Managed Private Firewall - User Guide

Version 1.0, October 2024

Contents

1. Introduction

It's about focusing on what truly matters, business objectives, while maintaining a secure, impenetrable network environment.

Managed Private Firewall (MPF) diligently monitors and manages incoming and outgoing network traffic, following a customer-controlled firewall rule set. Our global team of technical experts provides guaranteed infrastructure uptime, self-serve administration, and turnkey access to market-leading technology.

MPF is a virtual appliance built in a redundant configuration on High Availability digital infrastructure, ensuring accelerated time to market, eliminating logistical risk, and predictable expense management.

The benefits of the service include the following:

- Access to Market Leading technology.
- No major investments upfront
- Easy and quick upscaling of the required capacity
- Choice of additional functionality on top of the Next-Generation Firewall, such as Intrusion Prevention and Threat Protection.
- Self-service portal for policy configuration and access to reporting.
- High availability through an active-passive firewall pair setup.
- Managed by an experienced and certified Equinix Security Team.

Please refer to MPF Service Description for a full list of features and information.

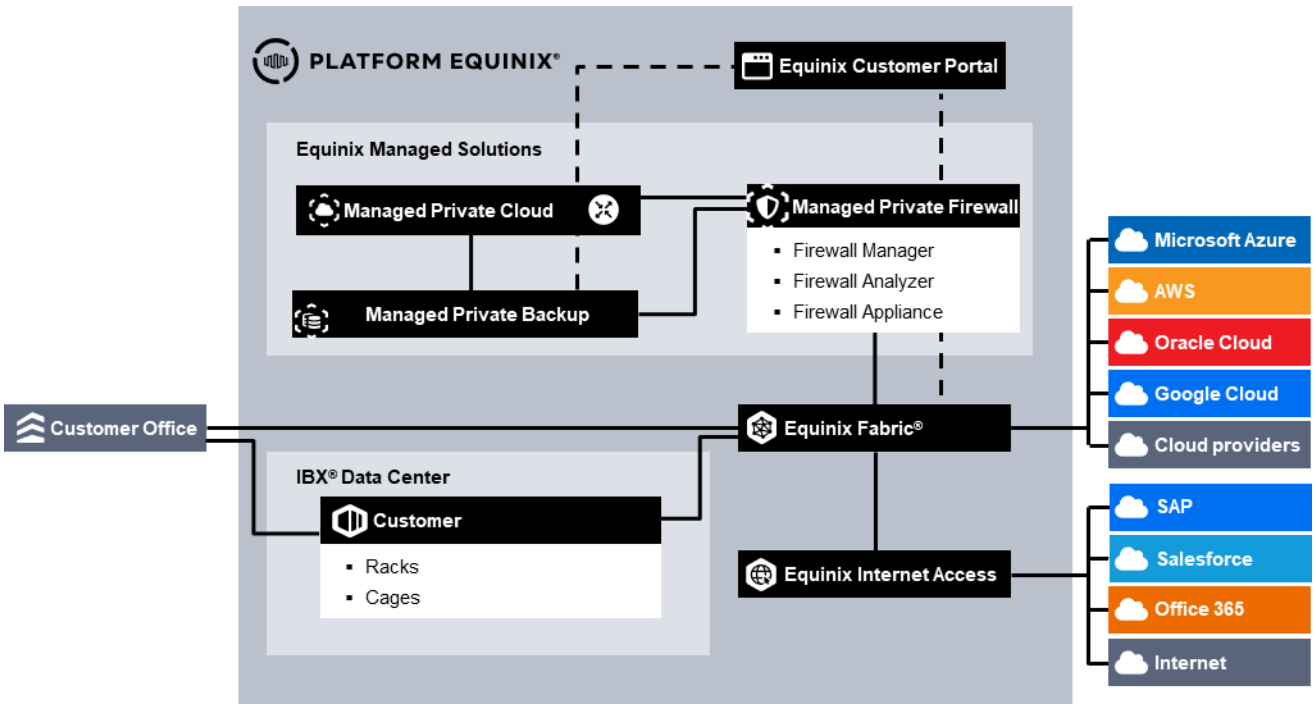


Figure 1 Overview MPF

2. Concepts

To gain a good understanding of the names and terms used later on in in this document, they will be explained first.

