FortiNAC

Group Design and Configuration for Enforcement

Version: 9.x

Date: April 7, 2023

Rev: A

FORTINET DOCUMENT LIBRARY
http://docs.fortinet.com

FORTINET VIDEO GUIDE
http://video.fortinet.com

FORTINET KNOWLEDGE BASE
https://community.fortinet.com/t5/Knowledge-Base/ct-p/knowledgebase

FORTINET BLOG
http://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
http://support.fortinet.com

FORTINET COOKBOOK
http://cookbook.fortinet.com

NSE INSTITUTE
http://training.fortinet.com

FORTIGUARD CENTER
http://fortiguard.com

FORTICAST
http://forticast.fortinet.com

END USER LICENSE AGREEMENT
http://www.fortinet.com/doc/legal/EULA.pdf

Contents

Overview

This document provides the steps necessary to design and configure groups that will be used for enabling enforcement. These are necessary for implementing network control for the wired network infrastructure (switches). It is intended to be used in conjunction with the Deployment Guide in the Fortinet Document Library.

Tip: For hyperlinks referencing other documentation, right-click the link and select **Open in New Tab**.

What it Does

Enforcement groups are used to specify which ports and switches FortiNAC should dynamically provision network access. Each enforcement group controls a different function. The enforcement groups used are dependent upon the network access requirements.

User must be authenticated to access the network (Forced Authentication)

When a device connects and the associated user is not authenticated, the port is switched to an "isolation" VLAN. The device is released from isolation once the user has authenticated.

Must be a known device to access the network (Forced Registration)

When an unknown (rogue) device connects, the port is switched to an "isolation" VLAN. The device is released from isolation once it is registered.

Must be a known, trusted device to access the network (Forced Remediation)

When an untrusted device (due to failing a scan, etc) connects, the port is switched to an "isolation" VLAN. The device is released from isolation once it has remediated and meets compliance.

Devices marked as "Disabled" are not granted network access (Physical Address Filtering)

When a disabled device connects, the port is switched to an "isolation" VLAN. The device is released from isolation once it has been re-enabled. For more information, see Enable or disable hosts in the Administration Guide.

Provision network access based on security policies (Role-Based Access)

When a known device connects, VLAN is switched based upon matching one of the following:

- Network Access Policy (applies to registered hosts)
- Network Device Role (applies to Devices in Network Inventory)

For more information, see Network access and Network device roles in the Administration Guide.

Requirements

Prior to enforcement, ensure the following have been completed. For details, refer to the Deployment Guide:

- Network Visibility
- Endpoint Visibility

Procedure Overview

1. **Plan Enforcement Groups**: Determine which enforcement groups to use and how they will be organized based upon use case requirements.
2. **Configure Enforcement Groups**: Configure and arrange groups.

Step 1: Plan Enforcement Groups

Determine the Required Enforcement Groups

Review the table below to decide which groups will be required. For additional details see System groups in the Administration guide.

System Enforcement Groups

System Group	Definition
Forced Authentication (Port Group)	The “isolation” VLAN value is determined by the value set for the **Authentication** host state in **Model Configuration**.
Forced Registration (Port Group)	The “isolation” VLAN value is determined by the value set for the **Registration** host state in **Model Configuration**.
Forced Remediation (Port Group)	The “isolation” VLAN value is determined by the value set for the **Quarantine** host state in **Model Configuration**.
Physical Address Filtering (Device Group)	The “isolation” VLAN value is determined by the value set for the **Dead End** host state in **Model Configuration**.
Role-Based Access (Port Group)	Port is switched to a VLAN based upon matching either a Network Access Policy or Network Device Role. Ports must be members of this group in order to use Network Access Policies to dynamically provision network access.

