Configurazione della gestione di utenti e domini sui router VPN serie RV320 e RV325

Obiettivo

La pagina *Gestione utenti* viene utilizzata per configurare i domini e gli utenti. Un dominio è una sottorete costituita da un gruppo di client e server. L'autenticazione a un dominio è controllata da un server di sicurezza locale. La serie RV32x VPN Router supporta l'autenticazione tramite il database locale, un server RADIUS, un server Active Directory o un server LDAP.

Questo articolo spiega come gestire i domini e gli utenti sui router VPN serie RV32x.

Dispositivi interessati

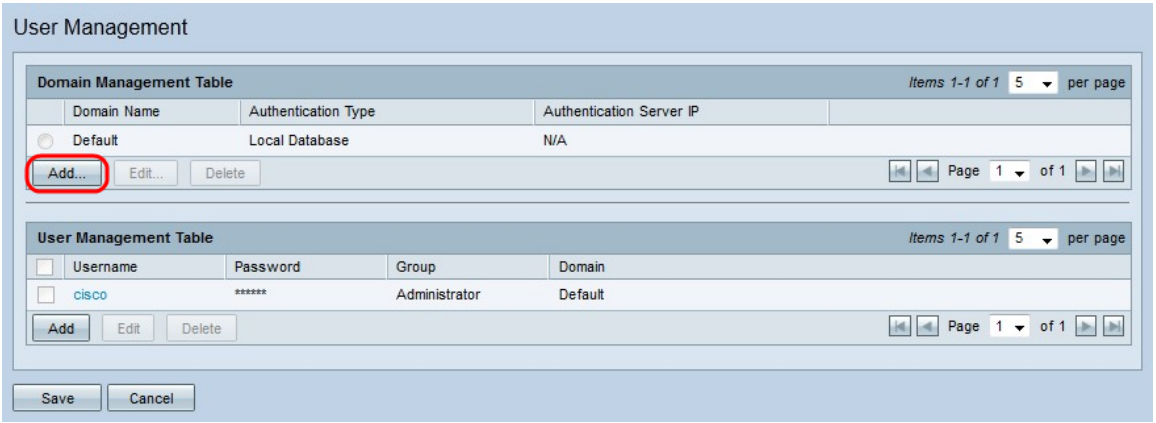
·RV320 Dual WAN VPN Router
· RV325 Gigabit Dual WAN VPN Router

Versione del software

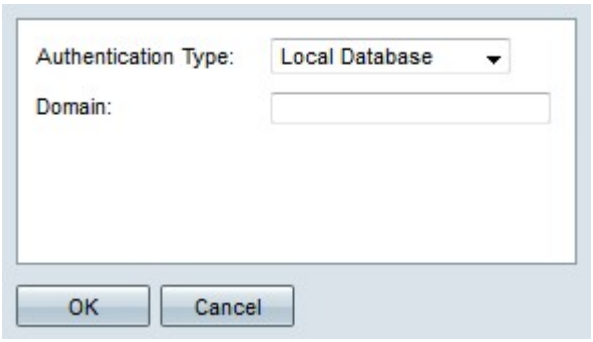
·v1.1.0.09

Gestione dei domini

Passaggio 1. Accedere all'utilità Configurazione Web e scegliere **Gestione utente**. Viene visualizzata la pagina *Gestione utente*:



Passaggio 2. Fare clic su **Add** nella tabella Domain Management per configurare un nuovo dominio. Viene visualizzata la finestra *Aggiungi dominio*.



Passaggio 3. Scegliere il tipo di autenticazione utilizzato per il dominio dall'elenco a discesa Tipo di autenticazione.

·Database locale: l'autenticazione viene eseguita dal router.

·RADIUS: un server RADIUS remoto esegue l'autenticazione per il dominio.

- RADIUS-PAP — Password Authentication Protocol (PAP) è un protocollo di autenticazione che utilizza solo una password semplice per l'autenticazione. Questa autenticazione è considerata non sicura e deve essere utilizzata solo se il server RADIUS remoto non supporta un metodo di autenticazione più avanzato.

