

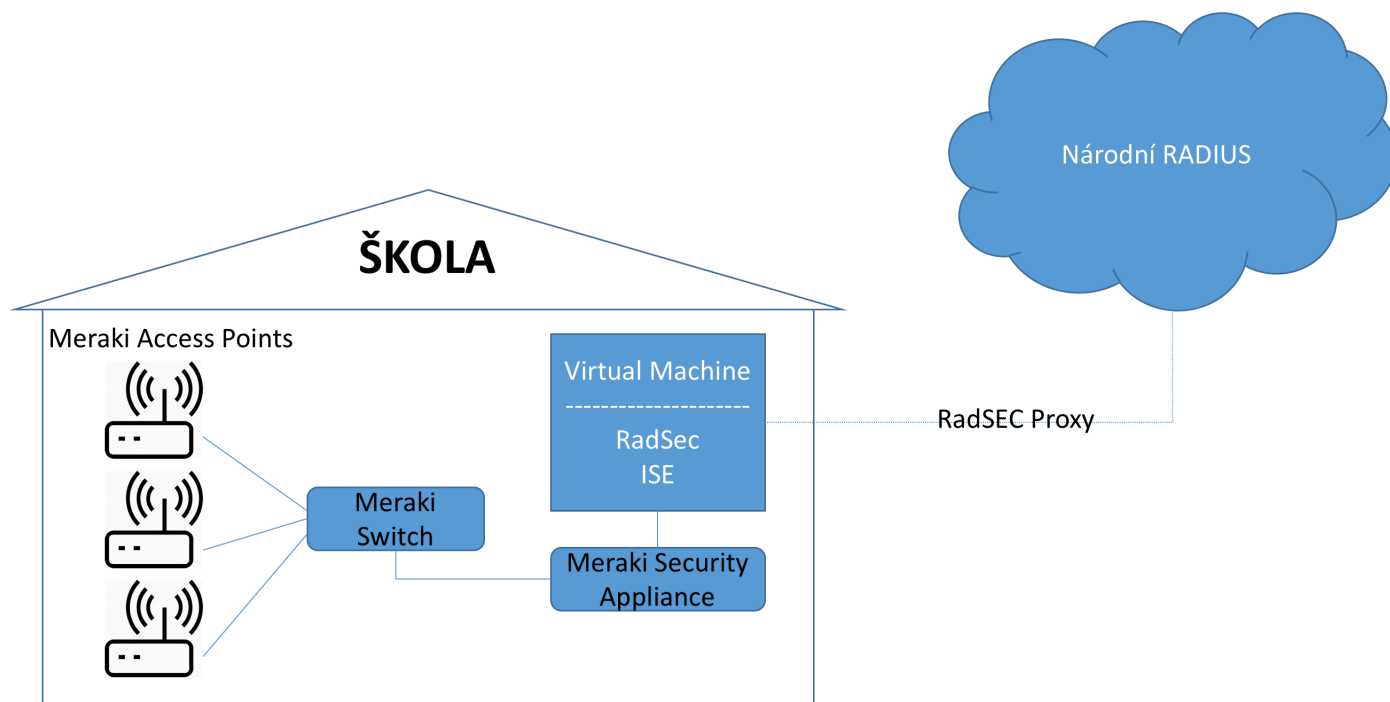
Připojení k eduroam.cz: Nastavení síťových komponent Meraki a konfigurace ISE

Podrobní postup připojení organizace k eduroamu v ČR je detailně popsán na stránkách eduroam.cz (<https://www.eduroam.cz/cs/spravce/pripojovani/uvod>)

Nezbytnou součástí připojení k českému eduroam systému jsou RadSec/IPsec server a RADIUS server.

Jak postupovat při konfiguraci RadSec / IPsec -

<https://www.eduroam.cz/cs/spravce/pripojovani/ipsec/uvod>




Obrázek č.1 – Schématické zobrazení komponent

Nastavení Meraki AP pro autentizaci s ISE

Správné nastavení přístupového bodu Meraki MR pro šifrovanou komunikace s ISE (eduroam).
Wireless – Configuration overview – SSIDs

(eduroam) → edit settings

 Network: **Skola1** ▼

This network contains both an MR access point and a security appliance with integrated wireless. The security appliance will not mesh with the negatively affected by this network configuration.

Configuration overview

SSIDs Showing 4 of 15 SSIDs. [Show all my SSIDs.](#)

	guest-access	eduroam
Enabled	<input type="button" value="enabled ▼"/>	<input type="button" value="enabled ▼"/>
Name	rename	rename
Access control	edit settings	edit settings
Encryption	WPA2-PSK	802.1X with custom RADIUS
Sign-on method	None	None
Bandwidth limit	unlimited	unlimited
Client IP assignment	Local LAN	Meraki DHCP
Clients blocked from using LAN	n/a	no
Wired clients are part of Wi-Fi network	no	no
VLAN tag ⓘ	n/a	n/a
VPN	Disabled	Disabled
Splash page		
Splash page enabled	no	no
Splash theme	n/a	n/a

or [cancel](#)

(Please allow 1-2 minutes for changes to take effect.)