Example Requirements

Function	System Group	Configuration	Resulting Action
Prevent unauthenticated devices from accessing the network.	Forced Authentication	Switch: Authentication VLAN 80. FortiNAC: • Model Configuration Authentication = 80 • Port is a member of the Forced Authentication group.	1. Computer connects. 2. Computer is detected on the network. Associated user is not yet authenticated. 3. FortiNAC switches port to VLAN 80.
Prevent unknown devices from accessing the network.	Forced Registration	Switch: Registration VLAN 100. FortiNAC: • Model Configuration Registration = 100 • Port is a member of the Forced Registration group.	1. Unknown computer connects. 2. Computer is detected on the network and identified as a Rogue. 3. FortiNAC switches port to VLAN 100.
Prevent known, untrusted devices from accessing the network.	Forced Remediation	Switch: Quarantine VLAN 150. FortiNAC: • Model Configuration Quarantine = 150 • Port is a member of the Forced Remediation group.	1. Computer fails AntiVirus compliance scan. 2. FortiNAC marks computer “At-Risk”. 3. FortiNAC switches port to VLAN 150.
Prevent devices marked as “Disabled” from accessing the network.	Physical Address Filtering	Switch: Dead End VLAN 175. FortiNAC: • Model Configuration Dead End = 175 • Port is a member of the Physical Address Filtering group.	1. Administrator disables computer in FortiNAC UI. 2. FortiNAC switches port to VLAN 175.
Provision network access for known devices based on security policies.	Role-Based Access	Switch: Accounting Department VLAN 200. FortiNAC: • Network Access policy configured to assign 200. • Port is a member of the Role-Based access group.	1. Computer is used by an employee in the Accounting department. 2. Computer connects. 3. Computer matches the “Accounting Dept” Network Access Policy. 4. FortiNAC switches port to VLAN 200.

Organize Groups

Once it has been determined which enforcement groups will be required, decide how groups will be organized. Members can be added directly to the enforcement groups or new groups can be nested within the enforcement group(s). Group nesting is advantageous because enforcement can be removed quickly (if necessary) by simply removing the nested group from the enforcement group. Three examples of group nesting are described.

Group organization can be done in several ways and is up to the customer to determine what works best for them. It is recommended to remain consistent with whichever method is decided upon for group organization.

In the following examples, groups will be organized based on 3 locations:

- Corporate office with 3 floors (1 department per floor)
- Two small branch offices

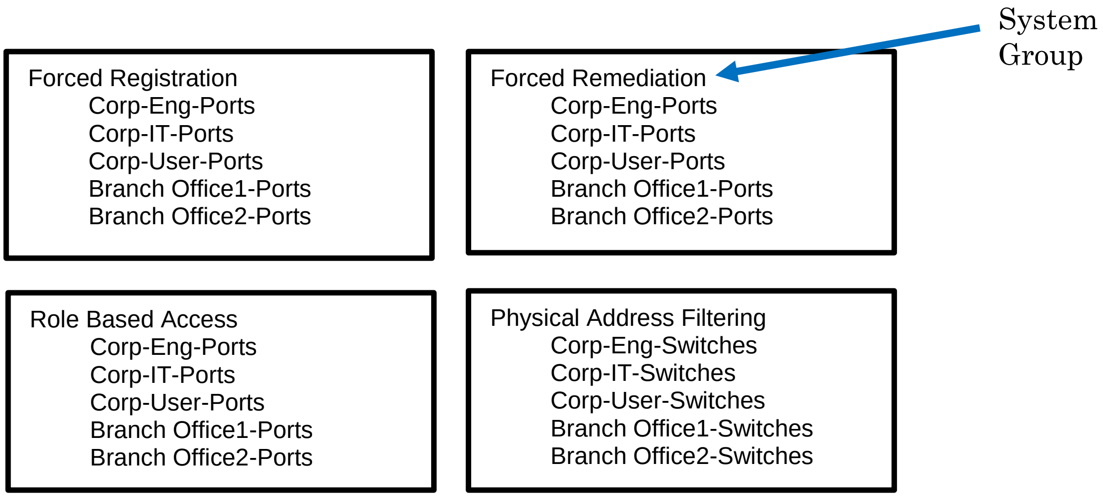
Example 1: Individual port groups

Create location or switch specific port groups and add them directly to the system enforcement groups.

