

### ขั้นตอนที่ 3 : เขียน Policy Auth ด้วย Local User

System

Router

Policy

Policy

DoS Policy

Proxy Options

SSL/SSH Inspection

Monitor

Firewall Objects

Security Profiles

VPN

User & Device

WAN Opt. & Cache

WiFi Controller

Log & Report

Edit Policy

Policy Type: Firewall VPN

Policy Subtype: Address User Identity Device Identity

Incoming Interface: port10 (LAN)

Source Address: LAN\_Zone

Outgoing Interface: port1 (WAN)

Enable NAT

Use Destination Interface Address Fixed Port

Use Dynamic IP Pool Click to add...

Configure Authentication Rules

| User/Group     | Destination Address | Service | Schedule | Security | Traffic Shaping | Logging | Action   |
|----------------|---------------------|---------|----------|----------|-----------------|---------|----------|
| firewall_local | all                 | ALL     | always   | -        | x               | ✓       | ✓ ACCEPT |
| ANY            | all                 | ALL     | always   | -        | x               | x       | ✗ DENY   |

Skip this policy for unauthenticated user

Disclaimer

Customize Authentication Messages

Comments: Write a comment... 0/1023

OK Cancel

จากนั้น User จะติดหน้า Firewall Auth

FORTINET

Authentication Required

Please enter your username and password to continue.

Username: \_\_\_\_\_

Password: \_\_\_\_\_

Continue

## Fortinet Single Sign On ( FSSO )

การรับค่าของการ Sign On User กับ Windows AD เข้ามาและตัว FortiGate จะรับทราบ Event นั้นๆ

และสามารถปล่อย User ออกได้เลยโดยไม่ต้อง Auth กับตัว Firewall อีก 1 ครั้ง

ขั้นตอนที่ 1: สร้าง Connector กับตัว Windows AD



System

Router

Policy

Firewall Objects

Security Profiles

VPN

User & Device

User

- User Definition
- User Group
- Guest Management

Device

Authentication

- Single Sign-On
- LDAP Server
- RADIUS Server
- Settings

Two-factor Authentication

WAN Opt. & Cache

WiFi Controller

Log & Report

New Single Sign-On Server

Type

☐ Poll Active Directory Server ☒ Fortinet Single-Sign-On Agent ☐ RADIUS Single-Sign-On Agent

Name

AD\_FSSO

Primary Agent IP/Name

192.168.2.111

Password

.....

Secondary Agent IP/Name

.....

Password

.....

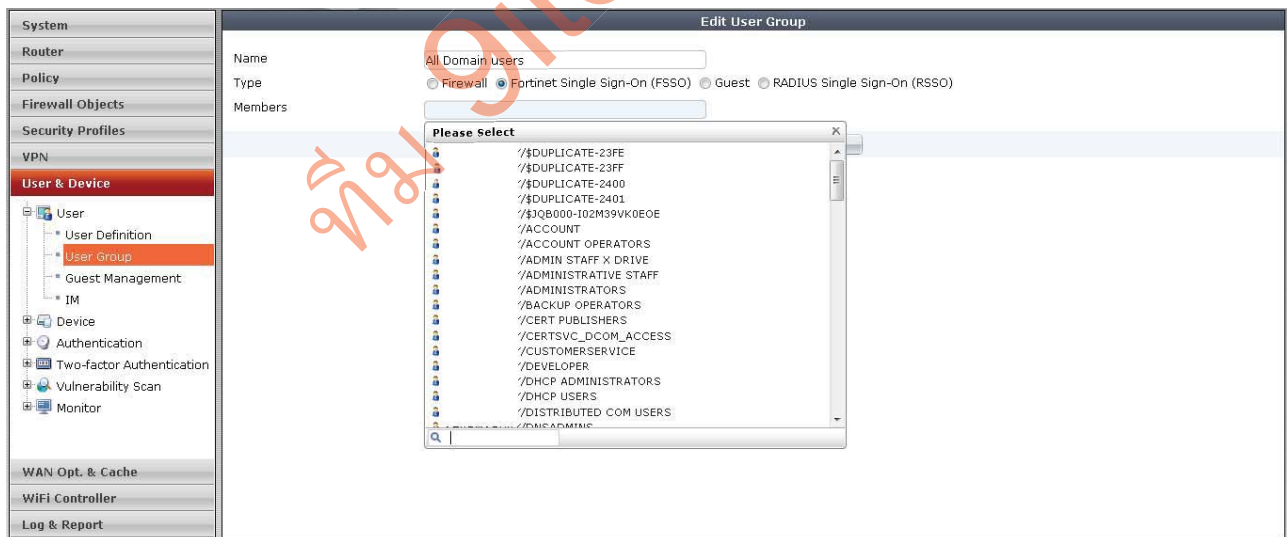
More FSSO agents

LDAP Server

Click to set...

