpnConfig>
    <version>32</version>
    <enabled>>true</enabled>
    <logging> <!-- optional . -->
        <enable>>false</enable>
        <logLevel>debug</logLevel>
    </logging>
    <serverSettings>
        <ip>10.112.243.109</ip>
        <port>443</port>
        <certificateId>certificate-1</certificateId> -->
    </serverSettings>
</sslvpnConfig>

```

```

    <cipherList>
      <cipher>RC4-MD5</cipher>
      <cipher>AES128-SHA</cipher>
      <cipher>AES256-SHA</cipher>
      <cipher>DES-CBC3-SHA</cipher>
    </cipherList>
  </serverSettings>
  <privateNetworks>
    <privateNetwork>
      <description>This is a private network for UI-team</description>
      <network>192.168.1.0/24</network>
      <sendOverTunnel>
        <ports>20-40</ports>
        <optimize>>false</optimize>
      </sendOverTunnel>
      <enabled>>true</enabled>
    </privateNetwork>
  </privateNetworks>
  <users>
    <user>
      <userId>stalin</userId>
      <password>apple@123</password>
      <firstName>STALIN</firstName>
      <lastName>RAJAKILLI</lastName>
      <description>This user belong to vsm team</description>
      <disableUserAccount>>false</disableUserAccount>
      <passwordNeverExpires>>true</passwordNeverExpires>
      <allowChangePassword>
        <changePasswordOnNextLogin>>false</changePasswordOnNextLogin>
      </allowChangePassword>
    </user>
  </users>
  <ipAddressPools>
    <ipAddressPool>
      <description>description</description>
      <ipRange>10.112.243.11-10.112.243.57</ipRange>
      <netmask>255.0.0.0</netmask>
      <gateway>192.168.1.1</gateway>
      <primaryDns>192.168.10.1</primaryDns>
      <secondaryDns>4.2.2.2</secondaryDns>
      <dnsSuffix></dnsSuffix>
      <winsServer>10.112.243.201</winsServer>
      <enabled>>true</enabled>
    </ipAddressPool>
  </ipAddressPools>
  <clientInstallPackages>
    <clientInstallPackage>
      <profileName>client</profileName>
      <gatewayList>
        <gateway>
          <hostName>10.112.243.123</hostName>
          <port>443</port>
        </gateway>
      </gatewayList>
      <!-- Optional Parameters-->
      <startClientOnLogon>>false</startClientOnLogon>
      <hideSystrayIcon>true</hideSystrayIcon>
      <rememberPassword>true</rememberPassword>
      <silentModeOperation>true</silentModeOperation>
      <silentModeInstallation>>false</silentModeInstallation>
      <hideNetworkAdaptor>false</hideNetworkAdaptor>
      <createDesktopIcon>true</createDesktopIcon>
      <enforceServerSecurityCertValidation>>false</enforceServerSecurityCertValidation>
      <createLinuxClient>false</createLinuxClient>
      <createMacClient>false</createMacClient>
      <description>windows client</description>
      <enabled>true</enabled>
    </clientInstallPackage>
  </clientInstallPackages>

```

```

</clientInstallPackages>
<webResources>
  <webResource>
    <name>VMware</name>
    <url>http://www.vmware.com</url>
    <method name="POST">
      <data>username=stalin </data>
    </method>
    <description>Click here to visit the corporate intranet Homepage </description>
    <enabled>true</enabled>
  </webResource>
</webResources>
<clientConfiguration>
  <autoReconnect>true</autoReconnect>
  <fullTunnel>
    <excludeLocalSubnets>true</excludeLocalSubnets>
    <gatewayIp>10.112.243.11</gatewayIp>
  </fullTunnel>
  <upgradeNotification>false</upgradeNotification>
</clientConfiguration>
<advancedConfig>
  <enableCompression>false</enableCompression>
  <forceVirtualKeyboard>false</forceVirtualKeyboard>
  <preventMultipleLogon>true</preventMultipleLogon>
  <randomizeVirtualkeys>false</randomizeVirtualkeys>
  <timeout>
    <forcedTimeout>16</forcedTimeout>
    <sessionIdleTimeout>10</sessionIdleTimeout>
  </timeout>
  <clientNotification></clientNotification>
  <enablePublicUrlAccess>false</enablePublicUrlAccess>
  <enableLogging>false</enableLogging>
</advancedConfig>
<authenticationConfiguration>
  <passwordAuthentication>
    <authenticationTimeout>1</authenticationTimeout>
    <primaryAuthServers>
      <com.vmware.vshield.edge.sslvpn.dto.LdapAuthServerDto>
        <ip>1.1.1.1</ip>
        <port>90</port>
        <timeOut>20</timeOut>
        <enableSsl>false</enableSsl>
        <searchBase>searchbasevalue</searchBase>
        <bindDomainName>binddnvalue</bindDomainName>
        <bindPassword>password</bindPassword>
        <loginAttributeName>cain</loginAttributeName>
        <searchFilter>found</searchFilter>
        <enabled>true</enabled>
      </com.vmware.vshield.edge.sslvpn.dto.LdapAuthServerDto>
      <com.vmware.vshield.edge.sslvpn.dto.RadiusAuthServerDto>
        <ip>3.3.3.3</ip>
        <port>90</port>
        <timeOut>20</timeOut>
        <secret>struct9870</secret>
        <nasIp>1.1.1.9</nasIp>
        <retryCount>10</retryCount>
      </com.vmware.vshield.edge.sslvpn.dto.RadiusAuthServerDto>
      <com.vmware.vshield.edge.sslvpn.dto.LocalAuthServerDto>
        <enabled>true</enabled>
        <passwordPolicy>
          <minLength>1</minLength>
          <maxLength>63</maxLength>
          <minAlphabets>0</minAlphabets>
          <minDigits>0</minDigits>
          <minSpecialChar>1</minSpecialChar>
          <allowUserIdWithinPassword>false</allowUserIdWithinPassword>
          <passwordLifeTime>20</passwordLifeTime>
          <expiryNotification>1</expiryNotification>
        </passwordPolicy>
      </com.vmware.vshield.edge.sslvpn.dto.LocalAuthServerDto>
    </primaryAuthServers>
  </passwordAuthentication>
</authenticationConfiguration>

```

```

    </passwordPolicy>
    <accountLockoutPolicy>
      <retryCount>3</retryCount>
      <retryDuration>3</retryDuration>
      <lockoutDuration>3</lockoutDuration>
    </accountLockoutPolicy>
  </com.vmware.vshield.edge.sslvpn.dto.LocalAuthServerDto>
  <!--<com.vmware.vshield.edge.sslvpn.dto.RsaAuthServerDto>
  <timeOut>20</timeOut>
  <sourceIp>1.2.2.3</sourceIp>
  </com.vmware.vshield.edge.sslvpn.dto.RsaAuthServerDto>
  </primaryAuthServers>
  <secondaryAuthServer>
    <com.vmware.vshield.edge.sslvpn.dto.AdAuthServerDto>
      <ip>1.1.1.1</ip>
      <port>90</port>
      <timeOut>20</timeOut>
      <enableSsl>false</enableSsl>
      <searchBase>searchbasevalue</searchBase>
      <bindDomainName>binddnvalue</bindDomainName>
      <bindPassword>password</bindPassword>
      <loginAttributeName>cain</loginAttributeName>
      <searchFilter>found</searchFilter>
      <terminateSessionOnAuthFails>false</terminateSessionOnAuthFails>
      <enabled>true</enabled>
    </com.vmware.vshield.edge.sslvpn.dto.AdAuthServerDto>
  </secondaryAuthServer>
</passwordAuthentication>
</authenticationConfiguration>
</sslvpnConfig>

```

---

## Delete SSL VPN Configuration

Deletes the SSL VPN configurations on the specified vShield Edge.

### Example 5-143. Delete SSL VPN Configuration

---

Request:

DELETE https://<vsm-ip>/api/3.0/edges/<edgeId>/sslvpn/config/

---

## Query SSL VPN Statistics

Retrieves SSL VPN statistics on the specified vShield Edge.

### Example 5-144. Get SSL VPN statistics

---

Request:

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/statistics/dashboard/sslvpn?interval=<range> <!--range can be 1 - 60 minutes or oneDay|oneWeek|oneMonth|oneYear. Default is 60 minutes -->

Response Body:

```

<?xml version="1.0" encoding="UTF-8"?>
<dashboardStatistics>
  <meta>
    <startTime>1344809160</startTime>    <!-- in seconds -->
    <endTime>1344809460</endTime>      <!-- in seconds -->
    <interval>300</interval>
  </meta>
  <data>
    <sslvpn>
      <sslvpnBytesOut>
        <dashboardStatistic>

```



```

        <timestamp>1344809160</timestamp>
        <value>0.0</value>
    </dashboardStatistic>
    <dashboardStatistic>
        <timestamp>1344809460</timestamp>
        <value>0.0</value>
    </dashboardStatistic>
</sslvpnBytesOut>
<sslvpnBytesIn>
    <dashboardStatistic>
        <timestamp>1344809160</timestamp>
        <value>0.0</value>
    </dashboardStatistic>
    <dashboardStatistic>
        <timestamp>1344809460</timestamp>
        <value>0.0</value>
    </dashboardStatistic>
</sslvpnBytesIn>
<activeClients>
    <dashboardStatistic>
        <timestamp>1344809160</timestamp>
        <value>3.0</value>
    </dashboardStatistic>
    <dashboardStatistic>
        <timestamp>1344809460</timestamp>
        <value>3.0</value>
    </dashboardStatistic>
</activeClients>
<authFailures>
    <dashboardStatistic>
        <timestamp>1344809160</timestamp>
        <value>2.0</value>
    </dashboardStatistic>
    <dashboardStatistic>
        <timestamp>1344809460</timestamp>
        <value>2.0</value>
    </dashboardStatistic>
</authFailures>
<sessionsCreated>
    <dashboardStatistic>
        <timestamp>1344809160</timestamp>
        <value>4.0</value>
    </dashboardStatistic>
    <dashboardStatistic>
        <timestamp>1344809460</timestamp>
        <value>4.0</value>
    </dashboardStatistic>
</sessionsCreated>
</sslvpn>
</data>
</dashboardStatistics>

```

---

## Configure Load Balancer

vShield Edge provides load balancing for TCP, HTTP, and HTTPS traffic. Load balancing, up to Layer 7, enables Web application auto scaling. You map an external, or public, IP address to a set of internal servers for load balancing. The load balancer accepts TCP, HTTP, or HTTPS requests on the external IP address and decides which internal server to use. Port 8090 is the default listening port for TCP, port 80 is the default port for HTTP, and port 443 is the default port for HTTPS.

When you enable the load balancing service, Layer-7 (L7 proxy) load balancing is automatically used which uses both Source Network Address Translation(SNAT) and Destination Network Address Translation(DNAT). You can enable an additional load balancing mode Layer-4 (L4) by setting the `accelerationEnabled` parameter to `true`. Layer-4 mode only uses DNAT and preserves the original client IP address of the request.

You can create a pool of backend servers and specify the services that the pool would support as well as healthcheck against the services. You can then associate two or more virtual machines behind a server pool for the load balancer service.

All Load Balancer settings configured by using REST requests appear under the **Load Balancer** tab for the appropriate vShield Edge in the vShield Manager user interface and in the vSphere Client plug-in.

#### Example 5-145. Configure load balancer

PUT https://<vsm-ip>/api/3.0/edges/<edgeId>/loadbalancer/config

Request Body:

```
<loadBalancer>
  <accelerationEnabled>true</accelerationEnabled>          <!-- optional, default false-->
  <enabled>true</enabled>                                     <!-- Optional, default true -->
  <virtualServer>                                             <!-- 0 ~ 64 virtualServers could be defined under loadBalancer -->
    <name>http_lb</name>                                     <!-- Needed, 0~255, the name should just contains upper and lower case
                                                                letters, digits, - (dash), _ (underscore) and start with letters -->
    <description>virtualServer for http traffic</description> <!-- Optional, 0~255 -->
    <ipAddress>192.168.1.101</ipAddress>
    <applicationProfile>                                     <!-- Define at least one serviceProfile -->
      <protocol>HTTP</protocol>                             <!-- HTTP/HTTPS/TCP -->
      <port>80</port>                                       <!-- Possible values 0~65535 -->
      <persistence>                                         <!-- Optional -->
        <method>COOKIE</method>                           <!-- Only COOKIE method supported for HTTP protocol -->
        <cookieName>JSESSIONID</cookieName>               <!-- Required if method=COOKIE -->
        <cookieMode>INSERT</cookieMode>                   <!-- Required if method=COOKIE -->
      </persistence>
    </applicationProfile>
    <applicationProfile>
      <protocol>HTTPS</protocol>
      <port>443</port>
      <persistence>
        <method>SSL_SESSION_ID</method>                   <!-- Only SSL_SESSION_ID method supported for
                                                                HTTPS protocol -->
      </persistence>
    </applicationProfile>
    <enabled>true</enabled>                                  <!--Optional, default is true -->
    <logging>                                                <!--Optional, default is false/INFO -->
      <enable>true</enable>
      <logLevel>INFO</logLevel>
    </logging>
    <pool>
      <id>1</id>
    </pool>
  </virtualServer>
</virtualServer>
...
</virtualServer>
<pool>                                                       <!-- 0 ~ 64 pools could be defined under loadBalancer -->
  <id>1</id>                                                 <!-- Required when doing bulk configuration; Optional when creating/updating
                                                                pool -->
  <name>http-https-pool</name>                                <!-- Required, 0~255, the name should just contains upper and lower
                                                                case letters, digits, - (dash), _ (underscore) and start with letters -->
  <description>pool for http and https traffic</description> <!-- Optional, 0~255 -->
  <servicePort>                                              <!-- At least one servicePort should be defined under pool -->
    <protocol>HTTP</protocol>
    <algorithm>ROUND_ROBIN</algorithm>                       <!-- Optional,
                                                                ROUND_ROBIN/IP_HASH/URI/LEAST_CONN, default is ROUND_ROBIN -->
    <port>80</port>                                           <!-- Optional -->
    <healthCheckPort>80</healthCheckPort>                   <!-- Optional-->
    <healthCheck>                                             <!-- Optional-->
      <mode>HTTP</mode>                                       <!-- Optional, HTTP/TCP/SSL -->
      <healthThreshold>2</healthThreshold>                  <!-- Optional 1~10 -->
      <unHealthThreshold>3</unHealthThreshold>              <!-- Optional 1~10 -->
      <interval>3</interval>                                 <!-- Optional -->
      <uri>/</uri>                                           <!-- Optional -->
      <timeout>5</timeout>                                   <!-- Optional -->
```

```

        </healthCheck>
    </servicePort>
    <servicePort>
        ...
    </servicePort>
    <member>                                <!-- Define at least one member under pool -->
        <ipAddress>192.168.4.103</ipAddress>
        <weight>10</weight>                <!-- Optional -->
        <servicePort>                        <!-- Optional -->
            <protocol>HTTPS</protocol>
            <port>8443</port>                <!-- Optional -->
            <healthCheckPort>8443</healthCheckPort> <!-- Optional -->
            <healthCheck>                    <!-- Optional -->
                <interval>1</interval>        <!-- Needed, only interval could be overridden -->
            </healthCheck>
        </servicePort>
    </member>
    <member>
        ...
    </member>
</pool>
<pool>
    ...
</pool>
</loadBalancer>

```

For the data path to work, you need to add firewall rules to allow required traffic as per the loadbalancer configuration.

## Query Load Balancer Configuration

Gets current load balancer configuration.

### Example 5-146. Retrieve load balancer configuration

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/loadbalancer/config

Response Body:

```

<?xml version="1.0" encoding="UTF-8"?>
<loadBalancer>
    <version>3</version>
    <accelerationEnabled>true</accelerationEnabled> <!-- optional, default is false-->
    <enabled>true</enabled> <!-- Optional, default is true -->
    <virtualServer> <!-- 0 ~ 64 virtualServers could be defined under loadBalancer -->
        <name>http_lb</name> <!-- Needed, 0~255, the name should just contains upper and lower case letters, digits, - (dash), _
            (underscore) and start with letters -->
        <description>virtualServer for http traffic</description> <!-- Optional, 0~255 -->
        <ipAddress>192.168.1.101</ipAddress> <!-- Needed -->
        <applicationProfile> <!-- At least one serviceProfile should be defined here under virtualServer -->
            <protocol>HTTP</protocol> <!-- Needed, HTTP/HTTPS/TCP -->
            <port>80</port> <!-- Needed, 0~65535 -->
            <persistence> <!-- Optional -->
                <method>COOKIE</method> <!-- Needed, COOKIE/SSL_SESSION_ID, but only COOKIE method could be
                    supported for HTTP protocol -->
                <cookieName>JSESSIONID</cookieName> <!-- Needed if method=COOKIE -->
                <cookieMode>INSERT</cookieMode> <!-- Needed if method=COOKIE -->
            </persistence>
        </applicationProfile>
    </virtualServer>
    <applicationProfile>
        <protocol>HTTPS</protocol>
        <port>443</port>
        <persistence>
            <method>SSL_SESSION_ID</method> <!-- Needed, Only SSL_SESSION_ID method could be supported for
                HTTPS protocol -->
        </persistence>
    </applicationProfile>

```

```

    <enabled>true</enabled> <!--Optional, default is true -->
    <logging> <!--Optional, default is false/INFO -->
        <enable>true</enable>
        <logLevel>INFO</logLevel>
    </logging>
    <pool> <!-- Needed -->
        <id>1</id>
    </pool>
</virtualServer>
<pool>
    <id>1</id>
    <name>http-https-pool</name>
    <servicePort>
        <protocol>HTTP</protocol>
        <algorithm>ROUND_ROBIN</algorithm>
        <port>80</port>
        <healthCheckPort>80</healthCheckPort>
        <healthCheck>
            <mode>HTTP</mode>
            <healthThreshold>2</healthThreshold>
            <unHealthThreshold>3</unHealthThreshold>
            <interval>3</interval>
            <uri>/</uri>
            <timeout>5</timeout>
        </healthCheck>
    </servicePort>
    <member>
        <ipAddress>192.168.4.103</ipAddress>
        <weight>10</weight>
    </member>
</pool>
</loadBalancer>

```

## Query Statistics

Retrieves load balancer statistics for the specified time interval. Default time interval is 1 hour. Other possible values are 1-60 minutes | one day | one week | one month | one year.

### Example 5-147. Retrieve load balancer statistics

---

```
GET https://<vsm-ip>/api/3.0/edges/<edgeId>/statistics/dashboard/loadbalancer?interval=<range>
```

Response Body:

```

<?xml version="1.0" encoding="UTF-8"?>
<dashboardStatistics>
    <meta>
        <startTime>1336068000</startTime>    <!-- in seconds -->
        <endTime>1336068300</endTime>    <!-- in seconds -->
        <interval>300</interval>
    </meta>
    <data>
        <loadBalancer>
            <lbSessions>
                <dashboardStatistic>
                    <timestamp>1336068000</timestamp>
                    <value>2.0</value>
                </dashboardStatistic>
                <dashboardStatistic>
                    <timestamp>1336068300</timestamp>
                    <value>2.0</value>
                </dashboardStatistic>
            </lbSessions>
            <lbHttpReqs>
                <dashboardStatistic>
                    <timestamp>1336068000</timestamp>
                    <value>2.0</value>
                </dashboardStatistic>
                <dashboardStatistic>

```

```

        <timestamp>1336068300</timestamp>
        <value>2.0</value>
      </dashboardStatistic>
    </lbHttpReqs>
    <lbBpsIn>
      <dashboardStatistic>
        <timestamp>1336068000</timestamp>
        <value>0.0</value>
      </dashboardStatistic>
      <dashboardStatistic>
        <timestamp>1336068300</timestamp>
        <value>0.0</value>
      </dashboardStatistic>
    </lbBpsIn>
    <lbBpsOut>
      <dashboardStatistic>
        <timestamp>1336068000</timestamp>
        <value>0.0</value>
      </dashboardStatistic>
      <dashboardStatistic>
        <timestamp>1336068300</timestamp>
        <value>0.0</value>
      </dashboardStatistic>
    </lbBpsOut>
  </loadBalancer>
</data>
</dashboardStatistics>

```

---

## Delete Load Balancer Configuration

**Example 5-148.** Delete load balancer configuration

---

Request:

DELETE https://<vsm-ip>/api/3.0/edges/<edgeId>/loadbalancer/config

---

## Manage all Backend Pools

You can add a server pool to manage and share backend servers flexibly and efficiently. A pool manages healthcheck monitors and load balancer distribution methods.

### Append Backend Pool

Adds a load balancer server pool to the specified vShield Edge.

**Example 5-149.** Append backend pool

---

Request:

POST https://<vsm-ip>/api/3.0/edges/<edgeId>/loadbalancer/config/pools

Request Body:

```

<?xml version="1.0" encoding="UTF-8"?>
<pool>
  <name>http-https-pool</name>
  <servicePort>
    <protocol>HTTP</protocol>
    <algorithm>ROUND_ROBIN</algorithm>
    <port>80</port>
    <healthCheckPort>80</healthCheckPort>
    <healthCheck>
      <mode>HTTP</mode>
      <healthThreshold>2</healthThreshold>
      <unHealthThreshold>3</unHealthThreshold>
    </healthCheck>
  </servicePort>
</pool>

```

```

        <interval>3</interval>
        <uri>/</uri>
        <timeout>5</timeout>
    </healthCheck>
</servicePort>
<member>
    <ipAddress>192.168.4.103</ipAddress>
    <weight>10</weight>
</member>
</pool>

```

---

### Query all Backend Pool Details

Gets all backend pools configured for the specified vShield Edge.

#### Example 5-150. Query all backend pools

---

Request:

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/loadbalancer/config/pools

Request Body:

```

<?xml version="1.0" encoding="UTF-8"?>
<loadBalancer>
    <version>3</version>
    <pool>
        <id>6</id>
        <name>http-pool</name>
        <servicePort>
            <protocol>HTTP</protocol>
            <algorithm>ROUND_ROBIN</algorithm>
            <port>80</port>
            <healthCheckPort>80</healthCheckPort>
            <healthCheck>
                <mode>HTTP</mode>
                <healthThreshold>2</healthThreshold>
                <unHealthThreshold>3</unHealthThreshold>
                <interval>3</interval>
                <timeout>5</timeout>
            </healthCheck>
        </servicePort>
        <member>
            <ipAddress>192.168.7.192</ipAddress>
            <weight>10</weight>
        </member>
        <member>
            <ipAddress>192.168.6.192</ipAddress>
            <weight>20</weight>
        </member>
    </pool>
</loadBalancer>

```

---

### Delete all Backend Pools

Deletes all backend pools configured for the specified vShield Edge.

#### Example 5-151. Delete backend pool

---

Request:

DELETE https://<vsm-ip>/api/3.0/edges/<edgeId>/loadbalancer/config/pools

---

## Manage a Specific Backend Pool

### Modify a Backend Pool

Updates the specified pool.

#### Example 5-152. Modify backend pool

---

Request:

PUT https://<vsm-ip>/api/3.0/edges/<edgeId>/loadbalancer/config/pools/*poolID*

Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<pool>
  <name>http-https-pool</name>
  <servicePort>
    <protocol>HTTP</protocol>
    <algorithm>ROUND_ROBIN</algorithm>
    <port>80</port>
    <healthCheckPort>80</healthCheckPort>
    <healthCheck>
      <mode>HTTP</mode>
      <healthThreshold>2</healthThreshold>
      <unHealthThreshold>3</unHealthThreshold>
      <interval>3</interval>
      <uri></uri>
      <timeout>5</timeout>
    </healthCheck>
  </servicePort>
  <member>
    <ipAddress>192.168.4.103</ipAddress>
    <weight>10</weight>
  </member>
  <member>
    <ipAddress>192.168.7.192</ipAddress>
    <weight>10</weight>
  </member>
</pool>
```

---

### Retrieve Backend Pool Details

Retrieves information about the specified pool.

#### Example 5-153. Get backend pool details

---

Request:

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/loadbalancer/config/pools/*poolID*

Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<pool>
  <name>http-https-pool</name>
  <servicePort>
    <protocol>HTTP</protocol>
    <algorithm>ROUND_ROBIN</algorithm>
    <port>80</port>
    <healthCheckPort>80</healthCheckPort>
    <healthCheck>
      <mode>HTTP</mode>
      <healthThreshold>2</healthThreshold>
      <unHealthThreshold>3</unHealthThreshold>
      <interval>3</interval>
      <uri></uri>
      <timeout>5</timeout>
    </healthCheck>
  </servicePort>
  <member>
    <ipAddress>192.168.4.103</ipAddress>
    <weight>10</weight>
  </member>
  <member>
    <ipAddress>192.168.7.192</ipAddress>
    <weight>10</weight>
  </member>
</pool>
```

```

        </healthCheck>
    </servicePort>
    <member>
        <ipAddress>192.168.4.103</ipAddress>
        <weight>10</weight>
    </member>
    <member>
        <ipAddress>192.168.7.192</ipAddress>
        <weight>10</weight>
    </member>
</pool>

```

---

### Delete a Backend Pool

Deletes the specified pool.

#### Example 5-154. Delete backend pool

---

Request:

```
DELETE https://<vsm-ip>/api/3.0/edges/<edgeId>/loadbalancer/config/pools/poolID
```

---

### Manage all Virtual Servers

You can create a virtual server and associate existing server pools with it. A virtual server should be assigned with a VIP to accept incoming TCP/HTTP/HTTPS traffic and distribute to the server pool.

#### Append Virtual Server

Adds a virtual server.

#### Example 5-155. Append virtual server

---

Request:

```
POST https://<vsm-ip>/api/3.0/edges/<edgeId>/loadbalancer/config/virtualserver
```

Request Body:

```

<?xml version="1.0" encoding="UTF-8"?>
<virtualServer>
    <name>http_lb</name>
    <description>virtualServer for http traffic</description>
    <ipAddress>192.168.1.101</ipAddress>
    <applicationProfile>
        <protocol>HTTP</protocol>
        <port>80</port>
        <persistence>
            <method>COOKIE</method>
            <cookieName>JSESSIONID</cookieName>
            <cookieMode>INSERT</cookieMode>
        </persistence>
    </applicationProfile>
    <logging>
        <enable>true</enable>
        <logLevel>INFO</logLevel>
    </logging>
    <pool> <!-- Needed -->
        <id>1</id>
    </pool>
</virtualServer>

```

---

### Retrieve Virtual Server Details

Gets information about all virtual servers on the specified vShield Edge.



**Example 5-156. Get all virtual server details**

---

Request:

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/loadbalancer/config/virtualservers

Response Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<virtualServer>
  <name>http_lb</name>
  <description>virtualServer for http traffic</description>
  <ipAddress>192.168.1.101</ipAddress>
  <applicationProfile>
    <protocol>HTTP</protocol>
    <port>80</port>
    <persistence>
      <method>COOKIE</method>
      <cookieName>JSESSIONID</cookieName>
      <cookieMode>INSERT</cookieMode>
    </persistence>
  </applicationProfile>
  <logging>
    <enable>true</enable>
    <logLevel>INFO</logLevel>
  </logging>
  <pool> <!-- Needed -->
    <id>1</id>
  </pool>
</virtualServer>
```

---

**Delete all Virtual Servers**

Deletes all virtual servers on the specified vShield Edge instance.

**Example 5-157. Delete virtual servers**

---

Request:

DELETE https://<vsm-ip>/api/3.0/edges/<edgeId>/loadbalancer/config/virtualservers

---

**Manage a Specific Virtual Server****Modify a Virtual Server**

Updates the specified virtual server.

