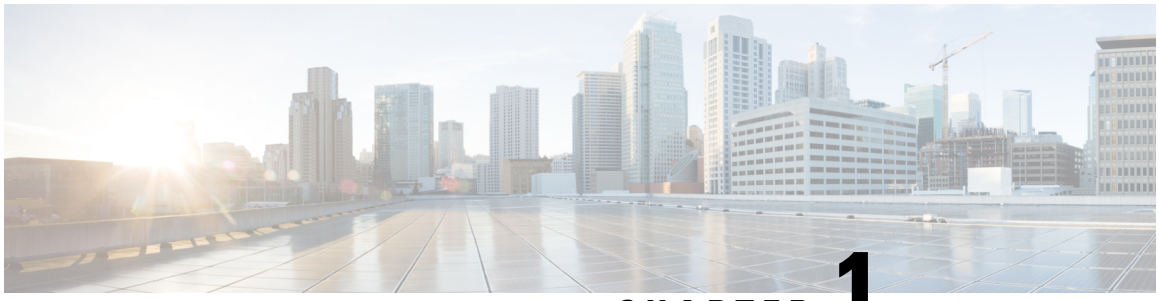
Deploy Cisco Secure Web Appliance on Microsoft Azure Marketplace

First Published: 2022-07-11

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Introduction

About Azure Marketplace

You can use an Azure image to create a virtual machine instance on Azure. Azure images for Secure Web Appliance are available in the Azure Marketplace.

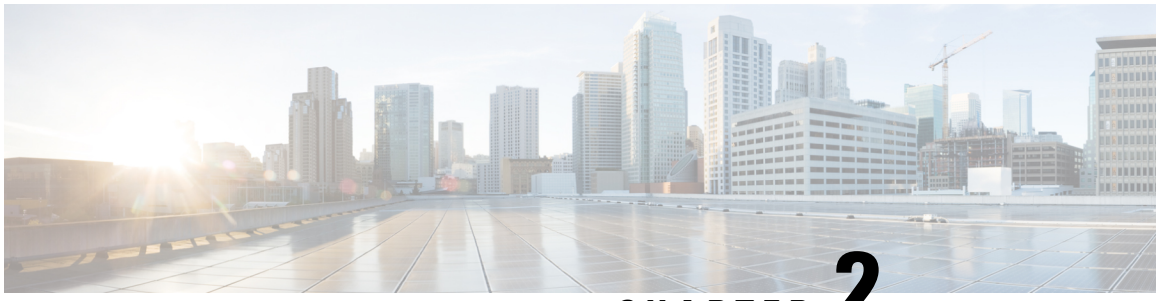
The Azure Marketplace is the premier destination for all your software needs - certified and optimized to run on Azure to provide end-to-end solutions.

Secure Web Appliance Licensing

You can use your existing Secure Web appliance license for deployments on Microsoft Azure. After you deploy and launch the instance, you can install the license. You will be required to pay only the Azure infrastructure charges.

If you are a new customer, contact your Cisco partner to obtain a license.

If you are an existing customer, see Obtain a Virtual License (VLN) in Best Practices for Virtual ESA, Virtual WSA, or Virtual SMA Licenses.



CHAPTER 2

Deploy Secure Web Appliance on Azure Marketplace

You can deploy Secure Web Appliance on Azure Marketplace using the Azure user interface and Azure CLI.

