Administration Guide

DATA SECURITY MANAGER IP POLICY RESTRICTIONS

VERSION 2.0

TABLE OF CONTENTS

1.0 INTRODUCTION

1.1 PURPOSE

Welcome to the Fortanix Data Security Manager (DSM) IP Policy Restrictions guide. The purpose of this guide is to describe the steps required to configure and provide network-based IP access control to the Fortanix DSM users.

1.2 INTENDED AUDIENCE

This administration Guide is intended to be used by technical stakeholders of DSM who will be responsible for planning, performing, or maintaining the Network-based IP restriction policies.

2.0 IP POLICY (NETWORK-BASED ACCESS CONTROLS)

In controlled-network environments (not the Internet), network-based access controls are used as a defence in-depth mechanism to allow access to only certain functionality from certain origins. Fortanix DSM allows you to control the following:

- **Principal Types**: Fortanix DSM allows specific security principals from a particular origin. It supports the following two types of authenticated principals:
  - User
  - App
- **API Classes**: Fortanix DSM divides all APIs into disjoint API classes. The API classes do not intersect.

  The following API classes are supported:
  - EKMS
  - KMIP
  - HEALTH
  - UNAUTHUSER
  - OTHER

An origin is defined as a non-empty set of IP subnets.

In order for an API to be ultimately allowed, the request is matched to the most specific policy item that applies to it. The request is allowed if and only if the policy item specifies that both the request's principal and the request's API class are allowed.

The whole policy is a list of policy items. One policy item must contain exactly the default origin 0.0.0.0/0. Except for the policy item with the default origin, each policy item's origin is a strict subset of another policy item in the policy.

3.0 IP POLICY VALIDITY REQUIREMENTS

The requirements on policy items and their origins work to ensure that a policy's items can be arranged in a tree like structure with the following properties:

- A node contains the policy item. This policy applies to all origins in the node's origin that are not members of a child node's origin.
- Every node with a parent must have their origin be a subset of their parent node's origin.
- Nodes with a common parent must define disjoint origins.
- The root node is the policy item containing exactly the default origin 0.0.0.0/0.

3.1 IP POLICY EXAMPLE

Restricting Apps to a subnet:

```
"policy_items": [
  {
    "origins": [ "0.0.0.0/0" ],
    "principals": { "users": true, "apps": false },
    "api_classes": { "other": true, "kmip": true, "ekms": true, "health": true,
"unauth_user": true }
  },
  {
    "origins": [ "10.1.0.0/16", "10.3.0.0/16" ],
    "principals": { "users": false, "apps": true },
    "api_classes": { "other": true, "kmip": true, "ekms": true, "health": true,
"unauth_user": false }
  }
]
```

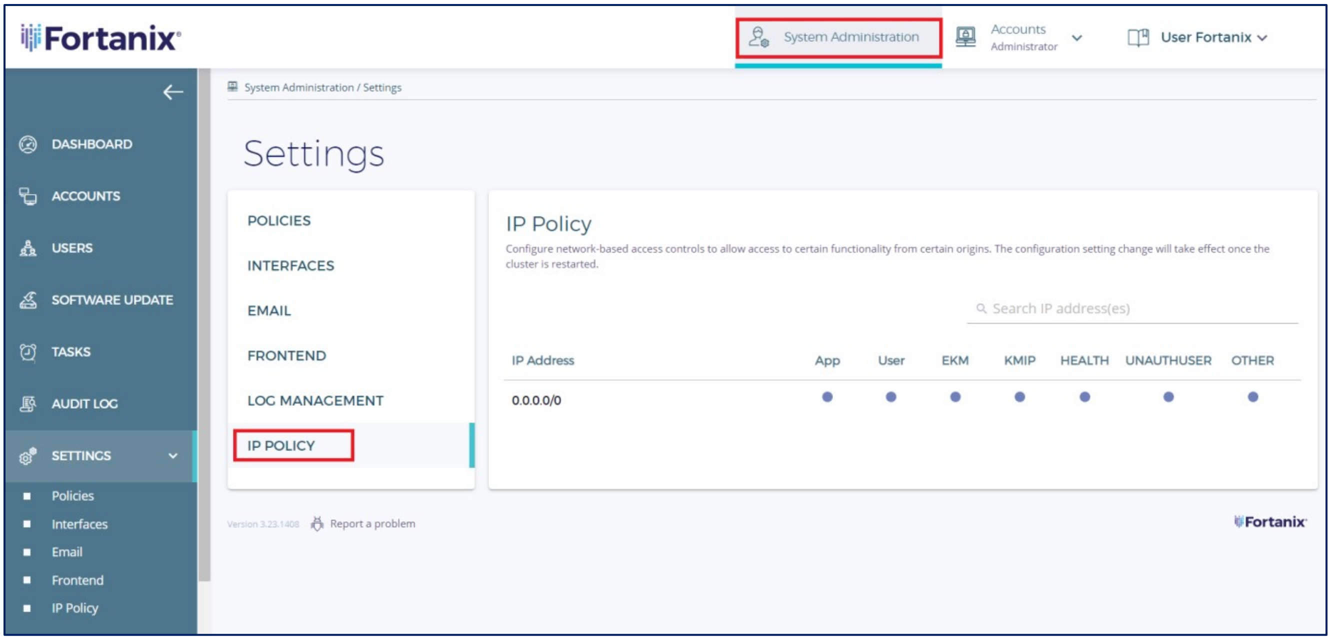
With this configuration, users will not be able use to the cluster from the subnets 10.1.0.0/16 and 10.3.0.0/16. They will still be able to see the index page, but they will not be able to authenticate or even see their authentication options.