Nastavení SSID přístupového bodu Meraki MR pro přímou komunikaci s ISE přes RADIUS, v sekci **Access control** vybereme dané SSID (eduroam) a v sekci **Network access** požadavku na **WPA2-Enterprise with my RADIUS server**.



Network: **Skola1** ▼

This network contains both an MR access point and a security appliance with integrated wireless. The security negatively affected by this network configuration.

Access control

SSID: **eduroam** ▼

Network access

Association requirements

- Open (no encryption)
Any user can associate
- Pre-shared key with **WPA2** ▼
Users must enter a passphrase to associate
- MAC-based access control (no encryption)
RADIUS server is queried at association time
- WPA2-Enterprise with **my RADIUS server** ▼**
User credentials are validated with 802.1X at association time

WPA encryption mode **WPA2 only** ▼

Nastavení/přidání RADIUS servru – IP adresa ISE (**Host IP** = dle určení v aktuální síti, **Port** = 1812, **Secret** = unikátní string řetězec, stejný jako na straně ISE)

RADIUS servers

#	Host	Port	Secret	Actions
1	192.168.43.54	1812	⊕ X Test

[Add a server](#)

RADIUS testing ⓘ **RADIUS testing disabled** ▼

RADIUS accounting **RADIUS accounting is disabled** ▼

RADIUS attribute specifying group policy name **Filter-Id** ▼ ⓘ

Assign group policies by device type ⓘ **Disabled: do not assign group policies automatically** ▼

Nastavení ověření přístupu do sítě na přepínači Meraki MS pro přímou komunikaci s ISE 802.1x řešením přes RADIUS, v sekci **Switch** → **Configure** → **Access policies** přidáním nové Access policy (eduroam).

Nastavení/přidání RADIUS serveru – IP adresa ISE (**Host IP** = dle určení v aktuální síti, **Port** = 1812, **Secret** = unikátní řetězec znaků, stejný jako na ISE)

Access policies

Access policies

Name

RADIUS servers

#	Host	Port	Secret	Actions
1	<input type="text" value="192.168.43.54"/>	<input type="text" value="1812"/>	<input type="text" value="....."/>	<input type="button" value="⊕"/> <input type="button" value="✕"/> <input type="button" value="Test"/>

[Add a server](#)

RADIUS testing ⓘ

Access policy type

Guest VLAN

Voice VLAN clients

Switch ports There are currently [0 Switch ports](#) using this policy

[Remove this access policy](#)

[Add an access policy](#)

Instalace ISE serveru

ISE lze provozovat jako appliance nebo jako virtuální stroj. V našem případě předpokládáme nasazení v prostředí VMware.

Požadavky na server, detailní popis instalace je uveden v kapitole 3 **Install ISE on a VMware Virtual Machine** v instalačním manuálu na tomto odkazu:

http://www.cisco.com/c/en/us/td/docs/security/ise/2-1/install_guide/b_ise_InstallationGuide21.pdf

Instalace je ukončena wizardem z příkazové řádky, který provede základní síťové nastavení ISE. Od tohoto okamžiku je již veškerá správa ISE vedena ve webovém rozhraní GUI.

Přidání síťových zařízení komunikujících s ISE

Pokud ISE dělá pouze RADIUS proxy oproti serveru organizace nejsou konfigurační kroky v této kapitole nutné. Ale v případě že ISE bude provádět ještě nějaké jiné služby, je toto vhodné nastavení, protože v logu snadno rozlišíme různé autentizační/autorizační požadavky z různých přístupových zařízení.

Vytvoření nové skupiny přístupových prvků. Toto umožní při použití více stejných typů zařízení pracovat v pravidlech se skupinami, případně je zohlednit v logu nebo reportech.

The screenshot displays the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Administration' menu is expanded, showing 'Network Resources' as the active section. Under 'Network Resources', 'Network Device Groups' is selected. The breadcrumb trail reads: 'Network Device Groups > All Device Types List > New Network Device Group'. The main content area is titled 'Network Device Groups' and contains the following fields:

- * Name: Meraki Wireless
- Description: (empty field)
- * Type: Device Type

At the bottom of the form are 'Submit' and 'Cancel' buttons. On the left side, there is a sidebar with a search bar and a tree view under 'Groups' containing 'All Device Types' and 'All Locations'.