Apply & Refresh OK Cancel

ขั้นตอนที่ 2: สร้าง User Group ที่ Link กับ FSSO



System

Router

Policy

Firewall Objects

Security Profiles

VPN

User & Device

User

- User Definition
- User Group
- Guest Management

Device

Authentication

- Single Sign-On
- LDAP Server
- RADIUS Server
- Settings

Two-factor Authentication

WAN Opt. & Cache

WiFi Controller

Log & Report

Edit User Group

Name

All Domain Users

Type

☐ Firewall ☒ Fortinet Single Sign-On (FSSO) ☐ Guest ☐ RADIUS Single Sign-On (RSSO)

Members

.....

Please Select

- /\*\$DUPLICATE-23FE
- /\*\$DUPLICATE-23FF
- /\*\$DUPLICATE-2400
- /\*\$DUPLICATE-2401
- /\*\$QB000-102M39VK0EOE
- /\*ACCOUNT
- /\*ACCOUNT OPERATORS
- /\*ADMIN STAFF X DRIVE
- /\*ADMINISTRATIVE STAFF
- /\*ADMINISTRATORS
- /\*BACKUP OPERATORS
- /\*CERT PUBLISHERS
- /\*CERTSVC\_DCOM\_ACCESS
- /\*CUSTOMERSERVICE
- /\*DEVELOPER
- /\*DHCP ADMINISTRATORS
- /\*DHCP USERS
- /\*DISTRIBUTED COM USERS

### ขั้นตอนที่ 3: สร้าง Policy Auth โดยใช้ User Group ที่รับมาจาก FSSO

System  
Router  
Policy  
Policy  
DoS Policy  
Proxy Options  
SSL/SSH Inspection  
Monitor

Firewall Objects  
Security Profiles  
VPN  
User & Device  
WAN Opt. & Cache  
WiFi Controller  
Log & Report

**Edit Policy**

Policy Type: Firewall (selected) | VPN  
Policy Subtype: Address | User Identity (selected) | Device Identity

Incoming Interface: port10 (LAN)  
Source Address: LAN\_Zone  
Outgoing Interface: port1 (WAN)

☒ Enable NAT  
☒ Use Destination Interface Address ☐ Fixed Port  
☐ Use Dynamic IP Pool [Click to add...](#)

**Configure Authentication Rules**

| User/Group      | Destination Address | Service | Schedule | Security | Traffic Shaping                     | Logging                             | Action   |
|-----------------|---------------------|---------|----------|----------|-------------------------------------|-------------------------------------|----------|
| All_Domain_User | all                 | ALL     | always   | -        | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | ✓ ACCEPT |
| ANY             | all                 | ALL     | always   | -        | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | ✗ DENY   |

☐ Skip this policy for unauthenticated user  
☐ Disclaimer  
☐ Customize Authentication Messages

Comments:  0/1023

จากนั้น User จะติดหน้า Firewall Auth

**FORTINET**

**Authentication Required**

Please enter your username and password to continue.

Username:

Password:

## LDAP User

### ขั้นตอนที่ 1 : สร้าง Connector ของ FortiGate กับ LDAP

The screenshot shows the 'New LDAP Server' configuration window in the FortiGate GUI. The left sidebar is expanded to 'User & Device' > 'Authentication' > 'LDAP Server'. The main panel contains the following fields:

- Name: LDAP
- Server Name/IP: 192.168.2.101
- Server Port: 389
- Common Name Identifier: cn
- Distinguished Name: cn=local,cn=lab
- Bind Type: ☒ Regular (Other options: Simple, Anonymous)
- User DN: ou=users,cn=local,cn=lab
- Password: (masked with dots)
- ☐ Secure Connection
- Buttons: Test, OK, Cancel

