Installing the Controller in Microsoft Azure Cloud Service

Using Private IP

Overview on Microsoft Azure Cloud Service

Microsoft Azure Cloud Service provides user capability to launch the controller in the cloud infrastructure. In this chapter, you will see how to make your controller as one of the services that can be initiated and used in Azure Cloud.

Note Cisco Catalyst 9800 Wireless Controller for Cloud - Ultra-Low Profile is not supported on public cloud.

Prerequisites

Before attempting to launch the controller on Azure, the following prerequisites should be met:

- Create an Azure account.
- Install an SSH client (for example, Putty on Windows or Terminal on Macintosh) to access the controller console.
- Determine the instance type that you want to deploy.
- Create a Virtual Network (VNet).
- Create a VPN gateway.
- Create subnets.
- For each remote site, create:
    - Create a customer gateway

- Create a VPN connection.

Note The AP in Sniffer mode is not supported in Azure Cloud.

Note You need to create the Resource Groups beforehand.

The following services must be created in the Resource Group:

- Create a Virtual Network (VNet).
- Create a VPN gateway.

Additionally, the following services must be created in the Resource Group:

- Create a customer gateway.
- Create a VPN connection.

Creating a Resource Group

Perform the following procedure to create a resource group:

Step 1 Log in to the Azure Web UI.

Step 2 In the search area, type **resource group**.

Step 3 Under **Services**, choose **Resource groups**.

The **Resource groups** window is displayed.

Step 4 Click **Create**.

The **Create a resource group** window is displayed.

Step 5 In the **Basics** tab, configure the **Project details** and **Resource details**.

Perform the following in the **Project details** and **Resource details** area:

- **Subscription**: Verify if the subscription listed is the correct one. You can change the subscriptions using the drop-down list.
- **Resource group**: Select an existing resource group, or click **Create new** to create a new one. For more information about resource groups, see Azure Resource Manager Overview.
- **Region**: Select the location for your resource group.

Step 6 Click **Review + create** to validate the resource group.

Step 7 Click **Create** after the resource group is validated.

Creating a Virtual Network (VNet)

Perform the following procedure to configure a VNet in Azure:

Before you begin

You can specify an IP address range for the VNet, add subnets, associate security groups, and configure route tables.

Note The AP join to public IP does not require VPN connection.

Step 1 Log in to the Azure Web UI.

Step 2 In the search area, type **virtual network**.

Step 3 Under **Services**, choose **Virtual Network**.

The **Virtual Network** window is displayed.

Step 4 Click **Create**.

The **Create virtual network** window is displayed.

Step 5 In the **Basics** tab, configure the **Project details** and **Instance details** for Azure Virtual Network (VNet) settings.

In the **Project details** and **Instance details** area, perform the following:

- **Subscription**: Verify if the subscription listed is the correct one. You can change the subscriptions using the drop-down list.
- **Resource group**: Select an existing resource group, or click **Create new** to create a new one. For more information about resource groups, see Azure Resource Manager Overview.
- **Name**: Enter the name for your virtual network.
- **Region**: Select the location for your VNet.

Step 6 In the **IP Addresses** tab, configure the following:

- **IPv4 address space**: By default, an address space is automatically created. You can click the address space to adjust it to reflect your own values.
- **Subnet**: If you use the default address space, a default subnet is created automatically. If you change the address space, you need to add a subnet. Select **+ Add subnet** to open the **Add subnet** window. You need to configure the following settings and click **Add** to add the values:
  - **Subnet name**: For example, you can name the subnet as **FrontEnd**.
  - **Subnet address range**: You can provide the subnet address range for this subnet.

Step 7 In the **Security** tab, retain the default values for the following:

- **DDos protection**: Disabled
- **Firewall**: Disabled

Step 8 Click **Review + create** to validate the virtual network settings.

Step 9 Click **Create** after the settings are validated.

Creating a Virtual Private Gateway

Perform the following procedure to create an Azure Virtual Private Gateway:

Step 1 Log in to the Azure Web UI.

Step 2 In the search area, type **virtual network gateway**.

Step 3 Under **Services**, choose **Virtual network gateway**.

The **Virtual network gateways** window is displayed.

Step 4 Click **Create**.

The **Create virtual network gateway** window is displayed.

Step 5 In the **Basics** tab, configure the **Project details** and **Instance details** for Azure Virtual Network (VNet) settings.