- RADIUS-CHAP — Challenge Handshake Authentication Protocol (CHAP) è un protocollo di autenticazione che verifica l'autenticazione tramite un handshake a tre vie. Questo handshake viene eseguito al momento della connessione iniziale e a intervalli casuali dopo la connessione iniziale.

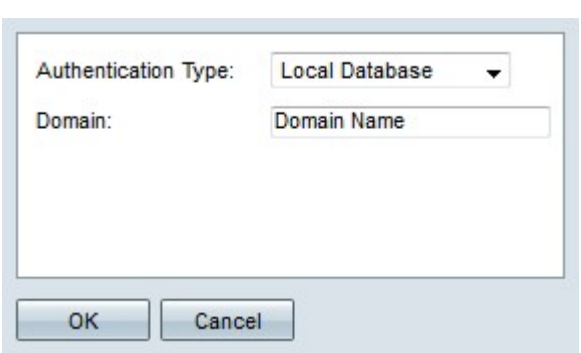
- RADIUS-MSCHAP — MS-CHAP è la versione Microsoft della protezione CHAP. Il formato MS-CHAP è stato progettato per essere compatibile con i prodotti Windows NT.

- RADIUS-MSCHAPV2 — MS-CHAPV2 è un'estensione di MS-CHAP che fornisce una chiave di crittografia più avanzata.

·Active Directory: un server che esegue Active Directory esegue l'autenticazione per il dominio. Active Directory è un servizio che fornisce protezione di rete su una rete di dominio Windows.

·LDAP - Un server remoto che esegue un servizio di directory esegue l'autenticazione per il dominio. Il protocollo LDAP (Lightweight Directory Access Protocol) è un protocollo di accesso utilizzato per accedere al servizio directory.

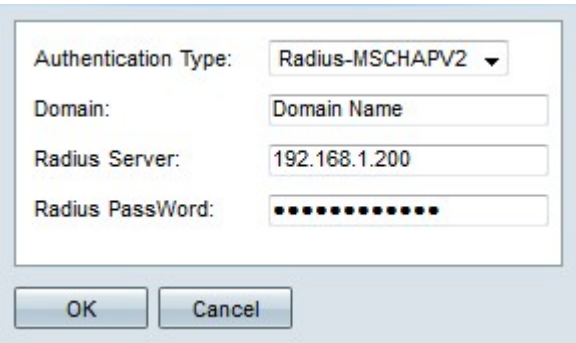
Autenticazione database locale



Passaggio 1. Immettere un nome per il dominio nel campo Dominio.

Passaggio 2. Fare clic su **OK**. Il dominio viene creato.

Autenticazione RADIUS



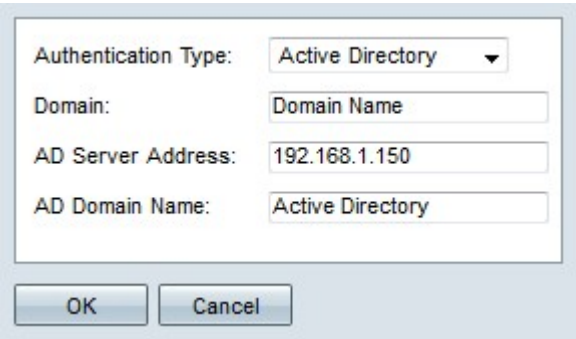
Passaggio 1. Immettere un nome per il dominio nel campo Dominio.

Passaggio 2. Immettere l'indirizzo IP del server RADIUS nel campo Server RADIUS.

Passaggio 3. Immettere la password utilizzata dal router per l'autenticazione al server RADIUS nel campo Radius PassWord. La password consente al router e al server RADIUS di crittografare le password e scambiare le risposte. Questo campo deve corrispondere alla password configurata nel server RADIUS.

Passaggio 4. Fare clic su **OK**. Il dominio viene creato.

