FORTINET

Azure Administration Guide

FortiSRA 1.6.0

FORTINET DOCUMENT LIBRARY

https://docs.fortinet.com

FORTINET VIDEO LIBRARY

https://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com
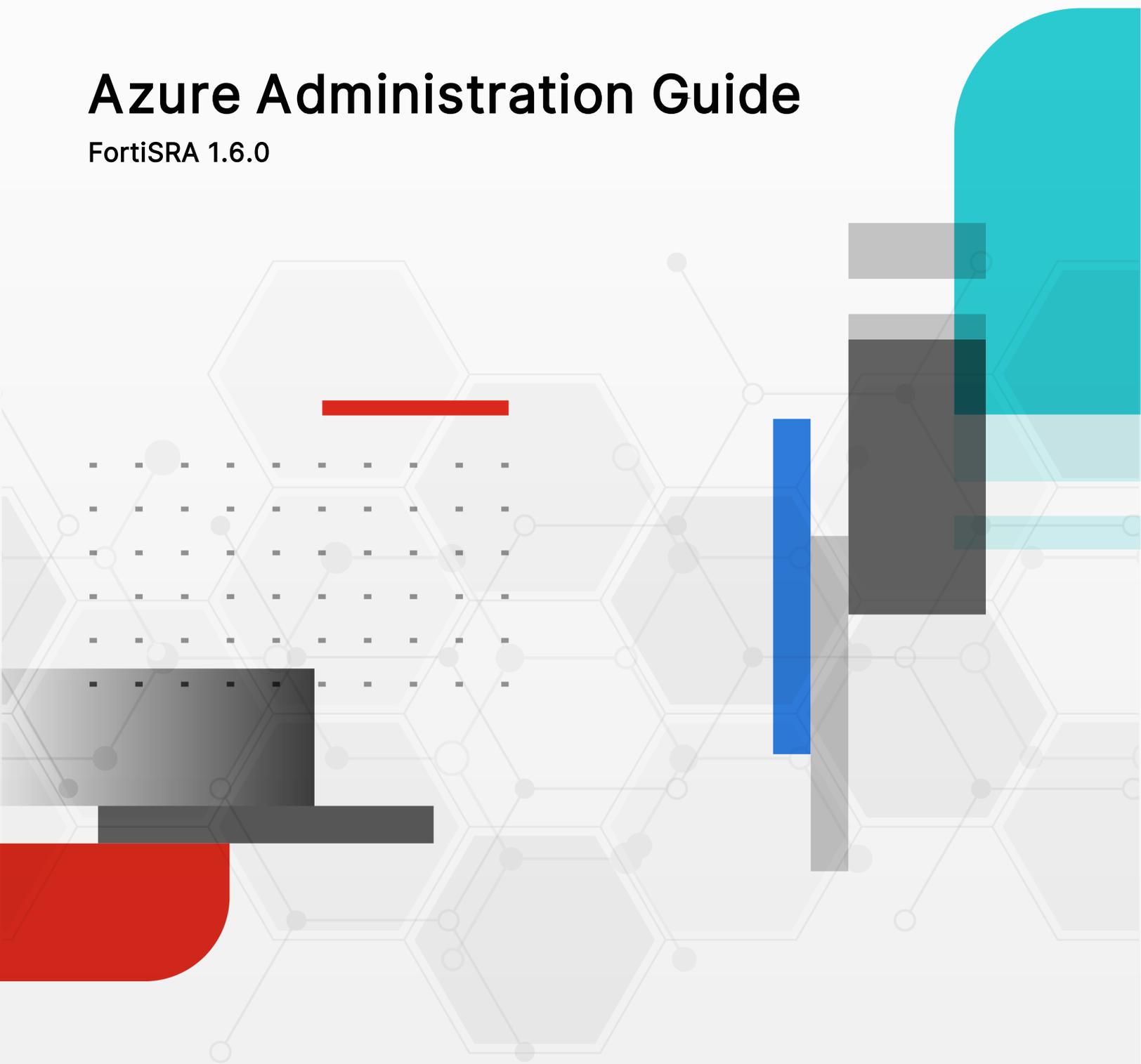
CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM

https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE

https://training.fortinet.com

FORTIGUARD LABS

https://www.fortiguard.com

END USER LICENSE AGREEMENT

https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdoc@fortinet.com

TABLE OF CONTENTS

Change Log

Date	Change Description
2025-05-06	Initial release.

