

DEPLOYMENT GUIDE

SparkView Configuration Guide for FortiGate NGFW V7.0.1



Table of Content

- Overview 3
 - System-side entry/bookmark on the SSL-VPN portal 3
 - System-side entry/bookmark on the SSL-VPN portal with SSO 5
 - Direct redirection to SparkView after successful registration 7
- Supported FortiGate Models 9



Overview

These instructions describe the example configuration of a FortiGate NGFW in conjunction with SparkView. The name “FortiGate NGFW” is the property of Fortinet.

System-side entry/bookmark on the SSL-VPN portal

The user should find the link to SparkView on the SSL-VPN portal after successful authentication at FortiGate.

1. Configure SSL settings.

The screenshot displays the FortiGate web interface for configuring SSL-VPN settings. The left sidebar shows the navigation menu with 'VPN' expanded and 'SSL-VPN Settings' selected. The main content area is titled 'SSL-VPN Settings' and is divided into several sections:

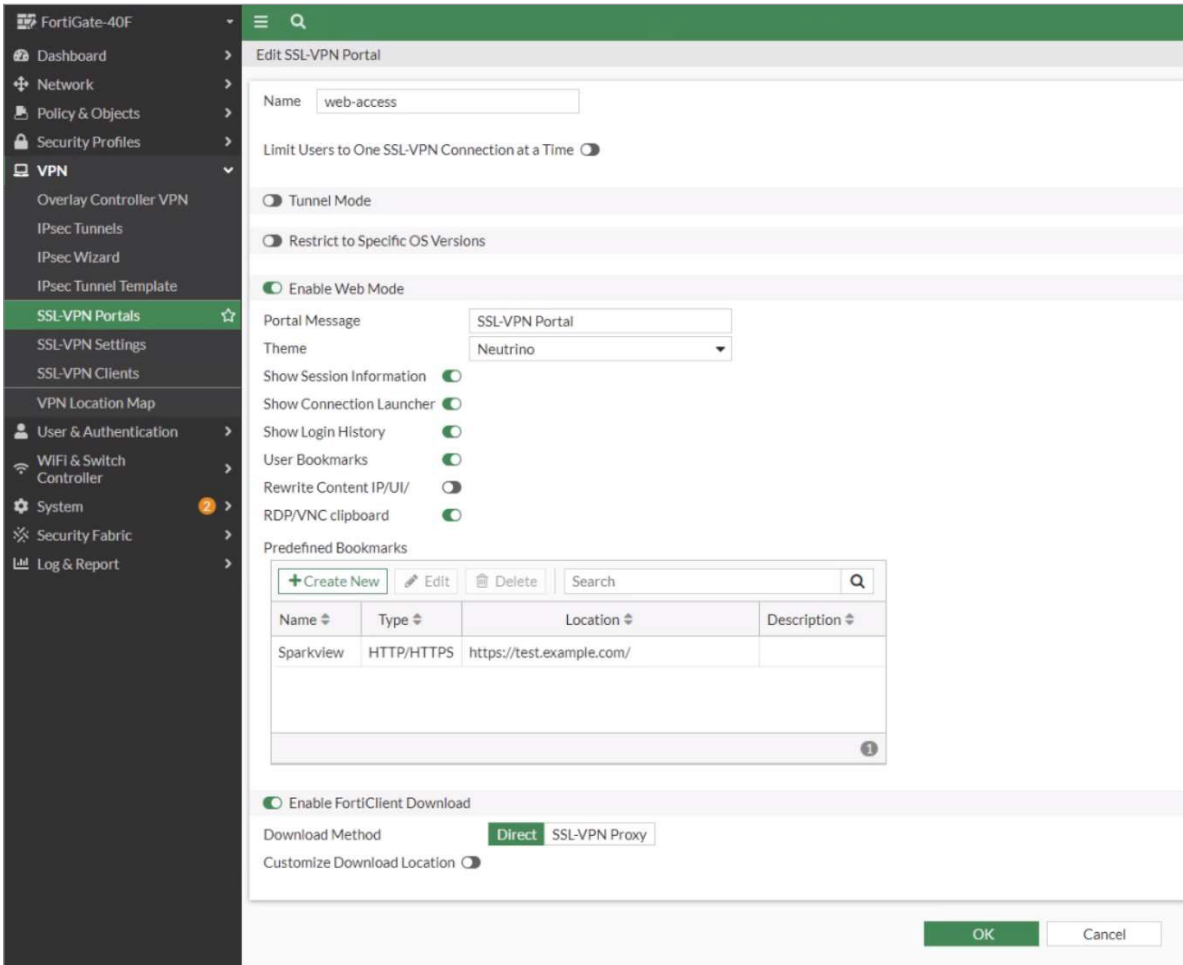
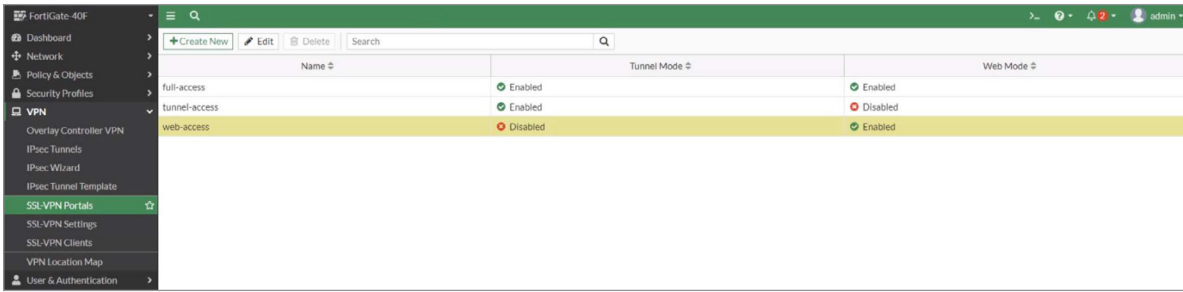
- Connection Settings:** Includes 'Enable SSL-VPN' (checked), 'Listen on Interface(s)' (wan), and 'Listen on Port' (8080). A blue information box states: 'Web mode access will be listening at https://172.26.5.223:8080'.
- Redirect HTTP to SSL-VPN:** A toggle switch is turned off.
- Restrict Access:** Two radio buttons are present: 'Allow access from any host' (selected) and 'Limit access to specific hosts'.
- Idle Logout:** Includes 'Inactive For' (300 Seconds) and 'Server Certificate' (Fortinet_Factory). A yellow warning box states: 'You are using a default built-in certificate, which will not be able to verify your server's domain name (your users will see a warning). Let's Encrypt can be used to easily generate a trusted certificate if you do not have one. To do this simply import a new local certificate and select type "Automated". Click here to learn more'.
- Require Client Certificate:** A toggle switch is turned off.
- Tunnel Mode Client Settings:** Includes 'Address Range' (Automatically assign addresses selected), 'DNS Server' (Same as client system DNS selected), and 'Specify WINS Servers' (turned off). A blue information box states: 'Tunnel users will receive IPs in the range of 10.212.134.200 - 10.212.134.210'.
- Authentication/Portal Mapping:** A table with buttons for '+ Create New', 'Edit', 'Delete', and 'Send SSL-VPN Configuration'. The table contains one entry:

Users/Groups	Portal
All Other Users/Groups	web-access

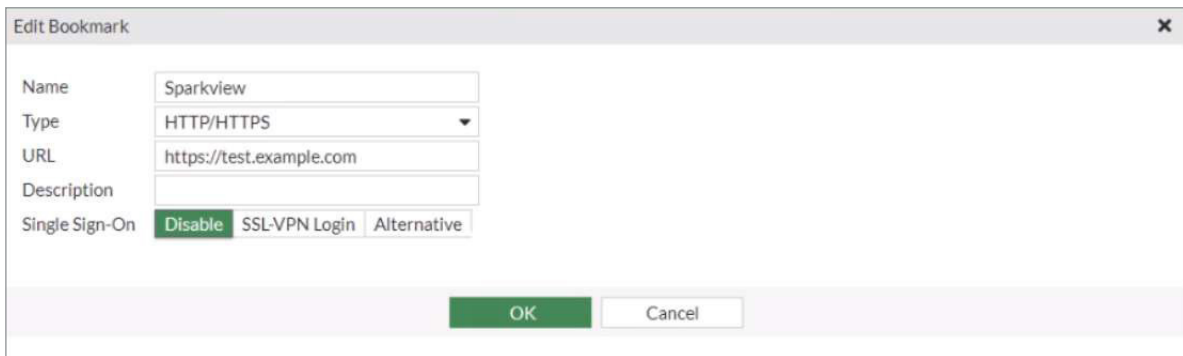
The screenshot shows a dialog box titled 'Edit Default Authentication/Portal Mapping'. It contains two dropdown menus: 'Users/Groups' is set to 'All Other Users/Groups' and 'Portal' is set to 'web-access'. At the bottom of the dialog, there are two buttons: 'OK' and 'Cancel'.