**Example 5-158. Update virtual server**

---

Request:

PUT https://<vsm-ip>/api/3.0/edges/<edgeId>/loadbalancer/config/virtualservers/*virtualserverID*

Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<virtualServer>
  <name>http_lb</name>
  <description>virtualServer for http traffic</description>
  <ipAddress>192.168.1.101</ipAddress>
  <applicationProfile>
    <protocol>HTTP</protocol>
    <port>80</port>
    <persistence>
      <method>COOKIE</method>
      <cookieName>JSESSIONID</cookieName>
      <cookieMode>INSERT</cookieMode>
    </persistence>
  </applicationProfile>
</virtualServer>
```

```

        </persistence>
    </applicationProfile>
    <logging>
        <enable>true</enable>
        <logLevel>INFO</logLevel>
    </logging>
    <pool> <!-- Needed -->
        <id>1</id>
    </pool>
</virtualServer>

```

---

## Retrieve Virtual Server Details

### Example 5-159. Get virtual server details

---

Request:

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/loadbalancer/config/virtualservers/*virtualserverID*

Response Body:

```

<?xml version="1.0" encoding="UTF-8"?>
<virtualServer>
    <name>http_lb</name>
    <description>virtualServer for http traffic</description>
    <ipAddress>192.168.1.101</ipAddress>
    <applicationProfile>
        <protocol>HTTP</protocol>
        <port>80</port>
        <persistence>
            <method>COOKIE</method>
            <cookieName>JSESSIONID</cookieName>
            <cookieMode>INSERT</cookieMode>
        </persistence>
    </applicationProfile>
    <logging>
        <enable>true</enable>
        <logLevel>INFO</logLevel>
    </logging>
    <pool> <!-- Needed -->
        <id>1</id>
    </pool>
</virtualServer>

```

---

## Delete a Virtual Server

Deletes the specified virtual server.

### Example 5-160. Delete virtual server

---

Request:

DELETE https://<vsm-ip>/api/3.0/edges/<edgeId>/loadbalancer/config/virtualservers/*virtualserverID*

---

## Retrieve Load Balancer Statistics

Gets load balancer statistics.

### Example 5-161. Get load balancer statistics

---

Request:

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/loadbalancer/statistics

Response Body:

```

<?xml version="1.0" encoding="UTF-8"?>
<loadBalancerStatusAndStats>
  <timeStamp>1344286008</timeStamp>
  <pool>
    <id>1</id>
    <name>http_https_pool</name>
    <description>pool for http and https traffic</description>
    <servicePort>
      <protocol>HTTP</protocol>
      <status>DOWN</status>
      <bytesIn>0</bytesIn>
      <bytesOut>0</bytesOut>
      <curSessions>0</curSessions>
      <maxSessions>0</maxSessions>
      <rate>0</rate>
      <rateMax>0</rateMax>
      <totalSessions>0</totalSessions>
    </servicePort>
    <servicePort>
      <protocol>HTTPS</protocol>
      <status>DOWN</status>
      <bytesIn>0</bytesIn>
      <bytesOut>0</bytesOut>
      <curSessions>0</curSessions>
      <maxSessions>0</maxSessions>
      <rate>0</rate>
      <rateMax>0</rateMax>
      <totalSessions>0</totalSessions>
    </servicePort>
    <member>
      <ipAddress>172.16.1.101</ipAddress>
      <servicePort>
        <protocol>HTTP</protocol>
        <status>DOWN</status>
      </servicePort>
      <servicePort>
        <protocol>HTTPS</protocol>
        <status>DOWN</status>
      </servicePort>
    </member>
    <member>
      ...
    </member>
  </pool>
  <virtualServer>
    <id>1</id>
    <name>http_lb</name>
    <description>virtualServer for http traffic</description>
    <ipAddress>10.117.35.172</ipAddress>
    <applicationProfileStats>
      <protocol>HTTP</protocol>
      <status>OPEN</status>
      <bytesIn>0</bytesIn>
      <bytesOut>0</bytesOut>
      <curSessions>0</curSessions>
      <httpReqTotal>0</httpReqTotal>
      <httpReqRate>0</httpReqRate>
      <httpReqRateMax>0</httpReqRateMax>
      <maxSessions>0</maxSessions>
      <rate>0</rate>
      <rateLimit>0</rateLimit>
      <rateMax>0</rateMax>
      <totalSessions>0</totalSessions>
    </applicationProfileStats>
    <applicationProfileStats>
      <protocol>HTTPS</protocol>
      <status>OPEN</status>
      <bytesIn>0</bytesIn>

```

```

    <bytesOut>0</bytesOut>
    <curSessions>0</curSessions>
    <httpReqTotal>0</httpReqTotal>
    <httpReqRate>0</httpReqRate>
    <httpReqRateMax>0</httpReqRateMax>
    <maxSessions>0</maxSessions>
    <rate>0</rate>
    <rateLimit>0</rateLimit>
    <rateMax>0</rateMax>
    <totalSessions>0</totalSessions>
  </applicationProfileStats>
</virtualServer>
</loadBalancerStatusAndStats>

```

---

## Enable Layer-4 Mode for Load Balancer

When you enable the load balancing service, Layer-7 (L7 proxy) load balancing is automatically used which uses both Source Network Address Translation(SNAT) and Destination Network Address Translation(DNAT). You can enable an additional load balancing mode Layer-4 (L4) by setting the accelerationEnabled parameter to true. Layer-4 mode only uses DNAT and preserves the original client IP address of the request.

### Example 5-162. Modify Acceleration for Load Balancer

---

Request:

POST https://<vsm-ip>/api/3.0/edges/edge-id/loadbalancer/acceleration?enable=true/false

---

## Configure High Availability (HA)

High Availability (HA) ensures that a vShield Edge appliance is always available on your virtualized network. You can enable HA either when installing vShield Edge or on an installed vShield Edge instance.

If a single appliance is associated with vShield Edge, the appliance configuration is cloned for the standby appliance. If two appliances are associated with vShield Edge and one of them is deployed, this REST call deploys the remaining appliance and push HA configuration to both.

HA relies on an internal interface. If an internal interface does not exist, this call will not deploy the secondary appliance, or push HA config to appliance. The enabling of HA will be done once an available internal interface is added.

If the PUT call includes an empty xml <highAvailability /> or enabled=false, it acts as a DELETE call.

### Example 5-163. Configure high availability

---

Request:

PUT https://<vsm-ip>/api/3.0/edges/<edgeId>/highavailability/config

Request Body:

```

<highAvailability>
  <vnic>1</vnic> <!-- Optional. User can provide the vNic Index. If not provided, the first internal-connected vnic will be used as the vnic -->
  <ipAddresses> <!-- Optional. It is a pair of ipAddresses with /30 subnet mandatory, one for each appliance. If provided, they must NOT overlap with any subnet defined on the Edge vNics. If not specified, a pair of ips will be picked up from reserved subnet 169.254.0.0/16. -->
    <ipAddress>192.168.10.1/30</ipAddress>
    <ipAddress>192.168.10.2/30</ipAddress>
  </ipAddresses>
  <declareDeadTime>6</declareDeadTime> <!-- Optional. Default is 6 seconds -->
  <enabled>true</enabled> <!-- optional, defaults to true. The enabled flag will cause the HA appliance be deployed or destroyed. -->

```

---

```
</highAvailability>
```

---

## Retrieve High Availability Configuration

**Example 5-164.** Get high availability configuration

---

Request:api/

GET https://<vsm-ip>/3.0/edges/<edgeId>/highavailability/config

Request Body:

```
<highAvailability>
  <vnic>1</vnic>
  <ipAddresses>
    <ipAddress>192.168.10.1/30</ipAddress>
    <ipAddress>192.168.10.2/30</ipAddress>
  </ipAddresses>
  <declareDeadTime>6</declareDeadTime>  <!-- Optional. Default is 6 seconds -->
</highAvailability>
```

---

## Delete High Availability Configuration

vShield Manager deletes the standby appliance and removes the HA config from the active appliance.

You can also delete the HA configuration by using a PUT call with empty xml <highAvailability /> or with <highAvailability><enabled>false</enabled></highAvailability>.

**Example 5-165.** Delete high availability configuration

---

Request:

DELETE https://<vsm-ip>/api/3.0/edges/<edgeId>/highavailability/config

---

## Force Syncing vShield Edge

Forces a vShield Edge to re-synchronize with the vShield Manager.

**Example 5-166.** Force sync vShield Edge

---

Request:

GET https://<vsm-ip>/api/3.0/edges/<edgeId>?action=forcesync

---

## Configuring Advanced Options for vShield Edge

The set of APIs in this section help you configure vShield Edge and its services. To retrieve the ID for a vShield Edge, see [Example , “Running Queries on all vShield Edges,”](#) on page 53.

### Change AESNI Setting for a vShield Edge

You can enable Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) for a vShield Edge instance. AESNI is disabled by default.

**Example 5-167.** Change AESNI setting

---

Request:

---

POST https://<vsm-ip>/api/3.0/edges/<edgeId>/aesni?enable=false|true

---

## Change FIPS Setting for a vShield Edge

Federal Information Processing Standard (FIPS) is disabled by default. If you enable this feature, SSL VPN will be disabled and IPSEC VPN cannot include a site using PSK authentication.

### Example 5-168. Change FIPS setting

---

Request:

POST https://<vsm-ip>/api/3.0/edges/<edgeId>/fips?enable=true

---

## Change Logging Level for vShield Appliance

### Example 5-169. Specify log level

---

Request:

POST https://<vsm-ip>/api/3.0/edges/<edgeId>/logging?level=debug|info|emergency|alert|critical|error|warning|notice

---

Default value is info.

## Manage Auto Configuration Settings

Auto configuration default settings is enabled by default and the priority is high.

If you disable auto configuration settings, you must add the required NAT, firewall, routing rules to enable control-channel traffic for other services such as load balancing, VPN, etc.

If you change the priority of the auto configuration settings to low, the internal/auto configured rules are placed in lower precedence than the rules you create. With this, you can again control special allow/deny rules for these services too. For example, you can block specific IP addresses from accessing the VPN services.

### Modify Auto Configuration Settings

Changes the auto configuration settings for the vShield Edge.

#### Example 5-170. Modify auto configuration settings

---

PUT https://<vsm-ip>/api/3.0/edges/<edgeId>/autoconfiguration

Request Body:

```
<autoConfiguration>
  <enabled>true</enabled>
  <rulePriority>high</rulePriority>
</autoConfiguration>
```

---

### Query Auto Configuration Settings

Retrieves auto configuration settings for the vShield Edge.

#### Example 5-171. Retrieve auto configuration settings

---

GET https://<vsm-ip>/api/3.0/edges/<edgeId>/autoconfiguration

Response Body:

```
<autoConfiguration>
  <enabled>true</enabled>
  <rulePriority>high</rulePriority>
```

```
</autoConfiguration>
```

---

## Change TCP Loose Setting

Changes TCP loose settings on the vShield Edge. By default, TCP loose setting is disabled.

### Example 5-172. Modify TCP loose setting

---

Request:

```
POST https://vsm-ip>/api/3.0/edges/<edgeId>/tcploose?enable=<true|false>
```

---

## Replacing the Configuration of a vShield Edge

Replaces the complete configuration of a vShield Edge. Note that this call replaces all prior configurations made with the POST call or other modular calls.

### Example 5-173. Replace the configuration of a vShield Edge

---

Request:

```
PUT /api/3.0/edges/<edgeId>
```

Request Body:

```
<edge>
  <id>edge-79</id>
  <description>testEdge</description>
  <datacenterMoid>datacenter-2</datacenterMoid>
  <name>testEdge</name>
  <fqdn>testEdge</fqdn>
  <enableAesni>true</enableAesni>
  <enableFips>false</enableFips>
  <enableTcpLoose>false</enableTcpLoose>
  <vseLogLevel>info</vseLogLevel>
  <vnics>
    <vnic>
      <index>0</index>
      <name>uplink-vnic-network-2581</name>
      <type>uplink</type>
      <portgroupId>network-2581</portgroupId>
      <addressGroups>
        <addressGroup>
          <primaryAddress>10.112.2.40</primaryAddress>
          <secondaryAddresses>
            <ipAddress>10.112.2.42</ipAddress>
          </secondaryAddresses>
          <subnetMask>255.255.254.0</subnetMask>
        </addressGroup>
      </addressGroups>
      <mtu>1500</mtu>
      <enableProxyArp>false</enableProxyArp>
      <enableSendRedirects>true</enableSendRedirects>
      <isConnected>true</isConnected>
      <inShapingPolicy>      <!-- optional -->
      <averageBandwidth>200000000</averageBandwidth>
      <peakBandwidth>200000000</peakBandwidth>
      <burstSize>0</burstSize>
      <enabled>true</enabled>
      <inherited>false</inherited>
    </inShapingPolicy>
    <outShapingPolicy>      <!-- optional -->
      <averageBandwidth>400000000</averageBandwidth>
      <peakBandwidth>400000000</peakBandwidth>
```

```

    <burstSize>0</burstSize>
    <enabled>true</enabled>
    <inherited>>false</inherited>
  </outShapingPolicy>
</vnic>
</vnic>
....
</vnics>
<appliances>
  <applianceSize>compact</applianceSize>
  <appliance>
    <resourcePoolId>resgroup-2454</resourcePoolId>
    <datastoreId>datastore-2457</datastoreId>
    <vmFolderId>group-v3</vmFolderId>
  </appliance>
</appliances>
<cliSettings>
  <remoteAccess>>false</remoteAccess>
  <userName>admin</userName>
</cliSettings>
<features>
  <firewall>
    <defaultPolicy>
      <action>deny</action>
      <loggingEnabled>>false</loggingEnabled>
    </defaultPolicy>
    <firewallRules>
      <firewallRule>
        <id>131078</id>
        <ruleTag>131078</ruleTag>
        <name>rule1</name>
        <ruleType>user</ruleType>
        <source>
          <groupingObjectId>ipset-938</groupingObjectId>
          &lt;source>&gt;
          <sourcePort>any</sourcePort>
          <destination/>
          <application>
            <applicationId>application-666</applicationId>
          </application>
          <action>accept</action>
          <enabled>true</enabled>
          <loggingEnabled>>false</loggingEnabled>
          <matchTranslated>>false</matchTranslated>
        </firewallRule>
        ....
      </firewallRules>
    </firewall>
  <dns>
    <enabled>>false</enabled>
    <cacheSize>16</cacheSize>
    <listeners>
      <ipAddress>any</ipAddress>
    </listeners>
    <logging>
      <enable>>false</enable>
      <logLevel>info</logLevel>
    </logging>
  </dns>
  <staticRouting>
    <defaultRoute>
      <vnic>0</vnic>
      <gatewayAddress>10.112.3.253</gatewayAddress>
      <description>defaultGw on the external interface</description>
    </defaultRoute>
    <staticRoutes>
      <route>
        <vnic>0</vnic>

```



```

    <network>192.168.30.0/24</network>
    <nextHop>10.112.2.41</nextHop>
    <type>user</type>
  </route>
  ...
</staticRoutes>
</staticRouting>
<highAvailability>
  <enabled>>false</enabled>
  <declareDeadTime>6</declareDeadTime>
  <logging>
    <enable>>false</enable>
    <logLevel>info</logLevel>
  </logging>
</highAvailability>
<syslog>
  <protocol>udp</protocol>
  <serverAddresses>
    <ipAddress>1.1.1.1</ipAddress>
    <ipAddress>1.1.1.2</ipAddress>
  </serverAddresses>
</syslog>
<loadBalancer>
  <enabled>true</enabled>
  <accelerationEnabled>>false</accelerationEnabled>
  <virtualServer>
    <id>1</id>
    <name>listener1</name>
    <enabled>true</enabled>
    <ipAddress>10.112.2.42</ipAddress>
    <applicationProfile>
      <protocol>HTTP</protocol>
      <port>80</port>
    </applicationProfile>
    <logging>
      <enable>>false</enable>
      <logLevel>INFO</logLevel>
    </logging>
    <pool>
      <id>1</id>
    </pool>
  </virtualServer>
  ....
  <pool>
    <id>1</id>
    <name>pool1</name>
    <servicePort>
      <protocol>HTTP</protocol>
      <algorithm>IP_HASH</algorithm>
      <port>80</port>
      <healthCheckPort>80</healthCheckPort>
    </servicePort>
    <member>
      <ipAddress>192.168.10.7</ipAddress>
      <weight>1</weight>
      <servicePort>
        <protocol>HTTP</protocol>
        <port>80</port>
      </servicePort>
    </member>
  </pool>
  ...
</loadBalancer>
<ipsec>
  <enabled>true</enabled>
  <logging>
    <enable>>false</enable>
    <logLevel>info</logLevel>

```

```

</logging>
<sites>
  <site>
    <enabled>true</enabled>
    <name>site1</name>
    <localId>10.112.2.40</localId>
    <localIp>10.112.2.40</localIp>
    <peerId>10.112.2.41</peerId>
    <peerIp>10.112.2.41</peerIp>
    <encryptionAlgorithm>aes256</encryptionAlgorithm>
    <mtu>1500</mtu>
    <enablePfs>true</enablePfs>
    <dhGroup>dh2</dhGroup>
    <localSubnets>
      <subnet>192.168.10.0/24</subnet>
    </localSubnets>
    <peerSubnets>
      <subnet>192.168.40.0/24</subnet>
    </peerSubnets>
    <psk>1234</psk>
    <authenticationMode>psk</authenticationMode>
  </site>
  ....
</sites>
<global>
  <caCertificates/>
  <crlCertificates/>
</global>
</ipsec>
<dhcp>
  <enabled>true</enabled>
  <staticBindings>
    <staticBinding>
      <autoConfigureDNS>true</autoConfigureDNS>
      <bindingId>binding-1</bindingId>
      <vmId>vm-2460</vmId>
      <vnicId>1</vnicId>
      <hostname>test</hostname>
      <ipAddress>192.168.10.6</ipAddress>
      <defaultGateway>192.168.10.1</defaultGateway>
      <leaseTime>86400</leaseTime>
    </staticBinding>
    ....
  </staticBindings>
  <ipPools>
    <ipPool>
      <autoConfigureDNS>true</autoConfigureDNS>
      <poolId>pool-1</poolId>
      <ipRange>192.168.10.2-192.168.10.5</ipRange>
      <defaultGateway>192.168.10.1</defaultGateway>
      <leaseTime>86400</leaseTime>
    </ipPool>
    ....
  </ipPools>
  <logging>
    <enable>false</enable>
    <logLevel>info</logLevel>
  </logging>
</dhcp>
<nat>
  <natRules>
    <natRule>
      <ruleId>196610</ruleId>
      <ruleTag>196610</ruleTag>
      <ruleType>user</ruleType>
      <action>dnat</action>
      <vnic>1</vnic>
      <originalAddress>10.112.196.162</originalAddress>
    </natRule>
  </natRules>

```

```

    <translatedAddress>192.168.10.3</translatedAddress>
    <loggingEnabled>>false</loggingEnabled>
    <enabled>true</enabled>
    <protocol>tcp</protocol>
    <originalPort>80</originalPort>
    <translatedPort>80</translatedPort>
  </natRule>
  ....
</natRules>
</nat>
</features>
<autoConfiguration>
  <enabled>true</enabled>
  <rulePriority>high</rulePriority>
</autoConfiguration>
</edge>

```

---

## Redeploying vShield Edge Appliances

Redeploys the vShield Edge appliances and re-applies the feature configuration stored in the vShield Manager database.

### Example 5-174. Redeploy vShield Edge appliances

---

Request:

POST https://<vsm-ip>/api/3.0/edges/<edgeId>?action=redeploy

---

## Managing CLI Credentials and Access

You can modify the CLI credentials and enable or disable SSH services for a vShield Edge.

### Change CLI Credentials

Changes the CLI credentials for the specified vShield Edge. You can modify the:

- password for an existing CLI user.
- username and password for the user. This deletes the old user and creates a new user with the specified username and password.

The CLI password must be at least 7 characters long and must contain at least one special character, digit, and alphabet.

### Example 5-175. Change CLI credentials

---

Request:

PUT https://<vsm-ip>/api/3.0/edges/<edgeId>/clisettings

Request Body:

```

<cliSettings>    <!-- optional. Default user/pass is admin/default, and remoteAccess is false (i.e. disabled) -->
  <userName>test</userName>
  <password>testpass</password>
  <remoteAccess>true</remoteAccess>
</cliSettings>

```

---

### Change CLI Remote Access

Enables or disables the SSH service on the specified vShield Edge.

**Example 5-176.** Change CLI remote access

---

Request:

POST https://<vsm-ip>/api/3.0/edges/<edgeId>/cliremoteaccess?enable=true|false

---

## Managing the Remote Syslog Server

### Query Remote Syslog Server

Retrieves details about the configured syslog server.

**Example 5-177.** Get syslog server

---

Request:

GET https://&lt;vsm-ip&gt;/api/3.0/edges/&lt;edgeId&gt;/syslog/config

Response Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<syslog>
  <protocol>udp</protocol>
  <serverAddresses>
    <ipAddress>1.1.1.1</ipAddress>
    <ipAddress>1.1.1.2</ipAddress>
  </serverAddresses>
</syslog>
```

---

### Reconfigure Remote Syslog Server

Updates syslog server values.

**Example 5-178.** Reconfigure syslog server

---

Request:

PUT https://&lt;vsm-ip&gt;/api/3.0/edges/&lt;edgeId&gt;/syslog/config

Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<syslog>
  <protocol>udp</protocol>
  <serverAddresses>
    <ipAddress>1.1.1.1</ipAddress> <!-- Optional. Default is "udp". Valid values : tcp|udp -->
    <ipAddress>1.1.1.2</ipAddress> <!-- Maximum 2 remote IPs can be configured. -->
  </serverAddresses>
</syslog>
```

---

### Delete Remote Syslog Server

Deletes syslog server.

**Example 5-179.** Delete syslog server

---

Request:

DELETE https://<vsm-ip>/api/3.0/edges/<edgeId>/syslog/config

---

## Debugging and Support

To help with your own debugging and to provide information for VMware technical support, APIs are available to retrieve vShield logs and get statistics about Edge services.

### Query Technical Support Log

This call provides the technical support logs from vShield Edge. These are often required for debugging purposes. The call returns the location where the compressed log files are downloaded.

#### Example 5-180. Get support logs

Request:

```
GET https://<vsm-ip>/api/3.0/edges/<edgeId>/techsupportlogs
```

The technical support log is placed in a file, however the REST API has no provision for downloading it, and wget and curl do not have permission to download it, either. You can retrieve the log with vShield Manager by clicking **Settings & Reports > Configuration > Support > [Log Download] Initiate.A**

### Query vShield Edge Service Statistics

Retrieves service statistics about the specified vShield Edge.

#### Example 5-181. Get vShield Edge service statistics

Request:

```
GET https://<vsm-ip>/api/3.0/edges/<edgeId>/statistics/dashboard/?interval=<range><!-- Optional. Default is 60 min. Possible values are 1-60 minutes, or oneDay|oneWeek|oneMonth|oneYear
```

Response Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<dashboardStatistics>
  <meta>
    <startTime>1344809160</startTime>    <!-- in seconds -->
    <endTime>1344809460</endTime>    <!-- in seconds -->
    <interval>300</interval>
  </meta>
  <data>
    <interfaces>
      <vNic_0_in_pkt>
        <dashboardStatistic>
          <timestamp>1344809160</timestamp>
          <value>0.0</value>
        </dashboardStatistic>
        <dashboardStatistic>
          <timestamp>1344809460</timestamp>
          <value>0.0</value>
        </dashboardStatistic>
      </vNic_0_in_pkt>
      ...
      <vNic_9_in_pkt>
        <dashboardStatistic>
          <timestamp>1344809160</timestamp>
          <value>0.0</value>
        </dashboardStatistic>
        <dashboardStatistic>
          <timestamp>1344809460</timestamp>
          <value>0.0</value>
        </dashboardStatistic>
      </vNic_9_in_pkt>
    </interfaces>
  </data>
</ipsec>
```

```

    <ipsecTunnels>
      <dashboardStatistic>
        <timestamp>1344809160</timestamp>
        <value>0.0</value>
      </dashboardStatistic>
      <dashboardStatistic>
        <timestamp>1344809460</timestamp>
        <value>0.0</value>
      </dashboardStatistic>
    </ipsecTunnels>
    <ipsecBytesIn>
      <dashboardStatistic>
        <timestamp>1344809160</timestamp>
        <value>0.0</value>
      </dashboardStatistic>
      <dashboardStatistic>
        <timestamp>1344809460</timestamp>
        <value>0.0</value>
      </dashboardStatistic>
    </ipsecBytesIn>
    <ipsecBytesOut>
      <dashboardStatistic>
        <timestamp>1344809160</timestamp>
        <value>0.0</value>
      </dashboardStatistic>
      <dashboardStatistic>
        <timestamp>1344809460</timestamp>
        <value>0.0</value>
      </dashboardStatistic>
    </ipsecBytesOut>
  </ipsec>
  <sslvpn>
    <sslvpnBytesOut>
      <dashboardStatistic>
        <timestamp>1344809160</timestamp>
        <value>0.0</value>
      </dashboardStatistic>
      <dashboardStatistic>
        <timestamp>1344809460</timestamp>
        <value>0.0</value>
      </dashboardStatistic>
    </sslvpnBytesOut>
    <sslvpnBytesIn>
      <dashboardStatistic>
        <timestamp>1344809160</timestamp>
        <value>0.0</value>
      </dashboardStatistic>
      <dashboardStatistic>
        <timestamp>1344809460</timestamp>
        <value>0.0</value>
      </dashboardStatistic>
    </sslvpnBytesIn>
    <activeClients>
      <dashboardStatistic>
        <timestamp>1344809160</timestamp>
        <value>0.0</value>
      </dashboardStatistic>
      <dashboardStatistic>
        <timestamp>1344809460</timestamp>
        <value>0.0</value>
      </dashboardStatistic>
    </activeClients>
    <authFailures>
      <dashboardStatistic>
        <timestamp>1344809160</timestamp>
        <value>NaN</value>
      </dashboardStatistic>
      <dashboardStatistic>

```

```

        <timestamp>1344809460</timestamp>
        <value>0.0</value>
    </dashboardStatistic>
</authFailures>
<sessionsCreated>
    <dashboardStatistic>
        <timestamp>1344809160</timestamp>
        <value>NaN</value>
    </dashboardStatistic>
    <dashboardStatistic>
        <timestamp>1344809460</timestamp>
        <value>0.0</value>
    </dashboardStatistic>
</sessionsCreated>
</sslvpn>
<firewall>
    <connections>
        <dashboardStatistic>
            <timestamp>1344809160</timestamp>
            <value>7.0</value>
        </dashboardStatistic>
        <dashboardStatistic>
            <timestamp>1344809460</timestamp>
            <value>9.0</value>
        </dashboardStatistic>
    </connections>
</firewall>
<loadBalancer>
    <lbSessions>
        <dashboardStatistic>
            <timestamp>1344809160</timestamp>
            <value>0.0</value>
        </dashboardStatistic>
        <dashboardStatistic>
            <timestamp>1344809460</timestamp>
            <value>0.0</value>
        </dashboardStatistic>
    </lbSessions>
    <lbHttpReqs>
        <dashboardStatistic>
            <timestamp>1344809160</timestamp>
            <value>0.0</value>
        </dashboardStatistic>
        <dashboardStatistic>
            <timestamp>1344809460</timestamp>
            <value>0.0</value>
        </dashboardStatistic>
    </lbHttpReqs>
    <lbBpsIn>
        <dashboardStatistic>
            <timestamp>1344809160</timestamp>
            <value>0.0</value>
        </dashboardStatistic>
        <dashboardStatistic>
            <timestamp>1344809460</timestamp>
            <value>0.0</value>
        </dashboardStatistic>
    </lbBpsIn>
    <lbBpsOut>
        <dashboardStatistic>
            <timestamp>1344809160</timestamp>
            <value>0.0</value>
        </dashboardStatistic>
        <dashboardStatistic>
            <timestamp>1344809460</timestamp>
            <value>0.0</value>
        </dashboardStatistic>
    </lbBpsOut>

```

```
</loadBalancer>  
</data>  
</dashboardStatistics>
```

---



## Working with VXLAN Virtual Wires

---

In large cloud deployments, applications within virtual networks may need to be logically isolated. For example, a three-tier application can have multiple virtual machines requiring logically isolated networks between the virtual machines. Traditional network isolation techniques such as VLAN (4096 LAN segments through a 12-bit VLAN identifier) may not provide enough segments for such deployments. In addition, VLAN based networks are bound to the physical fabric and their mobility is restricted.

vShield VXLAN virtual wire is a scalable flat Layer 2 network segment. This feature allows you provides network agility by allowing you to deploy an application on any available cluster and transport virtual machines across a broader diameter. The underlying technology, referred to as Virtual eXtensible LAN (or VXLAN), defines a 24-bit LAN segment identifier to provide segmentation at cloud-deployment scale. VXLAN virtual wires enable you to grow your cloud deployments with repeatable pods in different subnets. Cross cluster placement of virtual machines helps you to fully utilize your network resources without any physical re-wiring. VXLAN virtual wires thus provide application level isolation.

