Cisco ISE on Azure Cloud Services

Cisco ISE on Azure Cloud

Cisco ISE is available on Azure Cloud Services. To configure and install Cisco ISE on Azure Cloud, you must be familiar with Azure Cloud features and solutions. Some Azure Cloud concepts that you should be familiar with before you begin are:

- Subscriptions and Resource Groups
- Azure Virtual Machines: See Instances, Images, SSH Keys, Tags, VM Resizing.

You can deploy Cisco ISE on Microsoft Azure using an Azure Application or an Azure Virtual Machine. There are no differences in cost or Cisco ISE features when you deploy Cisco ISE using an Azure Application or an Azure Virtual Machine. We recommend using the Azure Application for the following advantages it offers in comparison to the Azure Virtual Machine:

- Azure Application allows you to easily configure Cisco ISE-specific choices directly through its UI instead of a user-data field as in the case of Azure Virtual Machine configuration.
- At the initial configuration of an Azure Application, you can choose an OS disk volume ranging between 300 and 2400 GB. However, during the initial configuration of an Azure Virtual Machine, you can change the OS disk volume to a fixed set of values provided by Azure portal in their drop-down menu. You must carry out more steps after Cisco ISE installation and launch to reconfigure the virtual machine.
- You can directly choose from the specific Azure VM sizes that Cisco ISE supports.
- You can configure a static private IP address at the initial configuration.

You can use the Azure Virtual Machine when:

- You do not use the Azure portal UI to deploy Cisco ISE.

- If you need to use one of the additional settings that are available in the Azure Virtual Machine configuration workflow.

The following task flows guide you through deploying Cisco ISE on Microsoft Azure using an Azure Application or an Azure Virtual Machine.

- Create A Cisco ISE Instance Using Azure Application, on page 8
- Create A Cisco ISE Instance Using Azure Virtual Machine, on page 5

Cisco ISE can be installed by using one of the following Azure VM sizes.

Table 1: 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..

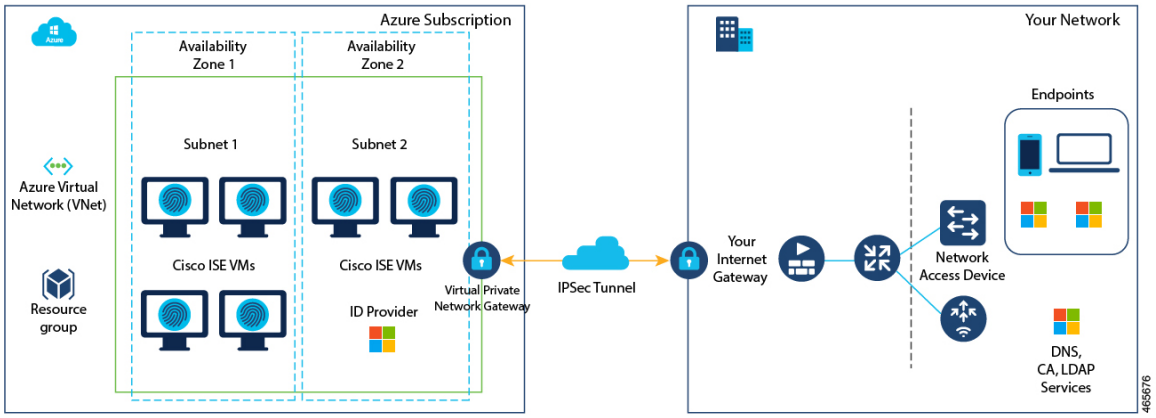
The Dsv4-series are general purpose Azure VM sizes that are best suited for use as PAN or MnT nodes or both and are intended for data processing tasks and database operations.

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.

For information on the scale and performance data for Azure VM sizes, see the *Performance and Scalability Guide for Cisco Identity Services Engine*.

Figure 1: Example of a Deployment Connected to Azure Cloud



Note Do not clone an existing Azure Cloud image to create a Cisco ISE instance.