2. Select the web portal.

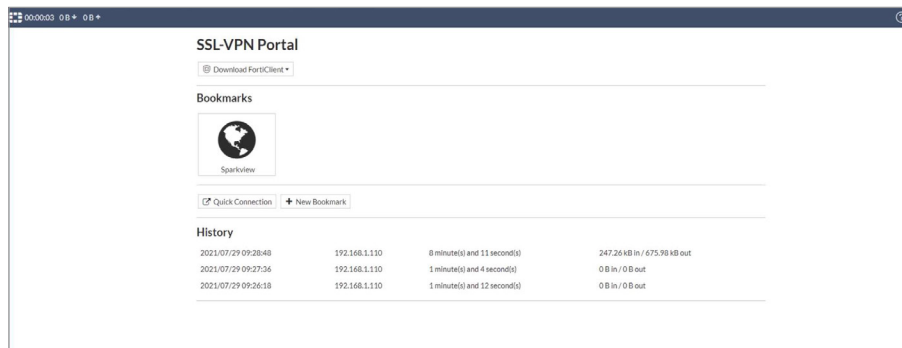


3. Configure the bookmark in the selected portal.





4. Log in to the SSL portal.



System-side entry/bookmark on the SSL-VPN portal with SSO

The user should find the link to SparkView on the SSL-VPN portal after successful authentication at FortiGate. When calling up SparkView, the user should be automatically logged on to SparkView with his login data (single sign-on).

Name	Tunnel Mode	Web Mode
full-access	Enabled	Enabled
tunnel-access	Enabled	Disabled
web-access	Disabled	Enabled

The portal used has the name “web-access” and is then configured via the CLI.

CLI configuration for SSO:

```

CLI Console (2)
FortiGate-40F # config ssl vp
command parse error before 'ssl'

FortiGate-40F # config vpn ssl web portal

FortiGate-40F (portal) # edit web-access
FortiGate-40F (web-access) # set hide-sso-credential disable
FortiGate-40F (web-access) # end

FortiGate-40F #
    
```



Edit Bookmark ✕

Name:

Type:

URL:

Description:

Single Sign-On: Disable **SSL-VPN Login** Alternative

SSO Form Data:

Please Login

SSL-VPN Portal

Bookmarks

Sparkview

History

2021/07/29 09:28:48	192.168.1.110	8 minute(s) and 11 second(s)	247.26 kB in / 675.98 kB out
2021/07/29 09:27:36	192.168.1.110	1 minute(s) and 4 second(s)	0 B in / 0 B out
2021/07/29 09:26:18	192.168.1.110	1 minute(s) and 12 second(s)	0 B in / 0 B out

Spark View ✕

← → 🏠 🔍 🔧 👤

My Computers and Programs:

Back Remote Desktop

Desktop

Writer

Office

Calc

Finos

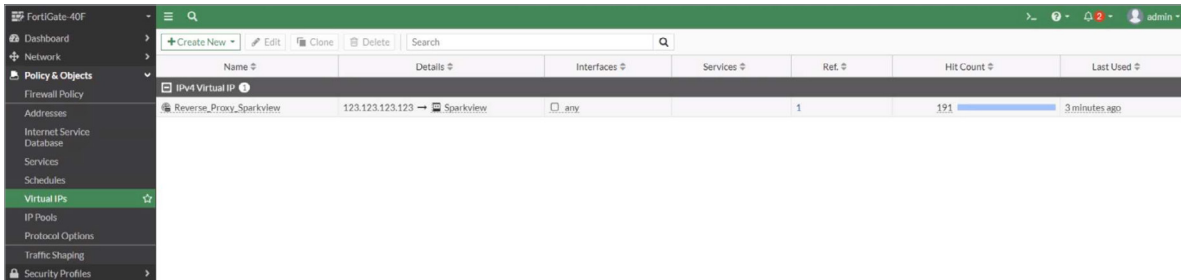
Touchpad mode(Relative mouse movement)
 German (Germany) Open in existing window Use multiple monitors

