FortiNAC

Device Profiler Configuration

Version: 8.x

Date: September 16, 2022

Rev: F

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

What it Does

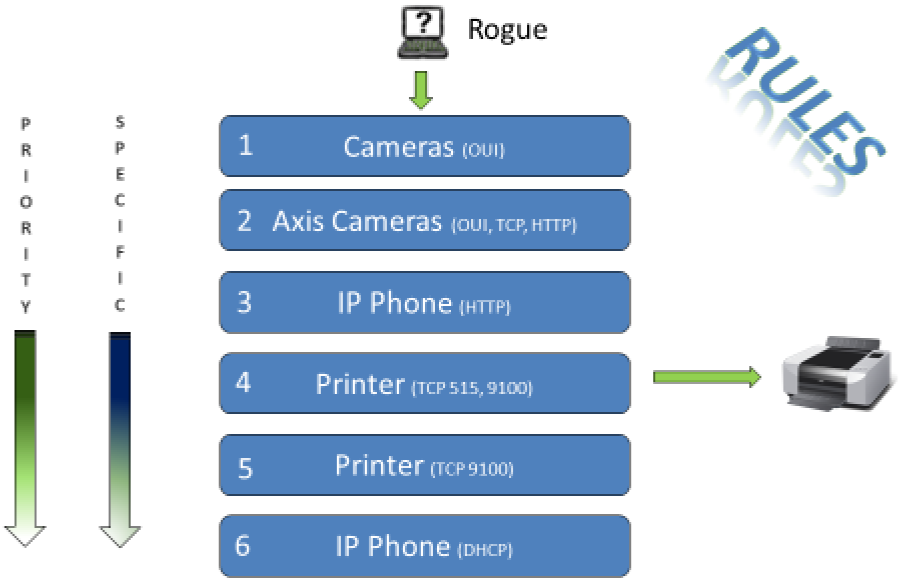
Device Profiling is a FortiNAC process to classify rogue devices and create an organized inventory of known trusted registered devices. Additionally, Device Profiling can be used to re-validate the trust of a registered device.

Device Profiler is FortiNAC's rule-based device evaluation and classification solution. It is a set of pre-defined and custom built ordered rules for evaluating and classifying rogue devices. A rule is comprised of classification settings and evaluation methods. Methods evaluate devices for a pass/fail result. A "pass" results in the assignment of the classification settings.

Profiling Overview

When a rogue device record is created, the device is evaluated against the active Device Profiling rules. FortiNAC evaluates a device against each rule until a “fail” or “pass” result is reached.

Example: A rogue device that is a printer device with printer specific open TCP ports 515 and 9100 is evaluated using the following rules:



<u>Rule Configuration</u>
Rule 1: “Cameras” - Method: Vendor OUI only
Rule 2: “Axis Cameras”- Method: Vendor OUI, open TCP Ports and HTTP query
Rule 3: “IP Phone” – Method: HTTP query only
Rule 4: “Printer” – Method: TCP Ports 515 and 9100
Rule 5: “Printer” – Method: TCP Port 9100
Rule 6: “IP Phone” – Method: Vendor OUI, open TCP Ports and HTTP query

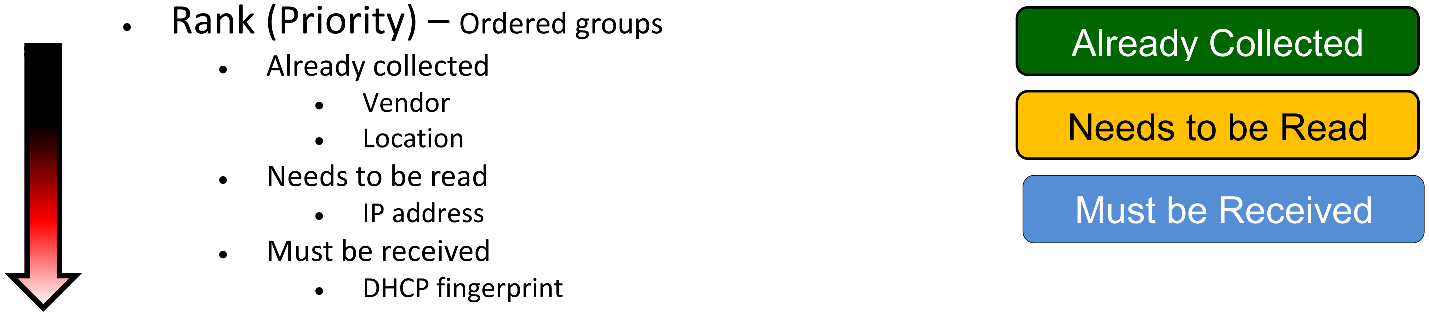
<u>Evaluation Process</u>

1. The rule 1 “Axis Cameras” evaluation result of “fail” continues the device evaluation process with the next ranked rule.
2. The rule 2 “IP Phone” evaluation results in “fail” and the device evaluation process continues with the next ranked rule.
3. The rule 3 “Printer” evaluation result of “Pass**”** classifies the device as “Printer” as defined by the rule classification settings.
4. Rules 4 and 5 are not evaluated for this device.

Profiling Prioritization

Efficient and specific ranking of the rules is required so that a device is evaluated against all of the available rules. FortiNAC evaluates a device against each rule until a pass, fail or cannot evaluate (due to insufficient data) result is reached.

- A rule evaluation result of “Pass” classifies the device as defined by the rule classification settings.
- A rule evaluation result of “Fail” continues the device evaluation process with the next ranked rule.
- A rule evaluation result of “Cannot Evaluate” stops the device evaluation process. This occurs when a method within the rule requires data that is not available or able to be validated as current.

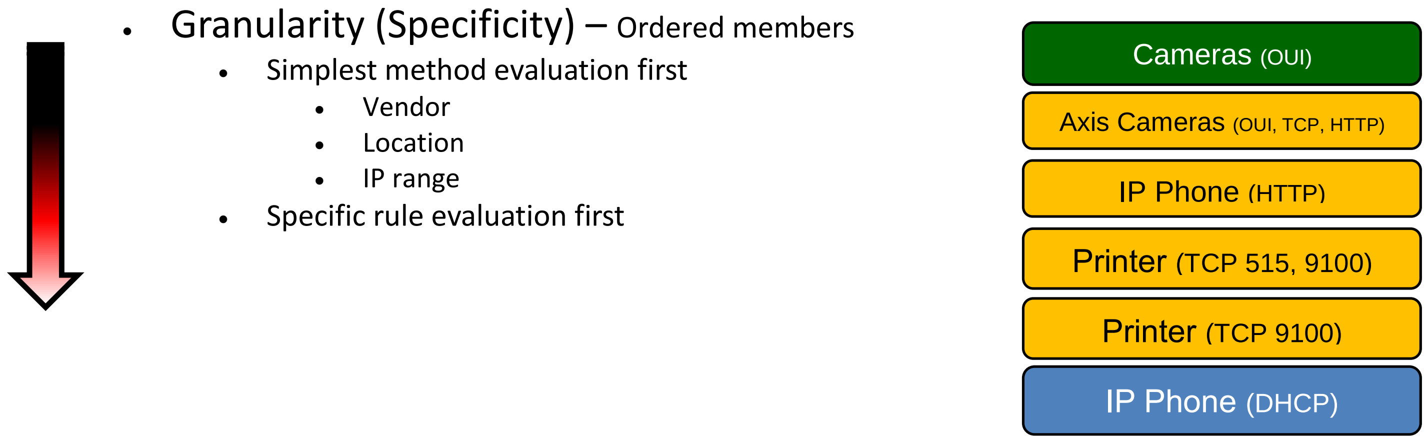


- Rank (Priority) – Ordered groups
  - Already collected
    - Vendor
    - Location
  - Needs to be read
    - IP address
  - Must be received
    - DHCP fingerprint

Already Collected

Needs to be Read

Must be Received



- Granularity (Specificity) – Ordered members
  - Simplest method evaluation first
    - Vendor
    - Location
    - IP range
  - Specific rule evaluation first

Cameras (OUI)

Axis Cameras (OUI, TCP, HTTP)

IP Phone (HTTP)

Printer (TCP 515, 9100)

Printer (TCP 9100)

IP Phone (DHCP)

As a best practice, rules should be categorized into one of three **Prioritized Groupings:**

1. Already Collected Data
2. Needs to Be Read
3. Must be Received

Then organized within each grouping based on granularity.

Prioritized Groups

Already Collected Data

Method	Definition
Location	Compares device's connected location to the specified location objects
Vendor OUI	Compares device's OUI to FortiNAC's OUI database

Needs to be Read

Method	Definition
Active	OS evaluation using NMAP's OS detection database
HTTP/HTTPS	URL query with or without authentication and the ability to match content within the result
IP Range	Compares device's IP to the specified IP range(s)
SNMP	OID query with V1/V2/V3 authentication and the ability to match content within the result. For more details on this method, see section Adding a rule of the Administration Guide. See also Profiling Rule Method Examples in the Appendix.
SSH	Authenticated session with the ability to execute commands and match content within the result of the command
TCP	Open port scan using NMAP
Telnet	Authenticated session with the ability to execute commands and match content within the result of the command
UDP	Open port scan using NMAP
WinRM **(Version 8.5 and above)**	Windows Remote Manager authenticated connection with the ability to execute commands and match content within the result of the command
WMI Profile **(Version 8.5 and above)**	Authenticated WinRM or SSH connection with the ability to evaluate: • OS, Windows Security Center, Serial Number and Asset Tag • Windows Services • Running processes • Installed Application
Network Traffic / Network Flow **(Version 8.6 and above)**	Device type evaluation based on FortiGate session information. See FortiGate Session Information in the Appendix. **Requirement:** Firewall session polling must be enabled. See section **Firewall session polling** of the Administration Guide in Fortinet Document Library.
FortiGate / Firewall **(Version 8.6 and above)**	Device type evaluation based on matching a firewall policy. See FortiGate Session Information in the Appendix. **Requirement:** Firewall session polling must be enabled. See section **Firewall session polling** of the Administration Guide in Fortinet Document Library.
ONVIF **(Version 8.7 and above)**	Determines whether or not an endpoint supports a specific ONVIF Profile. For more details on this method, see section Adding a rule of the Administration Guide in Fortinet Document Library.

Must Be Received

Method	Definition
DHCP Fingerprinting	Device type evaluation based on the DHCP fingerprint compared to FortiNAC's Device Type database. Provides Operating System (OS) and hostname information **Requirement:** In order for FortiNAC to receive fingerprint data, IP Helper must be configured on L3 switches/routers for all production VLANs that use DHCP. The helper must point to the management (eth0) IP address of the FortiNAC Server or Application Server. The management interface only listens and *does not* respond to DHCP requests **Note:** • Not all DHCP fingerprints provide the hostname • The OS is not always able to be determined via DHCP fingerprint. In some cases, the fingerprint may unknown or too similar to other devices to name an OS • Regardless if FortiNAC sees a host offline or online, a Host record will be updated or created if a DHCP packet is received (discover, request or inform) that provides OS and/or hostname.
Passive	OS evaluation through analyzing network traffic with P0f database.
Persistent Agent	Device type evaluation based on the Persistent Agent reported OS compared to FortiNAC's Device Type database

Rule Confirmation and Validation

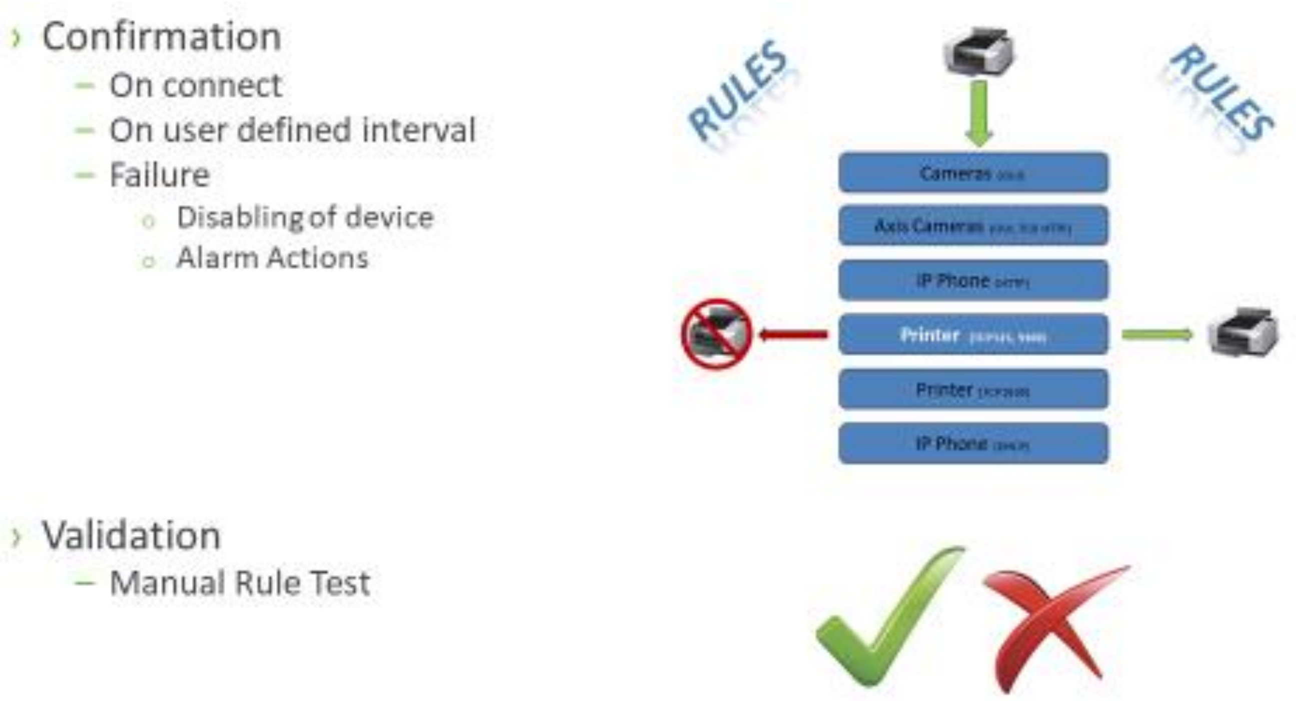
Confirmation

Rule confirmation is an automated re-validation of a previously profiled device.

Note: When a device is initially profiled and matches a rule, the rule information is stored with the classified device record for re-validation purposes.

Confirmation can be performed On-Connect or a time interval. Rule confirmation failure results in event generation. The event can be mapped to an alarm action and/or disabling of the device through a rule action.

The timing and retry settings configuration is currently done through the CLI and applies to all Rules. The default values are 3 additional retries with a 20 second interval between each retry. This allows for 4 confirmation test failures before declaring the device failed.



- Confirmation
  - On connect
  - On user defined interval
  - Failure
    - Disabling of device
    - Alarm Actions
- Validation
  - Manual Rule Test

Validation

Rule validation is the manual testing of a specific rule against a selected host adapter record. Validation results are informational only and used to test rule validity.

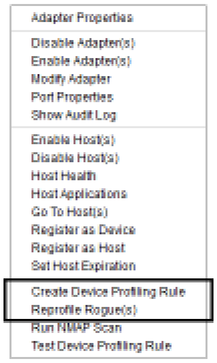
Re-Profiling Rogues and Assisted Rule Creation

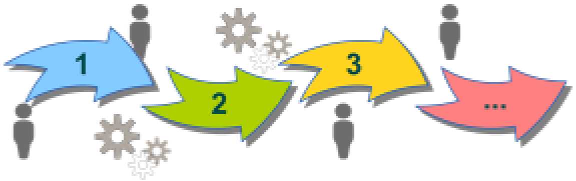
Previously Rogue devices can be re-profiled by all enabled Device Profiling rules. This is a manual process and can be performed on a single rogue or on multiple rogues.

Rules can be revalidated against previously profiled hosts/devices

Create a new rule with vendor OUI and/or DHCP fingerprint information pre-populated. The populated information can then be modified to support necessary criteria. Method attribute data field value matching can include exact, prefix, suffix or substring comparisons.

- Re-profiling Rogues
  - Manual Validation
- Assisted Rule Creation
  - Configured from existing host adapters
  - Method values are pre-populated with known information





How it Works

As new, unknown devices connect to the network, Device Profiler categorizes them and places the devices within FortiNAC based on its Device Profiling Rules:

Device Connection Detected

1. A device or host connects to the network or a device moves to a new port.
2. FortiNAC learns that something has connected or moved.

Is the Device Registered?

3. The Device Identity feature checks for a MAC address. If the MAC address is available, Device Identity compares it to known (registered) MAC addresses.
4. If the MAC address is unknown, the device is placed in the host database as a rogue with any additional information available, such as, IP address or operating system. The time interval that Device Profiler waits to resolve a MAC address to an IP address is 30 minutes, thus allowing time for normal IP to MAC polling to occur.

Rogue Device Evaluation

5. If the device has an IP address, Device Profiler begins to compare the available device information to its Device Profiling Rules. It starts with the rule that is ranked number one and works its way through the list of rules in order by rank until it finds a match to one of the rule's criteria or matching methods. Disabled rules are ignored.

Rogue Device Identification

6. A match is determined by a combination of the **Device Type** selected on the **General** tab for the rule and one or more methods selected on the **Methods** tab.

Example:
Device Type = Mobile Device
Method = DHCP Fingerprinting

A hand held device running Windows CE would match this rule. DHCP Fingerprinting would determine that the device is using Windows CE which is an operating system that corresponds to a Mobile Device. However, if the device type selected is Gaming Device and the Method selected is DHCP Fingerprinting, then a hand held device running Windows CE would not match this rule because Gaming Devices do not use Windows CE.

Fingerprinting and Vendor OUI Methods
Identification methods based on fingerprinting use the FortiNAC fingerprint database which cannot be modified by the user. The exception to this is the **Vendor OUI** method. This method ignores the device type selected on the General tab and uses the information selected within the method, such as the OUI, Vendor name, Vendor Alias or Device Type. Multiple entries are allowed, but the device only has to match one item to match the rule.

7. (Optional) **Notify Sponsor checkbox**: Configure FortiNAC to email Device managers when a host has been evaluated and matches a rule. The email indicates that a new device has been processed. For rules where registration is set to "Manual", administrators know when there are hosts requiring review under Profiled Devices.

   Device managers must have permission to receive notifications and manage profiled devices. See "Profiles for device managers" in the Administration Guide for instructions.

Rogue Device Classification

8. The device is assigned the following:
    - **Device Type** contained within the rule. The exception is the "Catch All" rule (which has no type). The type assigned by Device Profiler takes precedence over any type associated with the device's Vendor in the FortiNAC database.
    - **Role** contained within the rule. If no role is selected, the device is assigned the NAC Default role. The role assigned by Device Profiler takes precedence over any role associated with the device's Vendor OUI in the FortiNAC database.
9. Devices can be registered automatically or manually. If the rule is set to register manually, you must go to the Profiled Devices window to register the device.
10. If **Register As** is enabled in the matching rule, the device can be placed in the Host View or the Topology View or both.
    - If a Host View option was chosen, the device can be added to a specific group as it is added to the Host View.
    - If a Topology View option was chosen, the device is added to a user-specified Container.
11. If the **Access Availability** option has been set to Specify Time, network access for devices placed in the Host View is limited to the configured times. To prevent devices from accessing the network outside the configured timeframe, they are marked "At Risk" for the Guest No Access admin scan.
12. When the device has been through the entire process and has been registered either automatically or manually, it will no longer display as a rogue. Depending on the options you chose in the rule it is displayed in the Host View, the Topology View or both.
13. If the device does not match any rule, it is associated with the default Catch All rule. Depending on the settings configured within this rule, the device can be associated with the rule but still remain a rogue.
14. Devices that are registered and associated with a user are placed in the Host View and removed from the Profiled Devices window. Devices that are placed in Topology only are removed from Profiled Devices. All other devices processed by Device Profiler remain in the Profiled Devices window and in the Host View.

Considerations

- Invalid Physical Address Handling (OUI Method): If the MAC address matches a rule, the host will be registered regardless if vendor OUI is in the database. Device Profiler does not check to determine if the MAC address is valid. For details regarding the vendor OUI database, see Vendor OUIs in the Administration Guide.
- Devices connecting via 802.1x but not using an agent may get registered using Device Profiler before the logged on user is detected.

Configuration

Determine Method(s) to Use for Profiling

Method	Definition
Location	Compares device's connected location to the specified location objects
Vendor OUI	Compares device's OUI to FortiNAC's OUI database
Active	OS evaluation using NMAP's OS detection database To verify the OS detected on a host, see NMAP scan
HTTP/HTTPS	URL query with or without authentication and the ability to match content within the result
IP Range	Compares device's IP to the specified IP range(s). Wildcard (*) can also be used. Examples: Starting IP: 10.10.124.140 Ending IP: 10.10.124.180 Starting IP: 10.10.124.* Ending IP: 10.10.125.* Starting IP: *.*.*.140 Ending IP: *.*.*.180
SNMP	OID query with V1/V2/V3 authentication and the ability to match content within the result. For more details on this method, see Adding a rule in the Administration Guide. See also Profiling Rule Methods Examples in the Appendix.
SSH	Authenticated session with the ability to execute commands and match content within the result of the command.
TCP	Open port scan using NMAP To identify open ports on a host, see NMAP scan
Telnet	Authenticated session with the ability to execute commands and match content within the result of the command.

UDP	Open port scan using NMAP To identify open ports on a host, see NMAP scan
WinRM **(Version 8.5 and above)**	Windows Remote Manager authenticated connection with the ability to execute commands and match content within the result of the command.
WMI Profile **(Version 8.5 and above)**	Authenticated WinRM or SSH connection with the ability to evaluate: • OS, Windows Security Center, Serial Number and Asset Tag • Windows Services • Running processes • Installed applications • Logged On User • Associated adapters For more details, see Using WMI and WinRM for Device Profiling.
DHCP Fingerprinting	Device type evaluation based on the DHCP fingerprint compared to FortiNAC's Device Type database To verify fingerprint data FortiNAC is currently receiving, see Identify Available Fingerprints
Passive	OS evaluation through analyzing network traffic with P0f database.
Persistent Agent	Device type evaluation based on the Persistent Agent reported OS compared to FortiNAC's Device Type database
ONVIF **(Version 8.7 and above)**	Determines whether or not an endpoint supports a specific ONVIF Profile. For more details on this method, see section Adding a rule of the Administration Guide in Fortinet Document Library.
Network Traffic / Network Flow **(Version 8.6 and above)**	Device type evaluation based on FortiGate session information. **Requirement:** Firewall session polling must be enabled. See section **Firewall session polling** of the Administration Guide in Fortinet Document Library.
FortiGate / Firewall **(Version 8.6 and above)**	Device type evaluation based on matching a firewall policy. **Requirement:** Firewall session polling must be enabled. See section **Firewall session polling** of the Administration Guide in Fortinet Document Library.
FortiGuard	Pulls IoT device information from the FortiGuard IoT Service based on the MAC address. **Note**: • Requires FortiCare support contract to enable FortiGuard IoT Service. Otherwise, the checkbox will not be selectable. • IoT service responses are enhanced when the "FortiGuard Collect Service" is enabled in **System > Settings > Device Profiler**. For more details on this method, see section Adding a rule of the Administration Guide.

NMAP Scan

1. Navigate to **Hosts > Adapter View**
2. Search for MAC address of example host used for profiling
3. Right click on adapter record and select **Run NMAP Scan**

Example:

```
Starting Nmap 7.40 ( https://nmap.org ) at 2019-09-11 10:39 EDT
Nmap scan report for 192.168.10.21
Host is up (0.0048s latency).
Not shown: 96 filtered ports
PORT    STATE SERVICE    VERSION
22/tcp  open  ssh        (protocol 2.0)
23/tcp  open  telnet     Linux telnetd
80/tcp  open  http?
443/tcp open  ssl/https?
2 services unrecognized despite returning data. If you know the
service/version, please submit the following fingerprints at
https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=7.40%I=2%D=9/11%Time=5D79071F%P=x86_64-redhat-linux-gnu%r(
SF:GetRequest,140,"HTTP/1\.1\x20200\x20OK\r\nDate:\x20Wed,\x2011\x20Sep\x2
SF:02019\x2014:45:58\x20GMT\r\nServer:\x20xxxxxxxx-xxxxx\r\nLast-Modified:
SF:\x20Fri,\x2001\x20Sep\x202017\x2004:29:27\x20GMT\r\nAccept-Ranges:\x20b
SF:ytes\r\nContent-Length:\x2079\r\nConnection:\x20close\r\nContent-Type:\
SF:x20text/html\r\nX-Frame-
Options:\x20SAMEORIGIN\r\n\r\n&lt;html&gt;\n&lt;script\x
<…>
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10, Linux 2.6.32 - 3.13, Linux 3.2 - 3.16, Linux
3.4
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.84 seconds
```

Identify Available Fingerprints

1. Navigate to **Hosts > Device Identity**
2. From **Filter** drop down menu, select **Physical Address**
3. Enter MAC address and click **Update**

WinRM - Identify System Product Type

1. In FortiNAC CLI, set logger yams.dpc.WindowsDetailMethod.files to FINEST to write the output to disk:
CampusMgrDebug -logger yams.dpc.WindowsDetailMethod.files -level FINEST

2. Run the following powershell command on the system:
Get-WmiObject -namespace root/cimv2 Win32_OperatingSystem | select-object ProductType

3. Search the resulting file in **/home/cm/fingerprints** for the product type.
zgrep ProductType /home/cm/fingerprints/<filename>

Example:

```
> zgrep ProductType /home/cm/fingerprints/WindowsDetails_10.12.12.28.json.gz
"ProductType":  1,
```

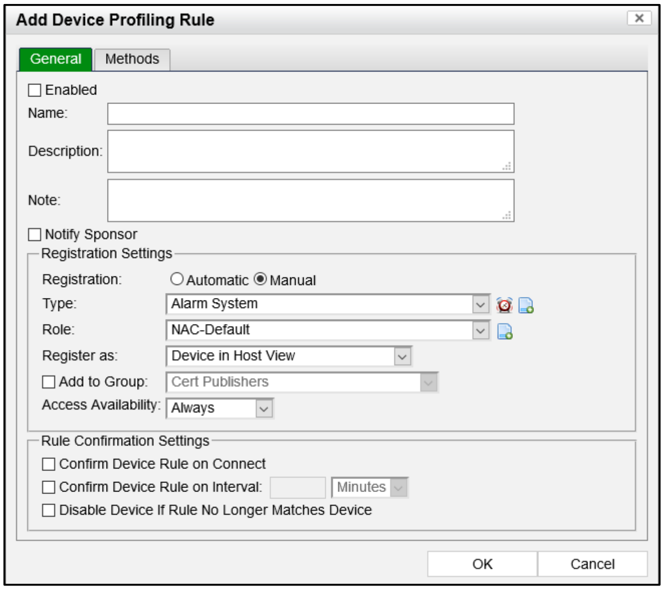
4. Disable logger
CampusMgrDebug -logger yams.dpc.WindowsDetailMethod.files -level INFO

Build Profiling Rules

These steps are also outlined under Adding a rule in the Administration Guide.