Introduction

FortiSRA is an agentless secure remote access solution for OT environments. FortiSRA solutions are an important part of an enterprise network, providing role-based access, auditing, and security options for privileged users (users that have system access beyond that of a regular user).

For information on FortiSRA features, see the latest *FortiSRA Administration Guide*.

This document includes an overview of the FortiSRA-VM, its deployment with Azure, and information on how to perform an initial configuration.

FortiSRA-VM Overview

This section provides an overview of FortiSRA-VM.

The following topics are included in this section:

Licensing

Fortinet offers FortiSRA in a yearly user subscription model.

Contact your Fortinet Authorized Reseller for more information.

Virtualization environment supported:
- Azure

FortiSRA-VM support options:

SKU	Description
FC1-10-RAVUL-687-02-12	One year subscription for one FortiSRA Virtual Machine seat for 5 to 9 users. • Includes FortiClient VRS agent for FortiSRA. • Includes 24/7 FortiCare support. **Note**: HA requires additional license.
FC2-10-RAVUL-687-02-12	One year subscription for one FortiSRA Virtual Machine seat for 10 to 24 users. • Includes FortiClient VRS agent for FortiSRA. • Includes 24/7 FortiCare support. **Note**: HA requires additional license.
FC3-10-RAVUL-687-02-12	One year subscription for one FortiSRA Virtual Machine seat for 25 to 49 users. • Includes FortiClient VRS agent for FortiSRA. • Includes 24/7 FortiCare support. **Note**: HA requires additional license.
FC4-10-RAVUL-687-02-12	One year subscription for one FortiSRA Virtual Machine seat for 50 to 99 users. • Includes FortiClient VRS agent for FortiSRA. • Includes 24/7 FortiCare support. **Note**: HA requires additional license.

SKU	Description
FC5-10-RAVUL-687-02-12	One year subscription for one FortiSRA Virtual Machine seat for 100 to 249 users. • Includes FortiClient VRS agent for FortiSRA. • Includes 24/7 FortiCare support. **Note**: HA requires additional license.
FC6-10-RAVUL-687-02-12	One year subscription for one FortiSRA Virtual Machine seat for 250 or more users. • Includes FortiClient VRS agent for FortiSRA. • Includes 24/7 FortiCare support. **Note**: HA requires additional license.

Note: The SKUs are user license/seats for different pricing level.

After placing an order for FortiSRA-VM, a license registration code is sent to the email address used in the order form. Use the license registration code provided to register the FortiSRA-VM with FortiCloud.

Upon registration, you can download the license file. You will need this file to activate your FortiSRA-VM. For more information on configuring basic network settings and applying your license, see the *FortiSRA Administration Guide*.

System requirements

Prior to deploying the FortiSRA-VM virtual appliance, your virtual machine manager must be installed and configured. The installation instructions for FortiSRA-VM assume you are familiar with both VM platforms and their related terminology. FortiSRA-VM includes support for:

• Azure

For the latest information on virtualization software support, see the corresponding *FortiSRA Release Notes* on the Fortinet Docs Library.

⚠	Upgrade to the latest stable server update and patch release.

VM requirements

The following table provides a detailed summary on FortiSRA virtual machine (VM) system requirements. Installing FortiSRA-VM requires that you have already installed a supported VM environment.

Virtual machine	Requirement
Virtual CPUs supported (maximum)	256

Virtual machine	Requirement
Virtual NICs supported (maximum)	10
Storage support (maximum)	16 TB
Memory support (minimum)	2 GB
High Availability (HA) support	Yes (Active-Passive HA)

FortiSRA-VM sizing guidelines

The following table provides FortiSRA-VM sizing guidelines based on typical usage. Actual requirements may vary based on usage patterns.

Users	Virtual CPUs	Memory	Storage
20 - 1000	4 - 64	16 GB to 256 GB	2 TB to 16 TB

Log and video disk size guidelines

The following tables provide FortiSRA log and video disk sizing guidelines.

Disk	Requirement
Log (minimum)	10 GB
Video (minimum)	10 GB

Video length	Video file size
1 hour	250 MB

Video disk size should be planned according to the number of video recording sessions and the duration of each session.

