

Genera report FMC per utenti VPN

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Configurazioni](#)

[Genera report](#)

[Procedura](#)

[Risultato](#)

Introduzione

In questo documento viene descritto come generare report che forniscono una panoramica immediata delle informazioni consolidate sugli utenti VPN, inclusi lo stato corrente di utenti, tipi di dispositivi, sistema operativo client, applicazioni client e durata delle connessioni su Firepower Management Center.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Firepower Threat Defense (FTD)
- Cisco Firepower Management Center (FMC)
- Anyconnect Secure Mobility

Componenti usati

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

- Cisco FMC per VMware versione 7.x
- AnyConnect Secure Mobility Client 4.x

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.

Premesse

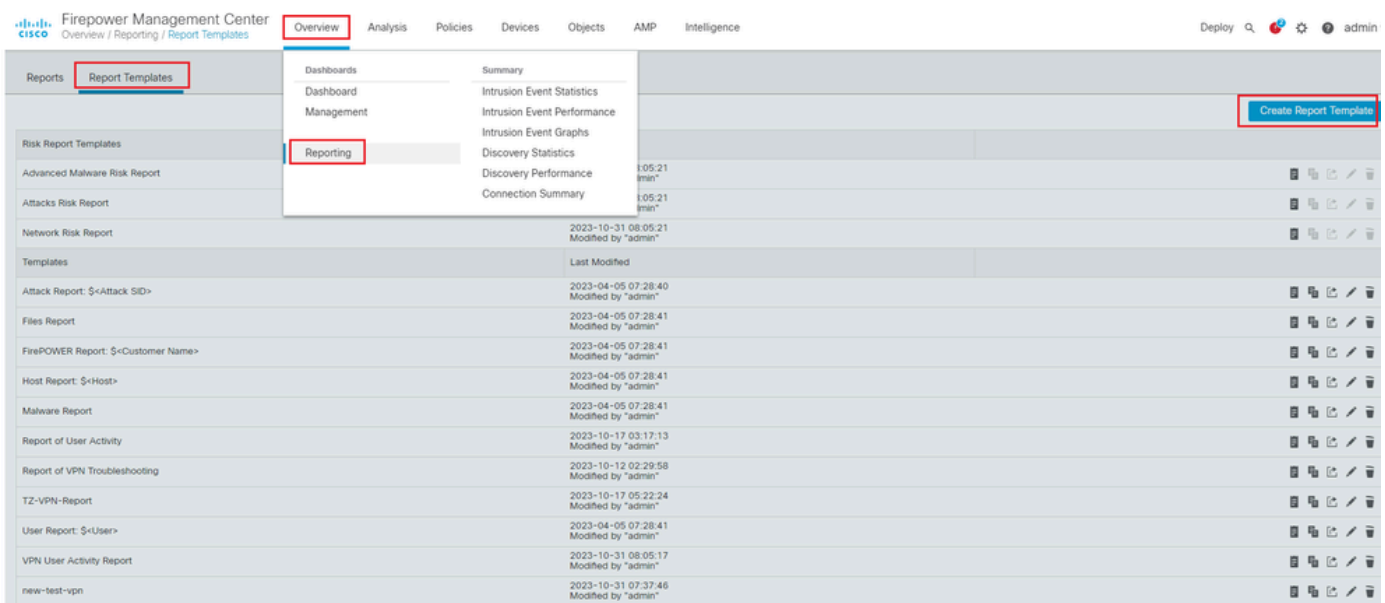
Firepower System fornisce un sistema di reporting flessibile che consente di generare in modo rapido e semplice report su Firepower Management Center. È inoltre possibile progettare report personalizzati da zero. Un report è un file di documento formattato in PDF, HTML o CSV con il contenuto che si desidera comunicare mentre un modello di report specifica le ricerche di dati e i formati per il report e le relative sezioni. Firepower System include un potente strumento di progettazione dei report che automatizza la progettazione dei modelli di report. È possibile includere parametri di campo quali il tipo di autenticazione, la durata della connessione e così via in un modello per aumentarne l'utilità.

Le VPN ad accesso remoto offrono connessioni protette per gli utenti remoti, ad esempio gli utenti mobili o i telelavoratori. Il monitoraggio di queste connessioni fornisce importanti indicatori delle prestazioni della connessione e della sessione utente. Per eseguire questa attività, è necessario essere un utente Admin in un dominio foglia. Le funzionalità di monitoraggio di Firepower System consentono di determinare rapidamente se esistono problemi VPN di accesso remoto e di applicare queste conoscenze e utilizzare gli strumenti di gestione della rete per ridurre o eliminare i problemi per la rete e gli utenti.