2.1 Equinix Customer Portal and Managed Solutions Portal

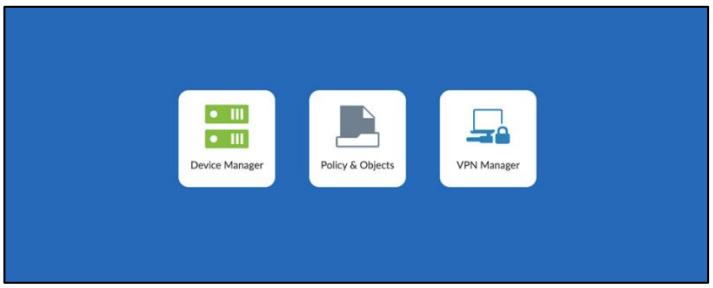
The Equinix Customer Portal (ECP) is the portal where the user management for the users who need access to the Operational console is performed. Part of the ECP is the Managed Solutions Portal (MSP) where you can raise tickets, services requests and get insights in the usage of the MPF service. On the ECP you will find the Product page where you can access the Operational Console.

2.2 Operational Console

The Operational Console is the portal where all the tasks for managing your MPF environment can be performed. The Operational Console gives you access to MPF in a certain region, MPF has four Regions, e.g. South America, North America, Europe and Asia. If you have an MPF in a specific region, the Operational Console will be accessible via one of the four buttons on the page.

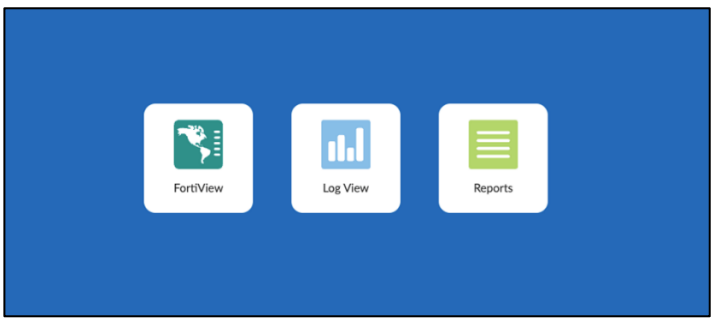
2.3 Administrator Console

The standard service uses a central self-service portal, technically defined as an Administrative Domain (ADOM). The ADOM enables the customer's Firewall administrator to create, delete and change firewall rules and policies as well as administer Virtual Private Networks specific to their Virtual Appliances.



2.4 Log Analyzer Console

The standard service uses a central log-analyzer that customers can access via an Administrative Domain (ADOM). This console enables the customer's Firewall administrator to control log management, analytics, and reporting. The Log Analyzer Console, which is separate from Network Console, ensures the Customer's administrators can automate, orchestrate, and respond to logged events.



2.5 Administrative Domain

An Administrative Domain (Adom) defines the customer within the Operational Console. The Adom can be viewed as a container that groups together all MPF resources like firewalls and policy packs and policy objects. A customer can have multiple ADOMs with different characteristics such as the geographic location of an Equinix IBX (for instance Amsterdam, London or Ashburn) or with different purposes (for instance Production and Test).
If the existing Firewall capacity is not sufficient, you can contact your Service Delivery Manager or Account Manager.

2.6 Customer Roles

In the Operational Console, two pre-defined roles exist, that can be assigned to users:

- Customer-Admin
- Customer-ReadOnly

1. Customer-Admin

Permissions:
Manager Portal

- View Device Configuration
- View Routing Table
- Create Policy Objects
- Create Policy Packs
- Create Firewall Rules
- Deploy Policy Packs to associated Firewalls
- Create VPN settings(IPsec and SSLVPN)

Analyzer Portal

- View Logs
- Create and view Reports
- Schedule Reports

2. Customer-ReadOnly

Permissions:
Manager Portal

- View Device Configuration
- View Routing Table
- View Policy Objects
- View Policy Packs
- View Firewall Rules
- View VPN settings(IPsec and SSLVPN)

Analyzer Portal

- View Logs

3. Onboarding

When you order MPF, an Equinix delivery team will guide you and your team through the fulfillment process for each location. In summary, we will:

- Evaluate your order for related products, such as Managed Private Cloud.
- Confirm your team's contact point for MPF.
- Ensure users have access to the Equinix Customer Portal, Managed Solutions Portal, and necessary permissions to manage MPF.
- Verify that all required connectivity to protect your environment is in place and functioning.
- Confirm that your contact point has administrator-equivalent credentials.

