

Install ISE on Azure Cloud Services

Contents

[Introduction](#)

[Prerequisites](#)

[Component Used](#)

[Azure VM Sizes that are Supported by Cisco ISE](#)

[Limitations of Cisco ISE in Microsoft Azure Cloud Services](#)

[Configure](#)

[Example of ISE deployment Connected to Azure Cloud](#)

[Configurations](#)

[What to do next](#)

[Post Installation Tasks](#)

[Password Recovery and Reset on Azure Cloud](#)

[1. Reset Cisco ISE GUI Password Through Serial Console](#)

[2. Create New Public Key Pair for SSH Access](#)

Introduction

This document describes how to Install Cisco ISE IOS instance using Azure Virtual Machine. Cisco ISE IOS is available on Azure Cloud Services.

Prerequisites

- Subscriptions and Resource Groups.

Navigate to All Services > Subscriptions. Make sure that Azure account with active subscription which has enterprise agreement with Microsoft is present. Using Microsoft PowerShell Azure module CLI execute commands to reserve space: (Refer to <[How to install Azure PowerShell](#)> for installing power shell and relevant packages).

```
Connect-AzAccount -TenantID <Tenant-ID>  
Register-AzResourceProvider -ProviderNamespace Microsoft.AVS |  
Register-AzResourceProvider -ProviderNamespace Microsoft.Batch
```



Note: Replace The Tenant-ID with your actual Tenant ID

Complete the prerequisites at [Request host quota for Azure VMware Solution](#) for more details.

Create resource group after right subscription, navigating to **All Services > Resource groups**. Click **Add**. Enter the **Resource group** name.

Create a resource group

Basics Tags Review + create

Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. [Learn more](#)

Project details

Subscription * ⓘ

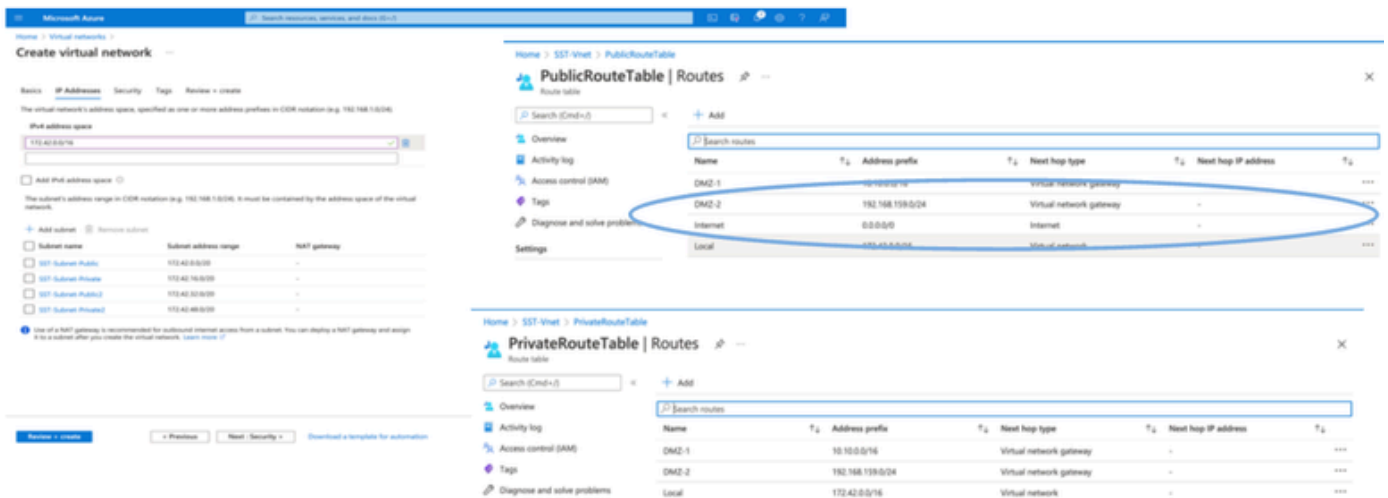
Resource group * ⓘ

Resource details

Region * ⓘ

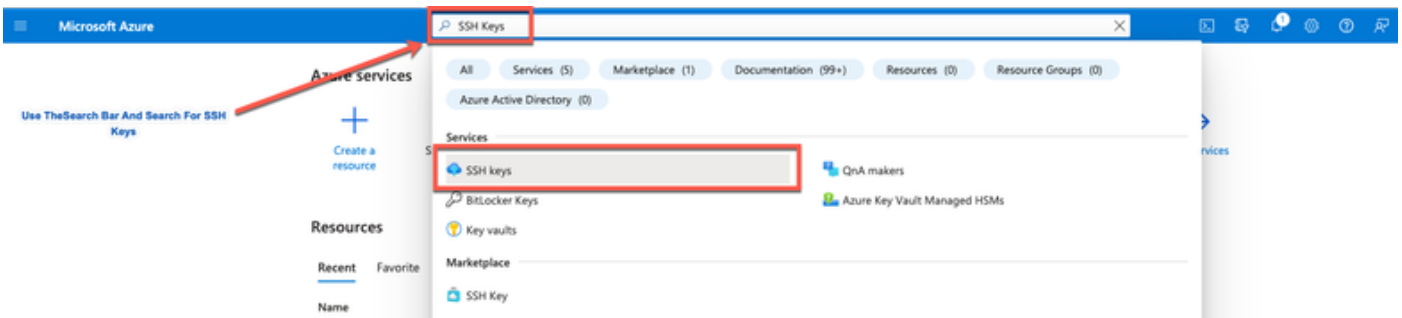
- Virtual Network and Security Groups.

The Subnet which requires internet reachability must have the route table configured with next hop as internet. See examples of public and private subnetwork. PAN with public IP Have both offline and online feed update working, PAN with private ip need to rely on offline feed updates.



- Create an SSH Key Pair.

a. Use the search bar from the Azure Web Portal home page and search for **SSH Keys**.



b. From the Next Window click **Create**.

Microsoft Azure

Search resources, services, and docs (G+)

Home > SSH keys [Click Create](#)

cxsecurity

+ Create Manage view Refresh Export to CSV Open query Assign tags

Filter for any field... Subscription equals all Resource group equals all Location equals all Add filter

Showing 0 to 0 of 0 records.

Name ↑↓	Type ↑↓	Resource group ↑↓	Location ↑↓
<p>No SSH keys to display</p> <p>SSH is an encrypted connection protocol that allows secure sign-ins over unsecured connections. SSH keys allow secure connections to virtual machines, without having to use passwords.</p> <p>Create SSH key</p>			

c. From the next window select the **Resource Group** and **Key Name**. Then click **Review + Create**.

Home > SSH keys > Create an SSH key

Basics Tags Review + create

Creating an SSH key resource allows you to manage and use public keys stored in Azure with Linux virtual machines. [Learn more](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Resource group *

Instance details

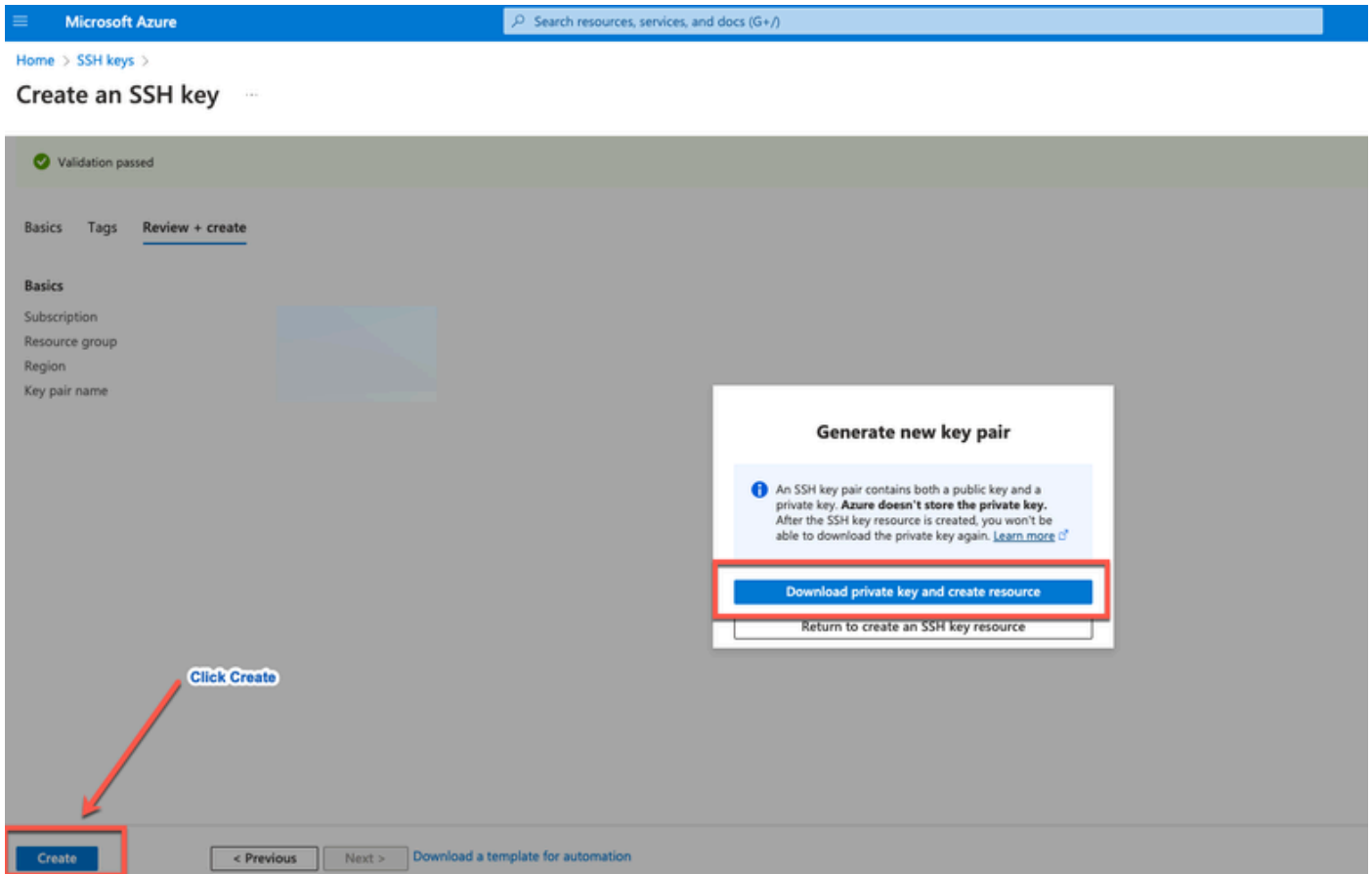
Region *

Key pair name *

SSH public key source

Review + create < Previous Next : Tags >

d. From next window click **Create** and Download **Private Key**.



