



Granting IronFort Access to Your Microsoft Azure Environment

What Is This?

IronFort is a compliance and security platform that scans your Microsoft Azure environment to identify vulnerabilities, misconfigurations, and potential risks. This helps your organization stay secure and meet compliance requirements.

To perform these scans, IronFort uses a **Microsoft Entra application (service principal)** with **read-only access** to your Azure subscription or resource group. This means IronFort can view your configuration and security posture, but **cannot make any changes** to your environment.

How IronFort Accesses Your Azure Environment

- You create a dedicated **App registration** in your Microsoft Entra tenant for IronFort.
 - Azure automatically creates a corresponding **service principal** for that application.
 - You assign that service principal **read-only Azure RBAC roles** at the appropriate scope.
 - You provide IronFort with the application's **Tenant ID**, **Client ID**, and **Client Secret** using a secure sharing method.
 - When a scan runs, IronFort authenticates as that application and reads your Azure configuration. Nothing is modified, deleted, or written.
 - All data collected is handled in accordance with IronFort's privacy and security policies.
-

Step-by-Step Setup Instructions

What You Will Need

- Access to the [Azure portal](#)
 - One of the following permission sets:
 - Rights to register an application in **Microsoft Entra ID**
 - Rights to assign Azure roles at the target scope, such as **Owner**, **User Access Administrator**, or **Role Based Access Control Administrator**
 - The Azure subscription(s) or resource group(s) you want IronFort to scan
 - A secure method to share credentials with IronFort
-

Step 1 — Sign In to the Azure Portal

1. Go to <https://portal.azure.com>
 2. Sign in with an account that has permission to register applications and assign Azure roles.
-

Step 2 — Create an App Registration

1. In the portal search bar, search for **Microsoft Entra ID** and open it.
2. In the left-hand menu, select **App registrations**.
3. Click **+ New registration**.
4. In the **Name** field, enter a descriptive name such as:

`ironfort-compliance`

5. Under **Supported account types**, leave the default selection for accounts in your organization only unless your internal policy requires otherwise.
6. Leave the **Redirect URI** blank.
7. Click **Register**.

Step 3 — Record the Application Details

After the app registration is created, Azure displays the app overview page.

Record the following values:

- **Application (client) ID**
- **Directory (tenant) ID**

You will provide these values to IronFort later.

Step 4 — Create a Client Secret

1. Inside the app registration, select **Certificates & secrets**.
2. Under **Client secrets**, click **+ New client secret**.
3. Enter a description such as:

`IronFort scanning access`

4. Choose an expiration period that aligns with your internal policy.
5. Click **Add**.

Important: Azure only shows the client secret value once. Copy it immediately and store it securely.

Record the following value:

- **Client secret Value**

Step 5 — Decide the Scope of Access

Choose the scope you want IronFort to scan:

- **Subscription scope** if IronFort should review an entire Azure subscription

- **Resource group scope** if IronFort should only review a specific workload or environment

Recommendation: Use the narrowest scope that meets your requirements. If you want IronFort to scan multiple subscriptions, repeat the role assignment steps for each subscription.

Step 6 — Assign Read-Only Azure Roles

1. Go to the subscription or resource group you want IronFort to scan.
2. In the left-hand menu, select **Access control (IAM)**.
3. Open the **Role assignments** tab.
4. Click **Add > Add role assignment**.

Assign the Reader Role

1. On the **Role** tab, search for **Reader**.
2. Select **Reader**.
3. Click **Next**.
4. On the **Members** tab, select **User, group, or service principal**.
5. Click **Select members**.
6. Search for the application name you created earlier, for example:

`ironfort-compliance`

7. Select it and click **Select**.
8. Click **Review + assign**.
9. Click **Review + assign** again to complete the assignment.

Assign the Security Reader Role

1. Repeat the same process.
2. On the **Role** tab, search for **Security Reader**.
3. Select **Security Reader**.
4. Assign it to the same service principal.