4.0 CREATE/DELETE/EDIT AN IP POLICY

A Fortanix DSM account administrator can restrict which types of IP addresses are allowed for all the IP policies in the account.

Perform the following steps to create an account level IP policy:

1. Click the **System Administration** tab of the Fortanix DSM UI and click the **Settings** tab. In the **Account Settings** page, click the **IP POLICY** tab. The root node policy item containing the default origin (0.0.0.0/0) appears. Here, default policy effectively means that there is no filtering based on IP.



IP Policy

Configure network-based access controls to allow access to certain functionality from certain origins. The configuration setting change will take effect once the cluster is restarted.

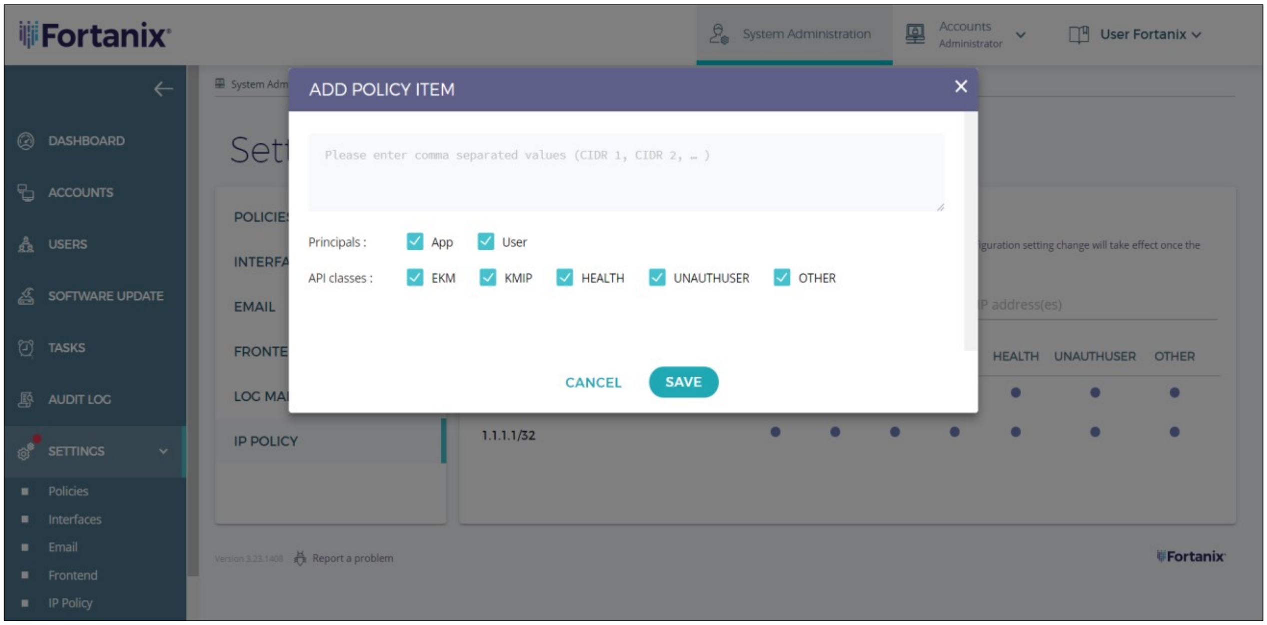
IP Address	App	User	EKM	KMIP	HEALTH	UNAUTHUSER	OTHER
0.0.0.0/0	●	●	●	●	●	●	●