### ขั้นตอนที่ 2 : สร้าง User Group เพื่อใช้งาน User ที่ได้จาก LDAP

The screenshot shows the 'New User Group' configuration window in the FortiGate GUI. The left sidebar is expanded to 'User & Device' > 'Authentication' > 'User Group'. The main panel contains the following fields:

- Name: LDAP\_User
- Type: ☒ Firewall (Other options: Fortinet Single Sign-On (FSSO), Guest, RADIUS Single Sign-On (RSSO))
- Members: Click to set...
- Remote authentication servers: Add, Edit, Delete buttons
- Table with 2 columns: Remote Server, Group Name
- Table content: LDAP | ou=users,cn=local,cn=lab
- Buttons: OK, Cancel

### ขั้นตอนที่ 3: สร้าง Policy Auth โดยใช้ User Group ที่รับมาจาก LDAP

System  
Router  
Policy  
Policy  
DoS Policy  
Proxy Options  
SSL/SSH Inspection  
Monitor

Firewall Objects  
Security Profiles  
VPN  
User & Device  
WAN Opt. & Cache  
WiFi Controller  
Log & Report

**Edit Policy**

Policy Type: ☒ Firewall ☐ VPN  
Policy Subtype: ☐ Address ☒ User Identity ☐ Device Identity

Incoming Interface: port10 (LAN)  
Source Address: LAN\_Zone  
Outgoing Interface: port1 (WAN)

☒ Enable NAT  
☒ Use Destination Interface Address ☐ Fixed Port  
☐ Use Dynamic IP Pool [Click to add...](#)

**Configure Authentication Rules**

| User/Group | Destination Address | Service | Schedule | Security | Traffic Shaping | Logging                             | Action   |
|------------|---------------------|---------|----------|----------|-----------------|-------------------------------------|----------|
| LDAP_User  | all                 | ALL     | always   | -        | -               | <input checked="" type="checkbox"/> | ✓ ACCEPT |
| ANY        | all                 | ALL     | always   | -        | -               | <input checked="" type="checkbox"/> | ✗ DENY   |

☐ Skip this policy for unauthenticated user  
☐ Disclaimer  
☐ Customize Authentication Messages

Comments:  0/1023

จากนั้น User จะติดหน้า Firewall Auth

**FORTINET**  
Authentication Required

Please enter your username and password to continue.

Username:   
Password:

## LDAP User

### ขั้นตอนที่ 1 : สร้าง Connector ของ FortiGate กับ RADIUS

System  
Router  
Policy  
Firewall Objects  
Security Profiles  
VPN  
**User & Device**  
  User Group  
  Guest Management  
  Device  
  Device Definitions  
  Device Groups  
  Endpoint Profile  
  Authentication  
    Single Sign-On  
    LDAP Server  
    **RADIUS Server**  
    Settings  
WAN Opt. & Cache  
WiFi Controller  
Log & Report

**New RADIUS Server**

Name: RADIUS  
Primary Server Name/IP: 192.168.2.103  
Primary Server Secret: [masked] [Test]  
Secondary Server Name/IP: [ ]  
Secondary Server Secret: [ ] [Test]  
Authentication Scheme: ☒ Use Default Authentication Scheme  
                                  ☐ Specify Authentication Protocol  
                                  PAP  
NAS IP/Called Station ID: [ ]  
Include in every User Group: ☐ Enable  
[OK] [Cancel]

### ขั้นตอนที่ 2 : สร้าง User Group เพื่อใช้งาน User ที่ได้จาก RADIUS ( ต้องกำหนด Group Name )

System  
Router  
Policy  
Firewall Objects  
Security Profiles  
VPN  
**User & Device**  
  **User Group**  
  Guest Management  
  Device  
  Device Definitions  
  Device Groups  
  Endpoint Profile  
  Authentication  
    Single Sign-On  
    LDAP Server  
    RADIUS Server  
    Settings  
WAN Opt. & Cache  
WiFi Controller  
Log & Report

**New User Group**

Name: RADIUS\_User  
Type: ☒ Firewall ☐ Fortinet Single Sign-On (FSSO) ☐ Guest ☐ RADIUS Single Sign-On (RSSO)  
Members: Click to set...  
Remote authentication servers: Add Edit Delete  
Remote Server: RADIUS Group Name: Any user\_g1  
[OK] [Cancel]