- **Add/Remove enforcement per port:** Add/remove switch port from the switch port group
- **Add/Remove enforcement per switch or location:** Add/remove switch port group from the system enforcement groups
- **Add/Remove enforcement for all locations:** Add/remove all switch port groups from the system enforcement groups

Groups to Create

Corporate Office	Branch Offices
Port Groups • Corp-Eng-Ports • Corp-IT-Ports • Corp-User-Ports Device Groups • Corp-Eng-Switches • Corp-IT-Switches • Corp-User-Switches	Port Groups • Branch Office1-Ports • Branch Office2-Ports Device Groups • Branch Office1-Switches • Branch Office2-Switches



System Group

Forced Registration
Corp-Eng-Ports
Corp-IT-Ports
Corp-User-Ports
Branch Office1-Ports
Branch Office2-Ports

Forced Remediation
Corp-Eng-Ports
Corp-IT-Ports
Corp-User-Ports
Branch Office1-Ports
Branch Office2-Ports

Role Based Access
Corp-Eng-Ports
Corp-IT-Ports
Corp-User-Ports
Branch Office1-Ports
Branch Office2-Ports

Physical Address Filtering
Corp-Eng-Switches
Corp-IT-Switches
Corp-User-Switches
Branch Office1-Switches
Branch Office2-Switches

Example 2: Hierarchical port groups

Port Groups: Create a top level enforcement port group ("Enforcement") and add it to the appropriate system enforcement groups (e.g. Forced Registration, Forced Remediation and Role-Based Access). Adding the port groups to this top level group automatically enables enforcement on those ports within the groups.

For larger sites with several buildings with several floors, create a port group to represent each building and add the switch or location port groups to it. This is illustrated in the multi-level example on p.11.

- **Add/Remove enforcement per port:** Add/remove switch port from the switch port group
- **Add/Remove enforcement per switch or location:** Add/remove switch port group from the system enforcement groups
- **Add/Remove enforcement for all locations:** Add/remove all switch port groups from the system enforcement groups

Device Group (Dead End enforcement): Create a top level enforcement device group ("Enforce Dead End") and add it to the Physical Address Filtering group. Adding switch or location based device groups to the top level enforcement group automatically enables enforcement on those devices within the groups.

For larger sites with several buildings with several floors, create a device group to represent each building and add the switch or location device groups to it. This is illustrated in the multi-level example on p.11.

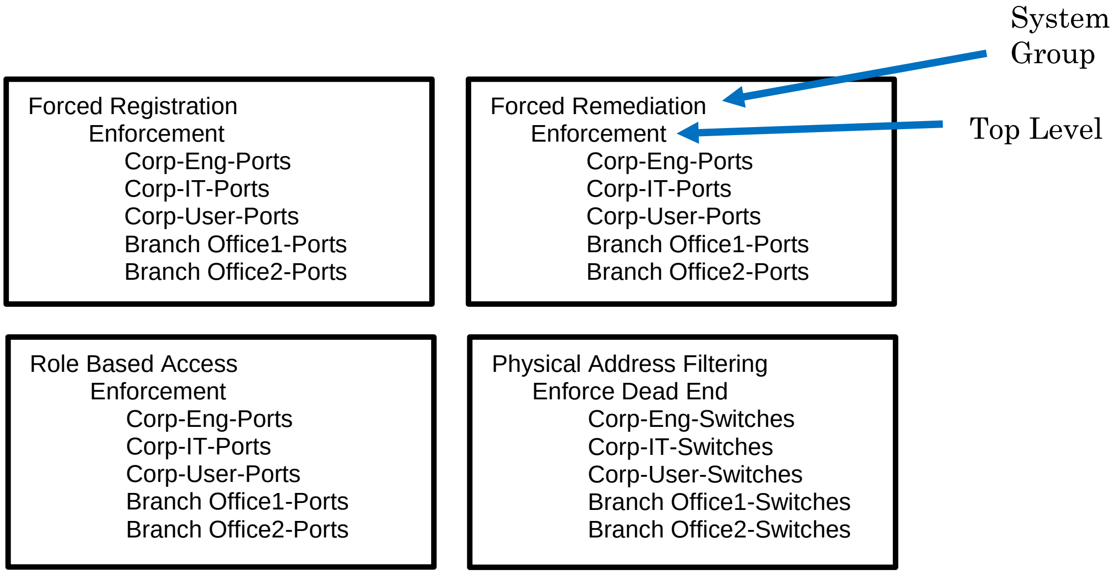
- **Add/Remove enforcement per device/switch:** Add/remove switch from the device group
- **Add/Remove enforcement per location:** Add/remove device group from the top level enforcement port group
- **Add/Remove enforcement for all locations:** Add/remove top level enforcement device group from the system enforcement groups