FIGURE 1: DEFAULT IP POLICY

4.1 ADD A NEW POLICY

To add a new policy item, perform the following:

1. Click the **+** icon to add another IP policy.



ADD POLICY ITEM

Please enter comma separated values (CIDR 1, CIDR 2, …)

Principals : ☑ App ☑ User

API classes : ☑ EKM ☑ KMIP ☑ HEALTH ☑ UNAUTHUSER ☑ OTHER

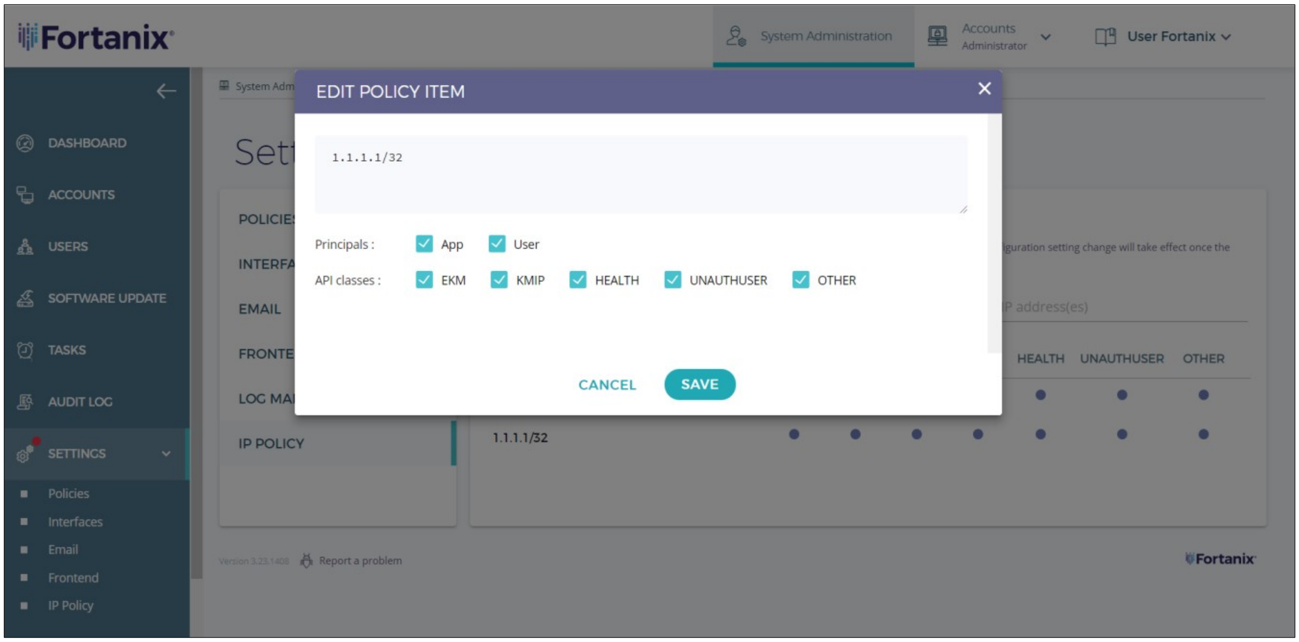
FIGURE 2: ADD A NEW IP POLICY

2. In the **ADD POLICY ITEM** page, you can restrict some functionalities originating from the configured CIDRs. Type the CIDRs that you want to restrict, separated by commas. Then, select the Principals and API classes that you want to allow.
3. Click **SAVE** to save the policy settings.