For example: If, on average, there are 100 one-hour launching sessions with video recording enabled every day, 25 GB (250 MB x 100) video files are added to the video disk.

For the log disk size, we recommend log and video disk ratio should be 1:3. For example, if the video disk size is 2 TB, log disk size should be 700 GB.

Register FortiSRA-VM on FortiCloud

To obtain the FortiSRA-VM license file you must first register your FortiSRA-VM on FortiCloud.

To register your FortiSRA-VM:

1. Go to the FortiCloud portal and create a new account or log in with an existing account.
   The *Asset Management* portal opens.
2. In *Asset Management*, select *Register Now* to register FortiSRA.
3. Provide your registration code:
   a. Enter your product serial number, service contract registration code, or license certificate number.
   b. Choose your end user type as either a government or non-government user.
   c. Click *Next*.
4. The *Fortinet Product Registration Agreement* page displays. Select the check box to indicate that you have read, understood, and accepted the service contract. Click *Next*.
5. The *Verification* page displays. Select the checkbox to indicate that you accept the terms. Click *Confirm*.
   Registration is now complete and your registration summary is displayed.
6. On the *Registration Complete* page, download the license file (`.lic`) to your computer.
   You will upload this license to activate the FortiSRA-VM.

⚠️	After registering a license, Fortinet servers can take up to 30 minutes to fully recognize the new license. When you upload the license file to activate the FortiSRA-VM, if you get an error that the license is invalid, wait 30 minutes and try again.

Download the FortiSRA-VM software

Fortinet provides the FortiSRA-VM software for 64-bit environments in two formats:

Upgrades: Download this firmware image to upgrade your existing FortiSRA-VM installation.

- FRA_AZURE-v1xx-build0xxx-FORTINET.out

New Installations: Download for a new FortiSRA-VM installation.

- FRA_AZURE-v1xx-build0xxx-FORTINET.out.hyperv.zip

For more information see the FortiSRA product datasheet available on the Fortinet web site.

Azure deployment package contents

The **FRA_AZURE-v1xx-build0xxx-FORTINET.out.hyperv.zip** file contains the following hard disk image file:

- fortisra: FortiSRA system disk format file used by the OVF file.

FortiSRA-VM firmware images in the FortiCloud FTP directory are organized by firmware version, major release, and patch release. The firmware images in the directories follow a specific naming convention and each firmware image is specific to the device model. For example, the FRA_VMWARE-v100-build0012-FORTINET.out.ovf.zip image found in the v1.0 directory is specific to the FortiSRA-VM VMware environment.

💡	You can download the *FortiSRA Release Notes* available on the Fortinet web site.

To download the FortiSRA-VM .zip package:

1. Log into FortiCloud.
2. Go to *Support > Downloads*, and select *Firmware Download* from the dropdown list.
   The *Firmware Images* page opens.
3. In the *Firmware Images* page, select *FortiSRA*.
4. On the *Download* tab, browse to the appropriate directory in the FTP site for the version that you would like to download.
5. Download the Azure `hyperv.zip` file and *FortiSRA Release Notes*, and save these files to your management computer. Select the `.zip` file on your management computer and extract the files to a new file folder.

Unlicensed FortiSRA-VM

Evaluation license is not available on Azure.

DLP is available for secret launching only when you have a valid Advanced Malware Protection (`AVDB & DLP`) license.

FortiSRA-VM Deployment and Initial Configuration

The following sections detail deployments for Azure:

Deploying FortiSRA-VM on Azure from a VHD image file
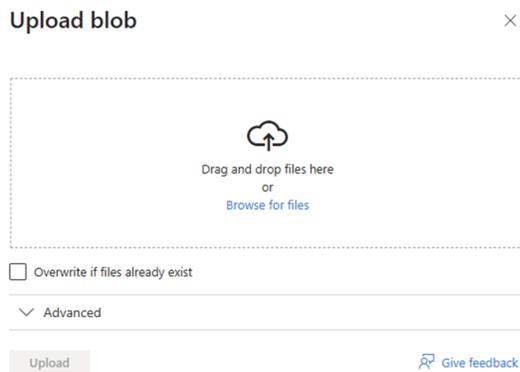
Uploading the VHD file to an Azure storage account