In addition to the procedures explained above, you can also use the following Cisco developed solution to install and automatically create multi-node Cisco ISE deployments on Azure:

- Cisco Developed Terraform Script

Known Limitations of Cisco ISE in Microsoft Azure Cloud Services

- If you create Create A Cisco ISE Instance Using Azure Application, 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. For information on upgrading hybrid Cisco ISE deployments, see Upgrade Guidelines for Hybrid Deployments.
- 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. For more information about the Cisco ISE backup and restore processes, see the Chapter "Maintain and Monitor" in the *Cisco ISE Administrator Guide* for your release.
- 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 will 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.
- Azure's VPN gateway in Gen 8 cannot be used as a result of fragmentation. This is an Azure's first party gateway limitation.
- In Azure, a networking virtual network stack drops out-of-order fragments without forwarding them to the end virtual machine host. This design aims to address the network security vulnerability FragmentSmack, as documented in Azure and fragmentation.

  Cisco ISE 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 may not receive complete RADIUS packets and an authentication failure occurs without triggering a failure error log.

  Due to this known issue, do one of the following:

  1. Select regions where Azure Cloud has already implemented the fixes: East Asia (eastasia) and West Central US (westcentralus).
  2. Cisco ISE customers should raise an Azure support ticket. Microsoft has agreed to take the following actions:
     a. Pin the subscription to ensure all instances within that subscription are deployed on hardware generation 7.
     b. Enable the "allow out-of-order fragments" option, which allows fragments to pass through to the destination instead of being dropped.

- Cisco ISE deployments on Azure Cloud do not support the Accelerated Networking feature. If you enable this feature at any stage in a Cisco ISE deployment, it might cause operations such as node registration and deregistration to fail.

Create A Cisco ISE Instance Using Azure Virtual Machine

Before you begin

- Create an SSH key pair.
- Create the VN gateways, subnets, and security groups that you require.
- The subnet that you want to use with Cisco ISE must be able to reach the internet. In Microsoft Azure, in the Public Route Table window, configure the next hop of the subnet as the internet.

Note From Cisco ISE Release 3.4, OpenAPI services are enabled automatically, and hence, there's no need to send OpenAPI-related options while launching an instance.

Step 1 Go to https://portal.azure.com 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, on page 1.

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

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

Note The only permitted username is **iseadmin**. Use of any other username is not supported.

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.

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

j) From the **Select inbound ports** drop-down list, choose all the protocol ports that you want to allow accessibility to.

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

Step 7 Click **Next: Disks**.

Step 8 In the **Disks** tab, choose a disk size from the **OS Disk Size** drop-down list or retain the default value.

Note We recommend that you use a customer-managed key for disk encryption in the **Key Management** field. By default, a platform-managed key is used. For more information on key creation, see About encryption key management.

For rest of the mandatory fields, you can retain the default values.

Step 9 Click **Next: Networking**.

Step 10 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 that a 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.

Step 11 Click **Next: Management**.

Step 12 In the **Management** tab, retain the default values for the mandatory fields and click **Next: Advanced**.

Step 13 In the **User data** area, check the **Enable user data** check box.

In the **User data** field, enter the following information:

hostname=<*hostname of Cisco ISE*>

primarynameserver=<*IPv4 address*>

secondarynameserver=<*IPv4 address of secondary nameserver*> (Applicable to Cisco ISE 3.4 and later releases)

tertiarynameserver=<*IPv4 address of tertiary nameserver*> (Applicable to Cisco ISE 3.4 and later releases)

dnsdomain=<*example.com*>

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

secondaryntpserver=<*IPv4 address or FQDN of the secondary NTP server*> (Applicable to Cisco ISE 3.4 and later releases)

tertiaryntpserver=<*IPv4 address or FQDN of the tertiary NTP server*> (Applicable to Cisco ISE 3.4 and later releases)

timezone=<*timezone*>

password=<*password*>

ersapi=<*yes/no*>

openapi=<*yes/no*>

pxGrid=<*yes/no*>

pxgrid_cloud=<*yes/no*>

Important From Cisco ISE Release 3.4,

a. The **ntpserver** field name is changed to **primaryntpserver**. If you use **ntpserver**, Cisco ISE services will not start.

b. OpenAPI is enabled by default. Hence, the **openapi=<yes/no>** field is not required.

c. If you leave the **secondarynameserver** field blank and use only the **tertiarynameserver** field, the Cisco ISE services will not start.

d. If you leave the **secondaryntpserver** field blank and use only the **tertiaryntpserver** field, the Cisco ISE services will not start.