In the **Project details** and **Instance details** area, perform the following:

- **Subscription**: Select the subscription you want to use from the drop-down list.
- **Resource group**: This setting is auto-filled when you select your virtual network on this page.
- **Name**: Enter the name for your gateway.
- **Region**: Select the region you want to create this resource.

  Note The region for the gateway must be the same as the virtual network.

- **Gateway type**: Select VPN.
- **VPN type**: Select the VPN type that is specified for your configuration.
- **SKU**: Select the gateway SKU you want to use from the drop-down list. Based on the VPN type you selected earlier, you get to view the SKUs. For more information about gateway SKUs, see Gateway SKUs.
- **Generation**: Select the generation you want to use. For more information, see Gateway SKUs.
- **Virtual network**: From the drop-down list, select the virtual network to which you want to add this gateway.
- **Gateway subnet address range**: This field appears only if your VNet does not have a gateway subnet.

  Note We recommend you create a range greater than /28.

  Click **Subnets** to view the range. If you want to change the range, you can delete and recreate the Gateway subnet.

Step 6 Specify the values for **Public IP address**.

In the **Public IP address** area, perform the following:

- **Public IP address**: Retain **Create new** value.

- **Public IP address name**: Enter a name for your Public IP address instance.
- **Assignment**: By default, the VPN gateway supports only **Dynamic**.
- **Enable active-active mode**: Select this mode only if you want to create an active-active gateway. Otherwise, leave this setting as **Disabled**.
- **Configure BGP**: Disable this mode unless your configuration specifically requires this setting. If you require this setting, the default ASN is 65515, although this can be changed.

Step 7 Click **Review + create** to validate.

Step 8 Click **Create** after the settings are validated and deploy the VPN gateway.

You can view the deployment status in the **Overview** page for your gateway.

Note A gateway takes approximately 45 minutes to create and deploy.

After creating the gateway, you can view the IP address assigned to the gateway by viewing the virtual network in the Azure Web UI.

The gateway appears as a connected device.

Creating a Customer Gateway

Perform the following procedure to create a local network gateway:

Before you begin

The local network gateway is a specific object that represents your on-premises location (the site) for routing purposes. You give the site a name by which Azure can refer to it, then specify the IP address of the on-premise VPN device to which you will create a connection. You also specify the IP address prefixes that will be routed through the VPN gateway to the VPN device. The address prefixes you specify are the prefixes located on your on-premises network. If your on-premises network changes or you need to change the public IP address for the VPN device, you can easily update the values later.

Step 1 Log in to the Azure Web UI.

Step 2 In the search area, type **local network gateway**.

Step 3 Under **Services**, choose **Local network gateway**.

The **Create local network gateway** window is displayed.

Step 4 Specify the following for your local network gateway:

- **Name**: Specify a name for your local network gateway object.
- **Endpoint**: Select the endpoint type for the on-premises VPN device **IP address** or **FQDN (Fully Qualified Domain Name)**.
  - **IP address**: If you have a static public IP address allocated from your Internet service provider for your VPN device, select the IP address option and fill in the IP address as shown in the example. This is the public IP address of the VPN device that you want Azure VPN gateway to connect to. If you don't have the IP address

right now, you can use the values shown in the example, but you'll need to go back and replace your placeholder IP address with the public IP address of your VPN device. Otherwise, Azure will not be able to connect.

- **FQDN**: If you have a dynamic public IP address that could change after certain period of time, usually determined by your Internet service provider, you can use a constant DNS name with a Dynamic DNS service to point to your current public IP address of your VPN device. Your Azure VPN gateway will resolve the FQDN to determine the public IP address to connect to.

- **Address Space**: Refers to the address range for the local network. You can add multiple address space ranges. Make sure that the ranges you specify here do not overlap with ranges of other networks that you want to connect to. Azure will route the address range that you specify to the on-premises VPN device IP address.
- **Configure BGP settings**: Use only when configuring BGP. Otherwise, don't select this.
- **Subscription**: Verify is the correct subscription is displayed or not.
- **Resource Group**: Select the resource group that you want to use. You can either create a new resource group, or select one that you have already created.
- **Location**: The location is the same as **Region** in other settings. Select the location that this object will be created in. You may want to select the same location that your VNet resides in, but you are not required to do so.

Step 5 Click **Create** to create the local network gateway.

