**Manage Private Communications**

**Create a private endpoint for a secure connection to Azure AI Search**

**Why use a private endpoint?**

[Private endpoints](https://learn.microsoft.com/en-us/azure/private-link/private-endpoint-overview) for Azure AI Search allow a client on a virtual network to securely access data in a search index over a [Private Link](https://learn.microsoft.com/en-us/azure/private-link/private-link-overview). The private endpoint uses an IP address from the [virtual network address space](https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/private-ip-addresses) for your search service. Network traffic between the client and the search service traverses over the virtual network and a private link on the Microsoft backbone network, eliminating exposure from the public internet. For a list of other PaaS services that support Private Link, check the [availability section](https://learn.microsoft.com/en-us/azure/private-link/private-link-overview#availability) in the product documentation.

Private endpoints for your search service allow you to:

* Block all connections on the public endpoint for your search service.
* Increase security for the virtual network, by letting you block exfiltration of data from the virtual network.
* Securely connect to your search service from on-premises networks that connect to the virtual network using [VPN](https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways) or [ExpressRoutes](https://learn.microsoft.com/en-us/azure/expressroute/expressroute-locations) with private-peering.

**Create the virtual network**

In this section, you create a virtual network and subnet to host the VM that will be used to access your search service's private endpoint.

1. From the Azure portal home tab, select Create a resource > Networking > Virtual network.
2. In Create virtual network, enter or select the following values:

A screenshot of a phone

Description automatically generated

1. Accept the defaults for the rest of the settings. Select **Review + create** and then **Create**.

**Create a search service with a private endpoint**

In this section, you create a new Azure AI Search service with a private endpoint.

1. On the upper-left side of the screen in the Azure portal, select Create a resource > AI + machine learning > AI Search.
2. In Create a search service - Basics, enter or select the following values:

A screenshot of a computer

Description automatically generated

1. Select **Next: Scale**.
2. Accept the defaults and select **Next: Networking**.
3. In **Create a search service - Networking**, select **Private** for **Endpoint connectivity (data)**.
4. Select **+ Add** under **Private endpoint**.
5. In **Create private endpoint**, enter or select values that associate your search service with the virtual network you created:

**A screenshot of a computer

Description automatically generated**

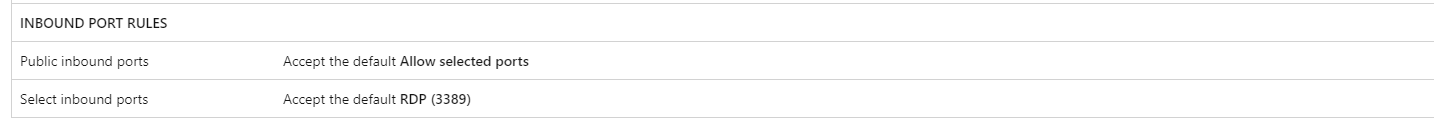
1. Select Add.
2. Select Review + create. You're taken to the Review + create page where Azure validates your configuration.
3. When you see the Validation passed message, select Create.
4. Once provisioning of your new service is complete, browse to the resource that you created.
5. Select Settings > Keys from the left content menu.
6. Copy the Primary admin key for later, when connecting to the service.

**Create a virtual machine**

1. On the upper-left side of the screen in the Azure portal, select Create a resource > Compute > Virtual machine.
2. In Create a virtual machine - Basics, enter or select the following values:

A screenshot of a computer

Description automatically generated



1. Select Next: Disks.
2. In Create a virtual machine - Disks, accept the defaults and select Next: Networking.
3. In Create a virtual machine - Networking, provide the following values:

**A screenshot of a phone

Description automatically generated**

1. Select Review + create for a validation check.
2. When you see the Validation passed message, select Create.

**Connect to the VM**

Download and then connect to the virtual machine as follows:

1. In the portal's search bar, search for the virtual machine created in the previous step.
2. Select **Connect**. After selecting the **Connect** button, **Connect to virtual machine** opens.
3. Select **Download RDP File**. Azure creates a Remote Desktop Protocol (*.rdp*) file and downloads it to your computer.
4. Open the downloaded *.rdp* file.

* If prompted, select **Connect**.
* Enter the username and password you specified when creating the VM.