Component Used

The content of this document is based on these software and cloud services.

- Cisco ISE version 3.2.
- Microsoft Azure Cloud Services

The information in this document was created in the device from specific lab environment. All the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Azure VM Sizes that are Supported by Cisco ISE

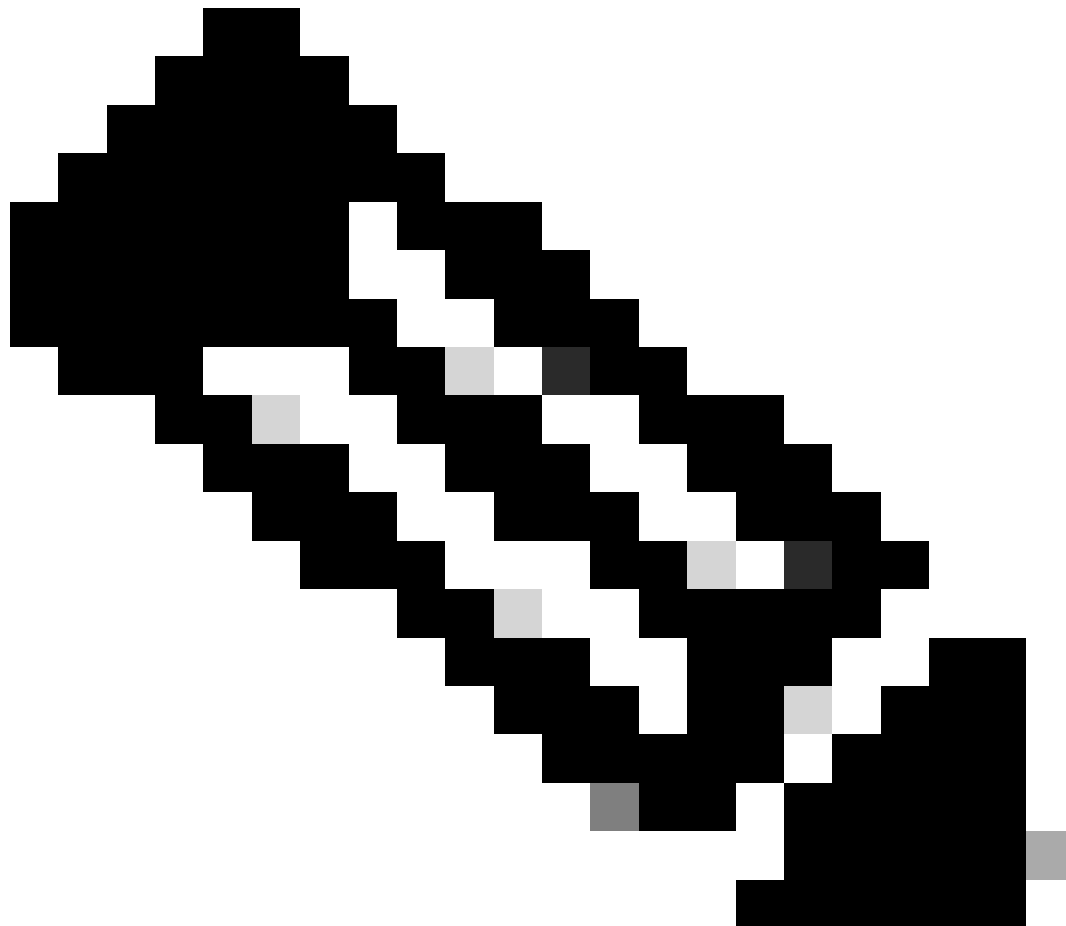
Azure VM Sizes	vCPU	RAM (in GB)
Standard_D4s_v4 (This instance supports the Cisco ISE evaluation use case. 100 concurrent active endpoints are supported.)	4	16
Standard_D8s_v4	8	32
Standard_F16s_v2	16	32
Standard_F32s_v2	32	64
Standard_D16s_v4	16	64
Standard_D32s_v4	32	128
Standard_D64s_v4	64	256

- The Fsv2-series Azure VM sizes are compute-optimized and are best suited for use as PSNs for

compute-intensive tasks and applications.

- The Dsv4-series are general purpose Azure VM sizes that are best suited for use as PAN or MnT nodes or both and are intended for data processing tasks and database operations.

If you use a general-purpose instance as a PSN, the performance numbers are lower than the performance of a compute-optimized instance as a PSN. The Standard_D8s_v4 VM size must be Used as an extra small PSN only.



Note: Do not clone an existing Azure Cloud image to create a Cisco ISE instance. Doing this can cause random and unexpected malfunctions in the created ISE machine.

Limitations of Cisco ISE in Microsoft Azure Cloud Services

- If you create [Cisco ISE using the Azure Virtual Machine](#), by default, Microsoft Azure assigns private IP addresses to VMs through DHCP servers. Before you create a Cisco ISE deployment on Microsoft Azure, you must update the forward and reverse DNS entries with the IP addresses assigned by Microsoft Azure.

Alternatively, after you install Cisco ISE, assign a static IP address to your VM by updating the

Network Interface object in Microsoft Azure:

1. Stop the VM.
 2. In the Private IP address settings area of the VM, in the Assignment area, click Static.
 3. Restart the VM.
 4. In the Cisco ISE serial console, assign the IP address as Gi0.
 5. Restart the Cisco ISE application server.
- Dual NIC is supported with only two NICs—Gigabit Ethernet 0 and Gigabit Ethernet 1. To configure a secondary NIC in your Cisco ISE instance, you must first create a network interface object in Azure, power off your Cisco ISE instance, and then attach this network interface object to Cisco ISE. After you install and launch Cisco ISE on Azure, use the Cisco ISE CLI to manually configure the IP address of the network interface object as the secondary NIC.
 - The Cisco ISE upgrade workflow is not available in Cisco ISE on Microsoft Azure. Only fresh installs are supported. However, you can carry out backup and restore of configuration data.
 - The public cloud supports Layer 3 features only. Cisco ISE nodes on Microsoft Azure do not support Cisco ISE functions that depend on Layer 2 capabilities. For example, working with DHCP SPAN profiler probes and CDP protocol functions through the Cisco ISE CLI are functions that are currently not supported.
 - When you carry out the restore and backup function of configuration data, after the backup operation is complete, first restart Cisco ISE through the CLI. Then, initiate the restore operation from the Cisco ISE GUI.
 - SSH access to Cisco ISE CLI using password-based authentication is not supported in Azure. You can only access the Cisco ISE CLI through a key pair, and this key pair must be stored securely. If you are using a Private Key (or PEM) file and you lose the file, you would not be able to access the Cisco ISE CLI.

Any integration that uses a password-based authentication method to access Cisco ISE CLI is not supported, for example, Cisco DNA Center Release 2.1.2 and earlier.

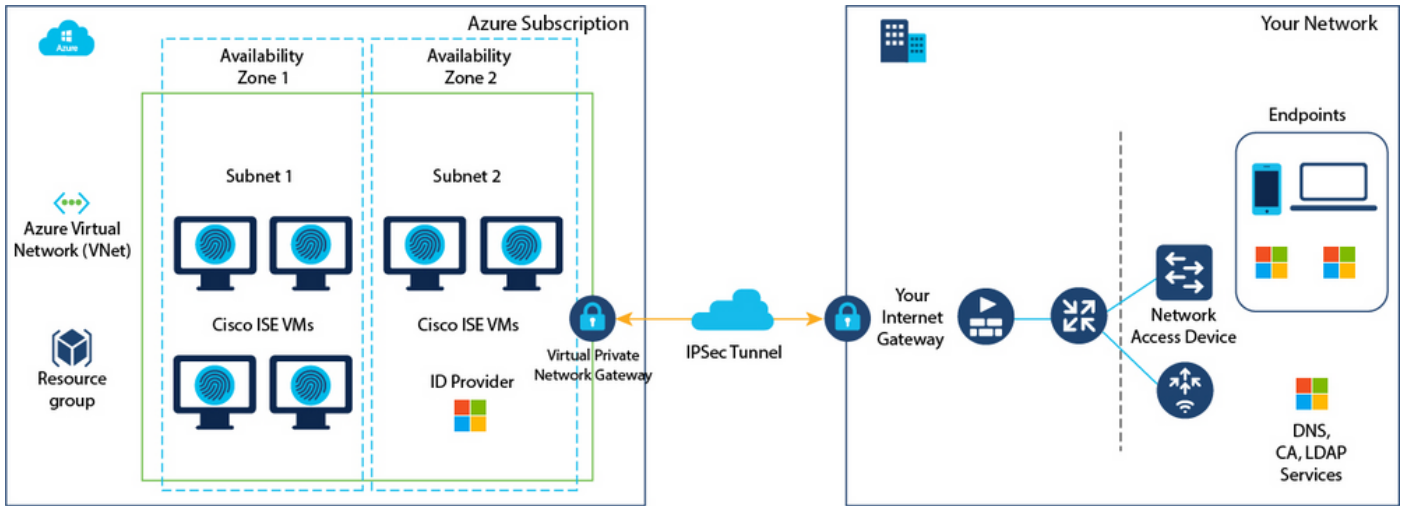
- Cisco ISE IOS deployments on Azure typically leverage VPN solutions like Dynamic Multipoint Virtual Private Networks (DMVPN) and Software-Defined Wide Area Networks (SD-WAN), where the IPsec tunnel overheads can cause MTU and fragmentation issues. In such scenarios, Cisco ISE IOS would not receive complete RADIUS packets and an authentication failure occurs without triggering a failure error log.

