Meraki VPN

Contents

Meraki configuration for SMS PASSCODE®

This guide outlines the process of configuring a Meraki for Authentication with SMS PASSCODE®.

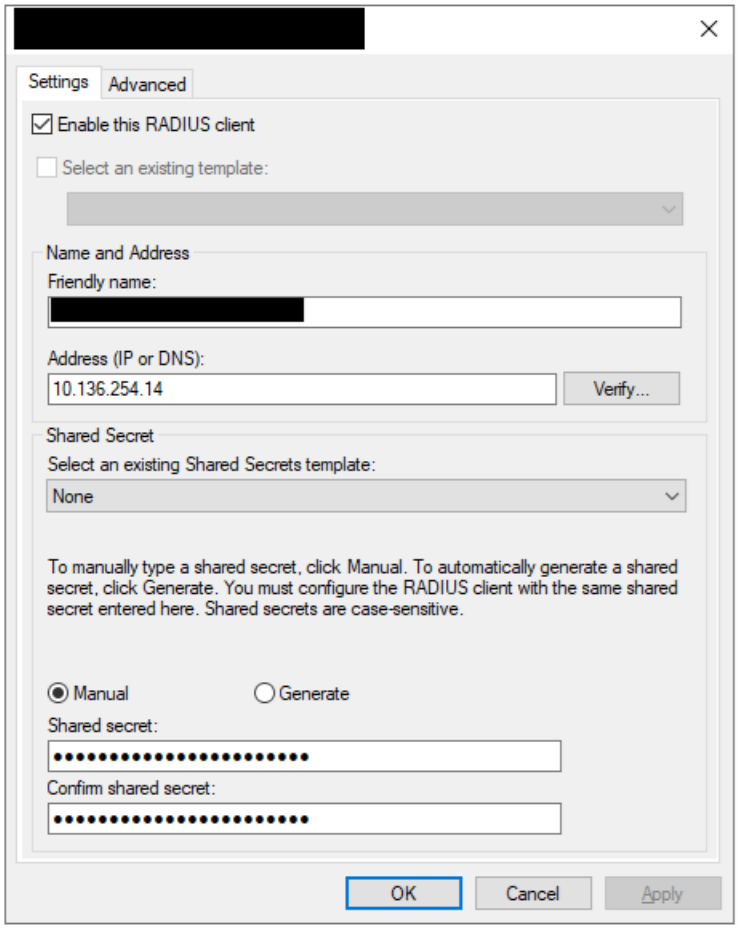
NOTE: Censornet MFA integration with Meraki only supports Soft token Push if using the Microsoft VPN Client.

censornet.

Microsoft NPS RADIUS Client

In order for the Meraki to use RADIUS as an authentication method, it must be added as a RADIUS client on the Microsoft NPS.