During the MPF onboarding process you receive the following information:

- Organization name
- One or more customer accounts with one of the above roles assigned
- The ordered Firewalls that are provisioned, according to the design
- Information about the connectivity to Internet, Cloud Service Providers, Colocation and/or WAN providers

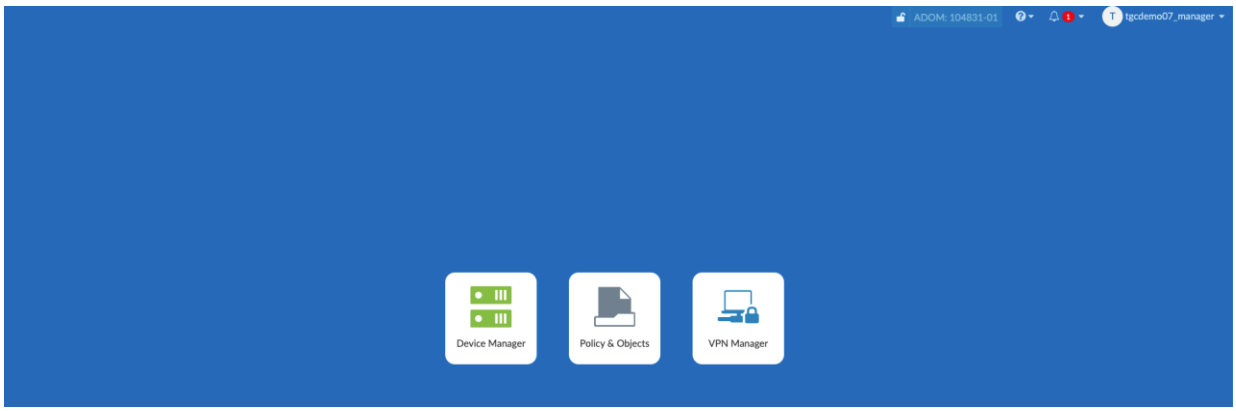
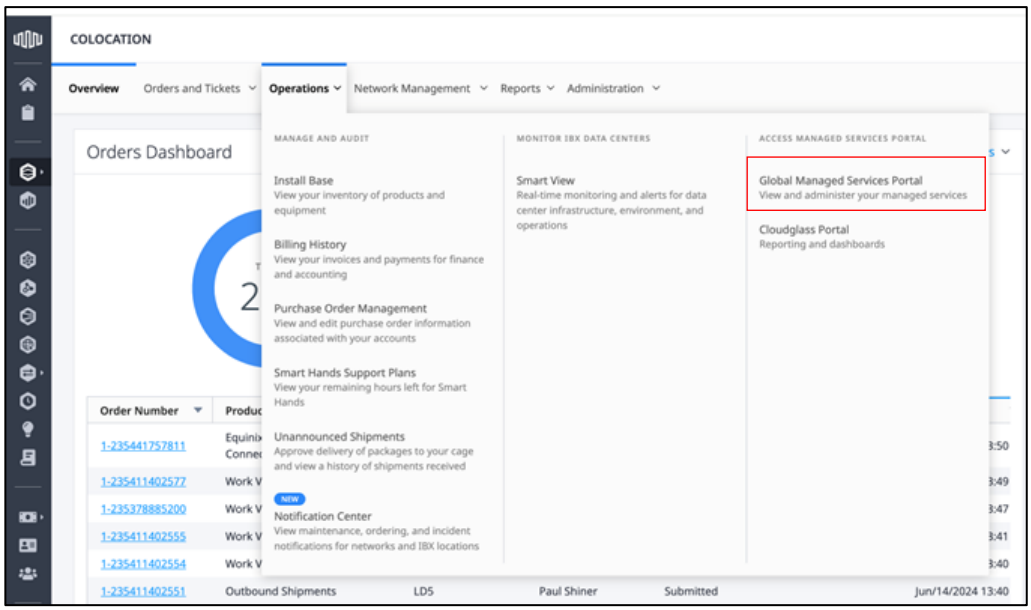