A possible workaround is to seek Microsoft technical support to explore any solutions in Azure that can allow out-of-order fragments to pass to the destination instead of being dropped.

- CLI Admin user must be "iseadmin".

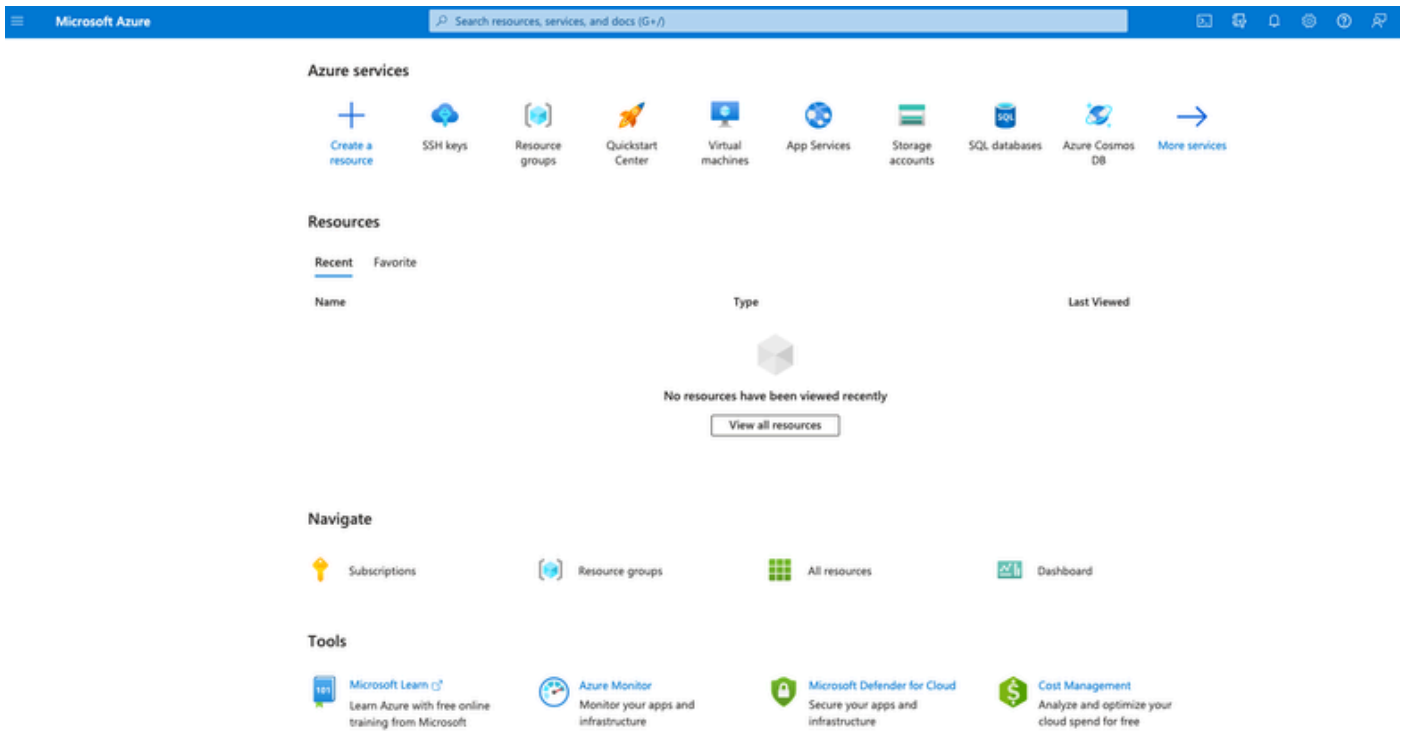
Configure

Example of ISE deployment Connected to Azure Cloud

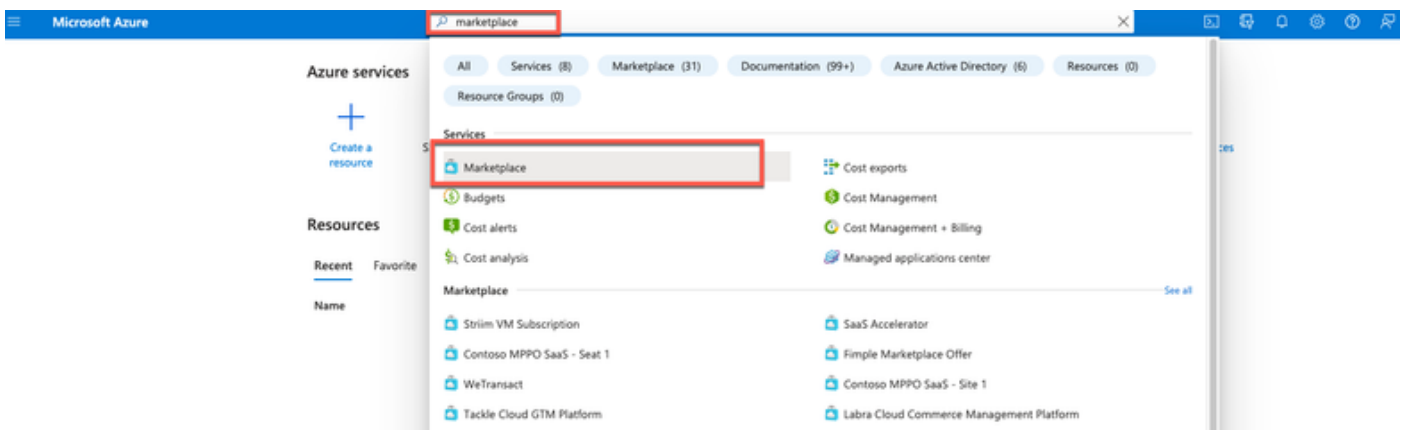


Configurations

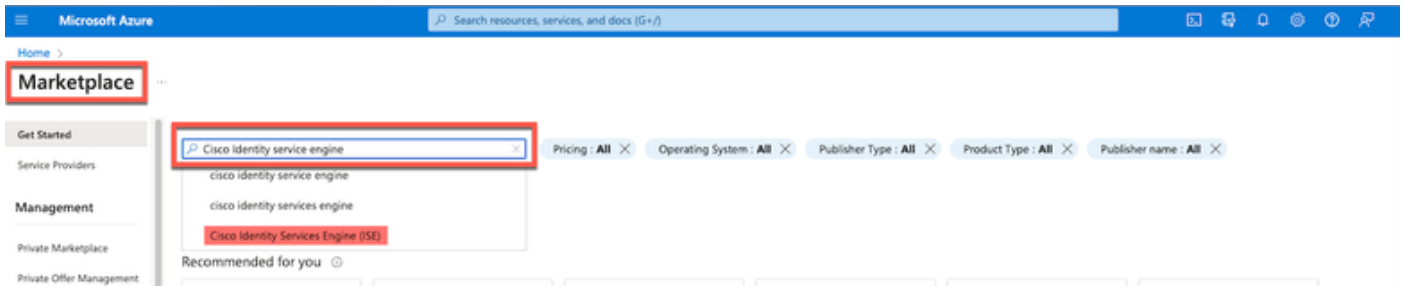
- Step (1): Go to [Azure portal](#) and log in to your Microsoft Azure account.



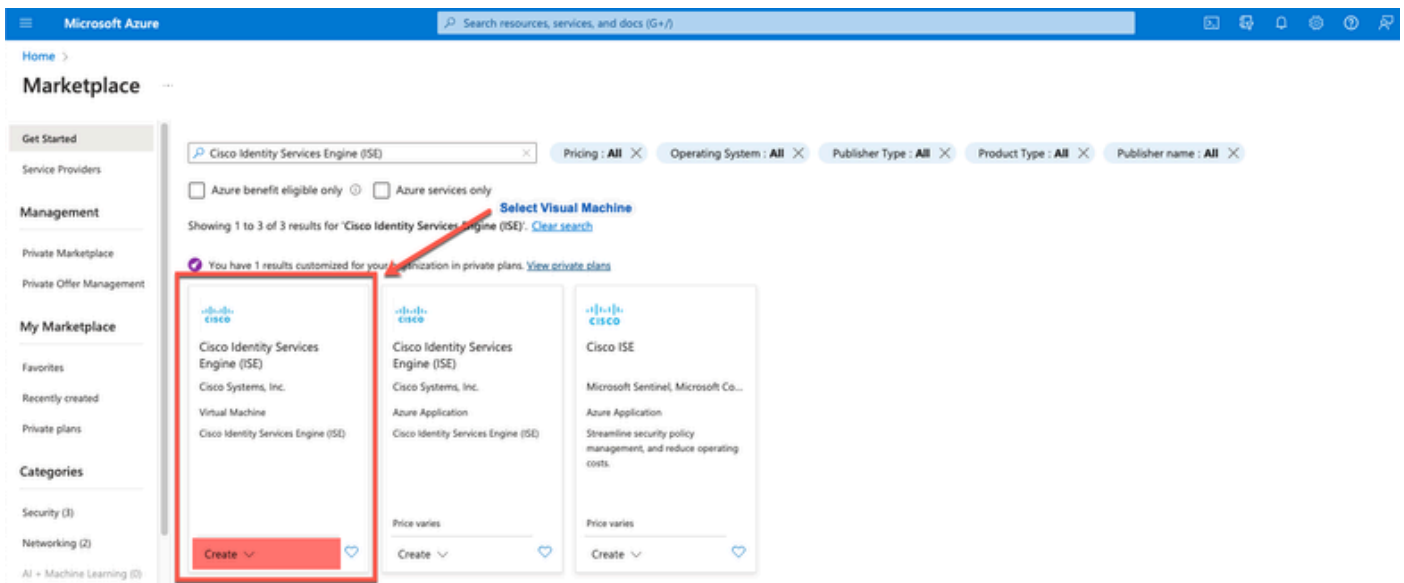
- Step (2): Use the search field at the top of the window to search for **Marketplace**.



