

Configurer les paramètres du serveur RADIUS (Remote Authentication Dial-In User Service) sur un commutateur

Objectif

RADIUS (Remote Authentication Dial-In User Service) est un protocole réseau qui fournit une gestion centralisée AAA (Authentication, Authorization and Accounting) pour les utilisateurs qui se connectent et utilisent un service réseau. Un serveur RADIUS régule l'accès au réseau en vérifiant l'identité des utilisateurs à l'aide des identifiants de connexion saisis. Par exemple, un réseau Wi-Fi public est installé sur un campus universitaire. Seuls les étudiants disposant du mot de passe peuvent accéder à ces réseaux. Le serveur RADIUS vérifie les mots de passe entrés par les utilisateurs et autorise ou refuse l'accès, le cas échéant.

La configuration d'un serveur RADIUS permet d'améliorer la sécurité car il s'authentifie avant d'autoriser un client ou un utilisateur à accéder au réseau. Le serveur RADIUS répond aux problèmes des clients liés à la disponibilité du serveur, à la retransmission et aux délais d'attente. Le serveur RADIUS traite également les demandes de connexion des utilisateurs, authentifie l'utilisateur et envoie les informations de configuration nécessaires au client pour fournir des services à l'utilisateur.

Le serveur RADIUS est un serveur qui centralise le contrôle d'un réseau constitué de périphériques compatibles RADIUS. Les serveurs RADIUS ont basé leurs décisions de transfert sur des adresses 802.1X ou MAC (Media Access Control).

Cet article explique comment configurer les paramètres RADIUS sur les commutateurs des gammes Sx350, SG350X et Sx550X.

Périphériques pertinents

- Gamme Sx350
- Gamme SG350X
- Gamme Sx550X

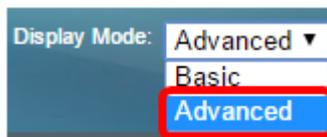
Version du logiciel

- 2.2.5.68

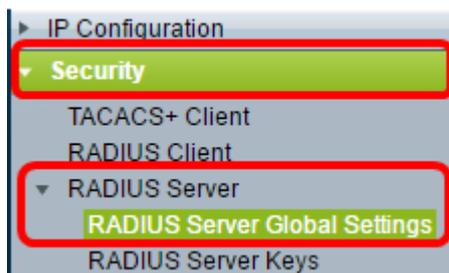
Configuration des paramètres du serveur RADIUS

Configuration des paramètres globaux du serveur RADIUS

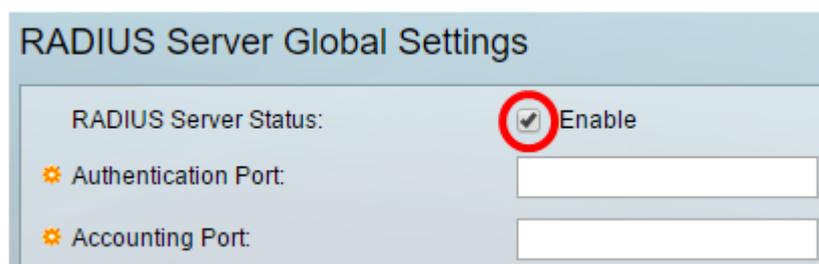
Étape 1. Connectez-vous à l'utilitaire Web du commutateur et sélectionnez **Avancé** dans la liste déroulante Mode d'affichage.



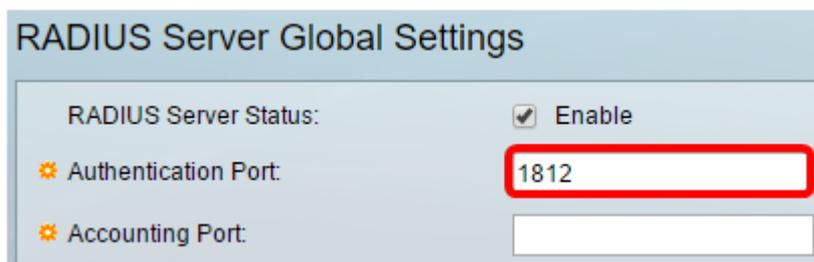
Étape 2. Choisissez **Security** > **RADIUS Server** > **RADIUS Server Global Settings**.