You must be a Security Administrator in order to create VXLAN networks.

**IMPORTANT** All vShield REST requests require authorization. See [“Using the vShield REST API”](#) on page 16 for details about basic authorization.

This chapter includes the following topics:

- [“Preparing for VXLAN Virtual Wires”](#) on page 153
- [“Configuring Switches”](#) on page 154
- [“Working with Cluster Switch Mappings”](#) on page 156
- [“Working with EAM Agencies”](#) on page 158
- [“Working with Segment IDs”](#) on page 160
- [“Working with Multicast Address Ranges”](#) on page 162
- [“Working with Network Scopes”](#) on page 164
- [“Working with Virtualized Networks”](#) on page 166
- [“Managing the VXLAN Virtual Wire UDP Port”](#) on page 168
- [“Querying Allocated Resources”](#) on page 169
- [“Testing Multicast Group Connectivity”](#) on page 169
- [“Performing Ping Test”](#) on page 170

### Preparing for VXLAN Virtual Wires

Before creating a network scope, you must have a vShield Edge installed per port group, vSphere distributed switch port group, or Cisco® Nexus 1000V, and connect the vShield Edge to your external network. All switches must be of same type.

In addition, you must have the following:

- VMware vCenter Server 5.1 or later
- The Managed IP address must be set in the vCenter Server Runtime Settings. For more information, see the *vCenter Server and Host Management*
- Only DHCP is supported for IP address allocation for the vmknics on the port groups.

## Configuring Switches

You must prepare each vDS by specifying the VLAN for your L2 domain and the MTU for each vDS.

### Prepare Switch

The MTU is the maximum amount of data that can be transmitted in one packet before it is divided into smaller packets. The frames are slightly larger in size because of the traffic encapsulation, so the MTU required is higher than the standard MTU. You must set the MTU for each switch to 1600 or higher.

#### Example 6-1. Prepare switch

---

Request:

POST https://<vsm-ip>/api/2.0/vdn/switches

Request Body:

```
<vdsContext>
  <switch>
    <objectId>dvs-7</objectId>
    <type><typeName>DistributedVirtualSwitch</typeName></type>
    <name>My Name</name>
    <revision>0</revision>
    <objectTypeName>DistributedVirtualSwitch</objectTypeName>
  </switch>
  <teaming>LACP_PASSIVE</teaming>
  <mtu>9000</mtu>
  <promiscuousMode>>false</promiscuousMode>
</vdsContext>
```

---

### Edit Teaming Policy

You can edit the teaming policy for a configured switch.

#### Example 6-2. Edit teaming policy

---

Request:

PUT https://<vsm-ip>/api/2.0/vdn/agency/agencyID

Request Body:

```
<clusterList>
  <cluster>domain-c56</cluster>
  ...
</clusterList>
```

---

### Query Configured Switches

You can retrieve all configured switches.

**Example 6-3.** Get all configured switches

---

Request:

GET https://<vsm-ip>/api/2.0/vdn/switches

Response Body:

```

<vdsContexts>
  <vdsContext>
    <switch>
      <objectId>dvs-26</objectId>
      <type><typeName>DistributedVirtualSwitch</typeName></type>
      <name>My Name</name>
      <revision>0</revision>
      <objectTypeName>DistributedVirtualSwitch</objectTypeName>
    </switch>
    <teaming>LACP_PASSIVE</teaming>
    <mtu>mtu-value</mtu>
  </vdsContext>
  ...
  <vdsContext>...</vdsContext>
  ...
</vdsContexts>

```

---

## Query Configured Switches on Datacenter

You can retrieve all configured switches on a datacenter.

**Example 6-4.** Get configured switches on a datacenter

---

Request:

GET https://<vsm-ip>/api/2.0/vdn/switches/datacenter/<datacenterID>

Response Body:

```

<vdsContexts>
  <vdsContext>
    <switch>
      <objectId>dvs-26</objectId>
      <type><typeName>DistributedVirtualSwitch</typeName></type>
      <name>My Name</name>
      <revision>0</revision>
      <objectTypeName>DistributedVirtualSwitch</objectTypeName>
    </switch>
    <teaming>LACP_PASSIVE</teaming>
    <mtu>mtu-value</mtu>
  </vdsContext>
  ...
  <vdsContext>...</vdsContext>
  ...
</vdsContexts>

```

---

## Query Specific Switch

You can retrieve a specific switch by specifying its ID.

**Example 6-5.** Get specific switch

---

Request:

GET https://<vsm-ip>/api/2.0/vdn/switches/<switchID>

Response Body:

```

<vdsContext>
  <switch>
    <objectId>dvs-26</objectId>
    <type><typeName>DistributedVirtualSwitch</typeName></type>
    <name>My Name</name>
    <revision>0</revision>
    <objectTypeName>DistributedVirtualSwitch</objectTypeName>
  </switch>
  <teaming>LACP_PASSIVE</teaming>
  <mtu>mtu-value</mtu>
</vdsContext>

```

---

## Delete Switch

You can delete a switch.

### Example 6-6. Delete switch

---

Request:

```
DELETE https://<vsm-ip>/api/2.0/vdn/switches/switchID
```

---

## Working with Cluster Switch Mappings

You must map each cluster that is to participate in a VXLAN virtual wire to a vDS. When you map a cluster to a switch, each host in that cluster is enabled for VXLAN virtual wires.

### Map a Cluster to a Switch

You must map each cluster that is to participate in a VXLAN virtual wire to a vDS. When you map a cluster to a switch, each host in that cluster is enabled for VXLAN virtual wires.

### Example 6-7. Map cluster to switch

---

Request:

```
POST https://<vsm-ip>/api/2.0/vdn/map/cluster/clusterID
```

Request Body:

```

<clusterMappingSpec>
  <switch>
    <objectId>dvs-26</objectId>
    <type><typeName>DistributedVirtualSwitch</typeName></type>
    <name>My Name</name>
    <revision>0</revision>
    <objectTypeName>DistributedVirtualSwitch</objectTypeName>
  </switch>
  <vlanId>23</vlanId>
</clusterMappingSpec>

```

---

## Synchronize hosts

Synchronize all the hosts in a cluster with their agency state and if applicable prepare each host for VXLAN traffic. Use this method in cases where automatic host preparation following a cluster preparation operation fails.

### Example 6-8. Synchronize hosts

---

Request:

POST https://<vsm-ip>/api/2.0/vdn/config/cluster/*clusterID*?action=synchronize

---

## Query all Cluster Mappings

You can retrieve all cluster mappings

### Example 6-9. Get all cluster mappings

---

Request:

GET https://<vsm-ip>/api/2.0/vdn/map/cluster

Response Body:

```
<clusterMappings>
  <clusterMapping>
    <cluster>
      <objectId>domain-c26</objectId>
      <type><typeName>ClusterComputeResource</typeName></type>
      <name>My Name</name>
      <revision>0</revision>
      <objectTypeName>ClusterComputeResource</objectTypeName>
    </cluster>
    <clusterMappingSpec>
      <switch>
        <objectId>dvs-26</objectId>
        <type><typeName>DistributedVirtualSwitch</typeName></type>
        <name>My Name</name>
        <revision>0</revision>
        <objectTypeName>DistributedVirtualSwitch</objectTypeName>
      </switch>
      <vlanId>23</vlanId>
    </clusterMappingSpec>
  </clusterMapping>
  ...
  <clusterMapping>...</clusterMapping>
  ...
</clusterMappings>
```

---

## Query Mappings by Switch

You can retrieve all clusters mapped to a switch.

### Example 6-10. Get all clusters mapped to a switch

---

Request:

GET https://<vsm-ip>/api/2.0/vdn/map/switches/*switchID*

Response Body:

```
<clusterMappings>
  <clusterMapping>
    <cluster>
      <objectId>domain-c26</objectId>
      <type><typeName>ClusterComputeResource</typeName></type>
      <name>My Name</name>
      <revision>0</revision>
      <objectTypeName>ClusterComputeResource</objectTypeName>
    </cluster>
    <clusterMappingSpec>
      <switch>
        <objectId>dvs-26</objectId>
        <type><typeName>DistributedVirtualSwitch</typeName></type>
        <name>My Name</name>
```

```

        <revision>0</revision>
        <objectTypeName>DistributedVirtualSwitch</objectTypeName>
    </switch>
    <vlanId>23</vlanId>
</clusterMappingSpec>
</clusterMapping>
...
<clusterMapping>...</clusterMapping>
...
</clusterMappings>

```

---

## Query Specific Cluster

Retrieves aa specific cluster.

### Example 6-11. Get specific cluster

---

Request:

GET https://<vsm-ip>/api/2.0/vdn/map/cluster/*clusterID*

Response Body:

```

<clusterMapping>
  <cluster>
    <objectId>domain-c26</objectId>
    <type><typeName>ClusterComputeResource</typeName></type>
    <name>My Name</name>
    <revision>0</revision>
    <objectTypeName>ClusterComputeResource</objectTypeName>
  </cluster>
  <clusterMappingSpec>
    <switch>
      <objectId>dvs-26</objectId>
      <type><typeName>DistributedVirtualSwitch</typeName></type>
      <name>My Name</name>
      <revision>0</revision>
      <objectTypeName>DistributedVirtualSwitch</objectTypeName>
    </switch>
    <vlanId>23</vlanId>
  </clusterMappingSpec>
</clusterMapping>

```

---

## Delete Cluster Switch Mapping

You can delete the mapping between a cluster a switch.

### Example 6-12. Delete mapping

---

Request:

DELETE https://<vsm-ip>/api/2.0/vdn/cluster/*ClusterID*/switches/*SwitchID*

---

## Working with EAM Agencies

An EAM agency prepares the hosts that are a part of the clusters to be included in a network scope. When you add a host to the cluster, it is automatically prepared for a VXLAN virtual wire.

## Install EAM Agency

Once the cluster-switch mapping is done you must create an agency on the vCenter Server to manage the network boundary.

### Example 6-13. Install or uninstall EAM agency

---

Request:

POST <https://<vsm-ip>/api/2.0/vdn/agency?action=install>

Request Body:

```
<clusterList>
  <cluster>domain-c56&lt;/cluster>
  ...
</clusterList>
```

---

The output of the call indicates the agency state: green (enabled), yellow (disabled), or red (uninstalled).

## Synchronize Agency State

You can synchronize the state of an agency in the database.

### Example 6-14. Synchronize agency state

---

Request:

POST <https://<vsm-ip>/api/2.0/vdn/agency/agencyID>

---

The output of the call indicates the agency state: green (enabled), yellow (disabled), or red (uninstalled).

## Replace Agency Scope

You can change the scope of a specific agency.

### Example 6-15. Synchronize agency state

---

Request:

PUT <https://<vsm-ip>/api/2.0/vdn/agency/agencyID>

Request Body:

```
<clusterList>
  <cluster>domain-c56&lt;/cluster>
  ...
</clusterList>
```

---

The output of the call indicates the agency state: green (enabled), yellow (disabled), or red (uninstalled).

## Query Agency by Cluster

You can retrieve all agencies on a specific cluster.

### Example 6-16. Get agency by cluster

---

Request:

GET <https://<vsm-ip>/api/2.0/vdn/agency/clusterID>

---

## Query Agency Status

You can retrieve the status of a specific agency.

### Example 6-17. Get agency status

---

Request:

GET https://<vsm-ip>/api/2.0/vdn/agency/*agencyID*

---

## Query Agency ID for Cluster

You can retrieve the agency ID for the specified cluster.

### Example 6-18. Get agency ID

---

Request:

POST https://<vsm-ip>/api/2.0/vdn/cluster/agency/*clusterID*

---

## Delete Agency

You can delete an agency.

### Example 6-19. Delete agency

---

Request:

DELETE https://<vsm-ip>/api/2.0/vdn/config/agency/*agencyID*

---

## Uninstall Agency Status

You can uninstall an agency by specifying its ID.

### Example 6-20. Uninstall agency

---

Request:

POST https://<vsm-ip>/api/2.0/vdn/config/agency/<agencyID>?action=uninstall

Request Body:

```
<clusterList>
  <cluster>domain-c67</cluster>
</clusterList>
```

---

## Working with Segment IDs

You can specify a segment ID pool to isolate your network traffic.

### Add a new Segment ID Range

You can add a segment ID range, from which an ID is automatically assigned to the VXLAN virtual wire.

### Example 6-21. Add a segment ID range

---

Request:

POST https://<vsm-ip>/api/2.0/vdn/config/segments



Request Body:

```
<segmentRanges>
  <segmentRange>
    <id>1</id>
    <name>name</name>
    <desc>desc</desc>
    <begin>1000</begin>
    <end>1500</end>
  </segmentRange>
  <segmentRange>
    ....
  </segmentRange>
  ....
</segmentRanges>
```

---

The segment range is inclusive – the beginning and ending IDs are included.

## Query all Segment ID Ranges

You can retrieve all segment ID ranges.

### Example 6-22. Get all Segment ID Ranges

---

Request:

GET https://<vsm-ip>/api/2.0/vdn/config/segments

Response Body:

```
<segmentRanges>
  <segmentRange>
    <id>1</id>
    <name>name</name>
    <desc>desc</desc>
    <begin>5000</begin>
    <end>9000</end>
  </segmentRange>
  <segmentRange>
    ....
  </segmentRange>
</segmentRanges>
```

---

## Query a Specific Segment ID Range

You can retrieve a segment ID range by specifying the segment ID.

### Example 6-23. Get a specific Segment ID Range

---

Request:

GET https://<vsm-ip>/api/2.0/vdn/config/segments/*SegmentID*

Response Body:

```
<segmentRange>
  <id>1</id>
  <name>name</name>
  <desc>desc</desc>
  <begin>10000</begin>
  <end>11000</end>
</segmentRange>
```

---

## Update a Segment ID Range

You can update the name, description, or end of a segment ID range.

### Example 6-24. Update a Segment ID Range

---

Request:

PUT https://<vsm-ip>/api/2.0/vdn/config/segments/*SegmentID*

Request Body:

```
<segmentRange>
  <end>3000</end>
  <name>name</name>
  <desc>desc</desc>
</segmentRange>
```

---

## Delete a Segment ID Range

You can delete a segment ID range.

### Example 6-25. Delete a Segment ID Range

---

Request:

DELETE https://<vsm-ip>/api/2.0/vdn/config/segments/*SegmentID*

---

## Working with Multicast Address Ranges

Specifying a multicast address range helps in spreading traffic across your network to avoid overloading a single multicast address. A virtualized network-ready host is assigned an IP address from this range.

## Add a new Multicast Address Range

You can add a new multicast address range.

### Example 6-26. Add a multicast address range

---

Request:

POST https://<vsm-ip>/api/2.0/vdn/config/multicasts

Request Body:

```
<multicastRanges>
  <multicastRange>
    <id>1</id>
    <name>name</name>
    <desc>desc</desc>
    <begin>239.1.1.1</begin>
    <end>239.3.3.3</end>
  </multicastRange>
  <multicastRange>
    ....
  </multicastRange>
  ....
</multicastRanges>
```

---

The address range is inclusive – the beginning and ending addresses are included.

## Query all Multicast Address Ranges

You can retrieve all multicast address ranges.

**Example 6-27. Get all multicast ranges**

---

Request:

GET https://<vsm-ip>/api/2.0/vdn/config/multicasts

Response Body:

```

<multicastRanges>
  <multicastRange>
    <id>1</id>
    <name>name</name>
    <desc>desc</desc>
    <begin>239.1.1.1</begin>
    <end>239.3.3.3</end>
  </multicastRange>
  <multicastRange>
    ...
  </multicastRange>
  ...
</multicastRanges>

```

---

## Get a Specific Multicast Address Range

You can retrieve a specific multicast address range.

**Example 6-28. Get a multicast range**

---

Request:

GET https://<vsm-ip>/api/2.0/vdn/config/multicasts/*multicastAddressRangeID*

Response Body:

```

<multicastRange>
  <id>1</id>
  <name>name</name>
  <desc>desc</desc>
  <begin>239.1.1.1</begin>
  <end>239.3.3.3</end>
</multicastRange>

```

---

## Update a Multicast Address Range

You can update the name, description, or end address of a multicast address range.

**Example 6-29. Update a multicast range**

---

Request Header:

PUT https://<vsm-ip>/api/2.0/vdn/config/multicasts/*multicastAddressRangeID*

Request Body:

```

<<segmentRange>
  <end>3000</end>
  <name>name</name>
  <desc>desc</desc>
</segmentRange>

```

---

## Delete a Multicast Address Range

You can delete a multicast address range.

**Example 6-30. Delete multicast address range**

---

Request:

```
DELETE https://<vsm-ip>/api/2.0/vdn/config/multicasts/<multicasts/multicasts/
multicastAddressRangeID
```

---

## Working with Network Scopes

A network scope is the networking infrastructure within provider virtual datacenters.

### Create a Network Scope

You must specify the clusters that are to be part of the network scope. You must have the VLAN ID, UUID of the vCenter Server, and vDS ID.

**Example 6-31. Create a network scope**

---

Request:

```
POST https://<vsm-ip>/api/2.0/vdn/scopes
```

Request Body:

```
<vdnScope>
  <clusters>
    <cluster><cluster><objectId>domain-c59</objectId></cluster></cluster>
  </clusters>
</vdnScope>
```

---

### Edit a Network Scope

You can add a cluster to or delete a cluster from a network scope.

**Example 6-32. Create a network scope**

---

Request:

```
POST https://<vsm-ip>/api/2.0/vdn/scopes/scopeID?action=patch
```

Request Body:

```
<vdnScope>
  <objectId>{id}</objectId>
  <clusters>
    <cluster><cluster><objectId>domain-c59</objectId></cluster></cluster>
  </clusters>
</vdnScope>
```

---

### Update Attributes on a Network Scope

You can update the attributes of a network scope.

**Example 6-33. Update attributes of a network scope**

---

Request:

```
PUT https://<vsm-ip>/api/2.0/vdn/scopes/scopeID/attributes
```

Request Body:

```
<vdnScope>
  <objectId>vdnScope-1</objectId>
```

```

    <name>new name</name>
    <description>new description</description>
  </vdnScope>

```

---

## Query existing Network Scopes

You can retrieve all existing network scopes.

### Example 6-34. Get all network scopes

---

Request:

GET https://<vsm-ip>/api/2.0/vdn/scopes

Response Body:

```

<vdnScopes>
<vdnScope>
  <objectId>vdnscope-2</objectId>
  <type><typeName>VdnScope</typeName></type>
  <name>My Name</name>
  <description>My Description</description>
  <revision>0</revision>
  <objectTypeName>VdnScope</objectTypeName>
  <extendedAttributes/>
  <id>vdnscope-2</id>
  <clusters>
    <cluster>
      <cluster>
        <objectId>domain-c124</objectId>
        <type><typeName>ClusterComputeResource</typeName></type>
        <name>vxlan-cluster</name>
        <scope><id>datacenter-2</id><objectTypeName>Datacenter</objectTypeName><name>dc1</name></scope>
        <extendedAttributes/>
      </cluster>
    </cluster>
    ...
  </clusters>
  <virtualWireCount>10</virtualWireCount>
</vdnScope>
...
<vdnScope>...</vdnScope>
...
</vdnScopes>

```

---

## Query a Specific Network Scope

You can retrieve a specific network scope.

### Example 6-35. Get a network scope

---

Request:

GET https://<vsm-ip>/api/2.0/vdn/scopes/scopeID

Response Body:

```

<vdnScope>
  <objectId>vdnscope-2</objectId>
  <type><typeName>VdnScope</typeName></type>
  <name>My Name</name>
  <description>My description</description>
  <revision>0</revision>
  <objectTypeName>VdnScope</objectTypeName>
  <extendedAttributes/>

```

```

<id>vdsnscope-2</id>
<clusters>
<cluster>
<cluster>
<objectId>domain-c124</objectId>
<type><typeName>ClusterComputeResource</typeName></type>
<name>vxlan-cluster</name>
<scope><id>datacenter-2</id><objectTypeName>Datacenter</objectTypeName><name>dc1</name></scope>
<extendedAttributes/>
</cluster>
</cluster>
...
</clusters>
<virtualWireCount>10</virtualWireCount>
</vdnScope>

```

---

## Delete a Network Scope

You can delete a network scope.

### Example 6-36. Delete network scope

---

Request:

DELETE https://<vsm-ip>/api/2.0/vdn/scopes/*scopeID*

---

## Working with Virtualized Networks

A VXLAN virtual wire is a collection of vDS port groups across multiple virtual distributed switches (vDS) within a network scope.

## Create a VXLAN Virtual Wire

You can create a new VXLAN virtual wire on the specified network scope. You must have defined a segment ID range and a multicast address range before creating a VXLAN virtual wire.

### Example 6-37. Create a VXLAN virtual wire

---

Request:

POST https://<vsm-ip>/api/2.0/vdn/scopes/*scopeID*/virtualwires

Request Body:

```

<virtualWireCreateSpec>
  <name>virtual wire name</name>
  <description>virtual wire description</description>
  <tenantId>virtual wire tenant</tenantId>
</virtualWireCreateSpec>

```

---

## Query all VXLAN Virtual Wires on a Network Scope

You can retrieve all VXLAN virtual wires on the specified network scope.

### Example 6-38. Get all VXLAN virtual wires

---

Request:

GET https://<vsm-ip>/api/2.0/vdn/scopes/*scopeID*/virtualwires

Response Body:

<virtualWires>

```

<sortedDataPage>
  <datapart class="virtualWire">
    <objectId>virtualwire-1</objectId>
    <name>vWire1</name>
    <description>virtual wire 1</description>
    <tenantId>virtual wire tenant</tenantId>
    <revision>0</revision>
    <vdnScopeId>vDNSscope-7</vdnScopeId>
    <vdsContextWithBacking>
      <teaming>ETHER_CHANNEL</teaming>
      <switchId>dvs-81</switchId>
      <backingType>portgroup</backingType>
      <backingValue>dvportgroup-88</backingValue>
    </vdsContextWithBacking>
    <vdnId>5002</vdnId>
    <multicastAddr>239.0.0.3</multicastAddr>
  </datapart>
  ....
  <datapart class="virtualWire">
  ....
</datapart>
<pagingInfo>
  <pageSize>20</pageSize>
  <startIndex>0</startIndex>
  <totalCount>3</totalCount>
  <sortOrderAscending>false</sortOrderAscending>
</pagingInfo>
</sortedDataPage>
</virtualWires>

```

---

## Query all VXLAN Virtual Wires on all Network Scopes

You can retrieve all VXLAN virtual wires across all network scopes.

**Example 6-39.** Get all VXLAN virtual wires on all network scopes

---

Request:

GET https://<vsm-ip>/api/2.0/vdn/virtualwires

Response Body:

```

</virtualWires>
  <sortedDataPage>
    <datapart class="virtualWire">
      <objectId>virtualwire-1</objectId>
      <name>vWire1</name>
      <description>virtual wire 1</description>
      <tenantId>virtual wire tenant</tenantId>
      <revision>0</revision>
      <vdnScopeId>vDNSscope-7</vdnScopeId>
      <vdsContextWithBacking>
        <teaming>ETHER_CHANNEL</teaming>
        <switchId>dvs-81</switchId>
        <backingType>portgroup</backingType>
        <backingValue>dvportgroup-88</backingValue>
      </vdsContextWithBacking>
      <vdnId>5002</vdnId>
      <multicastAddr>239.0.0.3</multicastAddr>
    </datapart> ....
    <datapart class="virtualWire"> ....
  </datapart>
  <pagingInfo>
    <pageSize>20</pageSize>
    <startIndex>0</startIndex>
    <totalCount>3</totalCount>
    <sortOrderAscending>false</sortOrderAscending>
  </pagingInfo>
</sortedDataPage>
</virtualWires>

```

```

    </pagingInfo>
  </sortedDataPage>
</virtualWires>

```

---

## Query a Specific VXLAN Virtual Wire

You can retrieve the definition for a VXLAN virtual wire.

**Example 6-40.** Get a VXLAN virtual wire definition

---

Request:

GET https://<vsm-ip>/api/2.0/vdn/virtualwires/*virtualWireID*

Response Body:

```

<virtualWire>
  <name>Test Virtual Wire</name>
  <description>Test Virtual Wire Description</description>
  <objectid>virtualwire-4</objectid>
  <vdnScopeId>vdnscope-3</vdnScopeId>
  <revision>1</revision>
  <vdsContextWithBacking>
    <teaming>ETHER_CHANNEL</teaming>
    <switchId>dvs-162</switchId>
    <backingType>PortGroup</backingType>
    <backingValue>pg-moid</backingValue>
  </vdsContextWithBacking>
  <vdnId>5002</vdnId>
  <multicastAddr>239.0.0.3</multicastAddr>
</virtualWire>

```

---

## Delete a VXLAN Virtual Wire

You can delete a VXLAN virtual Wire.

**Example 6-41.** Delete virtual wire

---

Request:

DELETE https://<vsm-ip>/api/2.0/vdn/virtualwires/*virtualWireID*

---

## Managing the VXLAN Virtual Wire UDP Port

You can retrieve or update the UDP port.

### Get UDP Port

You can retrieve the UDP port for the VXLAN virtual wire.

**Example 6-42.** Get UDP port

---

Request:

Get https://<vsm-ip>/api/2.0/vdn/config/vxlan/udp/port

---

### Update UDP Port

You can change the UDP port for the VXLAN virtual wire. If not set, the port defaults to port 8472.



**Example 6-43. Change UDP port**

Request:

```
PUT https://<vsm-ip>/api/2.0/vdn/config/vxlan/udp/port/port
```

## Querying Allocated Resources

You can retrieve a list of resources allocated to VXLAN virtual wires in your network.