Přidání konkrétního Access Pointu do skupiny. Jelikož tato konfigurace slouží pro provoz ISE v RADIUS proxy režimu není nutné nastavovat RADIUS parametry. Adresa 192.168.43.190 je v našem případě lokální adresa přístupového prvku Meraki MR.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service PassiveID Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Network devices

Default Device

Network Devices List > Meraki_AP

Network Devices

* Name

Description

* IP Address: /

* Device Profile

Model Name

Software Version

* Network Device Group

Device Type

Location

▶ RADIUS Authentication Settings

▶ TACACS Authentication Settings

▶ SNMP Settings

▶ Advanced TrustSec Settings

Definice externího RADIUS serveru

RADIUS komunikace mezi sítí organizace a eduroam RADIUS servery musí být zabezpečena. eduroam podporuje metodu RadSec nebo IPsec v transparentním módu. My využijeme RadSec.

Způsob autentizace je tedy: Meraki odesílá RADIUS zprávu na svůj definovaný AAA server (tj. ISE), ISE v režimu RADIUS proxy posílá dále na radsecproxy službu, kde dojde k zabezpečenému odeslání RADIUS zprávy na národní RADIUS server. Analogicky probíhá komunikace zpět (eduroam RADIUS → radsecproxy → ISE → Meraki AP).

ISE pracuje v režimu RADIUS proxy, tj. radsecproxy instance je pro ISE externí RADIUS server. Vlastní zabezpečená komunikace mezi radsecproxy a eduroam RADIUS je již pro ISE plně transparentní.

Protože ISE je pro přístupové prvky sítě RADIUS proxy server, fungující oproti externímu RADIUS serveru (zde radsecproxy instance) je potřeba tento externí server (radsecproxy) nakonfigurovat:

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > External RADIUS Servers. The page title is "External RADIUS Servers List > radsec". The main heading is "External RADIUS Server". The configuration form includes the following fields and controls:

- * Name: radsec
- Description: (empty text area)
- * Host IP: 192.168.43.52
- * Shared Secret: (masked with dots) [Show]
- Enable KeyWrap: [i]
- * Key Encryption Key: (masked) [Show]
- * Message Authenticator Code Key: (masked) [Show]
- Key Input Format: ASCII HEXADECIMAL
- * Authentication Port: 1812 (Valid Range 1 to 65535)
- * Accounting Port: 1813 (Valid Range 1 to 65535)
- * Server Timeout: 5 Seconds (Valid Range 5 to 120)
- * Connection Attempts: 3 (Valid Range 1 to 9)

At the bottom of the form are "Save" and "Reset" buttons.

V našem případě používáme instanci radsecproxy běžící na adrese 192.168.43.52. Tento server spuštěný např. s parametry:

```
/usr/local/sbin/radsecproxy -d 3
```

přebírá proxyované RADIUS požadavky od ISE a v zabezpečené formě je odesílá na RADIUS server eduroam.

Autentizace

V ISE lze pracovat s tzv. Policy Sets. Tento koncept zjednodušuje a zpřehledňuje konfiguraci, zvláště pokud provádíme více typů autentizačních a autorizačních služeb pro různé typy přístupů.

Před konfigurací autentizačních a autorizačních pravidel si tedy jedním tlačítkem zapneme používání Policy Sets:

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Settings. The 'Policy Sets' configuration page is displayed, showing two radio buttons: 'Disabled' and 'Enabled'. The 'Enabled' radio button is selected. Below the radio buttons are 'Save' and 'Reset' buttons. A left-hand navigation menu lists various settings categories: Client Provisioning, FIPS Mode, Alarm Settings, Posture, Profiling, Protocols, Proxy, SMTP Server, SMS Gateway, System Time, Policy Sets, ERS Settings, Smart Call Home, and DHCP & DNS Services.

Nyní již můžeme kliknout na volbu „Policy Sets“:

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Policy Sets. The 'Policy Sets' configuration page is displayed. There is a search bar with the text 'Search policy names & descriptions.' and a magnifying glass icon. Below the search bar are buttons for adding, deleting, and refreshing the list. The 'Access Policy Sets' section shows a summary of the defined policy sets and a link to 'Administration' for policy export. A table with columns 'Status' and 'Name' is visible at the bottom.

Tímto se nám zobrazí nabídka pro vytváření vlastních autentizačních a následně i autorizačních pravidel. Vytvoříme si nový Policy Set, zda nazvaný DOT1X. Tento rozklikneme a nastavíme autentizační pravidla. Tj. jakým způsobem bude prováděna autentizace přístupujících zařízení.

Pravidla autentizačních politik mohou být velmi exaktní. Přesně lze nastavit kde je jaký typ přístupu do sítě ověřován. V našem případě si můžeme podmínku jednoduše vytvořit na základě parametrů ve jménu uživatele: pokud je obsažen znak „@“ a není následován lokální doménou odesíláme autentizační požadavek na „Identity Sekvenci“ eduroam, tj. náš externí RADIUS server – radsecproxy.