Creating a VPN Connection

Perform the following procedure to create a VPN connection:

Step 1 Log in to the Azure Web UI.

Step 2 In the search area, type **virtual network gateway**.

Step 3 Under **Services**, choose **Virtual network gateway**.

The **Virtual network gateways** window is displayed.

Step 4 Choose **Name of your VNet** > **Overview** > **Connected devices** > **Name of your gateway**.

Step 5 In the **Gateway** window, select **Connections** to view the **Connections** window.

Step 6 Select **+Add** to view the **Add connection** window.

In the **Add connection** window, configure the following values for your connection:

- **Name**: Enter a name for your connection.
- **Connection type**: Choose **Site-to-site (IPSec)**.
- **Virtual network gateway**: The value is fixed because you are connecting from this gateway
- **Local network gateway**: Select **Choose a local network gateway** and select the local network gateway that you want to use.
- **Shared Key**: This value must match the value you are using for your local on-premise VPN device. The important thing is that the value you specify here must be the same value that you specify when configuring your VPN device.

Note We recommend that you specify the same value when configuring the VPN device.

- Leave **Use Azure Private IP Address** unchecked.
- Leave **Enable BGP** unchecked.
- Choose **IKEv2** as the IKE protocol.

Note The **Subscription**, **Resource Group**, and **Location** values are fixed.

Step 7 Click **OK** to create your connection.

You can view the connection in the **Connections** page of the virtual network gateway. The Status goes from *Unknown* to *Connecting*, and then to *Succeeded*.

Installing the Controller Using Azure Portal

Perform the following procedure to install controller with Azure portal:

Step 1 Log in to the Azure Web UI.

Step 2 In the search area, type **virtual machines**.

Step 3 Under **Services**, choose **Virtual machines**.

Step 4 In the **Virtual machines** window, select **Create** and then **Virtual machine**.

Step 5 In the **Basics** tab and **Project details** section, perform the following:

- **Subscription**: Verify if the subscription listed is the correct one. You can change the subscriptions using the drop-down list.
- **Resource group**: Select an existing resource group, or click **Create new** to create a new one. For more information about resource groups, see Azure Resource Manager Overview.

Step 6 In the **Instance details** area, perform the following:

- **Virtual machine name**: Enter the name of your virtual machine or controller name.
- **Region**: Select the Azure data center region.
- **Image**: Choose a C9800-CL image.
- **Size**: Choose the VM size for different scale.

Note You can retain the other defaults.

The following table shows the scale and VM size details:

Table 1: Scale and VM Size Details

Scale	VM Size
Small	F4s v2

Scale	VM Size
Medium	F8s v2
High	F16s v2

Step 7 Under **Administrator account**, perform the following:

- **Authentication type**: Choose the **Password** option.
- **Username**: Enter a username.
- **Password**: Enter a password.

Note The password must be at least 12 characters long. For information about the requirements, see defined complexity requirements.

Step 8 Under **Inbound port rules**, perform the following:

- **Public inbound ports**: Choose **Allow selected ports**.
- **Select inbound ports**: Choose **HTTPS (443), SSH (22)** from the drop-down list.

Step 9 From the **Licensing** area, choose **License type** as **Other**.

Step 10 Click **Review + create** to validate the details.

The **Create a virtual machine** window appears.

Step 11 Click the **Networking** tab and perform the following:

- **Virtual network**: Choose the virtual network created while creating the VPN.
- **Subnet**: Choose an appropriate subnet created while creating the VPN.
- **Public IP**: Creates a new one.
- **NIC network security group**: Choose **Advanced**.
- **Configure network security group**: Choose an existing security group from the drop-down list, if you had created one earlier. (Or) Click **Create new** to create a new network security group.

Note You can restrict access to your security group instance for security reasons. For example, if you want to permit only CAPWAP from a certain IP range so that only those APs register to the controller, you need to enable inbound and outbound.

The following table lists the ports and protocols that may be enabled on the controller:

By default, all the outbound traffics are unblocked only the inbound traffics are blocked.

You may allow these protocols based on your service and security requirements.

Table 2: Ports and Protocol

Ports	Protocols
UDP 5246/5247/5248	CAPWAP
TCP 22	SSH, SCP
TCP 21	FTP
ICMP	Ping
UDP 161, 162	SNMP/SNMP traps
TCP 443/80	HTTPs/HTTP
TCP/UDP 49	TACACS+
UDP 53	DNS Server
UDP 1812/1645/1813/1646	Radius
UDP 123	NTP Server
UDP 514	Syslog

Step 12 Click the **Advanced** tab and perform the following:

- **Custom data**: Enter the custom IOS config meta data.