4.2 EDIT AN EXISTING POLICY

To edit a policy item, perform the following:

1. Hover on the policy item and, click the **Edit** icon.



EDIT POLICY ITEM

```
1.1.1.1/32
```

Principals : ☑ App ☑ User

API classes : ☑ EKM ☑ KMIP ☑ HEALTH ☑ UNAUTHUSER ☑ OTHER

CANCEL SAVE

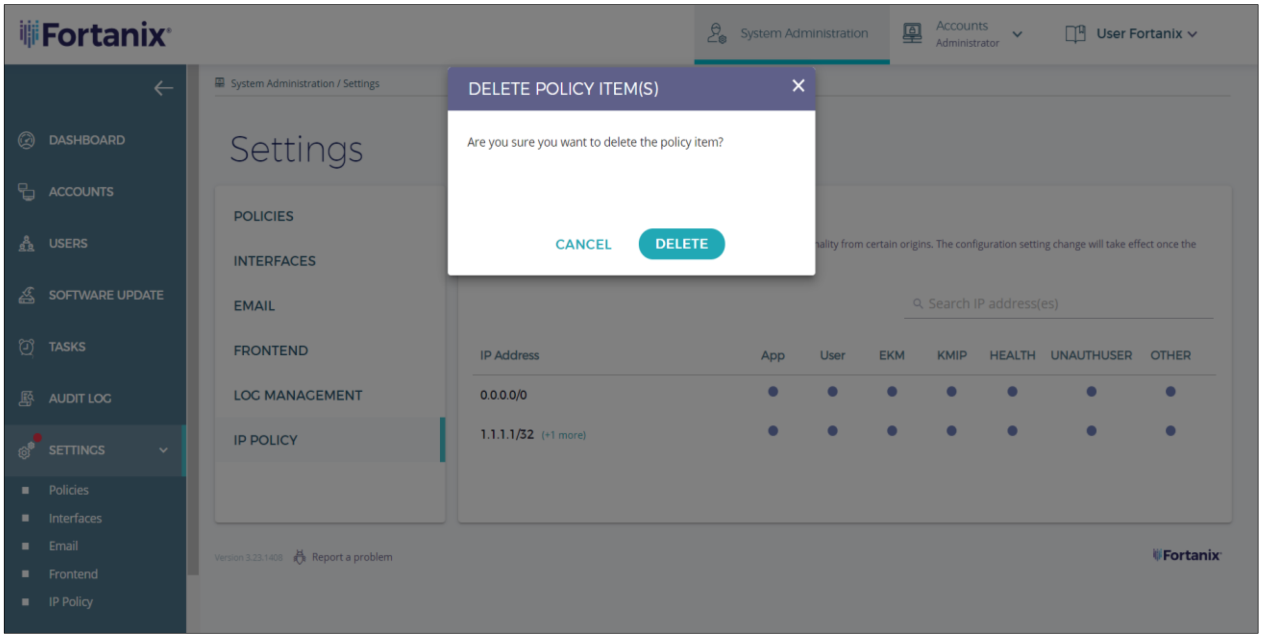
FIGURE 3: EDIT AN IP POLICY

2. In the **EDIT POLICY ITEM** dialog, modify the desired principals and API classes. You can also edit the CIDRs here.
3. Click **SAVE** to save the policy settings.

4.3 DELETE AN EXISTING POLICY

To delete a policy item, perform the following:

1. Hove on the policy item, and click the **DELETE** icon.



DELETE POLICY ITEM(S)

Are you sure you want to delete the policy item?

CANCEL DELETE

…ality from certain origins. The configuration setting change will take effect once the

IP Address	App	User	EKM	KMIP	HEALTH	UNAUTHUSER	OTHER
0.0.0.0/0	●	●	●	●	●	●	●
1.1.1.1/32 (+1 more)	●	●	●	●	●	●	●