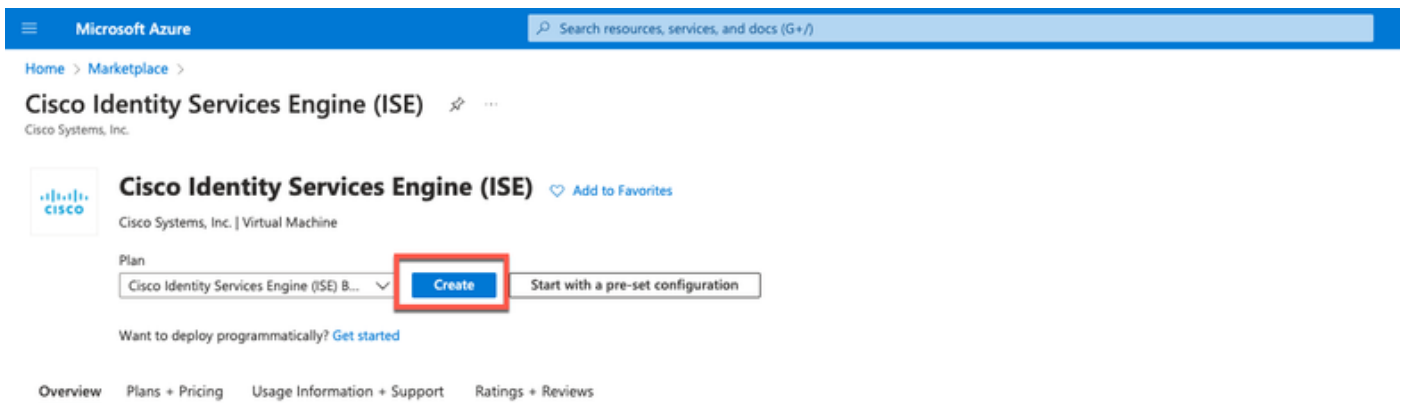
- Step (3): Use the **Search the Marketplace** search field to search for **Cisco Identity Services Engine (ISE)**.



- Step (4): Click **Virtual Machine**.



- Step (5): In the new window that is displayed, click **Create**.



- Step (6): In the Basics tab:

a. In the **Project details** area, choose the required values from the **Subscription** and **Resource group** drop-down lists.

b. In the **Instance details** area, enter a value in the **Virtual Machine name** field.

c. From the **Image** drop-down list, choose the Cisco ISE image.

d. From the **Size** drop-down list, choose the instance size that you want to install Cisco ISE with. Choose an instance that is supported by Cisco ISE, as listed in the table titled **Azure Cloud**

Instances that are supported by Cisco ISE, in the section [Cisco ISE on Azure Cloud](#).

e. In the **Administrator account > Authentication type** area, click the **SSH Public Key** radio button.

f. In the **Username** field, enter **iseadmin**.

g. From the **SSH public key source** drop-down list, choose **Use existing key stored in Azure**.

h. From the **Stored keys** drop-down list, choose the key pair that you created as a prerequisite for this task.

j. In the **Inbound port rules** area, click the **Allow selected ports** radio button.

k. In the **Licensing** area, from the **Licensing type** drop-down list, choose **Other**.

[Home](#) > [Virtual machines](#) >

Create a virtual machine

[Basics](#) [Disks](#) [Networking](#) [Management](#) [Monitoring](#) [Advanced](#) [Tags](#) [Review + create](#)

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

[Select Your Subscription](#)

Resource group *

[Resource Group You Created](#)[Create new](#)

Instance details

Virtual machine name *

ise-vm-name

Region *

(US) East US

Availability options

Availability zone

Availability zone *

Zones 1

You can now select multiple zones. Selecting multiple zones will create one VM per zone. [Learn more](#)

Security type

Standard

Image *

Cisco Identity Services Engine (ISE) BYOL 3.2 - x64 Gen1

[See all images](#) | [Configure VM generation](#)

VM architecture

 Arm64 x64

Arm64 is not supported with the selected image.

[Click Here To Select ISE Image](#)

Run with Azure Spot discount

Size *

Standard_D32s_v4 - 32 vcpus, 128 GiB memory (\$863.59/month)

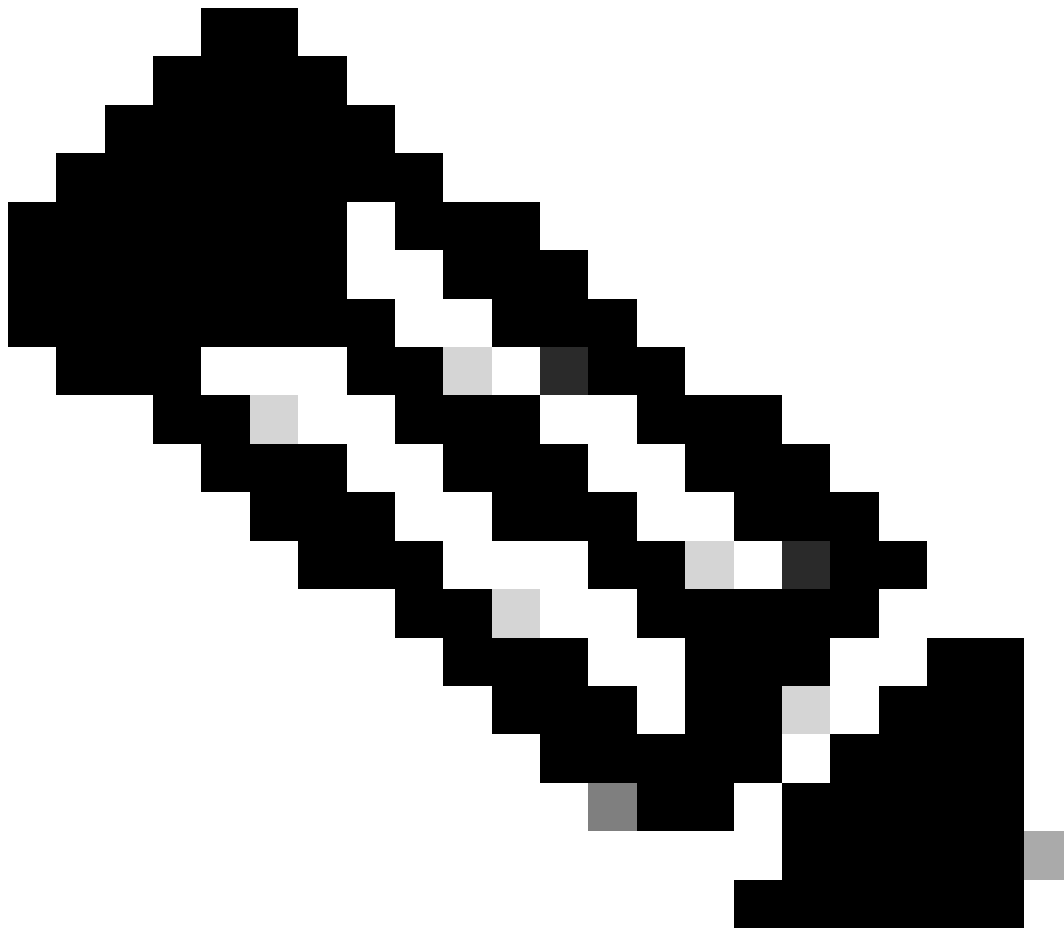
[See all sizes](#)

Administrator account

Authentication type

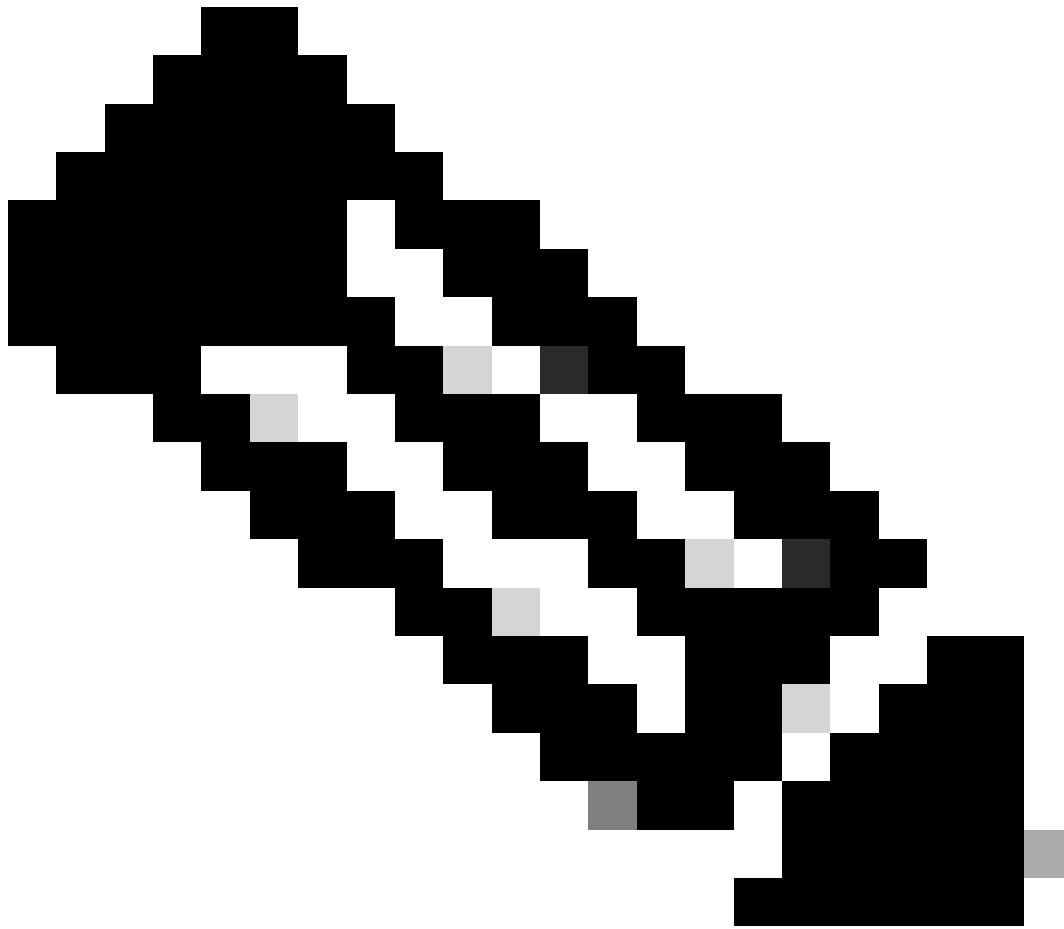
 SSH public key Password[Click Here To Select ISE Template](#)