Configurazione

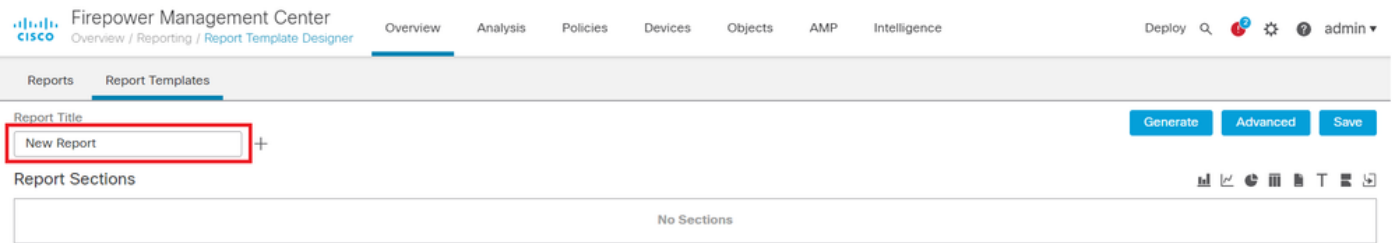
Configurazioni

Passaggio 1. Selezionate Overview > Dashboards > Reporting > Report Templates e fate clic su Create Report Template come mostrato nell'immagine.



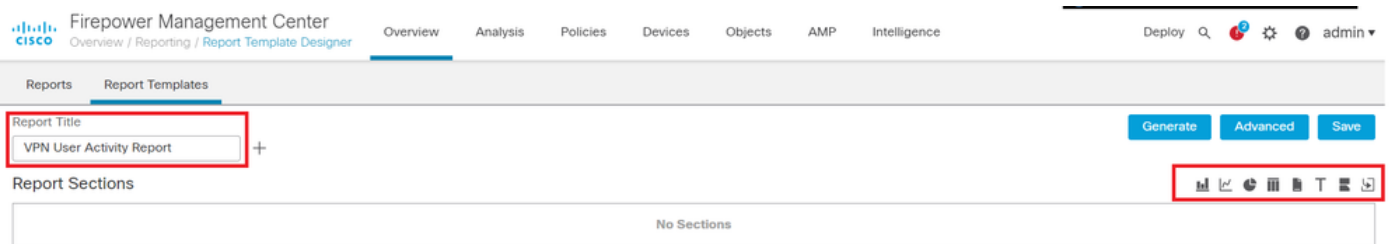
Crea modello di report

Passaggio 2. Immettere un nome per il modello nel campo, Report Title come mostrato nell'immagine.