1. In the Administration UI, navigate to **Hosts > Device Profiling Rules.**
2. Click **Add** to create new rule**,** or highlight existing rule and click **Modify.**

General (Classification Settings)



Add Device Profiling Rule

□ Enabled

Name:

Description:

Note:

□ Notify Sponsor

Registration Settings

Registration: ○ Automatic ● Manual

Type: Alarm System

Role: NAC-Default

Register as: Device in Host View

□ Add to Group: Cert Publishers

Access Availability: Always

Rule Confirmation Settings

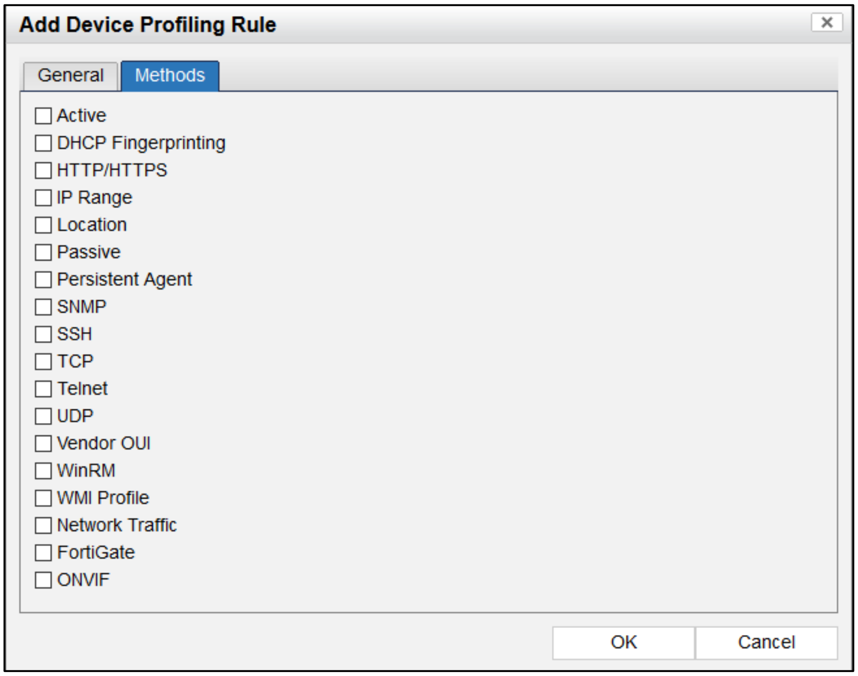
□ Confirm Device Rule on Connect

□ Confirm Device Rule on Interval: Minutes

□ Disable Device If Rule No Longer Matches Device

Setting	Definition
Enabled	Select to make rule active
Notify Sponsor	Users whose Admin Profile gives them permission to manage devices associated with this rule are notified whenever a device has been matched to this rule. This includes rogues that have been processed again by clicking the Run button on the Device Profiling Rules window. **Note:** Device managers must have permission to receive notifications and manage profiled devices. See Profiles for device managers in the Administration Guide for instructions.
Registration	• Automatic • Manual (with or without sponsorship) **Note:** It is recommended to test rules first using Manual registration. This allows the Administrator to verify the new rule is matching properly.
Type	Device label and icon
Role	Attribute whose value further defines a device
Group	Collection of like devices
Access Availability	Authorized access time
Rule Confirmation Settings	• **Confirm Device Rule on Connect** - upon reconnect, verifies the device still matches the previously profiled rule • **Confirm Device Rule on Interval** - Revalidates device • **Disable Device If Rule No Longer Matches Device** - Changes host status to disabled and generates event (Rule Confirmation Failure/Rule Confirmation Success)

Methods



Add Device Profiling Rule

□ Active
□ DHCP Fingerprinting
□ HTTP/HTTPS
□ IP Range
□ Location
□ Passive
□ Persistent Agent
□ SNMP
□ SSH
□ TCP
□ Telnet
□ UDP
□ Vendor OUI
□ WinRM
□ WMI Profile
□ Network Traffic
□ FortiGate
□ ONVIF

3. Click **OK** to save.

Validate Rule

1. Navigate to **Hosts > Adapter View**
2. Search for rogue device MAC address that is expected to match rule.
3. Right click on adapter record and select **Test Device Profiling Rule**.
4. From drill-down menu, select the rule to be tested and click **OK**.

Note: If device matches a rule using WMI Profile method

- Host will appear under the Profiled Devices
- Adapter record fills in with any information collected from WMI Profile

If rule does not match as expected, see Troubleshooting section.

Prioritize Rules

1. **Categorize Rules into Prioritized Groupings**: Identify which rules belong in each grouping based on their methods.

   Priority 1: Already Collected Data

   - Location
   - Vendor OUI

   Priority 2: Needs to be Read

   - Active
   - HTTP/HTTPS
   - IP Range
   - SNMP
   - SSH
   - TCP
   - Telnet
   - UDP
   - WinRM
   - WMI Profile
   - Network Traffic
   - FortiGate
   - ONVIF

   Priority 3: Must Be Received

   - DHCP Fingerprinting
   - Passive
   - Persistent Agent

2. **Organize Rules within Groupings**:
    a. Place rules using simplest methods (Vendor OUI, Location or IP Range) first.
    b. Place rules with most granularity next
    c. Place rules with least granularity last

Example: The below rules are examples from the overview.
IP Phone (DHCP)
Axis cameras (OUI, TCP, HTTP)
Printer (TCP 9100)
Cameras (OUI)
IP Phone (HTTP)
Printer (TCP, 515. 9100)

Step 1: Categorize Rules into Prioritized Groupings

Priority 1: Already collected	Cameras (OUI)
Priority 2: Needs to be read	IP Phone (HTTP) Printer (TCP, 515. 9100) Printer (TCP 9100) Axis cameras (OUI, TCP, HTTP)
Priority 3: Must be received	IP Phone (DHCP)

Step 2: Organize Rules within Groupings

Priority 1: Already collected	Cameras (OUI)
Priority 2: Needs to be read	Axis cameras (OUI, TCP, HTTP) IP Phone (HTTP) Printer (TCP, 515. 9100) Printer (TCP 9100)
Priority 3: Must be received	IP Phone (DHCP)

Rules with more granular method criteria are placed ahead of other rules with less granular criteria (Printer rule with multiple open TCP ports is ranked ahead of Printer rule with one).

Resulting rule ranking:

1. Cameras (OUI)
2. Axis cameras (OUI, TCP, HTTP)
3. IP Phone (HTTP)
4. Printer (TCP, 515. 9100)
5. Printer (TCP 9100)
6. IP Phone (DHCP)

Validate Rule Prioritization

Re-Profile an Individual or Specified Set of Rogue Records

1. Once rules are prioritized, right-click on the rogue adapter record and select **Reprofile Rogue(s)**.
2. Navigate to **Hosts > Profiled Devices** and verify the device was profiled correctly.

If the device matched the wrong rule, navigate to **Hosts > Device Profiling Rules**. Review the ranking and rule settings and modify as necessary.

Once rules are validated, set registration to Automatic (if desired).

Re-profile All Rogue Records in the Database

To re-evaluate rogue hosts against all enabled Device Profiling Rules:

1. Navigate to **Hosts > Device Profiling Rules**.
2. Click **Run**.
3. A message displays asking if you would like to evaluate rogues. Click **Yes** to continue.
4. A new message displays indicating that x number of rogues are being evaluated.
5. Device Profiler compares any rogue hosts to the list of enabled Device Profiling Rules and processes them accordingly.
6. Navigate to **Hosts > Profiled Devices** to view the list of profiled devices and verify the number of rogues left to evaluate (Rogue Evaluation Queue Size).

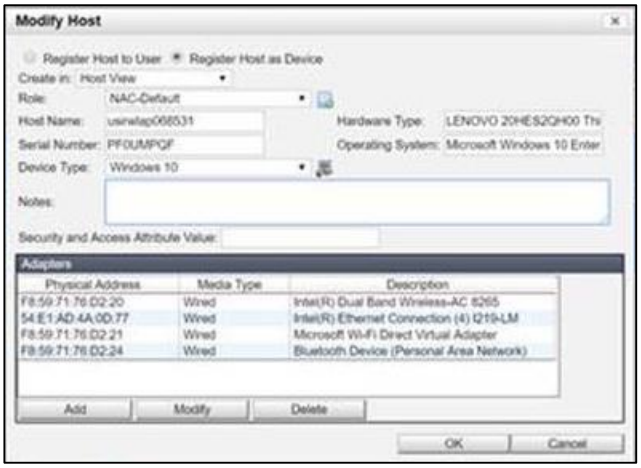
Note: Rogue hosts must have an **online** connection status in order to be profiled.

DHCP Fingerprinting

DHCP fingerprints will not be collected from a device until its DHCP lease is released. Depending upon the lease time, this can take days or weeks. Therefore, once the rule is configured, run the Device Profiling Rules regularly until a reasonable time has passed such that all the leases would have expired and renewed.

WMI Profiling

When re-profiling the device from adapter view, the host will display under Profiled devices. Once registered, all the reported adaptors are associated to the host record.



Modify Host

○ Register Host to User ● Register Host as Device

Create in: Host View

Role: NAC-Default

Host Name: usnwlap068531

Hardware Type: LENOVO 20HES2QH00 Thi

Serial Number: PF0UMPQF

Operating System: Microsoft Windows 10 Enter

Device Type: Windows 10

Notes:

Security and Access Attribute Value:

Adapters

Physical Address	Media Type	Description
F8:59:71:76:D2:20	Wired	Intel(R) Dual Band Wireless-AC 8265
54:E1:AD:4A:0D:77	Wired	Intel(R) Ethernet Connection (4) I219-LM
F8:59:71:76:D2:21	Wired	Microsoft Wi-Fi Direct Virtual Adapter
F8:59:71:76:D2:24	Wired	Bluetooth Device (Personal Area Network)

WMI Profiling Requirements

- Domain admin credentials must use format user@domain.com in the WMI Profile method
- Windows Management Framework 3.0
- Endstation requirements:
    - WRM Service running
    - Registry settings
        - AllowUnencrypted = true
        - AllowRemoteShellAccess = true

Using WMI and WinRM for Device Profiling

Overview

Starting on version 8.5, FortiNAC Device Profiling has been enhanced with two new methods:

- **WinRM:** Similar to the SSH method, with WinRM you can run powershell commands on Windows machines and match on the output.

  Windows Remote Management (WinRM) is a SOAP based management protocol for Windows which means it's much more practical for firewall usage than the old DCOM protocol used previously in the Agentless solution. SOAP uses HTTP so it's a relatively simple one-port opening. SOAP may be awful, but at least it's practical. The previously existing "Agentless Scanner" functionality has been removed. (https://docs.microsoft.com/en-us/windows/desktop/winrm/portal)

- **WMI Profile:** Method with built-in filtering on Windows version, applications, services, Logged on User, etc.

  Windows Management Instrumentation (WMI) is the Microsoft implementation of Web-Based Enterprise Management (WBEM), which is an industry initiative to develop a standard technology for accessing management information in an enterprise environment. WMI uses the Common Information Model (CIM) industry standard to represent systems, applications, networks, devices, and other managed components. (https://docs.microsoft.com/en-us/windows/desktop/wmisdk/about-wmi)

Requirements

- Windows Remote Management (WS-Management) service must be enabled on endpoints.
- The WinRM HTTP/S port(s) [TCP 5986 or 5985 (insecure)] must be enabled and available through the firewall to communicate with FortiNAC. HTTPS (port TCP 5986) is strongly encouraged for security purposes.
- NTLM Authentication with domain credentials authorized to run powershell commands get-wmiobject, get-itemproperty, get-service, get-process, convertto-json, and read the registry.
- Minimum Windows Management Framework (WMF) version: 3.0.
  - Requiring WMF 3.0 greatly simplifies the code and makes it much more reliable due to the ConvertTo-Json powershell command.
  - Using whatever tools normally used to install software, ensure WMF 3.0 or later is installed. (mainly for Windows 7 SP1)
- Supported Windows Versions:
  - Windows Server 2008 R2 SP1 - With WMF 3.0
  - Windows 7 SP1 - With WMF 3.0
  - Windows 8.1
  - Windows Server 2012 R2
  - Windows 10 (All versions)
  - Windows Server 2016
  - Windows Server 2019

Note: The following documentation was built based on a Windows 2012 Server R2, FortiNAC version 8.5 and a Windows 10 Machine.

Endpoint Setup

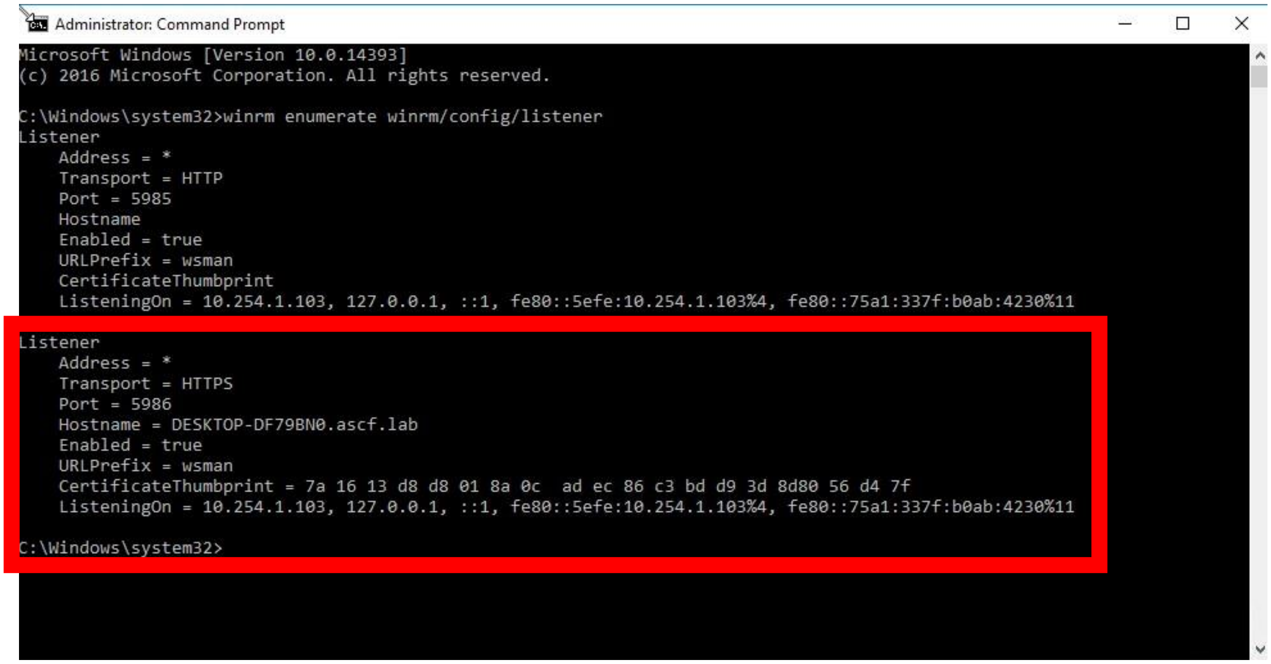
Ensure that the endpoints support WinRM. Run the following command to see if WinRM is already configured.

winrm enumerate winrm/config/listener

The output should be similar to the result below:

```
Listener
      Address = *
      Transport = HTTPS Port = 5986
      Hostname = [host.example.com] Enabled = true
      URLPrefix = wsman
      CertificateThumbprint = [cert fingerprint]
      ListeningOn = [ip addresses]
```

If you see a listener on port 5986 with Transport = HTTPS, you already have WinRM over HTTPS configured and are ready on the Windows side. Below there is an image representing the command output.



```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>winrm enumerate winrm/config/listener
Listener
    Address = *
    Transport = HTTP
    Port = 5985
    Hostname
    Enabled = true
    URLPrefix = wsman
    CertificateThumbprint
    ListeningOn = 10.254.1.103, 127.0.0.1, ::1, fe80::5efe:10.254.1.103%4, fe80::75a1:337f:b0ab:4230%11

Listener
    Address = *
    Transport = HTTPS
    Port = 5986
    Hostname = DESKTOP-DF79BN0.ascf.lab
    Enabled = true
    URLPrefix = wsman
    CertificateThumbprint = 7a 16 13 d8 d8 01 8a 0c  ad ec 86 c3 bd d9 3d 8d80 56 d4 7f
    ListeningOn = 10.254.1.103, 127.0.0.1, ::1, fe80::5efe:10.254.1.103%4, fe80::75a1:337f:b0ab:4230%11

C:\Windows\system32>
```

If not, you have 2 options to enable WinRM on the endpoint:

- Using GPO. This is the recommend method to use. This document will guide you on how to create a GPO that enables and configures everything you need in order to collect the machine data; or
- Running a command on each endpoint you want to profile (see **Enabling WinRM Manually**).

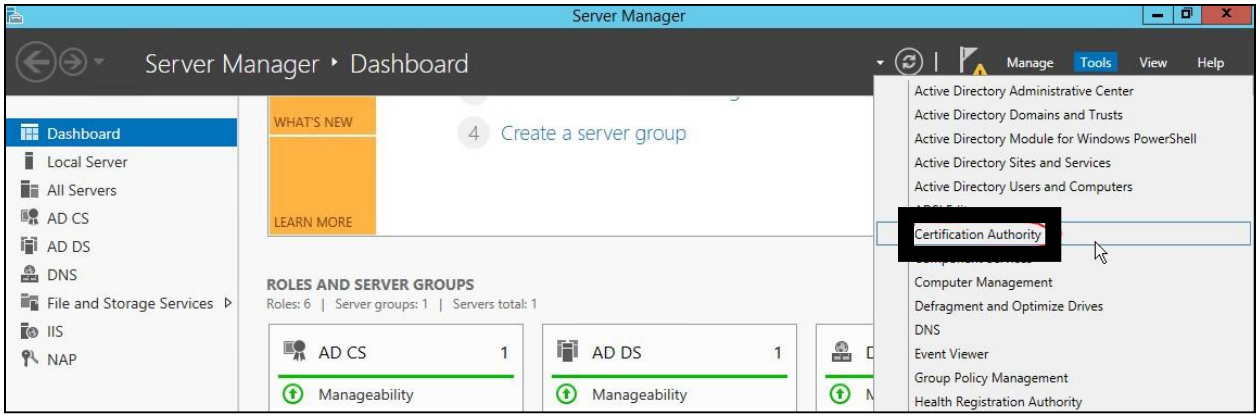
GPO / Certificate Configuration

Steps required to configure a secure HTTPS connection from FortiNAC to endpoints using WinRM:

- Certificate enrollment resulting in a certificate on the endpoint with hostname as subject (e.g. CN=hostname.example.com) and "Server Authentication" key usage;
- Windows Remote Management service enabled;
- WinRM Listener on port 5986 with transport HTTPS;
- Inbound Windows Firewall rule allowing connections on port TCP 5986;

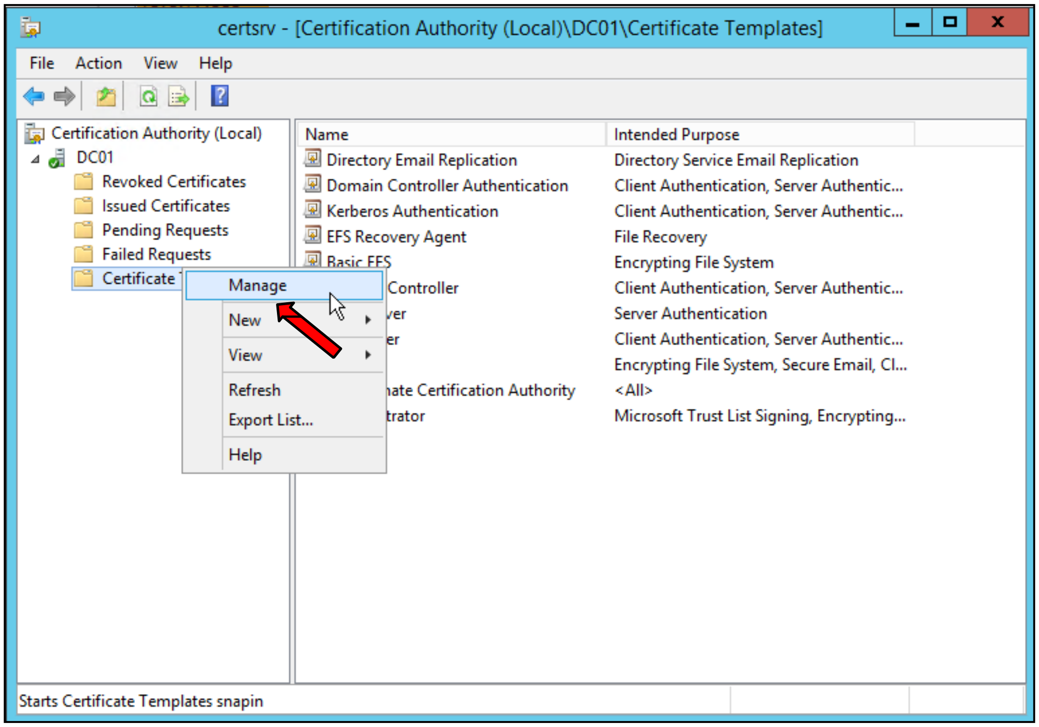
Note: To forego security (not recommended), configure and use HTTP while allowing unencrypted content. For instructions, see Alternate (Insecure) Configuration.

1. Create the Certificate Template. Go to W**indows Server Manager -> Tools -> Certification Authority**.



Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD CS
AD DS
DNS
File and Storage Services
IIS
NAP
WHAT'S NEW
LEARN MORE
4 Create a server group
ROLES AND SERVER GROUPS
Roles: 6 | Server groups: 1 | Servers total: 1
AD CS 1
Manageability
AD DS 1
Manageability
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
Certification Authority
Computer Management
Defragment and Optimize Drives
DNS
Event Viewer
Group Policy Management
Health Registration Authority

2. In Active Directory Certificate Services, expand the CA and select "Certificate Templates". Right click on it and select the action “Manage”.

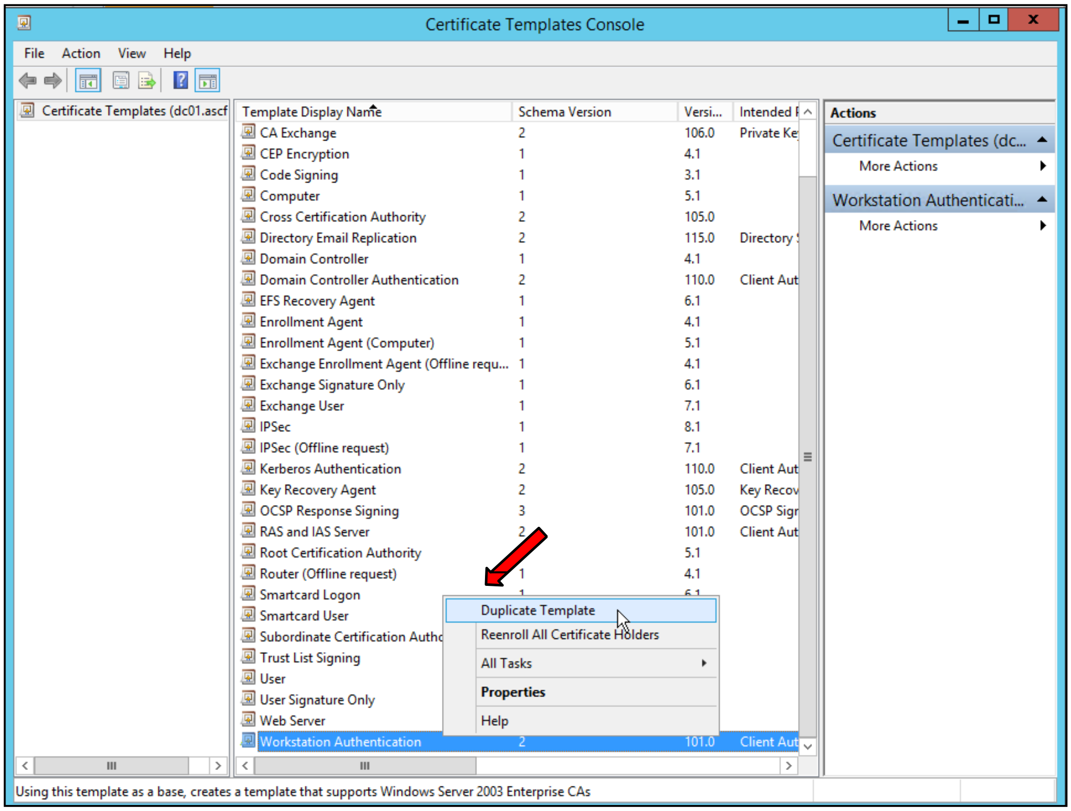

certsrv - [Certification Authority (Local)\DC01\Certificate Templates]
File
Action
View
Help
Manage
New
View
Refresh
Export List...
Help

Certification Authority (Local)
DC01
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate

Name	Intended Purpose
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authentic...
Kerberos Authentication	Client Authentication, Server Authentic...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Controller	Client Authentication, Server Authentic...
ver	Server Authentication
er	Client Authentication, Server Authentic...
	Encrypting File System, Secure Email, Cl...
ate Certification Authority	<All>
trator	Microsoft Trust List Signing, Encrypting...

Starts Certificate Templates snapin

3. Select the Workstation Authentication template, right click on it and choose the action “Duplicate Template”.

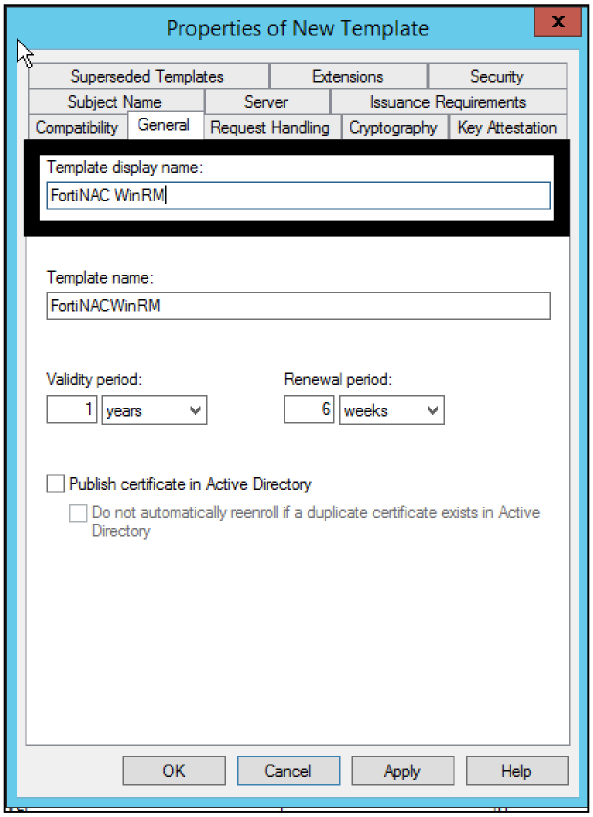

Certificate Templates Console
File
Action
View
Help
Actions
Certificate Templates (dc...
More Actions
Workstation Authenticati...
More Actions
Duplicate Template
Reenroll All Certificate Holders
All Tasks
Properties
Help

Certificate Templates (dc01.ascf

Template Display Name	Schema Version	Versi...	Intended F
CA Exchange	2	106.0	Private Ke
CEP Encryption	1	4.1	
Code Signing	1	3.1	
Computer	1	5.1	
Cross Certification Authority	2	105.0	
Directory Email Replication	2	115.0	Directory
Domain Controller	1	4.1	
Domain Controller Authentication	2	110.0	Client Aut
EFS Recovery Agent	1	6.1	
Enrollment Agent	1	4.1	
Enrollment Agent (Computer)	1	5.1	
Exchange Enrollment Agent (Offline requ...	1	4.1	
Exchange Signature Only	1	6.1	
Exchange User	1	7.1	
IPSec	1	8.1	
IPSec (Offline request)	1	7.1	
Kerberos Authentication	2	110.0	Client Aut
Key Recovery Agent	2	105.0	Key Recov
OCSP Response Signing	3	101.0	OCSP Sigr
RAS and IAS Server	2	101.0	Client Aut
Root Certification Authority	2	5.1	
Router (Offline request)	1	4.1	
Smartcard Logon	1	6.1	
Smartcard User			
Subordinate Certification Autho			
Trust List Signing			
User			
User Signature Only			
Web Server			
Workstation Authentication	2	101.0	Client Aut

Using this template as a base, creates a template that supports Windows Server 2003 Enterprise CAs

4. Change the “Template Display Name” to "FortiNAC WinRM" on the GENERAL Tab.



Template display name: FortiNAC WinRM

Template name: FortiNACWinRM

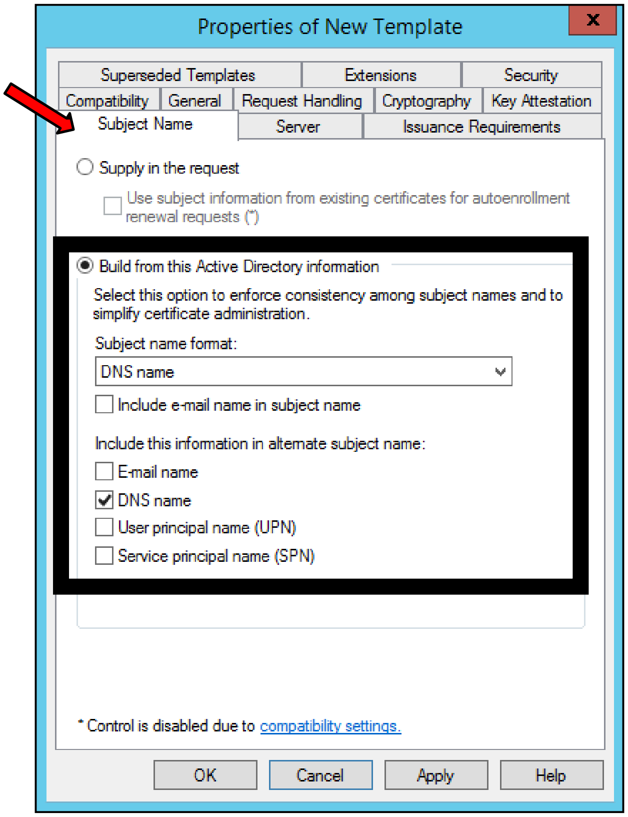
Validity period: 1 years

Renewal period: 6 weeks

☐ Publish certificate in Active Directory

☐ Do not automatically reenroll if a duplicate certificate exists in Active Directory

5. Click on the tab named as “Subject Name”. Select "Build from this Active Directory Information". Make sure the following options are configured as below:
    a. <u>Subject name format</u> = DNS name
    b. <u>Include this information in alternate subject name</u> = DNS Name



○ Supply in the request

□ Use subject information from existing certificates for autoenrollment renewal requests (*)

● Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format:

DNS name

□ Include e-mail name in subject name

Include this information in alternate subject name:

□ E-mail name

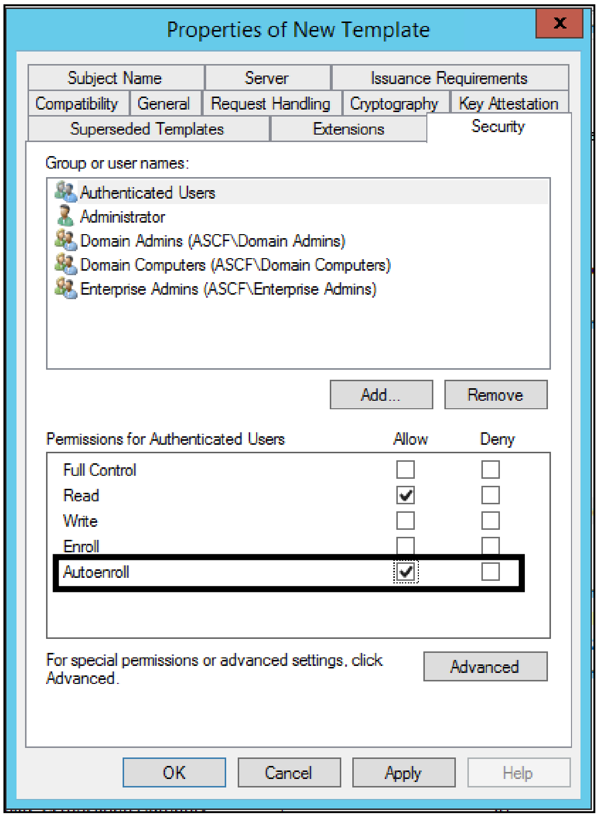
☑ DNS name

□ User principal name (UPN)

□ Service principal name (SPN)

* Control is disabled due to compatibility settings.

