Gestion de domaine sur RV220W et RV120W

Objectifs

Des domaines et les groupes sont utilisés pour rationaliser la Gestion des paramètres utilisateurs de VPN SSL. Au lieu de devoir spécifier des configurations pour chaque utilisateur individuellement, vous pouvez spécifier les configurations de domaine et de groupe une fois et alors affecter des utilisateurs aux groupes. Les configurations de domaine déterminent la méthode d'authentification. Un utilisateur peut ajouter un nouveau domaine aussi bien qu'éditer ou supprimer les domaines existants du domain list.

Ce document explique comment configurer la liste de domaines configurés sur le RV120W et le RV220W.

Périphériques applicables

- RV120W
- RV220W

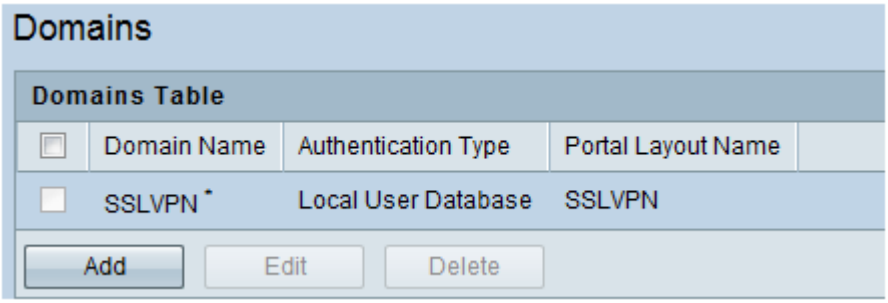
Version de logiciel

- v1.0.5.8

Configuration de domaine de gestion d'utilisateurs

Ajoutez un domaine

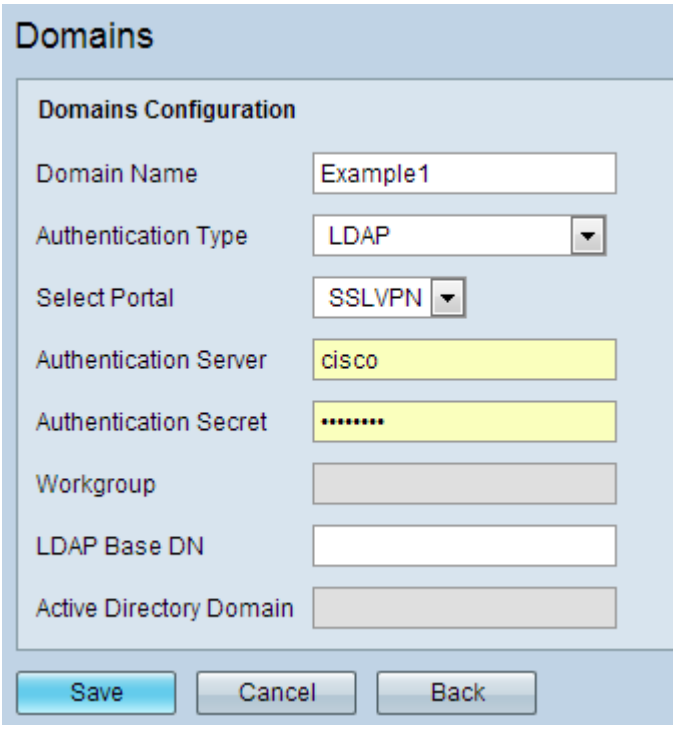
Étape 1. Ouvrez une session à l'utilitaire de configuration Web et choisissez la **gestion > la gestion des utilisateurs > les domaines**. La page de *domaines* s'ouvre :



Les informations suivantes peuvent être visualisées à cette page :

- Nom de domaine — Un identifiant unique pour le nom de domaine.
- Type d'authentification — Le type d'authentification pour le domaine créé.
- Nom portail d'affichage — L'affichage portail pour le domaine.

Étape 2. Cliquez sur Add **pour ajouter un nouveau domaine.** La page de *configuration de domaines* s'ouvre :



Étape 3. Écrivez le nom de domaine désiré à utiliser dans le domaine de *nom de domaine*.

Étape 4. Choisissez le type de serveur d'authentification à utiliser par le domaine de la liste déroulante de *type d'authentification*.

Les options sont décrites comme suit :

• Base de données locale des utilisateurs — Utilise la base de données utilisateur trouvée localement.

• RADIUS-PAP — Une implémentation de RADIUS où le client s'authentifie en envoyant un nom d'utilisateur et un mot de passe au serveur, que le serveur compare à sa base de données.