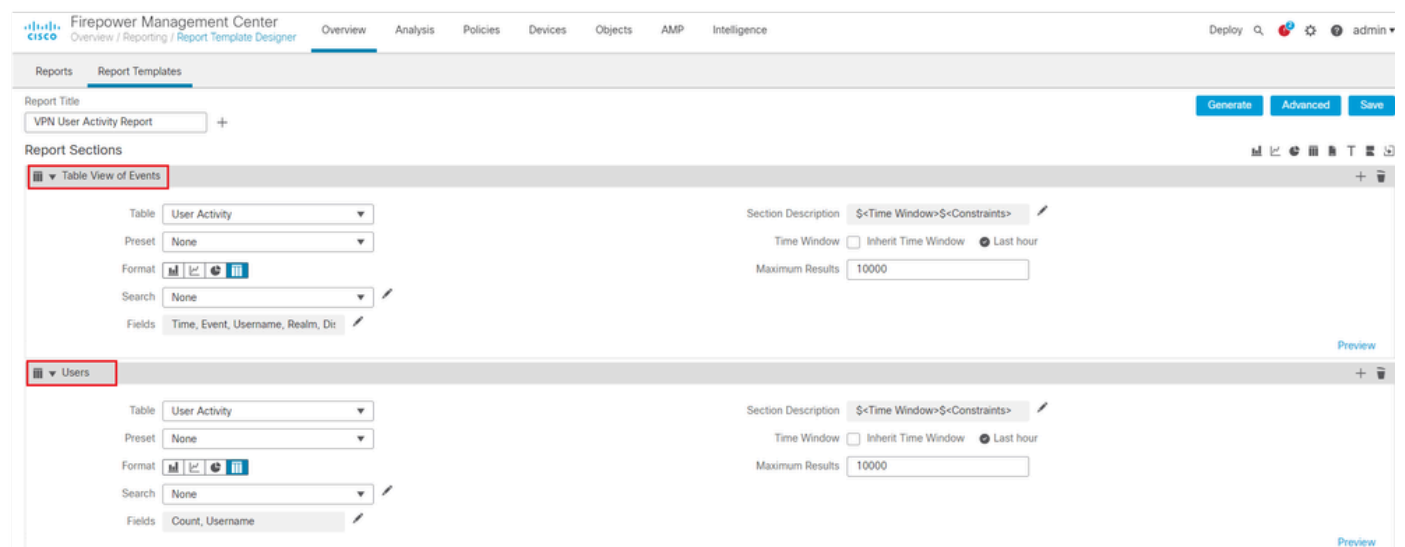
Titolo del report

Passaggio 3. Selezionate Add Table View una delle viste disponibili sul lato destro. È inoltre possibile utilizzare grafici a barre, a linee, a torta e così via in base alle proprie esigenze.



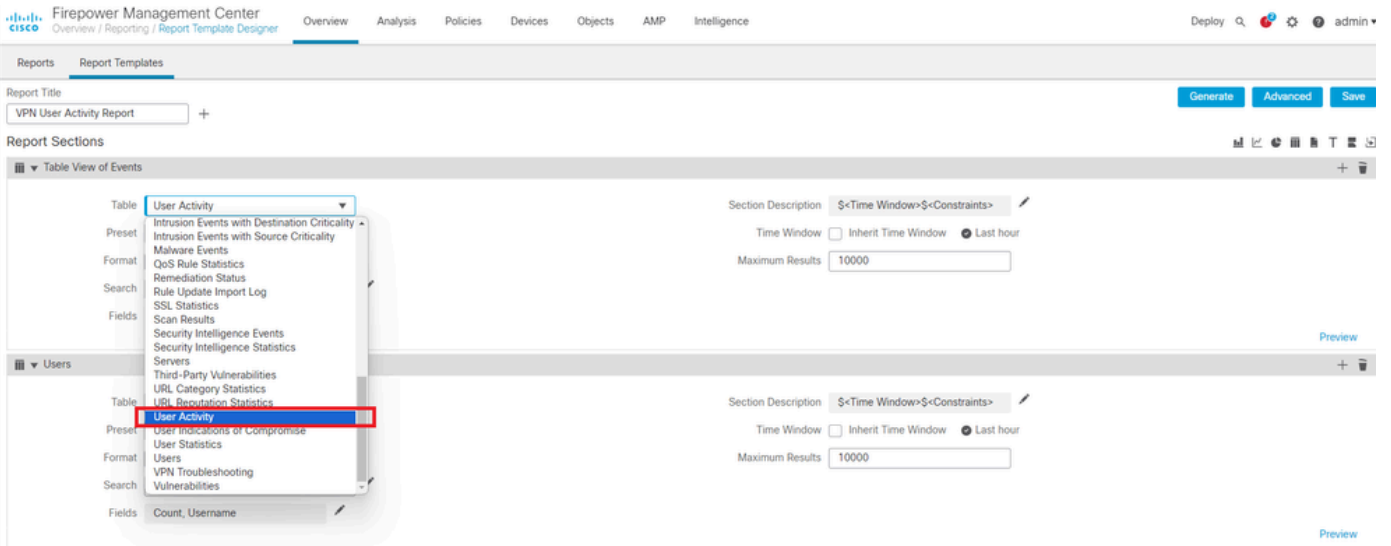
Aggiungi visualizzazione tabella

Passaggio 4. Immettere un titolo per la sezione nel campo Report Section Title. Qui sono state aggiunte le viste tabella Table View of Events e Users come mostrato nell'immagine.