1. Select **OK**.
2. You might receive a certificate warning during the sign-in process. If you receive a certificate warning, select **Yes** or **Continue**.
3. Once the VM desktop appears, minimize it to go back to your local desktop.

**Test connections**

In this section, you verify private network access to the search service and connect privately to the using the Private Endpoint.

When the search service endpoint is private, some portal features are disabled. You can view and manage service level settings, but portal access to index data and various other components in the service, such as the index, indexer, and skillset definitions, is restricted for security reasons.

1. In the Remote Desktop of *myVM*, open PowerShell.
2. Enter nslookup [search service name].search.windows.net.

You'll receive a message similar to this:

**A screenshot of a computer

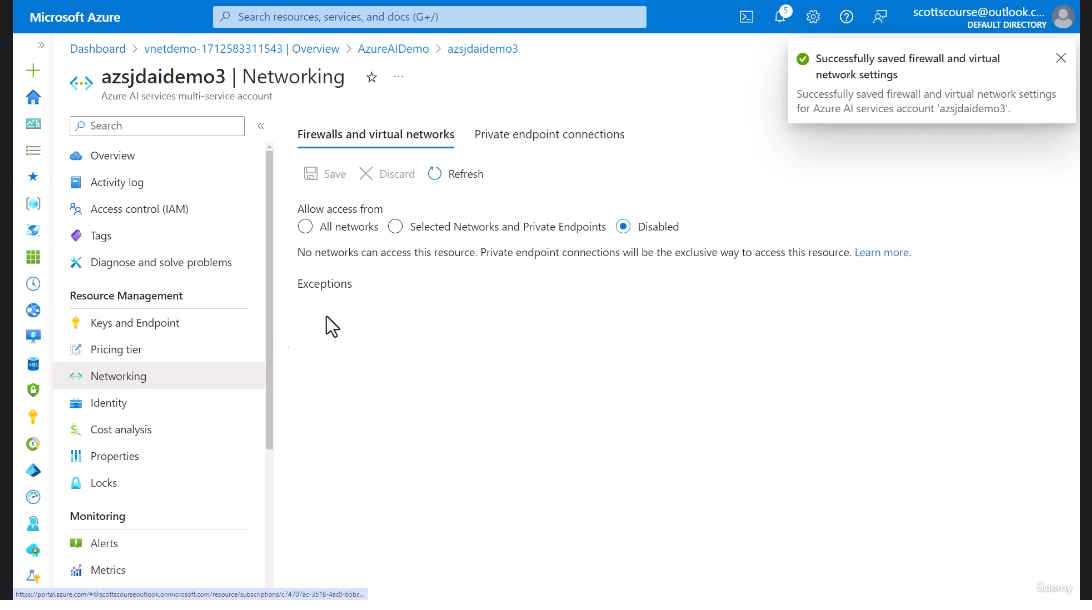
Description automatically generated**

1. From the VM, connect to the search service and create an index. You can follow this [quickstart](https://learn.microsoft.com/en-us/azure/search/search-get-started-rest) to create a new search index in your service using the REST API. Setting up requests from a Web API test tool requires the search service endpoint (https://[search service name].search.windows.net) and the admin api-key you copied in a previous step.
2. Completing the quickstart from the VM is your confirmation that the service is fully operational.
3. Close the remote desktop connection to *myVM*.
4. To verify that your service isn't accessible on a public endpoint, open a REST client on your local workstation and attempt the first several tasks in the quickstart. If you receive an error that the remote server doesn't exist, you successfully configured a private endpoint for your search service.

**Disable public network access**

You can lock down a search service to prevent it from admitting any request from the public internet. You can use the Azure portal for this step.

1. In the Azure portal, on the leftmost pane of your search service page, select Networking.
2. Select Disabled on the Firewalls and virtual networks tab.



You can also use the [Azure CLI](https://learn.microsoft.com/en-us/cli/azure/search/service?view=azure-cli-latest#az-search-service-update&preserve-view=true), [Azure PowerShell](https://learn.microsoft.com/en-us/powershell/module/az.search/set-azsearchservice), or the [Management REST API](https://learn.microsoft.com/en-us/rest/api/searchmanagement/), by setting public-access or public-network-access to disabled.