• RADIUS-CHAP — Une implémentation de RADIUS où le serveur envoie une chaîne aléatoirement générée au client, avec son adresse Internet. Le client utilise l'adresse Internet à la consultation la chaîne appropriée, la combine avec le défi, et chiffre la chaîne utilisant une fonction de hachage à sens unique. Le résultat est retourné au serveur pour confirmer avec l'adresse Internet du client.

• RADIUS-MSCHAP — L'implémentation de Microsoft de RADIUS-CHAP qui inclut une modification contrôlée par l'authentificateur de mot de passe et des mécanismes de relance d'authentification.

• RADIUS-MSCHAPv2 — La deuxième version de l'implémentation de Microsoft de RADIUS-CHAP qui inclut l'authentification mutuelle entre les pipi en couvrant un défi de pair.

• Domaine NT — Le Domaine NT est défini en ayant au moins un Primary Domain Controller (PDC) où toutes les informations relatives à la sécurité sont centralement continuées le rendre facile pour des administrateurs de mettre à jour. Dans un pair à scruter réseau aucun contrôleur de domaine, toutes les informations de compte utilisateur n'est gardé sur chaque machine cliente individuelle.

• Répertoire actif — Un service d'annuaire que Microsoft a développé pour des réseaux de

domaine windows. Le contrôleur de domaine authentifie et autorise tous les utilisateurs et les ordinateurs dans un domaine windows tapent le réseau, assignant et imposant des stratégies de sécurité et installer/mettant à jour le logiciel sur tous les ordinateurs.

• LDAP — Le Protocole LDAP (Lightweight Directory Access Protocol) est un protocole de service d'annuaire qui fonctionne sur une couche au-dessus de la pile TCP/IP. Il fournit un mécanisme utilisé pour se connecter à, pour rechercher, et modifier des répertoires d'Internet.

Étape 5. Choisissez le portail que les utilisateurs les utiliseront pour connecter de la liste déroulante *portaile choisie*. Seulement les utilisateurs des domaines associés avec certains portails peuvent employer ces portails pour ouvrir une session.

Remarque: Le portail SSLVPN est sélectionné par défaut. Pour des informations sur ajouter les affichages portaiux se réfèrent *configurant le serveur de VPN SSL* en *chapitre 5 du* guide d'admin.

Étape 6. Écrivez le nom du serveur utilisé pour authentifier des utilisateurs dans le *champ de serveur d'authentification*.

Étape 7. Entrez le mot de passe d'authentification pour accéder au serveur de domaine dans le domaine *secret d'authentification*.

Étape 8. (facultative) si l'*authentification de Domaine NT* était choisie dans l'étape 4, écrivent le nom ou l'ID du groupe de travail de NT dans le domaine de *groupe de travail*.

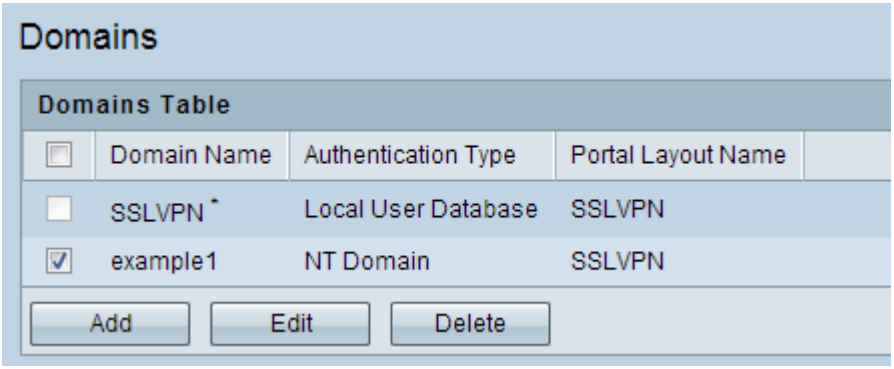
Étape 9. (facultative) si le *LDAP* était choisi dans l'étape 4, écrivent le nom de domaine de base dans le domaine de *DN de base de LDAP*.

Étape 10. (facultative) si le *Répertoire actif* était choisi dans l'étape 4, écrivent le nom de domaine actif de répertoire dans le *champ Domain de Répertoire actif*. Les utilisateurs qui sont enregistrés dans la base de données de Répertoire actif peuvent accéder au portail de VPN SSL.