Simple Hierarchical

Departments nested under top level enforcement groups

Groups to Create

Top Level Enforcement	Corporate Office	Branch Offices
Port Groups • Enforcement Device Groups • Enforce Dead End	Port Groups • Corp-Eng-Ports • Corp-IT-Ports • Corp-User-Ports Device Groups • Corp-Eng-Switches • Corp-IT-Switches • Corp-User-Switches	Port Groups • Branch Office1-Ports • Branch Office2-Ports Device Groups • Branch Office1-Switches • Branch Office2-Switches



Forced Registration
- Enforcement
  - Corp-Eng-Ports
  - Corp-IT-Ports
  - Corp-User-Ports
  - Branch Office1-Ports
  - Branch Office2-Ports

Forced Remediation
- Enforcement
  - Corp-Eng-Ports
  - Corp-IT-Ports
  - Corp-User-Ports
  - Branch Office1-Ports
  - Branch Office2-Ports

Role Based Access
- Enforcement
  - Corp-Eng-Ports
  - Corp-IT-Ports
  - Corp-User-Ports
  - Branch Office1-Ports
  - Branch Office2-Ports

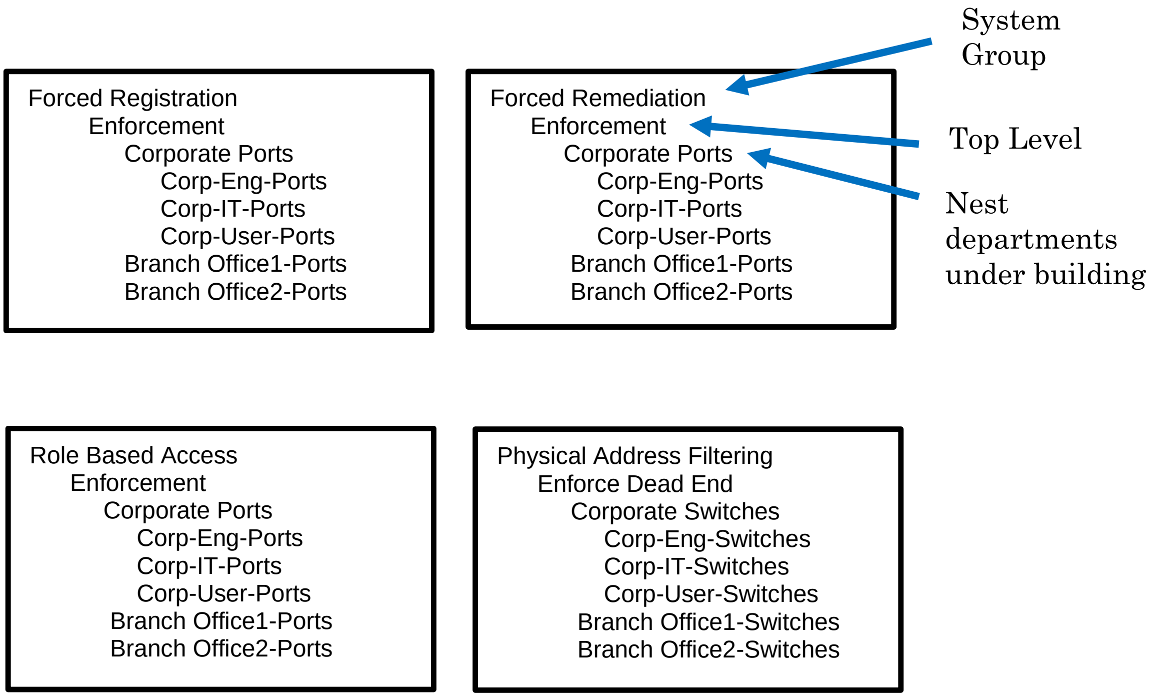
Physical Address Filtering
- Enforce Dead End
  - Corp-Eng-Switches
  - Corp-IT-Switches
  - Corp-User-Switches
  - Branch Office1-Switches
  - Branch Office2-Switches