### ขั้นตอนที่ 3: สร้าง Policy Auth โดยใช้ User Group ที่รับมาจาก LDAP

System  
Router  
Policy  
Policy  
DoS Policy  
Proxy Options  
SSL/SSH Inspection  
Monitor  
Firewall Objects  
Security Profiles  
VPN  
User & Device  
WAN Opt. & Cache  
WiFi Controller  
Log & Report

Edit Policy

Policy Type: Firewall  
Policy Subtype: User Identity  
Incoming Interface: port10 (LAN)  
Source Address: LAN\_Zone  
Outgoing Interface: port1 (WAN)  
Enable NAT: ☒  
Use Destination Interface Address: ☒  
Use Dynamic IP Pool: ☐  
Fixed Port: ☐  
Click to add...

Configure Authentication Rules

| User/Group  | Destination Address | Service | Schedule | Security | Traffic Shaping | Logging | Action |
|-------------|---------------------|---------|----------|----------|-----------------|---------|--------|
| RADIUS_User | all                 | ALL     | always   | -        | x               | x       | ACCEPT |
| ANY         | all                 | ALL     | always   | -        | x               | x       | DENY   |

☐ Skip this policy for unauthenticated user  
☐ Disclaimer  
☐ Customize Authentication Messages

Comments: Write a comment... 0/1023

OK Cancel

จากนั้น User จะติดหน้า Firewall Auth

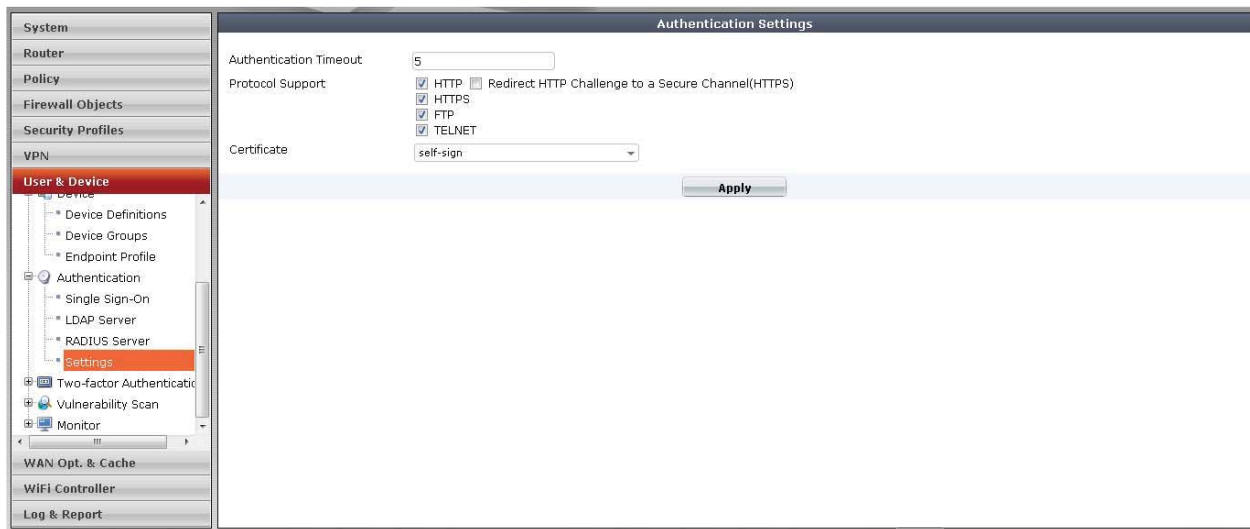
FORTINET  
Authentication Required

Please enter your username and password to continue.