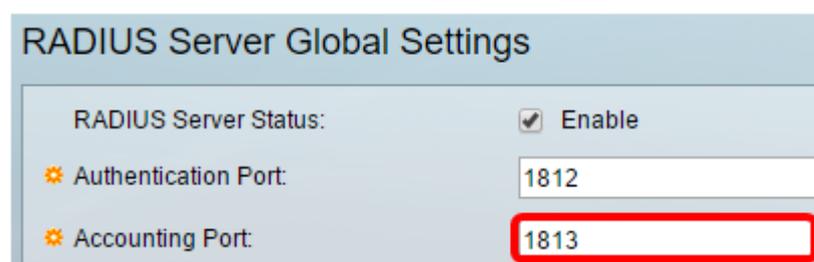
Étape 3. Cochez la case **Activer** pour l'état du serveur RADIUS.



Étape 4. Entrez le numéro de port UDP (User Datagram Protocol) du port du serveur RADIUS pour les demandes d'authentification. La plage est comprise entre 1 et 65535 et la valeur par défaut est 1812.



Étape 5. Entrez le numéro de port UDP du port serveur RADIUS pour les demandes de comptabilité. La plage est comprise entre 1 et 65535 et la valeur par défaut est 1813.



Étape 6. (Facultatif) Pour générer des interruptions pour les événements de comptabilité RADIUS, cochez la case **Activer** pour les interruptions de comptabilité RADIUS sous Paramètres de déroutement.



Étape 7. (Facultatif) Pour générer des interruptions pour les connexions ayant échoué, cochez la case **Activer** pour les interruptions d'échec d'authentification RADIUS.



Étape 8. (Facultatif) Pour générer des interruptions pour les connexions ayant réussi, cochez la case **Activer** pour les interruptions de réussite de l'authentification RADIUS.

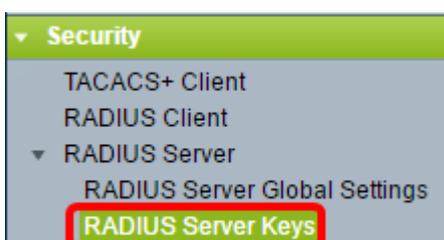


Étape 9. Cliquez sur Apply.

Étape 10. Une  icône indique que la configuration a été enregistrée avec succès. Pour enregistrer définitivement la configuration, accédez à la page Opérations de fichiers ou cliquez sur l'  Save icône située dans la partie supérieure de la page. Sinon, cliquez sur **Fermer**.

Configurer les clés du serveur RADIUS

Étape 1. Choisissez **RADIUS Server Keys** sous RADIUS Server.



Étape 2. (Facultatif) Saisissez la clé RADIUS par défaut si nécessaire. Les valeurs entrées dans la clé par défaut sont appliquées à tous les serveurs configurés (dans la page Ajouter un serveur RADIUS) pour utiliser la clé par défaut.

RADIUS Server Keys

Default Key: Keep existing default key
 Encrypted
 Plaintext (0/128 characters used)

MD5 Digest: bed128365216c019988915ed3add75fb

Default Key - Choisissez la chaîne de clé par défaut que vous voulez utiliser pour l'authentification et le chiffrement entre le périphérique et le client RADIUS. Les options sont les suivantes :

- Conserver la clé par défaut existante : pour les serveurs spécifiés, le périphérique tente d'authentifier le client RADIUS à l'aide de la chaîne de clé par défaut existante.
- Encrypted : pour chiffrer les communications à l'aide de l'algorithme MD5 (Message Digest 5), saisissez la clé sous forme chiffrée.
- Texte clair : saisissez la chaîne de clé en mode texte clair.