**Example 6-44. Get resources**

Get segment IDs allocated to VXLAN virtual wires:

```
GET https://<vsm-ip>/api/2.0/vdn/config/resources/allocated?type=segmentId&pagesize={ pageSize }&startindex={ startIndex }
```

Get multicast address range allocated to VXLAN virtual wires:

```
GET https://<vsm-ip>/api/2.0/vdn/config/resources/allocated?type=multicastAddress&pagesize={ pageSize }&startindex={ startIndex }
```

where

- start index is an optional parameter which specifies the starting point for retrieving the resources. If this parameter is not specified, resources are retrieved from the beginning.
- page size is an optional parameter that limits the maximum number of entries returned by the API. The default value for this parameter is 256 and the valid range is 1-1024.

## Testing Multicast Group Connectivity

You can perform a multicast group connectivity test in a network scope or VXLAN virtual wire.

### Test Multicast Group Connectivity in a Network Scope

**Example 6-45. Test multicast group connectivity in network scope**

Request:

```
PUT https://<vsm-ip>/api/2.0/vdn/scopes/ScopeID/conn-check/multicast
```

Request Body:

```
<testParameters>
  <gateway>172.23.233.1</gateway>
  <packetSize>1600</packetSize>
  <expectedResponse>5</expectedResponse>
  <returnHopCount>true</returnHopCount>
  <returnRecordIp>true</returnRecordIp>
  <sourceHost>
    <hostId>host-9</hostId>
    <switchId>dvs-22</switchId>
    <vlanId>54</vlanId>
  </sourceHost>
  <destinationHost>
    <hostId>host-92</hostId>
    <switchId>dvs-22</switchId>
    <vlanId>54</vlanId>
  </destinationHost>
</testParameters>
```

## Test Multicast Group Connectivity in a VXLAN Virtual Wire

### Example 6-46. Test multicast group connectivity in virtual wire

---

Request:

PUT https://<vsm-ip>/api/2.0/vdn/scopes/*virtualWireID*/conn-check/multicast

Request Body:

```
<testParameters>
  <gateway>172.23.233.1</gateway>
  <packetSize>1600</packetSize>
  <expectedResponse>5</expectedResponse>
  <returnHopCount>true</returnHopCount>
  <returnRecordIp>true</returnRecordIp>
  <sourceHost>
    <hostId>host-9</hostId>
    <switchId>dvs-22</switchId>
    <vlanId>54</vlanId>
  </sourceHost>
  <destinationHost>
    <hostId>host-92</hostId>
    <switchId>dvs-22</switchId>
    <vlanId>54</vlanId>
  </destinationHost>
</testParameters>
```

---

## Performing Ping Test

You can perform a point to point connectivity test between two hosts across which a VXLAN virtual wire spans.

### Example 6-47. Perform point to point test

---

Request:

PUT https://<vsm-ip>/api/2.0/vdn/virtualwires/*virtualWireID*/conn-check/p2p

Request Body:

```
<testParameters>
  <gateway>172.23.233.1</gateway>
  <packetSize>1600</packetSize>
  <expectedResponse>5</expectedResponse>
  <returnHopCount>true</returnHopCount>
  <returnRecordIp>true</returnRecordIp>
  <sourceHost>
    <hostId>host-9</hostId>
    <switchId>dvs-22</switchId>
    <vlanId>54</vlanId>
  </sourceHost>
  <destinationHost>
    <hostId>host-92</hostId>
    <switchId>dvs-22</switchId>
    <vlanId>54</vlanId>
  </destinationHost>
</testParameters>
```

---

# vShield App Management

---

You can configure vShield App firewall rules and syslog service by using REST API calls.

This chapter includes the following topics:

- [“Modifying the State of a Datacenter”](#) on page 171
- [“Configuring Firewall Rules for vCenter”](#) on page 172
- [“Configuring the vShield App Firewall”](#) on page 172
- [“Configuring Fail-Safe Mode for vShield App Firewall”](#) on page 183
- [“Working with SpoofGuard”](#) on page 184
- [“Working with Namespaces”](#) on page 186
- [“Excluding Virtual Machines from vShield App Protection”](#) on page 190
- [“Configuring Syslog Service for a vShield App”](#) on page 191
- [“Synchronizing vShield App”](#) on page 192
- [“Querying vShield App Technical Support Log”](#) on page 192
- [“Upgrading vShield App”](#) on page 193

---

**IMPORTANT** All vShield REST requests require authorization. See [“Using the vShield REST API”](#) on page 16 for details about basic authorization.

---

## Modifying the State of a Datacenter

The state of a datacenter is determined by the version of the vShield Manager on that datacenter. For a 5.0 vShield Manager, the datacenter is in the regular state which means only the 5.0 API calls are supported.

When the vShield Manager on a datacenter is upgraded from a previous release, the datacenter is in the backwardCompatible mode which means that only the APIs from the previous release are supported. When the vShield App components on that datacenter are upgraded to 5.0, the datacenter state is automatically changed from backwardCompatible to backwardCompatibleReadyForSwitch. This means that the vShield App components are running in backward compatible mode, so only the APIs from the previous release are supported.

When the datacenter is in the backwardCompatibleReadyForSwitch state, you can switch the datacenter state. While data from the old vShield App is being migrated to the 5.0 vShield App, the datacenter is in the migrating state. Once the data migration is complete, the datacenter state switches automatically to regular.

## Retrieve Datacenter State

You can retrieve the state of the datacenter.

**Example 7-1. Retrieve the datacenter state**

---

Example:

```
GET https://<vsm-ip>/api/2.0/app/firewall/datacenter-2/state
```

---

The XML response represents the DatacenterState object, containing an enumeration of datacenter status. The state could be regular, upgrading, migrating, backwardCompatible, or backwardCompatibleReadyForSwitch.

**Modify Datacenter State**

You can change the state of a datacenter only if it is in the backwardCompatibleReadyForSwitch state.

**Example 7-2. Change datacenter state to migrating**

---

Example:

```
POST https://<vsm-ip>/api/2.0/app/firewall/datacenter-2/state
```

**Configuring Firewall Rules for vCenter**

The primary function of a vShield App is to provide firewall protection on an ESX host by inspecting each session and returning details to the vShield Manager. Traffic details include sources, destinations, direction of sessions, applications, and ports being used. Traffic details can be used to create firewall allow or deny rules.

In the vShield Manager user interface or vSphere Client plug-in, the **App Firewall** tab contains the firewall rules enforced by vShield App instances. You can manage App Firewall rules on a namespace level to provide a consistent set of rules across multiple vShield App instances under these containers. Namespace levels include datacenter, virtual wires, and port group with an independent namespace. As membership in these containers can change dynamically, App Firewall maintains the state of existing sessions without requiring reconfiguration of firewall rules. In this way, App Firewall effectively has a continuous footprint on each ESX host under the managed containers.

All firewall rules configured by using REST requests appear under the **App Firewall** tab for the appropriate container in the vShield Manager user interface and vSphere Client plug-in.

For the complete firewall XML schema, see “[vShield App Firewall Schema](#)” on page 229.

**Configuring the vShield App Firewall**

Firewall precedence is hierarchical at each level (datacenter, virtual wire, or port group with an independent namespace). Choices are DEFAULT or NONE. Only one DEFAULT rule is accepted at layer2 and layer3 containers. The default rule should be at the end of all NONE precedence rules (user defined rules)

Each vShield App enforces the firewall rules in top-to-bottom ordering. A vShield App checks each traffic session against the top rule in the firewall table before moving down the subsequent rules in the table. The first rule in the table that matches the traffic parameters is enforced. See the *vShield Administration Guide* for more information about the hierarchy of vShield App firewall rules.

**Query Firewall Configuration**

You can retrieve the firewall configuration associated with a datacenter, virtual wire, or port group with independent namespace. The template for the API is as follows:

```
GET https://<vsm-ip>/api/2.0/app/firewall/<context>/config?list=<L>&precedence=<P>&rulesType=<R>&configId=<C>
```

Where

- <context> is the context ID of a datacenter, cluster, or dvPortGroup.
- <L> is the listing type, one of the following:
  - status for brief current state

- config for firewall configuration (the default)
- history for configuration history
- consolidated for combined configuration including all rules applicable in the context/
- <P> is the rule precedence, either DEFAULT or NONE.
- <R> can be LAYER3 or LAYER2 to filter the configuration rules for layer 3 or layer 2.
- <C> is the configuration ID used in conjunction with the history listing type.

---

**Example 7-3. Queries for firewall configuration**


---

Get quick status:

GET https://<vsm-ip>/api/2.0/app/firewall/dvportgroup-63/config?list=status

Get complete firewall configuration for context datacenter-21:

GET https://<vsm-ip>/api/2.0/app/firewall/datacenter-21/config?list=config

GET https://<vsm-ip>/api/2.0/app/firewall/dvportgroup-63/config?list=config&precedence=DEFAULT

Get configuration of only Layer 3 rules:

GET https://<vsm-ip>/api/2.0/app/firewall/datacenter-21/config?list=config&rulesType=LAYER3

Get configuration of only default precedence layer 3 firewall rules:

GET https://<vsm-ip>/api/2.0/app/firewall/datacenter-21/config?list=config&rulesType=LAYER3

Get configuration of only layer 2 firewall rules:

GET https://<vsm-ip>/api/2.0/app/firewall/datacenter-21/config?list=config&rulesType=LAYER2

Get configuration of only default precedence layer 2 firewall rules:

GET https://<vsm-ip>/api/2.0/app/firewall/datacenter-21/config?list=config&precedence=DEFAULT&rulesType=LAYER2

Get consolidated configurations for the context:

GET https://<vsm-ip>/api/2.0/app/firewall/datacenter-2/config?list=consolidated

Get a configuration history for a given context:

GET https://<vsm-ip>/api/2.0/app/firewall/datacenter-2/config?list=history&configID=241

---

Configuration is returned as XML.

**Example 7-4. Get complete firewall configuration for a datacenter**


---

GET https://<vsm-ip>/api/2.0/app/firewall/datacenter-21/config?list=config

Response Body:

```
<VshieldAppConfiguration>
  <firewallConfiguration generationNumber="1312802020950" timestamp="1312802020950" contextId="datacenter-21"
    provisioned="true">
    <layer3FirewallRule disabled="false" id="1510">
      <action>allow</action>
      <logged>false</logged>
      <notes>XYZ</notes>
      <source>
        <address exclude="true">
          <containerId>domain-c26</containerId>
        </address>
      </source>
      <destination>
        <address exclude="false">
          <containerId>domain-c26</containerId>
        </address>
        <application>
```

```

        <applicationSetId>application-24</applicationSetId>
      </application>
    </destination>
  </layer3FirewallRule>
  <layer3FirewallRule disabled="false" id="1509">
    <action>allow</action>
    <logged>>false</logged>
    <notes>XYZ</notes>
    <source>
      <address exclude="true">
        <containerId>domain-c26</containerId>
      </address>
    </source>
    <destination>
      <address exclude="false">
        <containerId>network-43</containerId>
      </address>
      <application>
        <applicationSetId>application-24</applicationSetId>
      </application>
    </destination>
  </layer3FirewallRule>
  <layer3FirewallRule disabled="false" id="1508">
    <action>allow</action>
    <logged>>false</logged>
    <notes></notes>
    <source>
      <address exclude="true">
        <containerId>domain-c26</containerId>
      </address>
    </source>
    <destination>
      <address exclude="false">
        <containerId>domain-c26</containerId>
      </address>
      <application>
        <applicationSetId>application-25</applicationSetId>
      </application>
    </destination>
  </layer3FirewallRule>
  <layer2FirewallRule disabled="false" id="1506">
    <action>allow</action>
    <logged>>false</logged>
    <notes></notes>
    <destination>
      <protocol>2303</protocol>
      <address exclude="false">
        <containerId>domain-c26</containerId>
      </address>
      <protocolName>BPQ</protocolName>
    </destination>
  </layer2FirewallRule>
  <layer2FirewallRule disabled="false" id="1502">
    <action>allow</action>
    <logged>>false</logged>
    <notes></notes>
    <source exclude="false">
      <containerId>datacenter-21</containerId>
    </source>
    <destination>
      <protocol>1535</protocol>
      <address exclude="true">
        <containerId>datacenter-21</containerId>
      </address>
      <protocolName>LLC</protocolName>
    </destination>
  </layer2FirewallRule>
  <layer2FirewallRule disabled="false" id="1505">

```

```

    <action>allow</action>
    <logged>>false</logged>
    <notes></notes>
    <source exclude="false">
        <containerId>datacenter-21</containerId>
    </source>
    <destination>
    <address exclude="false">
        <containerId>network-43</containerId>
    </address>
    </destination>
</layer2FirewallRule>
</firewallConfiguration>
</VshieldAppConfiguration>

```

---

**Example 7-5.** Get configuration of only default precedence firewall rules:

GET https://<vsm-ip>/api/2.0/app/firewall/datacenter-21/config?list=config&precedence=DEFAULT

Response Body:

```

<VshieldAppConfiguration>
  <firewallConfiguration generationNumber="1312802020950" timestamp="1312802020950" contextId="datacenter-21"
    provisioned="true">
    <layer3FirewallRule disabled="false" precedence="default" id="1340">
      <action>allow</action>
      <logged>>false</logged>
      <notes></notes>
      <source/>
      <destination/>
    </layer3FirewallRule>
    <layer2FirewallRule disabled="false" precedence="default" id="1341">
      <action>allow</action>
      <logged>>false</logged>
      <notes></notes>
      <destination/>
    </layer2FirewallRule>
  </firewallConfiguration>
</VshieldAppConfiguration>

```

---

**Example 7-6.** Get configuration of only Layer 3 firewall rules:

GET https://<vsm-ip>/api/2.0/app/firewall/datacenter-21/config?list=config&rulesType=LAYER3

Response Body:

```

<VshieldAppConfiguration>
  <firewallConfiguration generationNumber="1312802020950" timestamp="1312802020950" contextId="datacenter-21"
    provisioned="true">
    <layer3FirewallRule disabled="false" id="1510">
      <action>allow</action>
      <logged>>false</logged>
      <notes></notes>
      <source>
        <address exclude="true">
          <containerId>domain-c26</containerId>
        </address>
      </source>
      <destination>
        <address exclude="false">
          <containerId>domain-c26</containerId>
        </address>
        <application>
          <applicationSetId>application-24</applicationSetId>
        </application>
      </destination>
    </layer3FirewallRule>

```

```

<layer3FirewallRule disabled="false" id="1509">
  <action>allow</action>
  <logged>>false</logged>
  <notes></notes>
  <source/>
  <destination>
    <address exclude="false">
      <containerId>network-43</containerId>
    </address>
    <application>
      <applicationSetId>application-24</applicationSetId>
    </application>
  </destination>
</layer3FirewallRule>
<layer3FirewallRule disabled="false" id="1508">
  <action>allow</action>
  <logged>>false</logged>
  <notes></notes>
  <source>
    <address exclude="true">
      <containerId>domain-c26</containerId>
    </address>
  </source>
  <destination>
    <address exclude="false">
      <containerId>domain-c26</containerId>
    </address>
  </destination>
</layer3FirewallRule>
<layer3FirewallRule disabled="false" id="1507">
  <action>allow</action>
  <logged>>false</logged>
  <notes></notes>
  <source/>
  <destination>
    <address exclude="true">
      <containerId>domain-c26</containerId>
    </address>
    <application>
      <applicationSetId>application-20</applicationSetId>
    </application>
  </destination>
</layer3FirewallRule>
<layer3FirewallRule disabled="false" id="1504">
  <action>allow</action>
  <logged>>false</logged>
  <notes></notes>
  <source>
    <address exclude="false">
      <containerId>domain-c26</containerId>
    </address>
  </source>
  <destination>
    <address exclude="true">
      <containerId>domain-c26</containerId>
    </address>
    <application>
      <applicationSetId>application-24</applicationSetId>
    </application>
  </destination>
</layer3FirewallRule>
<layer3FirewallRule disabled="false" id="1503">
  <action>allow</action>
  <logged>>false</logged>
  <notes></notes>
  <source>
    <address exclude="false">
      <containerId>network-43</containerId>

```



```

        </address>
      </source>
      <destination>
        <address exclude="true">
          <containerId>network-43</containerId>
        </address>
      </destination>
    </layer3FirewallRule>
    <layer3FirewallRule disabled="false" precedence="default" id="1340">
      <action>allow</action>
      <logged>false</logged>
      <notes></notes>
      <source/>
      <destination/>
    </layer3FirewallRule>
  </firewallConfiguration>
</VshieldAppConfiguration>

```

---

### Example 7-7. Get configuration of only Layer 2 firewall rules:

GET https://<vsm-ip>/api/2.0/app/firewall/datacenter-21/config?list=config&rulesType=LAYER3

Response Body:

```

<VshieldAppConfiguration>
  <firewallConfiguration generationNumber="1312802020950" timestamp="1312802020950" contextId="datacenter-21"
    provisioned="true">
    <layer2FirewallRule disabled="false" id="1506">
      <action>allow</action>
      <logged>false</logged>
      <notes></notes>
      <destination>
        <protocol>2303</protocol>
        <address exclude="false">
          <containerId>domain-c26</containerId>
        </address>
        <protocolName>BPQ</protocolName>
      </destination>
    </layer2FirewallRule>
    <layer2FirewallRule disabled="false" id="1502">
      <action>allow</action>
      <logged>false</logged>
      <notes></notes>
      <source exclude="false">
        <containerId>datacenter-21</containerId>
      </source>
      <destination><protocol>1535</protocol>
        <address exclude="true">
          <containerId>datacenter-21</containerId>
        </address>
        <protocolName>LLC</protocolName>
      </destination>
    </layer2FirewallRule>
    <layer2FirewallRule disabled="false" id="1505">
      <action>allow</action>
      <logged>false</logged>
      <notes></notes>
      <source exclude="false">
        <containerId>datacenter-21</containerId>
      </source>
      <destination>
        <address exclude="false">
          <containerId>network-43</containerId>
        </address>
      </destination>
    </layer2FirewallRule>
    <layer2FirewallRule disabled="false" id="1501">
      <action>allow</action>

```

```

    <logged>>false</logged>
  </notes>
  <source exclude="false">
    <containerId>network-43</containerId>
  </source>
  <destination>
    <protocol>2303</protocol>
    <address exclude="true">
      <containerId>network-43</containerId>
    </address>
    <protocolName>BPQ</protocolName>
  </destination>
</layer2FirewallRule>
<layer2FirewallRule disabled="false" id="1500">
  <action>allow</action>
  <logged>>false</logged>
  <notes></notes>
  <destination>
    <protocol>24581</protocol>
    <protocolName>DIAG</protocolName>
  </destination>
</layer2FirewallRule>
<layer2FirewallRule disabled="false" id="1499">
  <action>allow</action>
  <logged>>false</logged>
  <notes></notes>
  <destination>
    <protocol>2054</protocol>
    <protocolName>ARP</protocolName>
  </destination>
</layer2FirewallRule>
<layer2FirewallRule disabled="false" precedence="default" id="1341">
  <action>allow</action>
  <logged>>false</logged>
  <notes></notes>
  <destination/>
</layer2FirewallRule>
</firewallConfiguration>
</VshieldAppConfiguration>

```

---

## Add a Firewall Rule

This section describes how you can add a firewall rule. The default rule should always be at the bottom of the rule chain.

- 1 Query the firewall rules for the context you want to configure. The context should be a namespace context. Namespace levels include datacenter, virtual wires, and port group with an independent namespace.

### Example 7-8. Query firewall configuration for datacenter

---

Example:

GET <https://<vsm-ip>/api/2.0/app/firewall/datacenter-28/config>

Response Body:

```

<VshieldAppConfiguration>
  <firewallConfiguration generationNumber="1347501121780" timestamp="1347501121780" contextId="datacenter-28"
    provisioned="true">
    <layer3FirewallRule id="1005" precedence="none" disabled="false">
      <name> </name>
      <action>allow</action>
      <logged>>false</logged>
      <notes></notes>
      <source>
        <address exclude="false">
          <containerId>datacenter-28</containerId>
        </address>

```

```

        <portInfo></portInfo>
    </source>
    <destination>
        <address exclude="false">
            <containerId>ipset-1</containerId>
        </address>
        <application>
            <applicationSetId>application-6</applicationSetId>
            <applicationSetId>application-7</applicationSetId>
            <applicationSetId>application-2</applicationSetId>
            <applicationSetId>application-4</applicationSetId>
        </application>
    </destination>
</layer3FirewallRule>
<layer3FirewallRule id="1004" precedence="default" disabled="false">
    <name>Default Rule</name>
    <action>allow</action>
    <logged>false</logged>
    <notes></notes>
</layer3FirewallRule>
<layer2FirewallRule id="1003" precedence="default" disabled="false">
    <name>Default Rule</name>
    <action>allow</action>
    <logged>false</logged>
    <notes></notes>
</layer2FirewallRule>
</firewallConfiguration>
</VshieldAppConfiguration>

```

- 2 Extract the XML from the response body in step 1 and add the desired rule to it with layer3FirewallRule id="0".
- 3 Extract the value of the generation number from the Etag header of the response in Step 1, and add it as the if-match header in the POST call.

For example, the generation number in the GET response for the firewall configuration of a datacenter is 1347501121780 (from [Example 7-8](#)). You must now specify the following header in the Request Body of a POST command for changing the datacenter firewall configuration:

If-Match: "1347501121780"

- 4 Pass the modified XML as the Request Body in a POST call.

#### Example 7-9. Add a Layer 3 rule (Test Rule 1) to allow TELNET traffic from IPSet-1 to datacenter

Example:

POST https://<vsm-ip>/api/2.0/app/firewall/datacenter-28/config  
 --header 'Content-Type:text/xml' --header 'if-match:"1347501121780"'

Request Body:

```

<VshieldAppConfiguration>
  <firewallConfiguration provisioned="true" contextId="datacenter-28" timestamp="1347501121780"
    generationNumber="1347501121780">
    <layer3FirewallRule id="1005" precedence="none" disabled="false">
      <name></name>
      <action>allow</action>
      <logged>false</logged>
      <notes></notes>
      <source>
        <address exclude="false">
          <containerId>datacenter-28</containerId>
        </address>
        <portInfo></portInfo>
      </source>
      <destination>
        <address exclude="false">

```

```

        <containerId>ipset-1</containerId>
    </address>
    <application>
        <applicationSetId>application-6</applicationSetId>
        <applicationSetId>application-7</applicationSetId>
        <applicationSetId>application-2</applicationSetId>
        <applicationSetId>application-4</applicationSetId>
    </application>
</destination>
</layer3FirewallRule>
<layer3FirewallRule id="0" precedence="none" disabled="false">
    <name>Test Rule1</name>
    <action>allow</action>
    <logged>false</logged>
    <notes></notes>
    <source>
        <address exclude="false">
            <containerId>ipset-1</containerId>
        </address>
        <portInfo></portInfo>
    </source>
    <destination>
        <address exclude="false">
            <containerId>datacenter-28</containerId>
        </address>
        <application>
            <applicationSetId>application-6</applicationSetId>
        </application>
    </destination>
</layer3FirewallRule>
<layer3FirewallRule id="1004" precedence="default" disabled="false">
    <name>Default Rule</name>
    <action>allow</action>
    <logged>false</logged>
    <notes></notes>
</layer3FirewallRule>
<layer2FirewallRule id="1003" precedence="default" disabled="false">
    <name>Default Rule</name>
    <action>allow</action>
    <logged>false</logged>
    <notes></notes>
</layer2FirewallRule>
</firewallConfiguration>
</VshieldAppConfiguration>

```

---

The response of the POST command returns the Rule ID for the new rule.

## Modify a Firewall Rule

This section describes how you can modify a firewall rule. The default rule should always be at the bottom of the rule chain.

- 1 Query the firewall rules for the context you want to modify. The context should be a namespace context. Namespace levels include datacenter, virtual wires, and port group with an independent namespace.

### Example 7-10. Query firewall configuration for datacenter

---

Example:

GET https://<vsm-ip>/api/2.0/app/firewall/datacenter-28/config

Response Body:

```

<VshieldAppConfiguration>
  <firewallConfiguration generationNumber="1347501121980" timestamp="1447501121780" contextId="datacenter-28"
    provisioned="true">
    ...
  </firewallConfiguration>

```

<VshieldAppConfiguration>

- 2 Extract the XML from the response body in step 1 and make the desired modifications.
- 3 Extract the value of the generation number from the Etag header of the response in Step 1, and add it as the if-match header in the POST call.

For example, the generation number in the GET response for the firewall configuration of a datacenter is 1347501121980 (from [Example 7-10](#)). You must now specify the following header in the Request Body of a POST command for changing the datacenter firewall configuration:

If-Match: "1347501121980"

- 4 Pass the modified XML as the Request Body in a POST call.

### Example 7-11. Modify Test Rule 1 to include LDAP

Example:

POST https://<vsm-ip>/api/2.0/app/firewall/datacenter-28/config  
 --header 'Content-Type:text/xml' --header 'if-match:"1347501121980" '

Request Body:

```
<VshieldAppConfiguration>
  <firewallConfiguration provisioned="true" contextId="datacenter-28" timestamp="1447501121780"
    generationNumber="1347501121980">
    <layer3FirewallRule id="1005" precedence="none" disabled="false">
      <name></name>
      <action>allow</action>
      <logged>>false</logged>
      <notes></notes>
      <source>
        <address exclude="false">
          <containerId>datacenter-28</containerId>
        </address>
        <portInfo></portInfo>
      </source>
      <destination>
        <address exclude="false">
          <containerId>ipset-1</containerId>
        </address>
        <application>
          <applicationSetId>application-6</applicationSetId>
          <applicationSetId>application-7</applicationSetId>
          <applicationSetId>application-2</applicationSetId>
          <applicationSetId>application-4</applicationSetId>
        </application>
      </destination>
    </layer3FirewallRule>
    <layer3FirewallRule id="1039" precedence="none" disabled="false">
      <name>Test Rule1</name>
      <action>allow</action>
      <logged>>false</logged>
      <notes></notes>
      <source>
        <address exclude="false">
          <containerId>ipset-1</containerId>
        </address>
        <portInfo></portInfo>
      </source>
      <destination>
        <address exclude="false">
          <containerId>datacenter-28</containerId>
        </address>
        <application>
          <applicationSetId>application-6</applicationSetId>
          <applicationSetId>application-7</applicationSetId>
        </application>
      </destination>
    </layer3FirewallRule>
  </firewallConfiguration>
</VshieldAppConfiguration>
```

```

        </destination>
      </layer3FirewallRule>
      <layer3FirewallRule id="1004" precedence="default" disabled="false">
        <name>Default Rule</name>
        <action>allow</action>
        <logged>>false</logged>
        <notes></notes>
      </layer3FirewallRule>
      <layer2FirewallRule id="1003" precedence="default" disabled="false">
        <name>Default Rule</name>
        <action>allow</action>
        <logged>>false</logged>
        <notes></notes>
      </layer2FirewallRule>
    </firewallConfiguration>
  </VshieldAppConfiguration>

```

---

## Delete a Firewall Rule

This section describes how you can delete a firewall rule. The default rule should always be at the bottom of the rule chain.

- 1 Query the firewall rules for the context. The context should be a namespace context. Namespace levels include datacenter, virtual wires, and port group with an independent namespace.

### Example 7-12. Query firewall configuration for datacenter

---

Example:

GET https://<vsm-ip>/api/2.0/app/firewall/datacenter-28/config

Response Body:

```

<VshieldAppConfiguration>
  <firewallConfiguration generationNumber="1347501121990" timestamp="1449501121780" contextId="datacenter-28"
    provisioned="true">
    ...
  </firewallConfiguration>
</VshieldAppConfiguration>

```

---

- 2 Extract the XML from the response body in step 1 and delete the desired rule.
- 3 Extract the value of the generation number from the Etag header of the response in Step 1, and add it as the if-match header in the POST call.