Note: These roles are read-only. They allow IronFort to view Azure resources, configuration, and security findings, but they do not allow any changes to be made.

Step 7 — Share the Credentials with IronFort

Provide the following values to your IronFort contact using a secure sharing method:

- **Directory (tenant) ID**
- **Application (client) ID**
- **Client secret value**
- The **subscription ID(s)** or **resource group name(s)** that should be scanned

Security Note: Treat the client secret like a password. Do not send it over unsecured email or chat unless your organization approves that method. Your IronFort contact can provide a secure alternative if needed.

Step 8 — Confirm Access

Once IronFort receives the required values, your IronFort contact will verify the connection and begin your first scan.

If the connection test succeeds but the scan still fails, the most common causes are:

- The app registration was created in the wrong tenant
- The wrong client secret was shared
- The service principal was not granted access at the correct scope
- The required role assignments have not propagated yet

Azure role assignment changes can take a short time to become fully effective.

Optional Part 2 — Granting Access to the IronFort Compliance Team for Manual Review

Why Is This Needed?

In addition to automated scans, IronFort's compliance specialists may conduct **manual reviews** of your Azure environment. These reviews help assess your organization against recognized compliance frameworks, including:

- **HIPAA** — Health Insurance Portability and Accountability Act
- **SOC 2** — System and Organization Controls 2
- **ISO 27001** — International information security standard
- **ITSG-33** — IT Security Guidance for the Government of Canada
- **NIST** — National Institute of Standards and Technology Cybersecurity Framework

These reviews go beyond what automated tools can catch. Our compliance specialists examine how resources are configured together, identify gaps in controls, and map findings to the specific requirements of each framework.

How This Works

If a manual review is required, your IronFort contact can provide the **Microsoft Entra user or group** that should receive read-only access for the review.

The recommended access model is the same:

- Assign **Reader**
- Assign **Security Reader**
- Use the narrowest practical scope, such as subscription or resource group

Step-by-Step: Add the IronFort Compliance Reviewer

1. Go to the subscription or resource group to be reviewed.
2. Open **Access control (IAM)**.
3. Click **Add > Add role assignment**.
4. Assign **Reader** to the Microsoft Entra user or group provided by IronFort.
5. Repeat and assign **Security Reader** to the same identity.
6. Confirm the role assignments appear in the role assignment list.

Note: This access is intended to remain read-only. No changes can be made to your environment with these roles.

Frequently Asked Questions

Can IronFort make changes to my Azure environment?

No. The recommended Azure RBAC roles in this guide are read-only. IronFort cannot create, modify, or delete your Azure resources.

What data does IronFort collect?

IronFort reads resource configurations, role assignments, security findings, and related metadata needed to identify security and compliance issues. No application data or customer business data is accessed as part of this read-only scan setup.

Can I revoke access?

Yes. At any time, you can remove the **Reader** and **Security Reader** role assignments from the service principal or delete the app registration entirely.

Do I need to repeat this for multiple subscriptions?

Yes. If you want IronFort to scan multiple Azure subscriptions, assign the required roles at each subscription or at another approved scope that covers the resources you want reviewed.

Can I use a resource group instead of a whole subscription?

Yes. If you want to limit the scan to a specific workload, you can assign the roles at the **resource group** scope instead of the subscription scope.

What if the connection test succeeds but the scan still fails?

The most common causes are:

- The service principal does not have both required read-only roles
- Access was assigned at the wrong scope
- The wrong tenant ID, client ID, or client secret was provided
- Azure role assignments have not fully propagated yet

Should we use a client secret or a certificate?

Azure supports both. A certificate is generally more secure, but a client secret is simpler to set up and is appropriate if that matches your internal process and IronFort onboarding flow.

Need Help?

If you have any questions or need assistance with these steps, please don't hesitate to reach out.

Email: hello@goironfort.com

We're happy to walk you through the setup or answer any questions you may have.