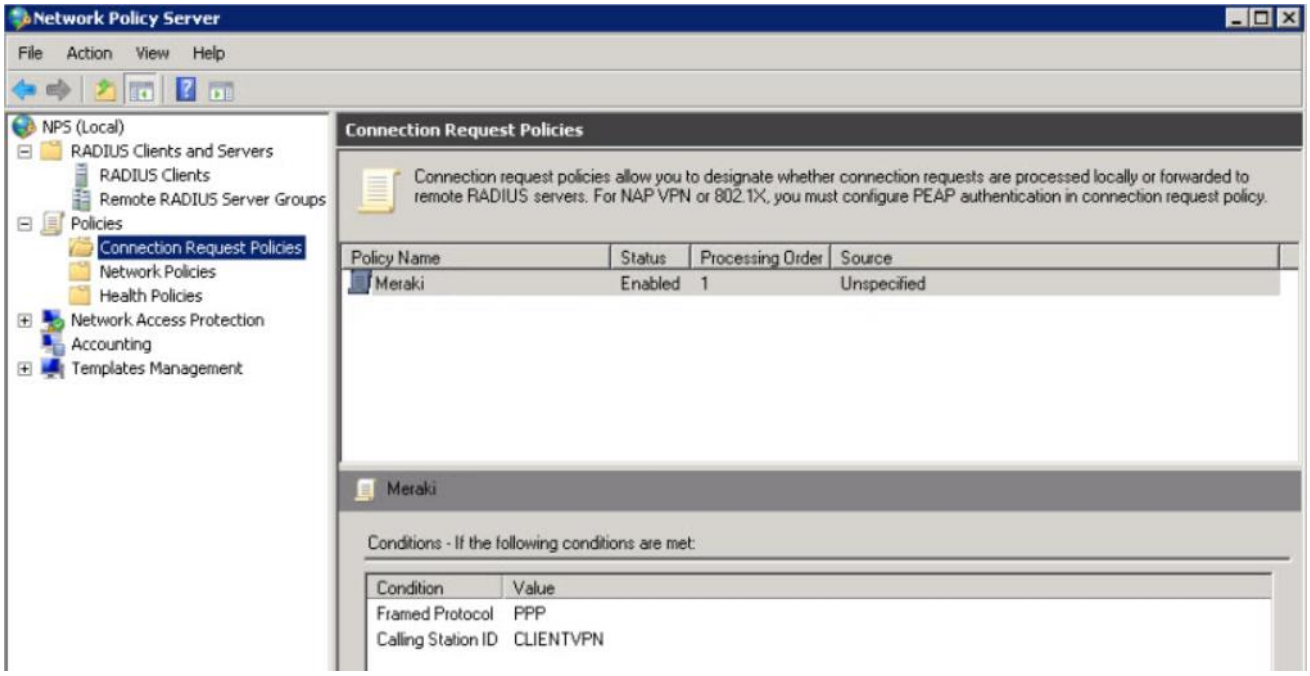
1. In the left pane of the NPS console, expand the RADIUS Clients and Servers option.
2. Right-click the RADIUS Clients option and select New.
3. Enter a Friendly Name for the Meraki device.
4. Enter the IP Address of your Meraki device.
5. Create and enter a RADIUS Shared Secret.



censornet.

Microsoft NPS RADIUS Connection Request

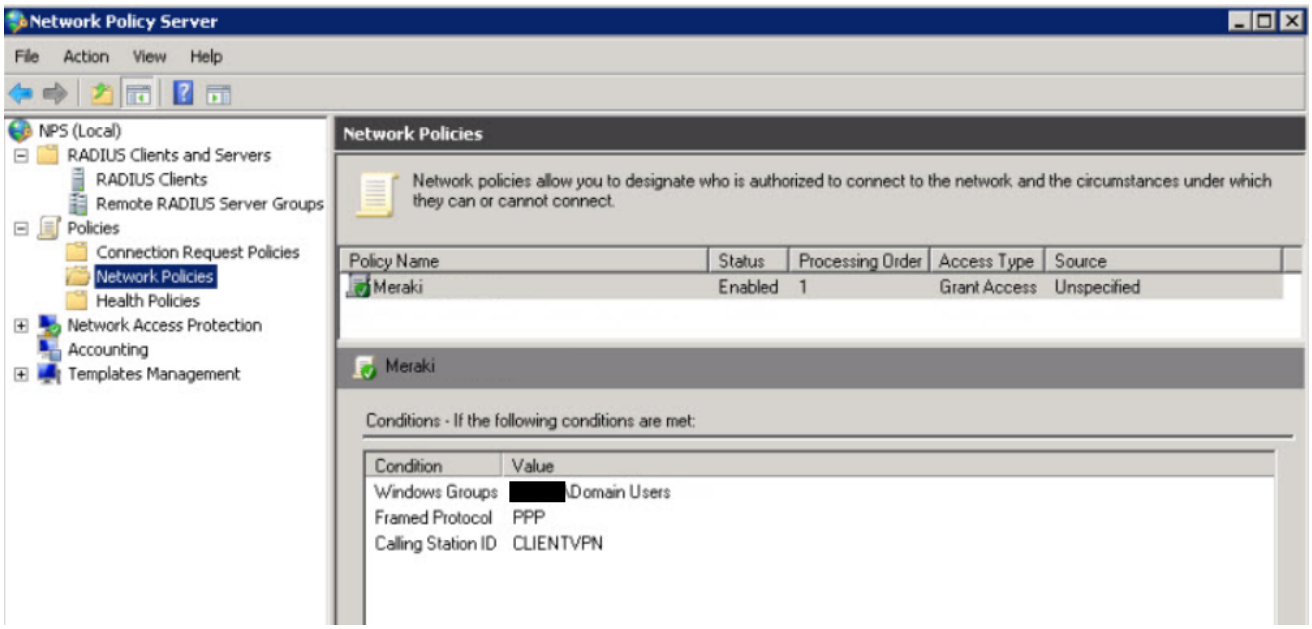
1. Within the NPS console run the Connection Request Policy Wizard, enter a Policy Name then select the Network Access Server Type *unspecified* then press Next.
2. Select Add to add conditions to your policy. Access Request messages will need to meet these conditions to be allowed access.
3. From the list of conditions, select the option for Framed-Protocol. Add and place a check next to the PPP option then press Ok.
4. Select Add to add another condition and select the option for CallingStationID. Enter CLIENTVPN into the text box and press Next.
5. On the next three pages of the wizard, leave the default settings. Select Next on these pages to continue.
6. Review the settings then select Finish.