For example, the generation number in the GET response for the firewall configuration of a datacenter is 1347501121990 (from [Example 7-12](#)). You must now specify the following header in the Request Body of a POST command for changing the datacenter firewall configuration:

If-Match: "1347501121990"

- 4 Pass the modified XML as the Request Body in a POST call.

**IMPORTANT** You must specify the complete configuration in the POST call.

### Example 7-13. Delete Test Rule 1

---

Example:

POST https://<vsm-ip>/api/2.0/app/firewall/datacenter-28/config  
 --header 'Content-Type:text/xml' --header 'if-match:"1347501121990"'

Request Body:

```

<VshieldAppConfiguration>
  <firewallConfiguration provisioned="true" contextId="datacenter-28" timestamp="1449501121780"
    generationNumber="1347501121990">
    <layer3FirewallRule id="1005" precedence="none" disabled="false">
      <name></name>
    </layer3FirewallRule>
  </firewallConfiguration>
</VshieldAppConfiguration>

```

```

<action>allow</action>
<logged>>false</logged>
<notes></notes>
<source>
  <address exclude="false">
    <containerId>datacenter-28</containerId>
  </address>
  <portInfo></portInfo>
</source>
<destination>
  <address exclude="false">
    <containerId>ipset-1</containerId>
  </address>
  <application>
    <applicationSetId>application-6</applicationSetId>
    <applicationSetId>application-7</applicationSetId>
    <applicationSetId>application-2</applicationSetId>
    <applicationSetId>application-4</applicationSetId>
  </application>
</destination>
</layer3FirewallRule>
<layer3FirewallRule id="1004" precedence="default" disabled="false">
  <name>Default Rule</name>
  <action>allow</action>
  <logged>>false</logged>
  <notes></notes>
</layer3FirewallRule>
<layer2FirewallRule id="1003" precedence="default" disabled="false">
  <name>Default Rule</name>
  <action>allow</action>
  <logged>>false</logged>
  <notes></notes>
</layer2FirewallRule>
</firewallConfiguration>
</VshieldAppConfiguration>

```

---

## Revert to Default Firewall Configuration

You can revert the firewall configuration for the node to its default by deleting all rules that were created for the specified context ID, including default rules. For a datacenter or IP namespace, a fresh set of default rules are substituted.

**Example 7-14.** Delete firewall configuration and revert to default

---

Example:

DELETE <https://<vsm-ip>/api/2.0/app/firewall/<contextID>/config>

---

## Configuring Fail-Safe Mode for vShield App Firewall

By default, failure or unavailability of the vShield App appliance results in traffic being blocked (fail close). You can change this to allow traffic (fail open).

### Configure Fail-Safe Mode for vShield App Firewall

**Example 7-15.** Configure fail-safe mode

---

Example:

PUT <https://<vsm-ip>/api/2.1/app/failsafemode>

Request Body

```

<VshieldAppConfiguration>
  <failsafeConfiguration>
    <failsafemode>FAIL_OPEN</failsafemode>
  </failsafeConfiguration>
</VshieldAppConfiguration>

```

---

## Query Fail-Safe Mode Configuration for vShield App Firewall

**Example 7-16.** Get fail-safe mode configuration

---

Example:

GET https://<vsm-ip>/api/2.1/app/failsafemode

---

## Working with SpoofGuard

It is possible for a guest operating system to spoof its IP address so that VMware Tools would misreport it to vCenter Server. The SpoofGuard feature allows the datacenter administrator to certify and authorize reported IP addresses, and if necessary, alter them. This is done by checking the IP address against the virtual machine's MAC address, which comes from the VMX and cannot be spoofed.

The SpoofGuard feature is orthogonal to firewall rules. SpoofGuard blocks traffic if it thinks the IP is spoofed, whether or not firewall rules say to block.

## Get SpoofGuard Settings at Context Level

You can retrieve SpoofGuard settings for the specified datacenter, VXLAN virtual wire, or port group with independent namespace.

**Example 7-17.** Get SpoofGuard settings

---

Example:

GET https://<vsm-ip>/api/2.0/spoofguard/setting/<datacenterID>|<virtualWireID>|  
 <portGroupwithIndependentNamespace>

Response Body:

```

<?xml version="1.0" encoding="UTF-8"?>
<spoofguardsetting>
  <id>spoofguard-2</id>
  <scopeId>datacenter-21</scopeId>
  <operationMode>DISABLE</operationMode>
</spoofguardsetting>

```

---

## Replace SpoofGuard Settings

You can change the SpoofGuard settings.

**Example 7-18.** Change SpoofGuard settings

---

Example:

POST https://<vsm-ip>/api/2.0/spoofguard/setting/<datacenterID>|<virtualWireID>|  
 <portGroupAsIndependentNamespace>

Request Body:

```

<?xml version="1.0" encoding="UTF-8"?>
<spoofguardsetting>
  <scopeId>datacenter-21</scopeId>

```



```
<operationMode>DISABLE</operationMode>
</spoofiguardsetting>
```

---

Spoof guard setting is defined with datacenter-21. Status can be enabled or disabled. Mode can be trustOnFirstUse or manual.

## Get SpoofGuard IP Settings

You can retrieve a list of SpoofGuard settings.

### Example 7-19. Get SpoofGuard IP settings

---

Example:

```
GET https://<vsm-ip>/api/2.0/services/spoofguard/<contextID>?list=ACTIVE|INACTIVE|PUBLISHED|
UNPUBLISHED|DUPLICATE
```

Response Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<list>
  <spoofguard>
    <revision>0</revision>
    <inheritanceAllowed>>false</inheritanceAllowed>
    <vnicId>50204903-f1c9-0e97-e222-4b96f87ec7fe.000</vnicId>
    <approvedIpAddress>
      <string>10.24.123.129</string>
    </approvedIpAddress>
    <approvedMacAddress>00:50:56:be:00:06</approvedMacAddress>
    <approvedBy>system_user</approvedBy>
    <approvedOn>2011-10-28 16:12:20.0</approvedOn>
    <publishedIpAddress>
      <string>10.24.123.129</string>
    </publishedIpAddress>
    <publishedMacAddress>00:50:56:be:00:06</publishedMacAddress>
    <publishedBy>system_user</publishedBy>
    <publishedOn>2011-10-28 16:12:20.0</publishedOn>
    <reviewRequired>>false</reviewRequired>
    <duplicateCount>0</duplicateCount>
    <state>0</state>
  </spoofguard>
  <spoofguard>
    <spoofguard>
  </list>
```

---

Where contextID can be the ID of the datacenter, VXLAN virtual wire, or port group marked as namespace.

## Change SpoofGuard IP Settings

You can change the IP SpoofGuard settings for the specified context.

### Example 7-20. Save SpoofGuard IP settings

---

Example:

```
POST https://<vsm-ip>/api/2.0/spoofGuard/<contextID>?action=approve|delete|publish|saveApproved
```

---

An XML representation of VnicIdList is expected in the message body for delete and approve actions. If the action is publish then no message body is required. If the action is saveApproved then an XML representation of VnicInfo is expected.

## Working with Namespaces

A vShield namespace is a set of vNICs that share a common IP address domain. They do not have overlapping IP addresses, so they are reachable all-at-once by simple routing or switching. There is no NAT between them. Any IP address in the namespace refers to the same vNIC regardless of where you look at it from within the IP address domain.

A datacenter (as managed by vCenter Server) stores a list of vShield namespaces. The namespace itself can specify a network name as an object ID, or it can contain a list of IP addresses.

### Add Namespace in a Datacenter

You can define a new vShield namespace in the datacenter specified by <datacenter-id>.

---

#### Example 7-21. Add namespace in a datacenter

---

Request:

POST https://<vsm-ip>/api/2.0/namespace/datacenter/<datacenter-id>

Request Body:

```
<VshieldConfiguration xmlns="vmware.vshield.global.20.namespace">
  <namespace type="PORTGROUP" id="0">
    <namespacePortGroup>
      <id>network-184</id>
    </namespacePortGroup>
  </namespace>
</VshieldConfiguration>
```

---

In the request, <namespace-id> specifies the vShield namespace name.

In the example request body, the namespace is defined as being synonymous with object network-184.

### Get Namespace Details

You can retrieve details about a previously added vShield namespace.

---

#### Example 7-22. Get namespace details

---

Request:

GET https://<vsm-ip>/api/2.0/namespace/datacenter/<datacenter-id>/<namespace-id>

---

### Delete a Namespace

You can delete a previously added vShield namespace designated by <namespace-id>.

---

#### Example 7-23. Delete namespace

---

Request:

DELETE https://<vsm-ip>/api/2.0/namespace/datacenter/<datacenter-id>/<namespace-id>

---

### Show Namespaces in a Datacenter

You can retrieve a list of all vShield namespaces in the datacenter specified by <datacenter-id>.

---

#### Example 7-24. Get datacenter namespaces

---

Example:

GET https://<vsm-ip>/api/2.0/namespace/datacenter/datacenterID?list=candidate|configured

where candidate displays the list of candidate portgroups which can be marked as separate namespace and configured returns a list of configured namespace in the datacenter.

## Getting Flow Statistic Details

You can retrieve a detailed view of the traffic on your virtual network that passed through a vShield App.

### Get Flow Statistics

You can retrieve flow statistics for a datacenter, port group, virtual machine, or vNIC.

#### Example 7-25. Retrieve flow statistics

Example:

GET https://<vsm-ip>/api/2.1/app/flow/flowstats?contextId=datacenter-21&flowType=TCP\_UDP  
&startTime=0&endTime=1320917094000&startIndex=0&pageSize=2

```
<FlowStatsPage>
  <pagingInfo>
    <contextId>datacenter-2538</contextId>
    <flowType>TCP_UDP</flowType>
    <startTime>1327405883000</startTime>
    <endTime>1327482600000</endTime>
    <totalCount>817</totalCount>
    <startIndex>0</startIndex>
    <pageSize>2</pageSize>
  </pagingInfo>
  <flowStatsTcpUdp>
    <startTime>1327405883000</startTime>
    <endTime>1327446000000</endTime>
    <ruleId>1001</ruleId>
    <blocked>0</blocked>
    <protocol>5</protocol>
    <direction>1</direction>
    <sessions>1449</sessions>
    <sourcePackets>1449</sourcePackets>
    <destinationPackets>0</destinationPackets>
    <sourceBytes>227493</sourceBytes>
    <destinationBytes>0</destinationBytes>
    <networkId>network-2553</networkId>
    <sourceIp>10.112.199.174</sourceIp>
    <destinationIp>255.255.255.255</destinationIp>
    <destinationPort>17500</destinationPort>
    <controlProtocol></controlProtocol>
    <controlSourceIp>0.0.0.0</controlSourceIp>
    <controlDestinationIp>0.0.0.0</controlDestinationIp>
    <controlDestinationPort>0</controlDestinationPort>
    <controlDirection>0</controlDirection>
  </flowStatsTcpUdp>
  <flowStatsTcpUdp>
    <startTime>1327405883000</startTime>
    <endTime>1327446000000</endTime>
    <ruleId>1001</ruleId>
    <blocked>0</blocked>
    <protocol>5</protocol>
    <direction>1</direction>
    <sessions>69</sessions>
    <sourcePackets>69</sourcePackets>
    <destinationPackets>0</destinationPackets>
    <sourceBytes>17832</sourceBytes>
    <destinationBytes>0</destinationBytes>
    <networkId>network-2553</networkId>
```

```

    <sourceIp>10.112.199.13</sourceIp>
    <destinationIp>10.112.199.255</destinationIp>
    <destinationPort>138</destinationPort>
    <controlProtocol></controlProtocol>
    <controlSourceIp>0.0.0.0</controlSourceIp>
    <controlDestinationIp>0.0.0.0</controlDestinationIp>
    <controlDestinationPort>0</controlDestinationPort>
    <controlDirection>0</controlDirection>
  </flowStatsTcpUdp>
</FlowStatsPage>

```

Query parameters are described in the table below.

**Table 7-1.** Query parameters for retrieving flow statistics call

Parameter	Description
flowStats	Type of the flow to be retrieved. Possible values are TCP_UDP, LAYER2, and LAYER3
contextId	vc-moref-id of the datacenter, port group, virtual machine, or UUID of the vNIC for which traffic flow is to be retrieved.
startTime	Flows with start time greater than the specified time are to be retrieved.
endTime	Flows with start time lower than the specified time are to be retrieved.
startIndex	Optional parameter that specifies the starting point for retrieving the flows. If this parameter is not specified, flows are retrieved from the beginning.
pageSize	Optional parameter that limits the maximum number of entries returned by the API. The default value for this parameter is 256 and the valid range is 1-1024.

**Table 7-2.** Response values for retrieving flow statistics call

Value	Description
startTime	Start time for current flow.
endTime	End time for current flow.
ruleId	rule Id for current flow.
blocked	Indicates whether traffic is blocked – 0:Flow allowed, 1:Flow blocked, 2:Flow blocked by Spoofguard.
protocol	protocol in flow – 0:TCP, 1:UDP, 2:ICMP.
direction	Direction of flow – 0:To virtual machine, 1:From virtual machine.
sessions	Number of sessions in current flow.
sourcePackets	Count of Packets from Source to Destination in current flow.
destinationPackets	Count of Packets from Destination to Source in current flow.
sourceBytes	Count of Bytes transferred from Source to Destination in current flow.
destinationBytes	Count of Bytes transferred from Destination to Source in current flow.
sourceIp	Source IP of current flow.
destinationIp	Destination IP of current flow.
sourceMac	Source Mac of current flow.
destinationMac	Destination Mac of current flow.
subtype	Identifies the sub type of current flow.
destinationPort	Port number of Destination for TCP/UDP traffic.
controlProtocol	Control protocol for dynamic TCP traffic.
controlSourceIp	Control source IP for dynamic TCP traffic.
controlDestinationIp	Control destination IP for dynamic TCP traffic.

**Table 7-2.** Response values for retrieving flow statistics call

Value	Description
controlDestinationPort	Control destination port for dynamic TCP traffic.
controlDirection	Control direction for dynamic TCP traffic – 0: Source->Destination, 1:Destination->Source.

## Get Flow Meta-Data

You can retrieve the following information for each flow type:

- minimum stats time
- maximum end time
- total flow count

### Example 7-26. Get flow meta-data for flow type

Example:

```
GET https://<vsm-ip>/api/2.1/app/flow/flowstats?contextId=datacenter-2538\&flowType=TCP_UDP\
&startTime=1327405883000\&endTime=1327482600000\&startIndex=0\&pageSize=2
```

Response Body:

```
<FlowStatsPage>
  <pagingInfo>
    <contextId>datacenter-2538</contextId>
    <flowType>TCP_UDP</flowType>
    <startTime>1327405883000</startTime>
    <endTime>1327482600000</endTime>
    <totalCount>817</totalCount>
    <startIndex>0</startIndex>
    <pageSize>2</pageSize>
  </pagingInfo>
  <flowStatsTcpUdp>
    <startTime>1327405883000</startTime>
    <endTime>1327446000000</endTime>
    <ruleId>1001</ruleId>
    <blocked>0</blocked>
    <protocol>5</protocol>
    <direction>1</direction>
    <sessions>1449</sessions>
    <sourcePackets>1449</sourcePackets>
    <destinationPackets>0</destinationPackets>
    <sourceBytes>227493</sourceBytes>
    <destinationBytes>0</destinationBytes>
    <networkId>network-2553</networkId>
    <sourceIp>10.112.199.174</sourceIp>
    <destinationIp>255.255.255.255</destinationIp>
    <destinationPort>17500</destinationPort>
    <controlProtocol></controlProtocol>
    <controlSourceIp>0.0.0.0</controlSourceIp>
    <controlDestinationIp>0.0.0.0</controlDestinationIp>
    <controlDestinationPort>0</controlDestinationPort>
    <controlDirection>0</controlDirection>
  </flowStatsTcpUdp>
  <flowStatsTcpUdp>
    <startTime>1327405883000</startTime>
    <endTime>1327446000000</endTime>
    <ruleId>1001</ruleId>
    <blocked>0</blocked>
    <protocol>5</protocol>
    <direction>1</direction>
    <sessions>69</sessions>
    <sourcePackets>69</sourcePackets>
    <destinationPackets>0</destinationPackets>
```

```

    <sourceBytes>17832</sourceBytes>
    <destinationBytes>0</destinationBytes>
    <networkId>network-2553</networkId>
    <sourceIp>10.112.199.13</sourceIp>
    <destinationIp>10.112.199.255</destinationIp>
    <destinationPort>138</destinationPort>
    <controlProtocol></controlProtocol>
    <controlSourceIp>0.0.0.0</controlSourceIp>
    <controlDestinationIp>0.0.0.0</controlDestinationIp>
    <controlDestinationPort>0</controlDestinationPort>
    <controlDirection>0</controlDirection>
  </flowStatsTcpUdp>
</FlowStatsPage>

```

---

## Configure Addresses to be Ignored by Flow Parser

Configures port and source/destination IP and MAC addresses to be ignored by the flow parser.

**Example 7-27.** Configure addresses to be ignored

---

Example:

POST https://<vsm-ip>/api/2.1/app/flow/config

---

## Query Addresses Ignored by Flow Parser

Retrieves port and source/destination IP and MAC addresses ignored by the flow parser.

**Example 7-28.** Query ignored addresses

---

Example:

GET https://<vsm-ip>/api/2.1/app/flow/config

---

## Excluding Virtual Machines from vShield App Protection

You can exclude a set of virtual machines from vShield App protection. This exclusion list is applied across all vShield App installations within the specified vShield Manager. If a virtual machine has multiple vNICs, all of them are excluded from protection.

### Add a Virtual Machine to the Exclusion List

You can add a virtual machine to the exclusion list.

**Example 7-29.** Add a virtual machine to exclusion list

---

Example:

PUT https://<vsm-ip>/api/2.1/app/excludelist/<memberId>

---

Where memberId is the vc-moref-id of a virtual machine.

### Get Virtual Machine Exclusion List

You can retrieve the set of virtual machines in the exclusion list.

**Example 7-30.** Get exclusion list

---

Example:

GET https://<vsm-ip>/api/2.1/app/excludelist/

Response Body:

```
<VshieldAppConfiguration>
  <excludeListConfiguration>
    <objectId>excludeList-1</objectId>
    <type>
      <typeName>ExcludeList</typeName>
    </type>
    <revision>1</revision>
    <objectTypeName>ExcludeList</objectTypeName>
    <excludeMember>
      <member>
        <objectId>vm-2371</objectId>
        <type>
          <typeName>VirtualMachine</typeName>
        </type>
        <name>VC-Win2k3</name>
        <revision>2</revision>
        <objectTypeName>VirtualMachine</objectTypeName>
        <scope>
          <id>domain-c731</id>
          <objectTypeName>ClusterComputeResource</objectTypeName>
          <name>Database-CL</name>
        </scope>
      </member>
    </excludeMember>
  </excludeListConfiguration>
</VshieldAppConfiguration>
```

---

## Delete a Virtual Machine from Exclusion List

You can delete a virtual machines from the exclusion list.

**Example 7-31.** Delete virtual machine from exclusion list

---

Example:

DELETE https://<vsm-ip>/api/2.1/app/excludelist/<memberID>

---

Where memberId is the vc-moref-id of a virtual machine.

## Configuring Syslog Service for a vShield App

You can configure all vShield App instances to send system events to up to two syslog servers. All vShield App instances share the same syslog server configuration.

You can retrieve a list of syslog servers configured on the first vShield App instance that responds.

**Example 7-32.** Get the syslog server configuration for All vShield App instances

---

Request:

GET https://<vsm-ip>/api/1.0/zones/syslogServers

---

You can configure all vShield App instances connected to the vShield Manager to send events to the specified syslog servers.

**Example 7-33.** Post the syslog server configuration across all vShield App instances

---

Request:

---

POST https://<vsm-ip>/api/1.0/zones/syslogServers

---

You can delete the syslog server configuration across all vShield App instances connected to the vShield Manager.

**Example 7-34.** Delete the syslog server configuration across all vShield App instances

---

Request:

DELETE https://<vsm-ip>/api/1.0/zones/syslogServers

---

You can delete a syslog server across all vShield App instances connected to the vShield Manager.

**Example 7-35.** Delete a single syslog server by IP address from All vShield App instances

---

Request:

DELETE https://<vsm-ip>/api/1.0/zones/syslogServers/<ip\_of\_syslogServer>

---

## Synchronizing vShield App

You can force vShield App to synchronize with the last good configuration in the vShield Manager database.

**Example 7-36.** Force Sync vShield App

---

Request:

POST https://<vsm-ip>/api/1.0/zones/host-28/forceSync

---

## Querying vShield App Technical Support Log

You can generate and download the diagnostic log from a vShield App by host. You can then send the diagnostic log to technical support for assistance in troubleshooting an issue.

**Example 7-37.** Generate Tech Support Log File for a vShield App

---

Request:

GET https://<vsm-ip>/api/1.0/zones/<host-id>/techSupportLogs

Response Body:

```
<ZonesConfiguration>
  <TechSupportLogsTarFilePath>/tech_support_logs/vsz/vshield_zones_support_host-28_121311_065346GMT.log.gz</TechSupportLogsTarFilePath>
</ZonesConfiguration>
```

---

**Example 7-38.** Download Tech Support Log File for a vShield App

---

Request:

GET https://<vsm-ip>/<TechSupportLogsFilePath>

---

The technical support log is placed in a file, however the REST API has no provision for downloading it, and wget and curl do not have permission to download it, either. You can retrieve the log with vShield Manager by clicking **Settings & Reports > Configuration > Support > [Log Download] Initiate**.



## Querying vShield App Status

You can retrieve the state of a vShield App.

### Example 7-39. Query vShield App status

---

Request:

GET https://<vsm-ip>/api/2.0/app/firewall/<datacenterId>

Request Body:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<VshieldAppConfiguration>
  <datacenterState>
    <datacenterId>datacenter-21</datacenterId>
    <userId>admin</userId>
    <timestamp>0</timestamp>
    <status>backwardCompatibleReadyForSwitch</status>    <!-- Other possible states are Upgrading,
                                                             Backword_Compatible, Backword_Compatible_Ready_For_Switch, Migrating, Regular -->
  </datacenterState>
</VshieldAppConfiguration>
```

---

## Upgrading vShield App

You can upgrade vShield App.

### Example 7-40. Upgrade vShield App

---

Request:

POST https://<vsm-ip>/api/1.0/vshield/<host-id>/vsz

Request Body:

```
<VshieldConfiguration>
  <VszInstallParams>
    <DatastoreId>datastore-5131</DatastoreId>
    <ManagementPortSwitchId>network-5134</ManagementPortSwitchId>
    <MgmtInterface>
      <IpAddress>10.112.196.245</IpAddress>
      <NetworkMask>255.255.252.0</NetworkMask>
      <DefaultGw>10.112.199.253</DefaultGw>
    </MgmtInterface>
  </VszInstallParams>
  <InstallAction>upgrade</InstallAction>
</VshieldConfiguration>
```

---



# vShield Endpoint Management

---

A vShield Endpoint appliance delivers an introspection-based antivirus solution that uses the hypervisor to scan guest virtual machines from the outside with only a thin agent on each guest virtual machine.

This chapter includes the following topics:

- [“Overview of Solution Registration”](#) on page 195
- [“Registering a Solution with vShield Endpoint Service”](#) on page 195
- [“Querying Registration Status of vShield Endpoint”](#) on page 197
- [“Querying Activated Security Virtual Machines for a Solution”](#) on page 198
- [“Unregistering a Solution with vShield Endpoint”](#) on page 199
- [“Status Codes and Error Schema”](#) on page 200

---

**IMPORTANT** All vShield REST requests require authorization. See [“Using the vShield REST API”](#) on page 16 for details about basic authorization.

---

## Overview of Solution Registration

To register a third-party solution with vShield Endpoint, clients can use four REST calls to do the following:

- 1 Register the vendor.
- 2 Register one or more solutions.
- 3 Set the solution IP address and port (for all hosts).
- 4 Activate registered solutions per host.

**NOTE** Steps 1 through 3 need to be performed once per solution, while step 4 needs to be performed for each host.

To unregister a solution, clients essentially perform these steps in reverse:

- 5 Deactivate solutions per host.
- 6 Unset a solution’s IP address and port.
- 7 Unregister solutions.
- 8 Unregister the vendor.

To update registration information for a vendor or solution, clients must first unregister that entity and then reregister. The following sections detail the specific REST calls to perform registration and unregistration.

## Registering a Solution with vShield Endpoint Service

The APIs described in this section register a vendor, solutions, set network address, and activate solutions.

For a list of return status codes, see [“Return Status Codes”](#) on page 200.

## Register a Vendor

You can register the vendor of an antivirus solution.

### Example 8-1. Register a vendor

---

Request:

POST https://<vsm-ip>/api/2.0/endpointsecurity/registration

Request Body:

```
<VendorInfo>
  <id>vendor_id</id>
  <title>vendor_title</title>
  <description>vendor_description</description>
</VendorInfo>
```

---

In the request body, vendor\_id is the VMware-assigned ID for the vendor, while vendor\_title and vendor\_description are vendor provided strings.

## Register a Solution

You can register an antivirus solution.

### Example 8-2. Register a solution

---

Request:

POST https://<vsm-ip>/api/2.0/endpointsecurity/registration/<vendor\_id>

Request Body:

```
<SolutionInfo>
  <altitude>solution_altitude</altitude>
  <title>solution_title</title>
  <description>solution_description</description>
</SolutionInfo>
```

---

In the request, <vendor\_id> is the previously registered ID for the vendor.

In the request body, solution\_altitude is the VMware-assigned altitude for the solution, solution\_title and solution\_description are vendor provided strings. See [“Altitude of a Solution”](#) on page 196.

### Altitude of a Solution

Altitude is a number that VMware assigns to uniquely identify the solution. The altitude describes the type of solution and the order in which the solution receives events relative to other solutions on the same host.

## IP Address and Port for a Solution

You can set a solution’s IP address and port on the vNIC host.

### Example 8-3. Set IP address and port

---

Request:

POST https://<vsm-ip>/api/2.0/endpointsecurity/registration/<vendor\_id>/<altitude>/location

Request Body:

```
<LocationInfo>
  <ip>solution_ip_address</ip>
```

```
<port>solution_port</port>
</LocationInfo>
```

---

In the request, <vendor\_id> is the previously registered ID for the vendor, and <altitude> for the altitude.

In the request body, solution\_ip\_address is the solution's IPv4 address for the vNIC that is connected to the VMkernel port group (for example, 169.254.1.31). This address must be within the range of VMware-assigned IP addresses for the solution. The solution\_port is the port on which the solution accepts connections.

If you want to change the location of a solution, deactivate all security virtual machines, change the location, and then reactivate all security virtual machines.

## Activate a Solution

You can activate a solution that has been registered and located.

### Example 8-4. Activate solution

---

Request:

POST https://<vsm-ip>/api/2.0/endpointsecurity/activation/<vendor\_id>/<altitude>

Request Body:

```
<ActivationInfo>
  <moid>svm_moid</moid>
</ActivationInfo>
```

---

In the request, <vendor\_id> is the previously registered ID for the vendor, and <altitude> for the altitude.

In the request body, svm\_moid is the managed object ID of the activated solution's virtual machine.

## Querying Registration Status of vShield Endpoint

You can use the same URLs shown in the previous section with the GET method to retrieve vendor registration information, solution registration information, location information, and solution activation status.

### Get Vendor Registration

You can retrieve vendor registration information.