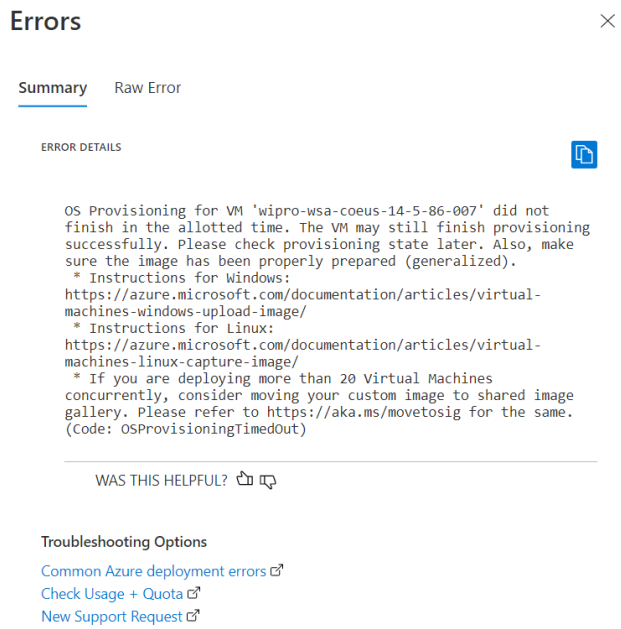
Configuration Limitations

- The following configurations are not supported to deploy Secure Web Appliance on Azure Marketplace:
  - Layer4 traffic monitor
  - Web traffic tap
- You can create multiple interfaces in the Secure Web Virtual Appliance using the Microsoft Azure CLI only.
- From the Azure user interface, Secure Web Appliance instance can be configured with only one interface.

Additional Information

- Azure instance of Secure Web Appliance does not have WAAgent support that is required to report the health status of the instance to the Azure infrastructure. Though Azure reports deployment failure (timeout) for Secure Web Appliance, the instance will be provisioned successfully. Select **Boot diagnostics** to check the current status of the virtual machine.

Figure 1: Provisioning Error



- Inbound rules are the set of rules which specify whether to allow or deny specific traffic incoming to the virtual machine.

  To change the inbound rules (access to Secure Web Appliance):

  - Select the desired VM instance under Virtual Machines.
  - Select the **Networking** option.

    Now, you can view the inbound rules getting listed against the management interface.

Note Do not delete the inbuilt three security rules that already exist.

The three default inbound rules are Azure specific services like virtual network, loadbalancer, and the service that makes all the inbound traffic block by default except the allowed ones.

- If instances are rebooted in Azure, dynamically allotted Public IPs may get changed. See https://www.linkedin.com/pulse/how-remote-desktop-centos-virtual-machine-running-azure-cretu
- Although Azure user interface supports deployment of Secure Web Appliance with a single interface, you can deploy instances with multiple interfaces using the Azure CLI.

  For deploying Azure instances with more than one interface, see Deploy Secure Web Appliance on Azure Environment using CLI, on page 9.

Deploy Secure Web Appliance on Azure Marketplace using the Azure User Interface

Note Virtual machine deployment is performed using the provisioned build available in the Azure Marketplace.

Table 1: Deploying On Azure using User Interface

	Do This	More Information
Step 1	Prepare your environment by completing prerequisite tasks and acquiring information that you require before setting up an instance in Azure.	Prepare Your Environment, on page 6
Step 2	Proceed to the Azure Marketplace and select the provisioned image for the desired build. Click **Create**.	Supported Instance Types for Deployment, on page 7.
Step 3	Select Resource Group, VM Name and Size (instance type which differs in RAM and CPU). Select Authentication type as password and License type as Other in the Azure environment.	Configure the Instance Details, on page 7
Step 4	Configure the virtual network, disk, subnet, and public IP options.	All the resources should be in the same region for the deployment.
Step 5	Create network security group. Go with the default inbound rules or add rules. If required, set **boot diagnostics** to **Yes**. Guest config is used to provide Day 0.	Configure the Instance Details, on page 7
Step 6	Create tags like Name, Group, Team, Model, and Purpose as per the requirement.	Configure the Instance Details, on page 7
Step7	Review changes and deploy the Azure instance.	Azure instance of Secure Web Appliance does not have WAAgent support that is required to report the health status of the instance to the Azure infrastructure. Though Azure reports deployment failure (timeout) for Secure Web Appliance, the instance is provisioned successfully.