Figure 1: Example of MPF environment after onboarding

4. User Management and SSO

4.2 User Management

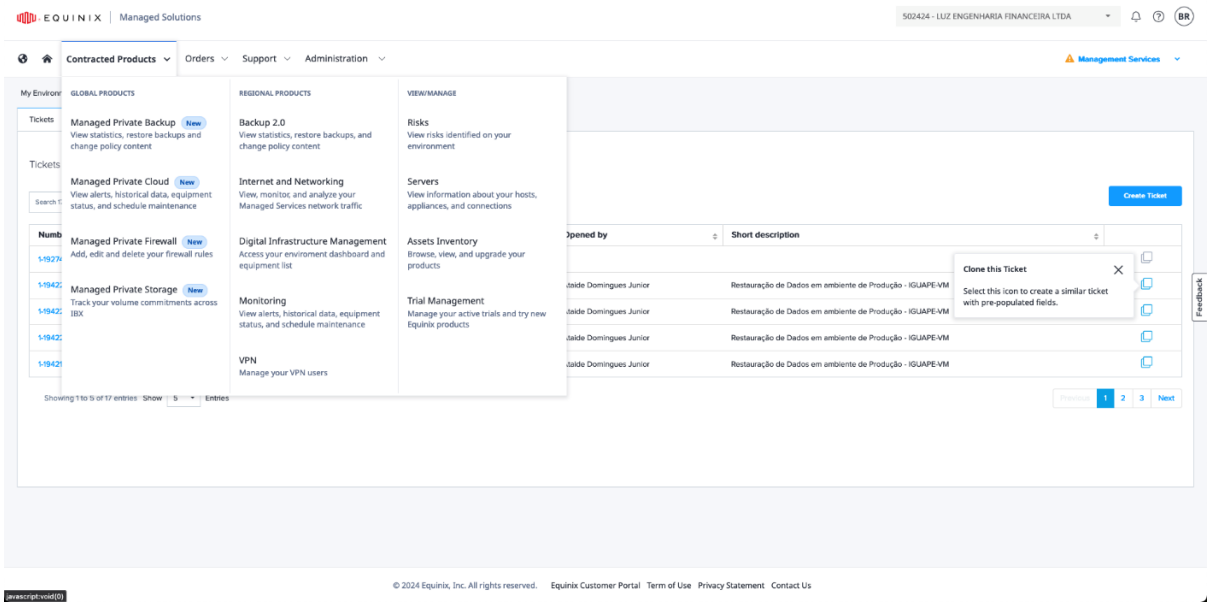
Users of the Operational Console are managed at the ECP, you can find the documentation on User Management and Password management at the following link.