MD5 Digest - Affiche le MD5 Digest du mot de passe saisi par l'utilisateur.

Note: Dans cet exemple, Conservez la clé par défaut existante sous Clé par défaut est sélectionné.

Étape 3. Cliquez sur Apply.

Étape 4. Une  icône indique que la configuration a été enregistrée avec succès. Pour enregistrer définitivement la configuration, accédez à la page Opérations de fichiers ou cliquez sur l'  icône située dans la partie supérieure de la page.

Étape 5. (Facultatif) Sous la zone Table des clés secrètes, cliquez sur le bouton **Ajouter** pour ajouter une clé secrète.

Secret Key Table

NAS Address	Secret Key's MD5
0 results found.	

Étape 6. Entrez l'adresse IP du NAS ou du commutateur qui contient le client RADIUS dans le champ *NAS Address*.

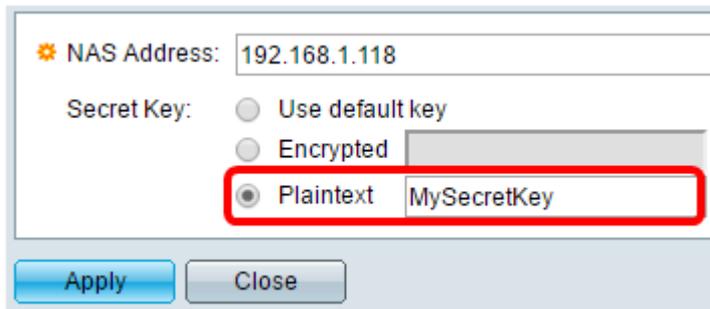
Note: Dans l'image ci-dessous, 192.168.1.118 est utilisé comme exemple d'adresse IP.

NAS Address:

Secret Key: Use default key
 Encrypted
 Plaintext

Étape 7. Choisissez votre clé secrète préférée.

Note: Dans l'image ci-dessous, le texte clair est choisi comme exemple.



Les options sont les suivantes :

- Use default key : pour les serveurs spécifiés, le périphérique tente d'authentifier le client RADIUS à l'aide de la chaîne de clé par défaut existante.
- Encrypted : pour chiffrer les communications à l'aide de MD5, entrez la clé sous forme chiffrée.
- Texte clair : saisissez la chaîne de clé en mode texte clair. Vous pouvez saisir jusqu'à 128 caractères.

Étape 8. Cliquez sur Apply.

Étape 9. Une  icône indique que la configuration a été enregistrée avec succès. Pour enregistrer définitivement la configuration, accédez à la page Opérations de fichiers ou cliquez sur l'  icône située dans la partie supérieure de la page. Sinon, cliquez sur Fermer.

Configurer les groupes de serveurs RADIUS

Les groupes de serveurs RADIUS sont un groupe d'utilisateurs qui utiliseront le périphérique comme serveur RADIUS. Pour configurer un groupe, suivez les instructions ci-dessous :

Étape 1. Sélectionnez **Groupes de serveurs RADIUS** sous Serveur RADIUS.



Étape 2. Cliquez sur le bouton **Ajouter** sous la table Groupe de serveurs RADIUS.



Étape 3. Dans la fenêtre contextuelle, saisissez un nom pour le groupe dans le champ *Nom du groupe*. Vous pouvez saisir jusqu'à 32 caractères.

Note: Dans l'image ci-dessous, GroupA1 est utilisé comme exemple.

Étape 4. Saisissez le niveau de privilège que vous souhaitez attribuer au groupe. Le niveau de privilège détermine le niveau d'accès que vous attribuerez à chaque groupe que vous avez créé. Vous pouvez définir les niveaux de 1 à 15. La valeur par défaut est 1.

Note: Dans cet exemple, 7 est utilisé.