To upload the VHD file to an Azure storage account:

1. Unzip the `FRA_AZURE-v1xx-build0xxx-FORTINET.out.hyperv.zip` file and store the `fortisra.vhd` file on your management computer.
2. Go to your storage account on the Microsoft Azure Portal and click *Upload*.
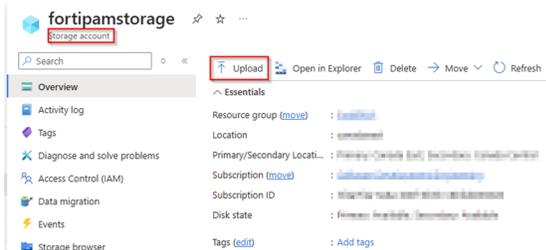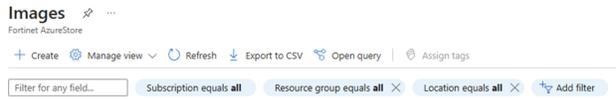

The *Upload blob* window opens.

3. Select *Browse for files* and locate the `fortisra.vhd` file that you downloaded and unzipped in step 1.
4. Click *Upload*.

Creating an image on Azure Images

To create an image:

1. Go to *Images* on the Azure Portal and select *Create*.

   The *Create an image wizard* opens.

2. From the *Resource Group* dropdown, select a resource group.
3. In *Name*, enter the name for the image.
4. In the *Region* dropdown, select a region.
5. In *OS type*, select *Linux*.
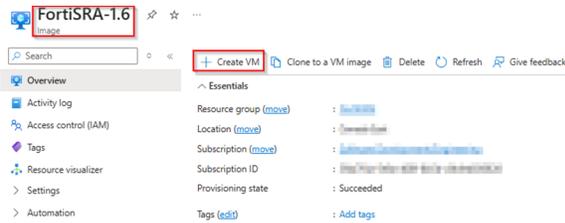6. In *VM generation*, you can select *Gen 1* or *Gen 2*.

   > Gen 1 VMs use BIOS-based architecture, whereas Gen 2 VMs use the new UEFI-based boot architecture.

7. In the *Storage* blob, click *Browse*, locate the `fortisra.vhd` file that you uploaded to your storage account, and click *Next: Tags*.
8. Optionally, in *Tags*, enter tags, and click *Next: Review + Create*.
9. Review your settings and then click Create.
   Note: The deployment may take several minutes to finish.

Create the FortiSRA-VM

To create the FortiSRA-VM:

1. On the Azure Portal, open the image you created in Creating an image on Azure Images on page 12, and click *Create VM*.

   The *Create a virtual machine wizard* opens.

   a. In *Virtual machine name*, enter a name for the VM being created.

   b. In the *Region* dropdown, select a region if the region is not automatically selected.

   c. In the *Image* dropdown, select the image created in Creating an image on Azure Images on page 12 if the image is automatically selected.

   d. In the *Size* dropdown, select a size that supports the workload you intend to perform.

2. In the *Administration* account panel:

   a. In *Authentication* type, select *Password*.

   b. In *Username*, enter a username.

   c. In *Password*, enter the password.

    d. In *Confirm password*, enter the password again to confirm.

> The account is created with the *SRA Default Admin* role on FortiSRA and does not occupy a FortiSRA license seat.

Administrator account

Authentication type ⓘ	○ SSH public key
	● Password
Username * ⓘ	azure
Password *	••••••••••••
Confirm password *	••••••••••••

3. In the *Inbound port rules* pane:

    a. In *Public inbound ports*, select *Allow selected ports*.

    b. In the *Select inbound ports* dropdown, select *HTTPS (443), SSH (22)*.

4. In the *License Type* dropdown, select *Other*, and click *Next*.

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ⓘ	○ None
	● Allow selected ports
Select inbound ports *	HTTPS (443), SSH (22)

⚠ **This will allow all IP addresses to access your virtual machine.** This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Licensing

License type *	Other

5. In *Data disks*, select *Create and attach a new disk*.

Create a disk for the log and another for the video, and click *Next*.

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. Learn more

VM disk encryption

Azure disk storage encryption automatically encrypts your data stored on Azure managed disks (OS and data disks) at rest by default when persisting it to the cloud.