#### Example 8-5. Get list of all registered vendors

---

Request:

GET https://<vsm-ip>/api/2.0/endpointsecurity/registration/vendors

---

#### Example 8-6. Get vendor registration information

---

Request:

GET https://<vsm-ip>/api/2.0/endpointsecurity/registration/<vendor\_id>

---

### Get Solution Registration

You can retrieve solution registration information.

#### Example 8-7. Get all registered solutions for a vendor

---

Request:

---

```
GET https://<vsm-ip>/api/2.0/endpointsecurity/registration/<vendor_id>/solutions
```

---

### Example 8-8. Get solution registration information

---

Request:

```
GET https://<vsm-ip>/api/2.0/endpointsecurity/registration/<vendor_id>/<altitude>
```

---

## Get IP Address of a Solution

This call retrieves the IP address and port associated with a solution.

### Example 8-9. Get IP address and port of a solution

---

Request:

```
GET https://<vsm-ip>/api/2.0/endpointsecurity/registration/<vendor_id>/<altitude>/location
```

---

## Get Activation Status of a Solution

This call retrieves solution activation status, given the managed object reference <moid> of its virtual machine.

### Example 8-10. Get activation status of a solution

---

Request:

```
GET https://<vsm-ip>/api/2.0/endpointsecurity/activation/<vendor_id>/<altitude>/<moid>
```

---

Status can be false (not activated) or true (activated).

## Querying Activated Security Virtual Machines for a Solution

You can retrieve a list of activated security virtual machines for a solution, as well as the activation information for all activated security virtual machines on a host.

## Query Activated Security Virtual Machines

You can retrieve a list of activated security virtual machines for the specified solution.

### Example 8-11. Get activated security virtual machines

---

Request:

```
GET https://<vsm-ip>/api/2.0/endpointsecurity/activation/<vendor_id>/<solution_id>
```

Response Body:

```
<ActivatedSVMs>
  <ActivationInfo>
    <moid>vm-819</moid>
    <hostMoid>host-9</hostMoid>
    <vmName>VMWARE-Data Security-10.24.130.174</vmName>
    <hostName>10.24.130.174</hostName>
    <clusterName>Dev</clusterName>
    <dcName>dev</dcName>
    <vendorId>VMWARE</vendorId>
    <solutionId>6341068275337723904</solutionId>
  </ActivationInfo>
  ...
```

---

```
</ActivatedSVMs>
```

---

In the request, `vendor_id` is the VMware-assigned ID for the vendor, while `solution_id` is the solution ID.

## Query Activation Information

You can retrieve activation information for all activated security virtual machines on the specified host.

### Example 8-12. Get activation information

---

Request:

```
GET https://<vsm-ip>/api/2.0/endpointsecurity/activation?hostId=<hostID>
```

Response Body:

```
<ActivatedSVMs>
  <ActivationInfo>
    <moid>vm-819</moid>
    <hostMoid>host-9</hostMoid>
    <vmName>VMWARE-Data Security-10.24.130.174</vmName>
    <hostName>10.24.130.174</hostName>
    <clusterName>Dev</clusterName>
    <dcName>dev</dcName>
    <vendorId>VMWARE</vendorId>
    <solutionId>6341068275337723904</solutionId>
  </ActivationInfo>
  ...
</ActivatedSVMs>
```

---

## Unregistering a Solution with vShield Endpoint

You can use the same URIs shown in the first section with the DELETE method to unregister a vendor, unregister a solution, unset location information, or deactivate a solution.

### Unregister a Vendor

This call unregisters a vendor.

#### Example 8-13. Unregister a vendor

---

Request:

```
DELETE https://<vsm-ip>/api/2.0/endpointsecurity/registration/<vendor_id>
```

---

### Unregister a Solution

This call unregisters a solution.

#### Example 8-14. Unregister a vendor

---

Request:

```
DELETE https://<vsm-ip>/api/2.0/endpointsecurity/registration/<vendor_id>/<altitude>
```

---

### Unset IP Address

This call unsets a solution's IP address and port.

**Example 8-15. Unset IP address and port**

---

Request:

DELETE https://<vsm-ip>/api/2.0/endpointsecurity/registration/<vendor\_id>/<altitude>/location

---

**Deactivate a Solution**

This call deactivates a solution on a host.

**Example 8-16. Deactivate a solution**

---

Request:

DELETE https://<vsm-ip>/api/2.0/endpointsecurity/activation/<vendor\_id>/<altitude>/<moid>

---

**Status Codes and Error Schema**

This section lists various status codes returned from the REST API, and shows the error schema.

**Return Status Codes**

The 200 codes indicate success, the 400 codes indicate some failure, and the 600 codes are call specific.

- 200 OK operation successful
- 201 Created: Entity successfully altered.
- 400 Bad Request: Internal error codes. Please refer to the Error Schema for more details.
- 401 Unauthorized: Incorrect user name or password.
- 600 Unrecognized vendor ID.
- 601 Vendor is already registered.
- 602 Unrecognized altitude.
- 603 Solution is already registered.
- 604 Invalid IPv4 address.
- 605 Invalid port.
- 606 Port out of range.
- 607 Unrecognized moid.
- 608 Location information is already set.
- 609 Location not set.
- 612 Solutions still registered.
- 613 Solution location information still set.
- 614 Solution still activated.
- 615 Solution not activated.
- 616 Solution is already activated.
- 617 IP:Port already in use.
- 618 Bad solution ID.
- 619 vShield Endpoint is not licensed.
- 620 Internal error.

**Error Schema**

Here is the XML schema for vShield Endpoint registration errors.

```
<?xml version="1.0" encoding="UTF-8"?><xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
    elementFormDefault="qualified">
```



```
<xs:element name="Error">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="code" type="xs:unsignedInt"/>
      <xs:element name="description" type="xs:string"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
```



# vShield Data Security Configuration

vShield Data Security provides visibility into sensitive data stored within your organization's virtualized and cloud environments. Based on the violations reported by vShield Data Security, you can ensure that sensitive data is adequately protected and assess compliance with regulations around the world.

This chapter includes the following topics:

- [“vShield Data Security User Roles”](#) on page 203
- [“Defining a Data Security Policy”](#) on page 204
- [“Saving and Publishing Policies”](#) on page 209
- [“Data Security Scanning”](#) on page 210
- [“Querying Scan Results”](#) on page 211
- [“Querying Violation Details”](#) on page 215

To begin using vShield Data Security, you create a policy that defines the regulations that apply to data security in your organization and specifies the areas of your environment and files to be scanned. When you start a Data Security scan, vShield analyzes the data on the virtual machines in your vSphere inventory and reports the number of violations detected and the files that violated your policy.

After you analyze the results of the scan, you can edit your policy as required. When you edit a policy, you must enable it by publishing the changes.

Note that you cannot install vShield Data Security using a REST API. For information on installing vShield Data Security, see the *vShield Quick Start Guide*.

To deploy vShield Data Security, you must install the latest version of VMware Tools on each virtual machine that you want to scan. This installs a Thin Agent, which allows the SVM to scan the virtual machines.

## vShield Data Security User Roles

A user's role determines the actions that the user can perform. A user can only have one role. You cannot add a role to a user, or remove an assigned role from a user, but you can change the assigned role for a user.

**Table 9-1.** vShield Data Security User Roles

Role	Actions Allowed
Enterprise administrator	All vShield operations and security.
vShield administrator	vShield operations only: for example, install virtual appliances, and configure port groups.
Security administrator	Create and publish policies, view violation reports. Cannot start or stop data security scans.
Auditor	View configured policies and violation reports. Read-only.

## Defining a Data Security Policy

In order to detect sensitive data in your environment, you must create a data security policy. You must be a Security Administrator to create policies.

To define a policy, you must specify the following:

- Regulations

A regulation is a data privacy law for protecting PCI (Payment Card Industry), PHI (Protected Health Information) and PII (Personally Identifiable Information) information. You can select the regulations that your company needs to comply to. When you run a scan, vShield Data Security identifies data that violates the regulations in your policy, and is hence sensitive for your organization.

- Participating areas

By default, your entire vCenter inventory is scanned. To scan a subset of your inventory, you can specify the security groups that you want to include or exclude.

- File filters

You can create filters to limit the data being scanned and exclude the file types unlikely to contain sensitive data from the scan.

In the data security APIs, dlp in the pathname stands for data loss prevention (DLP).

## Query Regulations

You can retrieve the list of available regulations for a policy. The output includes regulation IDs and the embedded classifications for each regulation.

### Example 9-1. Get all SDD policy regulations

Request:

GET https://<vsm-ip>/api/2.0/dlp/regulation

Response:

```
<set>
  <Regulation>
    <id>66</id>      ──────────▶ Regulation ID
    <name>California AB-1298</name>
    <description>Identifies documents and transmissions that contain protected health information (ePHI) and personally
                                identifiable information (PII) as regulated by California AB-1298 (Civil Code 56, 1785 and 1798)...
  <classifications>
    <Classification>
      <id>10</id>
      <name>Credit Card Track Data</name>
      <providerName>Credit Card Track Data</providerName>
      <description>Credit Card Track Data</description>
      <customizable>>false</customizable>
    </Classification>
    ...
```

## Enable a Regulation

You can enable one or more regulations by putting the regulation IDs into the policy. You can get the appropriate regulation IDs from the output of the retrieve regulations API (see [Example 9-1](#)). In the example request body, regulation 66 is California AB-1298, and regulations 67 and 68 originate elsewhere.

### Example 9-2. Enable a regulation

Request:

PUT https://<vsm-ip>/api/2.0/dlp/policy/regulations

Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<set>
  <long>66</long>
  <long>67</long>
  <long>68</long>
</set>
```

---

## Query Classification Value

You can retrieve the classification values associated with regulations that monitor Group Insurance Numbers, Health Plan Beneficiary Numbers, Medical Record Numbers, or Patient Identification Numbers. The output includes the classification ID.

**Example 9-3.** Get all classification values associated with customizable classifications

---

Request:

GET https://<vsm-ip>/api/2.0/dlp/classificationvalue

---

## Configure a Customized Regex as a Classification Value

You can configure a ClassificationValue with a customized regex that must be matched during violation inspection. You must include the appropriate classification ID, which you can get from the output of the retrieve classification value API.

**Example 9-4.** Configure a customized regex as a classification value

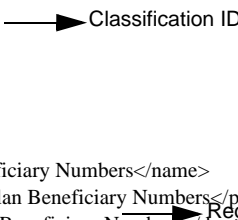
---

Request:

PUT https://<vsm-ip>/api/2.0/dlp/policy/classificationvalues

Authorization: Basic YWRtaW46ZGVmYXVsdA==

```
<set>
  <ClassificationValue>
    <id>3</id>
    <classification>
      <id>15</id>
      <name>Health Plan Beneficiary Numbers</name>
      <providerName>Health Plan Beneficiary Numbers</providerName>
      <description>Health Plan Beneficiary Numbers</description>
      <customizable>true</customizable>
    </classification>
    <value>PATNUM-[0-9]{10}</value>
  </ClassificationValue>
</set>
```



---

## View the List of Excludable Areas

You can retrieve the list of datacenters, clusters, and resource pools in your inventory to help you determine the areas you might want to exclude from policy inspection.

**Example 9-5.** View the list of excludable areas

---

Request:

GET https://<vsm-ip>/api/2.0/dlp/excludableareas

Response:

```
<set>
  <EnhancedInfo>
    <objectId>datacenter-2</objectId>
    <name>jdoe</name>
    <revision>32</revision>
    <objectTypeName>Datacenter</objectTypeName>
    <ownerName>VMware</ownerName>
  </EnhancedInfo>
  <EnhancedInfo>
    <objectId>datacenter-94</objectId>
    <name>jdoe</name>
    <revision>32</revision>
    <objectTypeName>Datacenter</objectTypeName>
    <ownerName>VMware</ownerName>
  </EnhancedInfo>
  <EnhancedInfo>
    <objectId>resgroup-3725</objectId>
    <name>ResourcePool1</name>
    <revision>2</revision>
    <objectTypeName>ResourcePool</objectTypeName>
    <ownerName>jdoe</ownerName>
  </EnhancedInfo>
  <EnhancedInfo>
    <objectId>domain-c2720</objectId>
    <name>Cluster1</name>
    <revision>17</revision>
    <objectTypeName>ClusterComputeResource</objectTypeName>
    <ownerName>jdoe</ownerName>
  </EnhancedInfo>
  <EnhancedInfo>
    <objectId>resgroup-3726</objectId>
    <name>ResourcePool2</name>
    <revision>1</revision>
    <objectTypeName>ResourcePool</objectTypeName>
    <ownerName>jdoe</ownerName>
  </EnhancedInfo>
</set>
```

---

## Exclude Areas from Policy Inspection

This API is deprecated as of vShield 5.0.1. Instead, use the API for excluding security groups from a scan. For more information, see [Example 9-8, “Exclude a security group from the scan,”](#) on page 207.

You can exclude one or more datacenters, resource pools or clusters from policy inspection by including the object ID of each area to exclude. You can get the object ID from the output of the View the list of excludable areas API (see [Example 9-5](#)).

### Example 9-6. Exclude areas from policy inspection

---

Request:

PUT https://<vsm-ip>/api/2.0/dlp/policy/excludedareas

Authorization: Basic YWRtaW46ZGVmYXVsdA==

```
<set>
  <string>datacenter-3720</string>
</set>
```

---

## Specify Security Groups to be Scanned

To scan a subset of your inventory, you can specify the security groups that you want to include or exclude in the data security scan.

### Example 9-7. Include a security group in the scan

---

Request:

PUT https://<vsm-ip>/api/2.0/dlp/policy/includedsecuritygroups/

Request Body:

```
<set>
  <string>securitygroup-id-1</string>
  <string>securitygroup-id-1</string>
</set>
```

---

### Example 9-8. Exclude a security group from the scan

---

Request:

PUT https://<vsm-ip>/api/2.0/dlp/policy/excludedsecuritygroups/

Request Body:

```
<set>
  <string>securitygroup-id-1</string>
  <string>securitygroup-id-1</string>
</set>
```

---

## Query Security Groups Being Scanned

You can retrieve the security groups that have been included or excluded from data security scans.

### Example 9-9. Get included security groups

---

Request:

GET https://<vsm-ip>/api/2.0/dlp/policy/includedsecuritygroups

Response:

```
<set>
  <basicinfo>
    <objectId>securitygroup-1</objectId>
    <type>
      <typeName>SecurityGroup</typeName>
    </type>
    <name>included</name>
    <revision>2</revision>
    <objectTypeName>SecurityGroup</objectTypeName>
    <scope>
      <id>datacenter-2</id>
      <objectTypeName>Datacenter</objectTypeName>
      <name>jkiryakoza</name>
    </scope>
  </basicinfo>
</set>
```

---

### Example 9-10. Get excluded security groups

---

Request:

GET https://<vsm-ip>/api/2.0/dlp/policy/excludedsecuritygroups/

Response:

```
<set>
  <basicinfo>
    <objectId>securitygroup-1</objectId>
    <type>
      <typeName>SecurityGroup</typeName>
    </type>
    <name>included</name>
    <revision>2</revision>
    <objectTypeName>SecurityGroup</objectTypeName>
    <scope>
      <id>datacenter-2</id>
      <objectTypeName>Datacenter</objectTypeName>
      <name>jkiryakoza</name>
    </scope>
  </basicinfo>
</set>
```

---

## Configure File Filters

You can restrict the files you want to scan based on size, last modified date, or file extensions.

The following file filters are available:

- `sizeLessThanBytes` – scan only files with a byte size less than the specified number.
- `lastModifiedBefore` – scan only files modified before the specified date. The date must be specified in GMT format (YYYY-MM-DD HH:MM:SS).
- `lastModifiedAfter` – scan only files modified after the specified date. The date must be specified in GMT format (YYYY-MM-DD HH:MM:SS).
- `extensionsIncluded` – Boolean value as in [Table 9-1](#).

**Table 9-2.** Included extensions parameter

Value of the <code>extensionsIncluded</code> parameter	Result
true followed by the extensions parameter containing one or more extensions	Only files with the specified extensions are scanned
false followed by the extensions parameter containing one or more extensions	All files are scanned except those with the specified extensions.

The `scanAllFiles` parameter determines if all files should be inspected during a scan operation. This parameter overrides all other parameters, so set this parameter to false if you are configuring a filter.

### Example 9-11. Scan only PDF and XLXS files modified after 10/19/2011

---

Request:

```
PUT https://<vsm-ip>/api/2.0/dlp/policy/FileFilters
<FileFilters>
  <scanAllFiles>false</scanAllFiles>
  <lastModifiedAfter>2011-10-19 15:16:04.0 EST</lastModifiedAfter>
  <extensionsIncluded>true</extensionsIncluded>
  <extensions>pdf,xlsx</extensions>
</FileFilters>
```

### Example 9-12. Scan all files except PDF and XLXS files

---

Request:

```
PUT https://<vsm-ip>/api/2.0/dlp/policy/FileFilters
<FileFilters>
```



```

    <scanAllFiles>false</scanAllFiles>
    <extensionsIncluded>false</extensionsIncluded>
    <extensions>pdf,xlsx</extensions>
  </FileFilters>

```

---

**Example 9-13.** Scan PDF and XLSX files that are less than 100 MB in size
 

---

Request:

```

PUT https://<vsm-ip>/api/2.0/dlp/policy/FileFilters
<FileFilters>
  <scanAllFiles>false</scanAllFiles>
  <sizeLessThanBytes>100000000</sizeLessThanBytes>
  <extensionsIncluded>true</extensionsIncluded>
  <extensions>pdf,xlsx</extensions>
</FileFilters>

```

---

## Saving and Publishing Policies

After you have defined a data security policy, you can edit it by changing the regulations selected, areas excluded from the scan, or the file filters. To apply the edited policy, you must publish it.

### Query Saved Policy

As a best practice, you should retrieve and review the last saved policy before publishing it. Each policy contains a revision value that can be used to track version history.

---

**Example 9-14.** Get saved SDD policy
 

---

Request:

```

GET https://<vsm-ip>/api/2.0/dlp/policy/saved
Authorization: Basic YWRtaW46ZGVmYXVsdA==

```

Response: the following response contains a policy with a single regulation, Indiana HB-1101.

```

<DlpPolicy>
  <objectId>DlpPolicy-1</objectId>
  <type>
    <typeName>DlpPolicy</typeName>
  </type>
  <name>DlpPolicy-One</name>
  <revision>6</revision>
  <objectTypeName>DlpPolicy</objectTypeName>
  <regulations>
    <Regulation>
      <id>37</id>
      <name>Indiana HB-1101</name>
      <description>Indiana HB-1101</description>
      <classifications>
        <Classification>
          <id>16</id>
          <name>US National Provider Identifier</name>
          <providerName>US National Provider Identifier</providerName>
          <description>US National Provider Identifier</description>
          <customizable>false</customizable>
        </Classification>
      </classifications>
      <regions>
        <string>North America</string>
        <string>USA</string>
      </regions>
      <categories>
        <string>PHI</string>
        <string>PCI</string>
      </categories>
    </Regulation>
  </regulations>
</DlpPolicy>

```

```

        <string>PII</string>
      </categories>
    </Regulation>
  </regulations>
  <regulationsChanged>>false</regulationsChanged>
  <excludedAreas/>
  <excludedAreasChanged>>false</excludedAreasChanged>
  <fileFilters>
    <scanAllFiles>>false</scanAllFiles>
    <sizeLessThanBytes>0</sizeLessThanBytes>
    <extensionsIncluded>>false</extensionsIncluded>
  </fileFilters>
  <fileFiltersChanged>>false</fileFiltersChanged>
  <classificationValues>
    <ClassificationValue>
      <id>1</id>
      <classification>
        <id>19</id>
        <name>Patient Identification Numbers</name>
        <providerName>Patient Identification Numbers</providerName>
        <description>Patient Identification Numbers</description>
        <customizable>true</customizable>
      </classification>
      <value>deg</value>
    </ClassificationValue>
  </classificationValues>
  <classificationValuesChanged>>false</classificationValuesChanged>
  <lastUpdatedOn class="sql-timestamp">2012-01-04 21:25:08.0</lastUpdatedOn>
  <lastUpdatedBy>admin</lastUpdatedBy>
</DlpPolicy>

```

---

## Query Published Policy

You can retrieve the currently published SDD policy that is active on all vShield Endpoint SVMs.

### Example 9-15. Get published SDD policy

---

Request:

```
GET https://<vsm-ip>/api/2.0/dlp/policy/published
Authorization: Basic YWRtaW46ZGVmYXVsdA==
```

---

## Publish the Updated Policy

After updating a policy with added regulations, excluded areas, or customized regex values publish the policy to enforce the new parameters.

### Example 9-16. Publish the updated policy

---

Request:

```
PUT https://<vsm-ip>/api/2.0/dlp/policy/publish
```

---

## Data Security Scanning

Running a data security scan identifies data in your virtual environment that violates your policy.

All virtual machines in your datacenter are scanned once during a scan. If the policy is edited and published while a scan is running, the scan restarts. This rescan ensures that all virtual machines comply with the edited policy. A rescan is triggered by publishing an edited policy, not by data updates on your virtual machines. After you start a scan, it continues to run until you pause or stop it.

If new virtual machines are added to your inventory while a scan is in progress, those machines will also be scanned. If a virtual machine is moved to an excluded cluster or resource pool while the data security scan is in progress, the files on that virtual machine are not scanned. In case a virtual machine is moved via vMotion to another host, the scan continues on the second host (files that were scanned while the virtual machine was on the previous host are not scanned again).

vShield Data Security scans one virtual machine on a host at a time to minimize impact on performance. VMware recommends that you pause the scan during normal business hours to avoid any performance overhead.

## Start, Pause, Resume, or Stop a Scan Operation

You can start or stop a scan operation. The scan operation options are as follows:

- **START:** Start a new scan.
- **PAUSE:** Pause a started scan.
- **RESUME:** Resume a paused scan.
- **STOP:** Stop any scan.

### Example 9-17. Start, pause, resume, or stop a scan operation

---

Request:

```
PUT https://<vsm-ip>/api/2.0/dlp/scanop
```

```
<ScanOp>STOP</ScanOp>
```

---

## Query Status for a Scan Operation

You can retrieve the status of the scan operation to determine if a scan is **STARTED** (that is, in progress), **PAUSED**, or **STOPPED**. The `nextScanOps` parameter indicates the scan operations possible from your current state. In the following example, the current scan state is **Stopped** and the only action you can perform is **Start** the scan.

### Example 9-18. Get scan status

---

Request:

```
GET https://<vsm-ip>/api/2.0/dlp/scanstatus
```

Response:

```
<DlpScanStatus>
  <currentScanState>STOPPED</currentScanState>
  <nextScanOps><ScanOp>START</ScanOp></nextScanOps>
  <vmsInProgress>0</vmsInProgress>
  <vmsCompleted>0</vmsCompleted>
</DlpScanStatus>
```

---

## Querying Scan Results

You can retrieve detailed results of the current data security scan as well as summary results for the previous five scans.

## Get List of Virtual Machines Being Scanned

You can retrieve information about the virtual machines being scanned by a scan.

**Example 9-19. Get list of virtual machines being scanned**

---

Request:

```
GET https://<vsm-ip>/api/2.0/dlp/scan/current/vms/<id>
?scanstatus=COMPLETED&pagesize=10&startindex=1
```

Response:

```
<?xml version="1.0" encoding="UTF-8"?>
<VmScanStatusDp>
  <dataPage>
    <pagingInfo>
      <pageSize>10</pageSize>
      <startIndex>1</startIndex>
      <totalCount>2</totalCount>
      <sortOrderAscending>false</sortOrderAscending>
    </pagingInfo>
    <VmScanStatus>
      <startTime>1320803585000</startTime>
      <endTime>1320803826000</endTime>
      <vmMoId>vm-25</vmMoId>
      <scanStatus>COMPLETED</scanStatus>
      <violationCount>8</violationCount>
      <vmName>jim-win2k8-32-mux</vmName>
      <dcName>jack</dcName>
    </VmScanStatus>
  </dataPage>
</VmScanStatusDp>
```

---

Where

- id is an optional parameter which limits the filter results by the VC MOID of a datacenter, cluster, or resource pool.
- scanstatus specifies the scan status of the virtual machines to be retrieved. Possible values are all, notstarted, started, and completed. This limits the results to virtual machines that have the specified scan state.
- pagesize limits the maximum number of entries returned by the API. The default value for this parameter is 256 and the valid range is 1-1024.
- startindex specifies the starting point for retrieving the logs. If this parameter is not specified, logs are retrieved from the beginning.

## Get Number of Virtual Machines Being Scanned

You can retrieve the number of virtual machines being scanned.

**Example 9-20. Get number of virtual machines being scanned**

---

Request:

```
GET https://<vsm-ip>/api/2.0/dlp/scan/current/vms/count/<id>?scanstatus=COMPLETED
```

---

Where

- scanstatus is an optional parameter that specifies the scan status of the virtual machines to be retrieved. Possible values are all, notstarted, started, and completed. This limits the results to virtual machines that have the specified scan state.
- id is an optional parameter which limits the filter results by the VC MOID of a datacenter, cluster, or resource pool.

## Get Summary Information about the Last Five Scans

You can retrieve the start and end time, total number of virtual machines scanned, and total number of violations for the last five completed data security scans.

---

### Example 9-21. Get summary information about last five scans

---

Request:

GET https://<vsm-ip>/api/2.0/dlp/completedscansummaries

Response:

```
<?xml version="1.0" encoding="UTF-8"?>
<list>
  <CompletedScanSummary>
    <globalScanId>5</globalScanId>
    <startTime class="sql-timestamp">2011-11-09 17:02:48.0</startTime>
    <endTime class="sql-timestamp">2011-11-09 17:02:55.0</endTime>
    <totalVmsScannedCount>0</totalVmsScannedCount>
    <totalViolationCount>0</totalViolationCount> ── Scan ID
  </CompletedScanSummary>
</list>
```

---

## Get Information for Virtual Machines Scanned During Previous Scan

You can retrieve the following information about the virtual machines scanned during the previous data security scan:

- ID
- Name
- Scan status
- Violation count

---

### Example 9-22. Get Information for virtual machines scanned during last scan

---

Request:

GET https://<vsm-ip>/api/2.0/dlp/scan/<scan\_ID>/detailsascsv

---

## Retrieve Information About Previous Scan Results

You can retrieve a detailed report about the results of the previous scan in a CSV format.

---

### Example 9-23. Retrieves Information for virtual machines scanned during last scan

---

Request:

GET https://<vsm-ip>/api/2.0/dlp/scan/<scan\_ID>/violatingfilesascsv

---

## Get XML Representation of Policy Used for Previous Scan

You can retrieve the XML representation of the policy used in the previous scan.

---

### Example 9-24. Get XML representation of policy used in previous scan

---

Request:

GET https://<vsm-ip>/api/2.0/dlp/scan/<scan\_ID>/policyasxml

---

Response:

```
<DlpPolicy>
  <objectId>dlppolicy-2</objectId>
  <type>
    <typeName>DlpPolicy</typeName>
  </type>
  <name>Published Policy</name>
  <revision>2</revision>
  <objectTypeName>DlpPolicy</objectTypeName>
  <regulations/>
  <regulationsChanged>>false</regulationsChanged>
  <excludedAreas/>
  <excludedAreasChanged>>false</excludedAreasChanged>
  <excludedSecurityGroups>
    <basicinfo>
      <objectId>securitygroup-1</objectId>
      <type>
        <typeName>SecurityGroup</typeName>
      </type>
      <name>included</name>
      <revision>2</revision>
      <objectTypeName>SecurityGroup</objectTypeName>
      <scope>
        <id>datacenter-2</id>
        <objectTypeName>Datacenter</objectTypeName>
        <name>jkiryakoza</name>
      </scope>
    </basicinfo>
  </excludedSecurityGroups>
  <excludedSecurityGroupsChanged>>false</excludedSecurityGroupsChanged>
  <includedSecurityGroups>
    <basicinfo>
      <objectId>securitygroup-1</objectId>
      <type reference=" ../ ../excludedSecurityGroups/basicinfo/type"/>
      <name>included</name>
      <revision>2</revision>
      <objectTypeName>SecurityGroup</objectTypeName>
      <scope>
        <id>datacenter-2</id>
        <objectTypeName>Datacenter</objectTypeName>
        <name>jkiryakoza</name>
      </scope>
    </basicinfo>
  </includedSecurityGroups>
  <includedSecurityGroupsChanged>>false</includedSecurityGroupsChanged>
  <fileFilters>
    <scanAllFiles>>false</scanAllFiles>
    <sizeLessThanBytes>0</sizeLessThanBytes>
    <extensionsIncluded>>true</extensionsIncluded>
  <extensions>doc,docm,docx,dot,dotx,dotm,wri,xla,xlam,xls,xlt,xltx,xltx,xlsm,xlsb,xlsm,ppt,pptx,pptm,pot,potx,potm,ppsx,ppsm,mdb,
    mpp,pdf,txt,log,csv,htm,html,xml,text,rtf,svg,ps,gs,vis,msg,rfc822,pm,swf,dgn,jpg,CATAnalysis,CATDrawing,C
    ATFCT,CATMaterial,CATPart,CATProcess,CATProduct,CATShape,CATSWL,CATSystem,3DXML,7z,cab,emx,
    gz,hqx,jar,lha,lzh,rar,tar,uue,z,zip,eml,mail,cal,cont,task,note,jrnl,pst</extensions>
  </fileFilters>
  <fileFiltersChanged>>false</fileFiltersChanged>
  <classificationValues>
    <ClassificationValue>
      <id>33</id>
      <classification>
        <id>90</id>
        <name>Custom Accounts</name>
        <providerName>Custom Accounts</providerName>
        <description>Custom Accounts</description>
        <customizable>true</customizable>
      </classification>
    </ClassificationValue>
  </ClassificationValue>
```

```

...
<classificationValuesChanged>false</classificationValuesChanged>
<lastUpdatedOn class="sql-timestamp">2011-11-09 16:59:01.0</lastUpdatedOn>
<lastUpdatedBy>dlp</lastUpdatedBy>
</DlpPolicy>

```

---

## Querying Violation Details

Once you start a data security scan, vShield reports the regulations that are being violated by the files in your inventory, and the violating files. If you fix a violating file (by deleting the sensitive information from the file, deleting or encrypting the file, or editing the policy), the file will continue to be displayed in the Violating files section until the current scan completes, and a new scan starts and completes.

You must be a Security Administrator or Auditor to view reports.

## Get List of Violation Counts

You can view a report that displays the violated regulations with the number of violations for each regulation. The violating files report requires filtering by node ID.

### Example 9-25. Get violation count for entire inventory

---

Request:

```
GET https://<vsm-ip>/api/2.0/dlp/violations/
```

---

### Example 9-26. Get violation count for specific resource

---

Request:

```
GET https://<vsm-ip>/api/2.0/dlp/violations/<context_ID>
```

Response Body

```

<list>
  <Violations>
    <scope>
      <objectId>group-d1</objectId>
      <type>
        <typeName>Folder</typeName>
      </type>
      <name>Datacenters</name>
      <revision>1</revision>
      <objectTypeName>Folder</objectTypeName>
    </scope>
    <regulation>
      <id>100</id>
      <name>California AB-1298</name>
      <description>Identifies documents and transmissions that contain protected health information (ePHI) and personally
        identifiable information (PII) as regulated by California AB-1298 (Civil Code 56, 1785 and
        1798). California residents medical and health insurance information, when combined with
        personally identifiable information must be protected from unauthorized access, destruction, use,
        modification, or disclosure. Any business that operates in California and owns or licenses
        computerized ePHI and PII data for California residents, regardless of the physical location of
        the business, is required to comply with this law. This policy detects US Social Security
        Numbers, credit card numbers, California drivers license numbers, US National Provider
        Numbers, group insurance numbers, health plan beneficiary numbers, medical record numbers,
        patient identifiers, birth and death certificates and Healthcare Dictionaries.
      </description>
      <classifications>
        <Classification>
          <id>76</id>
          <name>Health Plan Beneficiary Numbers</name>
          <providerName>Health Plan Beneficiary Numbers</providerName>
        </Classification>
      </classifications>
    </regulation>
  </Violations>
</list>

```

```

        <description>Health Plan Beneficiary Numbers</description> <customizable>true</customizable>
      </Classification>
    ...
    <regions>
      <string>NA</string>
    </regions>
    <categories>
      <string>PHI</string>
      <string>PCI</string>
      <string>PII</string>
    </categories>
  </regulation>
  <violationCount>1</violationCount>
</Violations>
<Violations>
</list>

```

---

Where context\_ID is the MOID of a datacenter, cluster, folder, resource pool, or virtual machine.

## Get List of Violating Files

You can view a report that displays the violating files and the regulations each file violated. This API requires filtering by context node ID, and returns a formatted XML report showing violating files.

### Example 9-27. Get violating files for entire inventory

---

Request:

```
GET https://<vsm-ip>/api/2.0/dlp/violatingfiles?pagesize=<i>&startindex=<j>
```

---

Where:

- pagesize is the number of results to view.
- startindex is the page number from which the results should be displayed.

### Example 9-28. Get violating files for a resource

---

Request:

```
GET https://<vsm-ip>/api/2.0/dlp/violatingfiles/<context_ID>?pagesize=<i>&startindex=<j>
```

Response Body:

```

<ViolatingFiles>
  <dataPage>
    <pagingInfo>
      <pageSize>10</pageSize>
      <startIndex>0</startIndex>
      <totalCount>1</totalCount>
      <sortOrderAscending>false</sortOrderAscending>
    </pagingInfo>
    <ViolatingFile>
      <identifier>59</identifier>
      <revision>0</revision>
      <fileName>C:\TruePositives\SocialSecurityNumbersTP1.05.txt</fileName>
      <fileExtension />
      <fileLastModifiedTime class="sql-timestamp">2011-02-01 15:02:00.0</fileLastModifiedTime>
      <vm>
        <name>jim-xp32-dlp1</name>
        <revision>0</revision>
      </vm>
      <cluster>
        <name>JimCluster</name>
        <revision>0</revision>
      </cluster> \
    </ViolatingFile>
  </dataPage>
</ViolatingFiles>

```



```

<dataCenter>
  <name>jkiryakoza</name>
  <revision>0</revision>
</dataCenter>
<violations>
  <ViolationInfo>
    <identifier>99</identifier>
    <revision>0</revision>
    <regulation>
      <objectId>152</objectId>
      <name>California SB-1386</name>
      <description>Identifies documents and transmissions that contain personally identifiable information
        (PII) as regulated by California SB-1386 (Civil Code 1798). Businesses that
        own or license computerized PII about California residents are required to
        maintain security procedures and practices to protect it from unauthorized
        access, destruction, use, modification, or disclosure. Any business that operates
        in California and owns or licenses computerized PII data for California
        residents, regardless of the physical location of the business, is required to
        comply with this law. This policy detects US Social Security numbers, credit
        card numbers and California drivers license numbers. This regulation has been
        amended to protect health and medical information that can be found in
        California AB-1298. </description>
      <revision>0</revision> </regulation>
      <firstViolationReportedTime class="sql-timestamp">2012-01-26
        12:56:42.0</firstViolationReportedTime>
      <lastViolationReportedTime class="sql-timestamp">2012-01-26
        12:56:42.0</lastViolationReportedTime>
      <cumulativeViolationCount>1</cumulativeViolationCount>
      <violationCount>0</violationCount>
    </ViolationInfo>
  </violations>
</ViolatingFile>
</dataPage>
</ViolatingFiles>

```

---

Where:

- context\_ID is the MOID of a datacenter, cluster, folder, resource pool, or virtual machine..
- pagesize is the number of results to view.
- startindex is the page number from which the results should be displayed.

## Get List of Violating Files in CSV Format

You can view a report that displays the violating files and the regulations each file violated in a CSV format.

**Example 9-29.** Get list of violating files in CSV format

---

Request:

GET https://<vsm-ip>/api/2.0/dlp/violatingfilesascsv

---

## Get Violations in Entire Inventory

You can view a report of the violated regulations and the violating files for the entire inventory in CSV (comma separated variable) format.

**Example 9-30.** Get list of violated regulations

---

Request:

GET https://<vsm-ip>/api/2.0/dlp/violatingfilesascsv/<context\_ID>

---

Where `context_ID` is the MOID of a datacenter, cluster, folder, resource pool, or virtual machine.

# Task Framework Management

---

The NSX Manager requires communication with your vCenter Server and services such as DNS and NTP to provide details on your VMware Infrastructure inventory.

The chapter includes the following topics:

- [“About Task Framework”](#) on page 219
- [“Query Job Instances for Job ID”](#) on page 220
- [“Query Latest Job Instances for Job ID”](#) on page 221
- [“Block REST Thread”](#) on page 221
- [“Query Job Instances by Criterion”](#) on page 221

---

**IMPORTANT** All REST requests require authentication. See [“Using the NSX REST API”](#) on page 25 for details about basic authorization.

---

## About Task Framework

The task framework provides the abstraction needed to execute asynchronous tasks using a global thread pool.

A Job is identified by a Job ID. A job has a set of tasks within it. These tasks are executed either synchronously or in parallel based on their dependencies with other tasks in the Job. The Job is the primary interface to interact with the Task Framework to get the details of the job and the tasks within it. This could be the status of the job, the status of the tasks within it, etc.

When a Job is scheduled for execution, it is put into a queued state. This is true for a job that has to execute immediately or a job that is scheduled for later execution.

At the scheduled time when the task runs it is put into executing state. Once the task finishes its execution, it is considered as completed. The task framework then queries the task to check if the execution was successful or not. Based on this status, the task is marked as completed or failed. If the task is successful, the next task in the Job is executed. If the task fails, the appropriate fault policy action is taken.

The fault policy specifies the type of action to be taken as one of the following:

- **Retry:** Framework attempts to retry the task. Job data / data populated during the earlier run is supplied to the task before execution.
- **Rollback:** Framework rolls back the task.
- **Rollback Retry:** Framework rolls back the task and retries it.
- **Abort:** Framework aborts the task (and the Job).
- **Ignore:** Framework ignores the failure / timeout and proceeds with execution of subsequent tasks, if any, in the job.

Every task can define a timeout value which indicates the maximum estimated time for the task to complete. Beyond this time, the task is considered to have timed out and an appropriate fault policy action is taken on the task. The task framework monitors the executing tasks at periodic intervals of time to check whether they have timed out. If the fault policy indicates that a retry has to be done in case of a time out, the task framework retries the task.

## Query Job Instances for Job ID

Retrieves all job instances for the specified job ID. If a job is a one-time job, a single job instance is returned. If a job is a recurring job, all instances for the given job ID are returned.

### Example 10-1. Query job instances

---

Request Body:

GET https://<nsxmgr-ip>/api/2.0/services/taskservice/job/<jobID>

Response Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<jobInstances>
  <jobInstance>
    <id>jobinstance-1</id>
    <name>SVM Updater</name>
    <taskInstances>
      <taskInstance>
        <id>taskinstance-1</id>
        <name>SVM Updater</name>
        <startTimeMillis>1375867719752</startTimeMillis>
        <endTimeMillis>1375867720025</endTimeMillis>
        <taskStatus>COMPLETED</taskStatus>
        <timeoutRetryCount>0</timeoutRetryCount>
        <failureRetryCount>0</failureRetryCount>
        <taskOutput />
        <taskData />
      </taskInstance>
    </taskInstances>
    <startTimeMillis>1375867719663</startTimeMillis>
    <endTimeMillis>1375867720050</endTimeMillis>
    <status>COMPLETED</status>
    <timeoutRetryCount>0</timeoutRetryCount>
    <failureRetryCount>0</failureRetryCount>
  </job>
  <id>jobdata-1</id>
  <name>SVM Updater</name>
  <description>Updating all sdd SVMs at startup.</description>
  <creationTimeMillis>1375867718710</creationTimeMillis>
  <nextExecutionTimeMillis>0</nextExecutionTimeMillis>
  <taskList>
    <task>
      <id>task-1</id>
      <name>SVM Updater</name>
      <description>Updating all sdd SVMs at startup.
      </description>
      <failurePolicy>
        <faultAction>RETRY</faultAction>
        <retryLimit>30</retryLimit>
        <retryInterval>60000</retryInterval>
      </failurePolicy>
      <timeoutPolicy>
        <faultAction>IGNORE</faultAction>
        <retryLimit>0</retryLimit>
        <retryInterval>-1</retryInterval>
      </timeoutPolicy>
      <priority>5</priority>
      <timeoutMillis>-1</timeoutMillis>
      <visible>false</visible>
    </task>
  </taskList>
</jobInstances>
```

```

<systemTask>true</systemTask>
<taskClass>com.vmware.vshield.dlp.service.impl.DlpServiceImpl$1
</taskClass>
<creationTimeMillis>1375867718729
</creationTimeMillis>
<jobId>jobdata-1</jobId>
<nextExecutionTime>0</nextExecutionTime>
</task>
</taskList>
<jobOwner>Unknown</jobOwner>
<scope>/globalroot-0</scope>
</job>
<jobOutput />
</jobInstance>
</jobInstances>

```

---

## Query Latest Job Instances for Job ID

In case of cron jobs or fixed-delay jobs, there can be multiple job instances for the same job depending upon the number of times the job was executed. This call fetches the latest job instance for a given job id.

### Example 10-2. Query job instances

---

Request Body:

GET https://<nsxmgr-ip>/api/2.0/services/taskservice/job/<jobID>

Response Body:

See [Example 10-1](#)

---

## Block REST Thread

This is a blocking call where a service has scheduled a job and a REST thread needs to be blocked till the job gets completed. If the job was already completed, then the job instance is returned immediately. If the job is still executing then the REST thread is blocked and returns after the job completes.

### Example 10-3. Query job instances

---

Request Body:

GET https://<nsxmgr-ip>/api/2.0/services/taskservice/job/<jobID>

Response Body:

See [Example 10-1](#).

---

## Query Job Instances by Criterion

You can specify filtering criteria and paging information and query the task framework.

### Example 10-4. Query job instances by criterion

---

Request Body:

GET

https://<nsxmgr-ip>/api/2.0/services/taskservice/job/startIndex=<0>&pageSize=<10>&sortBy=startTime&sortOrderAscending=false|true

Response Body:

See [Example 10-1](#).

---

# Appendix

---

The REST API configuration of the vShield Edge and vShield App virtual machines supports schemas for installation and service management.

This appendix covers the following topics:

- [“vShield Manager Global Configuration Schema”](#) on page 223
- [“ESX Host Preparation and Uninstallation Schema”](#) on page 228
- [“vShield App Schemas”](#) on page 229
- [“Error Message Schema”](#) on page 235

## vShield Manager Global Configuration Schema

The following schema shows vShield Manager REST configuration.

This replaces the 1.0 API schema items for vCenter synchronization, DNS service, virtual machine information, and security groups.

```
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
  targetNamespace="vmware.vshield.edge.2.0"
  xmlns:vse="vmware.vshield.edge.2.0"
  elementFormDefault="qualified">

  <xs:element name="vsmGlobalConfig">
    <xs:complexType>
      <xs:sequence>
        <xs:element minOccurs="0" name="vshieldEdgeReleaseInfo" type="vse:ReleaseInfoType"/> <!-- In response
          from server -->
        <xs:element minOccurs="0" name="vcInfo" type="vse:VcInfoType" />
        <xs:element minOccurs="0" name="hostInfo" type="vse:HostInfoType" />
        <xs:element minOccurs="0" name="techSupportLogsTarFilePath" type="xs:string"/>
        <xs:element minOccurs="0" name="auditLogs" type="vse:AuditLogsType" />
        <xs:element minOccurs="0" name="dnsInfo" type="vse:DnsInfoType" />
        <xs:element minOccurs="0" name="versionInfo" type="xs:string" /> <!-- only in response -->
        <xs:element minOccurs="0" name="vpnLicensed" type="xs:boolean" /> <!-- only in response -->
        <xs:element minOccurs="0" name="ipsecVpnTunnels" type="vse:IpssecVpnTunnels" /> <!-- only in response -->
        <xs:element minOccurs="0" maxOccurs="1" name="vsmCapability" type="vse:VsmCapabilityType"/>
        <!-- only in response -->
        <xs:element minOccurs="0" maxOccurs="1" name="timeInfo" type="vse:TimeInfoType"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>

  <xs:complexType name="ReleaseInfoType"> <!-- can be re-used for release information of vshield, vShield
    Manager, or vShield Edge-->
    <xs:sequence>
      <xs:element name="buildNumber" type="xs:NMTOKEN" /> <!-- add fields as required -->
      <xs:element minOccurs="0" name="vseLocationOnVsm" type="xs:string" />
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

```
</xs:sequence>
</xs:complexType>

<xs:complexType name="SSOInfoType">
  <xs:sequence>
    <xs:element minOccurs="0" name="vsmSolutionName">
      <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:minLength value="1"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>
    <xs:element name="lookupServiceUrl">
      <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:minLength value="1"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>
    <xs:element name="ssoAdminUserName">
      <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:minLength value="1"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>
    <xs:element name="ssoAdminPassword">
      <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:minLength value="1"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>
    <xs:element minOccurs="0" name="certificateThumbprint">
      <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:pattern
            value="[a-fA-F0-9]{2};[a-fA-F0-9]{2};[a-fA-F0-9]{2};[a-fA-F0-9]{2};[a-fA-F0-9]{2};[a-fA-F0-9]{2};[a-fA-F0-9]{2};[a-fA-F0-9]{2};[a-fA-F0-9]{2};[a-fA-F0-9]{2};[a-fA-F0-9]{2};[a-fA-F0-9]{2};[a-fA-F0-9]{2};[a-fA-F0-9]{2};[a-fA-F0-9]{2};[a-fA-F0-9]{2};[a-fA-F0-9]{2};[a-fA-F0-9]{2};[a-fA-F0-9]{2};[a-fA-F0-9]{2}"></xs:pattern>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="VcInfoType">
  <xs:sequence>
    <xs:element name="ipAddress">
      <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:minLength value="1"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>
    <xs:element name="userName">
      <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:minLength value="1"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>
    <xs:element name="password">
      <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:minLength value="1"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>
```



```
</xs:simpleType>
</xs:element>
    <xs:element minOccurs="0" name="token">
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:minLength value="1"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>
    <xs:element minOccurs="0" name="certificateThumbprint">
        <xs:simpleType>
            <xs:restriction base="xs:string">
<xs:pattern value="[a-fA-F0-9]{2}:[a-fA-F0-9]{2}:[a-fA-F0-9]{2}:[a-fA-F0-9]{2}:[a-fA-F0-9]{2}:[a-fA-F0-9]{2}:[a-fA-F0-9]{2}:[a-fA-F0-9]{2}:[a-fA-F0-9]{2}:[a-fA-F0-9]{2}:[a-fA-F0-9]{2}:[a-fA-F0-9]{2}:[a-fA-F0-9]{2}:[a-fA-F0-9]{2}:[a-fA-F0-9]{2}:[a-fA-F0-9]{2}:[a-fA-F0-9]{2}:[a-fA-F0-9]{2}:[a-fA-F0-9]{2}"></xs:pattern>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>
    <xs:element minOccurs="0" name="pluginDownloadServer">
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:minLength value="1"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>
    <xs:element minOccurs="0" name="pluginDownloadPort">
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:minLength value="1"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>
</xs:sequence>
</xs:complexType>

<xs:complexType name="HostInfoType">
    <xs:sequence>
        <xs:element name="hostId" type="xs:string" />
        <xs:element name="ipAddress" type="xs:string" />
        <xs:element name="userName" type="xs:string" />
        <xs:element name="password" type="xs:string" />
    </xs:sequence>
</xs:complexType>

<xs:complexType name="SecurityGroups">
    <xs:choice>
        <xs:element name="securityGroup" type="vse:SecurityGroup" maxOccurs="unbounded" />
        <xs:element name="securityGroupIdList" type="vse:SecurityGroupIdList" />
    </xs:choice>
</xs:complexType>

<xs:complexType name="SecurityGroup">
    <xs:sequence>
        <xs:element name="securityGroupBaseNode" type="xs:string"/>
        <xs:element name="securityGroupName" type="xs:string"/>
        <xs:element name="securityGroupId" type="xs:string" minOccurs="0" />
        <xs:element name="securityGroupNodeList" type="vse:NodeList" minOccurs="0"/>
        <xs:element name="securityGroupIpList" type="vse:IpList" minOccurs="0" />
    </xs:sequence>
</xs:complexType>

<xs:complexType name="SecurityGroupIdList">
    <xs:sequence>
        <xs:element name="securityGroupId" type="xs:string" maxOccurs="unbounded" />
    </xs:sequence>
</xs:complexType>

<xs:complexType name="IpList">
```

```

    <xs:sequence>
      <xs:element name="ip" type="xs:string" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="NodeList">
    <xs:sequence>
      <xs:element name="node" type="vse:SecurityGroupNode" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="SecurityGroupNode">
    <xs:sequence>
      <xs:element name="id" type="xs:string" />
      <xs:element name="name" type="xs:string" minOccurs="0" />
      <xs:element name="ipList" type="vse:IpList" minOccurs="0" />
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="VnicsType">
    <xs:sequence>
      <xs:element name="vnic" type="vse:VnicType" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="VnicType">
    <xs:sequence>
      <xs:element name="id" type="xs:string" />
      <xs:element name="name" type="xs:string" />
      <xs:element name="ipList" type="vse:IpList" minOccurs="0" maxOccurs="1"/>
      <!-- Will be good if we can also send this information -->
      <xs:element name="VLAN" type="xs:int" />
      <xs:element name="PortGroup" type="xs:string" />
      <xs:element name="Protected" type="xs:boolean"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="AuditLogsType">
    <xs:sequence>
      <xs:element name="auditLog" type="vse:AuditLogType" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="DnsInfoType">
    <xs:sequence>
      <xs:element name="primaryDns" type="xs:string"/>
      <xs:element minOccurs="0" name="secondaryDns" type="xs:string"/>
      <xs:element minOccurs="0" name="tertiaryDns" type="xs:string"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="AuditLogType">
    <xs:sequence>
      <xs:element name="id" type="xs:string" />
      <xs:element name="userName" type="xs:string" />
      <xs:element name="accessInterface" type="xs:string" />
      <xs:element name="module" type="xs:string" />
      <xs:element name="operation" type="xs:string" />
      <xs:element name="status" type="xs:string" />
      <xs:element name="operationSpan" type="xs:string" />
      <xs:element name="resource" type="xs:string" />
      <xs:element name="timestamp" type="xs:string" />
      <xs:element name="notes" type="xs:string" />
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="IpsecVpnTunnels">
    <xs:sequence>
      <xs:element name="lastEventId" type="xs:unsignedInt" />

```

```

        <xs:element minOccurs="0" maxOccurs="unbounded" name="ipsecVpnTunnelStatusList"
            type="vse:IpsecVpnTunnelStatus" />
    </xs:sequence>
</xs:complexType>

<xs:complexType name="IpsecVpnTunnelStatus">
    <xs:sequence>
        <xs:element name="networkId" type="xs:string" />
        <xs:element name="ipsecVpnTunnelConfig" type="vse:IpsecVpnTunnelConfigType" />
    </xs:sequence>
</xs:complexType>

<xs:complexType name="IpsecVpnTunnelConfigType"> <!--only in response -->
    <xs:sequence>
        <xs:element name="peerName">
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:minLength value="1"/>
                    <xs:maxLength value="256"/>
                </xs:restriction>
            </xs:simpleType>
        </xs:element>
        <xs:element name="peerId" type="xs:string" />
        <xs:element name="peerIpAddress" type="xs:string" />
        <xs:element maxOccurs="64" name="localSubnet" type="xs:string" /> <!-- localSubnet * peerSubnet * noOfSites
            should not be more than 64 -->
        <xs:element maxOccurs="64" name="peerSubnet" type="xs:string" /> <!-- localSubnet * peerSubnet * noOfSites should
            not be more than 64 -->
        <xs:element name="authenticationMode">
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:pattern value="((psk)|(x.509))"/>
                </xs:restriction>
            </xs:simpleType>
        </xs:element>
        <xs:element minOccurs="0" name="preSharedKey" type="xs:string" />
        <xs:element minOccurs="0" name="encryptionAlgorithm" type="xs:string" />
        <xs:element minOccurs="0" name="mtu" type="xs:unsignedInt" />
        <xs:element minOccurs="0" name="status" type="xs:string" />
        <xs:element minOccurs="0" name="stateChangeReason" type="xs:string" />
    </xs:sequence>
</xs:complexType>

<xs:complexType name="VsmCapabilityType">
    <xs:sequence>
        <xs:element name="ipsecVpnCapability" type="xs:boolean"/>
        <xs:element name="webLoadBalancerCapability" type="xs:boolean"/>
        <xs:element name="natCapability" type="xs:boolean"/>
        <xs:element name="firewallCapability" type="xs:boolean"/>
        <xs:element name="dhcpCapability" type="xs:boolean"/>
        <xs:element name="staticRoutingCapability" type="xs:boolean"/>
        <xs:element name="vsmVersion" type="xs:string"/>
    </xs:sequence>
</xs:complexType>

<xs:complexType name="TimeInfoType">
    <xs:sequence>
        <xs:element minOccurs="0" name="clock" type="xs:string"/>
        <xs:element minOccurs="0" name="ntpServer" type="xs:string"/>
        <xs:element minOccurs="0" name="zone" type="xs:string"/>
    </xs:sequence>
</xs:complexType>

</xs:schema>

```

## ESX Host Preparation and Uninstallation Schema

This schema can be used to install or uninstall vShield App and vShield Endpoint services on an ESX host.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">

  <xs:element name="VshieldConfiguration">
    <xs:complexType>
      <xs:all>
        <xs:element minOccurs="0" name="VszInstallParams" type="VszInstallParams"/>
        <xs:element minOccurs="0" name="EpsecInstallParams" type="xs:boolean"/>
        <xs:element name="InstallAction" type="InstallAction"/> <!-- InstallAction to be taken on appliance -
            install/upgrade -->
        <xs:element name="InstallStatus" type="InstallStatus"/> <!-- only in response -->
      </xs:all>
    </xs:complexType>
  </xs:element>

  <xs:complexType name="InstallStatus">
    <xs:sequence>
      <xs:element minOccurs="0" name="ProgressState" type="xs:string"/>
      <xs:element minOccurs="0" name="ProgressSubState" type="xs:string"/>
      <xs:element minOccurs="0" name="InstalledServices" type="InstalledServices"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="InstalledServices">
    <xs:sequence>
      <xs:element name="VszInstalled" type="xs:boolean"/>
      <xs:element name="EpsecInstalled" type="xs:boolean"/>
    </xs:sequence>
  </xs:complexType>

  <!-- Install parameters -->
  <xs:complexType name="VszInstallParams">
    <xs:sequence>
      <xs:element name="DatastoreId" type="Moid"/>
      <xs:element name="ManagementPortSwitchId" type="xs:string"/> <!-- contains the networkId of the mgmt
          portgroup -->
      <xs:element name="MgmtInterface" type="MgmtInterfaceType"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="MgmtInterfaceType">
    <xs:sequence>
      <xs:element name="IpAddress" type="IP"/>
      <xs:element name="NetworkMask" type="IP"/>
      <xs:element name="DefaultGw" type="IP"/>
    </xs:sequence>
  </xs:complexType>

  <xs:simpleType name="InstallAction">
    <xs:restriction base="xs:string">
      <xs:enumeration value="install"/>
      <xs:enumeration value="upgrade"/>
    </xs:restriction>
  </xs:simpleType>

  <xs:simpleType name="IP">
    <xs:restriction base="xs:string">
      <xs:pattern value="((25[0-5]|2[0-4][0-9]|1[0-9][0-9]|[1-9]?[0-9])\.){3}(25[0-5]|2[0-4][0-9]|1[0-9][0-9]|[1-9]?[0-9])" />
    </xs:restriction>
  </xs:simpleType>

</xs:schema>
```

```

<xs:simpleType name="Moid">
  <xs:restriction base="xs:string">
    <xs:pattern value="[a-zA-Z0-9\-\_]+"/>
  </xs:restriction>
</xs:simpleType>

</xs:schema>

```

## vShield App Schemas

The following schemas detail vShield App configuration via REST API.

