

Configuration Radius NPS pour l'authentification 802.1x via EAP-TLS

Cette documentation détaille la configuration du rôle NPS (Network Policy Server) sous Windows Server 2022 afin d'authentifier les utilisateurs ou ordinateurs au réseau Wifi. On peut également l'adapter pour la connexion filaire (non détaillée ici).

Parmi les méthodes d'authentification, le PEAP-TLS est la méthode la plus sécurisée, mais rarement supportée. De plus, elle chiffre la communication de la clé publique, qui n'a pas trop de sens.

Authentication Methods	RADIUS NPS Server	Requirements for Client	Security Level
PAP	N/A	Username and Password	Least Safe
CHAP	N/A	Username and Password	Unsafe
MS-CHAP-v2	N/A	Username and Password	Unsafe
EAP-MS-CHAP-v2	N/A	Username and Password	Unsafe
PEAP-MSCHAP-v2	Computer Certificate	Username and Password	Safe
EAP-TLS	Computer Certificate	User Certificate	Safer
PEAP-TLS	Computer Certificate	User Certificate	The safest

Vous trouverez plus d'informations ici : [Protocole EAP \(Extensible Authentication Protocol\) pour l'accès réseau dans Windows | Microsoft Learn](#)

Après l'installation du rôle NPS, on définit la stratégie réseau comme ceci :

NPS (Local)
RADIUS Clients and Servers
Policies
Connection Request Policies
Network Policies
Accounting
Templates Management

Network Policies

Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
EAP-TLS	Enabled	1	Grant Access	Non spécifié
Connexions au serveur Microsoft de Routage et Accès distants	Disabled	999998	Deny Access	Non spécifié
Connexions à d'autres serveurs d'accès	Disabled	999999	Deny Access	Non spécifié

EAP-TLS

Conditions - If the following conditions are met:

Condition	Value
Authentication Type	EAP
NAS Port Type	Sans fil - IEEE 802.11
Machine Groups	AD\Ordinateurs du domaine

Propriétés de EAP-TLS

Vue d'ensemble
Conditions
Contraintes
Paramètres

Nom de la stratégie :
EAP-TLS

État de la stratégie

Si la stratégie est activée, le serveur NPS l'évalue lors de l'autorisation. Si elle est désactivée, le serveur NPS ne l'évalue pas.

☒ Stratégie activée

Autorisation d'accès

Si la demande de connexion répond aux conditions et contraintes de la stratégie réseau, celle-ci peut soit accorder l'accès, soit le refuser. [Qu'est-ce qu'une autorisation d'accès ?](#)

☒ Accorder l'accès. Accorder l'accès si la demande de connexion correspond à cette stratégie.
☐ Refuser l'accès. Refuser l'accès si la demande de connexion correspond à cette stratégie.
☐ Ignorer les propriétés de numérotation des comptes d'utilisateurs.

Si la demande de connexion répond aux conditions et contraintes de cette stratégie réseau, et si la stratégie accorde l'accès, l'autorisation est basée uniquement sur la stratégie réseau ; les propriétés de numérotation des comptes d'utilisateurs ne sont pas évaluées.

Méthode de connexion réseau

Sélectionnez le type de serveur d'accès réseau qui envoie la demande de connexion au serveur NPS. Vous pouvez sélectionner une valeur dans Type de serveur d'accès réseau ou bien Spécifique au fournisseur, mais ces paramètres ne sont pas obligatoires. Si votre serveur d'accès réseau est un commutateur d'authentification ou un point d'accès sans fil 802.1X, sélectionnez Non spécifié.

☒ Type de serveur d'accès réseau :

Non spécifié

☐ Spécifique au fournisseur :




10

OK
Annuler
Appliquer

Overview Conditions Constraints Settings

Configure the conditions for this network policy.

If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.