Encryption at host ⓘ	☐

ⓘ Encryption at host is not registered for the selected subscription. Learn more

OS disk

OS disk size ⓘ	Image default (2 GiB)
OS disk type * ⓘ	Premium SSD (locally-redundant storage)
Delete with VM ⓘ	☐
Key management ⓘ	Platform-managed key
Enable Ultra Disk compatibility ⓘ	☐

Data disks for FSRA-Demo

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching	Delete with VM ⓘ		
0	FSRA-Demo_DataDis...	32	Premium SSD LRS	None	☑	🗑	✎
1	FSRA-Demo_DataDis...	128	Premium SSD LRS	None	☑	🗑	✎

Create and attach a new disk   Attach an existing disk

6. In the *Networking* tab:

    a. In the *Virtual network* dropdown, select a virtual network.

    b. In the *Subnet dropdown*, select a subnet.

    c. In the *Public IP dropdown*, select a public IP address or create a new public IP address.

    d. In *NIC network security group*, select *Basic*.

    e. In *Public inbound ports*, select *Allow selected ports*.

  f. In the Select inbound ports dropdown, select *HTTPS (443), SSH (22)*, and click *Next*.

7. Click *Next* and navigate through the remaining tabs.

8. Finally, review your settings and then click *Create*.
  Note: The VM deployment may take several minutes to finish.

Initial configuration

1. On the FortiSRA-VM *Networking* page, copy and save the network interface's private and public IP addresses.

2. In the VM serial console, log in as the SRA Default admin set up in step 2 in Create the FortiSRA-VM on page 13.

3. Using the following CLI commands, configure `port1`:

```
config system interface
 edit port1
   set mode static #by default, set as dhcp
   set ip 10.100.0.5/24 #set to the private IP address assigned by Azure in step 1
   set allowaccess ssh https #by default, only ssh
 next
 end
```

4. Configure a static router:

```
config router static
 edit 1
   set gateway 10.100.0.1
   set device port1
 next
 end
```

5. On a web browser, go to `https://<Public IP>` to access the FortiSRA GUI.
  Note: The public IP address was saved in step 1.

6. Log in with the SRA Default admin username and password as set up in step 2 of Create the FortiSRA-VM on page 13.
  The *FortiSRA VM license* window appears immediately after you log in.

7. In the *Upload License File* pane, select *Upload* and browse to the license file on your management computer.

8. Click *OK*.
  After the boot up, the license status changes to valid.
  You can now use your FortiSRA deployed on Azure.

Creating the *Default SRA Admin* on Azure

After performing a factory reset, the FortiSRA-VM does not come with a default admin user.

You must manually create the *Default SRA Admin* using the Azure CLI console:

1. Locate the account created when you freshly install the VM on Azure:

```
 az vm show --name <VM Name> --resource-group <resource group name> --query '
[osProfile.adminUsername]' -otsv
For example:
 PS /home/iven> az vm show --name SRAadmin --resource-group FortiPAM --query '
[osProfile.adminUsername]' -otsv azure
```

2. Create a user:

```
  az vm user update --resource-group <resource group name> --name <VM Name> --username
<admin name> --password <admin password>
For example:
  PS /home/iven> az vm user update --resource-group FortiPAM --name SRAadmin --username
azure --password QA@fortinet123
 on vm console, there will be following message. "Done" means the user is created
successfully.
SRAadmin login:
Create user azure ...
Done.
```

> The user is not created when the above message does not appear on the VM console.
>
> Rerun the CLI command on the Azure CLI console.
>
> You may need to restart Azure.

Uploading the license using SCP

To upload the license through the public IP address using SCP:

1. Use the following command:

```
 scp <license_file> admin@<public_ip_address>:vmlicense
```

For example - Example:

```
 $ scp FRAVULTM23000007.lic admin@23.99.66.210:vmlicense
 admin@23.99.66.210's password:
 FPAVULTM23000xxx.lic 100% 9128 344.0KB/s 00:00
 100-install VM license completed
```

Configure your FortiSRA-VM

Once the FortiSRA-VM license has been validated you can begin to configure your device. For more information on configuring your FortiSRA-VM see the *FortiSRA Administration Guide* on the Fortinet Document Library.

FORTINET

www.fortinet.com