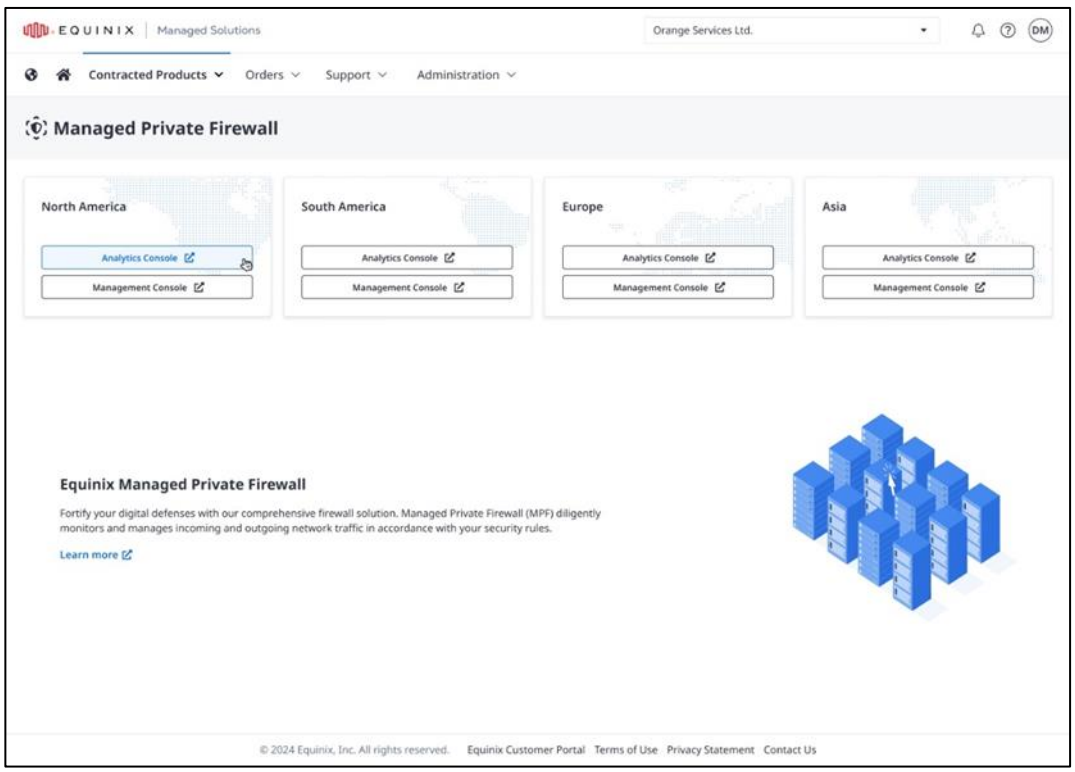


Once the users have been added to the ECP customer can raise a Service Request to assign a MPF Tenant role to the new user. Use the link to find the user guide for raising a service request in the Managed Solutions Portal.

4.3 The Operational Console

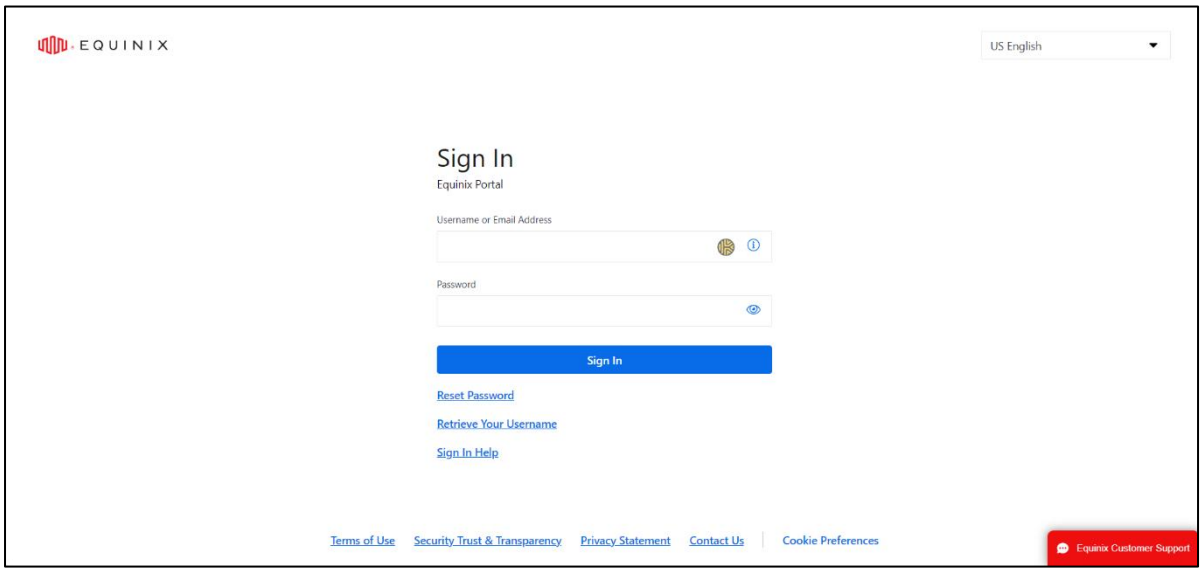
The Operations Consoles are portals where you can manage your MPF environment. Each console provides access to MPF in a specific region: South America, North America, Europe, or Asia. If you have an MPF in a specific region, the corresponding Operations Console will be accessible via one of the four buttons on the page.