censornet.

Microsoft NPS RADIUS Network Policy

1. Within the NPS console run the Network Policy Wizard enter a Policy Name and select the Network Access Server type *unspecified* then choose Next.
2. Select Add to add conditions to your policy.
3. From the list of conditions, select the option for Windows Groups. Select Add Groups and enter the name of Windows Group you would like to give VPN access.
4. Select Add to add an additional condition. Select the option for Framed Protocol, press add and check the PPP option then select Ok.
5. Click Add to add a final condition. Select the option for CallingStationID. Enter CLIENTVPN into the text box and select Next.
6. Keep the default settings on the Specify Access Permission page and select Next.
7. Unselect all checkboxes and select Unencrypted authentication (PAP, SPAP). An informational box will be displayed, select No to continue then select Next.
8. Select Next on the next few pages keeping the default settings.
9. Review the settings then select Finish.



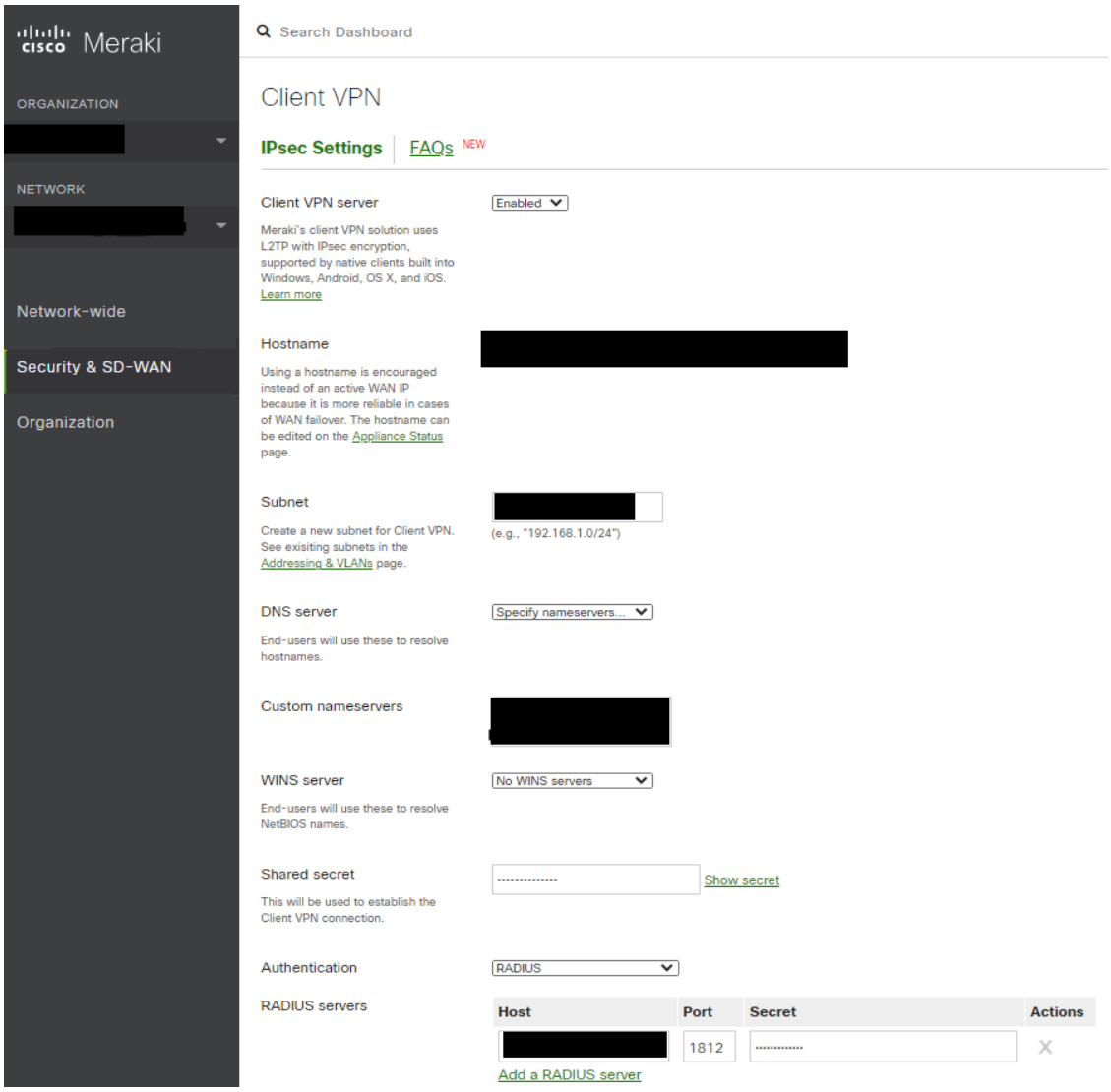
Meraki RADIUS Configuration

Once the NPS server has been configured, the below steps detail how to configure the Meraki Client VPN to use RADIUS:

1. Log onto the Meraki device and navigate to Configure > Client VPN.
2. Select the option to enable the Client VPN Server.
3. Set the Client VPN Subnet. This will be a unique IP subnet offered to clients connecting to the Meraki device via a Client VPN connection.
4. Specify the DNS servers.
5. Enter a shared secret* that will be used by the client devices to establish the VPN connection.
6. Select RADIUS as the Authentication method.
7. Select Add a RADIUS Server link.
    a. Enter your RADIUS Host IP Address (IP of the NPS).
    b. Enter 1812 as the RADIUS port.
    c. Enter the RADIUS Shared Secret (created in NPS).
8. Select Save changes.