	Do This	More Information
Step 8	Navigate to the instance **Overview** page, and check the status of the instance. It must be *Running*. Public IP should be assigned which can be used for logging through the console and browser.	
Step 9	• Access the Azure instance from CLI, SSH (provided, inbound rules is set to **Allow**). • Use the **loadlicense** command, and commit the change.	• See Prepare Your Environment, on page 6 for the required ports. • See Configure a Launched Instance, on page 8 for the SSH access and Web access. .
Step 10	Connect to the Secure Web Appliance's web interface. You can run the System Setup Wizard, upload a configuration file, or configure features.	Connect to the Secure Web Appliance User Interface, on page 8.
Step 11	Configure the Secure Web Appliance for license expiration alerts.	Configure the Secure Web Appliance to Send Alerts When License Expiration Nears, on page 9.

Prepare Your Environment

To deploy the Secure Web Appliance, you need the following:

- A valid license for Secure Web Virtual Appliance.
- The default username and password for the Secure Web Appliance:
  - Username—admin
  - Password—ironport

  You can change the default credentials in the System Setup Wizard configuration later.
- Resources required for the Azure deployment:
  - Resource group to which the instance belongs to
  - Virtual Network or Subnet
  - Public IP address (selected while creating the instance through user interface)
  - Network Security Group
  - Inbound and Outbound rules added to the Network Security Group
  - For the open virtual appliance to communicate, use the following ports:
    - SSH TCP 22 for SSH

- TCP 8443 UI and NGUI
- TCP 3128
- TCP 443

Supported Instance Types for Deployment

Select the instance type based on the Secure Web Appliance model.

From AsyncOS 14.5 and later, the following are the recommendations for deploying each model:

Table 2: Supported Instance Types for Deployment

Model	Maximum Interfaces	Azure
S100V 3 cores, 8GB RAM, disk 200 GB	2	Standard_F4s_v2 Standard F4s v2 has 4 vCPUs, 8 GiB RAM
S300V 5 cores, 12GB RAM, disk 500 GB	4	Standard_F8s_v2 Standard F8s v2 has 8 vCPUs, 16 GiB RAM
S600V 12 cores, 24GB RAM, disk 750GB	4	Standard_F16s_v2 Standard F16s v2 has 16 vCPUs, 32 GiB RAM

Configure the Instance Details

Step 1 Select the Resource Group.

Step 2 Enter the VM name.

Azure resource names cannot contain special characters \/""[]:|<>+=;,?*@&, whitespace, or begin with '_' or end with '.' or '-' .

Step 3 Select the Region.

This will be automatically retrieved based on the Resource Group.

Step 4 Select the image from the Azure Marketplace.

Step 5 Select the size based on the model to be deployed.

For example, the instance type F8_S_V2 is recommended for the S300V model deployment.

Step 6 Select the Authentication type as password:

Enter any strings for the Username and Password.

Note Username must not include reserved words.

But after deployment, you can access **SSH** using the default credentials:

- username—admin
- password—ironport

Step 7 Inbound ports can be SSH, HTTPS and so on.

You can change the same in the network security group.

Step 8 Choose the License type as **other**.

Step 9 Select the disks that can be SSD or HDD.

Step 10 Select the virtual network and configured subnet in the Virtual Network.

Step 11 Enable the management configuration with the custom storage account.

Step 12 Add tags, then review, and create the VM instance.

Configure a Launched Instance

Step 1 In the search bar, filter for a virtual machine.

Step 2 Select a virtual machine and search for the VM name.

The virtual machine should be running with the retrieved public IP address.

Step 3 Configure the customized DNS name.

Step 4 Add the required IP addresses to the inbound rules for security to the required ports.

Step 5 Use an SSH to connect to an instance using the following credentials:

- username—admin
- password—ironport

Step 6 Add the feature keys, if required.

Step 7 Use the **loadlicense** command, to paste the license through the CLI, or load from a file.

Note While deploying VM in Azure, there is no provision to select number of CPUs. The only option available is to select the set of instance types. You will get the follwing message when you use the **loadlicense** command:

```
This VM image is misconfigured. The expected configuration for this virtual model is 3 CPU(s);
It is currently configured with 4 CPU(s)
```

This is a general message and will not have any impact on the VM configuration. We recommend you to ignore this message.