4.4 Access MPF through ECP

To operate your Managed Private Firewall environment, we will provide access through the Equinix Customer Portal. You can access MPF on the product page inside the Managed Solutions Portal. Each user will need access to these portals to utilize MPF
https://customerportal.equinix.com



After logging in to the Equinix Customer Portal, you can access the Managed Solutions Portal and then the MPF product page from the menu.

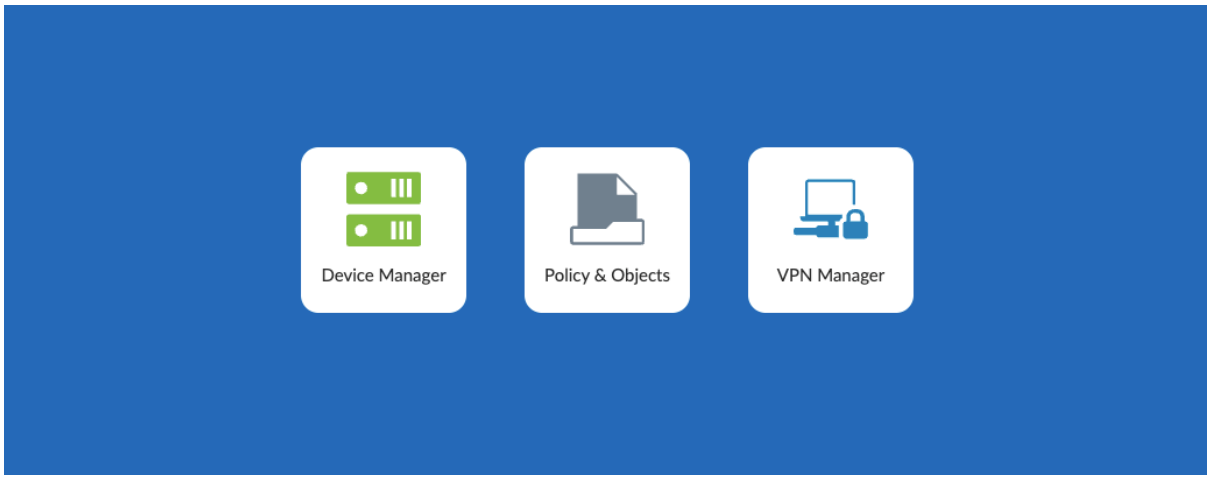
4.5 Using a Different Identity Source

In the ECP you can configure federation to your own identity provider so you can use your company credentials to login to the Operational Console, you can find the instructions about federation at docs.equinix.com