Autenticazione di Active Directory



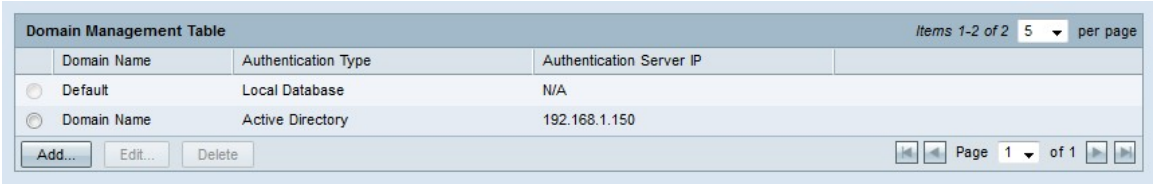
Passaggio 1. Immettere un nome per il dominio nel campo Dominio.

Passaggio 2. Immettere l'indirizzo IP del server Active Directory nel campo Indirizzo server AD.

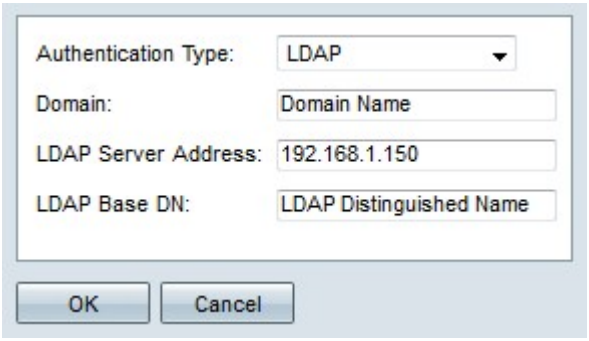
Passaggio 3. Immettere il nome di dominio del server Active Directory nel campo Nome

dominio Active Directory.

Passaggio 4. Fare clic su **OK**. Il dominio viene creato.



Autenticazione LDAP

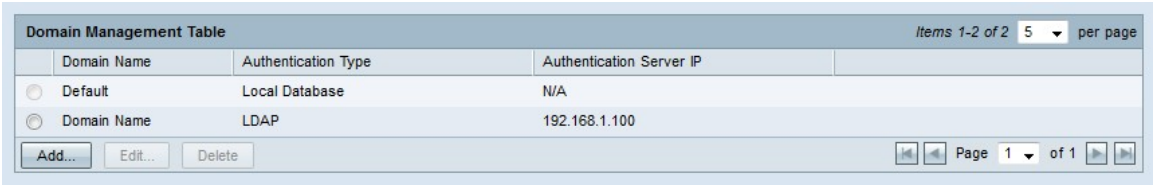


Passaggio 1. Immettere un nome per il dominio nel campo Dominio.

Passaggio 2. Immettere l'indirizzo IP del server LDAP nel campo Indirizzo server LDAP.

Passaggio 3. Inserire il nome distinto di base del server LDAP nel campo DN di base LDAP. Il DN di base è la posizione in cui il server LDAP cerca gli utenti quando riceve una richiesta di autorizzazione. Questo campo deve corrispondere al DN di base configurato nel server LDAP.

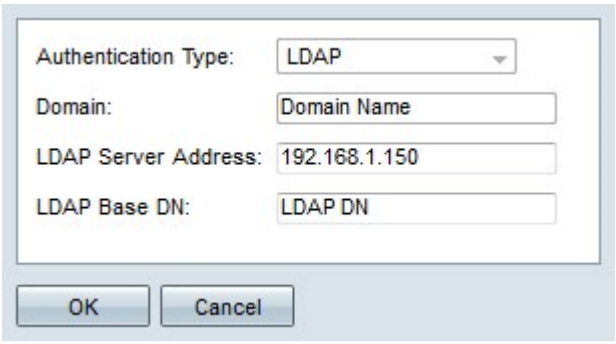
Passaggio 4. Fare clic su **OK**. Il dominio viene creato.



Modifica configurazione dominio

Passaggio 1. Fare clic sul pulsante di opzione del dominio che si desidera modificare.

Passaggio 2. Fare clic su **Modifica** nella tabella Gestione domini per modificare il dominio.