Poznámka: Authentication Policy *meraki.cesnet.cz* je třeba nahradit realmem organizace.
Příklad - <název.školy>.cz

The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring Policy Sets. The left sidebar shows a list of policy sets, including 'DOT1X' and 'Default'. The main area displays the configuration for the 'DOT1X' policy set, which is defined by the following rules:

Status	Name	Description	Conditions	Permissions
✓	DOT1X		DEVICE:Device Type EQUALS Device Type#All Device Types	Edit
Authentication Policy				
✓	eduroam - externi org		If Radius:User-Name CONTAINS @ AND Radius:User-Name NOT ENDS WITH @meraki.cesnet.cz	Use Proxy Service : eduroam Edit
✓	Default Rule (If no match)		Allow Protocols : Default Network Access and use : All_User_ID_Stores	Edit
Authorization Policy				
Exceptions (0)				
Standard				
Status	Rule Name	Conditions (identity groups and other conditions)	Permissions	
✓	Default	if no matches, then	PermitAccess	Edit

Logování

Úspěšné připojení na Meraki AP je v ISE logováno takto:

The screenshot shows the 'Overview' section of a log entry in Cisco ISE. The event details are as follows:

Field	Value
Event	5200 Authentication succeeded
Username	ba8ee@cesnet.cz
Endpoint Id	7C:01:91:16:AB:C7
Endpoint Profile	Apple-Device
Authentication Policy	DOT1X >> eduroam - externi org
Authorization Policy	DOT1X >> Default
Authorization Result	PermitAccess

Authentication Details

Source Timestamp 2016-08-30 17:25:00.716

Received Timestamp 2016-08-30 17:25:00.725

Policy Server ise21vm

Event 5200 Authentication succeeded

Username ba8ee@cesnet.cz

Endpoint Id 7C:01:91:16:AB:C7

Calling Station Id 7C-01-91-16-AB-C7

Endpoint Profile Apple-Device

Identity Group Profiled

Network Device AP

Device Type All Device Types

Location All Locations

NAS IPv4 Address 192.168.43.190

NAS Port Type Wireless - IEEE 802.11

Authorization Profile PermitAccess

Response Time 517

Other Attributes

ConfigVersionId	66
DestinationPort	1812
Protocol	Radius
UseCase	Proxy
NAS-Port	0
Framed-MTU	1400
VendorSpecific	00:00:73:e7:01:13:38:38:3a:31:35:3a:34:34:3a:61:38:3a:30:61:3a:34:34
Proxy-State	FirstProxy=192.168.43.54
Acct-Session-Id	A8197AB8-0000001B
Connect-Info	CONNECT 0Mbps 802.11b
undefined-186	◆
undefined-187	◆
undefined-188	◆
MS-MPPE-Send-Key	****
MS-MPPE-Recv-Key	****
NetworkDeviceProfileName	Cisco
NetworkDeviceProfileId	403ea8fc-7a27-41c3-80bb-27964031a08d
IsThirdPartyDeviceFlow	false
SSID	8E-15-54-A8-0A-44:eduroam-meraki
AcsSessionID	ise21vm/261937984/2387
AuthorizationPolicyMatchedRule	Default
CPMSessionID	c0a82b361kV4LNTwdTNpGUr7EGo0W0NbzjQL6tTyIDAaOXJcMwo
EndPointMACAddress	7C-01-91-16-AB-C7
ISEPolicySetName	DOT1X
AllowedProtocolMatchedRule	eduroam - externi org
HostIdentityGroup	Endpoint Identity Groups:Profiled
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types
RADIUS Username	ba8ee@cesnet.cz
Device IP Address	192.168.43.190
Called-Station-ID	8E-15-54-A8-0A-44:eduroam-meraki

Steps

11001 Received RADIUS Access-Request
11017 RADIUS created a new session
11117 Generated a new session ID for a 3rd party NAD
15049 Evaluating Policy Group
15008 Evaluating Service Selection Policy
15048 Queried PIP - DEVICE.Device Type
15048 Queried PIP - Radius.User-Name
15004 Matched rule - eduroam - externi org
11358 Received request for RADIUS server sequence.
11361 Valid incoming authentication request
11355 Start forwarding request to remote RADIUS server
11365 Modify attributes before sending request to external radius server
11100 RADIUS-Client about to send request - (port = 1812)
11101 RADIUS-Client received response
11357 Successfully forwarded request to current remote RADIUS server
24423 ISE has not been able to confirm previous successful machine authentication
15036 Evaluating Authorization Policy
15004 Matched rule - Default
15016 Selected Authorization Profile - PermitAccess
11002 Returned RADIUS Access-Accept