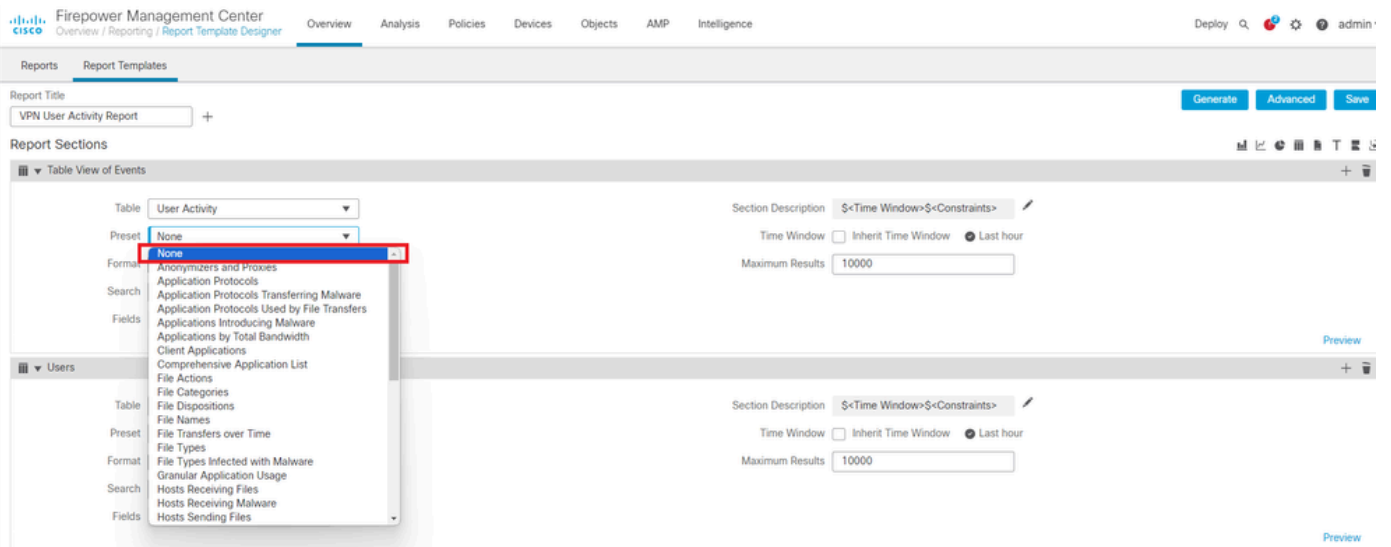
Titolo della sezione del report

Passaggio 5. Selezionate User Activity dal menu a discesa Tabella (Table) come illustrato nell'immagine.



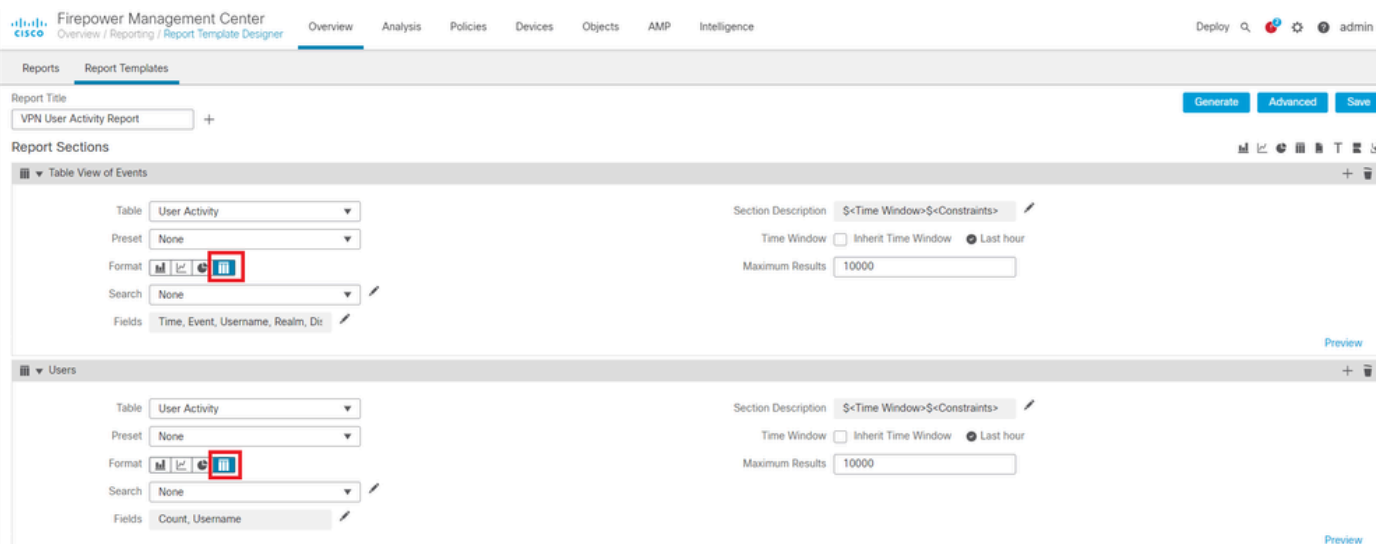
Seleziona attività utente

Passaggio 6. Se necessario, scegliete un valore preimpostato, altrimenti mantenete come None .