- 1 (Accès CLI en lecture seule) : les utilisateurs du groupe ne peuvent pas accéder à l'interface utilisateur graphique et ne peuvent accéder qu'aux commandes CLI qui ne modifient pas la configuration du périphérique.
- 7 (Accès CLI en lecture/écriture limitée) : les utilisateurs du groupe ne peuvent pas accéder à l'interface utilisateur graphique et ne peuvent accéder qu'à certaines commandes CLI qui modifient la configuration du périphérique. Consultez le [Guide de référence de l'interface de ligne de commande](#) pour plus d'informations.
- 15 (Read/Write Management Access) : les utilisateurs du groupe peuvent accéder à l'interface utilisateur graphique et configurer le périphérique.

Étape 5. (Facultatif) Si vous souhaitez appliquer une plage de temps pour ce groupe, cochez la case **Activer** pour la plage de temps. Sinon, passez à l'[étape 15](#).

Group Name: (7/32 characters used)

Privilege Level: (Range: 1 - 15, Default: 1)

Time Range: Enable

Étape 6. Cliquez sur le lien **Edit** en regard de Time Range Name (Nom de la plage de temps) pour configurer les paramètres Time (Heure).

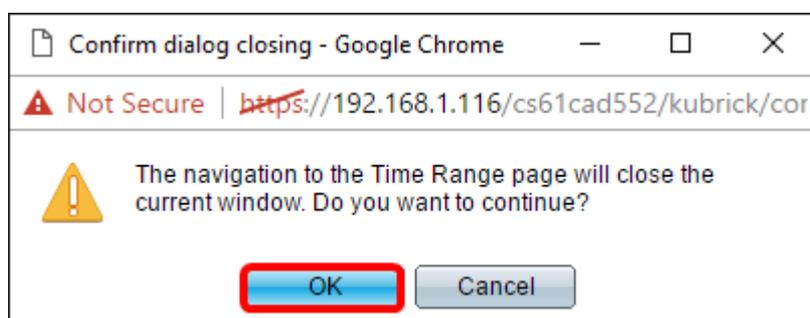
Group Name: (7/32 characters used)

Privilege Level: (Range: 1 - 15, Default: 1)

Time Range: Enable

Time Range Name:

Étape 7. Une fenêtre contextuelle s'affiche pour vous indiquer que la fenêtre actuelle sera fermée afin que vous puissiez continuer avec les paramètres de plage de temps. Cliquez OK.



Vous serez ensuite dirigé vers la page Plage de temps.

Étape 8. Cliquez sur le bouton **Ajouter** sous la table Plage de temps.

Time Range

Time Range Table			
<input type="checkbox"/>	Time Range Name	Absolute Starting Time	Absolute Ending Time
0 results found.			
<input checked="" type="button" value="Add..."/> <input type="button" value="Edit..."/> <input type="button" value="Delete"/>			

Étape 9. Entrez un nom pour l'intervalle de temps dans le champ *Nom de l'intervalle de temps*.

Note: Dans l'image ci-dessous, Reconnect est utilisé comme exemple.

Étape 10. Choisissez l'heure de début et de fin absolue de votre choix en cliquant sur la case d'option.

- Absolute Start Time : pour définir l'heure de début, choisissez l'une des options suivantes :
- Immédiat : sélectionnez cette option si vous souhaitez que la plage de temps démarre immédiatement.
- Date, Time : sélectionnez cette option si vous souhaitez spécifier la date et l'heure de début de la plage de temps.
- Absolute Ending Time : pour définir l'heure de début, choisissez l'une des options suivantes :
- Infinite : sélectionnez cette option si vous souhaitez que la plage de temps ne se termine jamais.
- Date, Time : sélectionnez cette option si vous souhaitez spécifier la date et l'heure de fin de la plage de temps.

Note: Dans cet exemple, la date et l'heure sont choisies.

Étape 11. Cliquez sur Apply.