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 might not come up when you launch the image. The following are the guidelines for the configurations that you submit through the user data field:

- 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 (_).
- primarynameserver: 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. However, from Cisco ISE Release 3.4, you can configure secondary and tertiary name servers during installation by using the **secondarynameserver** and **tertiarynameserver** fields.
- dnsdomain: Enter the FQDN of the DNS domain. The entry can contain ASCII characters, numerals, hyphens (-), and periods (.).
- ntpserver: Enter the IPv4 address or FQDN of the NTP server that must be used for synchronization, for example, time.nist.gov.

  You can add only one NTP server in this step. You can add additional NTP servers through the Cisco ISE CLI after installation. However, from Cisco ISE Release 3.4, you can configure secondary and tertiary NTP servers during installation by using the **secondaryntpserver** and **tertiaryntpserver** fields.
- timezone: Enter a timezone, for example, Etc/UTC. We recommend that you set all the Cisco ISE nodes to the Coordinated Universal Time (UTC) timezone, especially if your Cisco ISE nodes are installed in a distributed deployment. This procedure ensures that the timestamps of the reports and logs from the various nodes in your deployment are always synchronized.
- 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.
- ersapi: Enter **yes** to enable ERS, or **no** to disallow ERS.
- openapi: Enter **yes** to enable OpenAPI, or **no** to disallow OpenAPI.
- pxGrid: Enter **yes** to enable pxGrid, or **no** to disallow pxGrid.
- 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.

Step 14 Click **Next: Tags**.

Step 15 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.

Step 16 Click **Next: Review + Create**.

Step 17 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).

What to do next

Note This section is applicable only if the disk size of your Cisco ISE VM is 300 GB. If you have chosen any other disk size, then these steps are not applicable.

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 might 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 the following 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.

Create A Cisco ISE Instance Using Azure Application

Before you begin

Create the Azure resources that you need, such as Resource Groups, Virtual Networks, Subnets, SSH keys, and so on.

Note From Cisco ISE Release 3.4, OpenAPI services are enabled automatically. Therefore, there's no need to send OpenAPI-related options while launching an instance.

Step 1 Go to https://portal.azure.com and log in to the Azure portal.

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 **Azure Application**.

Step 5 In the new window that is displayed, click **Create**.
A five-step workflow is displayed.

Step 6 In the **Basics** tab:

a) From the **Resource Group** drop-down list, choose the option that you want to associate with Cisco ISE.
b) From the **Region** drop-down list, choose the region in which the Resource Group is placed.
c) In the **Hostname** field, enter the hostname.
d) From the **Time zone** drop-down list, choose the time zone.
e) From the **VM Size** drop-down list, choose the Azure VM size that you want to use for Cisco ISE.
f) From the **Disk Encryption Key** drop-down list, choose your key for disk encryption.

Note We recommend that you use a customer-managed key for disk encryption in the **Disk Encryption Key** field. By default, a platform-management key is used. This field is available from Cisco ISE Release 3.3. For more information, see About encryption key management.

g) From the **Disk Storage Type** drop-down list, choose an option.
h) In the **Volume Size** field, enter, in GB, the volume that you want to assign to the Cisco ISE instance. 600 GB is the default value.

Step 7 Click **Next**.

Step 8 In the **Network Settings** tab:

a) From the **Virtual Network** drop-down list, choose an option from the list of virtual networks available in the selected resource group.
b) From the **Subnet** drop-down list, choose an option from the list of subnets associated with the selected virtual group.
c) (Optional) From the **Network Security Group** drop-down list, choose an option from the list of security groups in the selected Resource Group.
d) From the **SSH public key source** drop-down list, choose whether you want to create a new key pair or use an existing key pair by clicking the corresponding option.
e) If you chose **the Use existing key stored in Azure** option in the previous step, from the **Stored Keys** drop-down list, choose the key you want to use.
f) To assign a static IP address to Cisco ISE, enter an IP address in the **Private IP address** field. Ensure that this IP address is not being used by any other resource in the selected subnet.
g) In the **Public IP Address** drop-down list, choose the address that you want to use with Cisco ISE. If this field is left blank, a public IP address is assigned to the instance by the Azure DHCP server.
h) In the **DNS Name** field, enter the DNS domain name.

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

i) In the **Name Server** field, enter the IP address of the name server.

   Note From Cisco ISE Release 3.4, the **Name Server** field name is changed to **Primary Name Server**.

   In the **Secondary Name Server** field, enter the IP address of the secondary name server. This field is available from Cisco ISE Release 3.4.

   In the **Tertiary Name Server** field, enter the IP address of the tertiary name server. This field is available from Cisco ISE Release 3.4. To use this field and to launch the application successfully, you must not leave the **Secondary Name Server** field blank.