Azure now automatically generates an SSH key pair for you and allows you to



Note: For The Disk Type, there is more options from the Drop Down List to select. You can select the one that Meets your Need. Premium SSD is the Recommended Type for Production and Performance Sensitive Workloads.

-
- Step (9): In the **Network Interface** area, from the **Virtual network**, **Subnet** and **Configure network security group** drop-down lists, choose the virtual network and subnet that you have created.



Note: The subnet with a public IP address receives online and offline posture feed updates, while a subnet with a private IP address only receives offline posture feed updates.

Create a virtual machine ...

Basics Disks **Networking** Management Monitoring Advanced Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. [Virtual Network You created Or Click Create New](#)
[Learn more](#)

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network * [Create new](#)

Subnet *

Public IP [Create new](#)

NIC network security group None
 Basic
 Advanced [Select Security Group You Created Or Click Create New](#)

Configure network security group * [Create new](#)

Delete public IP and NIC when VM is deleted

Enable accelerated networking The selected image does not support accelerated networking.

Load balancing

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. [Learn more](#)

[Review + create](#) [< Previous](#) [Next : Management >](#)

- Step (10): Click **Next: Management**.

Delete public IP and NIC when VM is deleted

Enable accelerated networking The selected image does not support accelerated networking.

[Review + create](#) [< Previous](#) [Next : Management >](#)

- Step (11): In the **Management** tab, retain the default values for the mandatory fields and click **Next: Advanced**.



Home > Virtual machines >

Create a virtual machine ...

“Click Next on This Page > Monitoring > Advanced”

Basics Disks Networking Management Monitoring Advanced Tags Review + create

Configure management options for your VM.

Microsoft Defender for Cloud

Microsoft Defender for Cloud provides unified security management and advanced threat protection across hybrid cloud workloads. [Learn more](#)

Your subscription is protected by Microsoft Defender for Cloud basic plan.

Identity

Enable system assigned managed identity

Azure AD

Login with Azure AD

This image does not support Login with Azure AD.

Auto-shutdown

Enable auto-shutdown

Create a virtual machine ...

Basics Disks Networking Management **Monitoring** Advanced Tags Review + create

Premium SSD "Recommended Type For Production"

Configure monitoring options for your VM.

Alerts

Enable recommended alert rules

Diagnostics

Boot diagnostics Enable with managed storage account (recommended)
 Enable with custom storage account
 Disable

Enable OS guest diagnostics

Review + create

< Previous

Next : Advanced >

- Step (12): In the **User data** area, check the **Enable user data** check box.

In the **User data** field, complete information:

hostname=<hostname of Cisco ISE>

primarynameserver=<IPv4 address>

dnsdomain=<domain name>

ntpserver=<IPv4 address or FQDN of the NTP server>

timezone=<timezone>

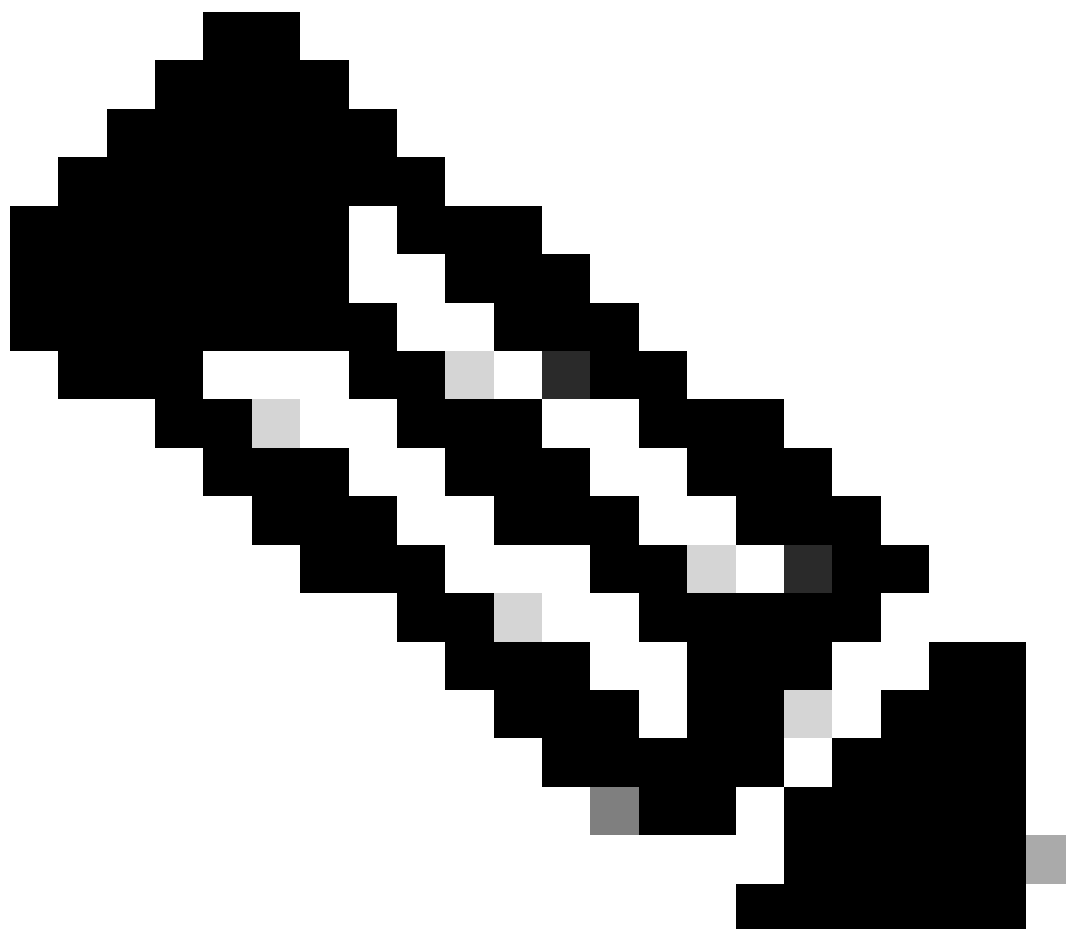
password=<password>

ersapi=<yes/no>

openapi=<yes/no>

pxGrid=<yes/no>

pxgrid_cloud=<yes/no>



Note: You must use the correct syntax for each of the fields that you configure through the user data entry. The information you enter in the User data field is not validated when it is entered. If you use the wrong syntax, Cisco ISE services would not come up when you launch the image.

See the **Guidelines** for the Configurations That You must Submit Through the User Data Field:

a. **hostname:** Enter a hostname that contains only alphanumeric characters and hyphens (-). The length of the hostname must not exceed 19 characters and cannot contain underscores (_).

b. **primary nameserver:** Enter the IP address of the primary name server. Only IPv4 addresses are supported.

You can add only one DNS server in this step. You can add additional DNS servers through the Cisco ISE CLI after installation.

c. **dnsdomain:** Enter the FQDN of the DNS domain. The entry can contain ASCII characters, numerals, hyphens (-), and periods (.).

d. ntpserver: Enter the IPv4 address or FQDN of the NTP server that must be used for synchronization.

You can add only one NTP server in this step. You can add additional NTP servers through the Cisco ISE CLI after installation. **Use a valid and reachable NTP Server** since this needed for ISE Operations.

e. time zone: Enter a time zone, for example, Etc/UTC. We recommend that you set all the Cisco ISE nodes to the Coordinated Universal Time (UTC) time zone, especially if your Cisco ISE nodes are installed in a distributed deployment. This procedure ensures that the time stamps of the reports and logs from the various nodes in your deployment are always synchronized.

f. password: Configure a password for GUI-based login to Cisco ISE. The password that you enter must comply with the Cisco ISE password policy. The password must contain 6 to 25 characters and include at least one numeral, one uppercase letter, and one lowercase letter. The password cannot be the same as the username or its reverse (iseadmin or nimdaesi), cisco, or ocsic. The allowed special characters are @~*!,+=_-. See the "User Password Policy" section in the Chapter "Basic Setup" of the [Cisco ISE Administrator Guide](#) for your release.

g. ersapi: Enter **yes** to enable ERS, or **no** to disallow ERS.

h. openapi: Enter **yes** to enable OpenAPI, or **no** to disallow OpenAPI.

i. pxGrid: Enter **yes** to enable pxGrid, or **no** to disallow pxGrid.

j. pxgrid_cloud: Enter **yes** to enable pxGrid Cloud or **no** to disallow pxGrid Cloud. To enable pxGrid Cloud, you must enable pxGrid. If you disallow pxGrid, but enable pxGrid Cloud, pxGrid Cloud services are not enabled on launch.