5. Use of the Administrator Console

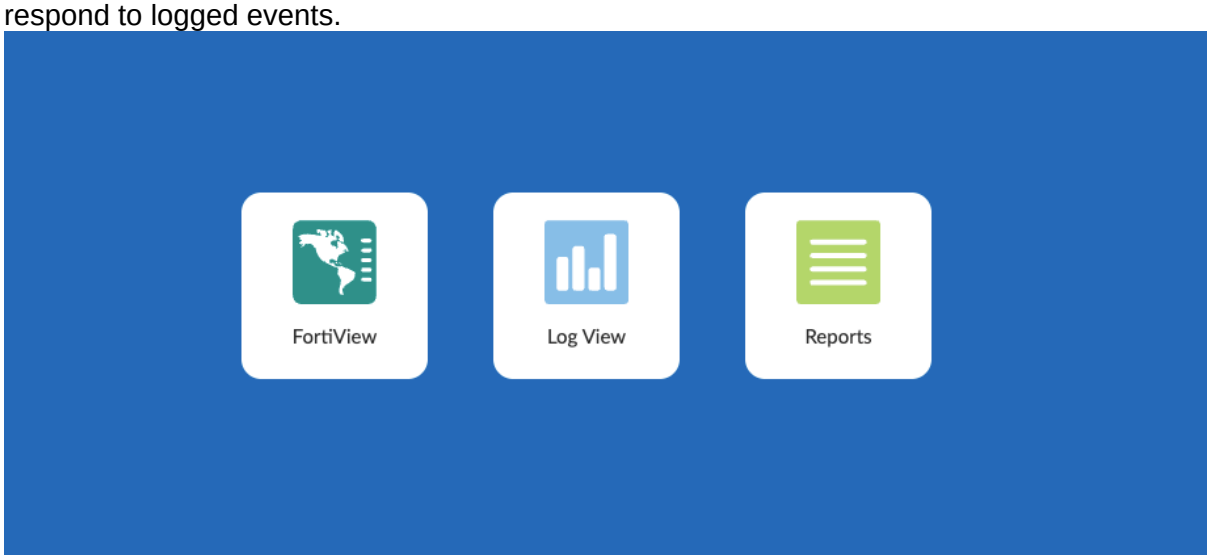
5.1 Administrator Console

The standard service uses a central self-service portal, technically defined as an Administrative Domain (ADOM). The ADOM enables the customer's Firewall administrator to create, delete and change firewall rules and policies as well as administer Virtual Private Networks specific to their Virtual Appliances



5.2 Log Analyzer Console

The standard service uses a central log-analyzer that customers access via Administrative Domain (ADOM). This console enables the customer's Firewall administrator to control log management, analytics, and reporting. The Log Analyzer Console, which is separate from Network Console, ensures the Customer's administrators can automate, orchestrate, and respond to logged events.



5.3 Steps for Policy Configuration

1. **Log in to FortiManager GUI:**

- Open a web browser and navigate to the Management console in the Managed Solutions Portal or directly to the FortiAnalyzer URL.

- Enter your username and password to log in.

2. **Select the Appropriate ADOM:** (Only applicable for customers with more than one ADOM)
- Click on the ADOM that corresponds to the environment you want to connect to.
- If you want to change to a different ADOM, from the top-right corner, click on the ADOM drop-down menu.
- Select the ADOM that corresponds to the environment you want to connect to.

3. **Navigate to Policy & Objects:** In the left-hand menu, go to Policy & Objects > IPv4 Policy.

4. **Create a New Policy:**
- Click on Create New to add a new policy.
- Define the **Name** of the policy for easy identification.
- Set the **Source** and **Destination** interfaces (e.g., LAN to WAN).
- Specify the **Source** and **Destination** addresses. You can choose from predefined addresses or create custom ones.
- Select the **Service** (e.g., HTTP, HTTPS) that the policy will apply to.
- Choose the **Action** (Allow or Deny) for the policy.
- Configure any additional settings, such as logging and security profiles (e.g., Antivirus, Web Filter).

5. **Save the Policy:** Click OK to save the policy.

6. **Arrange Policies:** Ensure the new policy is in the correct order in the list of policies, as FortiGate processes policies from top to bottom.

7. **Install Policies:** Click on the “Install Wizard” button and follow the screens.
- In the last step you can check what will be installed via the “Install preview” button, and the difference with the “Policy Package Diff” button.
- If everything is what you want to install click the “Install” button.

5.4 Steps for VPN Configuration

Steps to Configure an IPsec VPN:

1. **Log in to FortiManager GUI:**
- Open a web browser and navigate to the Management console in the Managed Solutions Portal or directly to the FortiAnalyzer URL.
- Enter your username and password to log in.

2. **Select the Appropriate ADOM:** (Only applicable for customers with more than one ADOM)
- Click on the ADOM that corresponds to the environment you want to connect to.
- If you want to change to a different ADOM, from the top-right corner, click on the ADOM drop-down menu.
- Select the ADOM that corresponds to the environment you want to connect to.

3. **Navigate to VPN:** In the left-hand menu, go to VPN > IPsec Wizard.

4. **Create a New VPN:**
- Click on Create New to start the VPN setup wizard.
- Choose the VPN type (e.g., Site-to-Site).
- Define the **Name** of the VPN.

5. **Configure the VPN Settings:**
- Set the **Remote Gateway** (the IP address of the remote site).
- Configure the **Authentication Method** (e.g., Pre-shared Key) and enter the key.
- Set the **Local Interface** (the interface that will be used for the VPN).

6. **Configure Phase 1 and Phase 2 Settings:**
- Define the encryption and authentication algorithms for both phases.
- Set the Diffie-Hellman group and key lifetime.

7. **Define the Quick Mode Selectors**: Specify the local and remote network subnets.

8. **Save and Apply:** Click OK to save the VPN configuration and apply the settings.