6. Click on the “Security” tab. Ensure the desired computers have the Autoenroll permission (e.g. select "Domain Computers" group, and tick the Autoenroll box under Allow)



Properties of New Template

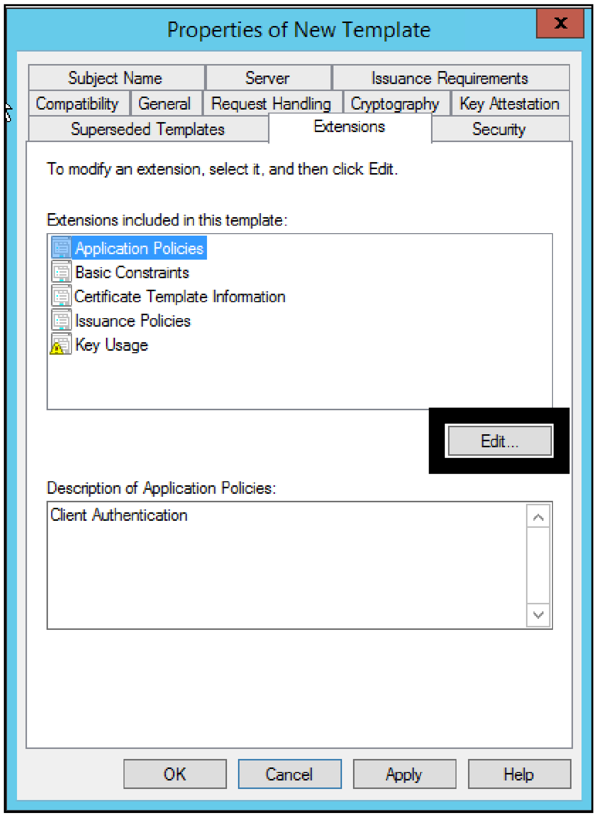
Group or user names:

- Authenticated Users
- Administrator
- Domain Admins (ASCF\Domain Admins)
- Domain Computers (ASCF\Domain Computers)
- Enterprise Admins (ASCF\Enterprise Admins)

Permissions for Authenticated Users	Allow	Deny
Full Control	□	□
Read	☑	□
Write	□	□
Enroll	□	□
Autoenroll	☑	□

For special permissions or advanced settings, click Advanced.

7. Click on the Extensions tab. Select Application Policies and then click on the Edit button.



Properties of New Template

To modify an extension, select it, and then click Edit.

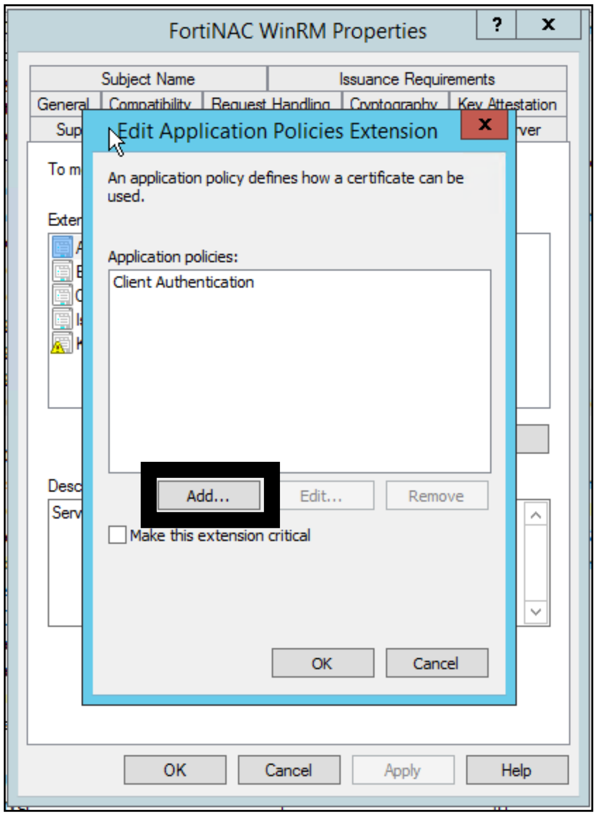
Extensions included in this template:

- Application Policies
- Basic Constraints
- Certificate Template Information
- Issuance Policies
- Key Usage

Description of Application Policies:

Client Authentication

8. Click on the Add button.



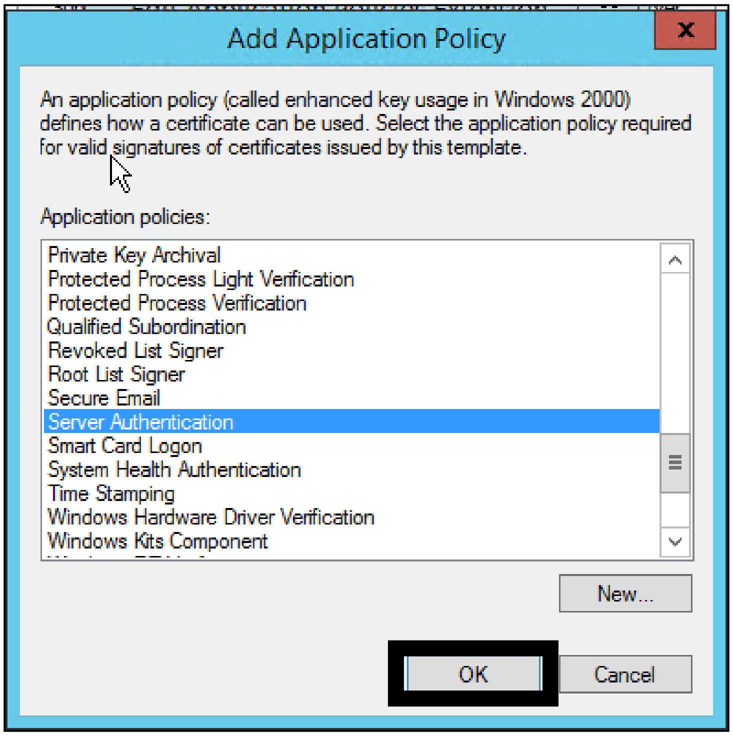
An application policy defines how a certificate can be used.

Application policies:

Client Authentication

□ Make this extension critical

9. Choose Server Authentication.

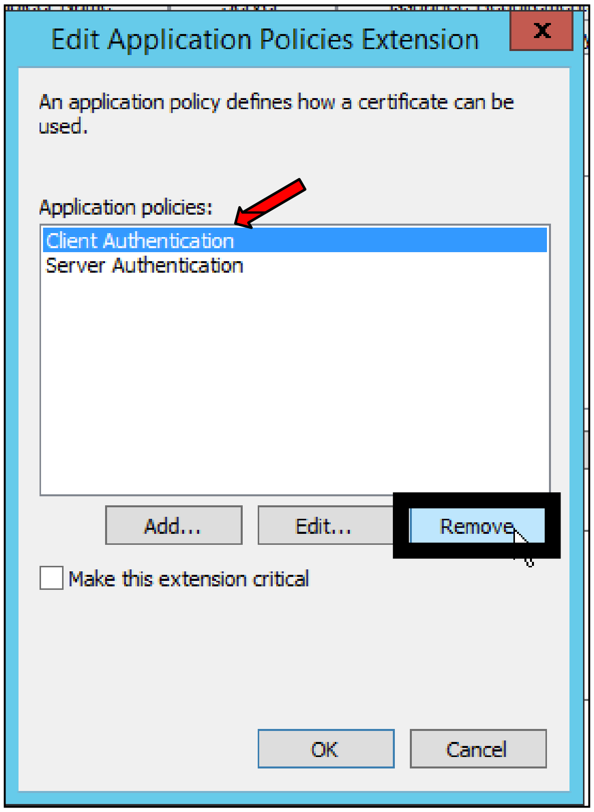


An application policy (called enhanced key usage in Windows 2000) defines how a certificate can be used. Select the application policy required for valid signatures of certificates issued by this template.

Application policies:

Private Key Archival
Protected Process Light Verification
Protected Process Verification
Qualified Subordination
Revoked List Signer
Root List Signer
Secure Email
Server Authentication
Smart Card Logon
System Health Authentication
Time Stamping
Windows Hardware Driver Verification
Windows Kits Component

10. Optionally, select "Client Authentication" and click on the remove button.


Edit Application Policies Extension

An application policy defines how a certificate can be used.

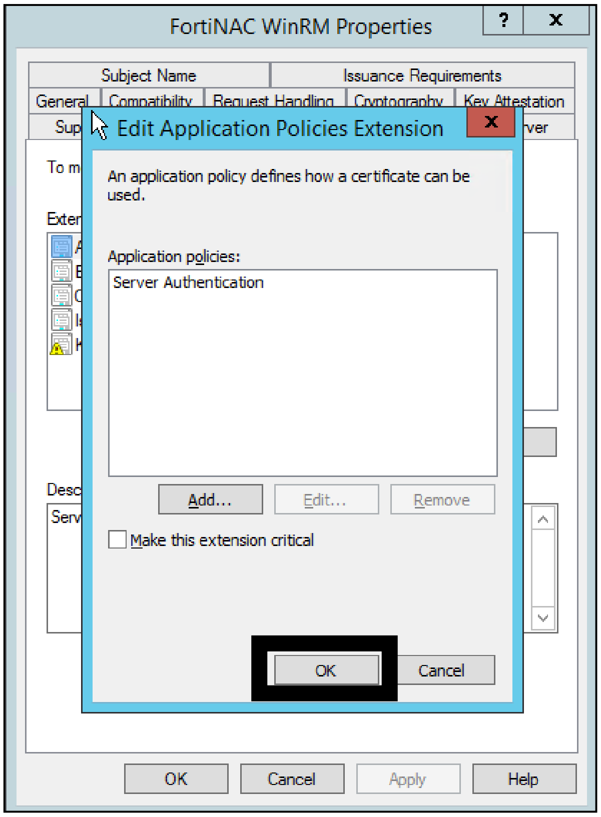
Application policies:

Client Authentication

Server Authentication

□ Make this extension critical

11. Click OK to dismiss the "Edit Application Policies Extension".


FortiNAC WinRM Properties

Edit Application Policies Extension

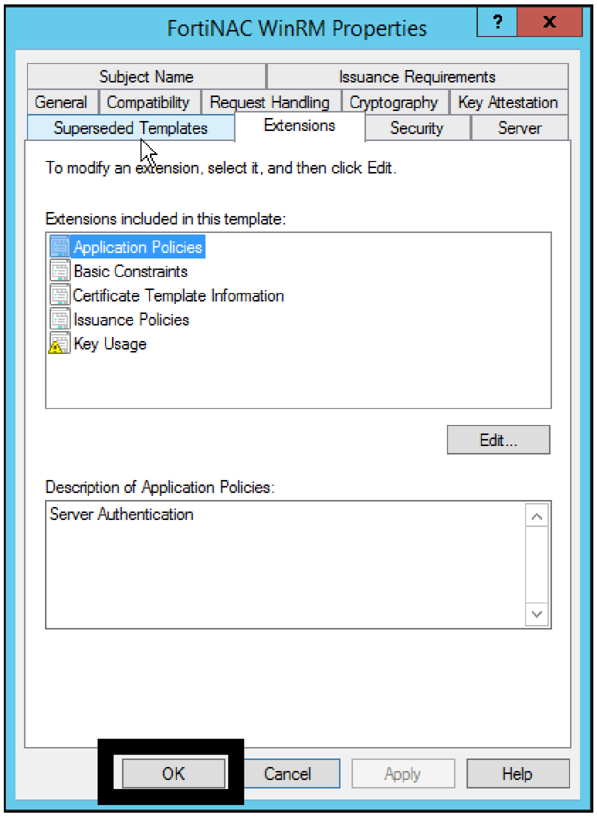
An application policy defines how a certificate can be used.

Application policies:

Server Authentication

□ Make this extension critical

12. Click OK to close the "FortiNAC WinRM Properties" dialog.



To modify an extension, select it, and then click Edit.

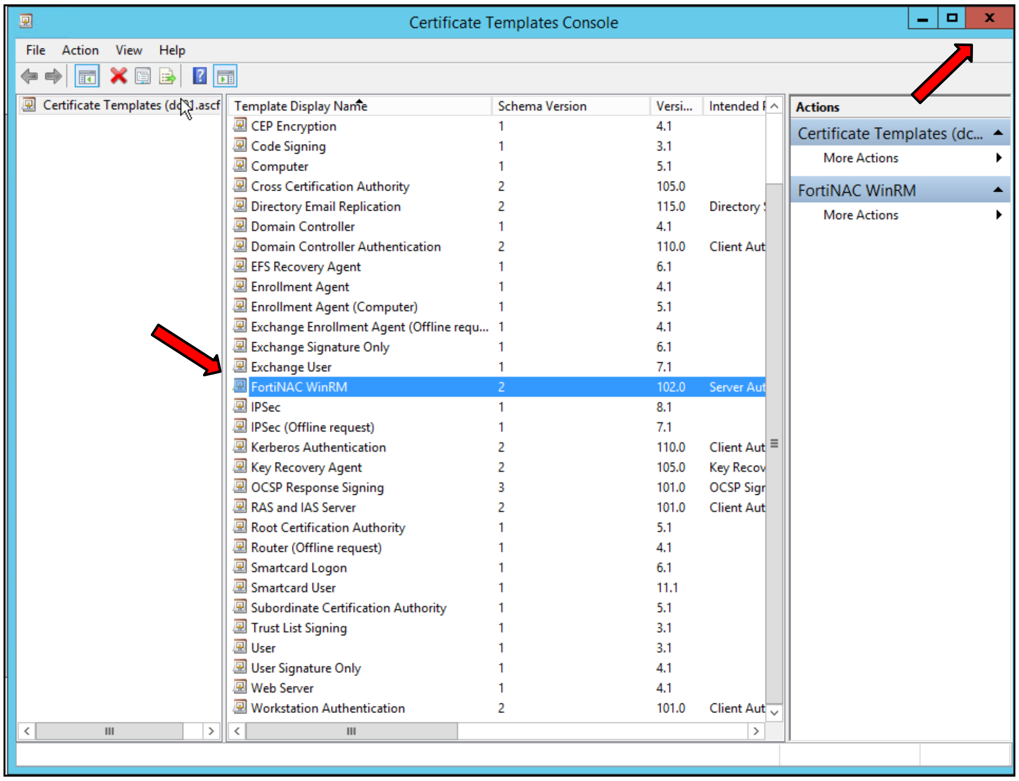
Extensions included in this template:

- Application Policies
- Basic Constraints
- Certificate Template Information
- Issuance Policies
- Key Usage

Description of Application Policies:

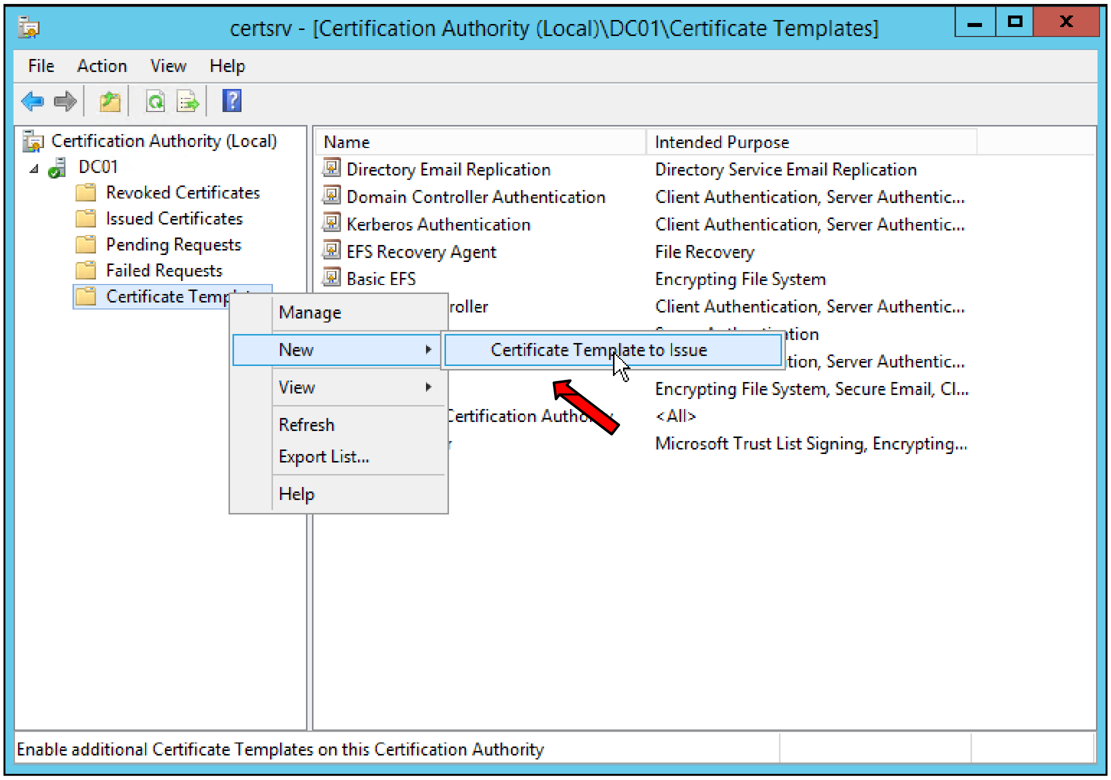
Server Authentication

13. Close the Certificate Template Console window.


Certificate Templates Console
File
Action
View
Help
Certificate Templates (dc1.ascf
Actions
Certificate Templates (dc...
More Actions
FortiNAC WinRM
More Actions

Template Display Name	Schema Version	Versi...	Intended F
CEP Encryption	1	4.1	
Code Signing	1	3.1	
Computer	1	5.1	
Cross Certification Authority	2	105.0	
Directory Email Replication	2	115.0	Directory !
Domain Controller	1	4.1	
Domain Controller Authentication	2	110.0	Client Aut
EFS Recovery Agent	1	6.1	
Enrollment Agent	1	4.1	
Enrollment Agent (Computer)	1	5.1	
Exchange Enrollment Agent (Offline requ...	1	4.1	
Exchange Signature Only	1	6.1	
Exchange User	1	7.1	
FortiNAC WinRM	2	102.0	Server Aut
IPSec	1	8.1	
IPSec (Offline request)	1	7.1	
Kerberos Authentication	2	110.0	Client Aut
Key Recovery Agent	2	105.0	Key Recov
OCSP Response Signing	3	101.0	OCSP Sigr
RAS and IAS Server	2	101.0	Client Aut
Root Certification Authority	1	5.1	
Router (Offline request)	1	4.1	
Smartcard Logon	1	6.1	
Smartcard User	1	11.1	
Subordinate Certification Authority	1	5.1	
Trust List Signing	1	3.1	
User	1	3.1	
User Signature Only	1	4.1	
Web Server	1	4.1	
Workstation Authentication	2	101.0	Client Aut

14. On the Certification Management tool, select Certificate Templates again and choose Action -> New -> Certificate Template to Issue.

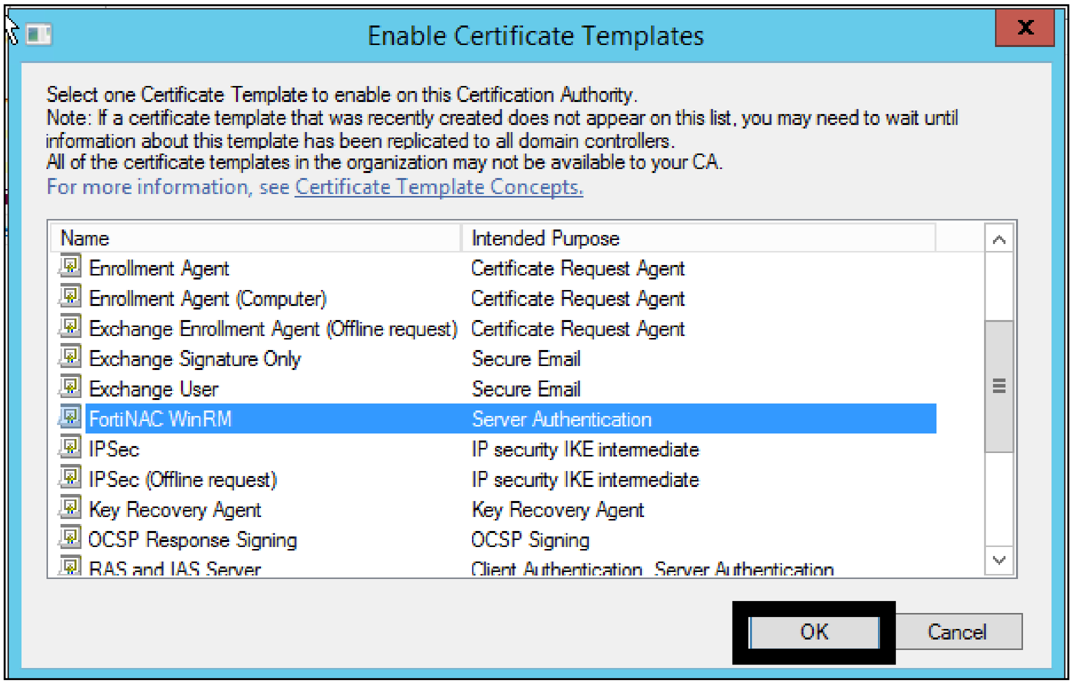


certsrv - [Certification Authority (Local)\DC01\Certificate Templates]

Name	Intended Purpose
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authentic...
Kerberos Authentication	Client Authentication, Server Authentic...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
roller	Client Authentication, Server Authentic...
	tion
	tion, Server Authentic...
	Encrypting File System, Secure Email, Cl...
Certification Autho	<All>
	Microsoft Trust List Signing, Encrypting...

Enable additional Certificate Templates on this Certification Authority

15. Choose the template named as "FortiNAC WinRM" and click on the OK button.



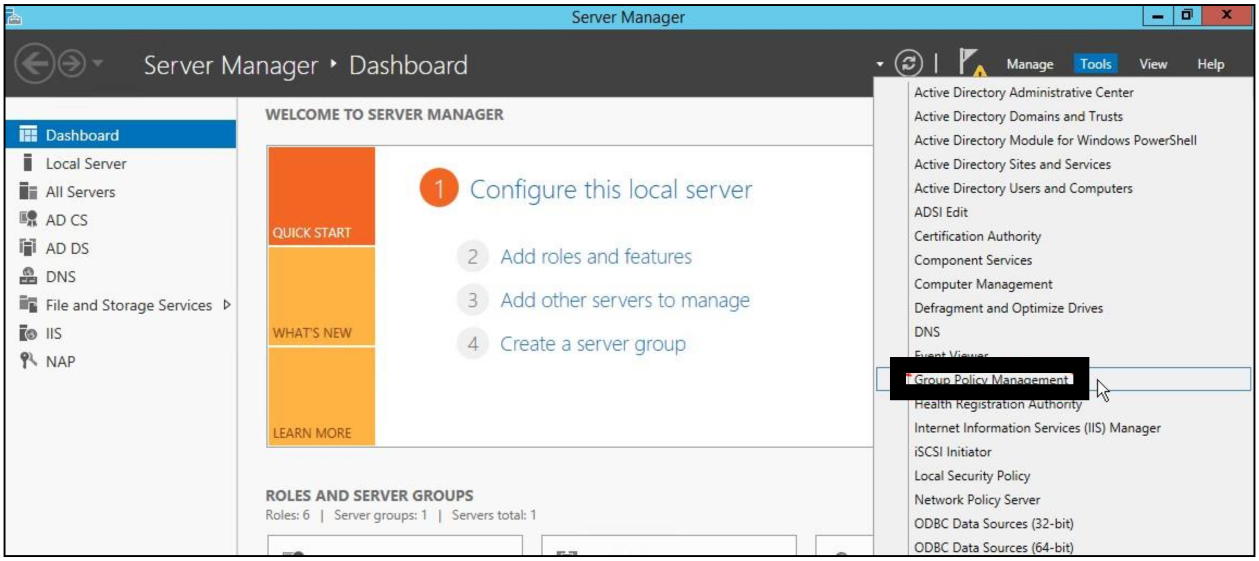
Enable Certificate Templates

Select one Certificate Template to enable on this Certification Authority.
Note: If a certificate template that was recently created does not appear on this list, you may need to wait until information about this template has been replicated to all domain controllers.
All of the certificate templates in the organization may not be available to your CA.
For more information, see Certificate Template Concepts.