### vShield App Configuration Schema

This schema configures a vShield App after installation.

```

<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">

  <xs:element name="ZonesConfiguration">
    <xs:complexType>
      <xs:all>
        <xs:element name="VszInstallParams" type="VszInstallParams" minOccurs="0"/>
      </xs:all>
    </xs:complexType>
  </xs:element>

  <!-- Install parameters -->
  <xs:complexType name="VszInstallParamsType">
    <xs:sequence>
      <xs:element name="NodeId" type="xs:string"/>
      <xs:element name="DatacenterId" type="xs:string"/>
      <xs:element name="DatastoreId" type="xs:string"/>
      <xs:element name="NameForZones" type="xs:string"/>
      <xs:element name="VswitchForMgmt" type="xs:string"/>
      <xs:element name="MgmtInterface" type="InterfaceType"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="InterfaceType">
    <xs:sequence>
      <xs:element name="IpAddress" type="xs:NMTOKEN"/>
      <xs:element name="NetworkMask" type="xs:NMTOKEN"/>
      <xs:element name="DefaultGw" type="xs:NMTOKEN"/>
      <xs:element minOccurs="0" name="VlanTag" type="xs:string"/>
    </xs:sequence>
  </xs:complexType>

</xs:schema>

```

### vShield App Firewall Schema

This schema configures the firewall rules enforced by a vShield App.

```

<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">

  <xs:element name="VshieldAppConfiguration">
    <xs:complexType>
      <xs:choice>
        <xs:element name="firewallConfiguration" type="FirewallConfigurationDto" />
        <xs:element name="firewallConfigurationHistoryList" type="FirewallConfigHistoryInfoListDto" />
        <xs:element name="consolidatedConfiguration" type="FirewallConfigurationDto" maxOccurs="unbounded" />
        <xs:element name="status" type="StatusDto" />
        <xs:element name="datacenterState" type="DatacenterStateDto" />
        <xs:element name="protocolsList" type="ProtocolListDto" />
        <xs:element name="protocolTypes" type="ProtocolsTypeEnum" maxOccurs="4" />
      </xs:choice>
    </xs:complexType>
  </xs:element>

</xs:schema>

```

```

        </xs:choice>
    </xs:complexType>
</xs:element>

<xs:complexType name="FirewallConfigHistoryInfoListDto">
    <xs:sequence>
        <xs:element name="contextId" type="xs:string" />
        <xs:element name="firewallConfigHistoryInfo" type="FirewallConfigHistoryInfoDto" maxOccurs="unbounded" />
    </xs:sequence>
</xs:complexType>

<xs:complexType name="FirewallConfigHistoryInfoDto">
    <xs:sequence>
        <xs:element name="configId" type="xs:long" />
        <xs:element name="userId" type="xs:string" />
        <xs:element name="timestamp" type="xs:long" />
        <xs:element name="status" type="xs:string" minOccurs="0" />
    </xs:sequence>
</xs:complexType>

<xs:complexType name="DatacenterStateDto">
    <xs:sequence>
        <xs:element name="datacenterId" type="xs:string" />
        <xs:element name="userId" type="xs:string" minOccurs="0" />
        <xs:element name="timestamp" type="xs:long" minOccurs="0" />
        <xs:element name="status" type="DatacenterStatusEnum" />
    </xs:sequence>
</xs:complexType>

<xs:complexType name="StatusDto">
    <xs:sequence>
        <xs:element name="currentState" type="ConfigStateEnum" />
        <xs:element name="failedPublishInfo" type="FailedPublishInfoDto" maxOccurs="unbounded" minOccurs="0" />
    </xs:sequence>
    <xs:attribute name="contextId" type="xs:string" use="required" />
    <xs:attribute name="generationNumber" type="xs:long" />
</xs:complexType>

<xs:complexType name="FailedPublishInfoDto">
    <xs:sequence>
        <xs:element name="applianceIp" type="xs:string" />
        <xs:element name="timestamp" type="xs:long" />
        <xs:element name="errorDescription" type="xs:string" />
    </xs:sequence>
</xs:complexType>

<xs:complexType name="FirewallConfigurationDto">
    <xs:sequence>
        <xs:element name="layer3FirewallRule" type="Layer3FirewallRuleDto" maxOccurs="unbounded" minOccurs="0" />
        <xs:element name="layer2FirewallRule" type="Layer2FirewallRuleDto" maxOccurs="unbounded" minOccurs="0" />
    </xs:sequence>
    <xs:attribute name="provisioned" type="xs:boolean" use="optional" />
    <xs:attribute name="contextId" type="xs:string" use="required" />
    <xs:attribute name="timestamp" type="xs:long" use="optional" />
    <xs:attribute name="generationNumber" type="xs:long" use="optional" />
</xs:complexType>

<xs:complexType name="ApplicationDto">
    <xs:choice>
        <xs:element name="applicationSetId" type="xs:string" />
    </xs:choice>
</xs:complexType>

<xs:complexType name="DestinationDto" abstract="true">
    <xs:sequence>
        <xs:element name="address" type="AddressDto" minOccurs="0" />
    </xs:sequence>

```

```

        <!-- Only in response, not considered in request -->
    </xs:sequence>
</xs:complexType>

<xs:complexType name="Layer2DestinationDto">
    <xs:complexContent>
        <xs:extension base="DestinationDto">
            </xs:extension>
            <xs:element name="application" type="ApplicationDto" minOccurs="0" />
        </xs:complexContent>
    </xs:complexType>

<xs:complexType name="Layer3DestinationDto">
    <xs:sequence>
        <xs:element name="address" type="AddressDto" minOccurs="0" />
        <xs:element name="application" type="ApplicationDto" minOccurs="0" />
    </xs:sequence>
</xs:complexType>

<xs:complexType name="Layer3SourceAddressDto">
    <xs:sequence>
        <xs:element name="address" type="AddressDto" minOccurs="0" />
        <xs:element name="portInfo" type="xs:string" minOccurs="0" />
    </xs:sequence>
</xs:complexType>

<xs:complexType name="FirewallRuleDto" abstract="true">
    <xs:sequence>
        <xs:element name="action" type="ActionEnum" />
        <xs:element name="logged" type="xs:boolean" />
        <xs:element name="notes" type="xs:string" minOccurs="0" />
    </xs:sequence>
    <xs:attribute name="id" type="xs:long" use="required" />
    <xs:attribute name="precedence" type="PrecedenceEnum" use="optional" />
    <xs:attribute name="disabled" type="xs:boolean" use="optional" />
</xs:complexType>

<xs:complexType name="Layer2FirewallRuleDto">
    <xs:complexContent>
        <xs:extension base="FirewallRuleDto">
            <xs:sequence>
                <xs:element name="source" type="AddressDto" minOccurs="0" />
                <xs:element name="destination" type="Layer2DestinationDto" />
            </xs:sequence>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>

<xs:complexType name="Layer3FirewallRuleDto">
    <xs:complexContent>
        <xs:extension base="FirewallRuleDto">
            <xs:sequence>
                <xs:element name="source" type="Layer3SourceAddressDto" minOccurs="0" />
                <xs:element name="destination" type="Layer3DestinationDto" minOccurs="0" />
            </xs:sequence>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>

<xs:complexType name="AddressDto">
    <xs:choice>
        <xs:element name="containerId" type="xs:string" minOccurs="0">
            </xs:element>
        </xs:choice>
        <xs:attribute name="exclude" type="xs:boolean" use="optional" default="false" />
    </xs:complexType>

```

```

<xs:simpleType name="ActionEnum">
  <xs:restriction base="xs:NCName">
    <xs:enumeration value="allow" />
    <xs:enumeration value="deny" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="PrecedenceEnum">
  <xs:restriction base="xs:NCName">
    <xs:enumeration value="default" />
    <xs:enumeration value="none" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="ConfigStateEnum">
  <xs:restriction base="xs:NCName">
    <!-- <xs:enumeration value="saved" /> -->
    <xs:enumeration value="published" />
    <xs:enumeration value="inprogress" />
    <xs:enumeration value="publishFailed" />
    <xs:enumeration value="Deleted" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="DatacenterStatusEnum">
  <xs:restriction base="xs:NCName">
    <xs:enumeration value="upgrading" />
    <xs:enumeration value="backwardCompatible" />
    <xs:enumeration value="backwardCompatibleReadyForSwitch" />
    <xs:enumeration value="migrating" />
    <xs:enumeration value="regular" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="ProtocolsTypeEnum">
  <xs:restriction base="xs:NCName">
    <xs:enumeration value="application" />
    <xs:enumeration value="ipv4" />
    <xs:enumeration value="icmp" />
    <xs:enumeration value="ethernet" />
  </xs:restriction>
</xs:simpleType>

</xs:schema>

```

## vShield App SpoofGuard Schema

The following schema details SpoofGuard configuration.

```

<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">

  <xs:element name="VshieldConfiguration">
    <xs:complexType>
      <xs:choice>
        <xs:element name="globalSettings" type="GlobalSettingsDto" />
        <xs:element name="ipAssignmentStatistic" type="IpAssignmentStatisticDto" />
        <xs:element name="vnicIdList" type="VnicIdListDto" />
        <xs:element name="ipAssignmentDetailsList" type="IpAssignmentDetailsListDto" />
        <xs:element name="pagedIpAssignmentDetailsList" type="PagedIpAssignmentDetailsListDto" />
        <xs:element name="approveIpInfo" type="VnicInfoDto" />
      </xs:choice>
    </xs:complexType>
  </xs:element>

  <xs:complexType name="PagedIpAssignmentDetailsListDto">
    <xs:sequence>

```



```

        <xs:element name="ipAssignmentDetails" type="IpAssignmentDetailsDto" maxOccurs="unbounded" />
        <xs:element name="pagingDetails" type="PagingInfoDto" />
    </xs:sequence>
</xs:complexType>

<xs:complexType name="PagingInfoDto">
    <xs:sequence>
        <xs:element name="pageSize" type="xs:int" />
        <xs:element name="startIndex" type="xs:int" />
        <xs:element name="totalCount" type="xs:int" />
        <xs:element name="sortOrderAscending" type="xs:boolean" />
        <xs:element name="sortBy" type="PagingSortByEnum" />
    </xs:sequence>
</xs:complexType>

<xs:complexType name="IpAssignmentDetailsListDto">
    <xs:sequence>
        <xs:element name="ipAssignmentDetails" type="IpAssignmentDetailsDto" maxOccurs="unbounded" />
    </xs:sequence>
</xs:complexType>

<xs:complexType name="IpAssignmentDetailsDto">
    <xs:sequence>
        <xs:element name="vnicId" type="xs:string" />
        <xs:element name="macAddress" type="xs:string" />
        <xs:element name="ipAddress" type="xs:string" />
        <xs:element name="vnicName" type="xs:string" />
        <xs:element name="networkId" type="xs:string" />
        <xs:element name="vmId" type="xs:string" />
        <xs:element name="vmName" type="xs:string" />
        <xs:element name="approvedIpAddress" type="xs:string" />
        <xs:element name="approvedBy" type="xs:string" />
        <xs:element name="approvedOn" type="xs:long" />
        <xs:element name="publishedIpAddress" type="xs:string" />
        <xs:element name="publishedBy" type="xs:string" />
        <xs:element name="publishedOn" type="xs:long" />
        <xs:element name="reviewRequired" type="xs:boolean" />
        <xs:element name="duplicateCount" type="xs:int" />
    </xs:sequence>
</xs:complexType>

<xs:complexType name="IpAssignmentStatisticDto">
    <xs:sequence>
        <xs:element name="contextId" type="xs:string" />
        <xs:element name="inSync" type="xs:boolean" />
        <xs:element name="activeCount" type="xs:long" />
        <xs:element name="inactiveCount" type="xs:long" />
        <xs:element name="activeSinceLastPublishedCount" type="xs:long" />
        <xs:element name="requireReviewCount" type="xs:long" />
        <xs:element name="duplicateCount" type="xs:long" />
        <xs:element name="unpublishedCount" type="xs:long" />
    </xs:sequence>
</xs:complexType>

<xs:complexType name="VnicIdListDto">
    <xs:sequence>
        <xs:element name="vnicId" type="xs:string" maxOccurs="unbounded" />
    </xs:sequence>
</xs:complexType>

<xs:complexType name="VnicInfoDto">
    <xs:sequence>
        <xs:element name="vnicId" type="xs:string" />
        <xs:element name="ipAddress" type="xs:string" />
    </xs:sequence>
</xs:complexType>

<xs:complexType name="GlobalSettingsDto">

```

```

    <xs:sequence>
      <xs:element name="status" type="OperationStatusEnum" />
      <xs:element name="mode" type="OperationModeEnum" />
      <!-- optional parameters will be part of response only -->
      <xs:element name="timestamp" type="xs:long" minOccurs="0" />
      <xs:element name="publishedBy" type="xs:string" minOccurs="0" />
    </xs:sequence>
  </xs:complexType>

  <xs:simpleType name="OperationStatusEnum">
    <xs:restriction base="xs:NCName">
      <xs:enumeration value="enabled" />
      <xs:enumeration value="disabled" />
    </xs:restriction>
  </xs:simpleType>

  <xs:simpleType name="OperationModeEnum">
    <xs:restriction base="xs:NCName">
      <xs:enumeration value="trustOnFirstUse" />
      <xs:enumeration value="manual" />
    </xs:restriction>
  </xs:simpleType>

  <xs:simpleType name="PagingSortByEnum">
    <xs:restriction base="xs:NCName">
      <xs:enumeration value="VM_NAME" />
      <xs:enumeration value="MAC" />
      <xs:enumeration value="APPROVED_IP" />
      <xs:enumeration value="CURRENT_IP" />
    </xs:restriction>
  </xs:simpleType>

</xs:schema>

```

## vShield App Namespace Schema

The following schema details namespace configuration.

```

<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" targetNamespace="vmware.vshield.global.20.namespace"
  xmlns:vsns="vmware.vshield.global.20.namespace" elementFormDefault="qualified">

  <xs:element name="VshieldConfiguration">
    <xs:complexType>
      <xs:choice>
        <xs:element maxOccurs="unbounded" name="namespace" type="vsns:NamespaceDto" />
        <xs:element maxOccurs="3" name="namespacesType" type="vsns:NamespacesTypeEnum" />
      </xs:choice>
    </xs:complexType>
  </xs:element>

  <xs:complexType name="NamespaceDto">
    <xs:sequence>
      <xs:element minOccurs="0" maxOccurs="unbounded" name="namespacePortGroup" type="vsns:PortGroupDto" />
    </xs:sequence>
    <xs:attribute name="type" use="required" type="vsns:NamespacesTypeEnum" />
    <xs:attribute name="id" use="optional" type="xs:long" />
  </xs:complexType>

  <xs:complexType name="PortGroupDto">
    <xs:sequence>
      <xs:element maxOccurs="1" name="Id" type="xs:string" />
    </xs:sequence>
  </xs:complexType>

  <xs:simpleType name="NamespacesTypeEnum">
    <xs:restriction base="xs:NCName">
      <xs:enumeration value="DEFAULT" />
    </xs:restriction>
  </xs:simpleType>

```

```

<xs:enumeration value="PORTGROUP" />
<xs:enumeration value="NONE" />
</xs:restriction>
</xs:simpleType>

</xs:schema>Retrieved from "https://wiki.eng.vmware.com/NS_DEV/vShieldManager/VSM30/App/ipad/xsd"

```

## Error Message Schema

This schema details error messages.

```

<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">

  <xs:element name="Errors">
    <xs:complexType>
      <xs:sequence>
        <xs:element maxOccurs="unbounded" name="Error" type="ErrorType"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>

  <xs:complexType name="ErrorType">
    <xs:sequence>
      <xs:element name="code" type="xs:unsignedInt"/>
      <xs:element name="description" type="xs:string"/>
      <xs:element minOccurs="0" name="detailedDescription" type="xs:string"/>
      <xs:element minOccurs="0" name="index" type="xs:int"/>
      <xs:element minOccurs="0" name="resource" type="xs:NMTOKEN"/>
      <xs:element minOccurs="0" name="requestId" type="xs:NMTOKEN"/>
      <xs:element minOccurs="0" name="module" type="xs:NMTOKEN"/>
    </xs:sequence>
  </xs:complexType>

</xs:schema>

```

If a REST API call results in an error, the HTTP reply contains the following information.

- An XML error document as the response body
- Content-Type: application/xml
- An appropriate 2xx, 4xx, or 5xx HTTP status code

**Table 11-1.** Error Message Status Codes

Code	Description
200 OK	The request was valid and has been completed. Generally, this response is accompanied by a body document (XML).
201 Created	The request was completed and new resource was created. The Location header of the response contains the URI of newly created resource.
204 No Content	Same as 200 OK, but the response body is empty (No XML).
400 Bad Request	The request body contains an invalid representation or the representation of the entity is missing information. The response is accompanied by Error Object (XML).
401 Unauthorized	An authorization header was expected. Request with invalid or no vShield Manager Token.
403 Forbidden	The user does not have enough privileges to access the resource.
404 Not Found	The resource was not found. The response is accompanied by Error Object (XML).
500 Internal Server Error	Unexpected error with the server. The response is accompanied by Error Object (XML).
503 Service Unavailable	Cannot proceed with the request, because some of the services are unavailable. Example: vShield Edge is Unreachable. The response is accompanied by Error Object (XML).



# Index

## A

AESNI setting, vShield Edge **141**

appliance

change size **67**

delete specific appliance **69**

modify configuration **67**

modify configuration of specific appliance **68**

auto configuration setting, vShield Edge **142**

## C

certificates

certificate revocation list (CRL) **95**

certificate signing requests (CSRs) **94**

self-signed certificates **93**

CLI remote access, change for vShield Edge **147**

CLI setting, change for vShield Edge **147**

## D

Data Security

scanning **210**

datacenter, modify state **171**

DHCP

about **89**

append pool **92**

append static binding **92**

delete configuration **91**

delete pool **93**

delete static binding **93**

query configuration **91**

query lease information **92**

DNS

configure **87**

delete configuration **88**

query configuration **88**

query statistics **89**

## E

ESX host preparation **47**

## F

FIPS setting, vShield Edge **142**

firewall

vShield App

about **172**

add rule **178**

change configuration **178, 180, 182**

delete rule **182**

fail safe mode **183**

modify rule **180**

query configuration **172**

revert to default configuration **183**

vShield Edge

about **75**

add configuration **75**

add rule above specific rule **78**

append rules **78**

delete configuration **77**

delete rule **80**

manage default policy **80**

modify rule **79**

query configuration **76**

query firewall statistics **81**

query specific rule **79**

flow statistics

about **187**

query **187**

force sync

vShield App **192**

vShield Edge **141**

## H

high availability

about **140**

delete configuration **141**

query configuration **141**

## I

installation

Port Group Isolation **47**

status **50**

vShield App **47**

vShield Edge **51**

vShield Endpoint **47**

interface

add **69**

delete **71**

manage a specific interface **71**

query **70**

query statistics **72**

## L

Load Balancer

about **129**

delete configuration **133**

L-4 mode **140**

- manage all virtual servers **136**
- manage backend pools **133**
- manage specific virtual server **137**
- query configuration **131**
- query statistics **132**
- logging level, vShield Edge **142**

## N

- namespace

- about **186**
- add **186**
- delete **186**
- query **186**

- NAT

- about **81**
- add rule above a specific rule **83**
- append rules **84**
- delete rule **84**
- modify rule **84**
- query rules **82, 83**

## P

- Port Group Isolation

- uninstall **50**

- preparing the ESX host **47**

## Q

- query

- active clients **119**
- advanced configuration **119**
- all private network **102**
- appliance configuration **66**
- authentication configuration **118**
- auto configuration setting **142**
- certificates **94**
- client installation package **112**
- configuration of specific appliance **68**
- CRL **95**
- CSR **95**
- default firewall policy **80**
- firewall statistics **81**
- high availability configuration **141**
- IP pool **108**
- IPSec configuration **97**
- IPSec statistics **98**
- IPSec tunnel traffic statistics **99**
- Load Balancer backend pool details **134**
- Load Balancer configuration **131**
- Load Balancer statistics **132**
- namespace **186**
- portal layout **116**
- portal web resource **104**
- script configuration **121**

- server settings **101**
- specific private network **102**
- specific vShield instance
  - vShield Edge details **58**
  - vShield Edge status **64**
  - vShield Edge summary **62**
- spoofguard IP settings **185**
- spoofguard settings **184**
- SSL configuration **125**
- SSL VPN details **100**
- user details **106**
- vShield App firewall configuration **172**
- vShield App flow statistics **187**
- vShield App status **193**
- vShield Edge interfaces **70**
- vShield Edge service statistics **149**
- vShield Edge tech support log **149**

## R

- redeploy appliance, vShield Edge **147**
- replace configuration, vShield Edge **143**
- return status codes **200**

- routing

- append static routes **86**
- change static routes **86**
- configure **85**
- configure default routes **87**
- delete **86**
- delete default routes **87**
- delete static routes **87**
- query **85**

## S

- spoofguard

- about **184**
- change settings **185**
- query IP settings **185**
- query settings **184**
- replace settings **184**

- status

- Port Group Isolation installation **50**
- vShield App installation **50**
- vShield Endpoint installation **50**

- status return codes **200**

- SVM

- get network info **198**
- registering with vShield Endpoint **196**
- retrieve status **197**
- unregistering **199**

- syslog server, vShield App **191**

## T

- TCP loose setting, vShield Edge

- vShield Edge
  - TCP loose setting **143**
- tech support log
  - vShield App **192**
  - vShield Edge **149**
  - vShield Manager **24**
- U**
- uninstallation
  - Port Group Isolation **50**
  - vShield App **50**
  - vShield Edge **55**
  - vShield Endpoint **50, 199**
- unregistering a vShield Endpoint SVM **199**
- upgrade
  - vShield App **193**
  - vShield Edge **55**
- V**
- VPN
  - IPSec
    - configure **96, 100**
    - query configuration **97**
    - query statistics **98**
    - query tunnel traffic statistics **99**
  - SSL
    - active clients **119**
    - configure authentication parameters **116**
    - configure IP pool **107**
    - configure network extension client parameters **110**
    - configure portal layout **114**
    - configure private networks **101**
    - configure users **105**
    - configure web resource **103**
    - enable **100**
    - logon and logoff scripts **120**
    - manage server settings **100**
    - query details **100**
    - reconfigure **122**
- vShield App
  - about **13**
  - datacenter, modify state **171**
  - exclude virtual machines **190**
  - fail safe mode **183**
  - firewall
    - about **172**
    - add rule **178**
    - change configuration **178, 180, 182**
    - delete rule **182**
    - modify rule **180**
    - query configuration **172**
    - revert to default configuration **183**
  - flow statistics
    - about **187**
    - query **187**
  - force sync **192**
  - install **47**
  - namespace
    - about **186**
    - add **186**
    - delete **186**
    - query **186**
  - query status **193**
  - spoofguard
    - about **184**
    - change settings **185**
    - query IP settings **185**
    - query settings **184**
    - replace settings **184**
  - syslog server **191**
  - tech support log **192**
  - uninstall **50**
  - upgrade **193**
- vShield Edge
  - about **14**
  - AESNI setting **141**
  - appliance
    - change size **67**
    - delete specific appliance **69**
    - modify configuration **67**
    - modify configuration of specific appliance **68**
    - query configuration **66**
  - auto configuration setting **142**
  - certificates
    - certificate revocation list (CRL) **95**
    - certificate signing requests (CSRs) **94**
    - self-signed certificates **93**
  - CLI remote access change **147**
  - CLI setting change **147**
  - DHCP
    - about **89**
    - append pool **92**
    - append static binding **92**
    - delete configuration **91**
    - delete pool **93**
    - delete static binding **93**
    - query configuration **91**
    - query lease information **92**
  - DNS
    - configure **87**
    - delete configuration **88**
    - query configuration **88**
    - query statistics **89**
  - FIPS setting **142**
  - firewall
    - about **75**
    - add configuration **75**
    - add rule above specific rule **78**
    - append rules **78**
    - delete configuration **77**
    - delete rule **80**

- manage default policy **80**
  - modify rule **79**
  - query configuration **76**
  - query firewall statistics **81**
  - query specific rule **79**
- force sync **141**
- high availability
  - about **140**
  - delete configuration **141**
  - query configuration **141**
- installation **51**
- interface
  - add **69**
  - delete **71**
  - manage a specific interface **71**
  - query **70**
  - query statistics **72**
- Load Balancer
  - about **129**
  - delete configuration **133**
  - manage all virtual servers **136**
  - manage backend pools **133**
  - manage specific virtual server **137**
  - query configuration **131**
  - query statistics **132**
- logging level **142**
- NAT
  - about **81**
  - add rule above a specific rule **83**
  - append rules **84**
  - delete rule **84**
  - modify rule **84**
  - query rules **82, 83**
- query
  - all instances **53**
  - appliance configuration **66**
  - configuration of specific appliance **68**
  - specific vShield Edge details **58**
  - specific vShield Edge status **64**
  - specific vShield Edge summary **62**
- query service statistics **149**
- redeploy appliance **147**
- replace configuration **143**
- routing
  - append static routes **86**
  - change static routes **86**
  - configure **85**
  - configure default routes **87**
  - delete **86**
  - delete default routes **87**
  - delete static routes **87**
  - query **85**
- support log **149**
- uninstallation **55**
- upgrading **55**
- VPN
  - IPSec

- configure **96, 100**
- query configuration **97**
- query statistics **98**
- query tunnel traffic statistics **99**

## SSL

- active clients **119**
- authentication parameters **116**
- configure IP pool **107**
- configure private networks **101**
- configure users **105**
- configure web resource **103**
- enable **100**
- logon and logoff scripts **120**
- manage server settings **100**
- network extension client parameters **110**
- portal layout **114**
- query details **100**
- reconfigure **122**

## vShield Endpoint

- about **14**
- error schema **200**
- get SVM network info **198**
- install **47**
- managing **195**
- registering an SVM **196**
- retrieve SVM status **197**
- uninstall **50**
- uninstalling **199**
- unregistering an SVM **199**

## vShield Manager

- about **13**
- configure DNS **19**
- sync with vCenter **19**
- tech support log **24**

## VXLAN virtual wire

- cluster switch mapping **156**
- create **166**
- EAM agency **158**
- multicast address range **162**
- multicast group connectivity **169**
- network scope **164**
- ping test **170**
- prepare for **153**
- query allocated resources **169**
- segment IDs **160**
- switches **154**
- UDP port **168**