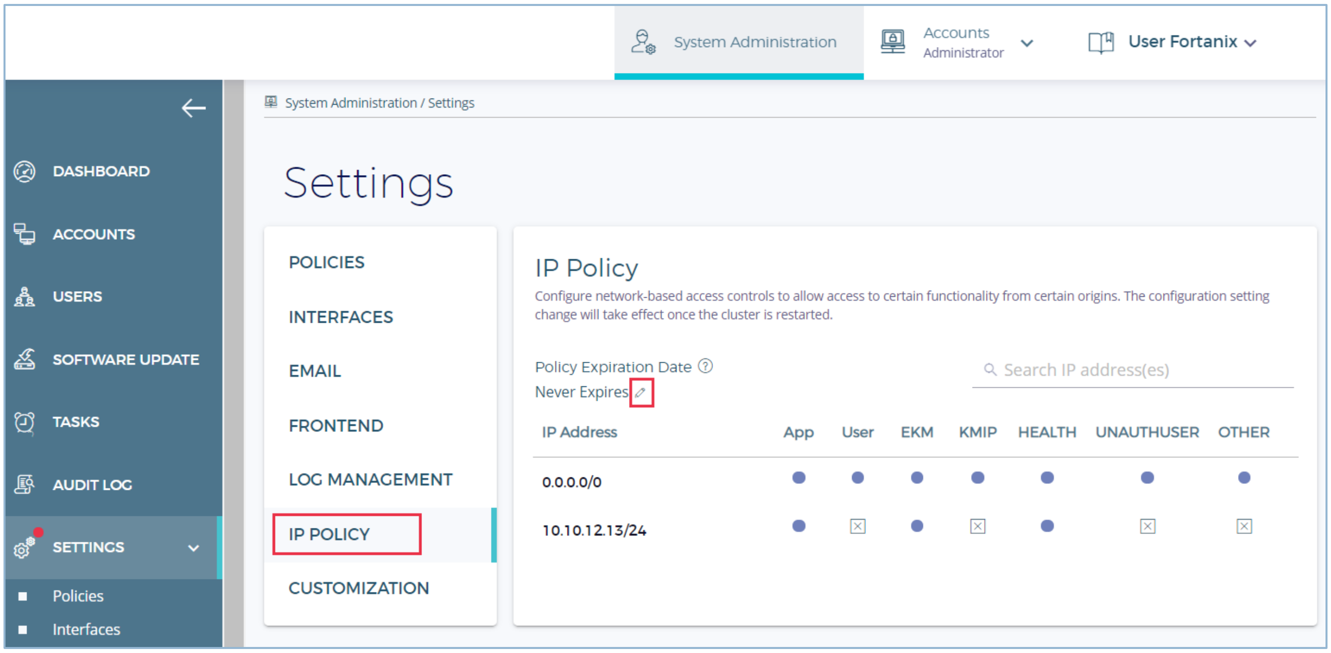
FIGURE 4: DELETE AN IP POLICY

2. In the **DELETE POLICY ITEM(S)** confirmation dialog, click **DELETE** to delete the policy setting(s).

4.4 ADD POLICY EXPIRY DATE

Sometime if you configure the cluster improperly, it results in a situation where the cluster becomes unusable. Cluster can also become inaccessible if the user does not configure the access properly from the cluster's pod subnet. To correct this, add an optional expiry date when creating a new policy in order to reset the policy and activate the default policy with no IP address restrictions. To add an optional expiry date:

1. Click the Edit icon ✎ in the IP Policy page.



Settings

IP Policy

Configure network-based access controls to allow access to certain functionality from certain origins. The configuration setting change will take effect once the cluster is restarted.