   Note If the entered IP address is incorrect or not reachable, Cisco ISE services may not be launched.

j) In the **NTP Server** field, enter the IP address or hostname of the NTP server. Your entry is not validated upon input.

Note From Cisco ISE Release 3.4, the **NTP Server** field name is changed to **Primary NTP Server**.

In the **Secondary NTP Server** field, enter the IP address or hostname of the secondary NTP server. Your entry is not validated upon input. This field is available from Cisco ISE Release 3.4.

In the **Tertiary NTP Server** field, enter the IP address or hostname of the tertiary NTP server. Your entry is not validated upon input. This field is available from Cisco ISE Release 3.4. To use this field and to launch the application successfully, you must not leave the **Secondary NTP Server** field blank.

Note If the entered IP address is incorrect or not reachable, Cisco ISE services may not be launched.

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

Step 9 Click **Next**.

Step 10 In the **Services** tab:

a) From the **ERS** drop-down list, choose **Yes** or **No**.

b) From the **Open API** drop-down list, choose **Yes** or **No**.

Note From Cisco ISE Release 3.4, OpenAPIs are enabled by default. Hence, this field is not available.

c) From the **pxGrid** drop-down list, choose **Yes** or **No**.

d) From the **pxGrid Cloud** drop-down list, choose **Yes** or **No**.

Step 11 Click **Next**.

Step 12 In the **User Details** tab:

a) In the **Enter Password for iseadmin** and **Confirm Password** fields, enter a password for Cisco ISE. The password must comply with the Cisco ISE password policy and contain a maximum of 25 characters.

Step 13 Click **Next**.

Step 14 In the **Review + create** tab, review the details of the instance.

Step 15 Click **Create**.

The **Overview** window displays the progress in the instance creation process.

Step 16 Use the search bar and navigate to the **Virtual Machines** window. The Cisco ISE instance that you created is listed in the window, with the **Status** as **Creating**. It takes about 30 minutes to create a Cisco ISE instance.

Postinstallation Tasks

For information about the postinstallation 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.

Compatibility Information for Cisco ISE on Azure Cloud

This section details compatibility information that is unique to Cisco ISE on Azure Cloud. For general compatibility details for Cisco ISE, see the Cisco Identity Services Engine Network Component Compatibility guide for your release.

Load Balancer Integration Support

You can integrate the Azure Load Balancer with Cisco ISE for load balancing RADIUS traffic. However, the following caveats are applicable:

- The Change of Authorization (CoA) feature is supported only when you enable client IP preservation when you configure Session Persistence property in the load balancing rule in the Azure portal.

- Unequal load balancing might occur because the Azure Load Balancer only supports source IP affinity and does not support calling station ID-based sticky sessions.
- Traffic can be sent to a Cisco ISE PSN even if the RADIUS service is not active on the node as the Azure Load Balancer does not support RADIUS-based health checks.

For more information on the Azure Load Balancer, see What is Azure Load Balancer?

You can integrate the Azure Load Balancer with Cisco ISE for load balancing TACACS traffic. However, traffic might be sent to a Cisco ISE PSN even if the TACACS service is not active on the node because the Azure Load Balancer does not support health checks based on TACACS+ services.

Password Recovery and Reset on Azure Cloud

The following tasks guide you through 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.

Note The **Help** > **Reset Password** option in the Azure portal is not supported for Cisco ISE Azure VM.

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 **Help** section, click **Serial console**.

Step 4 If you view an error message here, you may have to enable boot diagnostics by carrying out the following steps:

a) From the left-side menu, click **Boot diagnostics**.
b) Click **Enable with custom storage account**.
c) Choose the storage account and click **Save**.

Step 5 From the left-side menu, from the **Help** section, click **Serial console**.

Step 6 The Azure Cloud Shell is displayed in a new window.

Step 7 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. If you do not remember this password, see the Password Recovery section.

Step 9 Use the **application reset-passwd ise iseadmin** command to configure a new GUI password for the iseadmin account.

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. See Generate and store SSH keys in the Azure portal.

Step 2 Log in to the Azure Cloud serial console as detailed in the preceding task.

Step 3 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 4.

Step 4 To import the new Public Key, use the command **crypto key import <public key filename> repository <repository name>**

Step 5 When the import is complete, you can log in to Cisco ISE via SSH using the new public key.