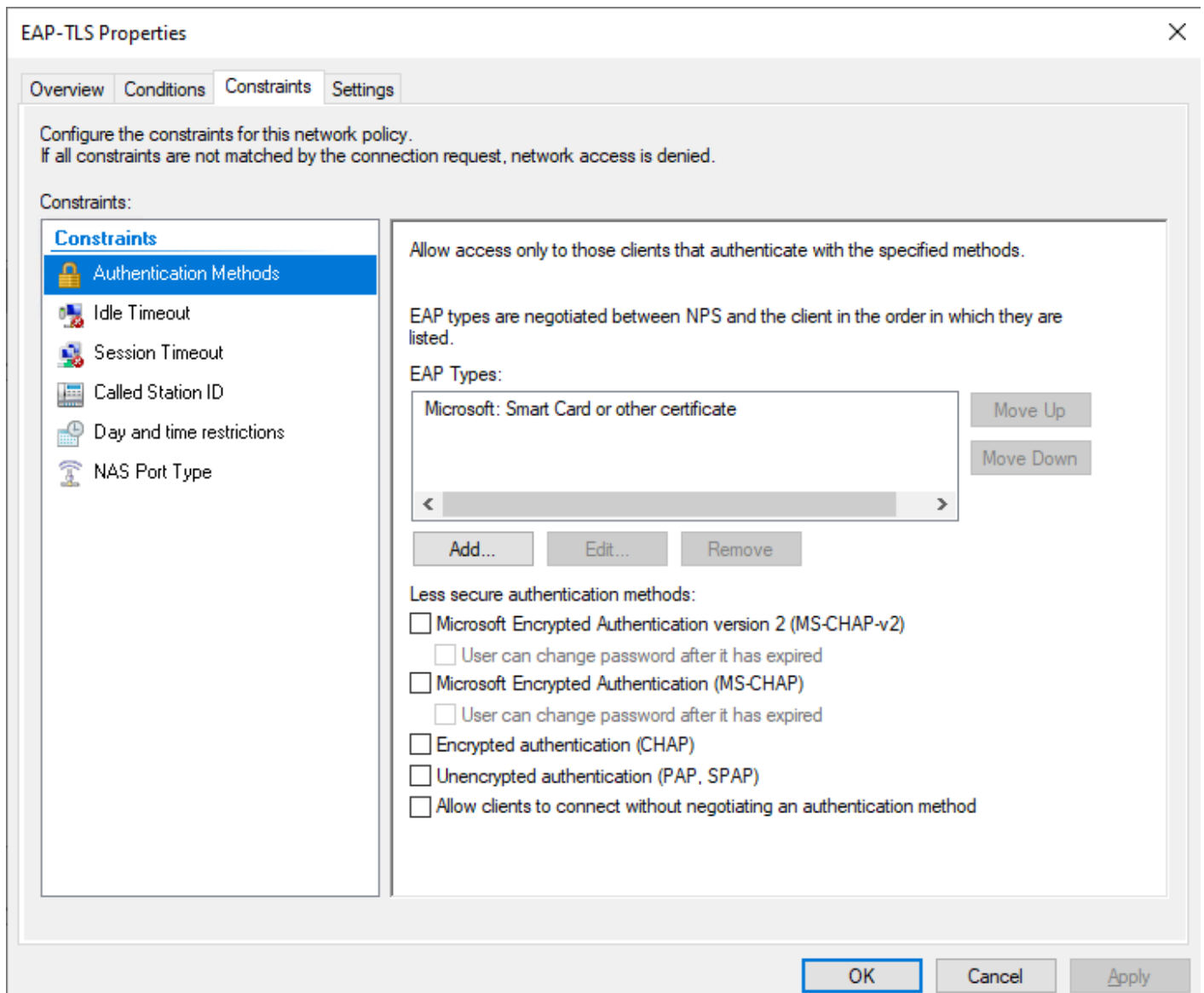
Condition	Value
 Authentication Type	EAP
 NAS Port Type	Sans fil - IEEE 802.11
 Machine Groups	AD\Ordinateurs du domaine

Condition description:
The Machine Groups condition specifies that the connecting computer must belong to one of the selected groups.

Add... Edit... Remove

OK Cancel Apply

Le "TLS" de "EAP-TLS" correspond à "Microsoft: Smart Card or other certificate".



On clique sur "Microsoft: Smart Card or other certificate" et "Modifier..." :

Sélectionnez le certificat que le serveur doit utiliser comme preuve de son identité auprès du client. Un certificat configuré pour EAP Protégé dans la stratégie de demande de connexion remplacera ce certificat.

Certificat délivré à : SRV-APP35-01.ad.khroners.fr

Nom convivial : SRV-APP35-01.ad.khroners.fr

Émetteur : Khroners Labs Enterprise CA

Date d'expiration : 02/10/2024 07:28:44

☒ Activer la reconnexion rapide

☐ Déconnecter les clients sans chiffrement forcé

Types EAP

Carte à puce ou autre certificat

Monter

Descendre

Ajouter

Modifier

Supprimer

OK

Annuler

Cela correspond au PEAP-TLS (ou également dit PEAP-EAP-TLS).