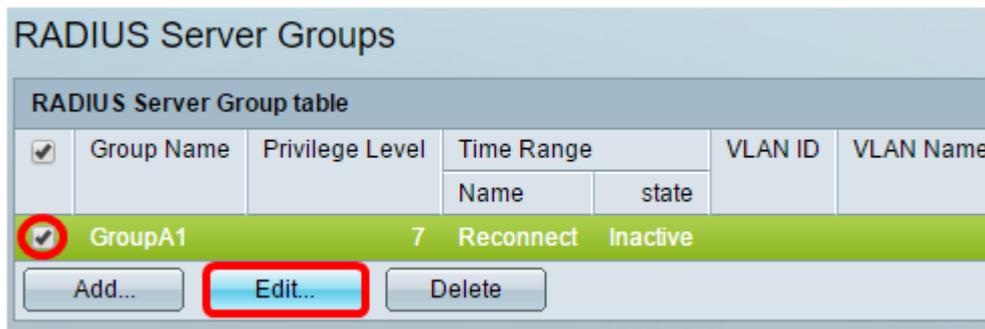
Étape 12. Une  icône indique que la configuration a été enregistrée avec succès. Pour enregistrer définitivement la configuration, accédez à la page Opérations de fichiers ou cliquez sur l'  icône située dans la partie supérieure de la page. Sinon, cliquez sur **Fermer**.

Vous serez ensuite dirigé vers la page principale.

Étape 13. Cliquez à nouveau sur **Groupes de serveurs RADIUS** sous Serveur RADIUS.



Étape 14. Le groupe nouvellement créé apparaîtra désormais dans la table Groupe de serveurs RADIUS. Cochez la case en regard du nom du groupe, puis cliquez sur **Modifier**.



Étape 15. (Facultatif) Sélectionnez le VLAN du groupe. Les options sont les suivantes :

- Aucun : aucun VLAN spécifié.
- VLAN ID : spécifiez un ID de VLAN.
- VLAN Name : spécifiez un nom de VLAN.

The screenshot shows the configuration form for a RADIUS Server Group. The fields are: Group Name: GroupA1 (dropdown); Privilege Level: 7 (text input, range 1-15, default 1); Time Range: Enable; Time Range Name: Reconnect (dropdown, with an 'Edit' link); VLAN: None, VLAN ID 8 (text input, range 1-4094), VLAN Name (text input, 0/32 characters used). At the bottom are 'Apply' and 'Close' buttons.

Note: Dans cet exemple, l'ID de VLAN 8 est utilisé.

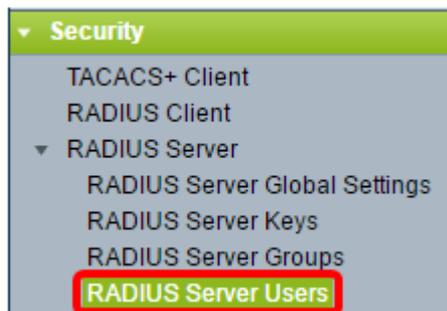
Étape 16. Cliquez sur Apply.

Étape 17. Une  icône indique que la configuration a été enregistrée avec succès. Pour enregistrer définitivement la configuration, accédez à la page Opérations de fichiers ou cliquez sur l'  icône située dans la partie supérieure de la page. Sinon, cliquez sur Fermer.

Configurer les utilisateurs du serveur RADIUS

Pour ajouter des utilisateurs au groupe précédemment créé :

Étape 1. Cliquez sur **Utilisateurs du serveur RADIUS** sous Serveur RADIUS.

