FortiNAC

Local RADIUS Server

Version: 9.2

Date: May 24, 2024

Rev: J

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

The information in this document provides guidance for configuring the FortiNAC Local RADIUS Server and managed infrastructure devices for 802.1x RADIUS authentication.

Related documentation: For example integrating Local RADIUS Server with the FortiGate, see Cookbook article (Tip: Right-click and select open link in new tab):
WiFi 802.1X based network using FortiNAC Local RADIUS Server

What it Does

The Local RADIUS Server processes RADIUS MAC and 802.1x EAP authentication requests. This feature eliminates the need for an external RADIUS server when using 802.1x RADIUS authentication.

Supported RADIUS Authentication:

- 802.1x EAP
- MAC

Supported Sources of RADIUS:

- Access Points
- Controllers
- Switches

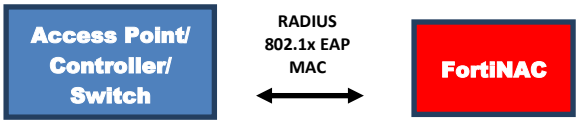
Network device authentication is not supported (Example: User authentication when logging into a switch).

How it Works

There are two RADIUS Authentication modes available for determining how RADIUS requests are processed. These can be configured in FortiNAC on a per-device basis:

- **Proxy**
  - Enabled by default.
  - Authentication: FortiNAC processes RADIUS MAC but proxies 802.1x EAP authentication to a customer-owned (external) RADIUS server.
  - Accounting:
    - FortiNAC processes accounting packets for several reasons, such as updating client status, as well as gather data required for certain third party CoA requests.
    - FortiNAC proxies accounting traffic to a customer-owned (external) RADIUS server.

- **Local**
  - Authentication: FortiNAC's Local RADIUS Server processes RADIUS MAC and 802.1x EAP authentication without the need to proxy to an external RADIUS server.
  - Accounting:
    - FortiNAC processes accounting packets for several reasons, such as updating client status, as well as gather data required for certain third party CoA requests.
    - The Local RADIUS server does not process accounting statistics. If accounting is required, FortiNAC can be configured to proxy Accounting traffic to an external RADIUS server.



Procedure Overview

1. Configure Device: Point RADIUS traffic to FortiNAC eth0 IP
2. Obtain SSL Certificates
3. Configure FortiNAC
    a. Install SSL Certificates: Install SSL Certificates for Local RADIUS Server EAP authentication and EAP-TLS end user certificate authentication
    b. Configure Local RADIUS Server Settings: This feature is disabled by default. Enable and define the appropriate authentication parameters.
    c. Configure device models: By default, FortiNAC will attempt to proxy 802.1x traffic received by devices modeled in Topology. Define which device models require 802.1x traffic to be processed by the Local RADIUS Server.

Requirements

FortiNAC

- Supported FortiNAC Engine Version: 8.8.0 and greater
- Latest CentOS updates have been applied to FortiNAC. See CentOS Updates in the Document Library.
- SSL certificates
    - Local RADIUS Server
        - 3rd party public or corporate owned internal Certificate Authority issued certificates
        - Wildcard certificates not recommended (some supplicants will not accept wildcard certificates)
    - Endpoint Trust Certificate: Required when using EAP-TLS to validate client-side certificate. Root CA certificate FNAC uses to match the incoming request certificate
        - Incoming certificate must be issued by the Root CA.
        - 3rd party public or corporate owned internal Certificate Authority issued certificates
        - Wildcard certificates not recommended (some supplicants will not accept wildcard certificates)
        - Either user or computer certificates
        - Supported using EAP-TLS, PEAPv0-EAP-TLS, EAP-TTLS/EAP-TLS
        - Multiple certificates can be uploaded to FortiNAC for this use.

Managed RADIUS Device (Access Point/Controller/Switch)

- Supported Firmware Version: See applicable integration reference manual in the Document Library.
- SNMP community or account
- Account for SSH or API access
    - Visibility only: System read access
    - Control: System read/write access
- Radius Access requests source IP must originate from the IP address of the device model in Topology. Otherwise, the request will be discarded.
- RADIUS requests for MAC Authentication must include the following:
    - User-Name
    - User-Password
    - Calling-Station-ID - include client MAC Address
- Accounting: When integrating with certain vendors, FortiNAC uses RADIUS accounting information for the management of endpoints. For this reason, RADIUS traffic for both authentication and accounting should be pointed to FortiNAC.