  Note This custom IOS configuration meta data is applied in bootstrap.

  If the same information is available in the deployment and custom data, the deployment data takes precedence.

Step 13 Retain the other default values and click **Review + create**.

Step 14 Click **Create** after the settings are validated.

Step 15 Click **Go to resource** after the deployment is complete.

Step 16 To make the Serial console accessible, navigate to **Boot diagnostics** in **Support + troubleshooting**.

Step 17 Choose the **Enable with custom storage account** settting.

Step 18 Choose an existing storage account or create a new one.

You can now navigate to the Day 0 configuration using either serial console, SSH to the controller, or Web UI.

Using Public IP

Creating a Resource Group

Perform the following procedure to create a resource group:

Step 1 Log in to the Azure Web UI.

Step 2 In the search area, type **resource group**.

Step 3 Under **Services**, choose **Resource groups**.

The **Resource groups** window is displayed.

Step 4 Click **Create**.

The **Create a resource group** window is displayed.

Step 5 In the **Basics** tab, configure the **Project details** and **Resource details**.

Perform the following in the **Project details** and **Resource details** area:

- **Subscription**: Verify if the subscription listed is the correct one. You can change the subscriptions using the drop-down list.
- **Resource group**: Select an existing resource group, or click **Create new** to create a new one. For more information about resource groups, see Azure Resource Manager Overview.
- **Region**: Select the location for your resource group.

Step 6 Click **Review + create** to validate the resource group.

Step 7 Click **Create** after the resource group is validated.

Creating a Virtual Network (VNet)

Perform the following procedure to configure a VNet in Azure:

Before you begin

You can specify an IP address range for the VNet, add subnets, associate security groups, and configure route tables.

Note The AP join to public IP does not require VPN connection.

Step 1 Log in to the Azure Web UI.

Step 2 In the search area, type **virtual network**.

Step 3 Under **Services**, choose **Virtual Network**.

The **Virtual Network** window is displayed.

Step 4 Click **Create**.

The **Create virtual network** window is displayed.

Step 5 In the **Basics** tab, configure the **Project details** and **Instance details** for Azure Virtual Network (VNet) settings.

In the **Project details** and **Instance details** area, perform the following:

- **Subscription**: Verify if the subscription listed is the correct one. You can change the subscriptions using the drop-down list.
- **Resource group**: Select an existing resource group, or click **Create new** to create a new one. For more information about resource groups, see Azure Resource Manager Overview.
- **Name**: Enter the name for your virtual network.
- **Region**: Select the location for your VNet.

Step 6 In the **IP Addresses** tab, configure the following:

- **IPv4 address space**: By default, an address space is automatically created. You can click the address space to adjust it to reflect your own values.
- **Subnet**: If you use the default address space, a default subnet is created automatically. If you change the address space, you need to add a subnet. Select **+ Add subnet** to open the **Add subnet** window. You need to configure the following settings and click **Add** to add the values:
  - **Subnet name**: For example, you can name the subnet as **FrontEnd**.
  - **Subnet address range**: You can provide the subnet address range for this subnet.

Step 7 In the **Security** tab, retain the default values for the following:

- **DDos protection**: Disabled
- **Firewall**: Disabled

Step 8 Click **Review + create** to validate the virtual network settings.

Step 9 Click **Create** after the settings are validated.

Installing the Controller Using Azure Portal

Perform the following procedure to install controller with Azure portal:

Step 1 Log in to the Azure Web UI.

Step 2 In the search area, type **virtual machines**.

Step 3 Under **Services**, select **Virtual machines**.

Step 4 In the **Virtual machines** window, select **Create** and then **Virtual machine**.

Step 5 In the **Basics** tab and **Project details** section, perform the following:

- **Subscription**: Verify if the subscription listed is the correct one. You can change the subscriptions using the drop-down list.
- **Resource group**: Select an existing resource group, or click **Create new** to create a new one. For more information about resource groups, see Azure Resource Manager Overview.

Step 6 In the **Instance details** area, perform the following:

- **Virtual machine name**: Enter the name of your virtual machine or controller name.
- **Region**: Select the Azure data center region.
- **Image**: Choose a C9800-CL image.
- **Size**: Choose the VM size for different scale.