Step 8 Perform the interface configuration and enable port 8443 to use the user interface using Azure VMs DNS name.

Step 9 Click **Commit**.

Connect to the Secure Web Appliance User Interface

Use the user interface to configure the appliance software.

When you select an instance, the Public IP address is displayed in the **Overview** page. The default credentials are:

- username—admin

- password—ironport

Step 1 Format for the web access `https://<hostname>:8443`.

Step 2 Run the **System Setup Wizard**.

Step 3 Upload a configuration file.

Step 4 Manually configure the features.

For instructions on accessing and configuring the appliance, including gathering required information, see the online help or user guide for your AsyncOS release. See Related Information, on page 13.

Configure the Secure Web Appliance to Send Alerts When License Expiration Nears

For more information, see Managing Alerts topic in the AsyncOS User Guide.

Deploy Secure Web Appliance on Azure Environment using CLI

You can deploy Secure Web Appliance on Azure environment using CLI.

Steps to install Azure CLI in different operating systems is available here: https://docs.microsoft.com/en-us/cli/azure/install-azure-cli.

Alternatively, in Azure user interface, you can find Cloud Shell next to the search bar. Cloud Shell can be used to execute the Azure CLI commands from the Azure user interface.

Step 1 Accept the Azure VM image terms. To accept the terms, execute the following commands in the Azure console:

az vm image terms accept --urn <publisher:offer:sku:version>

Example : `az vm image terms accept --urn cisco:cisco_secure_web_s100v:wsa_byol_15-2-0_gd_s100v:15.2.0`

Step 2 To login to your Azure account, execute the following commands in the Azure console:

az login -u <username> -p <password>

az account set --subscription <subscription_id>

The subscription_id can be obtained from storage accounts.

Step 3 To create NIC for the management interface, execute the following commands:

az network nic create --resource-group <Resource_group_name> --name <M1_interface_name> --vnet-name <Virtual_network>--subnet <Network_name_in_VNET> --network-security-group <NSG_Name>

Step 4 To create NIC for the for P1 interface, execute the following commands:

az network nic create --resource-group <Resource_group_name> --name <P1_interface_name > --vnet-name <Virtual_network> --subnet <Network_name_in_VNET> --network-security-group <NSG_Name>

Step 5 To create Public IP for management interface, execute the following commands:

az network public-ip create --resource-group <Resource_group_name> --name <M1-IP>

Step 6 To create Public IP for data interface, execute the following commands:

az network public-ip create --resource-group <Resource_group_name> --name <P1-IP>

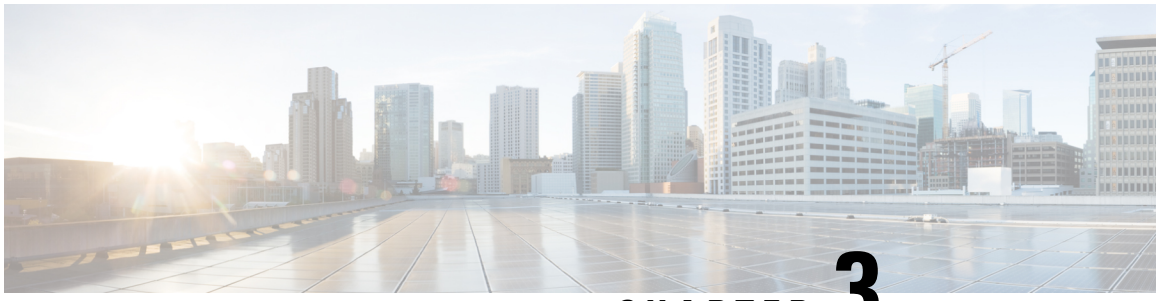
Step 7 To assign the created Public IP to the corresponding interfaces, execute the following commands:

az network nic ip-config update --resource-group <Resource_group_name> --nic-name <M1_interface_name> --name ipconfig1 --public-ip <M1-IP>

az network nic ip-config update --resource-group <Resource_group_name> --nic-name <P1_interface_name> --name ipconfig1 --public-ip <P1-IP>