Directory

- Required if using MSCHAPv2 authentication: LDAP account created for FortiNAC to join domain

Considerations

- At this time, one server is allowed per domain for Winbind.
- FortiNAC is currently unable to encrypt Winbind connections with LDAPs or starttls.
- Works only with pre-existing PKI (Public Key Infrastructure). FortiNAC does not include PKI to issue certificates.
- FortiNAC can be configured to authenticate RADIUS using external RADIUS server(s), the built-in local RADIUS server or a combination of both. These can be configured in FortiNAC on a per-device basis.
- If both Local and proxy modes are used, they must use different authentication ports.
- FortiNAC does not provide accounting statistics/logging. If accounting data is currently collected for statistical purposes and network monitoring, FortiNAC can be configured to proxy accounting traffic to those servers currently collecting the data.

Integration

Configure Device

Complete the steps in the following sections of the appropriate integration reference manual in the Fortinet Document Library:

- Configure the Device (It is recommended to configure a test SSID first)
- Configure FortiNAC, omitting RADIUS Server settings (Network > RADIUS).

Obtain SSL Certificates

In FortiNAC, navigate to **System > Certificate Management**.

The two Certificate Targets that apply to the Local RADIUS feature are:

Local RADIUS Server (EAP)

For use when FortiNAC is acting as the 802.1x EAP termination point. Connecting clients use this certificate to establish trust with the EAP termination point (FortiNAC). The Local RADIUS service will not start without a certificate installed at this target.

If certificate has not yet been generated, a CSR request can be generated on FortiNAC. For instructions, see section **UI Method: Obtaining a Valid SSL Certificate from CA** in the SSL Certificate Installation reference manual.

SSL Certificate Requirements:

- 3rd party public or corporate owned internal Certificate Authority issued certificates
- Wildcard certificates not recommended (some supplicants will not accept wildcard certificates)

RADIUS Endpoint Trust

Endpoint Trust Certificate used by FortiNAC to validate the client-side certificate when Local RADIUS Server is configured and EAP-TLS is used for authentication. Client will be unable to authenticate unless the RADIUS Endpoint Trust Certificate Target has the matching root certificate installed.

- Acquire the root certificate(s) used by the endstations.
- If multiple root certificates have been distributed, ensure each one has been collected.

For instructions on viewing and exporting root certificates from a Windows machine, refer to the following link:
http://woshub.com/updating-trusted-root-certificates-in-windows-10/

SSL Certificate Requirements for Endpoint Trust:

- Certificate must be issued by the Root CA.
- 3rd party public or corporate owned internal Certificate Authority issued certificates
- Wildcard certificates not recommended (some supplicants will not accept wildcard certificates)
- Either user or computer certificates
- Supported using EAP-TLS, PEAPv0-EAP-TLS, EAP-TTLS/EAP-TLS

Configure FortiNAC

Install SSL Certificates

1. Navigate to **System > Certificate Management.**
2. Click **Upload Certificate**.
3. From the Select target drill-down, select **Local RADIUS Server (EAP)**
4. Upload certificate(s) and click **OK**
5. If using EAP-TLS to validate client-side certificate, select **RADIUS Endpoint Trust**
6. Upload Root certificate(s) used by the endstations and click **OK***

*To export installed Root certificate to use with other workstations, see Export RADIUS Endpoint Trust Certificate in the Appendix.

For more details on this view, see section Certificate management in the Administration Guide.

Local RADIUS Server Settings

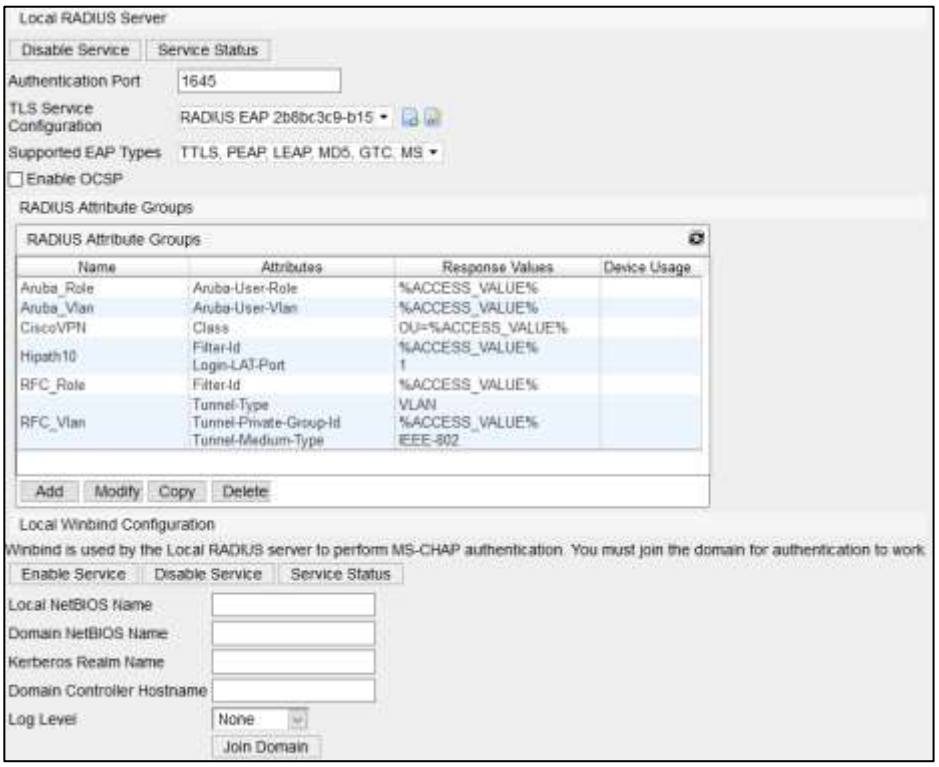
1. Navigate to **Network > RADIUS > Local Service**.
2. See section Configure Local RADIUS Server settings in the Administration Guide to complete configuration of the following:
   - Enable Local RADIUS service
   - Configure Local RADIUS Server settings as appropriate using table below