Username:   
Password:

Continue

## การกำหนดค่า Auth Time-Out ของ Global



Config Auth OverDrive เพื่อกำหนดให้ User บางกลุ่มสามารถ Auth ได้มากกว่า 1 Session

```
FortiGate # config system global
```

```
FortiGate (global) # set policy-auth-concurrent 1
```

```
FortiGate (global) # end
```

```
FortiGate # config user group
```

```
FortiGate (group) # edit Manager
```

```
FortiGate (Manager) # set auth-concurrent-override enable
```

```
FortiGate (Manager) # set auth-concurrent-value 2
```

```
FortiGate (Manager) # end
```





## Device Auth

### ขั้นตอนที่ 1 : เปิด Device Detect ที่ Interface ที่ต้องการทำ Policy

**System**

- Dashboard
  - Status
  - Top Sources
  - Top Destinations
  - Top Applications
- Network
  - Interfaces**
  - DNS
  - Explicit Proxy
  - Packet Capture
- Config

**Router**

- Policy**
- Firewall Objects
- Security Profiles
- VPN
- User & Device
- WAN Opt. & Cache
- WiFi Controller
- Log & Report

**Edit Interface**

Alias: LAN  
Link Status: Up  
Type: Physical Interface

Addressing mode: ☒ Manual ☐ DHCP ☐ PPPoE ☐ Dedicate to FortiAP  
IP/Network Mask: 192.168.1.100/255.255.255.0

Administrative Access: ☒ HTTPS ☒ PING ☐ HTTP ☐ FMG-Access ☐ CAPWAP  
☐ SSH ☐ SNMP ☐ TELNET ☐ FCT-Access

DHCP Server: ☐ Enable

Security Mode: None

Device Management:  
Detect and Identify Devices: ☒  
Add New Devices to Vulnerability Scan List: ☐

Enable Explicit Web Proxy: ☐  
Listen for RADIUS Accounting Messages: ☐  
Secondary IP Address: ☐

Comments: Write a comment... 0/255  
Administrative Status: ☒ Up ☐ Down

### ขั้นตอนที่ 2 : FortiGate จะสามารถ Detect Device ได้

**System**

- Router
- Policy
- Firewall Objects
- Security Profiles
- VPN
- User & Device**
  - Device
  - Device Definitions
  - Device Groups
  - Endpoint Profile
  - Authentication
    - Single Sign-On
    - LDAP Server
    - RADIUS Server
    - Settings
  - Two-factor Authentication
  - Vulnerability Scan
  - Monitor
- WAN Opt. & Cache
- WiFi Controller
- Log & Report

**Monitor**

Create New Edit Delete Refresh Total Devices Tracked: 1

| Online                              | Device            | OS                | User | IP Address    | FortiClient State |
|-------------------------------------|-------------------|-------------------|------|---------------|-------------------|
| <input checked="" type="checkbox"/> | 3c:97:0e:79:62:48 | Windows / 7 (x64) |      | 192.168.1.111 |                   |

### ขั้นตอนที่ 3 : ตั้งชื่อ Device

System

Router

Policy

Firewall Objects

Security Profiles

VPN

User & Device

Device Definitions

Device Groups

Endpoint Profile

Authentication

Single Sign-On

LDAP Server

RADIUS Server

Settings

Two-factor Authentication

Vulnerability Scan

Monitor

WAN Opt. & Cache

WiFi Controller

Log & Report

New Device

Alias: ENGINEER-001

MAC Address: 3c:97:0e:79:62:48

Additional MACs: Click to add...

Device Type: Windows PC

Discovered Device Status

OS: Windows / 7 (x64)

IP Address: 192.168.1.111

Last Seen: 12:22:23 (port10)

Custom Groups: None

Comments: Write a comment... 0/255

OK Cancel

### ขั้นตอนที่ 4 : นำ Device มาจัด Group

System

Router

Policy

Firewall Objects

Security Profiles

VPN

User & Device

Device Definitions

Device Groups

Endpoint Profile

Authentication

Single Sign-On

LDAP Server

RADIUS Server

Settings

Two-factor Authentication

Vulnerability Scan

Monitor

WAN Opt. & Cache

WiFi Controller

Log & Report

New Device Group

Name: ENGINEER\_DEVICE

Members: ENGINEER-001

Comments: Write a comment... 0/255

OK Cancel

## ขั้นตอนที่ 5 : เขียน Policy ที่ Auth ด้วย Device หรือ ใช้ Pre-Define Device Signature ก็ได้

**System**  
Router  
**Policy**  
Policy  
DoS Policy  
Proxy Options  
SSL/SSH Inspection  
Monitor

**Firewall Objects**  
Security Profiles  
VPN  
User & Device  
WAN Opt. & Cache  
WiFi Controller  
Log & Report

**Edit Policy**

Policy Type: ☒ Firewall ☐ VPN  
Policy Subtype: ☐ Address ☐ User Identity ☒ Device Identity

