

Come configurare Cisco VPN 3000 Concentrator per supportare l'autenticazione TACACS+ per gli account di gestione

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Configurazione del server TACACS+](#)

[Aggiungere una voce per VPN 3000 Concentrator nel server TACACS+](#)

[Aggiungere un account utente nel server TACACS+](#)

[Modifica del gruppo sul server TACACS+](#)

[Configurazione di VPN 3000 Concentrator](#)

[Aggiungere una voce per il server TACACS+ nel concentratore VPN 3000](#)

[Modificare l'account Admin sul concentratore VPN per l'autenticazione TACACS+](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

[Introduzione](#)

Questo documento offre istruzioni dettagliate per configurare i Cisco VPN serie 3000 concentrator per il supporto dell'autenticazione TACACS+ per gli account di gestione.

Non appena si configura un server TACACS+ sul concentratore VPN 3000, i nomi di account e le password configurati localmente, come admin, config, isp e così via, non vengono più utilizzati. Tutti i login al VPN 3000 Concentrator vengono inviati al server TACACS+ esterno configurato per la verifica di utenti e password.

La definizione di un livello di privilegio per ciascun utente sul server TACACS+ determina le autorizzazioni sul concentratore VPN 3000 per ciascun nome utente TACACS+. Quindi, associarlo al livello di accesso AAA definito nel nome utente configurato localmente sul concentratore VPN 3000. Questo è un punto importante perché, non appena si definisce un server TACACS+, i nomi utente configurati localmente su VPN 3000 Concentrator non sono più validi. Tuttavia, vengono ancora utilizzati solo per far corrispondere il livello di privilegio restituito dal server TACACS+ al livello di accesso AAA restituito dall'utente locale. Al nome utente TACACS+ vengono quindi assegnati i privilegi definiti dall'utente VPN 3000 Concentrator configurato localmente nel relativo profilo.

Ad esempio, come descritto in dettaglio nelle sezioni di configurazione, un utente/gruppo TACACS+ è configurato in modo da restituire un livello di privilegio TACACS+ di 15. Nella sezione Administrators di VPN 3000 Concentrator, anche l'utente amministratore ha il livello di accesso AAA impostato su 15. A questo utente è consentito modificare la configurazione in tutte le sezioni e leggere/scrivere file. Poiché il livello di privilegio TACACS+ e il livello di accesso AAA corrispondono, all'utente TACACS+ vengono concesse queste autorizzazioni sul concentratore VPN 3000.

Ad esempio, se si decide che un utente deve essere in grado di modificare la configurazione ma *non* i file di lettura/scrittura, assegnare loro un livello di privilegio di 12 sul server TACACS+. È possibile scegliere un numero qualsiasi compreso tra uno e 15. Quindi, nel concentratore VPN 3000, scegliere uno degli altri amministratori configurati localmente. Quindi, impostare il livello di accesso AAA su 12 e impostare le autorizzazioni sull'utente per consentirgli di modificare la configurazione ma non di leggere/scrivere file. A causa del livello di accesso/privilegio corrispondente, l'utente ottiene tali autorizzazioni al momento dell'accesso.

I nomi utente configurati localmente su VPN 3000 Concentrator non sono più utilizzati. Tuttavia, i diritti di accesso e i livelli di accesso AAA di ciascuno di questi utenti sono usati per definire i privilegi che un particolare utente TACACS+ ottiene quando si esegue il login.

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Verificare la presenza di connettività IP al server TACACS+ dal concentratore VPN 3000. Se il server TACACS+ è diretto all'interfaccia pubblica, non dimenticare di aprire TACACS+ (porta TCP 49) sul filtro pubblico.
- Garantire l'accesso ai backup tramite la console. È facile bloccare accidentalmente tutti gli utenti fuori dalla configurazione quando questa è stata configurata per la prima volta. L'unico modo per ripristinare l'accesso è tramite la console, che utilizza ancora i nomi utente e le password configurati localmente.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Software Cisco VPN 3000 Concentrator versione 4.7.2.B (in alternativa, è possibile usare qualsiasi versione del software del sistema operativo 3.0 o versioni successive).
- Cisco Secure Access Control Server per server Windows versione 4.0 (in alternativa, può funzionare qualsiasi versione del software 2.4 o successive).