Multi-Level Hierarchical

In this example, Corporate has a group to represent the building. The departments at Corporate are nested underneath.

Groups to Create

Top Level Enforcement	Corporate Office	Branch Offices
Port Groups • Enforcement Device Groups • Enforce Dead End	Port Groups • Corporate Ports • Corp-Eng-Ports • Corp-IT-Ports • Corp-User-Ports Device Groups • Corporate Switches • Corp-Eng-Switches • Corp-IT-Switches • Corp-User-Switches	Port Groups • Branch Office1-Ports • Branch Office2-Ports Device Groups • Branch Office1-Switches • Branch Office2-Switches



Forced Registration
Enforcement
Corporate Ports
Corp-Eng-Ports
Corp-IT-Ports
Corp-User-Ports
Branch Office1-Ports
Branch Office2-Ports

Forced Remediation
Enforcement
Corporate Ports
Corp-Eng-Ports
Corp-IT-Ports
Corp-User-Ports
Branch Office1-Ports
Branch Office2-Ports

System Group

Top Level

Nest departments under building

Role Based Access
Enforcement
Corporate Ports
Corp-Eng-Ports
Corp-IT-Ports
Corp-User-Ports
Branch Office1-Ports
Branch Office2-Ports

Physical Address Filtering
Enforce Dead End
Corporate Switches
Corp-Eng-Switches
Corp-IT-Switches
Corp-User-Switches
Branch Office1-Switches
Branch Office2-Switches

Step 2: Configure Enforcement Groups

Create and organize groups as designed in the previous step.

Important: Since enabling enforcement can disrupt network communication, do not add switches or ports to groups at this time.

Click on the appropriate link to proceed:
Individual Port Groups
Simple Hierarchical Port Groups
Multi-Level Hierarchical Port Groups

Individual Port Groups

For details on how to create and configure groups, see Add groups in Administration Guide.

1. Create port groups per switch or location and click **OK**. Do not add ports at this time.
2. Add the port groups to the desired system enforcement port groups. Using the above example requirements, this would be Forced Registration, Forced Remediation and Role-Based Access.
3. If enabling Dead-End VLAN switching, create device groups per switch or location. Do not add switches at this time.
4. Add the device groups to the Physical Address Filtering group.

The result should look like the following:

Forced Registration
- Corp-Eng-Ports
- Corp-IT-Ports
- Corp-User-Ports
- Branch Office1-Ports
- Branch Office2-Ports

Forced Remediation
- Corp-Eng-Ports
- Corp-IT-Ports
- Corp-User-Ports
- Branch Office1-Ports
- Branch Office2-Ports

Role Based Access
- Corp-Eng-Ports
- Corp-IT-Ports
- Corp-User-Ports
- Branch Office1-Ports
- Branch Office2-Ports

Physical Address Filtering
- Corp-Eng-Switches
- Corp-IT-Switches
- Corp-User-Switches
- Branch Office1-Switches
- Branch Office2-Switches

Enforcement Group configuration is complete.