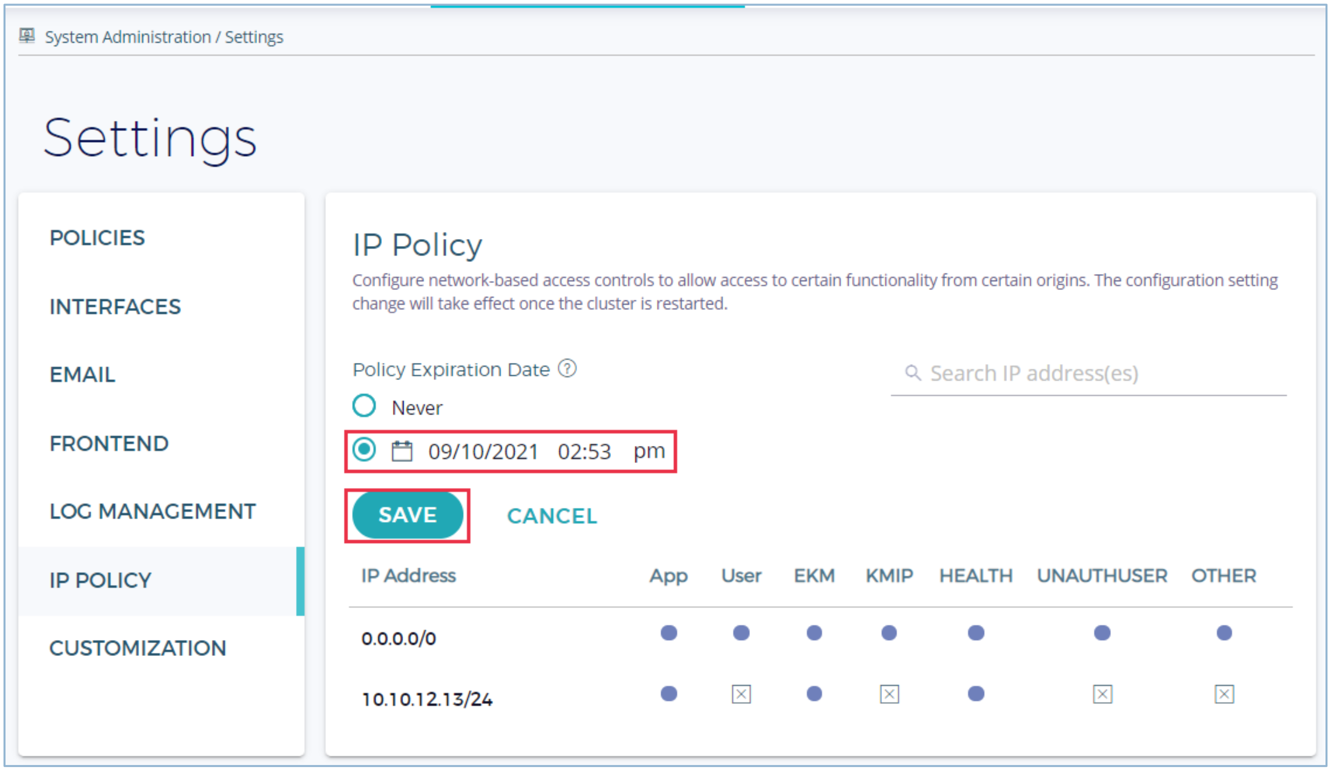
Policy Expiration Date

Never Expires

IP Address	App	User	EKM	KMIP	HEALTH	UNAUTHUSER	OTHER
0.0.0.0/0	●	●	●	●	●	●	●
10.10.12.13/24	●	☒	●	☒	●	☒	☒

Figure 5: Add policy expiry date

2. Set the expiry date for the policy.
3. Click **SAVE** to save the expiry date.



Settings

IP Policy

Configure network-based access controls to allow access to certain functionality from certain origins. The configuration setting change will take effect once the cluster is restarted.

Policy Expiration Date

○ Never

● 09/10/2021 02:53 pm

IP Address	App	User	EKM	KMIP	HEALTH	UNAUTHUSER	OTHER
0.0.0.0/0	●	●	●	●	●	●	●
10.10.12.13/24	●	☒	●	☒	●	☒	☒

Figure 6: Set expiry date

4. After the policy expires, the user can do one of the following:
    a. Edit the default policy and create a new configuration, or
    b. Restore the previous configuration and set a new expiry date

5.0 DOCUMENT INFORMATION

5.1 DOCUMENT LOCATION

The latest published version of this document is located at the URL:

https://support.fortanix.com/hc/en-us/articles/360055606411-Fortanix-Self-Defending-KMS-Sysadmin-Settings-IP-Policy

5.2 DOCUMENT UPDATES

This document will typically be updated on a periodic review and update cycle.

For any urgent document updates, please send an email to: support@fortanix.com

NOTICE: This document was produced by Fortanix, Inc. (Fortanix) and contains information which is proprietary and confidential to Fortanix. The document contains information that may be protected by patents, copyrights, and/or other IP laws. If you are not the intended recipient of this material, please destroy this document and inform info@fortanix.com immediately.