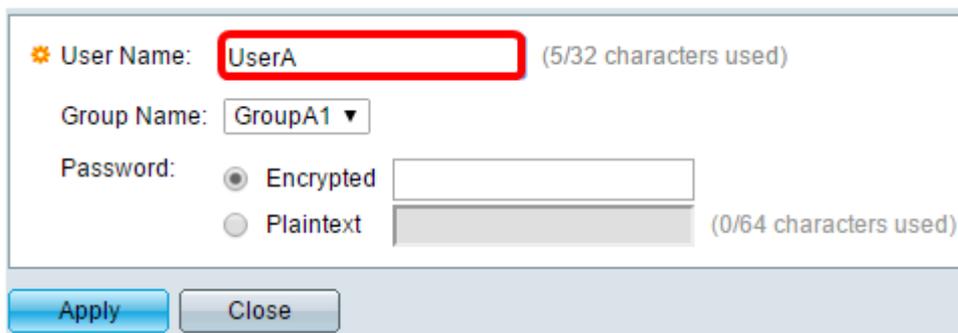


Étape 2. Cliquez sur le bouton **Ajouter** sous la table utilisateur RADIUS.

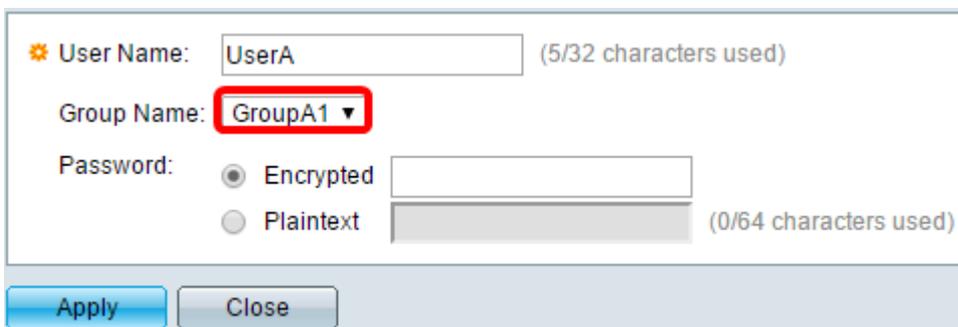


Étape 3. Entrez le nom de l'utilisateur dans le champ *Nom d'utilisateur*.

Note: Dans cet exemple, UserA est utilisé.

A screenshot of a user creation form. It contains the following fields: 'User Name:' with the value 'UserA' and '(5/32 characters used)' next to it; 'Group Name:' with a dropdown menu set to 'GroupA1'; and 'Password:' with two radio buttons: 'Encrypted' (selected) and 'Plaintext'. The 'Plaintext' option has '(0/64 characters used)' next to it. At the bottom, there are 'Apply' and 'Close' buttons. The 'User Name' input field is highlighted with a red rectangular box.

Étape 4. Sélectionnez le groupe auquel appartient l'utilisateur dans la liste déroulante Nom du groupe.

A screenshot of the same user creation form as in the previous step. The 'Group Name:' dropdown menu is now highlighted with a red rectangular box, and it shows 'GroupA1' as the selected option. All other elements, including the 'User Name' field, 'Password' options, and buttons, remain the same.

Étape 5. Sélectionnez une case d'option dans la zone Mot de passe.

Étape 6. Saisissez votre mot de passe préféré.

User Name: (5/32 characters used)

Group Name:

Password: Encrypted

Plaintext (9/64 characters used)

- Encrypted : une chaîne de clé est utilisée pour chiffrer les communications à l'aide de MD5. Pour utiliser le chiffrement, entrez la clé sous forme chiffrée.
- Texte clair : si vous n'avez pas de chaîne de clé chiffrée (provenant d'un autre périphérique), entrez la chaîne de clé en mode texte clair. La chaîne de clé chiffrée est générée et affichée.

Note: Dans cet exemple, Texte en clair est sélectionné.

Étape 6. Cliquez sur Apply.

Étape 7. Une  icône indique que la configuration a été enregistrée avec succès. Pour enregistrer définitivement la configuration, accédez à la page Opérations de fichiers ou cliquez sur l'  Save icône située dans la partie supérieure de la page. Sinon, cliquez sur **Fermer**.

Vous devez maintenant avoir correctement configuré les paramètres du serveur RADIUS sur votre commutateur.

©2016 Cisco Systems, Inc. Tous droits réservés.