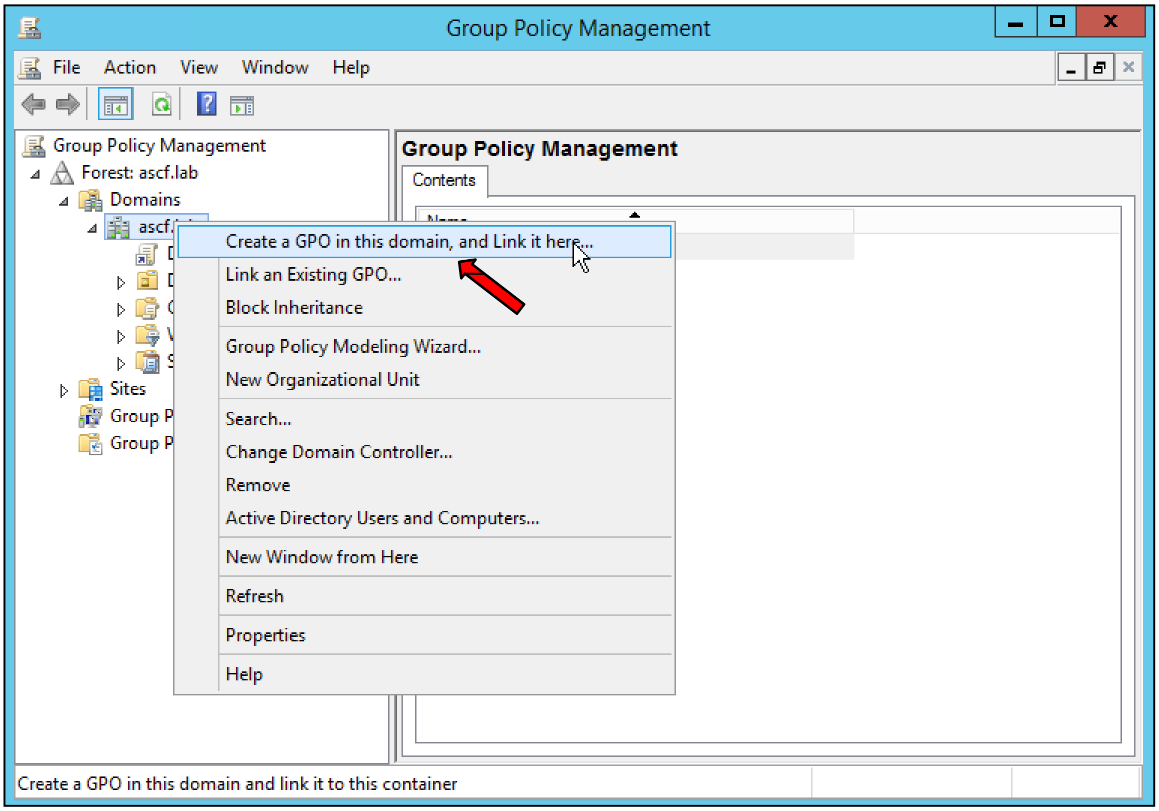
Name	Intended Purpose
Enrollment Agent	Certificate Request Agent
Enrollment Agent (Computer)	Certificate Request Agent
Exchange Enrollment Agent (Offline request)	Certificate Request Agent
Exchange Signature Only	Secure Email
Exchange User	Secure Email
FortiNAC WinRM	Server Authentication
IPSec	IP security IKE intermediate
IPSec (Offline request)	IP security IKE intermediate
Key Recovery Agent	Key Recovery Agent
OCSP Response Signing	OCSP Signing
RAS and IAS Server	Client Authentication, Server Authentication

Create a Group Policy Object (GPO)

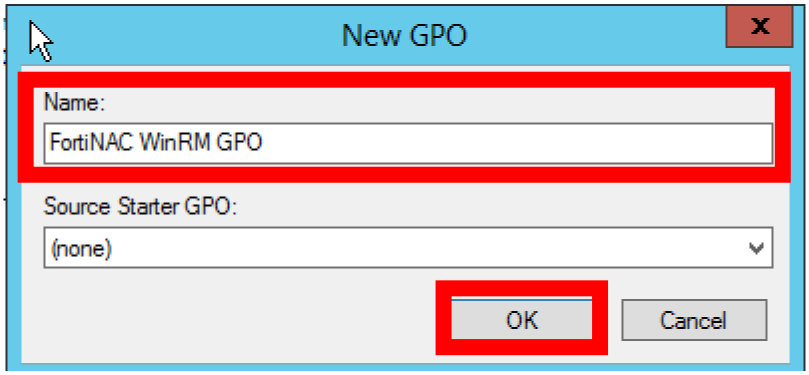
1. To create a GPO in order to configure WinRM, go to Windows Server Manager -> Tools -> Group Policy Management.


Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD CS
AD DS
DNS
File and Storage Services
IIS
NAP
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
ROLES AND SERVER GROUPS
Roles: 6 | Server groups: 1 | Servers total: 1
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Certification Authority
Component Services
Computer Management
Defragment and Optimize Drives
DNS
Event Viewer
Group Policy Management
Health Registration Authority
Internet Information Services (IIS) Manager
iSCSI Initiator
Local Security Policy
Network Policy Server
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)

2. Create a GPO named as "FortiNAC WinRM GPO".
3. Right click on the domain and then choose “Create a GPO in this domain, and Link it here…”



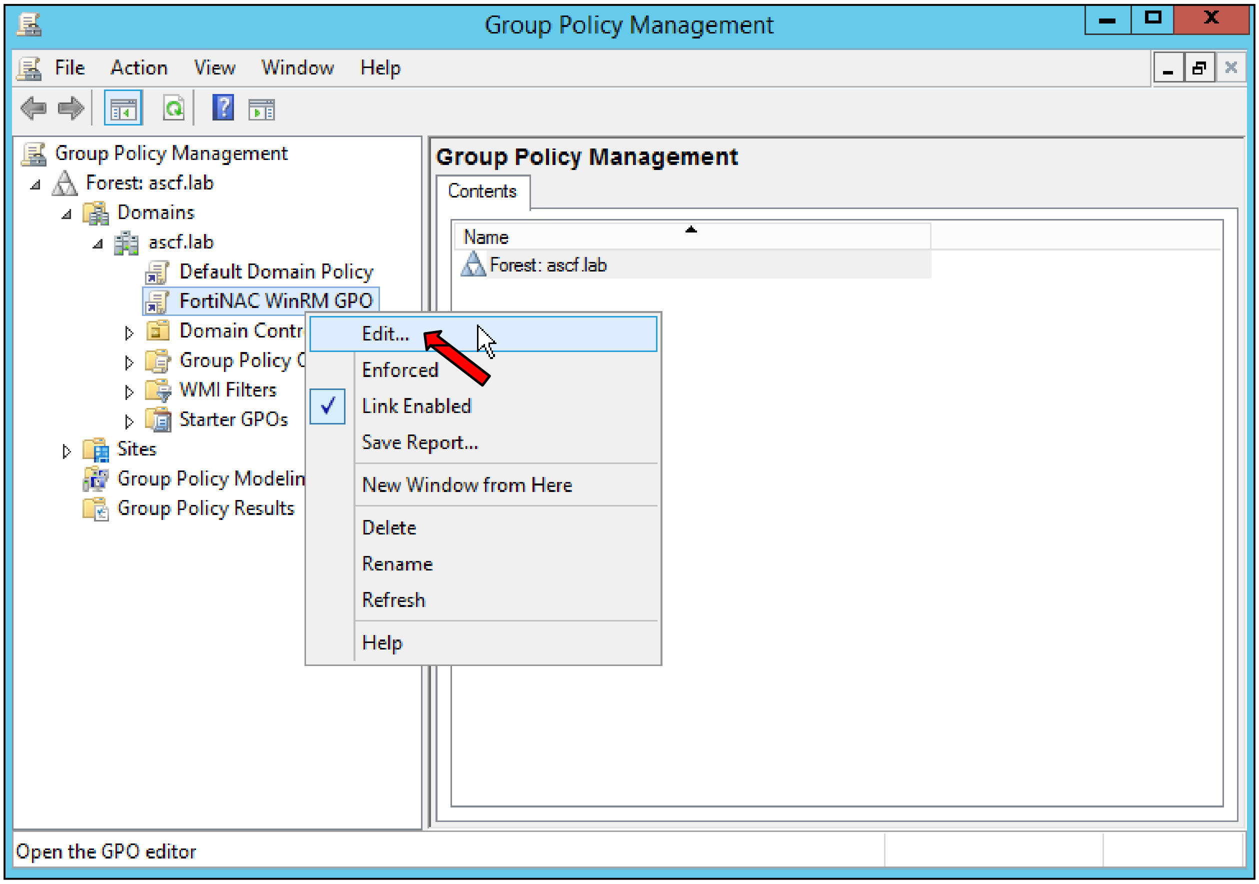
4. Name it as "FortiNAC WinRM GPO". Leave blank the “Source Starter GPO” field.



Name:
FortiNAC WinRM GPO

Source Starter GPO:
(none)

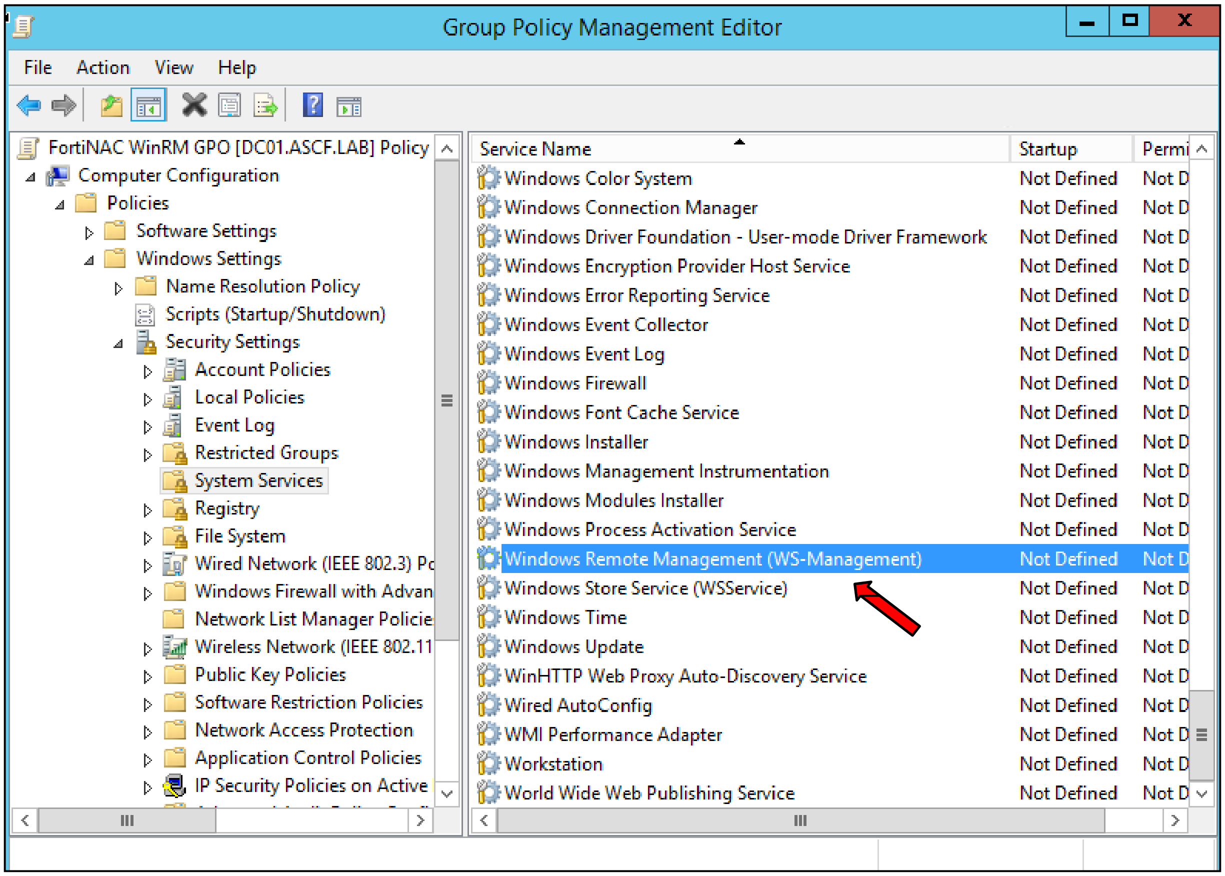
5. Right click on the GPO you just created and choose the action “Edit…”



Open the GPO editor

6. Navigate to Computer Configuration -> Policies -> Windows Settings -> Security Settings -> System Services.

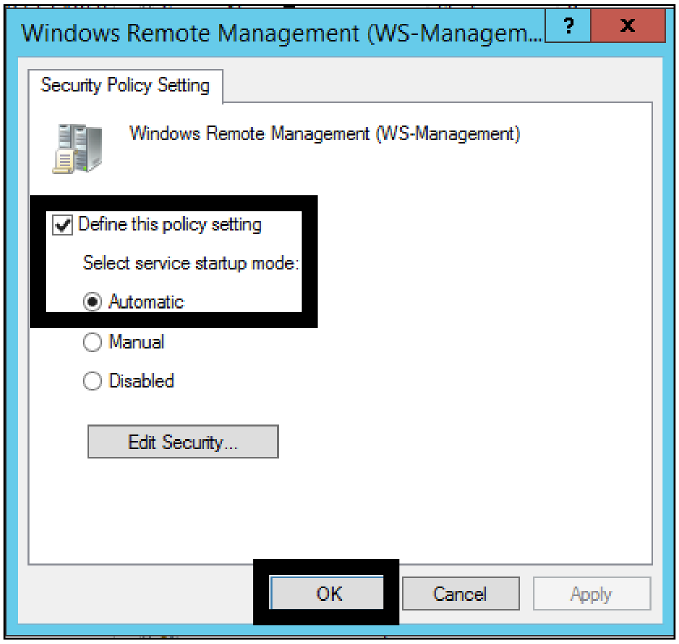
7. Double-click on the Service Name “Windows Remote Management (WS-Management)”.



- FortiNAC WinRM GPO [DC01.ASCF.LAB] Policy
  - Computer Configuration
    - Policies
      - Software Settings
      - Windows Settings
        - Name Resolution Policy
        - Scripts (Startup/Shutdown)
        - Security Settings
          - Account Policies
          - Local Policies
          - Event Log
          - Restricted Groups
          - System Services
          - Registry
          - File System
          - Wired Network (IEEE 802.3) Pc
          - Windows Firewall with Advan
          - Network List Manager Policie
          - Wireless Network (IEEE 802.11
          - Public Key Policies
          - Software Restriction Policies
          - Network Access Protection
          - Application Control Policies
          - IP Security Policies on Active

Service Name	Startup	Permi
Windows Color System	Not Defined	Not D
Windows Connection Manager	Not Defined	Not D
Windows Driver Foundation - User-mode Driver Framework	Not Defined	Not D
Windows Encryption Provider Host Service	Not Defined	Not D
Windows Error Reporting Service	Not Defined	Not D
Windows Event Collector	Not Defined	Not D
Windows Event Log	Not Defined	Not D
Windows Firewall	Not Defined	Not D
Windows Font Cache Service	Not Defined	Not D
Windows Installer	Not Defined	Not D
Windows Management Instrumentation	Not Defined	Not D
Windows Modules Installer	Not Defined	Not D
Windows Process Activation Service	Not Defined	Not D
Windows Remote Management (WS-Management)	Not Defined	Not D
Windows Store Service (WSService)	Not Defined	Not D
Windows Time	Not Defined	Not D
Windows Update	Not Defined	Not D
WinHTTP Web Proxy Auto-Discovery Service	Not Defined	Not D
Wired AutoConfig	Not Defined	Not D
WMI Performance Adapter	Not Defined	Not D
Workstation	Not Defined	Not D
World Wide Web Publishing Service	Not Defined	Not D

8. Tick "Define this policy setting" and select "Automatic". Click Ok.



Windows Remote Management (WS-Management)

☑ Define this policy setting

Select service startup mode:

● Automatic

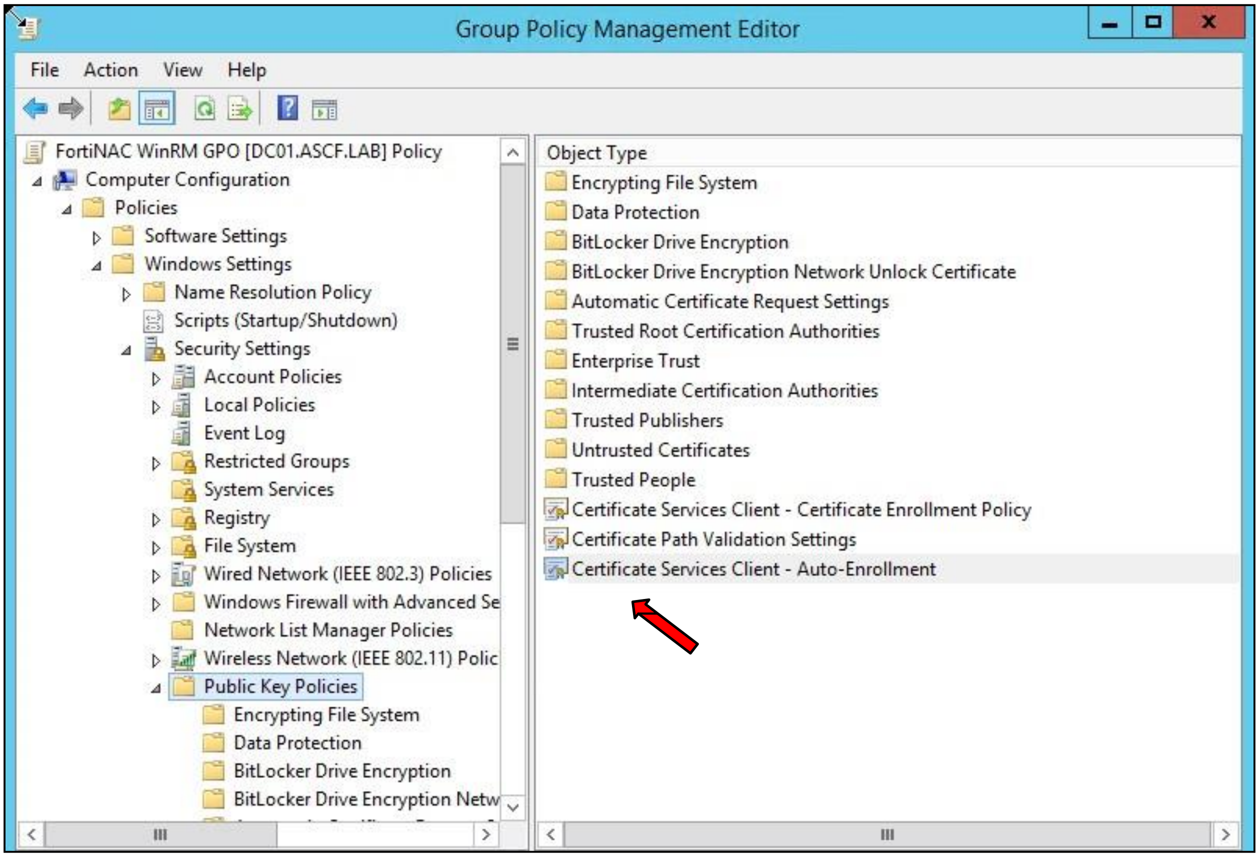
○ Manual

○ Disabled

Configure a Policy to Auto-Enroll Certificates

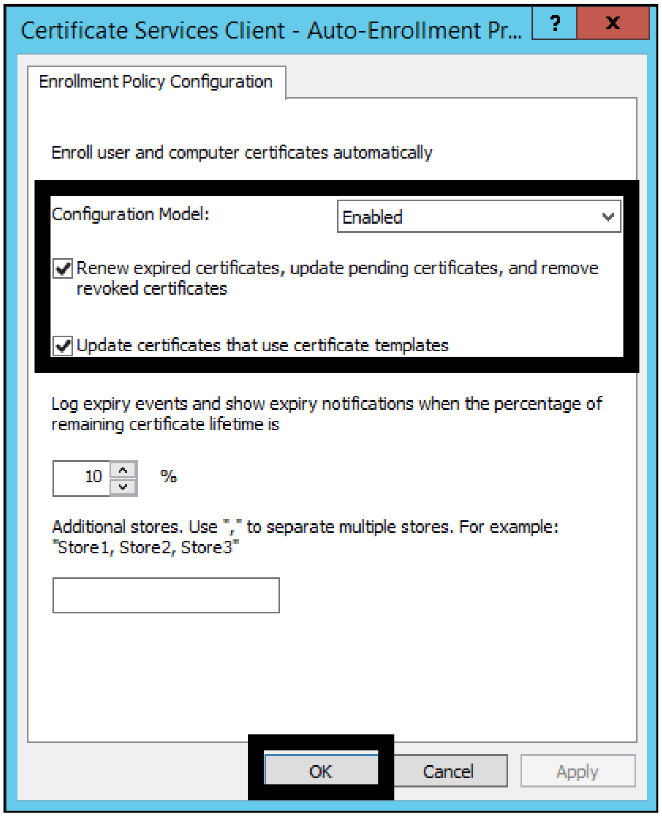
1. Navigate to Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Public Key Policies.

2. Double-click Certificate Services Client - Auto-Enrollment.


Group Policy Management Editor
File
Action
View
Help
FortiNAC WinRM GPO [DC01.ASCF.LAB] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Se
Network List Manager Policies
Wireless Network (IEEE 802.11) Polic
Public Key Policies
Encrypting File System
Data Protection
BitLocker Drive Encryption
BitLocker Drive Encryption Netw
Object Type
Encrypting File System
Data Protection
BitLocker Drive Encryption
BitLocker Drive Encryption Network Unlock Certificate
Automatic Certificate Request Settings
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Trusted People
Certificate Services Client - Certificate Enrollment Policy
Certificate Path Validation Settings
Certificate Services Client - Auto-Enrollment

3. In the Properties dialog box, change Configuration Model to Enabled and select both options:
4. Renew expired certificates, update pending certificates, and remove revoked certificates
5. Update certificates that use certificate templates.

6. Click OK to save your changes. Computers apply the GPO and download the certificate the next time Group Policy is refreshed.



Certificate Services Client - Auto-Enrollment Pr...

Enrollment Policy Configuration

Enroll user and computer certificates automatically

Configuration Model: Enabled

☑ Renew expired certificates, update pending certificates, and remove revoked certificates

☑ Update certificates that use certificate templates

Log expiry events and show expiry notifications when the percentage of remaining certificate lifetime is

10 %

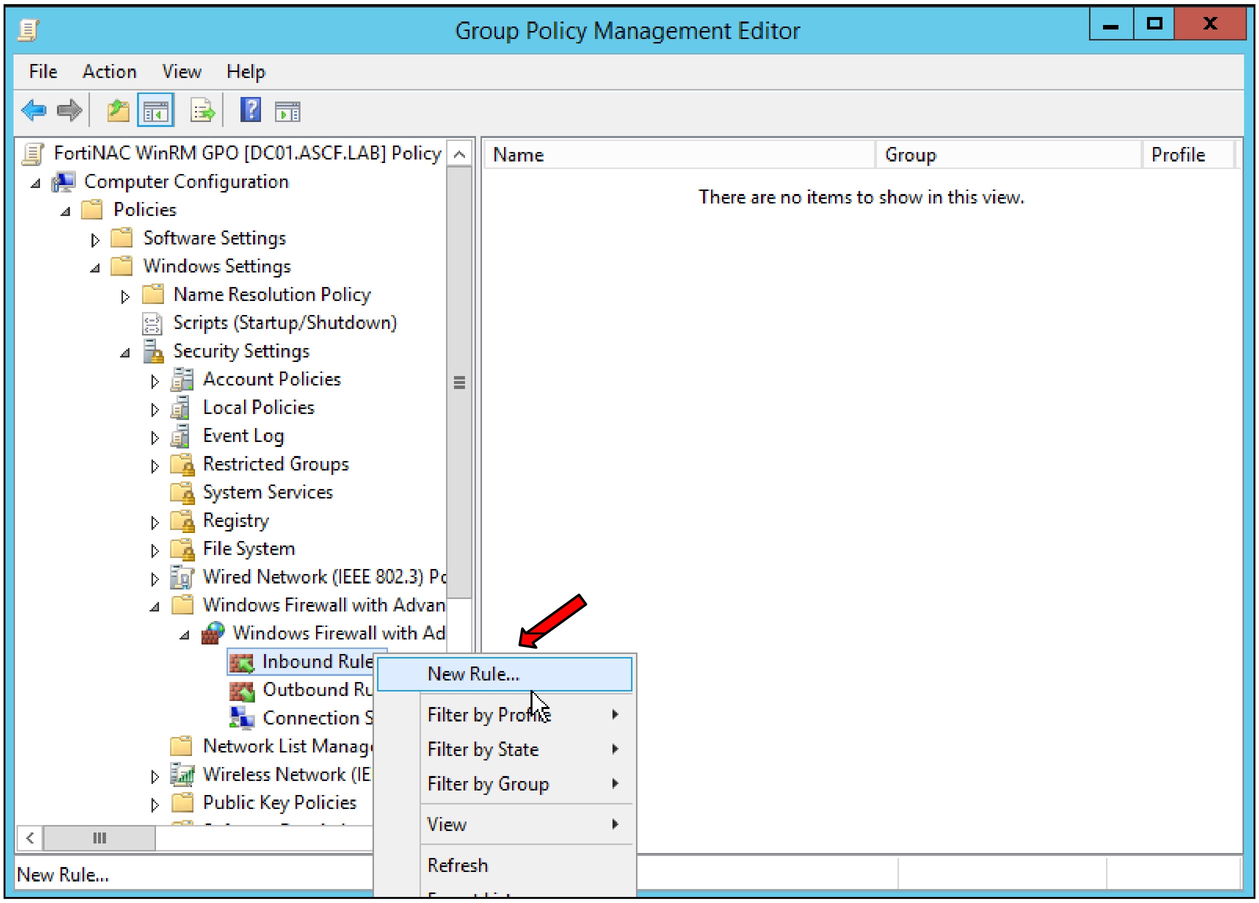
Additional stores. Use "," to separate multiple stores. For example: "Store1, Store2, Store3"

Source: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/configure-group-policy-to-autoenroll-and-deploy-certificates

Configure a Windows Firewall Inbound Rule

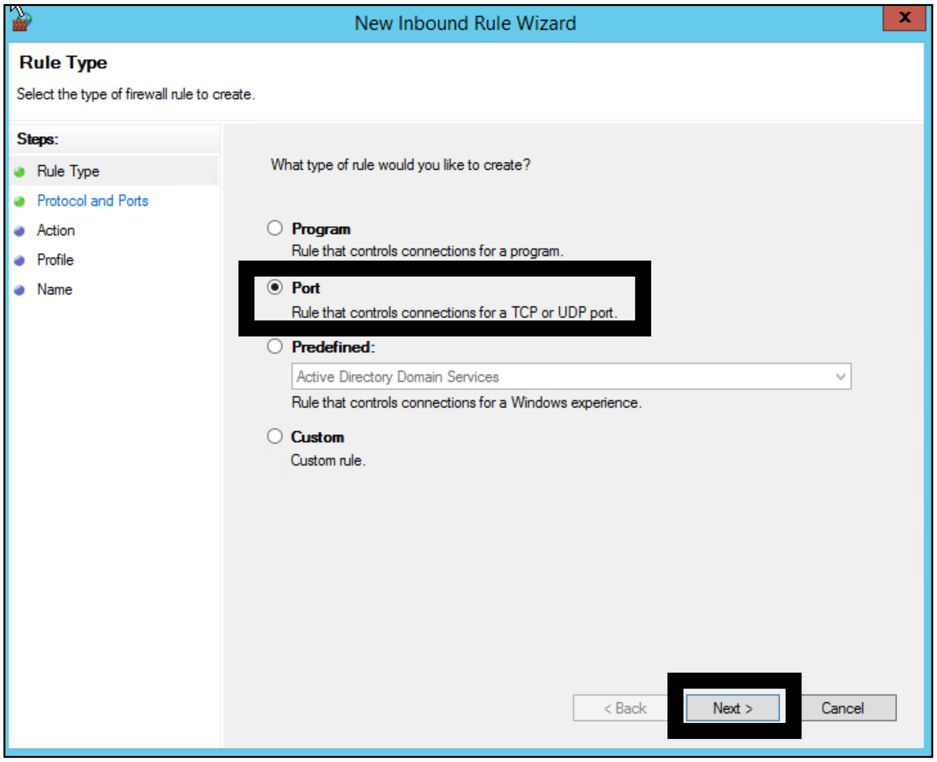
1. Navigate to Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security -> Inbound Rules.