Passaggio 3. Modificare i campi desiderati.

Passaggio 4. Fare clic su **OK**. La configurazione del dominio viene aggiornata.

Elimina configurazione dominio

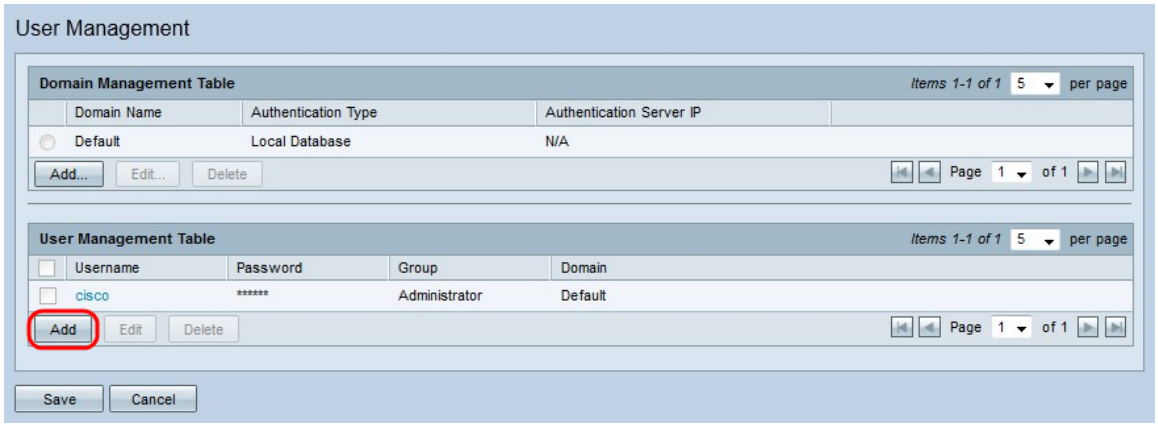
Passaggio 1. Fare clic sul pulsante di opzione del dominio che si desidera eliminare.

Passaggio 2. Fare clic su **Elimina** nella tabella Gestione dominio per eliminare il dominio. Viene visualizzata una finestra di avvertenza.

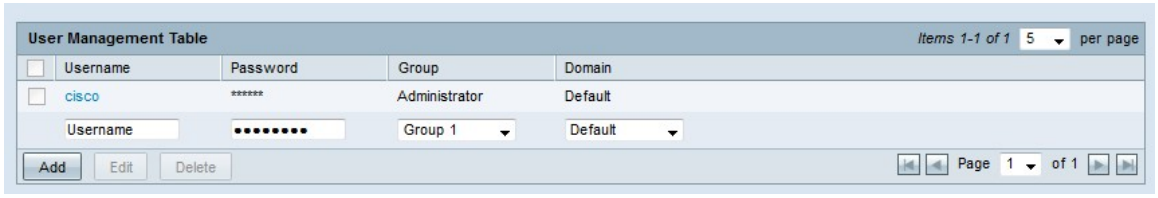
Passaggio 3. Fare clic su **Sì**. La configurazione del dominio viene eliminata.

Gestione utenti

Passaggio 1. Accedere all'utility di configurazione del router e scegliere **Gestione utenti**. Viene visualizzata la pagina *Gestione utente*:



Passaggio 2. Fare clic su **Add** nella tabella User Management per aggiungere un nuovo utente.



Passaggio 3. Inserire il nome utente desiderato nel campo Nome utente.

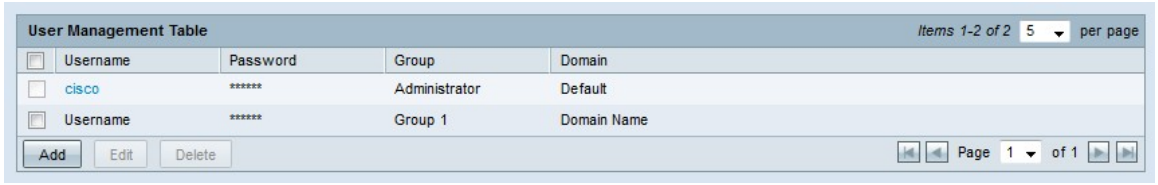
Passaggio 4. Immettere una password per il nome utente nel campo Password. La password viene utilizzata per autenticare l'utente nel dominio di database locale configurato.