Copyright © Remote Spark Corp. 2011 - 2021 www.remotespark.com

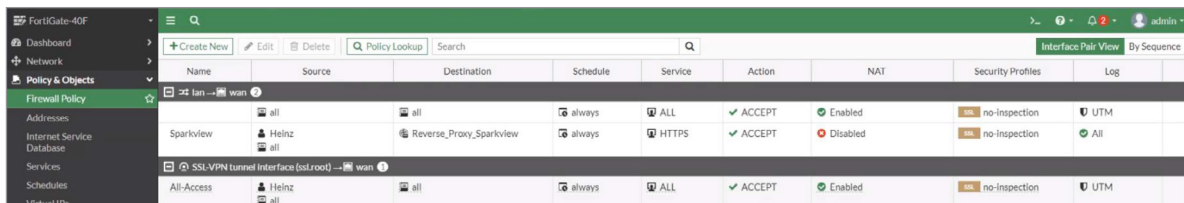
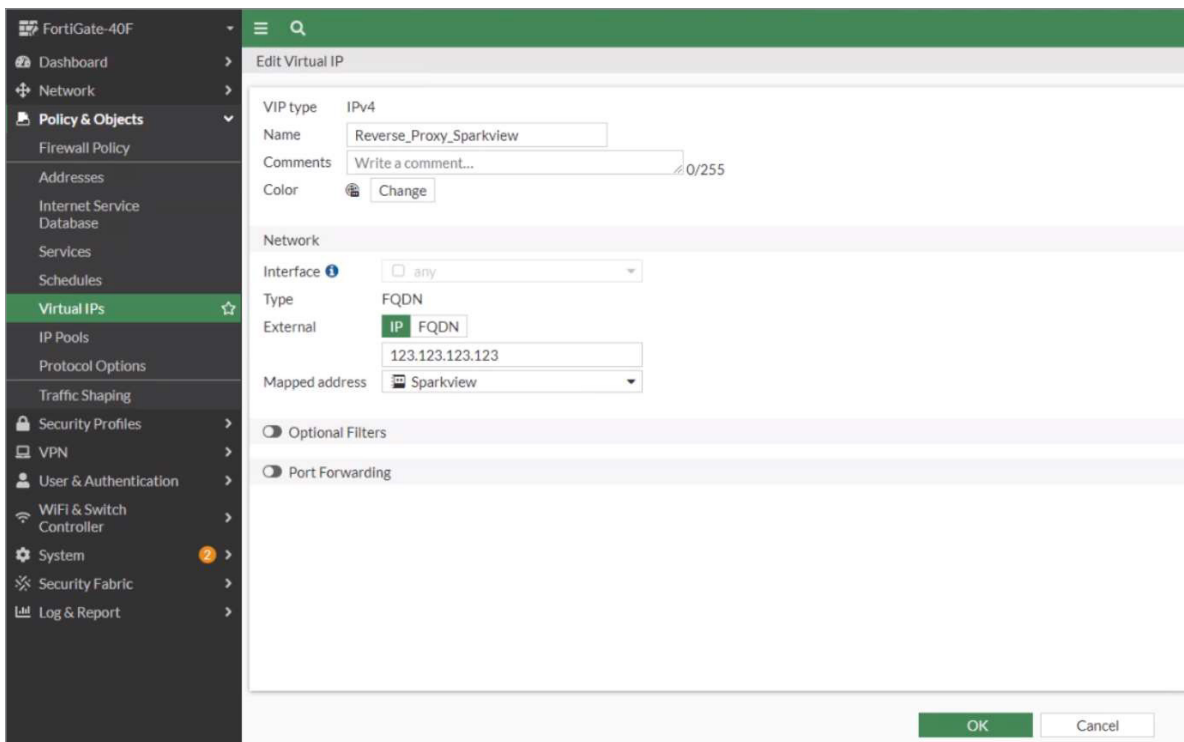