Simple Hierarchical Port Groups

For details on how to create and configure groups, see Add groups in Administration Guide.

1. Create port group named “Enforcement” and click **OK**.
2. Add “Enforcement” to the desired system enforcement port groups. Using the above example requirements, this would be Forced Registration, Forced Remediation and Role-Based Access.
3. Create port groups. Do not add ports at this time.
4. Add the port groups to “Enforcement”.
5. If enabling Dead-End VLAN switching, create device group “Enforce Dead End” and click **OK**.
6. Add “Enforce Dead End” to the Physical Address Filtering Group.
7. Create device groups. Do not add switches at this time.
8. Add the device groups to “Enforce Dead End”.

The result should look like the following:

- Forced Registration
  - Enforcement
    - Corp-Eng-Ports
    - Corp-IT-Ports
    - Corp-User-Ports
    - Branch Office1-Ports
    - Branch Office2-Ports

- Forced Remediation
  - Enforcement
    - Corp-Eng-Ports
    - Corp-IT-Ports
    - Corp-User-Ports
    - Branch Office1-Ports
    - Branch Office2-Ports

- Role Based Access
  - Enforcement
    - Corp-Eng-Ports
    - Corp-IT-Ports
    - Corp-User-Ports
    - Branch Office1-Ports
    - Branch Office2-Ports

- Physical Address Filtering
  - Enforce Dead End
    - Corp-Eng-Switches
    - Corp-IT-Switches
    - Corp-User-Switches
    - Branch Office1-Switches
    - Branch Office2-Switches

Enforcement Group configuration is complete.

Multi-Level Hierarchical Port Groups

For details on how to create and configure groups, see Add groups in Administration Guide.

1. Create port group named “Enforcement” and click **OK**.
2. Add “Enforcement” to the desired system enforcement port groups. Using the above example requirements, this would be Forced Registration, Forced Remediation and Role-Based Access.
3. Create port groups per building.
4. Create port groups per switch or location. Do not add ports at this time.
5. Add port groups to the appropriate building’s group.
6. Do this for each building’s group.
7. Add the group for each building to “Enforcement”.
8. If enabling Dead-End VLAN switching, create device group “Enforce Dead End” and click **OK**.
9. Add “Enforce Dead End” to the Physical Address Filtering Group.
10. Create device groups per switch or location. Do not add switches at this time.
11. Add newly created device groups to “Enforce Dead End”.

The result should look like the following:

- Forced Registration
    - Enforcement
        - Corporate
            - Corp-Eng-Ports
            - Corp-IT-Ports
            - Corp-User-Ports
        - Branch Office
            - Branch-Accounting-Ports
            - Branch-Financial-Ports
            - Branch-HR-Ports

- Forced Remediation
    - Enforcement
        - Corporate
            - Corp-Eng-Ports
            - Corp-IT-Ports
            - Corp-User-Ports
        - Branch Office
            - Branch-Accounting-Ports
            - Branch-Financial-Ports
            - Branch-HR-Ports

- Role Based Access
    - Enforcement
        - Corporate
            - Corp-Eng-Ports
            - Corp-IT-Ports
            - Corp-User-Ports
        - Branch Office
            - Branch-Accounting-Ports
            - Branch-Financial-Ports
            - Branch-HR-Ports

- Physical Address Filtering
    - Enforce Dead End
        - Corporate Switches
            - Corp-Eng
            - Corp-IT
            - Corp-User
        - Branch Office Switches
            - Branch-Accounting
            - Branch-Financial
            - Branch-HR

Enforcement Group configuration is complete.