2. Right-click -> New Rule



There are no items to show in this view.

3. Select Port and click Next.



New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What type of rule would you like to create?

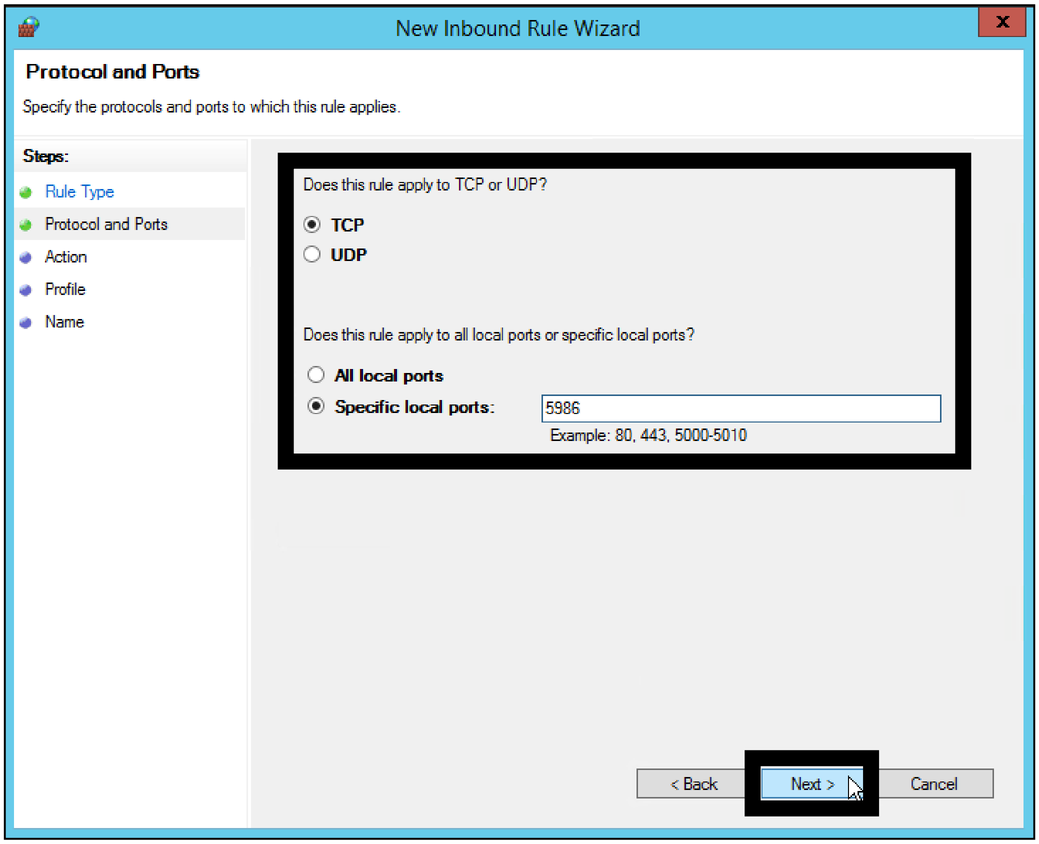
○ **Program**
Rule that controls connections for a program.

● **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
Active Directory Domain Services
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

4. Select TCP and enter "5986" in the "Specific local ports" field. Then click Next.



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

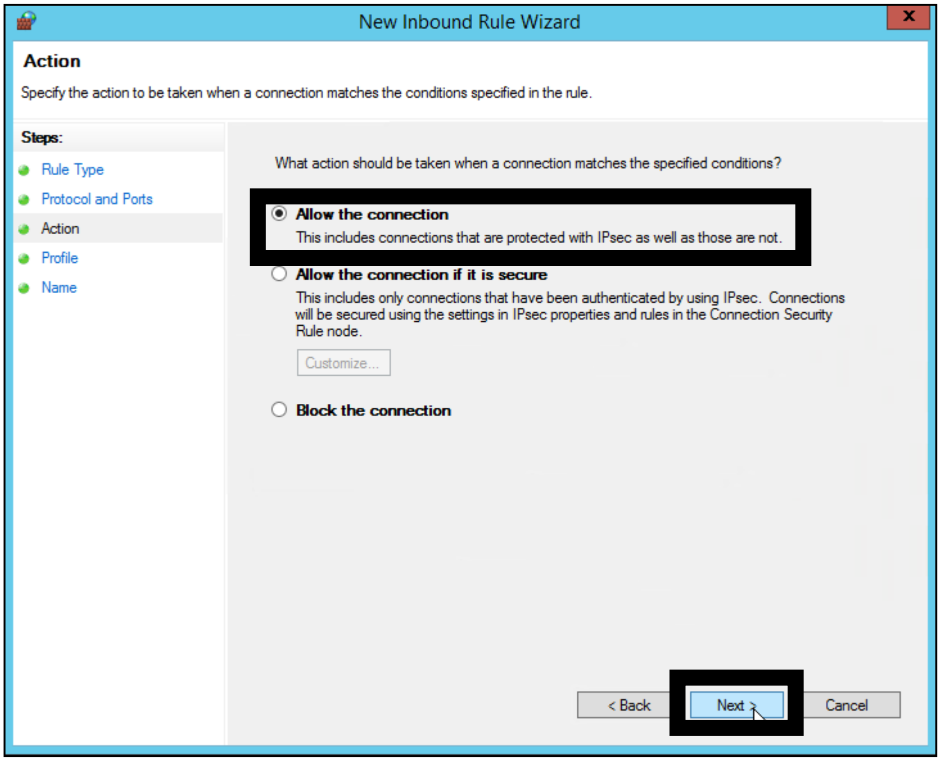
Does this rule apply to TCP or UDP?

● **TCP**
○ **UDP**

Does this rule apply to all local ports or specific local ports?

○ **All local ports**
● **Specific local ports:** 5986
Example: 80, 443, 5000-5010

5. Select “Allow the Connection” and click next.



New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

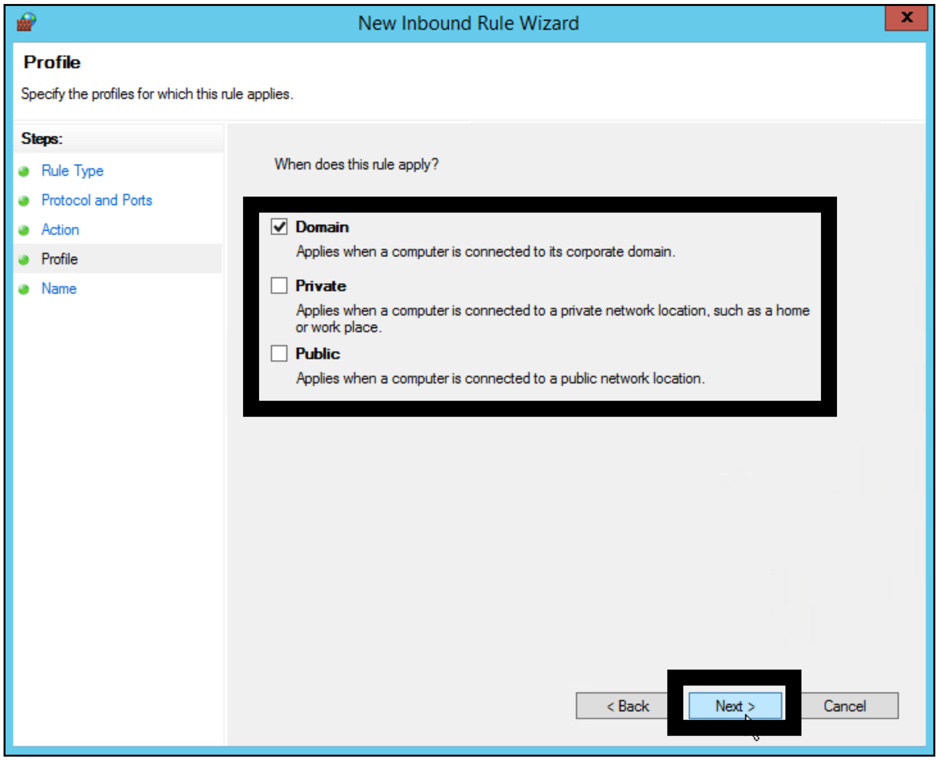
What action should be taken when a connection matches the specified conditions?

● **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

○ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

○ **Block the connection**

6. Remove the selection for Private and Public options, leaving only Domain ticked.



New Inbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

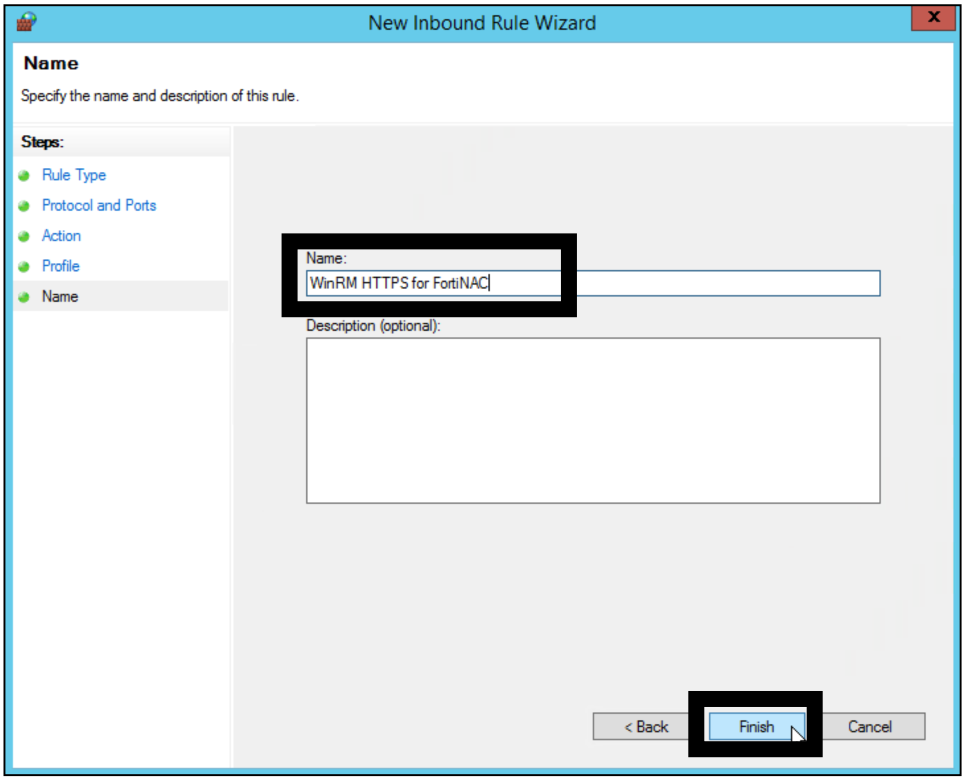
When does this rule apply?

☑ **Domain**
Applies when a computer is connected to its corporate domain.

☐ **Private**
Applies when a computer is connected to a private network location, such as a home or work place.

☐ **Public**
Applies when a computer is connected to a public network location.

7. Name the rule, "WinRM HTTPS for FortiNAC" and click on Finish.



Name

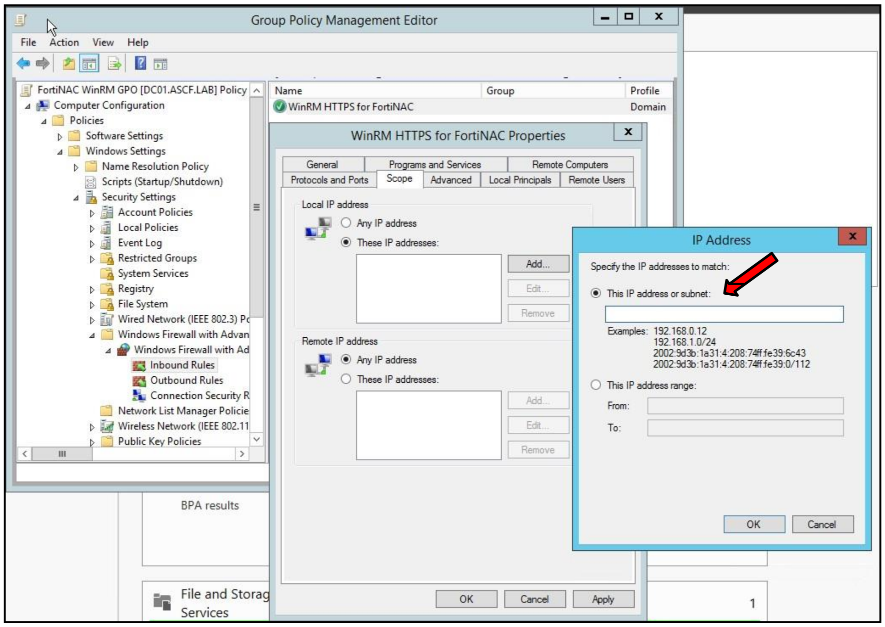
Specify the name and description of this rule.

Name: WinRM HTTPS for FortiNAC

Description (optional):

Optionally, restrict connections only to the FortiNAC IP addresses.

1. Double-click the rule.
2. Click the scope tab
3. Under Remote IP Address, Select "These IP Addresses"
4. Click Add, and enter the addresses for your FortiNAC



Name	Group	Profile
WinRM HTTPS for FortiNAC		Domain

WinRM HTTPS for FortiNAC Properties

Local IP address

○ Any IP address

● These IP addresses:

Remote IP address

● Any IP address

○ These IP addresses:

IP Address

Specify the IP addresses to match:

● This IP address or subnet:

Examples: 192.168.0.12
192.168.1.0/24
2002:9d3b:1a31:4:208:74ff:fe39:6c43
2002:9d3b:1a31:4:208:74ff:fe39:0/112

○ This IP address range:

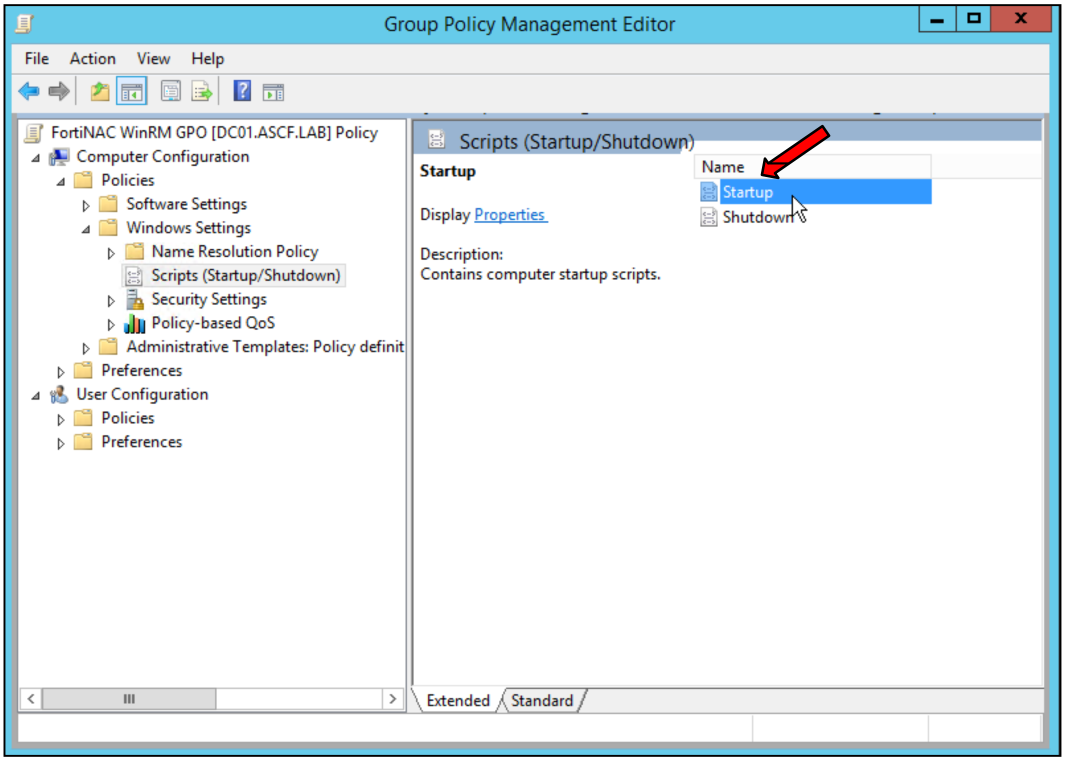
From:

To:

OK Cancel

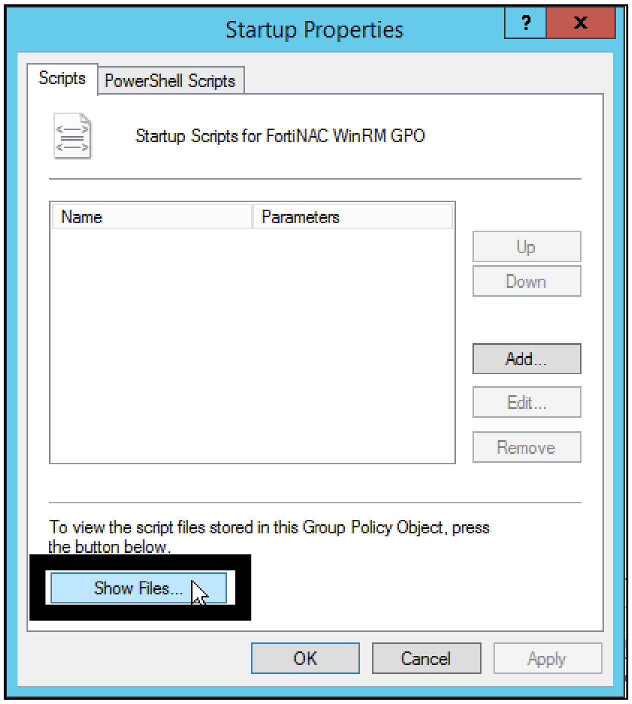
Modifying the Startup Script

1. Navigate to Computer Configuration -> Policies -> Windows Settings -> Scripts (Startup/Shutdown) Double-click on Startup.



Description:
Contains computer startup scripts.

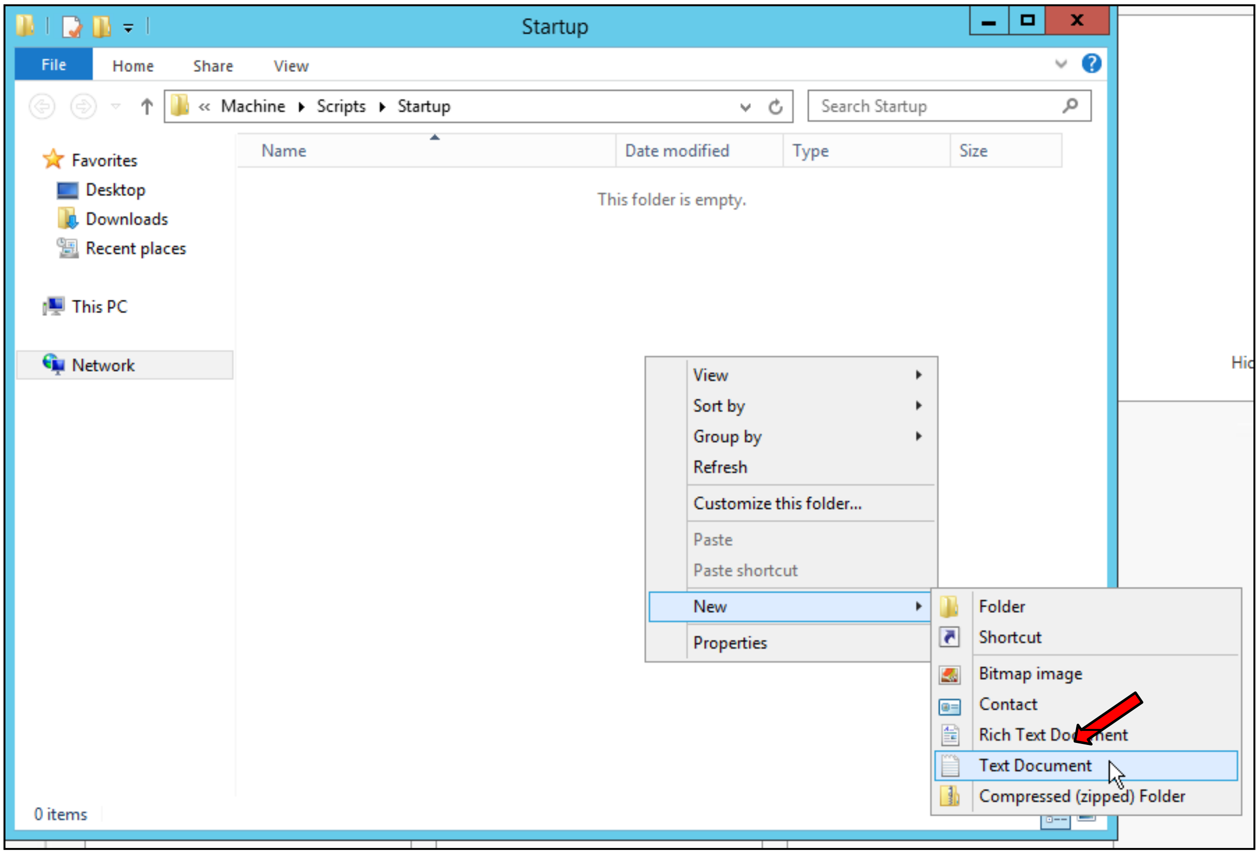
2. Click on “Show Files”



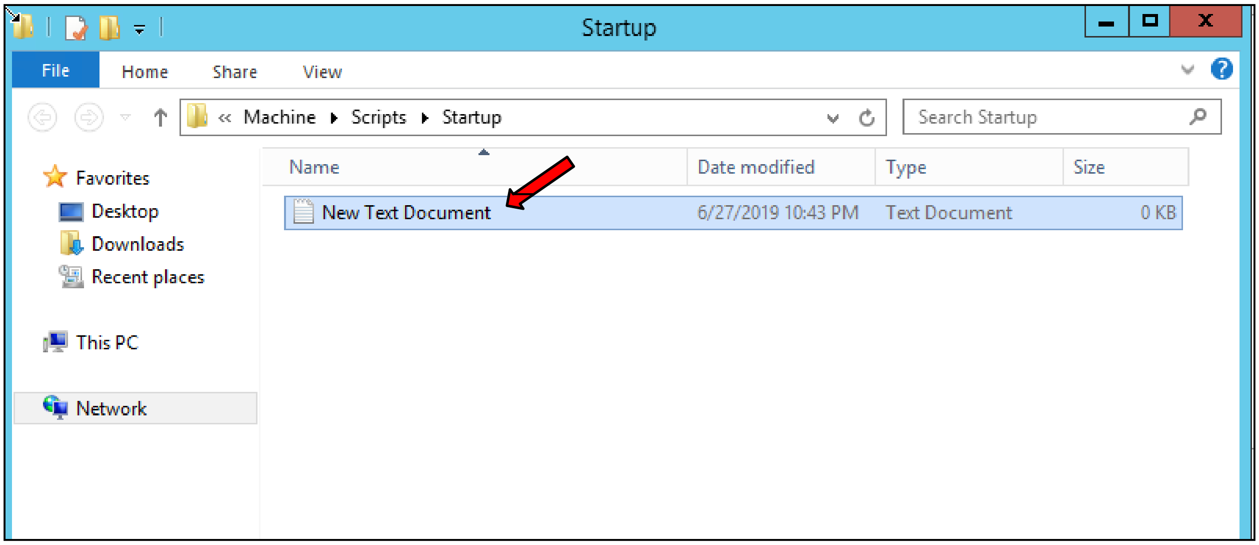
Startup Scripts for FortiNAC WinRM GPO

To view the script files stored in this Group Policy Object, press the button below.

3. Create a new batch file or other script you're comfortable with. Create a txt file first.

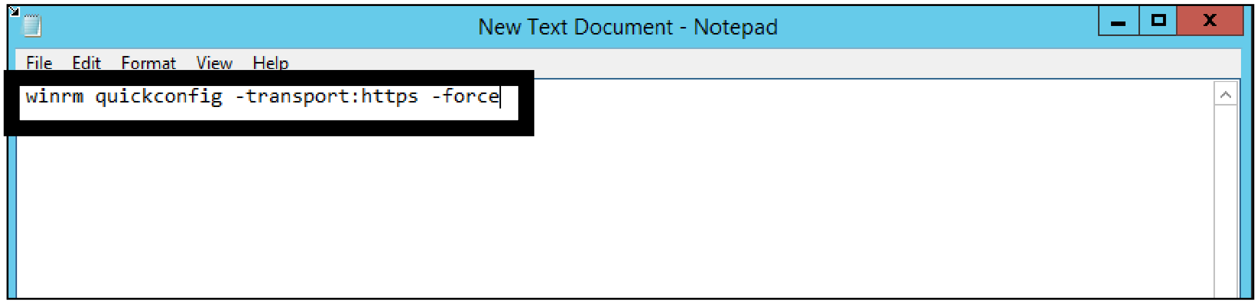


4. Open the file so you can edit it to include the command that will be executed on the startup process.



5. The content of the file should be the following command:

```
winrm quickconfig -transport:https -force
```

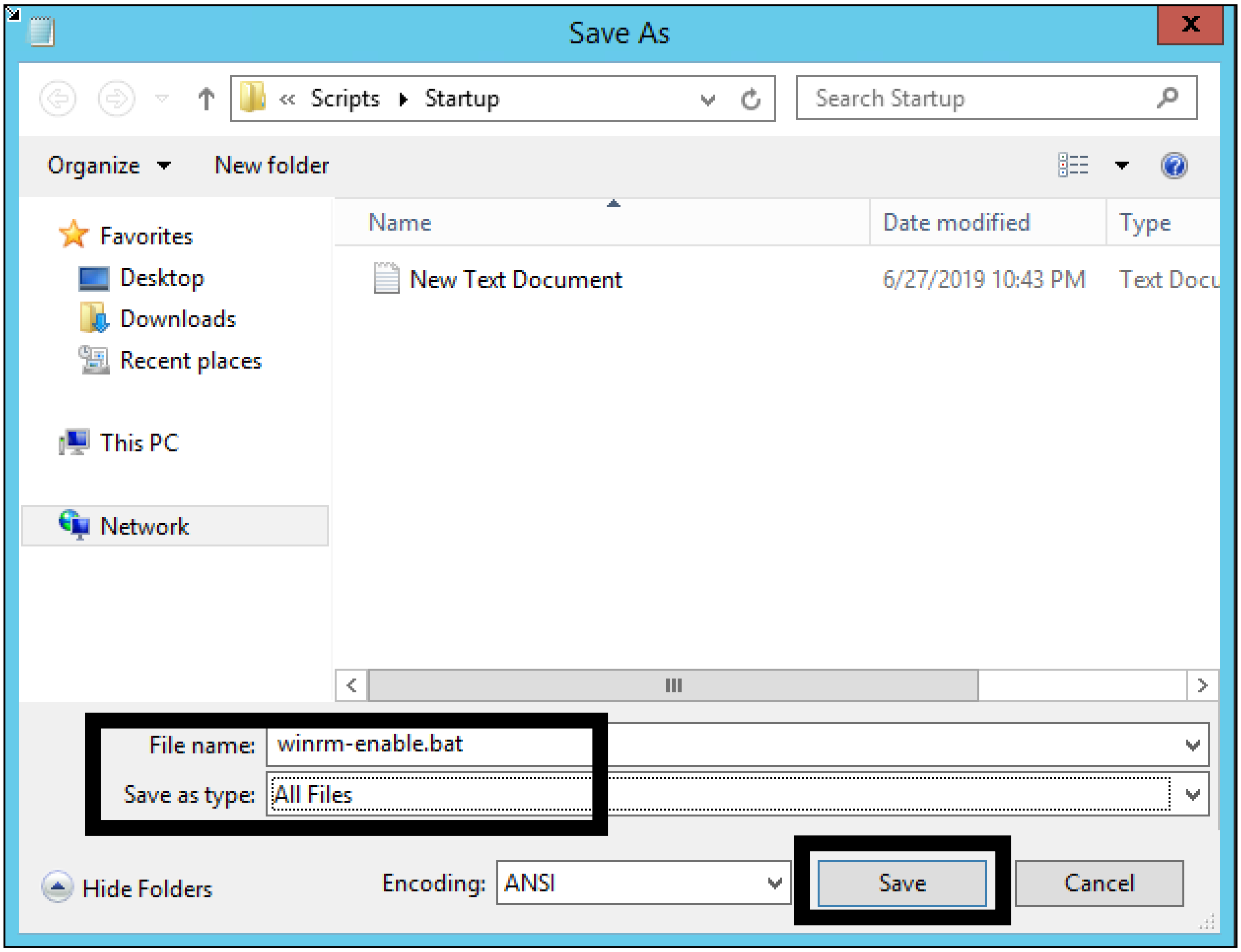


```
winrm quickconfig -transport:https -force
```

6. Select the menu File -> Save As.

File name: winrm-enable.bat

Save as type: ALL FILES



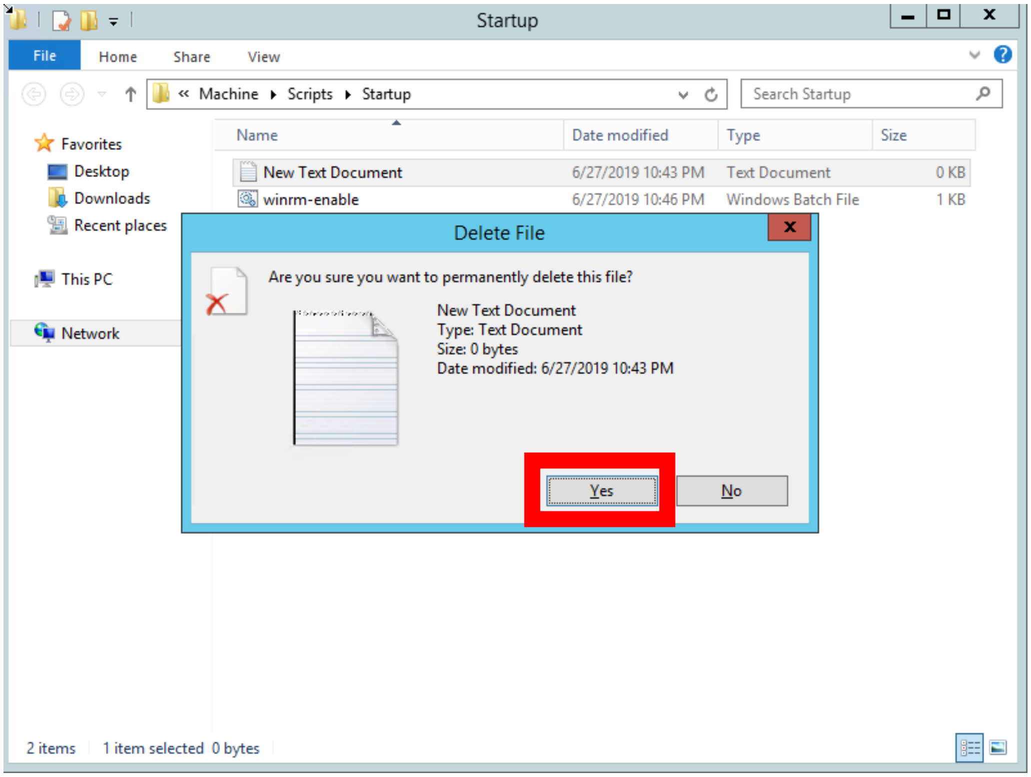
Name	Date modified	Type
New Text Document	6/27/2019 10:43 PM	Text Docu

File name: winrm-enable.bat

Save as type: All Files

Encoding: ANSI

7. Remove the TXT file you've created and make sure you have the BAT file already created.

a. 