Field	Description
Authentication Port	Authentication port for the Local RADIUS Server. Default: Disabled, 1645 **Important**: If Proxy RADIUS mode is also configured, ensure the authentication port is different than the Local RADIUS.
TLS Service Configuration	TLS Protocol versions and Ciphers for EAP in the Local RADIUS Server. Add or Modify using the icons. **Name**: Unique name used to identify the configuration. **Certificate Alias**: Select the Certificate to use when securing communication. Certificates may be uploaded using the Certificate Management view. **Automatically Update Ciphers And Protocols on Upgrade**: If true, the settings for both Ciphers and TLS Protocols will become managed by FortiNAC. Upon upgrade, the system will automatically configure the TLS Service Configuration to the latest recommended Ciphers and Protocols. **Ciphers**: The Cipher Suite to use when encoding messages using TLS. At least one Cipher must be selected. Ciphers must be supported by both client and server, so disabling Ciphers may prevent some Persistent Agents from communicating. **TLS Protocols**: The list of TLS Protocols to allow by the server. At least one TLS Protocol must be selected. TLS Protocols must be supported by both client and server, so disabling Protocols may prevent some Persistent Agents from communicating.
Supported EAP Types	Allows configuration of which EAP types are enabled. The field displays the EAP Types currently enabled. Click the drill down menu to view the available types. Click on a specific type to either enable or disable: TLS - Requires the Endpoint Trust Certificate to be installed. For installation instructions see Certificate management TTLS PEAP LEAP MD5 GTC MSCHAPV2
OCSP	If enabled, EAP-TLS client certificates will have OCSP verification performed, using the URL embedded in the client certificate. **Important**: Certificates must contain the OCSP URL. Otherwise, client authentication will fail.

- Create RADIUS Attribute Groups (optional) - Allows administrators to control the RADIUS attributes FortiNAC returns in an Access-Accept. For recommended values see Vendor Specific Attribute Value Pairs in the Appendix
- Local Winbind Configuration (optional) - Provides MSCHAPv2 authentication
    1. Fill out the Windbind configuration using the table below

Field	Description	Example
Local NetBIOS Name	NetBIOS name by which the FortiNAC Samba server is known. For High Availability configurations, this is the primary FortiNAC Samba server. Note that the maximum length for a NetBIOS name is 15 characters.	FortiNAC FQDN = hostname.corp.example.com Local NetBIOS Name = "HOSTNAME"
Secondary (HA) NetBIOS Name	For FortiNAC High Availability configurations. NetBIOS name by which the secondary FortiNAC Samba server is known. Note that the maximum length for a NetBIOS name is 15 characters. If High Availability is not used, this field is left blank.	FortiNAC FQDN =hostname2.corp.example.com Local NetBIOS Name = "HOSTNAME2"
Domain NetBIOS Name	NetBIOS name of your domain. This is the subdomain of the DNS domain name.	Domain Controller Hostname = dc01.example.com Domain NetBIOS Name = "EXAMPLE" Domain Controller Hostname = dc01.corp.example.com Domain NetBIOS Name = "CORP"
Kerberos Realm Name	The DNS-style domain name.	“example.com”
Domain Controller Hostname	The name or address of the Active Directory domain controller to use to authenticate.	“dc01.example.com”
Log Level	The log level for the Winbind service. Recommended value is “none”.	N/A

2. Click **Save Settings**
3. Click **Join Domain**
4. Click **Enable Service**



Model Configuration

1. Navigate to **Network > Inventory.**
2. Select the device model and click the **Model Configuration** tab. (Note: Right-clicking and selecting Model Configuration will not display the proper configuration)
3. Under **RADIUS**, select **Local Mode** (default is proxy)
4. Configure Shared Secret (must match secret configured in device)
5. Select a Default RADIUS Attribute Group if desired (Default is none). To deploy attributes in bulk, see section RADIUS attribute groups in the Administration Guide.