Aggiunta di un valore preimpostato

Passaggio 7. Selezionate il formato di outputTable View come illustrato nell'immagine.



Visualizzazione per tabella come formato di output

Passaggio 8. (Facoltativo) Dal menu di ricerca, selezionare gli attributi che si desidera utilizzare per vincolare il rapporto. Selezionare None se non si desidera applicare alcun vincolo di ricerca.

Search Editor

Search Information

Table: User Activity

Saved Searches: None

Search Information

Event		New User, Login, Delete, Dropped
Username		jsmith
Realm		REALM
Discovery Application		ldap
Authentication Type		No Authentication, Active Authentication
IP Address		192.168.1.0/24, 192.168.1.3, 2001:db8:85a3:1370
Start Port		2300
End Port		2500
Description		john
VPN Session Type		AnyConnect IKEv2, AnyConnect SSL, *IKEv2
VPN Group Policy		MyGroupPolicy

Cancel OK

Vincoli di ricerca

Passaggio 9. Selezionare l'intervallo di tempo per il quale si desidera generare il report. Fare clic su Last hour e si apre una nuova finestra pop-up con opzioni di 1 ora, 6 ore, 1 giorno, 1 mese e così via, come mostrato nell'immagine.

Firepower Management Center

Overview / Reporting / Report Template Designer

Reports Report Templates

Report Title: VPN User Activity Report

Report Sections

Table View of Events

Table: User Activity

Preset: None

Format: [Table]

Search: None

Fields: Time, Event, Username, Realm, Di:

Section Description: \$<Time Window>\$<Constraints>

Time Window: Inherit Time Window Last hour

Maximum Results: 10000

Preview

Users

Table: User Activity

Preset: None

Format: [Table]

Search: None

Fields: Count, Username

Section Description: \$<Time Window>\$<Constraints>

Time Window: Inherit Time Window Last hour

Maximum Results: 10000

Preview

Seleziona intervallo di tempo

Events Time Window Preferences

Sliding Time Window

Show the Last hour(s)

Presets

- Last Synchronize with
- 1 hour Audit Log Time Window
- 6 hours Health Monitoring Time Window
- 1 day
- 1 week
- 2 weeks
- 1 month

Any changes made will take effect on the next page load.

Reset Apply

Aggiungi TimeFrame

Passaggio 10. Per registrare il numero specifico di risultati, fornire un valore compreso tra 1 e 400000 nel Maximum Results campo.

Firepower Management Center Overview / Reporting / Report Template Designer

Reports Report Templates

Report Title: VPN User Activity Report

Report Sections

Table View of Events

Table: User Activity

Preset: None

Format: [Table Icon] [List Icon] [Bar Chart Icon]

Search: None

Fields: Time, Event, Username, Realm, Di

Section Description: \$<Time Window>\$<Constraints>

Time Window: Inherit Time Window Last hour

Maximum Results:

Preview

Users

Table: User Activity

Preset: None

Format: [Table Icon] [List Icon] [Bar Chart Icon]

Search: None

Fields: Count, Username

Section Description: \$<Time Window>\$<Constraints>

Time Window: Inherit Time Window Last hour

Maximum Results:

Preview

Numero massimo di risultati da visualizzare

Passaggio 11. Fare clic sul pulsante nella Save parte superiore delle sezioni del report per rendere il modello pronto per l'utilizzo.

Salva report

Genera report

Una volta creato e personalizzato il modello di report, è possibile generare il report. Per visualizzare i dati utente sono disponibili diversi formati di output, ad esempio HTML, PDF o CSV.



























































Nota: per i report PDF, i nomi di file che utilizzano caratteri Unicode (UTF-8) non sono supportati.

Procedura

Passaggio 1. Selezionare Overview > Reporting e fare clic su Report Templates .

Passaggio 2. Fare clic sull'Generate Report'icona accanto al modello configurato come mostrato nell'immagine.