***** This is a different shared secret from the RADIUS shared secret.

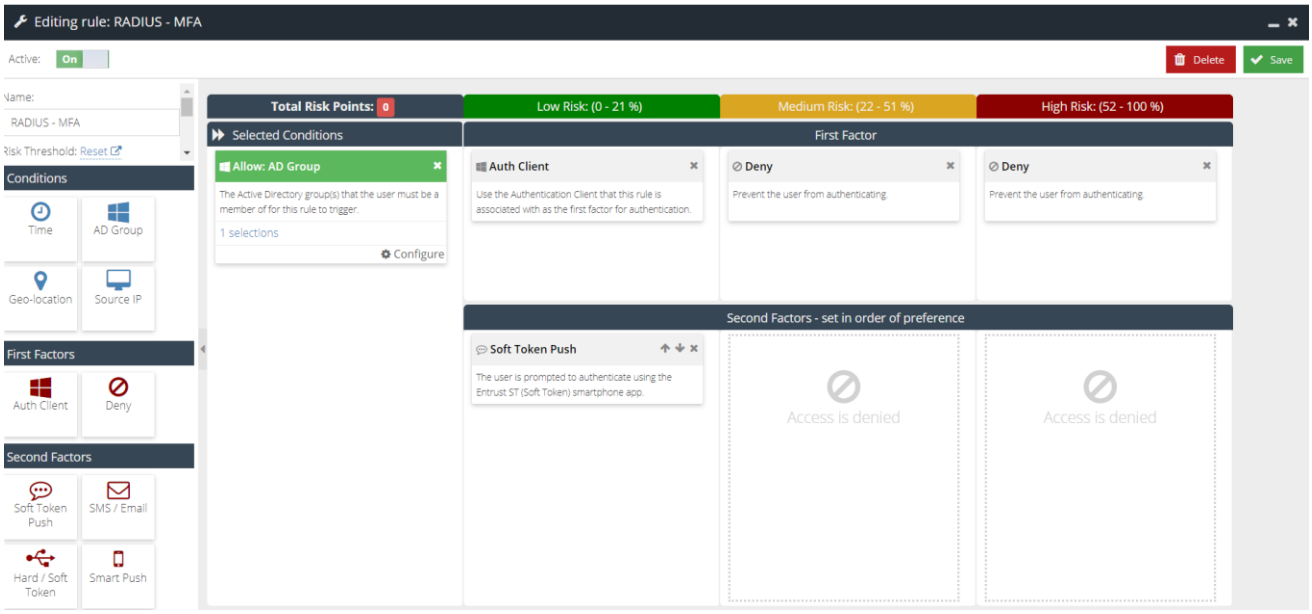
censornet.


Meraki
ORGANIZATION
[redacted]
NETWORK
[redacted]
Network-wide
Security & SD-WAN
Organization
Search Dashboard
Client VPN
IPsec Settings
FAQs NEW
Client VPN server
Enabled
Meraki's client VPN solution uses L2TP with IPsec encryption, supported by native clients built into Windows, Android, OS X, and iOS.
Learn more
Hostname
[redacted]
Using a hostname is encouraged instead of an active WAN IP because it is more reliable in cases of WAN failover. The hostname can be edited on the Appliance Status page.
Subnet
[redacted]
(e.g., "192.168.1.0/24")
Create a new subnet for Client VPN. See exisiting subnets in the Addressing & VLANs page.
DNS server
Specify nameservers...
End-users will use these to resolve hostnames.
Custom nameservers
[redacted]
WINS server
No WINS servers
End-users will use these to resolve NetBIOS names.
Shared secret
Show secret
This will be used to establish the Client VPN connection.
Authentication
RADIUS
RADIUS servers
Host
Port
Secret
Actions
[redacted]
1812
Add a RADIUS server

Configuration Censornet MFA Rule

If you are using the Microsoft VPN client with your Meraki solution for VPN access, then Push authentication must be used because the Microsoft VPN client does not support challenge-response.

Within your MFA rule only select Soft token Push as the Second Factor.



Additional information on RADIUS configuration for SMS PASSCODE®

Censornet's MFA integration with Meraki utilises the Censornet RADIUS protection. RADIUS installation and configuration should be in place before the Meraki configuration detailed in this document. Additional information on RADIUS installation and configuration can be found here:

https://help.clouduss.com/cloud-mfa/configuring-RADIUS-protection