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

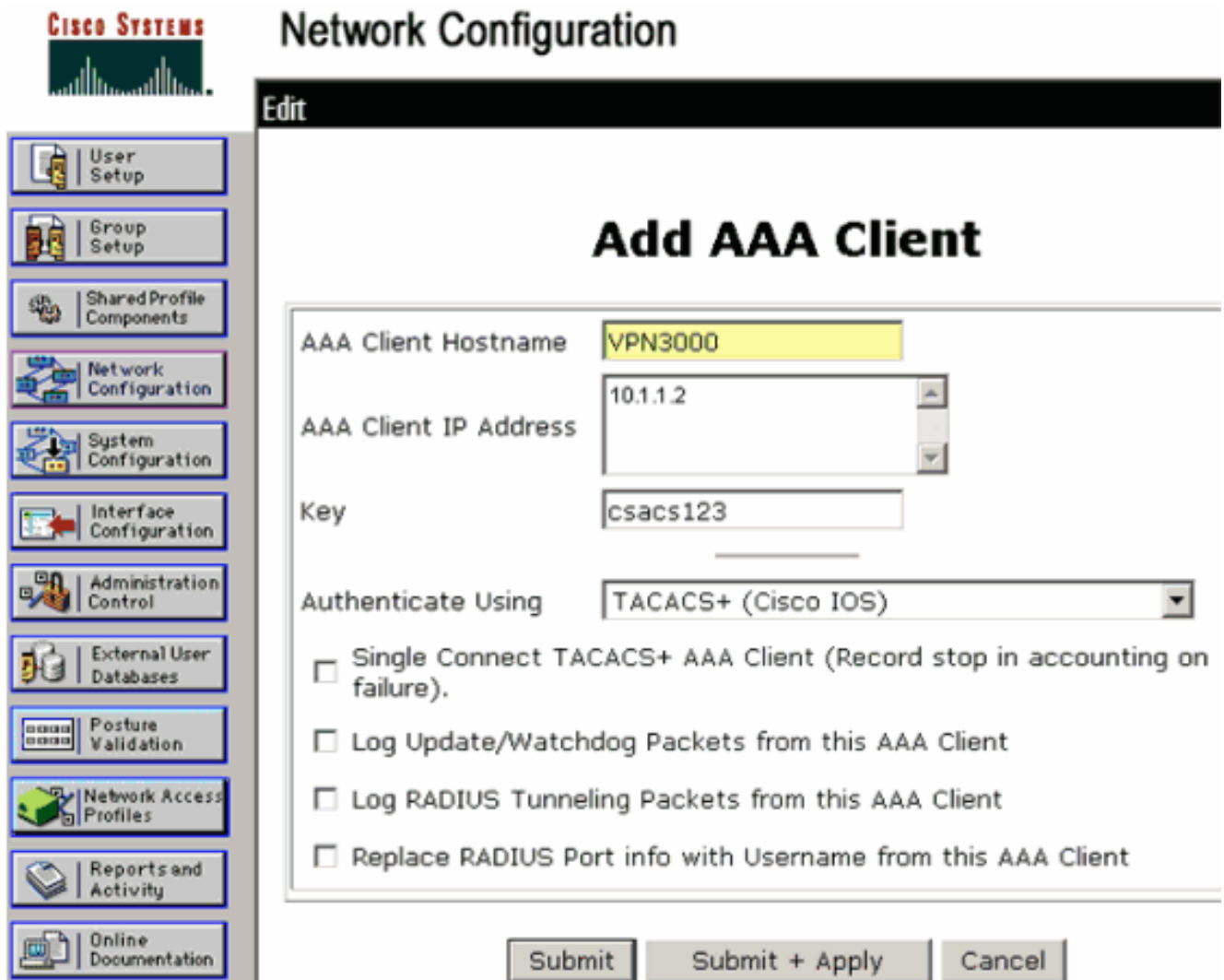
Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

[Configurazione del server TACACS+](#)

[Aggiungere una voce per VPN 3000 Concentrator nel server TACACS+](#)

Completare questa procedura per aggiungere una voce per il concentratore VPN 3000 nel server TACACS+.

1. Fare clic su **Network Configuration** (Configurazione rete) nel pannello sinistro. In Client AAA, fare clic su **Add Entry** (Aggiungi voce).
2. Nella finestra successiva, compilare il modulo per aggiungere il concentratore VPN come client TACACS+. In questo esempio vengono utilizzati: Nome host client AAA = VPN3000
Indirizzo IP client AAA = 10.1.1.2
Chiave = csacs123
Autentica con = TACACS+ (Cisco IOS)
Fare clic su **Invia + Riavvia**.