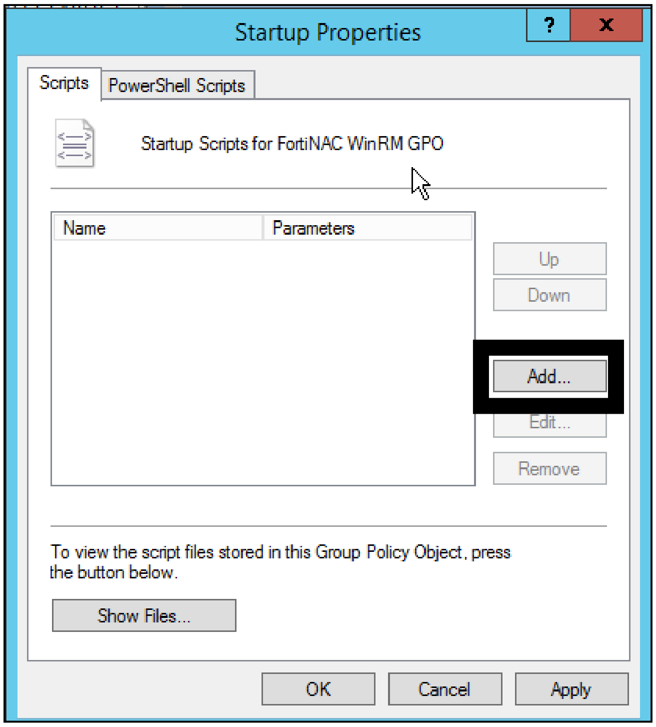
Name	Date modified	Type	Size
New Text Document	6/27/2019 10:43 PM	Text Document	0 KB
winrm-enable	6/27/2019 10:46 PM	Windows Batch File	1 KB

Delete File

Are you sure you want to permanently delete this file?

New Text Document
Type: Text Document
Size: 0 bytes
Date modified: 6/27/2019 10:43 PM

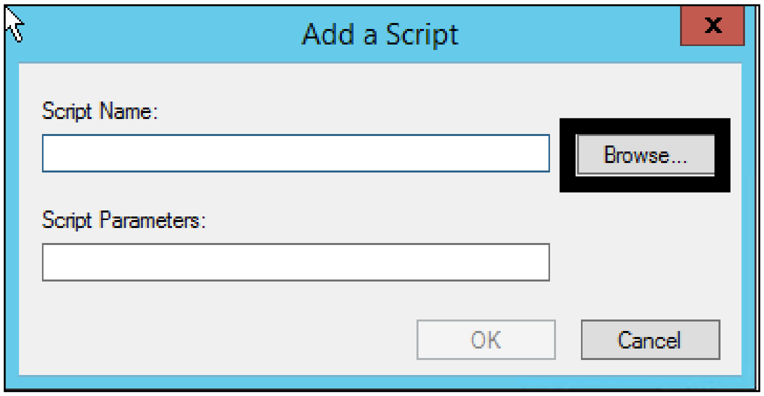
8. On the Startup Properties dialog, click on the Add button.



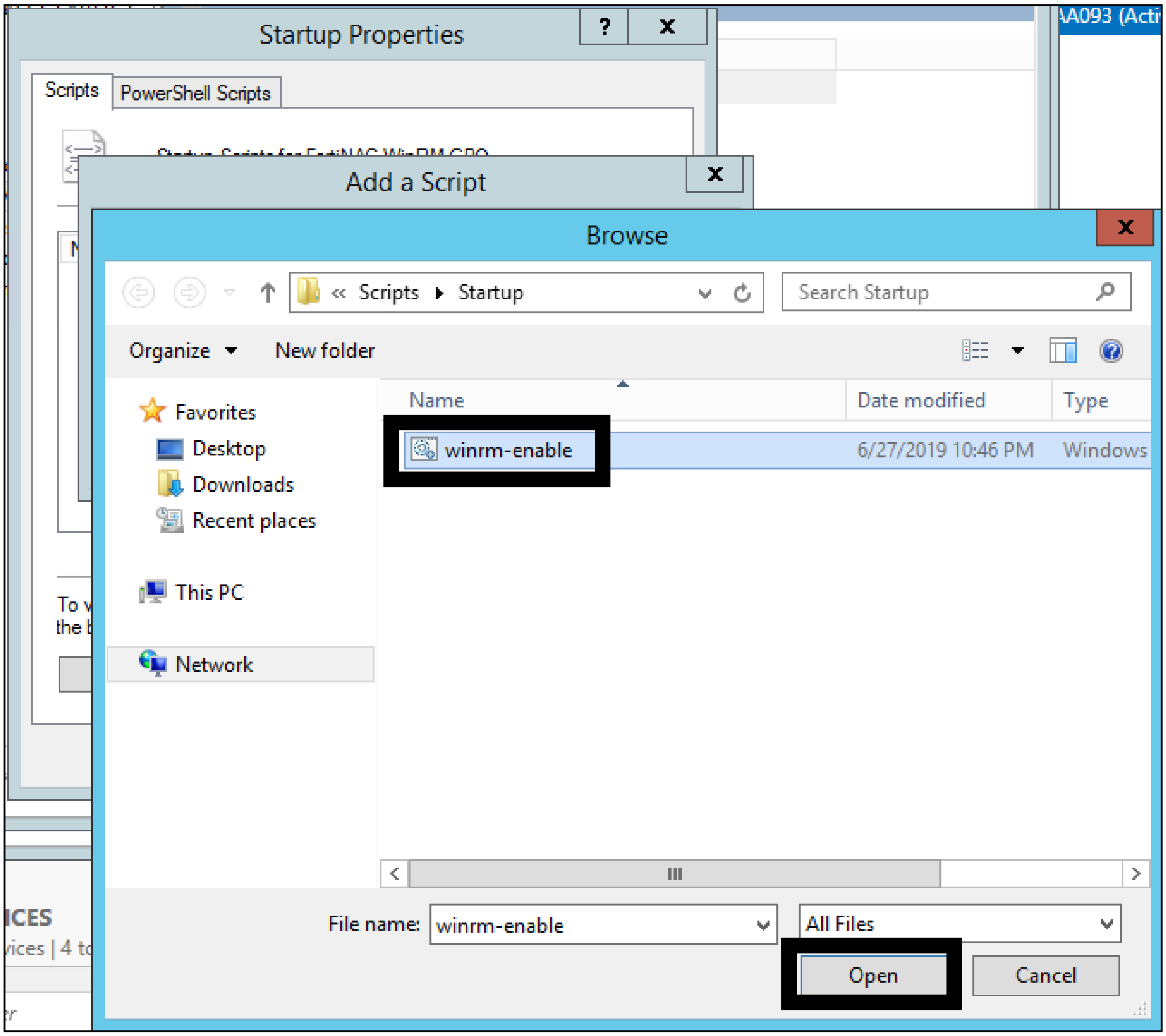
Startup Scripts for FortiNAC WinRM GPO

To view the script files stored in this Group Policy Object, press the button below.

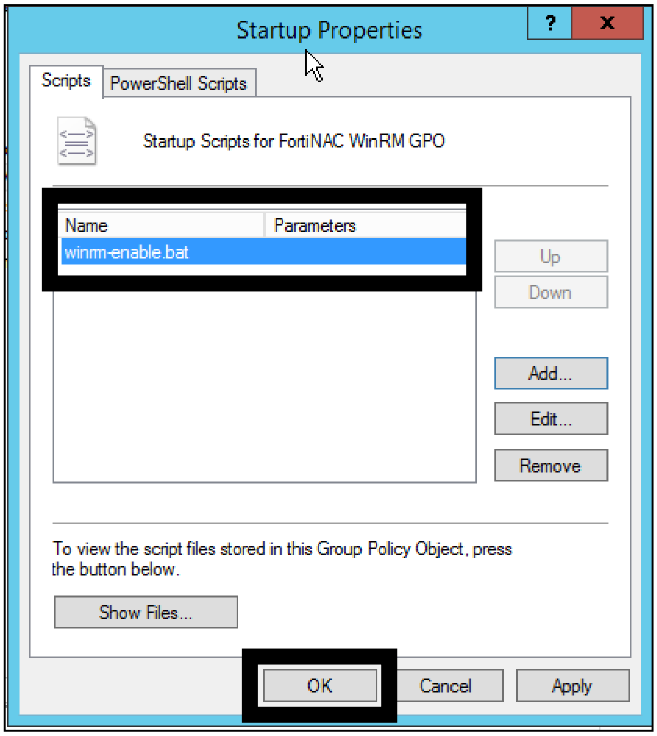
9. Click on Browse.



10. Select the “winrm-enable.bat” file that was created and click on the Open button.



11. Click OK and OK again to dismiss the dialogs.

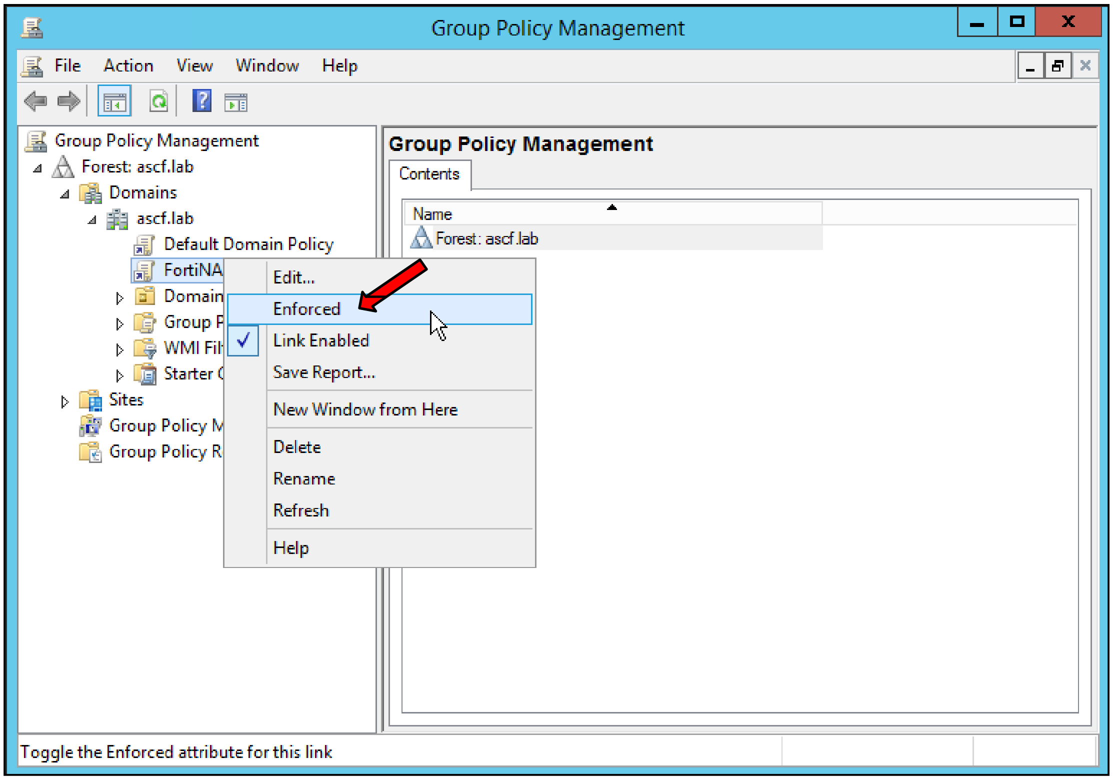


Startup Scripts for FortiNAC WinRM GPO

Name	Parameters
winrm-enable.bat	

To view the script files stored in this Group Policy Object, press the button below.

12. Close the Group Policy Management Editor.
13. Make sure the “FortiNAC WinRM GPO” is linked to your domain and enforce it.



Toggle the Enforced attribute for this link

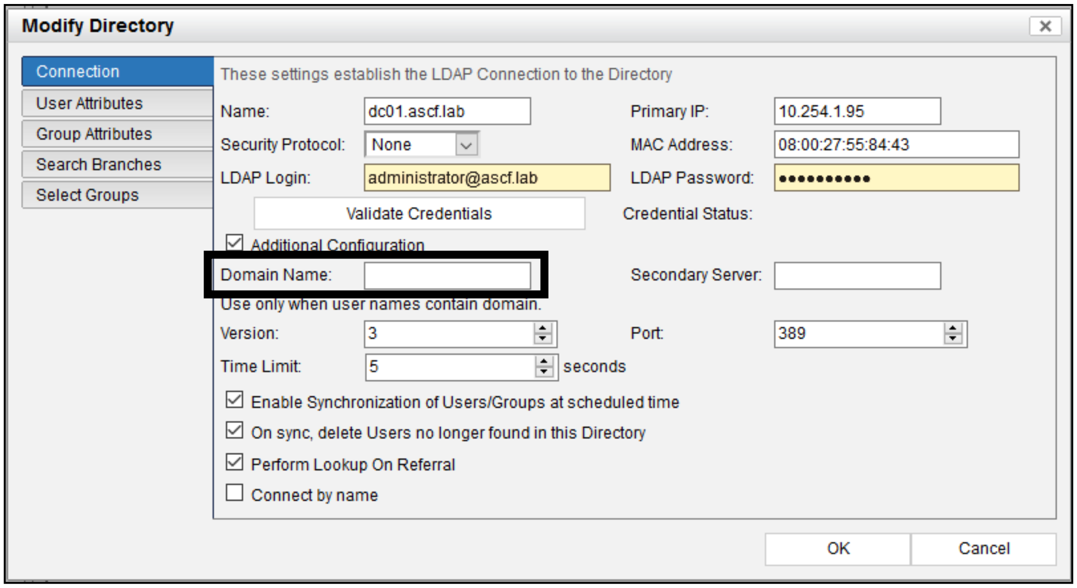
Configure FortiNAC

LDAP Configuration

Ensure there is a directory model created that does not require a domain included in the username.

This procedure is mandatory in order to collect the User information through WMI Profiling. Otherwise, a WMI connection will be established, but the User information won't be shown.

1. In the Administration UI, navigate to **System > Settings > Authentication > LDAP**
2. Double-click on the directory name or right click and select **Modify**.
3. Ensure the LDAP Connection has the "Domain Name" field empty.

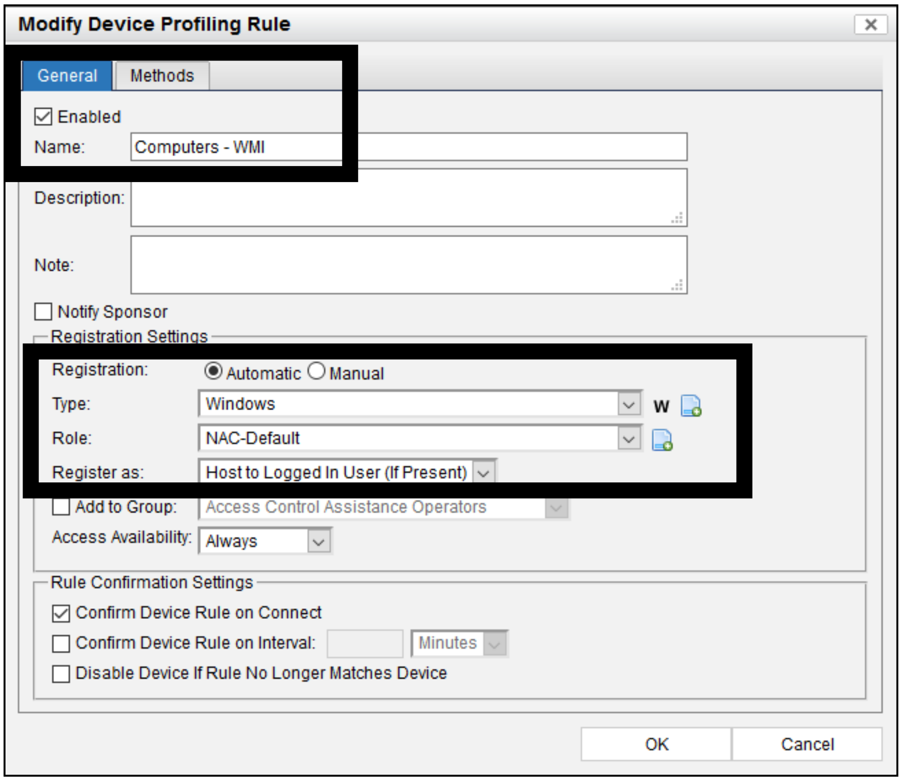


These settings establish the LDAP Connection to the Directory

Name: dc01.ascf.lab
Primary IP: 10.254.1.95
Security Protocol: None
MAC Address: 08:00:27:55:84:43
LDAP Login: administrator@ascf.lab
LDAP Password: ●●●●●●●●●●
Credential Status:
☑ Additional Configuration
Domain Name:
Secondary Server:
Use only when user names contain domain.
Version: 3
Port: 389
Time Limit: 5 seconds
☑ Enable Synchronization of Users/Groups at scheduled time
☑ On sync, delete Users no longer found in this Directory
☑ Perform Lookup On Referral
☐ Connect by name

Create Device Profiling Rule

1. Navigate to **Hosts > Device Profiling Rules**
2. Click **Add** to create new rule
3. Select the **Enabled** box.
4. Name the rule
5. Select the Registration method (Automatic or Manual)
6. On the **Register as** field, select **Host to Logged In User (if Present)**
7. Select Rule Confirmation Settings as desired.


Modify Device Profiling Rule

☑ Enabled

Name: Computers - WMI

Description:

Note:

☐ Notify Sponsor

Registration Settings

Registration: ● Automatic ○ Manual

Type: Windows

Role: NAC-Default

Register as: Host to Logged In User (If Present)

☐ Add to Group: Access Control Assistance Operators

Access Availability: Always

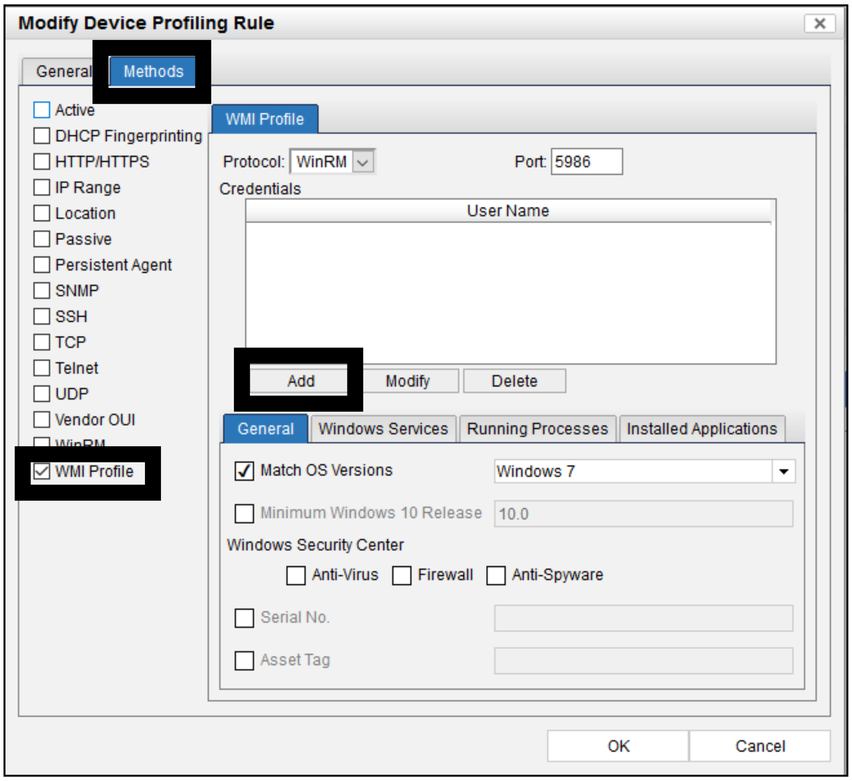
Rule Confirmation Settings

☑ Confirm Device Rule on Connect

☐ Confirm Device Rule on Interval: Minutes

☐ Disable Device If Rule No Longer Matches Device

8. On the **Methods** tab, select **WMI Profile** and click **Add**.


Modify Device Profiling Rule

☐ Active
☐ DHCP Fingerprinting
☐ HTTP/HTTPS
☐ IP Range
☐ Location
☐ Passive
☐ Persistent Agent
☐ SNMP
☐ SSH
☐ TCP
☐ Telnet
☐ UDP
☐ Vendor OUI
☐ WinRM
☑ WMI Profile

WMI Profile

Protocol: WinRM Port: 5986

Credentials

User Name

☑ Match OS Versions Windows 7

☐ Minimum Windows 10 Release 10.0

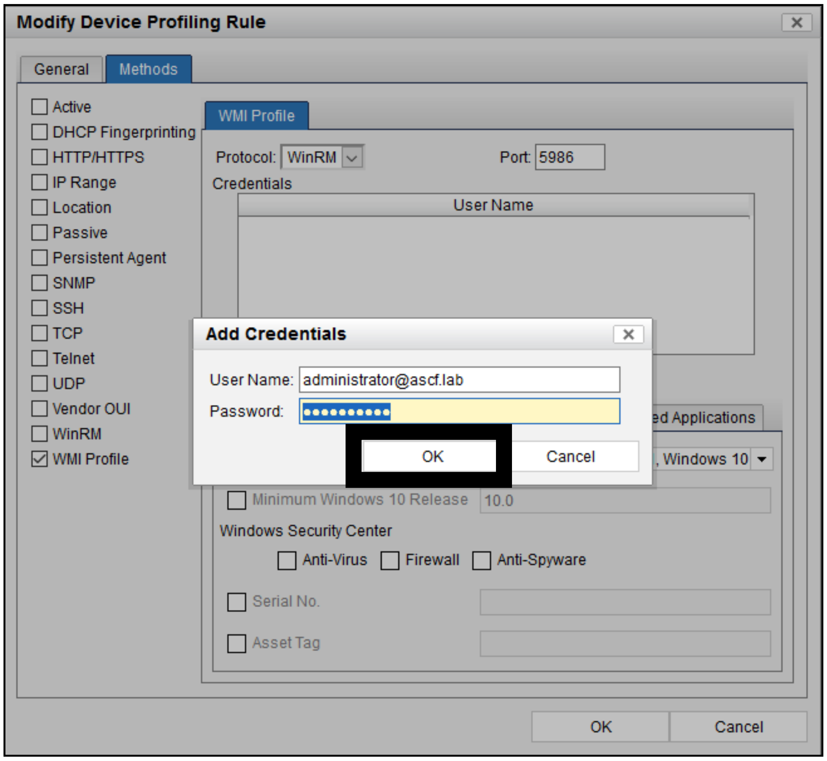
Windows Security Center

☐ Anti-Virus ☐ Firewall ☐ Anti-Spyware

☐ Serial No.