Incoming Interface: port10 (LAN)  
Source Address: LAN\_Zone  
Outgoing Interface: port1 (WAN)  
☒ Enable NAT  
☒ Use Destination Interface Address ☐ Fixed Port  
☐ Use Dynamic IP Pool

**Configure Authentication Rules**

Create New Edit Delete

| Destination Address | Device          | Endpoint Compliance                 | Service | Schedule | Security | Traffic Shaping                     | Logging                             | Action   |
|---------------------|-----------------|-------------------------------------|---------|----------|----------|-------------------------------------|-------------------------------------|----------|
| all                 | ENGINEER_DEVICE | <input checked="" type="checkbox"/> | ALL     | always   | -        | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | ✓ ACCEPT |
| all                 | All             | -                                   | ALL     | always   | -        | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | ✗ DENY   |

☐ Disclaimer  
☐ Customize Authentication Messages

**Device Policy Options**

☐ Attempt to detect all Unknown device types before implicit deny  
☐ Redirect all non-compliant/unregistered FortiClient compatible devices to a captive portal  
☐ Prompt E-mail Collection Portal for all devices

Comments: Write a comment... 0/1023

**System**  
Router  
**Policy**  
Policy  
DoS Policy  
Proxy Options  
SSL/SSH Inspection  
Monitor

**Firewall Objects**  
Security Profiles  
VPN  
User & Device  
WAN Opt. & Cache  
WiFi Controller  
Log & Report

**Edit Authentication Rule**

Policy Subtype: ☒ Address ☐ User Identity ☒ Device Identity

Incoming Interface: port10 (LAN)  
Source Address: LAN\_Zone  
Outgoing Interface: port1 (WAN)  
☒ Enable NAT  
☒ Use Destination Interface Address ☐ Fixed Port  
☐ Use Dynamic IP Pool

**Configure Authentication Rules**

Create New Edit Delete

| Destination Address | Device          | Endpoint Compliance                 | Service | Schedule | Security | Traffic Shaping                     | Logging                             | Action   |
|---------------------|-----------------|-------------------------------------|---------|----------|----------|-------------------------------------|-------------------------------------|----------|
| all                 | ENGINEER_DEVICE | <input checked="" type="checkbox"/> | ALL     | always   | -        | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | ✓ ACCEPT |
| all                 | All             | -                                   | ALL     | always   | -        | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | ✗ DENY   |

☐ Disclaimer  
☐ Customize Authentication Messages

**Device Policy Options**

☐ Attempt to detect all Unknown device types before implicit deny  
☐ Redirect all non-compliant/unregistered FortiClient compatible devices to a captive portal  
☐ Prompt E-mail Collection Portal for all devices

Comments: Write a comment... 0/1023

**Please Select**

- ENGINEER-001
- ENGINEER\_DEVICE
- All
- Android Phone
- Android Tablet
- BlackBerry Phone
- BlackBerry PlayBook
- Collected Emails
- Fortinet Device
- Gaming Console
- IP Phone
- iPad
- iPhone
- Linux PC
- Media Streaming
- Other Network Device
- Router/NAT Device
- Windows PC
- Windows Phone

default default

OK Cancel

## การส่ง Log ไปเก็บที่ FortiAnalyzer

**Log Settings**

**Logging and Archiving**

- ☒ Send Logs to FortiAnalyzer/FortiManager
  - IP Address: 192.168.2.254 [Test Connectivity](#)
- Upload Option
  - ☒ Realtime
- ☒ Encrypt Log Transmission
- ☐ Send Logs to FortiCloud
  - Account:  [Test Connectivity](#)
- ☒ Event Logging
  - ☒ Enable All
  - ☒ WiFi activity event ☒ System activity event ☒ User activity event
  - ☒ Router activity event ☒ VPN activity event ☒ Explicit web proxy event

**GUI Preferences**

- Display Logs From:
- ☒ Resolve Hostnames (Using reverse DNS lookup)
- ☒ Resolve Unknown Applications (Using remote application database)

[Apply](#)