Direct redirection to SparkView after successful registration

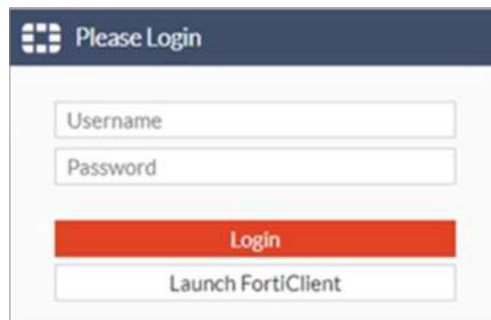
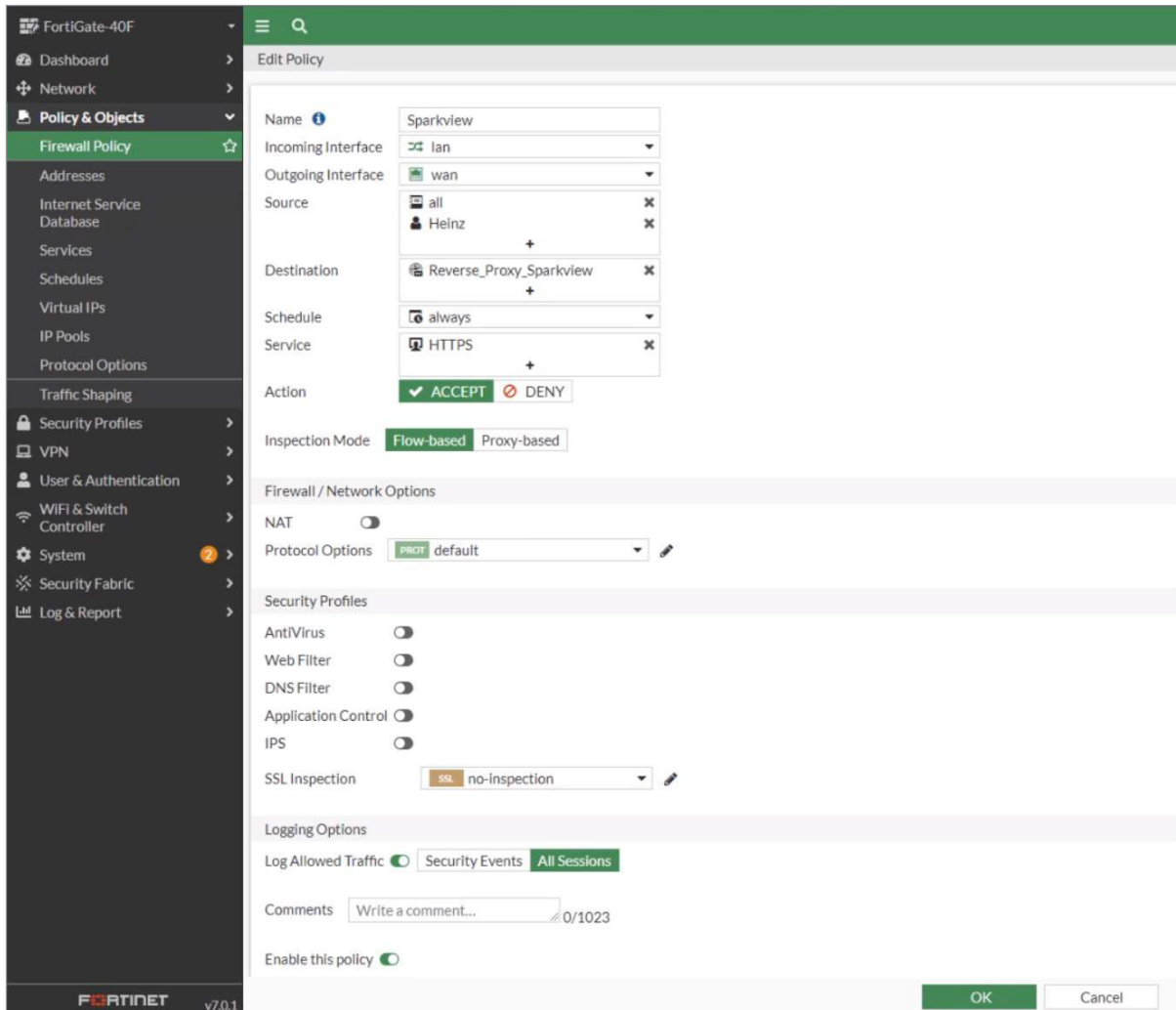
After successful authentication at the FortiGate, the user should be forwarded directly to the SparkView portal login. This is done by forwarding the public IP address to the SparkView server in the local network. An example is shown below using images.