☐ Asset Tag

9. Add the credentials of a user with privileges of Administrator for the domain and click **OK**.



Modify Device Profiling Rule

Add Credentials

User Name: administrator@ascf.lab

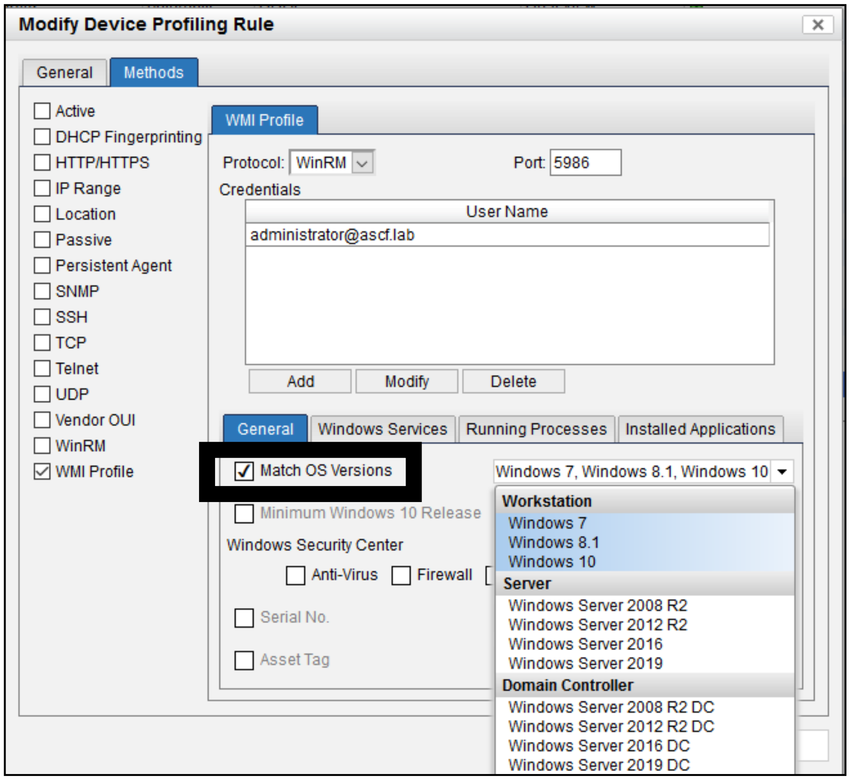
Password: ●●●●●●●●●●

Protocol: WinRM

Port: 5986

☑ WMI Profile

10. On **Match OS versions** select the applicable Windows versions for the environment and click **OK**.



Modify Device Profiling Rule

Protocol: WinRM

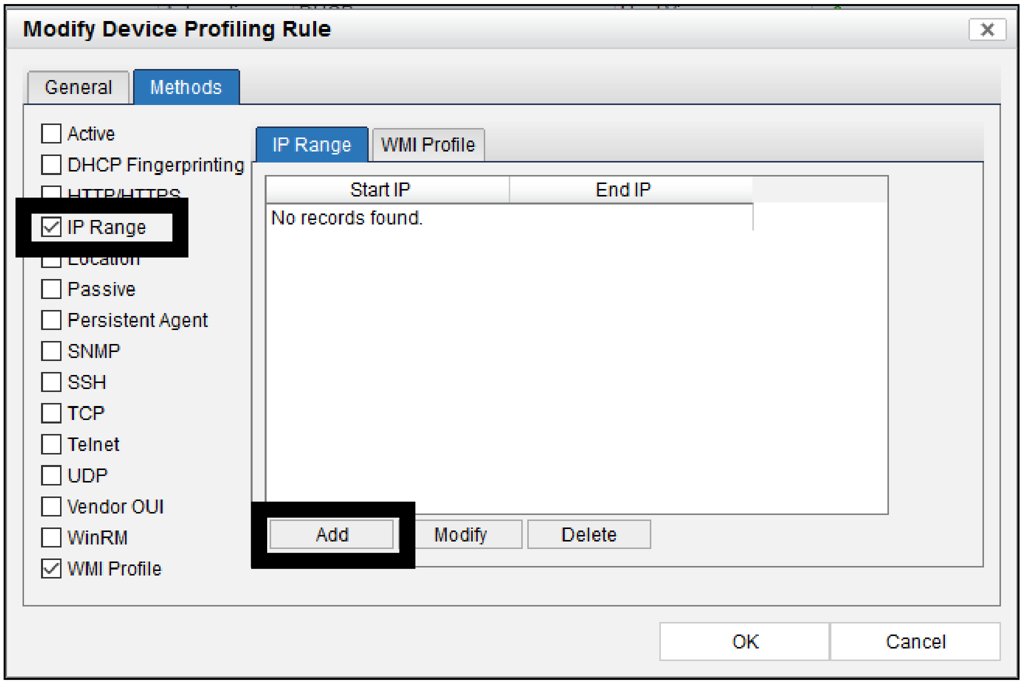
Port: 5986

Credentials: administrator@ascf.lab

☑ WMI Profile

☑ Match OS Versions: Windows 7, Windows 8.1, Windows 10

11. Select **IP Range** to limit the range of addresses scanned by this profile and click on **Add**.



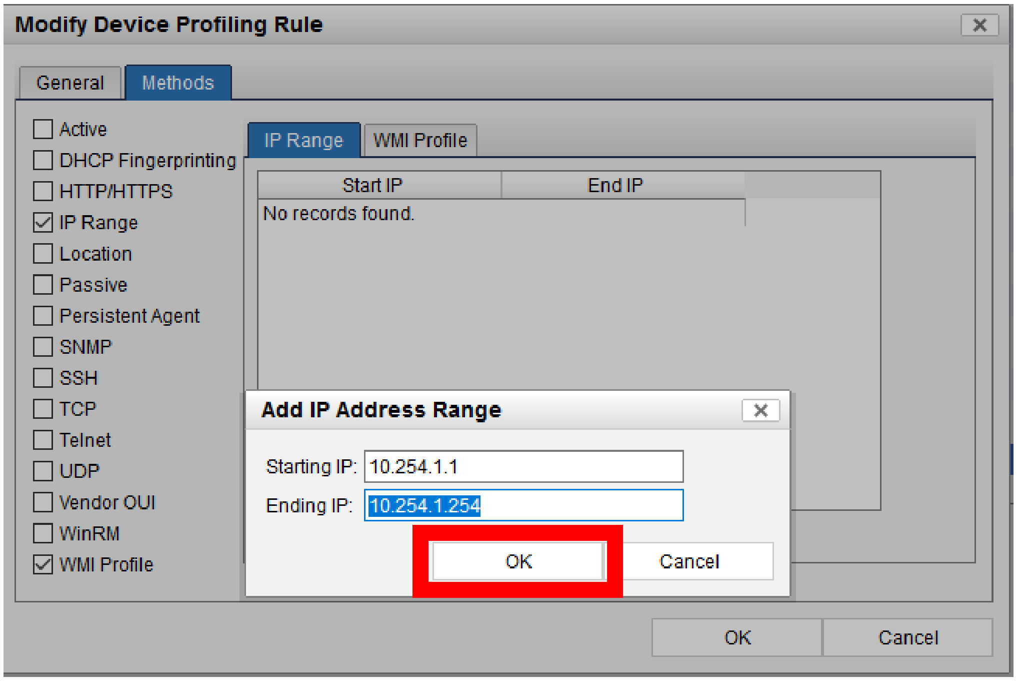
Modify Device Profiling Rule

General | Methods

□ Active
□ DHCP Fingerprinting
□ HTTP/HTTPS
☑ IP Range
□ Location
□ Passive
□ Persistent Agent
□ SNMP
□ SSH
□ TCP
□ Telnet
□ UDP
□ Vendor OUI
□ WinRM
☑ WMI Profile

Start IP	End IP
No records found.	

12. Enter the range of IP addresses to scan and click **OK**.



Modify Device Profiling Rule

General | Methods

□ Active
□ DHCP Fingerprinting
□ HTTP/HTTPS
☑ IP Range
□ Location
□ Passive
□ Persistent Agent
□ SNMP
□ SSH
□ TCP
□ Telnet
□ UDP
□ Vendor OUI
□ WinRM
☑ WMI Profile

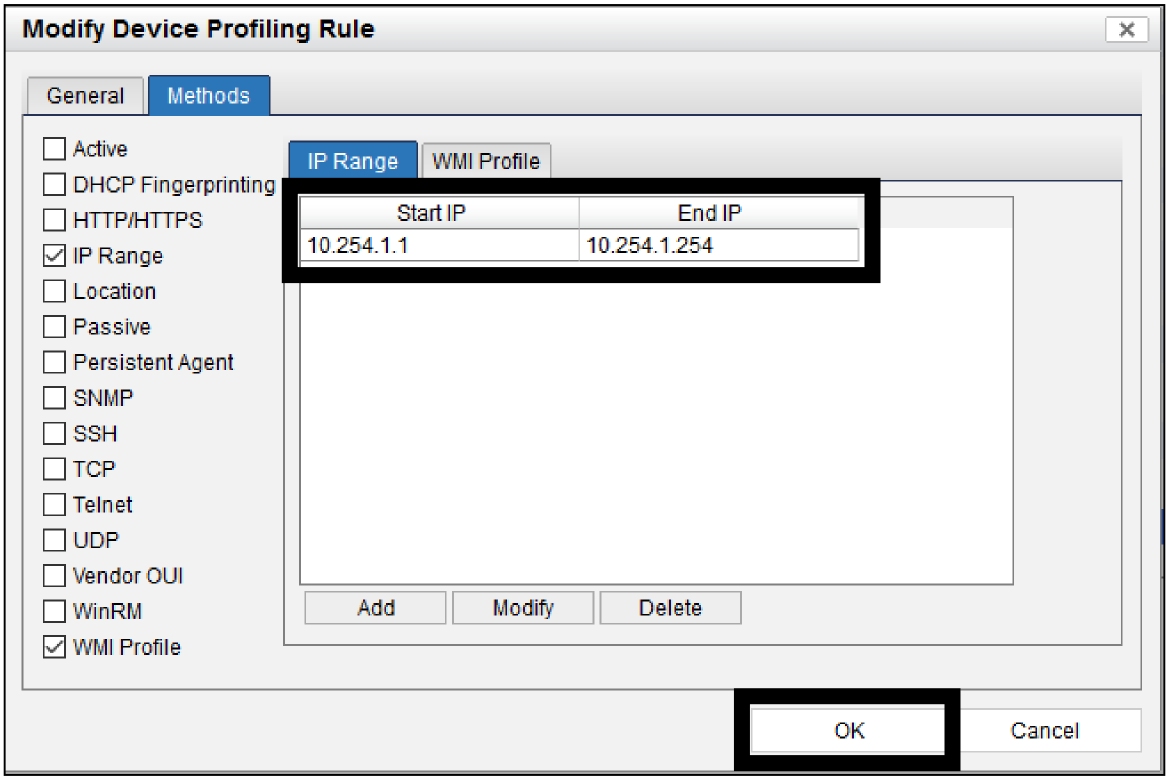
Start IP	End IP
No records found.	

Add IP Address Range

Starting IP: 10.254.1.1

Ending IP: 10.254.1.254

13. Review settings entered and click **OK** to save the rule.

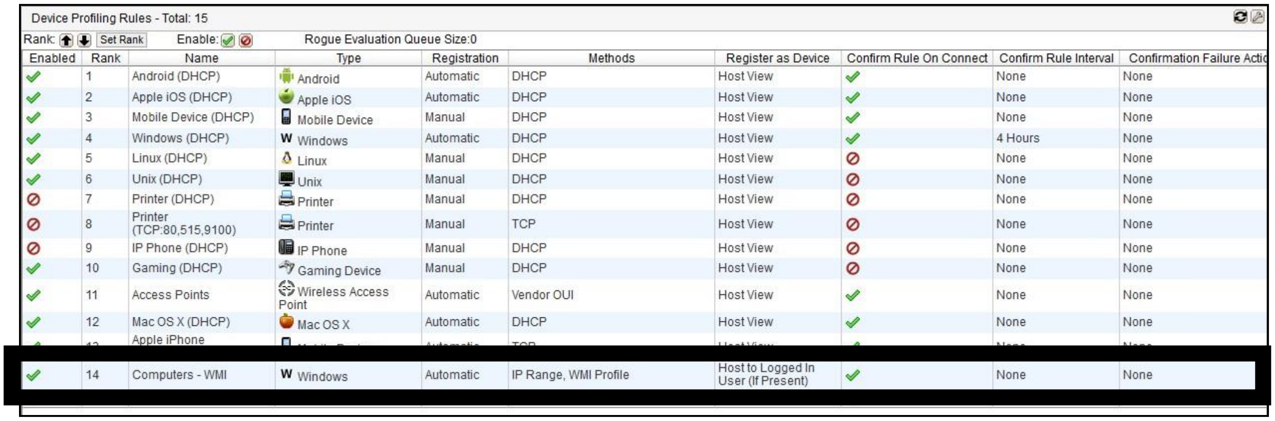


Modify Device Profiling Rule

☐ Active
☐ DHCP Fingerprinting
☐ HTTP/HTTPS
☑ IP Range
☐ Location
☐ Passive
☐ Persistent Agent
☐ SNMP
☐ SSH
☐ TCP
☐ Telnet
☐ UDP
☐ Vendor OUI
☐ WinRM
☑ WMI Profile

Start IP	End IP
10.254.1.1	10.254.1.254

14. The new Device Profiling Rule will be ranked last.



Device Profiling Rules - Total: 15

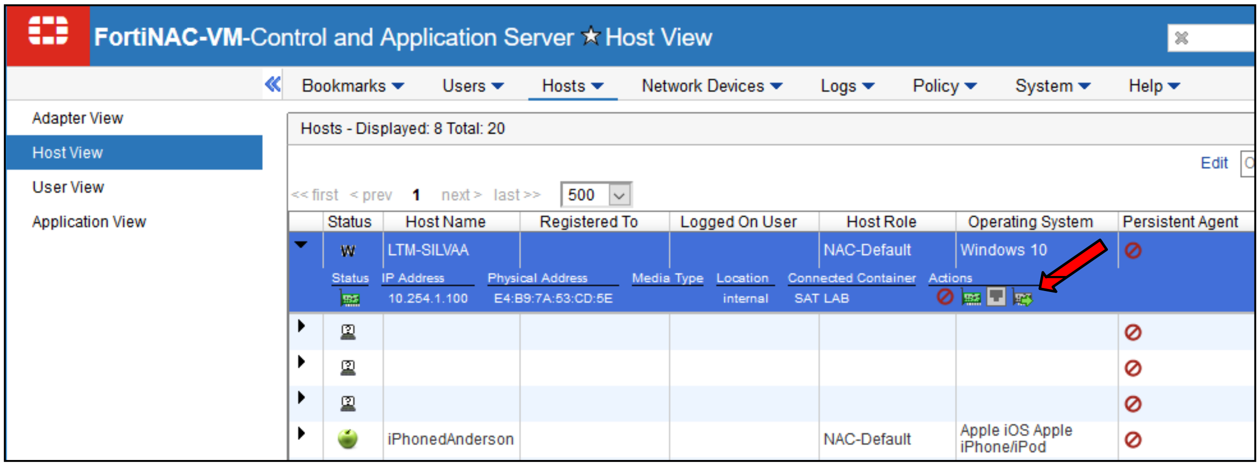
Rogue Evaluation Queue Size:0

Enabled	Rank	Name	Type	Registration	Methods	Register as Device	Confirm Rule On Connect	Confirm Rule Interval	Confirmation Failure Actic
✓	1	Android (DHCP)	Android	Automatic	DHCP	Host View	✓	None	None
✓	2	Apple iOS (DHCP)	Apple iOS	Automatic	DHCP	Host View	✓	None	None
✓	3	Mobile Device (DHCP)	Mobile Device	Manual	DHCP	Host View	✓	None	None
✓	4	Windows (DHCP)	Windows	Automatic	DHCP	Host View	✓	4 Hours	None
✓	5	Linux (DHCP)	Linux	Manual	DHCP	Host View	⊘	None	None
✓	6	Unix (DHCP)	Unix	Manual	DHCP	Host View	⊘	None	None
⊘	7	Printer (DHCP)	Printer	Manual	DHCP	Host View	⊘	None	None
⊘	8	Printer (TCP:80,515,9100)	Printer	Manual	TCP	Host View	⊘	None	None
⊘	9	IP Phone (DHCP)	IP Phone	Manual	DHCP	Host View	⊘	None	None
✓	10	Gaming (DHCP)	Gaming Device	Manual	DHCP	Host View	⊘	None	None
✓	11	Access Points	Wireless Access Point	Automatic	Vendor OUI	Host View	✓	None	None
✓	12	Mac OS X (DHCP)	Mac OS X	Automatic	DHCP	Host View	✓	None	None
✓	13	Apple iPhone	Mobile Device	Automatic	TCP	Host View	✓	None	None
✓	14	Computers - WMI	Windows	Automatic	IP Range, WMI Profile	Host to Logged In User (If Present)	✓	None	None

Validate New Rule

1. Navigate **Hosts > Hosts View**

2. Select a Windows machine and click on the adapter icon.

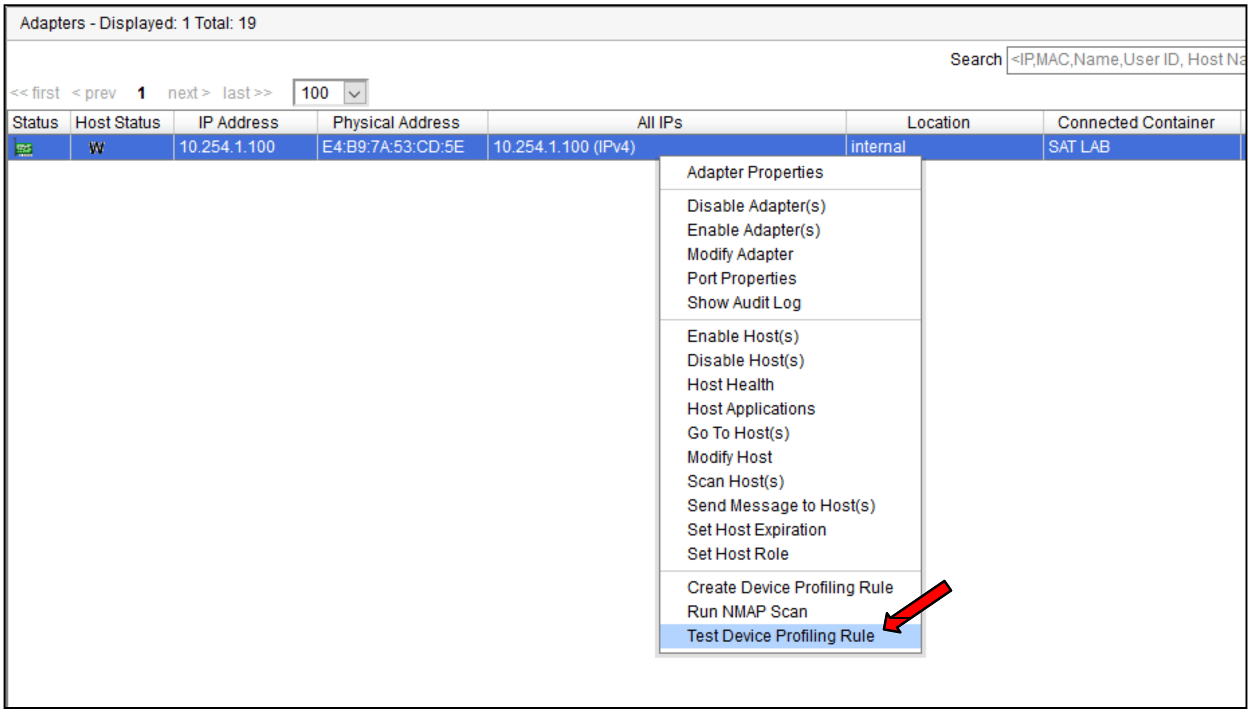


Hosts - Displayed: 8 Total: 20

	Status	Host Name	Registered To	Logged On User	Host Role	Operating System	Persistent Agent
▼	W	LTM-SILVAA			NAC-Default	Windows 10	⊘
▶							⊘
▶							⊘
▶							⊘
▶		iPhonedAnderson			NAC-Default	Apple iOS Apple iPhone/iPod	⊘

Status	IP Address	Physical Address	Media Type	Location	Connected Container	Actions
	10.254.1.100	E4:B9:7A:53:CD:5E		internal	SAT LAB	⊘

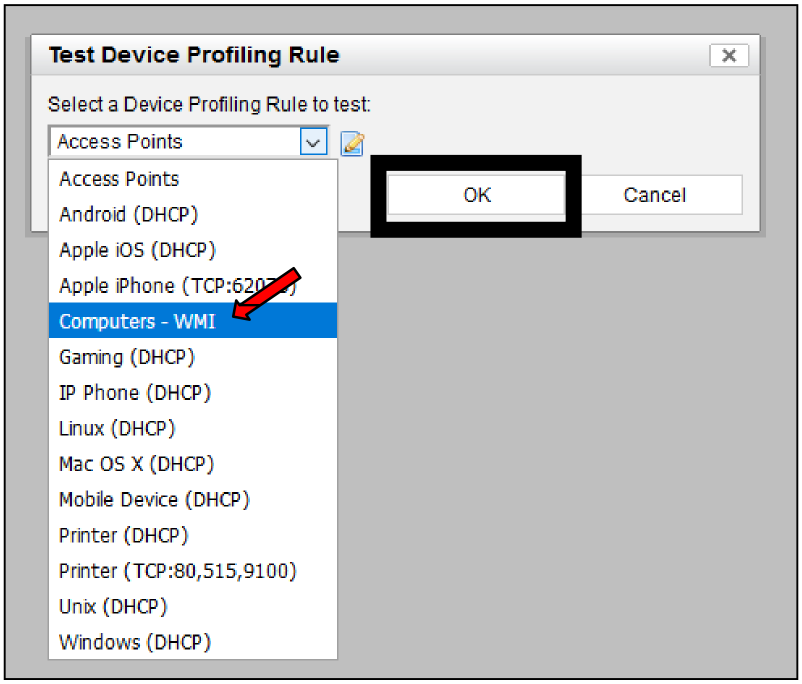
3. Right click and select **Test Device Profiling Rule**.



Adapters - Displayed: 1 Total: 19

Status	Host Status	IP Address	Physical Address	All IPs	Location	Connected Container
	W	10.254.1.100	E4:B9:7A:53:CD:5E	10.254.1.100 (IPv4)	internal	SAT LAB

4. Select the rule just created:



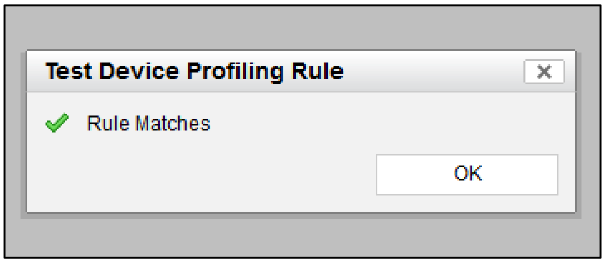
Test Device Profiling Rule

Select a Device Profiling Rule to test:

Access Points

- Access Points
- Android (DHCP)
- Apple iOS (DHCP)
- Apple iPhone (TCP:62078)
- Computers - WMI
- Gaming (DHCP)
- IP Phone (DHCP)
- Linux (DHCP)
- Mac OS X (DHCP)
- Mobile Device (DHCP)
- Printer (DHCP)
- Printer (TCP:80,515,9100)
- Unix (DHCP)
- Windows (DHCP)

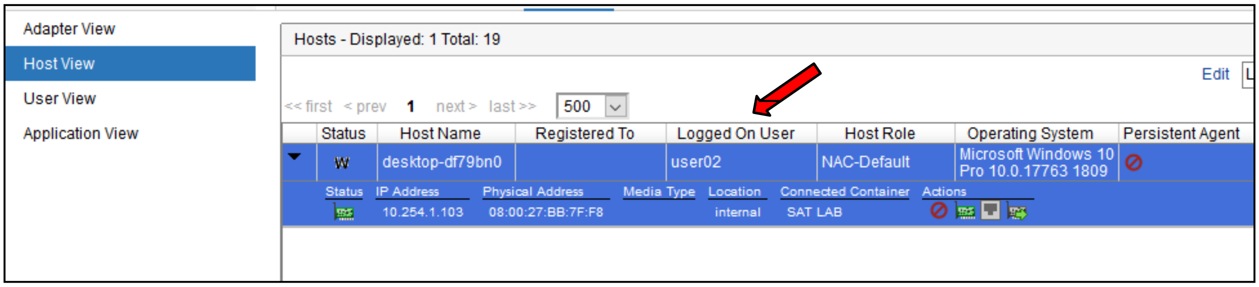
5. The rule should match.



Test Device Profiling Rule

✓ Rule Matches

6. Go to Host view and verify the host now has the information about Logged On User and all the applications installed on it.



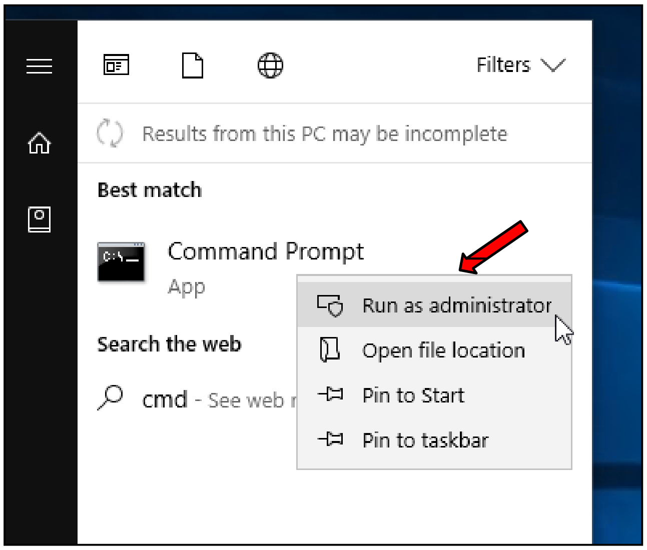
Hosts - Displayed: 1 Total: 19

	Status	Host Name	Registered To	Logged On User	Host Role	Operating System	Persistent Agent
▼	W	desktop-df79bn0		user02	NAC-Default	Microsoft Windows 10 Pro 10.0.17763 1809	⊘

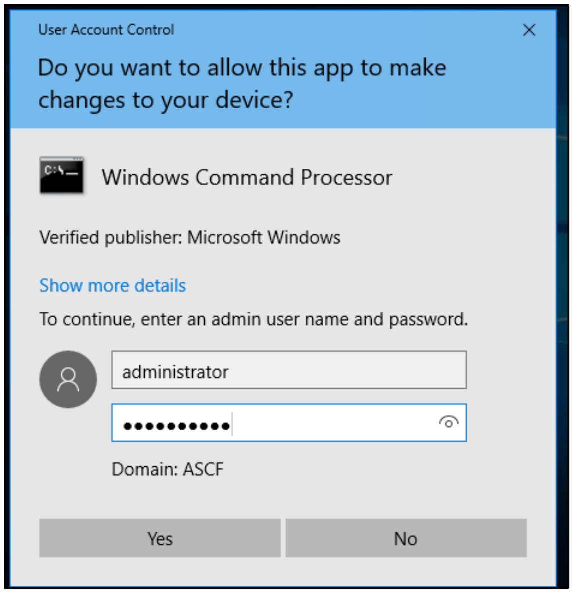
Status	IP Address	Physical Address	Media Type	Location	Connected Container	Actions
	10.254.1.103	08:00:27:BB:7F:F8		internal	SAT LAB	⊘

Enabling WinRM manually on each Windows machine.

1. Ensure machine has joined a domain.
2. On the Windows machine, run the Command Prompt as an Administrator. See the images below:



Results from this PC may be incomplete



Do you want to allow this app to make changes to your device?