Note You can retain the other defaults.

The following table shows the scale and VM size details:

Table 3: Scale and VM Size Details

Scale	VM Size
Small	F4s v2
Medium	F8s v2
High	F16s v2

Step 7 Under **Administrator account**, perform the following:

- **Authentication type**: Choose the **Password** option.
- **Username**: Enter a username.
- **Password**: Enter a password.

Note The password must be at least 12 characters long. For information about the requirements, see defined complexity requirements.

Step 8 Under **Inbound port rules**, perform the following:

- **Public inbound ports**: Choose **Allow selected ports**.
- **Select inbound ports**: Choose **HTTPS (443), SSH (22)** from the drop-down list.

Step 9 From the **Licensing** area, choose **License type** as **Other**.

Step 10 Click **Review + create** to validate the details.

The **Create a virtual machine** window appears.

Step 11 Click the **Networking** tab and perform the following:

- **Virtual network**: Choose the virtual network that was created earlier or create a new one.
- **Subnet**: Choose the subnet that was created earlier or create a new one.
- **Public IP**: Creates a new one.
- **NIC network security group**: Choose **Advanced**.
- **Configure network security group**: Choose an existing security group from the drop-down list, if you had created one earlier. (Or) Click **Create new** to create a new network security group.

Note You can restrict access to your security group instance for security reasons. For example, if you want to permit only CAPWAP from a certain IP range so that only those APs register to the controller, you need to enable inbound and outbound.

The following table lists the ports and protocols that may be enabled on the controller:

By default, all the outbound traffics are unblocked only the inbound traffics are blocked.

You may allow these protocols based on your service and security requirements.

Table 4: Ports and Protocol

Ports	Protocols
UDP 5246/5247/5248	CAPWAP
TCP 22	SSH, SCP
TCP 21	FTP
ICMP	Ping
UDP 161, 162	SNMP/SNMP traps
TCP 443/80	HTTPs/HTTP
TCP/UDP 49	TACACS+
UDP 53	DNS Server
UDP 1812/1645/1813/1646	Radius
UDP 123	NTP Server
UDP 514	Syslog

Step 12 Click the **Advanced** tab and perform the following:

- **Custom data**: Enter the custom IOS config meta data.

Note This custom IOS configuration meta data is applied in bootstrap.

If the same information is available in the deployment and custom data, the deployment data takes precedence.

Step 13 Retain the other default values and click **Review + create**.

Step 14 Click **Create** after the settings are validated.

Step 15 Click **Go to resource** after the deployment is complete.

Step 16 To make the Serial console accessible, choose **Boot diagnostics** > **Support + troubleshooting**.

Step 17 Choose **Enable with custom storage account** settting.

Step 18 Choose an existing storage account or create a new one.

You can now navigate to the Day 0 configuration using either serial console, SSH to the controller, or Web UI.

Enabling Public IP on the Controller

Perform the following procedure to enable the Wireless Management Interface with Public IP:

Before you begin

- The controller has two types of IPs:
  - Private IP
  - Public IP

Note By default, the public IP is not enabled.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device> configure terminal`	Enters global configuration mode.
Step 2	**wireless management interface** *interface-type interface-number* **Example:** `Device(config)# wireless management interface gigabit1`	Defines the management interface. Where, • *interface-type* refers to the Gigabit interface. • *interface-number* is 1.

	Command or Action	Purpose
		Note The Public cloud VM supports only the following: • Gigabit as the interface-type. • 1 as the interface-number.
Step 3	**public-ip** *public-ip* **Example:** `Device(config-mgmt-interface)# public-ip 2.2.2.2`	Defines the external Public IP.
Step 4	**end** **Example:** `Device(config-mgmt-interface)# end`	Returns to privileged EXEC mode.

Enabling CAPWAP Discovery to Respond Only with Public or Private IP

- By default, the CAPWAP discovery response covers both private and public IP.
- To enable the controller to respond only with a private or public IP, see the *Configuring CAPWAP Discovery to Respond Only with Public or Private IP (CLI)* section in Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide.

AP Authorization Configuration

Kindly refer to the following link:

https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213916-catalyst-9800-wireless-controllers-ap-au.html

Note When priming the AP, ensure that you use the Public IP to connect to the controller. You can restrict the APs using AP authorization.