The screenshot shows the Cisco Systems Network Configuration interface. On the left is a navigation menu with icons and labels for: User Setup, Group Setup, Shared Profile Components, Network Configuration (highlighted), System Configuration, Interface Configuration, Administration Control, External User Databases, Posture Validation, Network Access Profiles, Reports and Activity, and Online Documentation. The main area is titled 'Network Configuration' and 'Edit'. Below this is a form titled 'Add AAA Client'. The form contains the following fields and options:

- AAA Client Hostname: VPN3000
- AAA Client IP Address: 10.1.1.2
- Key: csacs123
- Authenticate Using: TACACS+ (Cisco IOS)
- Single Connect TACACS+ AAA Client (Record stop in accounting on failure).
- Log Update/Watchdog Packets from this AAA Client
- Log RADIUS Tunneling Packets from this AAA Client
- Replace RADIUS Port info with Username from this AAA Client

At the bottom of the form are three buttons: Submit, Submit + Apply, and Cancel.

[Aggiungere un account utente nel server TACACS+](#)

Completare questa procedura per aggiungere un account utente nel server TACACS+.

1. Creare un account utente nel server TACACS+ da utilizzare successivamente per l'autenticazione TACACS+. Fare clic su **User Setup** (Impostazione utente) nel pannello a sinistra, aggiungere l'utente "johnsmith" (fabbisogni utente) e fare clic su **Add/Edit** (Aggiungi/Modifica) per eseguire questa operazione.
2. Aggiungere una password per questo utente e assegnare l'utente a un gruppo ACS che contiene gli altri amministratori di VPN 3000 Concentrator.**Nota:** questo esempio definisce il livello di privilegio in questo particolare profilo di gruppo ACS dell'utente. Se l'operazione deve essere eseguita per singolo utente, scegliere **Configurazione interfaccia > TACACS+ (Cisco IOS)** e selezionare la casella **Utente** per il servizio Shell (exec). Solo allora le opzioni TACACS+ descritte in questo documento sono disponibili in ciascun profilo utente.

[Modifica del gruppo sul server TACACS+](#)

Completare questa procedura per modificare il gruppo sul server TACACS+.

1. Fare clic su **Group Setup** nel pannello sinistro.
2. Dal menu a discesa, scegliere il gruppo a cui è stato aggiunto l'utente nella sezione [Add a User Account in TACACS+ Server](#), che in questo esempio è Group 1, e fare clic su **Edit Settings**.
3. Nella finestra successiva, verificare che questi attributi siano selezionati in TACACS+ Settings:**Shell (esegui)****Livello di privilegio = 15**Al termine, fare clic su **Invia + Riavvia**.

CISCO SYSTEMS Group Setup

Jump To **Access Restrictions**

TACACS+ Settings

PPP IP

In access control list

Out access control list

Route

Routing Enabled

Note: PPP LCP will be automatically enabled if this service is enabled

Shell (exec)

Access control list

Auto command

Callback line

Callback rotary

Idle time

No callback verify Enabled

No escape Enabled

No hangup Enabled

Privilege level

Timeout

Shell Command Authorization Set

None

Assign a Shell Command Authorization Set for any network device

Per Group Command Authorization

Unmatched Cisco IOS commands

Permit

Deny

Submit Submit + Restart Cancel

[Configurazione di VPN 3000 Concentrator](#)

[Aggiungere una voce per il server TACACS+ nel concentratore VPN 3000](#)

Completare questa procedura per aggiungere una voce per il server TACACS+ nel concentratore VPN 3000.

1. Scegliere **Amministrazione > Diritti di accesso > Server AAA > Autenticazione** nella struttura di navigazione nel pannello sinistro, quindi fare clic su **Aggiungi** nel pannello destro. Non appena si fa clic su **Add** (Aggiungi) per aggiungere il server, il nome utente e le password configurati localmente su VPN 3000 Concentrator non vengono più utilizzati. Garantire l'accesso ai backup tramite la console in caso di blocco.

2. Nella finestra successiva, compilare il modulo come illustrato di seguito: Server di autenticazione = 10.1.1.1 (indirizzo IP del server TACACS+) Porta server = 0 (predefinita) Timeout = 4 Tentativi = 2 Segreto server = csacs123 Verify = csacs123

Administration | Access Rights | AAA Servers | Authentication | Add

Configure and add a TACACS+ administrator authentication server.

Authentication Server: 10.1.1.1 Enter IP address or hostname.