Passaggio 5. Scegliere il gruppo a cui l'utente deve appartenere dall'elenco a discesa Gruppo. I gruppi vengono utilizzati per dividere ulteriormente i domini in sottodomini più piccoli. Il gruppo Administrators può contenere un solo utente. Il nome utente e la password predefiniti dell'amministratore sono cisco/cisco.

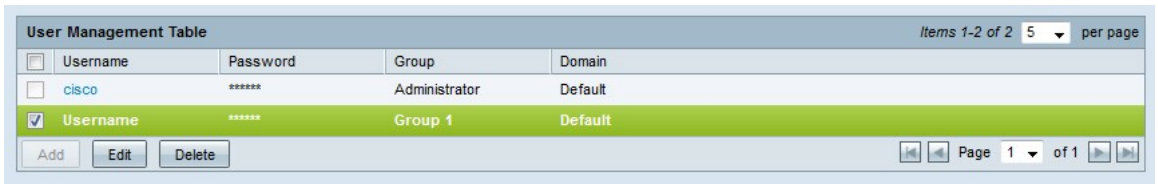
Nota: I gruppi possono essere configurati nella pagina *Gestione gruppi*. Per ulteriori informazioni, consultare l'articolo *Gestione gruppi su router RV320*.

Passaggio 6. Scegliere il dominio a cui l'utente deve appartenere dall'elenco a discesa Dominio.

Passaggio 7. Fare clic su **Salva**. Il nuovo utente è configurato.



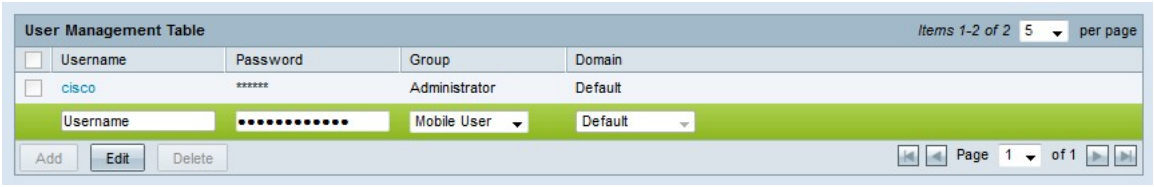
Modifica gestione utenti



Passaggio 1. Selezionare la casella di controllo del nome utente che si desidera modificare.

Passaggio 2. Fare clic su **Modifica** nella tabella Gestione utenti per modificare il nome

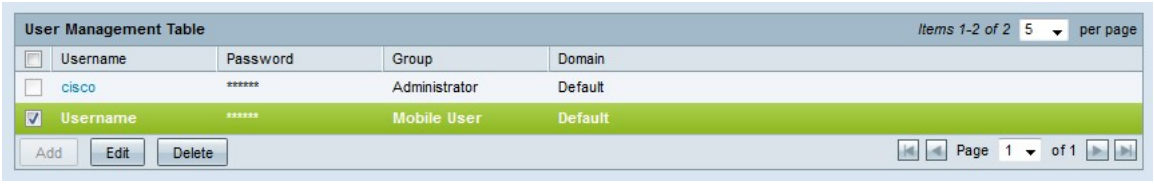
utente.



Passaggio 3. Modificare i campi desiderati.

Passaggio 4. Fare clic su **Salva**. La configurazione del nome utente viene aggiornata.

Elimina gestione utenti



Passaggio 1. Selezionare la casella di controllo del nome utente che si desidera eliminare.

Passaggio 2. Fare clic su **Elimina** nella tabella Gestione utenti per eliminare il nome utente.

Passaggio 3. Fare clic su **Salva**. La configurazione del nome utente viene eliminata.