Create a virtual machine

Select This

Enable user data

User data *

```
hostname=isehostname  
primarynameserver=primary sever ip address  
dnsdomain=domain fqdn  
ntpserver=ntp server ip address  
timezone=America/Chicago  
username= iseadmin  
password=passworded  
ersapi=yes  
openapi=yes  
pxGrid=no  
pxgrid_cloud=no
```

Performance (NVMe)

Enable capabilities to enhance the performance of your resources.

Higher remote disk storage performance with NVMe

i The selected image and size are not supported for NVMe. [See supported VM images and sizes](#)

Host

Azure Dedicated Hosts allow you to provision and manage a physical server within our data centers that are dedicated to your Azure subscription. A dedicated host gives you assurance that only VMs from your subscription are on the host, flexibility to choose VMs from your subscription that will be provisioned on the host, and the control of platform maintenance at the level of the host. [Learn more](#)

Host group

No host groups found

Capacity reservations

Capacity reservations allow you to reserve capacity for your virtual machine needs. You get the same SLA as normal virtual machines with the security of reserving the capacity ahead of time. [Learn more](#)

Review + create

< Previous

Next : Tags >

User Data Section

- Step (13): Click **Next: Tags**.

Performance (NVMe)

Enable capabilities to enhance the performance of your resources.

Higher remote disk storage performance with NVMe ⓘ

ⓘ The selected image and size are not supported for NVMe. [See supported VM images and sizes](#) ⓘ

Review + create

< Previous

Next : Tags >

- Step (14): To create name-value pairs that allow you to categorize resources, and consolidate multiple resources and resource groups, enter values in the **Name** and **Value** fields.

[Home](#) > [Virtual machines](#) >

Create a virtual machine ...

Basics Disks Networking Management Monitoring Advanced Tags Review + create

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. [Learn more about tags](#) ⓘ

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

Name ⓘ

Value ⓘ

Resource

Tag Name

Value Name

13 selected

- Step (15): Click **Next: Review + Create**.

Review + create

< Previous

Next : Review + create >

- Step (16): Review the information that you have provided so far and click **Create**.

The **Deployment is in progress** window is displayed. It takes about 30 minutes for the Cisco ISE instance to be created and available for use. The Cisco ISE VM instance is displayed in the

Virtual Machines window (use the main search field to find the window).

Create a virtual machine

Validation passed

Preferred e-mail address

Preferred phone number

Basics

Subscription

Resource group

Virtual machine name

Region

Availability options

Availability zone

Security type

Image

VM architecture

Size

Authentication type

Username

Key pair name

Azure Spot

Disks

[Download a template for automation](#)

CreateVm-cisco.cisco-ise-virtual-cisco-ise_3_2-20230926145056 | Overview

Deployment

Search

Overview **Deployment is in progress** Inputs Outputs Template

Deployment name: CreateVm-cisco.cisco-ise-virtual-cisco-ise_3_2-2... Start time: 9/26/2023, 4:06:05 PM
Subscription: Correlation ID:

Resource group:

Deployment details

Resource	Type	Status	Operation details
	Microsoft.Compute/virtualMachines	Created	Operation details
	Microsoft.Network/networkInterfaces	Created	Operation details
	Microsoft.Network/virtualNetworks	OK	Operation details
	Microsoft.Network/publicIpAddresses	OK	Operation details
	Microsoft.Network/networkSecurityGroups	OK	Operation details

Give feedback [Tell us about your experience with deployment](#)

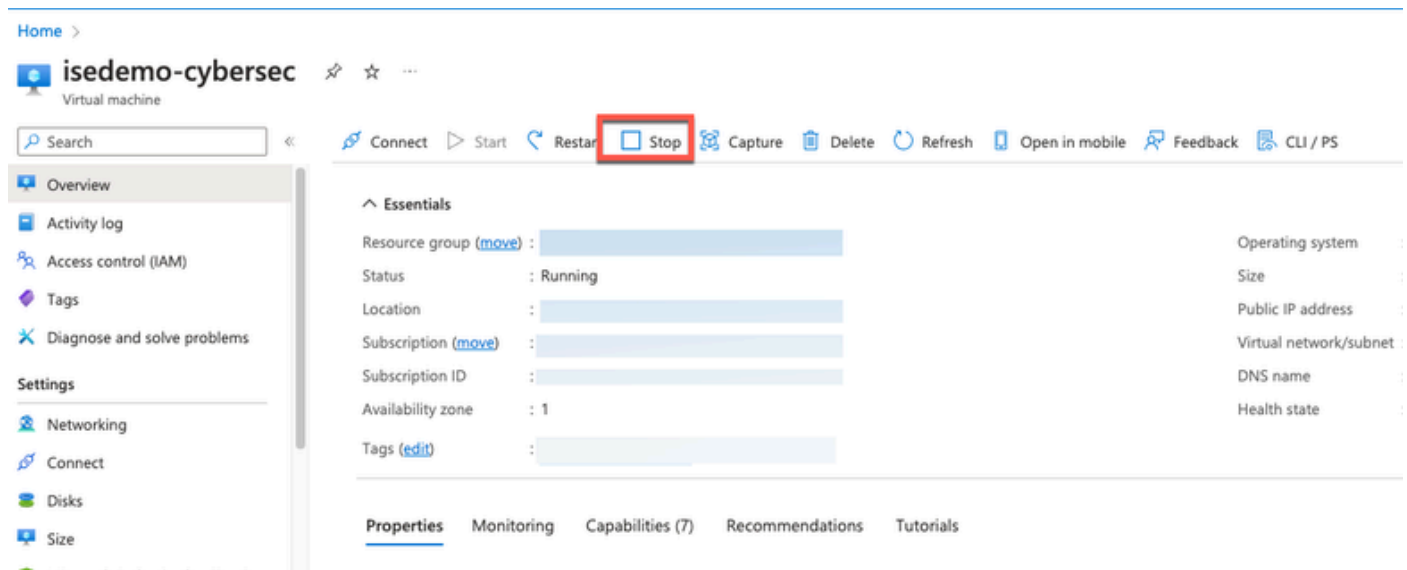
What to do next

Because of a Microsoft Azure default setting, the Cisco ISE VM you have created is configured with only 300 GB disk size. Cisco ISE nodes typically require more than 300 GB disk size. You can see the **Insufficient Virtual Memory** alarm when you first launch Cisco ISE from Microsoft Azure.

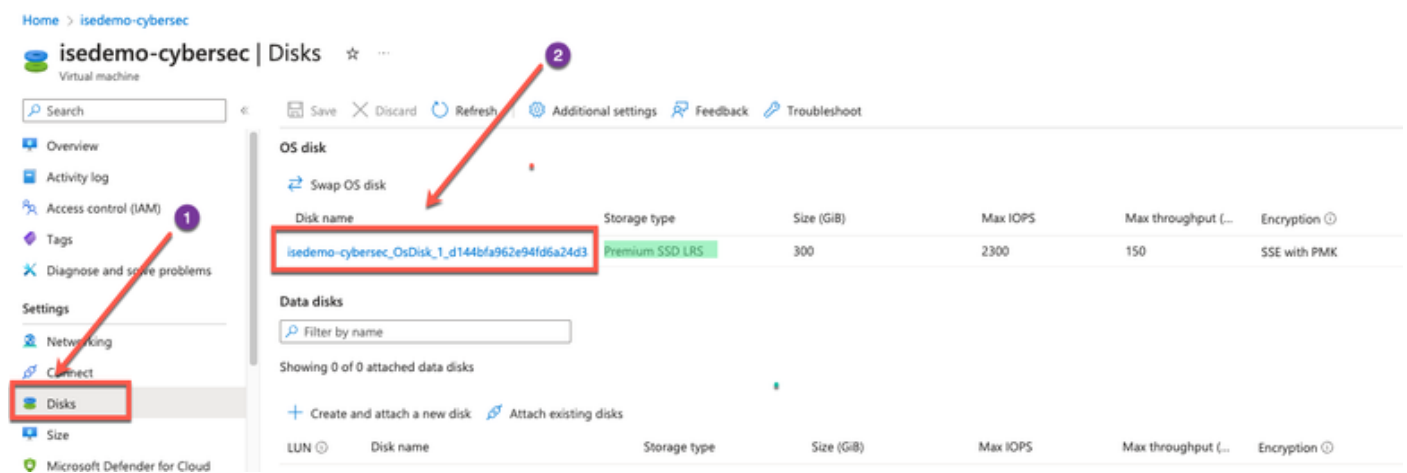
After the Cisco ISE VM creation is complete, log in to the Cisco ISE administration portal to verify that Cisco ISE is set up. Then, in the Microsoft Azure portal, carry out and complete steps in the **Virtual**

Machines window to edit the disk size:

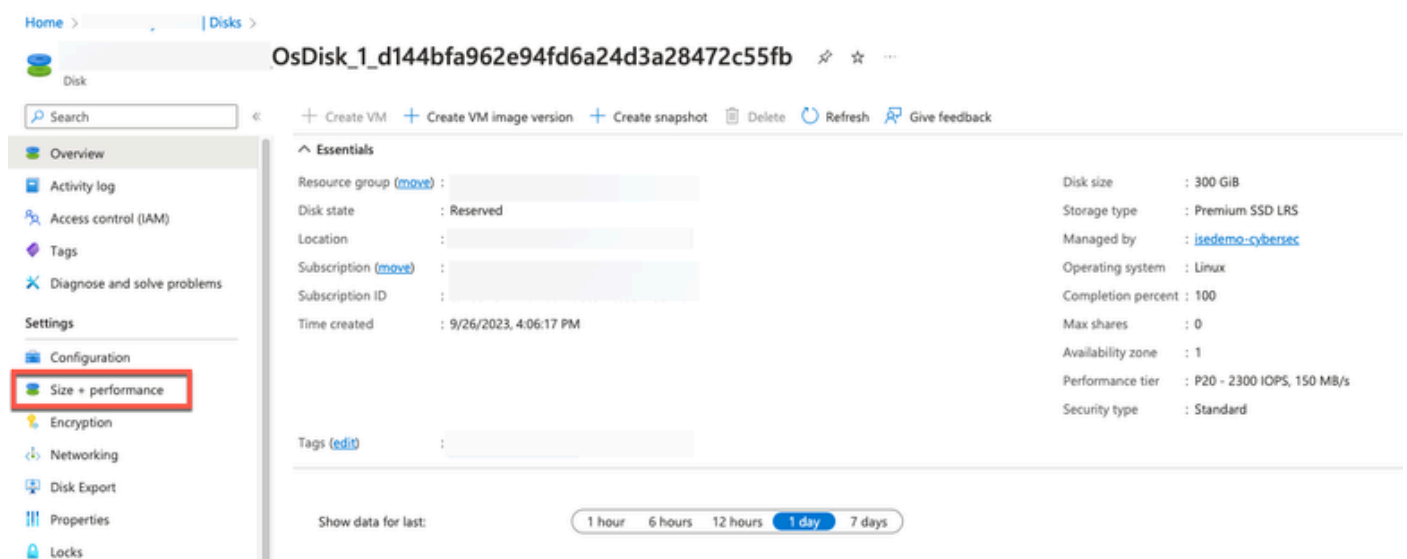
1. Stop the Cisco ISE instance.



2. Click **Disk** in the left pane and click the disk that you are using with Cisco ISE.



3. Click **Size + performance** in the left pane.



4. In the **Custom disk size** field, enter the disk size you want, in GiB.

Size	Disk tier	Provisioned IOPS	Provisioned throughput	Max Shares
4 GiB	P1	120	25	3
8 GiB	P2	120	25	3
16 GiB	P3	120	25	3
32 GiB	P4	120	25	3
64 GiB	P6	240	50	3
128 GiB	P10	500	100	3
256 GiB	P15	1100	125	3
512 GiB	P20	2300	150	3
1024 GiB	P30	5000	200	5
2048 GiB	P40	7500	250	5
4096 GiB	P50	7500	250	5
8192 GiB	P60	16000	500	10
16384 GiB	P70	18000	750	10
32767 GiB	P80	20000	900	10

Post Installation Tasks

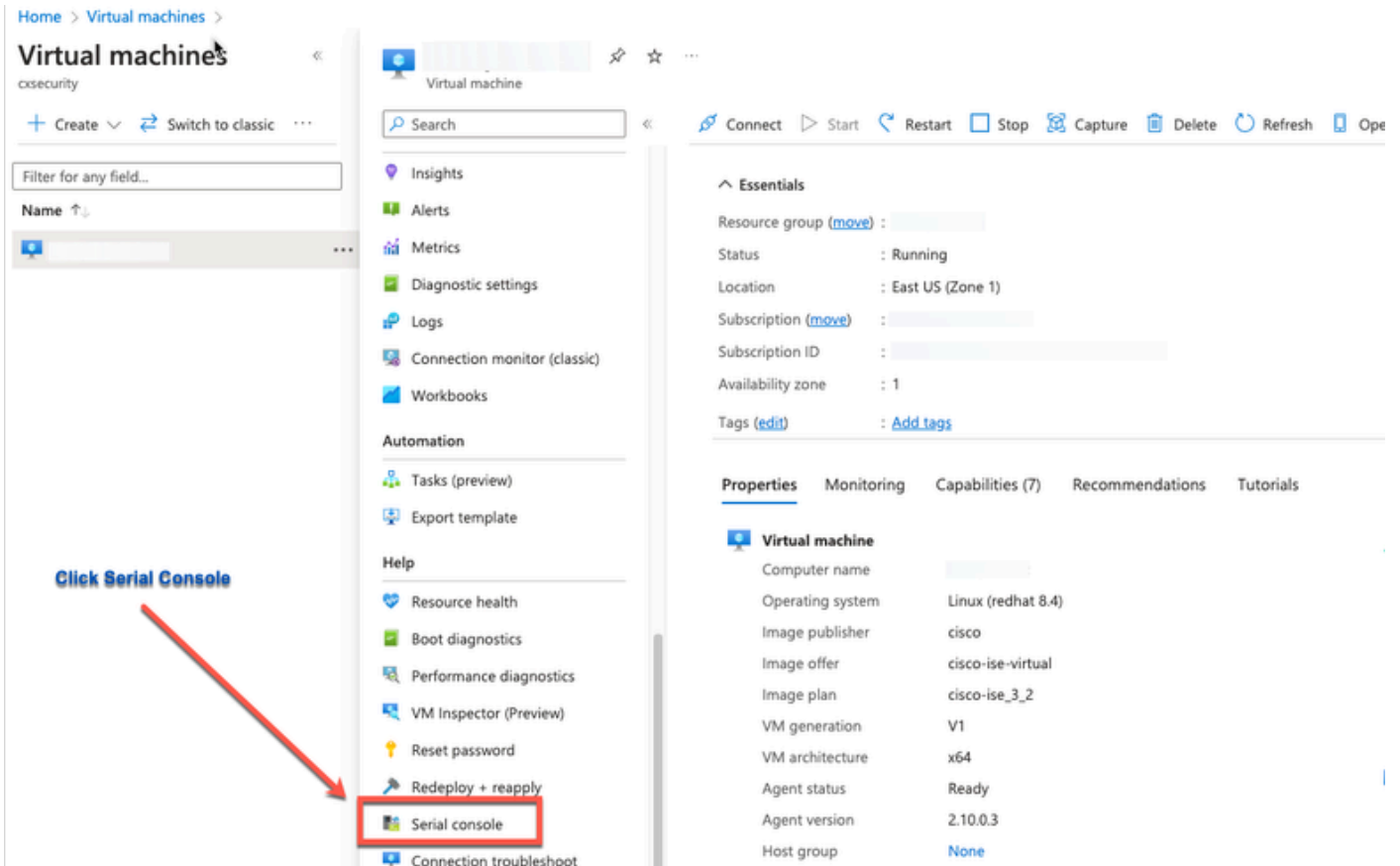
For information about the post installation tasks that you must carry out after successfully creating a Cisco ISE instance, see the Chapter "Installation Verification and Post Installation Tasks" in the [Cisco ISE Installation Guide](#) for your Cisco ISE release.

Password Recovery and Reset on Azure Cloud

Complete the tasks that help your reset or recover your Cisco ISE virtual machine password. Choose the tasks that you need and carry out the steps detailed.

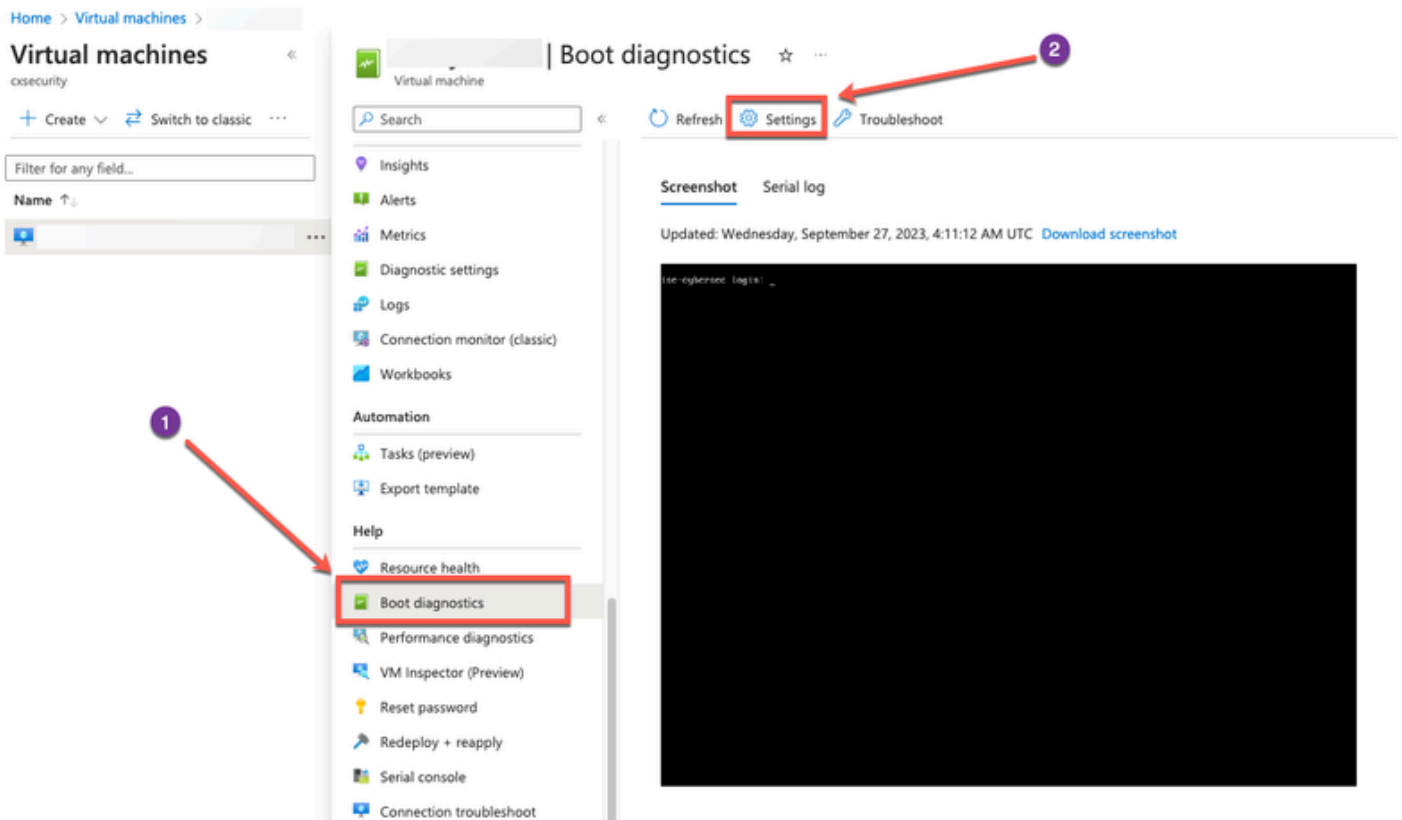
1. Reset Cisco ISE GUI Password Through Serial Console

- Step (1): Log in to Azure Cloud and choose the resource group that contains your Cisco ISE virtual machine.
- Step (2): From the list of resources, click the Cisco ISE instance for which you want to reset the password.
- Step (3): From the left-side menu, from the **Support + Troubleshooting** section, click **Serial console**.