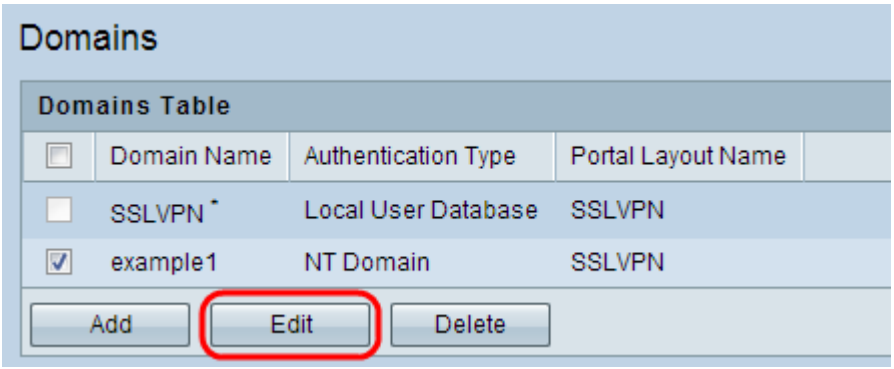
Étape 11. **Sauvegarde de** clic pour appliquer toutes les configurations.

Éditez un domaine

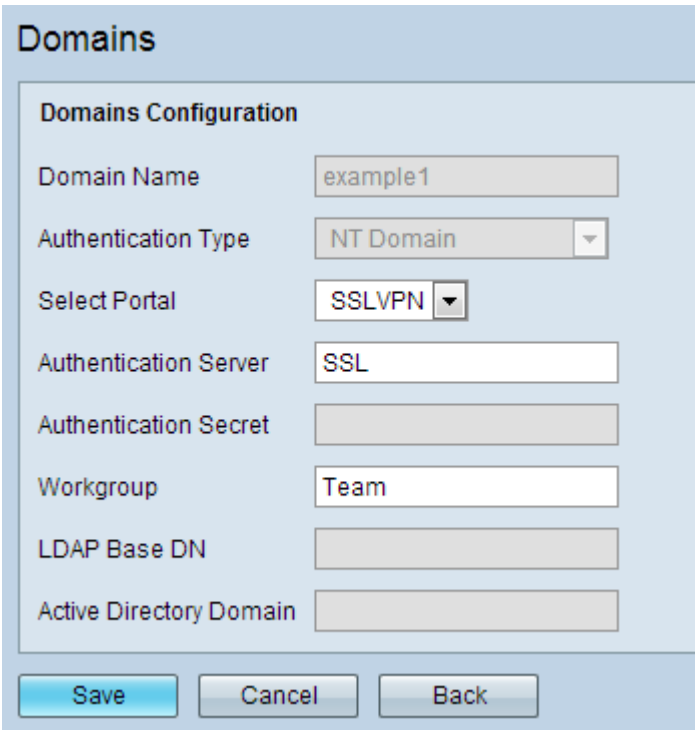
Étape 1. Ouvrez une session à l'utilitaire de configuration Web et choisissez la **gestion > la gestion des utilisateurs > les domaines**. La page de *domaines* s'ouvre :



Étape 2. Cochez la case de l'entrée désirée pour éditer.



Étape 3. Cliquez sur Edit **et la page de** *configuration de domaines* s'ouvre :



Étape 4. Écrivez le nom de domaine désiré à utiliser dans le domaine de *nom de domaine*.

Étape 5. Choisissez le type de serveur d'authentification à utiliser par le domaine de la liste déroulante de *type d'authentification*.

Les options sont décrites comme suit :

• Base de données locale des utilisateurs — Utilise la base de données utilisateur trouvée localement.

• RADIUS-PAP — Une implémentation de RADIUS où le client s'authentifie en envoyant un nom d'utilisateur et un mot de passe au serveur, que le serveur compare à sa base de données.

• RADIUS-CHAP — Une implémentation de RADIUS où le serveur envoie une chaîne aléatoirement générée au client, avec son adresse Internet. Le client utilise l'adresse Internet à la consultation la chaîne appropriée, la combine avec le défi, et chiffre la chaîne utilisant une fonction de hachage à sens unique. Le résultat est retourné au serveur pour confirmer avec l'adresse Internet du client.

• RADIUS-MSCHAP — L'implémentation de Microsoft de RADIUS-CHAP qui inclut une modification contrôlée par l'authentificateur de mot de passe et des mécanismes de

relance d'authentification.

• RADIUS-MSCHAPv2 — La deuxième version de l'implémentation de Microsoft de RADIUS-CHAP qui inclut l'authentification mutuelle entre les pipi en couvrant un défi de pair.

• Domaine NT — Le Domaine NT est défini en ayant au moins un Primary Domain Controller (PDC) où toutes les informations relatives à la sécurité sont centralement continuées le rendre facile pour des administrateurs de mettre à jour.