Server Port: 0 Enter the server TCP port number (0 for default).

Timeout: 4 Enter the timeout for this server (seconds)

Retries: 2 Enter the number of retries for this server.

Server Secret: csacs123 Enter the server secret.

Verify: csacs123 Re-enter the server secret.

Add Cancel

[Modificare l'account Admin sul concentratore VPN per l'autenticazione TACACS+](#)

Completare questa procedura per modificare l'account admin sul concentratore VPN per l'autenticazione TACACS+.

1. Per modificare le proprietà dell'utente, fare clic su **Modifica** per l'amministratore utente.

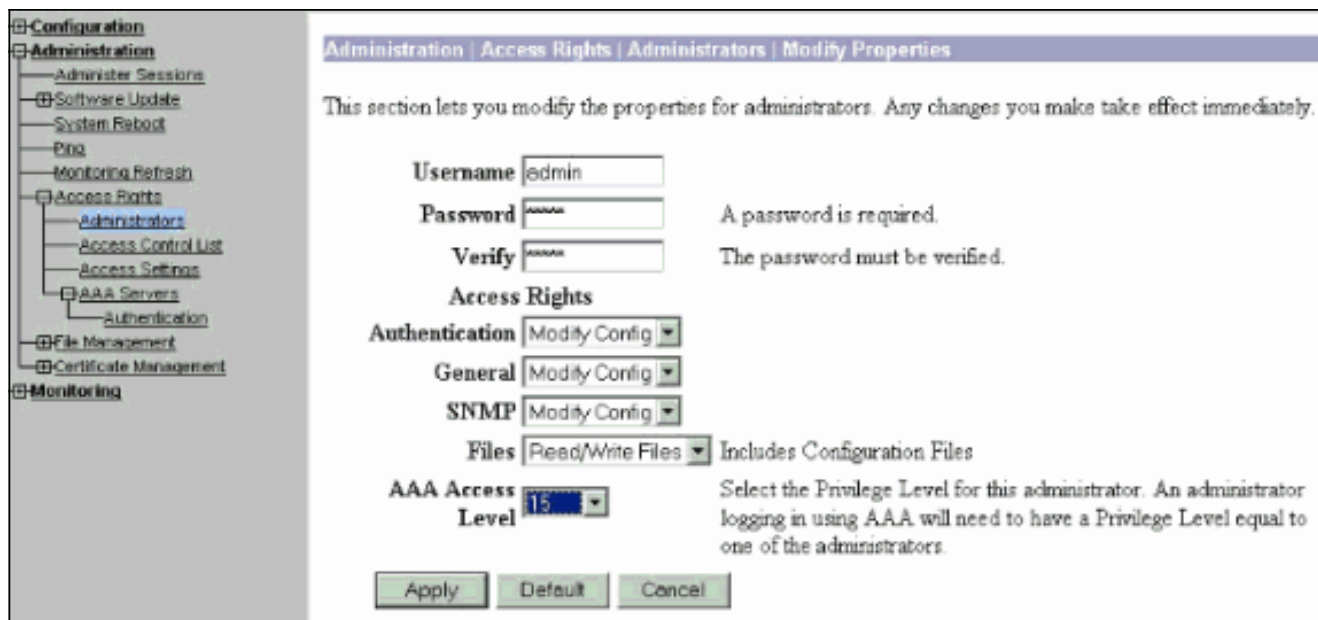
Administration | Access Rights | Administrators

This section presents administrator users. Any changes you make take effect immediately.

Group Number	Username	Properties	Administrator	Enabled
1	admin	Modify	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>
2	config	Modify	<input type="radio"/>	<input type="checkbox"/>
3	isp	Modify	<input type="radio"/>	<input type="checkbox"/>
4	mis	Modify	<input type="radio"/>	<input type="checkbox"/>
5	user	Modify	<input type="radio"/>	<input type="checkbox"/>

Apply Cancel

2. Selezionare il livello di accesso AAA come 15. Questo valore può essere un numero qualsiasi compreso tra uno e 15. Notare che deve corrispondere al livello di privilegio TACACS+ definito nel profilo utente/gruppo sul server TACACS+. L'utente TACACS+ riceve quindi le autorizzazioni definite in questo utente VPN 3000 Concentrator per la modifica della configurazione, la lettura/scrittura dei file e così via.



Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Completare la procedura descritta in queste istruzioni per risolvere i problemi relativi alla configurazione.