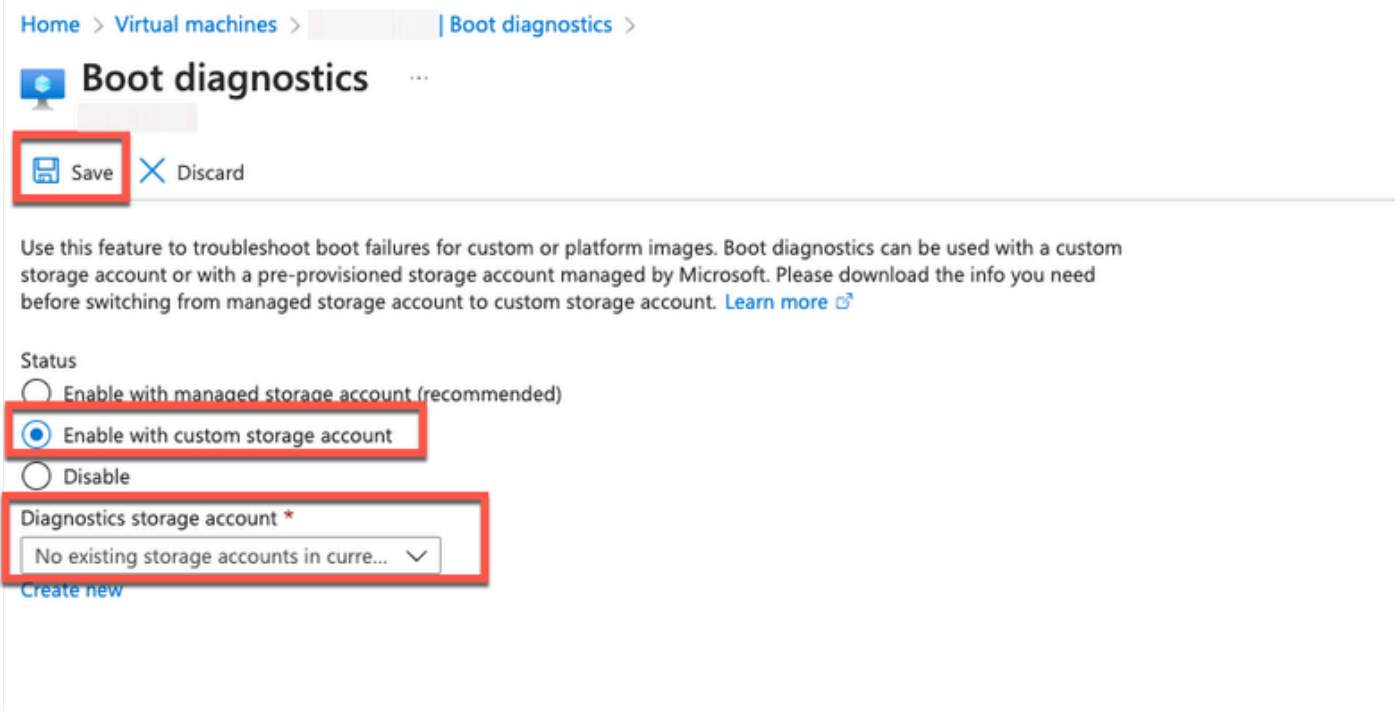


- Step (4): If you view an error message here, you would have to enable boot diagnostics by carrying out and complete steps:

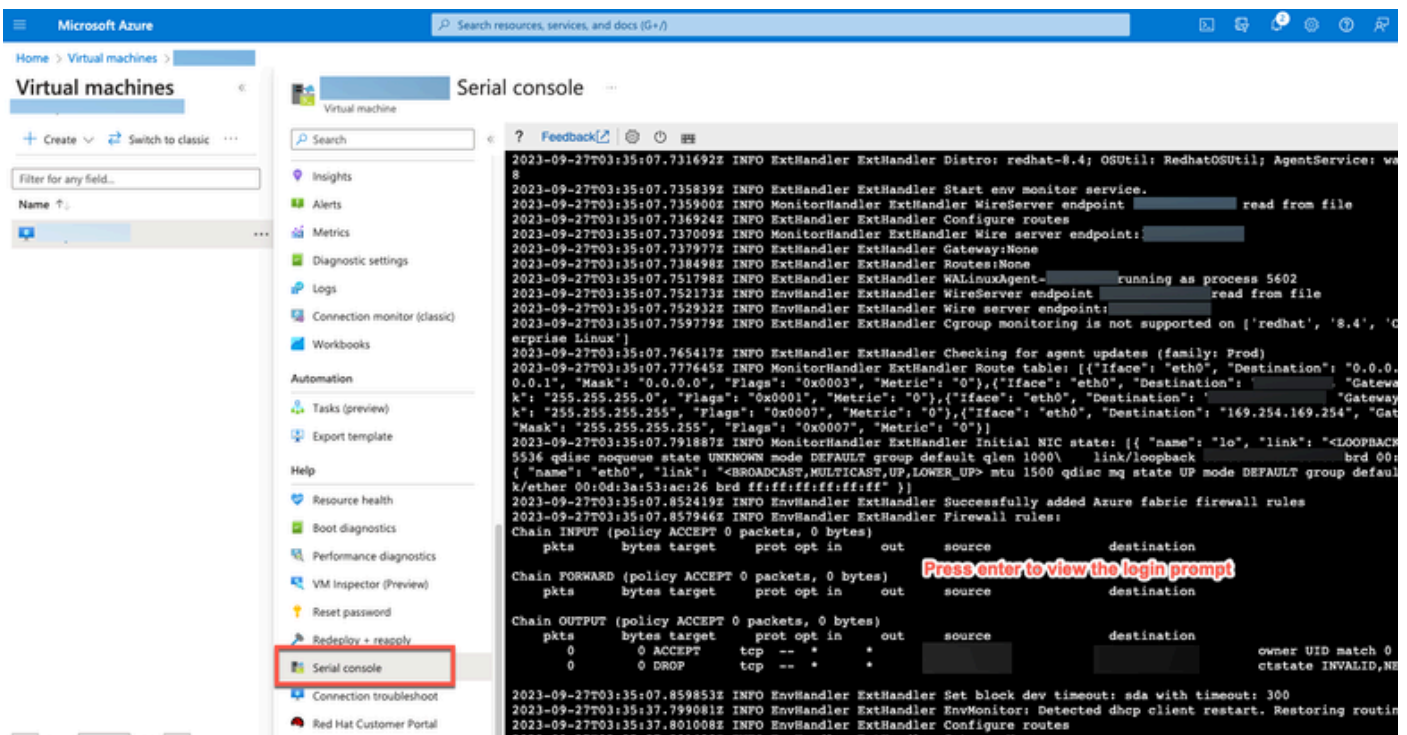
a. From the left-side menu, click **Boot diagnostics**.



b. Click **Enable with custom storage account**. Then click **Save**.



- Step (5): From the left-side menu, from the **Support + Troubleshooting** section, click **Serial console**. The Azure Cloud Shell is displayed in a new window. If the screen is black, press Enter to view the login prompt.



- Step (8): Log in to the serial console. To log in to the serial console, you must use the original password that was configured at the installation of the instance.
- Step (9): Use the **application reset-password iseadmin** command to configure a new GUI password for the iseadmin account.

2. Create New Public Key Pair for SSH Access

Through this task, you add additional key pairs to a repository. The existing key pair that was created at the time of Cisco ISE instance configuration is not replaced by the new public key that you create.

- Step (1): Create a new public key in Azure Cloud.

[Home](#) > [SSH keys](#) >

Create an SSH key ...

[Basics](#) [Tags](#) [Review + create](#)

Creating an SSH key resource allows you to manage and use public keys stored in Azure with Linux virtual machines. [Learn more](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Resource group *

Select Resource group you created from D Drop Down List

Instance details

Region *

Key pair name *

Create Key Pair Name

SSH public key source

Click Review + Create


[Review + create](#)

< Previous

Next: Tags >

You get a pop-up window to select **Download private key and create resource** that downloads the SSH key as a .pem file.

Generate new key pair

i An SSH key pair contains both a public key and a private key. **Azure doesn't store the private key.** After the SSH key resource is created, you won't be able to download the private key again. [Learn more](#) 

[Download private key and create resource](#)

[Return to create an SSH key resource](#)

- Step (2): To create a new repository to save the public key to, see [Azure Repos documentation](#).

If you already have a repository that is accessible through the CLI, skip to step 3.

- Step (3): To import the new Public Key, use the command **crypto key import <public key filename> repository <repository name>**.
- Step (4): When the import is complete, you can log in to Cisco ISE via SSH using the new public key.