See section Model configuration in the Administration Guide for more details.

Troubleshooting

Related KB Articles

Refer to the applicable KB article(s):
Local RADIUS does not start

Troubleshooting Tip: Local Radius server logs

Troubleshooting SNMP Communication Issues

Rogue Wireless Clients Cannot Connect to SSID

Troubleshooting RADIUS clients not connecting

Troubleshooting Wireless Clients Moved to the Wrong VLAN

Debugging

UI Method

Use the following KB article to gather the appropriate logs.
FortiNAC Local Radius Debug & Troubleshooting via GUI

CLI Method

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
FortiNAC Server*	`nacdebug -name RadiusAccess true`	/bsc/logs/output.master
RADIUS Service	`radiusd -X -l /var/log/radius/radius.log` Stop logging: Ctrl-C	/var/log/radius/radius.log
L2 related activity	`nacdebug -name BridgeManager true`	/bsc/logs/output.master
Disable debug	`nacdebug -name <debug name> false`	N/A

*Enables logging for a given MAC Address:

```
nacdebug -logger 'yams.RadiusAccess.RadiusAccessEngine.00:11:22:33:44:55' -level FINEST
```

To disable:

```
nacdebug -logger 'yams.RadiusAccess.RadiusAccessEngine.00:11:22:33:44:55'
```

Other Tools

Send a RADIUS Disconnect:
`SendCoA -ip <devip> -mac <clientmac> -dis`

Example:
`SendCoA -ip 10.1.0.25 -mac 00:1B:77:11:CE:2F -dis`

Appendix

SSL Certificate Location

SSL certificates applied via UI for Local RADIUS Server related targets are installed in the below directory. The certificate file modified is dependent upon the certificate target.

```
/etc/raddb/certs

-rw-rw----. 1 root radiusd 1001 Oct  2 14:48 ca.pem << RADIUS Endpoint Trust
-rw-rw----. 1 root radiusd 1.8K Oct  8 14:47 server.key
-rw-rw----. 1 root radiusd 4.3K Oct  8 14:47 server.pem << Local RADIUS Server (EAP)
```

Local Radius Service CLI Commands

The following functions can also be executed in the Administration UI under **Network > Settings > Authentication > Local RADIUS**.

Stop Service:
```
service radiusd stop
service winbind stop
```

Start Service:
```
service radiusd start
service winbind start
```

Restart Service:
```
service radiusd restart
service winbind restart
```

Display Status:
```
service radiusd status
service winbind status
```

Vendor Specific Attribute Value Pairs

IP Phones Connected to Cisco Meraki MS

Multi-Domain host mode recommended for switchports connected to an IP Phone with a device behind the phone. Hybrid Authentication is used and Voice VLAN authentication is required. Cisco Meraki switches require the following attribute pairs within the Access-Accept frame to put devices on the voice VLAN:

Name: Cisco-AVPair
Attribute: device-traffic-class
Response Value: voice

Reference article
https://documentation.meraki.com/MS/Access_Control/MS_Switch_Access_Policies_(802.1X)

Export RADIUS Endpoint Trust Certificate

If Endpoint Trust Certificate has been installed in FortiNAC to validate client-side certificates, it is possible to export the certificate to be used on workstations for authentication.

1. Login to CLI as root.
2. Navigate to directory desired to save the certificate
3. Run the command

```
keytool -exportcert -alias radius_trust_0 -keystore /bsc/campusMgr/.keystore
-storepass ^8Bradford%23 -file radius_trust_0.pem
```

Import the resulting file (radius_trust_0.pem) to the workstation.

Match Policies Based on RADIUS Attributes

As of version 9.2, policies can be configured to match criteria based upon RADIUS Attributes found within the RADIUS Access-Request.

1. Identify name and value of the desired attribute to match.
    a. Navigate to **Network > RADIUS > Local Service**
    b. Configure the following settings:
        - **Service Log Level**: Normal
        - **FortiNAC Server Log Debug**: Enabled
        - Click **Details & Logs** and click **Server Log**

    c. Have sample client connect.
    d. Click **Refresh** to view new entries printed since the window was opened.

    Example: Match Access-Requests that include the host name as the user name.

    Entry example in Service Log:

    ```
    (1784)   User-Name = "host/myhostname.mydomain.com"
    ```

2. Navigate to **Policy & Objects > User/Host Profiles**.
3. Click **Add** or select the desired existing profile and click **Modify**.
4. Next to **Who/What by RADIUS Attribute**, click **Add**.
5. Specify the name and value.

    Example:
    Name: User-Name
    Value: host/*