Step 8 To create VM with management and data interfaces, execute the following commands:

az vm create --resource-group <Resource_group_name> --name <VM_Name> --image <Image_name> --size <instance_type> --admin-username rtestuser --admin-password ironport_123 --nics <M1_interface_name > <P1_interface_name >



CHAPTER 3

Manage the Virtual Appliance

CLI Commands on the Virtual Appliance

The following are the CLI command changes for virtual appliances:

Table 3: CLI Commands on the Virtual Appliance

Command	Supported on Virtual Secure Web Appliance?	Information
loadlicense	Yes	Allows you to install a license for your virtual appliance. You cannot run System Setup Wizard on the virtual appliance without installing a license.
etherconfig	Yes	The Pairing option is not included on virtual appliances.
version	Yes	Returns all the information about the virtual appliance except for the UDI, RAID, and BMC information.
resetconfig	Yes	Retains the virtual appliance license and the feature keys on the appliance.
revert	Yes	Retains the virtual appliance license and the feature keys on the appliance.
reload	Yes	Removes the virtual appliance license and all the feature keys on the appliance. **Note** This command is available only for Secure Web Appliance.

Command	Supported on Virtual Secure Web Appliance?	Information

diagnostic	Yes	The following **diagnostic** > **raid** submenu options will not return information:
		`1. Run disk verify`
		`2. Monitor tasks in progress`
		`3. Display disk verify verdict`
		Note This command is only available for Secure Web Appliance.

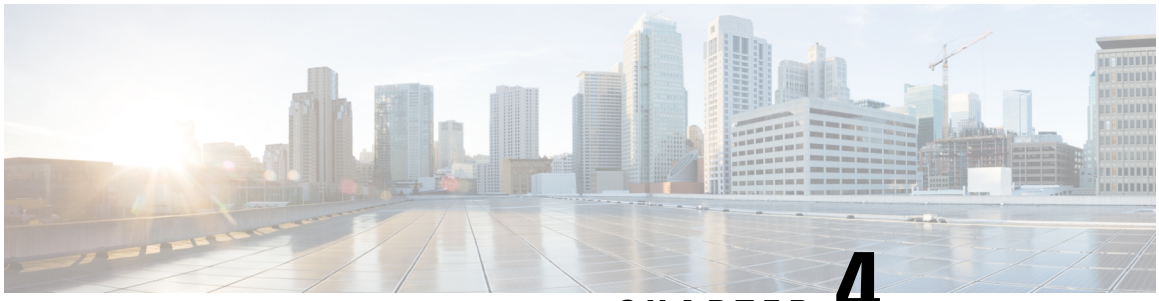
showlicense	Yes	View license details. For virtual Cisco Secure Web appliances, additional information is available through the **featurekey** command.

Azure Monitoring

This topic provides support for Microsoft Azure monitoring for the Secure Web Appliance

Table 4: Azure Monitoring

Monitor Type	Support to Secure Web Appliance	Comments
Application Insights	No	You cannot enable Application Insights because **Update Azure Agent** is not available for the Secure Web Appliance.
Alerts	Yes	Both Custom alerts and Default alerts are available.
Logs	No	You cannot enable Application Insights because "**Update Azure Agent**" is not available for the Secure Web Appliance.
Metrics	Yes	—
Diagnostic Settings	No	You cannot enable **Diagnostic Settings** for the Secure Web Appliance.



CHAPTER 4

Related Information

Related Information

For more information, including information about support options, see the related documentation for your AsyncOS release.

- User Guide for Secure Web Appliance
- Release Notes for Secure Web Appliance
- User Guide for Secure Email and Web Manager
- Release Notes for Secure Email and Web Manager
- User Guide for Secure Email Gateway
- Release Notes for Secure Email Gateway

Cisco TAC

For additional support, contact Cisco TAC at:

http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html