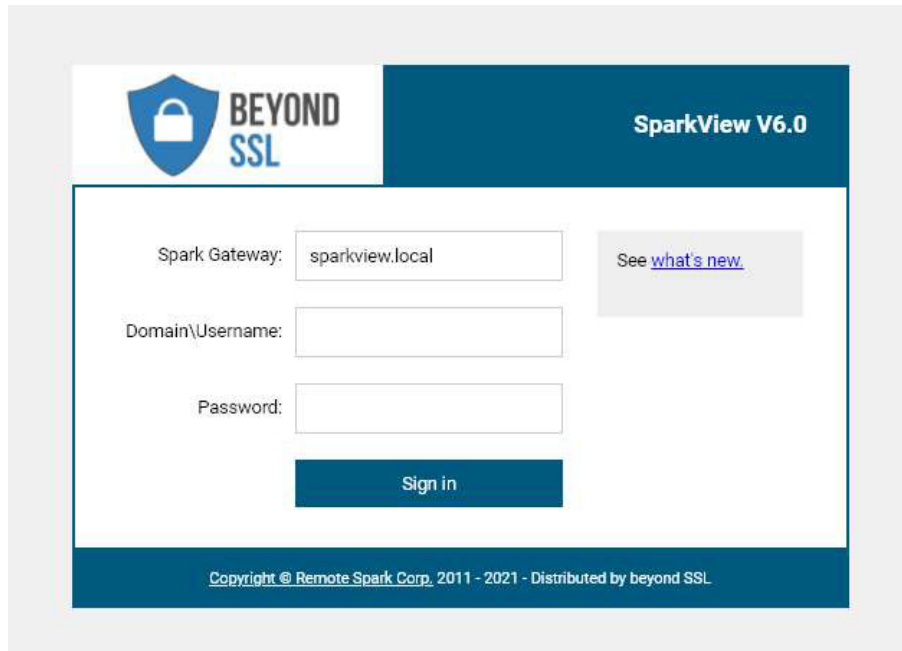


Setting up the forwarding of the public IP-address to the internal IP-address:



Creation of the policy, which activates the NAT. In addition, a locally created user is stored for authentication against the firewall, so that not everyone simply ends up on the SparkView portal. (Radius/LDAP users can also be stored.)





Supported FortiGate Models

This guide provides release information for FortiOS 7.0.1 build 0157.

For FortiOS documentation, see the [Fortinet Document Library](#).

FortiOS 7.0.1 supports the following models:

FortiGate	FG-40F, FG-40F-3G4G, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-80E, FG-80E-POE, FG-80F, FG-80F-BP, FG-81E, FG-81E-POE, FG-81F, FG-90E, FG-91E, FG-100E, FG-100EF, FG-100F, FG-101E, FG-101F, FG-140E, FG-140E-POE, FG-200E, FG-201E, FG-300E, FG-301E, FG-400E, FG-400E-BP, FG-401E, FG-500E, FG-501E, FG-600E, FG-601E, FG-800D, FG-900D, FG-1000D, FG-1100E, FG-1101E, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3600E, FG-3601E, FG-3700D, FG-3800D, FG-3960E, FG-3980E, FG-5001E, FG-5001E1
FortiWiFi	FWF-40F, FWF-40F-3G4G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F
FortiGate Rugged	FGR-60F, FGR-60F-3G4G
FortiGate VM	FG-VM64, FG-VM64-ALI, FG-VM64-AWS, FG-VM64-AZURE, FG-VM64-GCP, FG-VM64-HV, FG-VM64-IBM, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, FG-VM64-SVM, FG-VM64-VMX, FG-VM64-XEN
Pay-as-you-go images	FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-XEN