• Répertoire actif — Un service d'annuaire que Microsoft a développé pour des réseaux de domaine windows. Le contrôleur de domaine authentifie et autorise tous les utilisateurs et les ordinateurs dans un domaine windows tapent le réseau, assignant et imposant des stratégies de sécurité et installer/mettant à jour le logiciel sur tous les ordinateurs.

• LDAP — Le Protocole LDAP (Lightweight Directory Access Protocol) est un protocole de service d'annuaire qui fonctionne sur une couche au-dessus de la pile TCP/IP. Il fournit un mécanisme utilisé pour se connecter à, pour rechercher, et modifier des répertoires d'Internet.

Étape 6. Choisissez le portail que les utilisateurs les utiliseront pour connecter de la liste déroulante *portaile choisie*. Seulement les utilisateurs des domaines associés avec certains portails peuvent employer ces portails pour ouvrir une session.

Remarque: Le portail SSLVPN est sélectionné par défaut. Pour des informations sur ajouter les affichages portaiux se réfèrent *configurant le serveur de VPN SSL* en *chapitre 5 du* guide d'admin.

Étape 7. Écrivez le nom du serveur utilisé pour authentifier des utilisateurs dans le *champ de serveur d'authentification*.

Étape 8. Entrez le mot de passe d'authentification pour accéder au serveur de domaine dans le domaine *secret d'authentification*.

Étape 9. (facultative) si l'*authentification de Domaine NT* était choisie dans l'étape 5, écrivent le nom ou l'ID du groupe de travail de NT dans le domaine de *groupe de travail*.

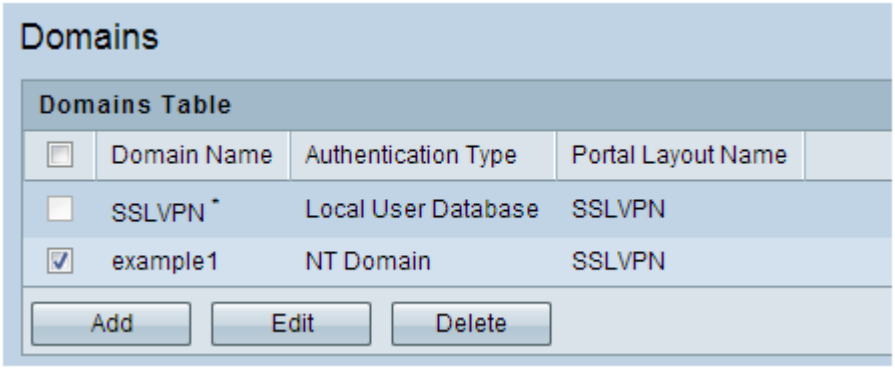
Étape 10. (facultative) si le *LDAP* était choisi dans l'étape 5, écrivent le nom de domaine de base dans le domaine de *DN de base de LDAP*.

Étape 11. (facultative) si le *Répertoire actif* était choisi dans l'étape 5, écrivent le nom de domaine actif de répertoire dans le *champ Domain de Répertoire actif*. Les utilisateurs qui sont enregistrés dans la base de données de Répertoire actif peuvent accéder au portail de VPN SSL.

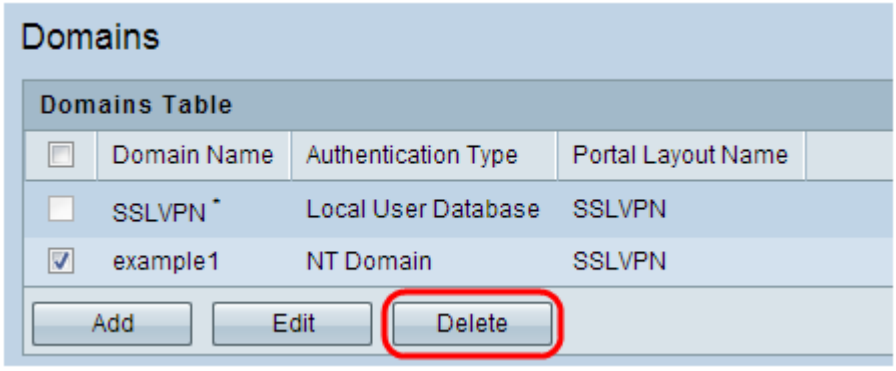
Étape 12. **Sauvegarde de** clic pour appliquer toutes les configurations.

Supprimez un domaine

Étape 1. Ouvrez une session à l'utilitaire de configuration Web et choisissez la **gestion > la gestion des utilisateurs > les domaines**. La page de *domaines* s'ouvre :



Étape 2. Cochez la case de l'entrée désirée pour supprimer.



Étape 3. Cliquez sur Delete. Le domaine est supprimé.