1. Per verificare l'autenticazione: Per server TACACS+ Scegliere **Amministrazione > Diritti di accesso > Server AAA > Autenticazione**. Selezionare il server e quindi fare clic su **Test**.



Nota: quando il server TACACS+ è configurato nella scheda Amministrazione, non è possibile configurare l'utente per l'autenticazione sul database locale VPN 3000. È possibile eseguire il fallback solo utilizzando un altro database esterno o server TACACS. Immettere il nome utente e la password TACACS+ e fare clic su

OK.

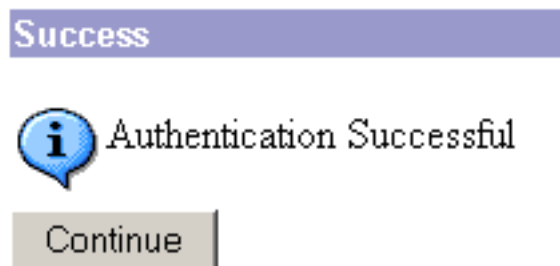
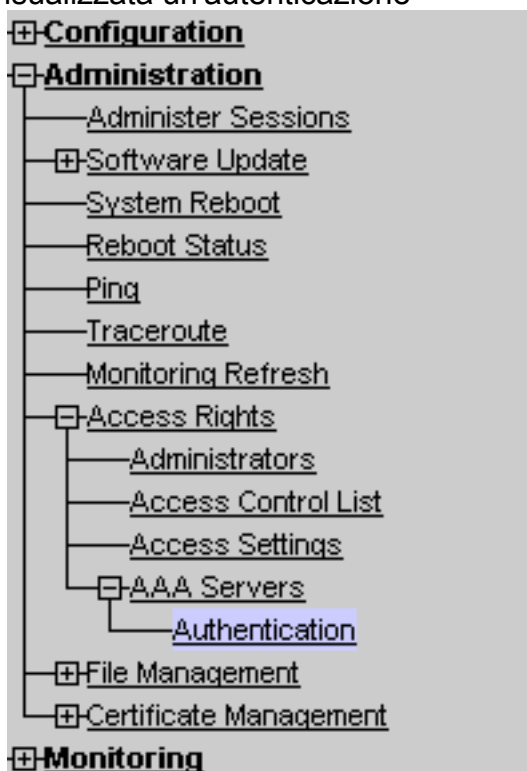
Administration | Access Rights | AAA Servers | Authentication | Test

Enter a username and password with which to test. Please wait for the operation to complete or timeout.

Username

Password

Viene visualizzata un'autenticazione



riuscita.

- In caso di errore, si è verificato un problema di configurazione o di connettività IP. Controllare il registro dei tentativi non riusciti sul server ACS per i messaggi relativi all'errore. Se in questo registro non viene visualizzato alcun messaggio, è probabile che si sia verificato un problema di connettività IP. La richiesta TACACS+ non raggiunge il server TACACS+. Verificare che i filtri applicati all'interfaccia VPN 3000 Concentrator appropriata consentano l'ingresso e l'uscita dei pacchetti TACACS+ (porta TCP 49). Se l'errore viene visualizzato come servizio negato nel log, il servizio Shell (exec) non è stato abilitato correttamente nel profilo utente o di gruppo sul server TACACS+.
- Se il test di autenticazione ha esito positivo, ma il login a VPN 3000 Concentrator continua a non riuscire, controllare il registro eventi filtrabile tramite la porta della console. Se viene visualizzato un messaggio simile:

```
65 02/09/2005 13:14:40.150 SEV=5 AUTH/32 RPT=2
```

```
User [ johnsmith ] Protocol [ HTTP ] attempted ADMIN logon.  
Status: <REFUSED> authorization failure. NO Admin Rights
```

Questo messaggio indica che il livello di privilegio assegnato sul server TACACS+ non ha un livello di accesso AAA corrispondente su nessuno degli utenti VPN 3000 Concentrator. Ad esempio, l'utente johnsmith ha un livello di privilegio TACACS+ di 7 sul server TACACS+, ma nessuno dei cinque amministratori VPN 3000 Concentrator ha un livello di accesso AAA di 7.

Informazioni correlate

- [Cisco VPN serie 3000 Concentrator Support Page](#)
- [Cisco VPN serie 3000 Client Support Page](#)
- [Pagina di supporto per la negoziazione IPsec/i protocolli IKE](#)
- [Pagina di supporto TACACS/TACACS+](#)
- [Documentazione relativa a TACACS+ in IOS](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)