Risk Report Templates		Last Modified	
Advanced Malware Risk Report	2023-10-31 08:11:02 Modified by "admin"		   
Attacks Risk Report	2023-10-31 08:11:02 Modified by "admin"		   
Network Risk Report	2023-10-31 08:11:02 Modified by "admin"		   
Templates		Last Modified	
Attack Report: \$<Attack SID>	2023-04-05 07:28:40 Modified by "admin"		   
Files Report	2023-04-05 07:28:41 Modified by "admin"		   
FirePOWER Report: \$<Customer Name>	2023-04-05 07:28:41 Modified by "admin"		   
Host Report: \$<Host>	2023-04-05 07:28:41 Modified by "admin"		   
Malware Report	2023-04-05 07:28:41 Modified by "admin"		   
Report of User Activity	2023-10-17 03:17:13 Modified by "admin"		   
Report of VPN Troubleshooting	2023-10-12 02:29:58 Modified by "admin"		   
TZ-VPN-Report	2023-10-17 05:22:24 Modified by "admin"		   
User Report: \$<User>	2023-04-05 07:28:41 Modified by "admin"		   
VPN User Activity Report	2023-10-31 08:05:17 Modified by "admin"		   
new-test-vpn	2023-10-31 07:37:46 Modified by "admin"		   

Genera visualizzazione report

Passaggio 3. Immettere un nuovo nome file. Questo nome viene utilizzato per salvare il report. Se non immettete un nuovo nome, il sistema utilizza il nome di default specificato nel modello di report.

Generate Report

Report Generation Information

File Name

VPN User Activity Report



Output Format



Time Window



Last hour

Relay Host

No Relay Host Configured!



Close

Generate

Aggiungi nome file

Passaggio 4. Scegliere il formato di output per il report facendo clic su: HTML, PDF o CSV.

Generate Report

Report Generation Information

File Name

VPN User Activity Report



Output Format



Time Window



Last hour

Relay Host

No Relay Host Configured!



Close

Generate

Seleziona formato di output file

Passaggio 5. (Facoltativo) Modificare l'intervallo di tempo globale per il rapporto da "Finestra temporale". Se nel modello di report non viene utilizzata l'opzione "Eredita finestra temporale", questa opzione viene ignorata.



Nota: l'impostazione della finestra temporale globale influisce sul contenuto delle singole sezioni del rapporto solo se sono configurate in modo da ereditare l'impostazione globale.

Passaggio 6. (Facoltativo) Se il report generato deve essere recapitato tramite posta elettronica, [configurare](#) un host di inoltro sul CCP.

Passaggio 7. Clicca su Generate e i file saranno disponibili per il download sotto "Rapporti". Per il formato CSV, verrà creata una cartella zip con ogni sezione del modello come file separato.

Generate Report

Report Generation Information

File Name

VPN User Activity Report



Output Format



Time Window

Last hour

Relay Host

No Relay Host Configured!

Close

Generate

Genera report

Firepower Management Center
Overview / Reporting / Reports

Overview Analysis Policies Devices Objects AMP Intelligence

Deploy 🔍 ⚙️ 👤 admin

Reports Report Templates

<input type="checkbox"/>	Name	Time Requested	Time Completed	User	Location	Status
<input type="checkbox"/>	VPN_User_Activity_Report-20231107030926-13615_csv.zip Reports	2023-11-06 22:09:26	2023-11-06 22:09:27	admin	Local	Successfully Processed
<input type="checkbox"/>	VPN_User_Activity_Report-20231107030926-13615.pdf Reports	2023-11-06 22:09:26	2023-11-06 22:09:27	admin	Local	Successfully Processed

Report generato

Risultato

Questa sezione fornisce le informazioni del report generato per l'utente VPN in formato PDF.

Table View of Users

Time Window: 2023-10-01 11:21:25 - 2023-10-01 13:02:03

User	Last Seen	Realm	Username	First Name	Last Name	E-Mail	Department	Phone	Discovery Application	Active Session Count	Available For Policy
cisco-ldap/cisco-ldap (LDAP)	2023-10-01 13:00:56	cisco-ldap	cisco-ldap						LDAP	1	no
cisco-local/admin (LDAP)	2023-10-01 10:05:12	cisco-local	admin						LDAP	0	no
Discovered Identities/cisco-radius (LDAP)	2023-10-01 09:45:44	Discovered Identities	cisco-radius						LDAP	0	no

Users

Time Window: 2023-10-01 11:21:25 - 2023-10-01 13:02:03

Count	User
1	cisco-ldap/cisco-ldap (LDAP)
1	cisco-local/admin (LDAP)
1	Discovered Identities/cisco-radius (LDAP)

Visualizza report generati

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).