Vue d'ensemble Conditions **Contraintes** Paramètres

Configurez les contraintes de cette stratégie réseau.
Si la demande de connexion ne répond pas à toutes les contraintes, l'accès réseau est refusé.

Contraintes :

Contraintes

- Méthodes d'authentification
- Délai d'inactivité
- Délai d'expiration de session
- ID de la station appelée
- Restrictions relatives aux jours et aux heures
- Type de port NAS**

Spécifier les types de médias d'accès nécessaires pour correspondre à cette stratégie

Types de tunnels pour connexions d'accès à distance et VPN standard

- ☐ Asynchrone (Modem)
- ☐ RNIS synchrone
- ☐ Synchrone (ligne T1)
- ☐ Virtuel (VPN)

Types de tunnels pour connexions 802.1X standard

- ☐ Ethernet
- ☐ FDDI
- ☒ Sans fil - IEEE 802.11
- ☐ Token Ring

Autres

- ☐ ADSL-CAP - Modulation de phase d'amplitude sans porteuse DSL asymétrique
- ☐ ADSL-DMT - Multi-tonalité discrète DSL asymétrique
- ☐ Asynchrone (Modem)
- ☐ Câble

OK Annuler Appliquer

Dans mon cas, j'ai dû ajouter l'attribut "Framed-MTU" avec une valeur de 1344, car j'ai l'erreur suivante :

Authentication failed due to an EAP session timeout; the EAP session with the access client was incomplete.

Vous pouvez observer les logs dans l'observateur d'événements, sous "Affichages Personnalisés" > "Rôles de serveurs" > Services de stratégie et d'accès réseau".

Observateur d'événements (Local) Services de stratégie et d'accès réseau Nombre d'événements : 35 (1) Nouveaux événements disponibles

Rôles de serveurs

- Serveur Web (IIS)
- Services Bureau à distance
- Services de stratégie et d'accès réseau
- Services WSUS (Windows Update Services)
- Événements d'administration
- Journaux Windows
- Journaux des applications et services
- Abonnements

Nombre d'événements : 35

Niveau	Date et heure	Source	ID de l'événement	Catégorie
Information	03/10/2023 19:33:20	Micros...	6273	Networ...
Information	03/10/2023 19:33:18	Micros...	6274	Networ...
Information	03/10/2023 19:33:17	Micros...	6274	Networ...
Information	03/10/2023 19:33:13	Micros...	6274	Networ...
Information	03/10/2023 19:33:12	Micros...	6274	Networ...

Événement 6274, Microsoft Windows security auditing.

Général Détails

Nom convivial du client : IAP-315-01
Adresse IP du client : 10.35.30.1

Informations détaillées de l'authentification :

Nom de stratégie de demande de connexion : Utiliser l'authentification Windows pour tous les utilisateurs
Nom de stratégie réseau : -
Fournisseur d'authentification : Windows
Serveur d'authentification : SRV-APP35-01.ad.khroners.fr
Type d'authentification : -
Type EAP : -
Identificateur de session de compte : -
Code raison : 96
Raison : L'authentification a échoué en raison d'un dépassement du délai d'expiration de la session EAP ; la session EAP avec le client d'accès était incomplète.

Propriétés de EAP-TLS

Vue d'ensemble Conditions Contraintes Paramètres

Configurez les paramètres de cette stratégie réseau.
Si la demande de connexion répond aux conditions et contraintes, et si la stratégie accorde l'accès, les paramètres sont appliqués.

Paramètres :

Attributs RADIUS

Standard

Spécifiques au fournisseur

Routage et accès à distance

Liaisons multiples et protocole BAP (Bandwidth Allocation Protocol)

Filtres IP

Chiffrement

Paramètres IP

Pour envoyer des attributs supplémentaires aux clients RADIUS, sélectionnez un attribut RADIUS standard, puis cliquez sur Modifier. Si vous ne configurez pas d'attribut, celui-ci n'est pas envoyé aux clients RADIUS. Consultez la documentation de votre client RADIUS pour connaître les attributs nécessaires.

Attributs :

Nom	Valeur
Framed-MTU	1344
Framed-Protocol	PPP
Service-Type	Framed

Ajouter... Modifier... Supprimer

OK Annuler Appliquer

On ajoute également le(s) client(s) RADIUS en définissant un secret partagé.

Dans les bornes wifi, on choisit WPA2 Entreprise (ou WPA3 Entreprise si supporté), en renseignant l'adresse IP du serveur NPS et le secret partagé.

Revision #6

Created 5 October 2023 20:12:59 by Khroners

Updated 24 October 2023 20:31:17 by Khroners