9. **Install VPN configuration:** Click on the “Install Wizard” button and follow the screens.
- In the last step you can check what will be installed via the “Install preview” button, and the difference with the “Policy Package Diff” button.
- If everything is what you want to install click the “Install” button.

5.5 Steps to setup Intrusion Prevention System (IPS)

Steps to Configure IPS:

1. **Log in to FortiManager GUI:**
- Open a web browser and navigate to the Management console in the Managed Solutions Portal or directly to the FortiAnalyzer URL. I
- Enter your username and password to log in.

2. **Select the Appropriate ADOM:** (Only applicable for customers with more than one ADOM)
- Click on the ADOM that corresponds to the environment you want to connect to.
- If you want to change to a different ADOM, from the top-right corner, click on the ADOM drop-down menu.
- Select the ADOM that corresponds to the environment you want to connect to.

3. **Navigate to Security Profiles:** In the left-hand menu, go to Security Profiles > Intrusion Prevention.

4. **Create or Edit an IPS Sensor:**
- Click on Create New to add a new IPS sensor or select an existing one to edit.
- Define the Name of the IPS sensor.

5. **Add IPS Signatures:**
- Under the Signature tab, add the desired IPS signatures by selecting them from the list. You can filter and search for specific signatures based on their characteristics.
- Configure the action for each signature (e.g., Monitor, Block).

6. **Apply the IPS Sensor to a Policy:**
- Navigate to Policy & Objects > IPv4 Policy.
- Edit the policy where you want to apply the IPS sensor.
- In the Security Profiles section, enable the IPS option and select the sensor you created.

7. **Save and Apply:** Click OK to save the changes.

5.6 Steps for Log Reporting

To report logs through an Administrative Domain (ADOM) in FortiAnalyzer, administrators would follow these steps:

1. **Log in to FortiAnalyzer GUI:**
- Open a web browser and navigate to the Analytics console in the Managed Solutions Portal or directly to the FortiAnalyzer URL.
- Enter your username and password to log in.

2. **Select the Appropriate ADOM:** (Only applicable for customers with more than one ADOM)
- Click on the ADOM that corresponds to the environment you want to connect to.
- If you want to change to a different ADOM, from the top-right corner, click on the ADOM drop-down menu.
- Select the ADOM that corresponds to the environment you want to connect to.

3. **Access Log View on FortiAnalyzer:**
- In the FortiAnalyzer GUI, go to the Log View section.
- Select the log type you want to view (e.g., Traffic, Event, Security).
- Use filters to narrow down the logs based on criteria such as source IP, destination IP, and time range.

4. **Generate Reports:**
- Navigate to Reports in the FortiAnalyzer GUI.
- Select Create New to generate a new report or choose an existing report template.
- Configure the report settings, including the log type, report period, and any specific filters or criteria.
- Schedule the report generation or run it immediately.

5. **Customize Reports:**
- Edit the report template to include specific data or visualizations.
- Add or remove charts, tables, and other report elements to tailor the report to your needs.
- Save the customized template for future use.

6. **View and Download Reports:**
- Once the report is generated, view it in the Reports section.
- Download the report in your preferred format (e.g., PDF, CSV).
- Share the report with relevant stakeholders as needed.

7. **Set Up Automated Reporting:**
- To automate reporting, go to the Report settings.
- Configure the scheduling options to generate reports at regular intervals (e.g., daily, weekly, monthly).
- Set up email notifications to send the reports to specified recipients automatically.

By following these steps, customer administrators can effectively report logs through an ADOM in FortiAnalyzer, ensuring they have the necessary insights to manage and secure their network environments.

How to give someone else permission to use the Operations Console?
In you need to give permission to someone else to access the MPF Service, you will need to first, request access for this person to the Equinix Customer Portal and then open a ticket to give this person the appropriate permissions to access the MPF.

You will find an option called “Create user in Operations Console” in the service catalog.

Other documentations

Where to find Service Description?

You will find the most up to date service description on docs.equinix.com website.

Where to find EMS policy?

You will find it on our website.

Where to find official Fortinet documentation?

You will find it on https://docs.fortinet.com

How to ask for help

Please make sure to open a ticket every time you need help. This is your guarantee that the right team has received your request and will work on that under the expected SLAs.