Windows Command Processor

Verified publisher: Microsoft Windows

To continue, enter an admin user name and password.

administrator

•••••••••••

Domain: ASCF

3. On the Command Prompt, run the following command (administrator mode):

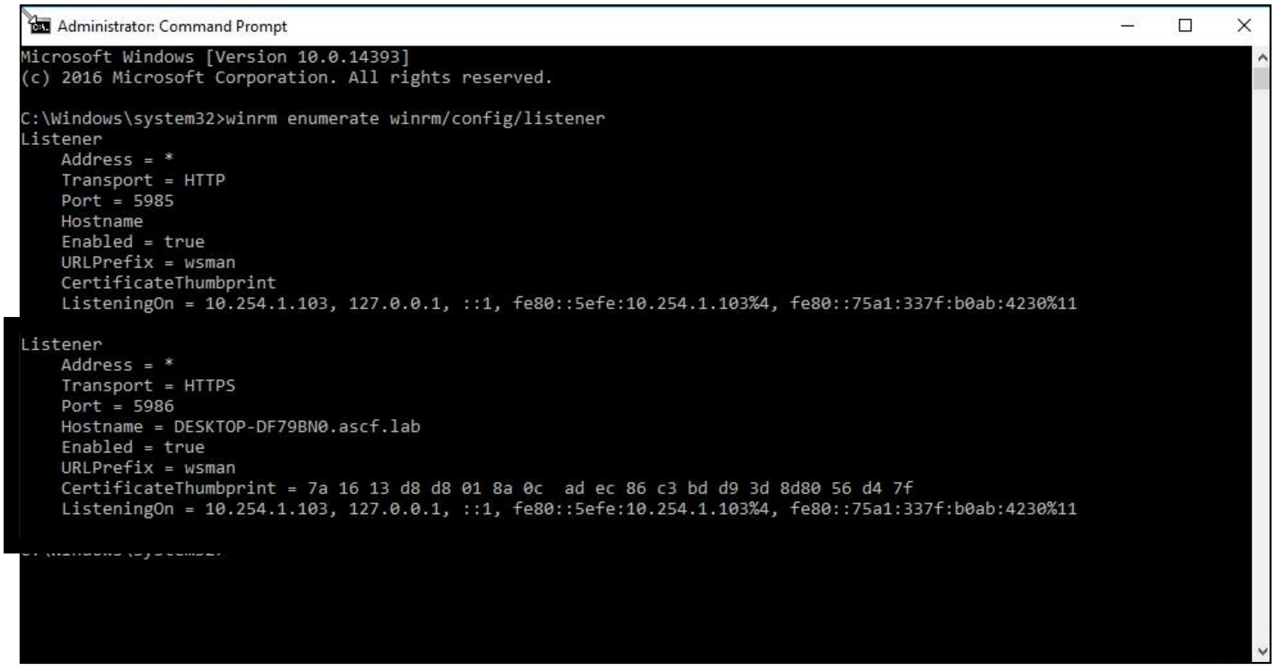
```
winrm quickconfig -transport:https -force
```

4. If there is no error, run the following command to verify you have configured the WinRM properly:

```
winrm enumerate winrm/config/listener
```

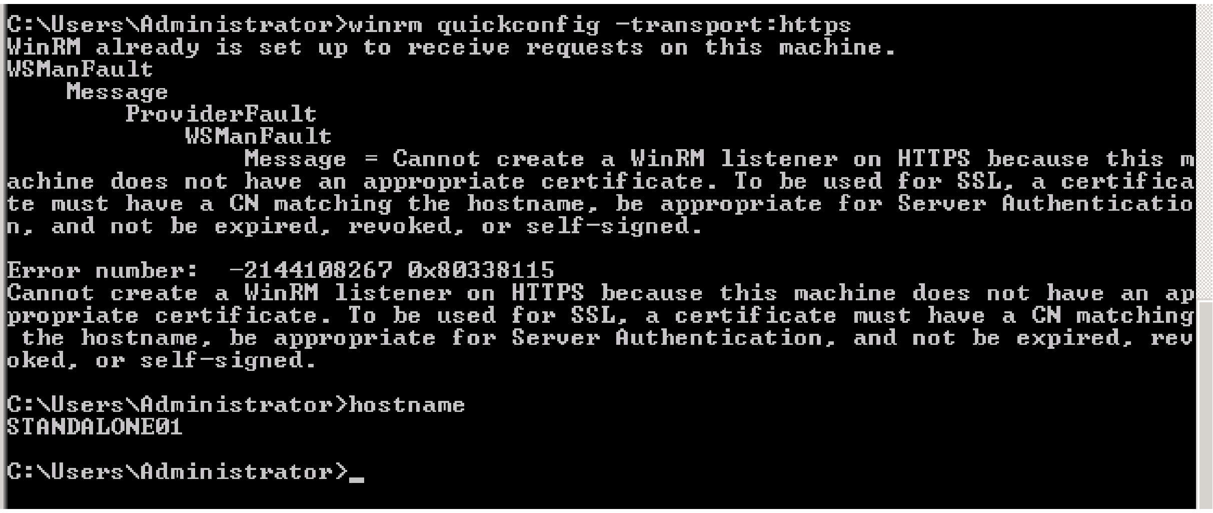
5. Ensure a result returns like the example on the image below, where the listener has a Transport Method configured as HTTPS.

Note: Some machines won’t show the Transport = HTTP. This can be ignored as it is not used for security purposes.



```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>winrm enumerate winrm/config/listener
Listener
    Address = *
    Transport = HTTP
    Port = 5985
    Hostname
    Enabled = true
    URLPrefix = wsman
    CertificateThumbprint
    ListeningOn = 10.254.1.103, 127.0.0.1, ::1, fe80::5efe:10.254.1.103%4, fe80::75a1:337f:b0ab:4230%11

Listener
    Address = *
    Transport = HTTPS
    Port = 5986
    Hostname = DESKTOP-DF79BN0.ascf.lab
    Enabled = true
    URLPrefix = wsman
    CertificateThumbprint = 7a 16 13 d8 d8 01 8a 0c  ad ec 86 c3 bd d9 3d 8d80 56 d4 7f
    ListeningOn = 10.254.1.103, 127.0.0.1, ::1, fe80::5efe:10.254.1.103%4, fe80::75a1:337f:b0ab:4230%11
```

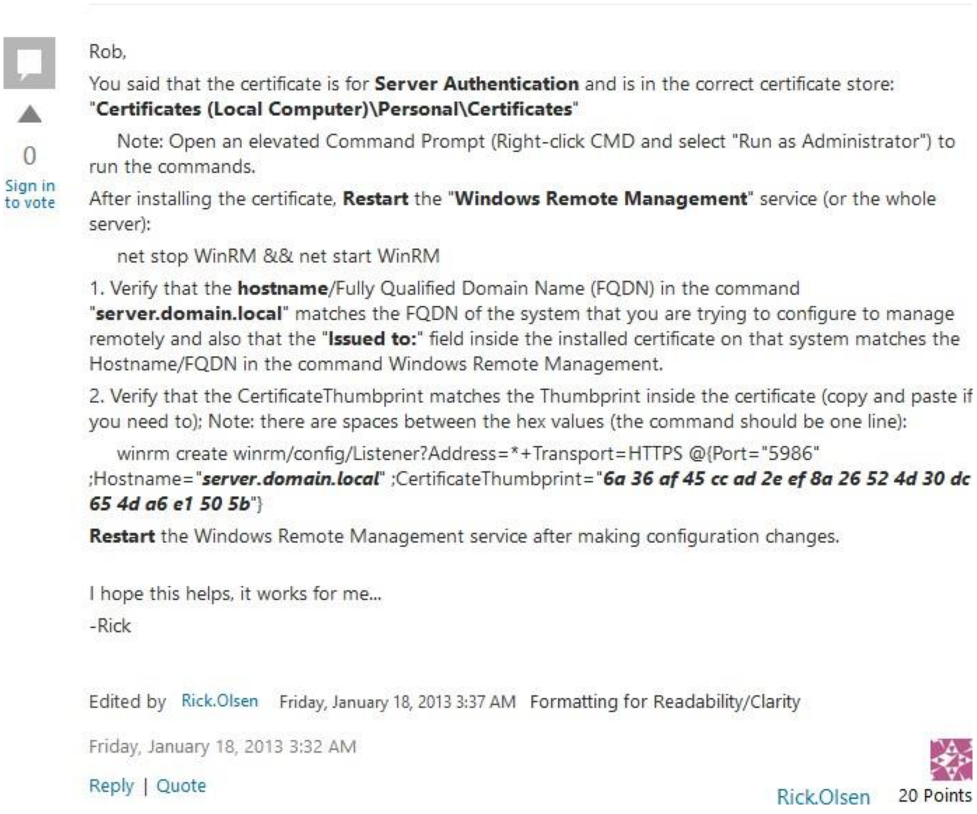
6. If an error displays stating there is no appropriate certificate (image below), either configure a certificate template for enrollment (see **Configure a Policy to Auto-Enroll Certificates**) or perform it manually.



```
C:\Users\Administrator>winrm quickconfig -transport:https
WinRM already is set up to receive requests on this machine.
WSManFault
    Message
        ProviderFault
            WSManFault
                Message = Cannot create a WinRM listener on HTTPS because this m
achine does not have an appropriate certificate. To be used for SSL, a certifica
te must have a CN matching the hostname, be appropriate for Server Authenticatio
n, and not be expired, revoked, or self-signed.

Error number:  -2144108267 0x80338115
Cannot create a WinRM listener on HTTPS because this machine does not have an ap
propriate certificate. To be used for SSL, a certificate must have a CN matching
 the hostname, be appropriate for Server Authentication, and not be expired, rev
oked, or self-signed.

C:\Users\Administrator>hostname
STANDALONE01

C:\Users\Administrator>_
```

Sample Error: Cannot create a WinRM listener on HTTPS because this machine does not have an appropriate certificate. To be used for SSL, a certificate must have a CN matching the hostname, be appropriate for Server Authentication, and not be expired, revoked, or self- signed.

To solve this error manually, following this procedure (**Note:** For testing purposes in Lab environment. Not recommended for use in a production network):



Rob,

You said that the certificate is for **Server Authentication** and is in the correct certificate store: "**Certificates (Local Computer)\Personal\Certificates**"

Note: Open an elevated Command Prompt (Right-click CMD and select "Run as Administrator") to run the commands.

After installing the certificate, **Restart** the "**Windows Remote Management**" service (or the whole server):

```
net stop WinRM && net start WinRM
```

1. Verify that the **hostname**/Fully Qualified Domain Name (FQDN) in the command "**server.domain.local**" matches the FQDN of the system that you are trying to configure to manage remotely and also that the "**Issued to:**" field inside the installed certificate on that system matches the Hostname/FQDN in the command Windows Remote Management.

2. Verify that the CertificateThumbprint matches the Thumbprint inside the certificate (copy and paste if you need to); Note: there are spaces between the hex values (the command should be one line):

```
winrm create winrm/config/Listener?Address=*+Transport=HTTPS @{Port="5986" ;Hostname="server.domain.local" ;CertificateThumbprint="6a 36 af 45 cc ad 2e ef 8a 26 52 4d 30 dc 65 4d a6 e1 50 5b"}
```

Restart the Windows Remote Management service after making configuration changes.

I hope this helps, it works for me...

-Rick

Edited by Rick.Olsen Friday, January 18, 2013 3:37 AM Formatting for Readability/Clarity

Friday, January 18, 2013 3:32 AM

Source:

https://social.technet.microsoft.com/Forums/windowsserver/en-US/cddbef93-1114- 4cca-9621-5a506d9b632b/winrm-https-listener-problem-with-hostname-property?forum=winserverManagement

Alternate (Insecure) Configuration

1. Create a GPO "FortiNAC WinRM"
2. Select the GPO and choose Action->Edit
3. Computer configuration -> Policies -> Windows Settings -> Security Settings -> System Services Double-click Windows Remote Management (WS-Management)
4. Tick "Define this policy setting" and select "Automatic" Click Ok.
5. Computer configuration -> Policies -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security -> Expand -> Inbound Rules
6. Right-click -> New Rule
7. Select Predefined, select "Windows Remote Management" and click Next. Untick the compatibility mode which opens port 80 and click Next.
8. Select Allow the Connection and click Finished.
9. Optionally, restrict to your FortiNAC Application Server IP addresses
10. Double-click the rule.
11. Click the scope tab
12. Under Remote IP Address, Select "These IP Addresses"
13. Click Add, and enter the addresses for your FortiNAC appliances.
14. Computer Configuration -> Policies -> Administrative Templates -> Windows Components -> Windows Remote Management (WinRM) -> WinRM Service
15. Enable "Allow remote server management through WinRM" with "*" as the IPv4 and IPv6 filters.
16. Enable "Allow unencrypted traffic"
17. Close the Group Policy Management Editor Link the FortiNAC WinRM GPO as needed.

Troubleshooting

Device Not Matching Rule

Verify the following:

- Adapter shows online.
- Ensure all information is available in the Host record for the applicable rule.
- Right click on Host and select **Show Events**. For a list of Device Profiler events and definitions, see Events section in the Appendix.

Then revalidate.

KB Articles

Device Profiler slow to register devices
DHCP Fingerprint Profiling Rule does not match upon initial connection
View DHCP Fingerprint information received form the production network
Frequent L3 polling when using Device Profiler

Debugging

Use the following KB article to gather the appropriate logs using the debugs below.
Gather logs for debugging and troubleshooting

Note: Debugs disable automatically upon restart of FortiNAC control and management processes.

Function	Syntax	Log File

LDAP lookup (WMI method)	`nacdebug -name DirectoryManager true`
	`nacdebug -name DirectoryAuthentication true`
		/bsc/logs/output.master

DPC Server processes	`nacdebug -name DpcRuleServer true`	/bsc/logs/output.master
Profiler evaluation details	`nacdebug -name ActiveFingerprint true`	/bsc/logs/output.nessus

Specific MAC address logging (FortiGuard method)	Enable:
	`nacdebug -logger yams.fortinet.iot -level FINEST`
	
	Disable:
	`nacdebug -logger yams.fortinet.iot`
		/bsc/logs/output.nessus

Disable debug	`nacdebug -name <debug name> false`	N/A

Appendix

Profiling Rule Method Examples

IP Range and Vendor OUI Name to Apply to Multiple Locations

Scenario: Create one profiling rule to classify cash machines that have the same vendor OUI but reside in multiple locations using IP range and Vendor OUI.

Location 1
IP address range 10.10.124.140 - 10.10.124.180
Vendor OUI name "MAXAN SYSTEMS"

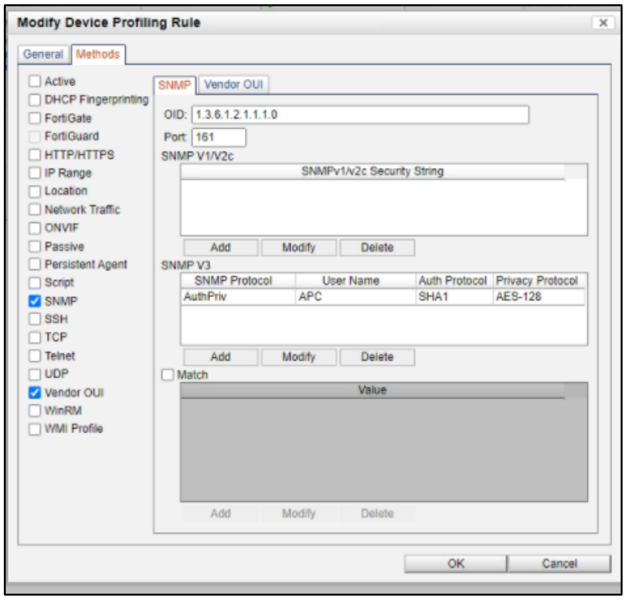
Location 2
IP address range 10.10.125.140 - 10.10.125.180
Vendor OUI name "MAXAN SYSTEMS"

Method Configuration:
IP Range: Starting IP 10.10.*.140 - Ending IP 10.10.*.180
Vendor OUI name: MAXAN SYSTEMS

SNMP OID

Scenario: Profile APC equipment.

Classify devices that answer to query for sysDescr OID string 1.3.6.1.2.1.1.1.0 using SNMP v3 credentials.



Modify Device Profiling Rule

☐ Active
☐ DHCP Fingerprinting
☐ FortiGate
☐ FortiGuard
☐ HTTP/HTTPS
☐ IP Range
☐ Location
☐ Network Traffic
☐ ONVIF
☐ Passive
☐ Persistent Agent
☐ Script
☑ SNMP
☐ SSH
☐ TCP
☐ Telnet
☐ UDP
☑ Vendor OUI
☐ WinRM
☐ WMI Profile

OID: 1.3.6.1.2.1.1.1.0
Port: 161

SNMP V1/V2c

SNMPv1/v2c Security String

SNMP V3

SNMP Protocol	User Name	Auth Protocol	Privacy Protocol
AuthPriv	APC	SHA1	AES-128

☐ Match

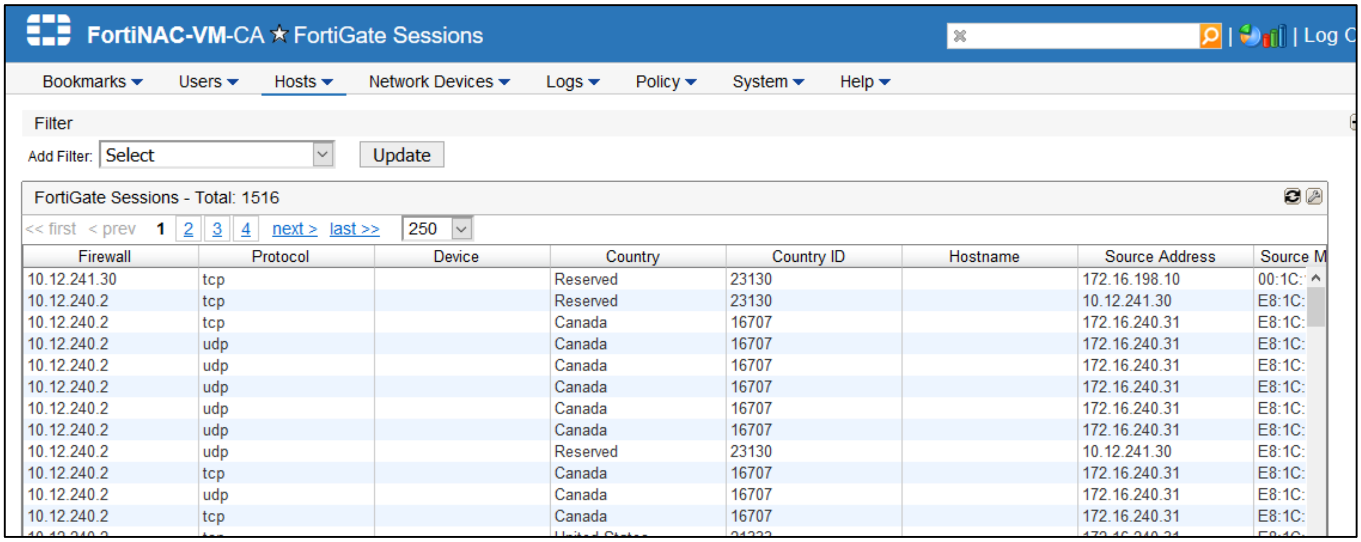
Value

Events

Event	Definition
Device Profile Rule Match	A rogue host has matched a Device Profiling rule allowing it to be assigned a device type and registered.
Device Profiling Automatic Registration	A rogue host has been registered by device profiling based on a device profiling rule.
Device Profiling Rule Missing Data	Indicates that Device Profiler cannot compare a rogue against a rule because FortiNAC does not have enough information about the rogue, such as a DHCP fingerprint. If Device Profiler cannot compare a rogue against a rule it does not continue processing that rogue, and moves on to the next rogue.
Device Rule Confirmation Failure **Device Rule Confirmation Success**	Devices identified by a Device Profiling rule maintain their association with that rule. If enabled, the associated rule and the device are checked periodically to see if the rule is still valid for the device. These event messages indicate whether or not the device matched the associated rule.

FortiGate Session Information

Hosts > FortiGate Sessions



FortiNAC-VM-CA ☆ FortiGate Sessions
| Log O
Bookmarks ▾ Users ▾ Hosts ▾ Network Devices ▾ Logs ▾ Policy ▾ System ▾ Help ▾
Filter
Add Filter: Select
Update

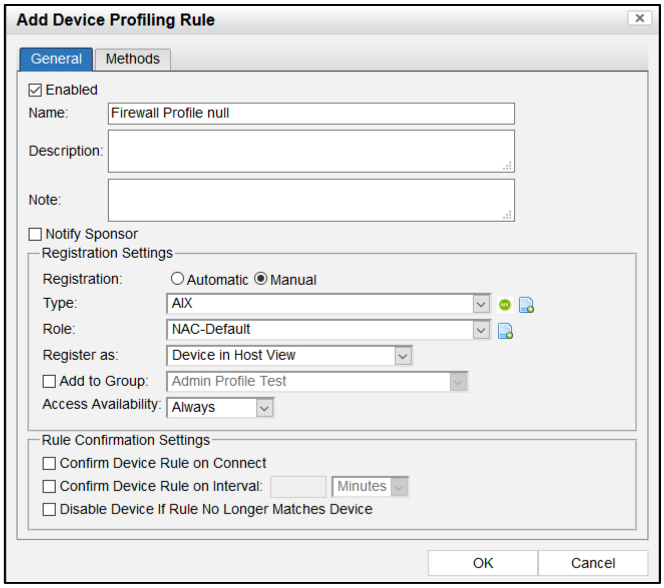
FortiGate Sessions - Total: 1516

<< first < prev 1 2 3 4 next > last >> 250

Firewall	Protocol	Device	Country	Country ID	Hostname	Source Address	Source M
10.12.241.30	tcp		Reserved	23130		172.16.198.10	00:1C:
10.12.240.2	tcp		Reserved	23130		10.12.241.30	E8:1C:
10.12.240.2	tcp		Canada	16707		172.16.240.31	E8:1C:
10.12.240.2	udp		Canada	16707		172.16.240.31	E8:1C:
10.12.240.2	udp		Canada	16707		172.16.240.31	E8:1C:
10.12.240.2	udp		Canada	16707		172.16.240.31	E8:1C:
10.12.240.2	udp		Canada	16707		172.16.240.31	E8:1C:
10.12.240.2	udp		Canada	16707		172.16.240.31	E8:1C:
10.12.240.2	udp		Reserved	23130		10.12.241.30	E8:1C:
10.12.240.2	tcp		Canada	16707		172.16.240.31	E8:1C:
10.12.240.2	udp		Canada	16707		172.16.240.31	E8:1C:
10.12.240.2	tcp		Canada	16707		172.16.240.31	E8:1C:
10.12.240.2	tcp		United States	21333		172.16.240.31	E8:1C:

Can select a session and create a Device Profiling rule based upon the session's characteristics.

Right click on desired session and select **Create Device Profiling Rule**.



Add Device Profiling Rule

☑ Enabled

Name: Firewall Profile null

Description:

Note:

□ Notify Sponsor

Registration Settings

Registration: ○ Automatic ● Manual

Type: AIX

Role: NAC-Default

Register as: Device in Host View

□ Add to Group: Admin Profile Test

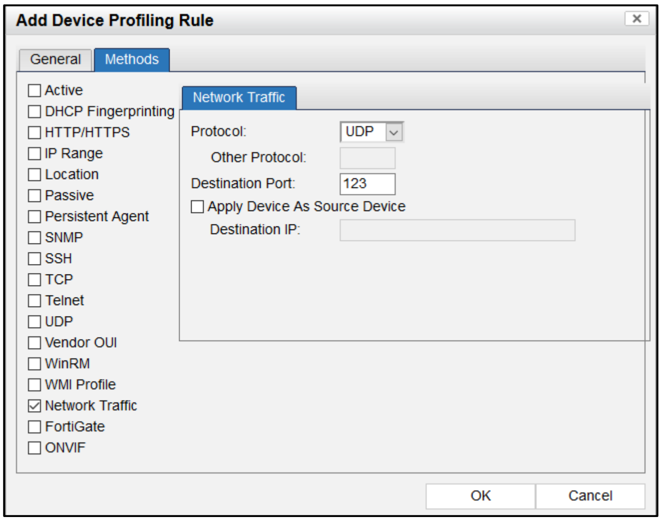
Access Availability: Always

Rule Confirmation Settings

□ Confirm Device Rule on Connect

□ Confirm Device Rule on Interval: Minutes

□ Disable Device If Rule No Longer Matches Device



Add Device Profiling Rule

□ Active
□ DHCP Fingerprinting
□ HTTP/HTTPS
□ IP Range
□ Location
□ Passive
□ Persistent Agent
□ SNMP
□ SSH
□ TCP
□ Telnet
□ UDP
□ Vendor OUI
□ WinRM
□ WMI Profile
☑ Network Traffic
□ FortiGate
□ ONVIF

Network Traffic

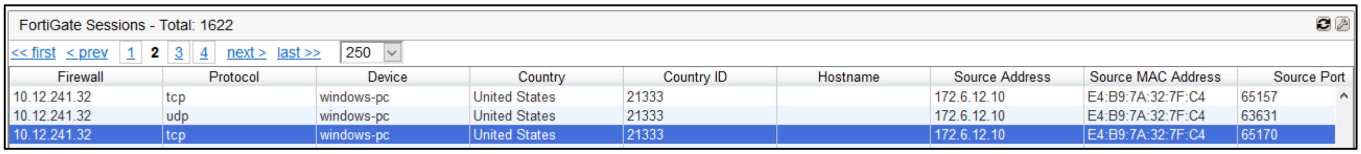
Protocol: UDP

Other Protocol:

Destination Port: 123

□ Apply Device As Source Device

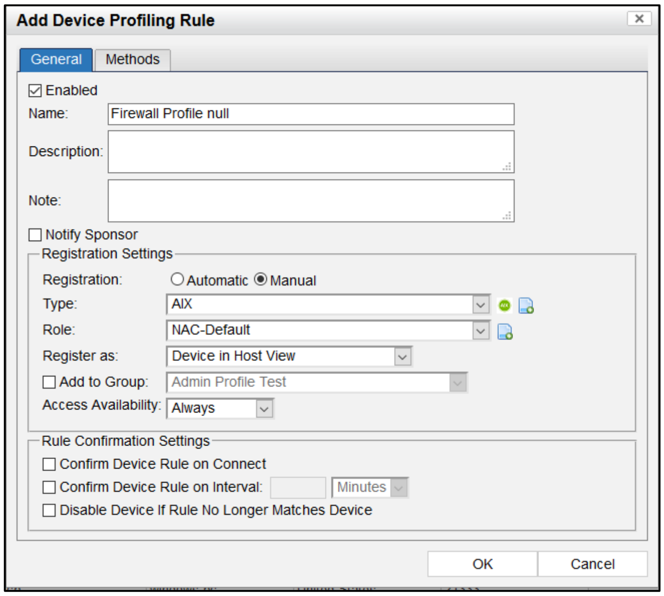
Destination IP:



FortiGate Sessions - Total: 1622

<< first < prev 1 2 3 4 next > last >> 250

Firewall	Protocol	Device	Country	Country ID	Hostname	Source Address	Source MAC Address	Source Port
10.12.241.32	tcp	windows-pc	United States	21333		172.6.12.10	E4:B9:7A:32:7F:C4	65157
10.12.241.32	udp	windows-pc	United States	21333		172.6.12.10	E4:B9:7A:32:7F:C4	63631
10.12.241.32	tcp	windows-pc	United States	21333		172.6.12.10	E4:B9:7A:32:7F:C4	65170



Add Device Profiling Rule ✕

General | Methods

☑ Enabled

Name: Firewall Profile null

Description:

Note:

□ Notify Sponsor

Registration Settings

Registration: ○ Automatic ● Manual

Type: AIX

Role: NAC-Default

Register as: Device in Host View

□ Add to Group: Admin Profile Test

Access Availability: Always

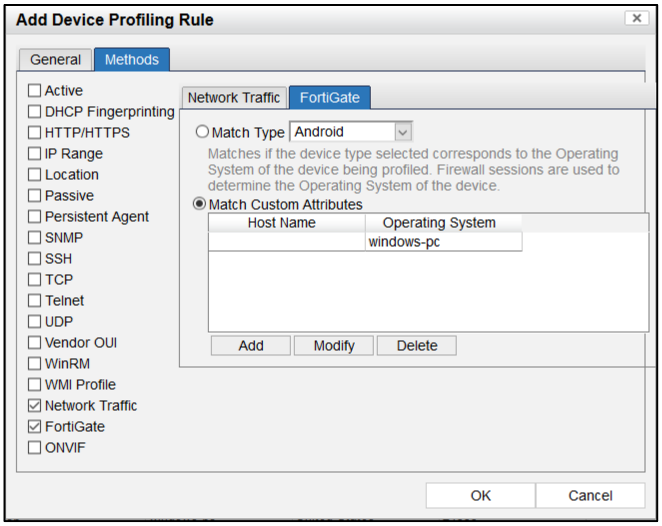
Rule Confirmation Settings

□ Confirm Device Rule on Connect

□ Confirm Device Rule on Interval: Minutes

□ Disable Device If Rule No Longer Matches Device

OK | Cancel



Add Device Profiling Rule ✕

General | Methods

□ Active
□ DHCP Fingerprinting
□ HTTP/HTTPS
□ IP Range
□ Location
□ Passive
□ Persistent Agent
□ SNMP
□ SSH
□ TCP
□ Telnet
□ UDP
□ Vendor OUI
□ WinRM
□ WMI Profile
☑ Network Traffic
☑ FortiGate
□ ONVIF

Network Traffic | FortiGate

○ Match Type Android

Matches if the device type selected corresponds to the Operating System of the device being profiled. Firewall sessions are used to determine the Operating System of the device.

● Match Custom Attributes

Host Name	Operating System
	windows-pc

Add | Modify | Delete

OK | Cancel