

Generar informes FMC para usuarios de VPN

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Configuraciones](#)

[Generar informe](#)

[Procedimiento](#)

[Resultado](#)

Introducción

En este documento se describe cómo generar informes que proporcionan vistas rápidas de información consolidada sobre usuarios de VPN, incluido el estado actual de los usuarios, los tipos de dispositivos, el sistema operativo del cliente, las aplicaciones cliente y la duración de las conexiones en Firepower Management Center.

Prerequisites

Requirements

Cisco recomienda que conozca estos temas:

- Cisco Firepower Threat Defence (FTD)
- Cisco Firepower Management Center (FMC)
- AnyConnect Secure Mobility Client

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Cisco FMC para VMware con versión 7.x
- AnyConnect Secure Mobility Client 4.x

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

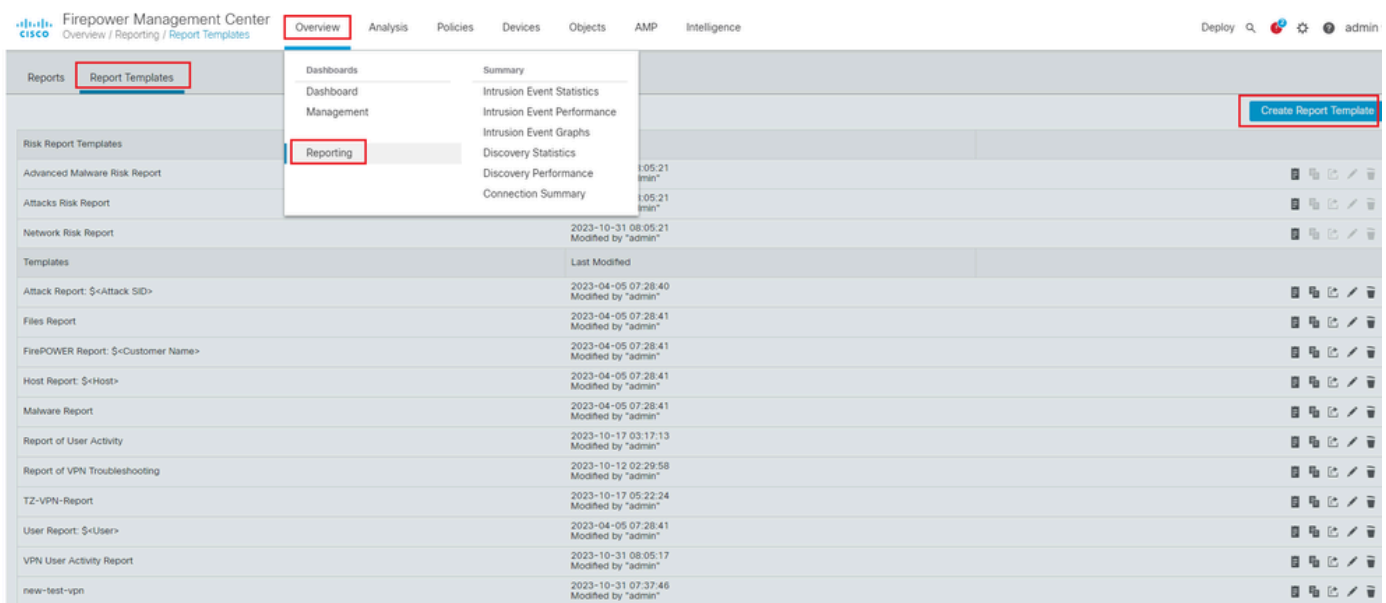
El sistema Firepower proporciona un sistema de generación de informes flexible que permite generar informes de forma rápida y sencilla en Firepower Management Center. También puede diseñar sus informes personalizados desde el principio. Un informe es un archivo de documento con formato PDF, HTML o CSV con el contenido que desea comunicar, mientras que una plantilla de informe especifica las búsquedas de datos y los formatos del informe y sus secciones. Firepower System incluye un potente diseñador de informes que automatiza el diseño de las plantillas de informes. Puede incluir parámetros de campo como el tipo de autenticación, la duración de la conexión, etc. en una plantilla para ampliar su utilidad.

Las VPN de acceso remoto proporcionan conexiones seguras para usuarios remotos, como usuarios móviles o teletrabajadores. La supervisión de estas conexiones proporciona indicadores importantes del rendimiento de la conexión y de la sesión de usuario de un vistazo. Debe ser un usuario administrador en un dominio de hoja para realizar esta tarea. Las capacidades de supervisión del sistema Firepower le permiten determinar rápidamente si existen problemas de VPN de acceso remoto y, a continuación, puede aplicar estos conocimientos y utilizar las herramientas de administración de redes para reducir o eliminar los problemas de la red y de los usuarios.

Configurar

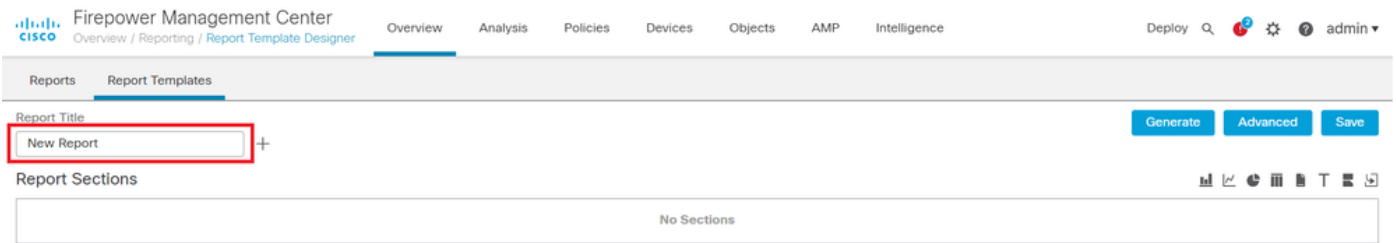
Configuraciones

Paso 1. Seleccione Overview > Dashboards > Reporting > Report Templates y haga clic en Create Report Template como se muestra en la imagen.



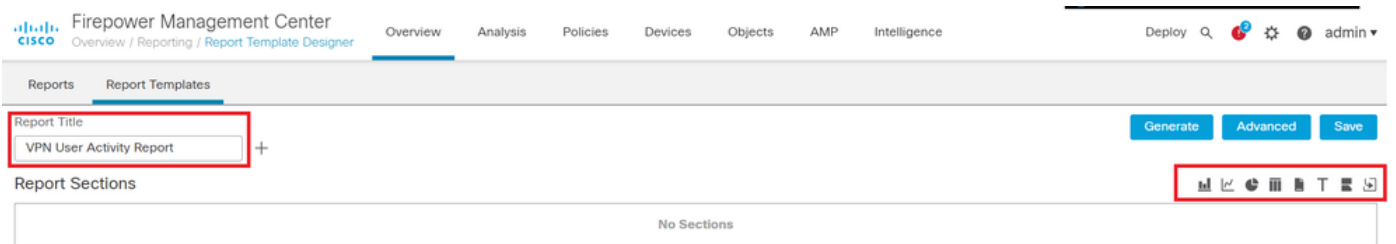
Crear plantilla de informe

Paso 2. Introduzca un nombre para la plantilla en el Report Title campo que se muestra en la imagen.



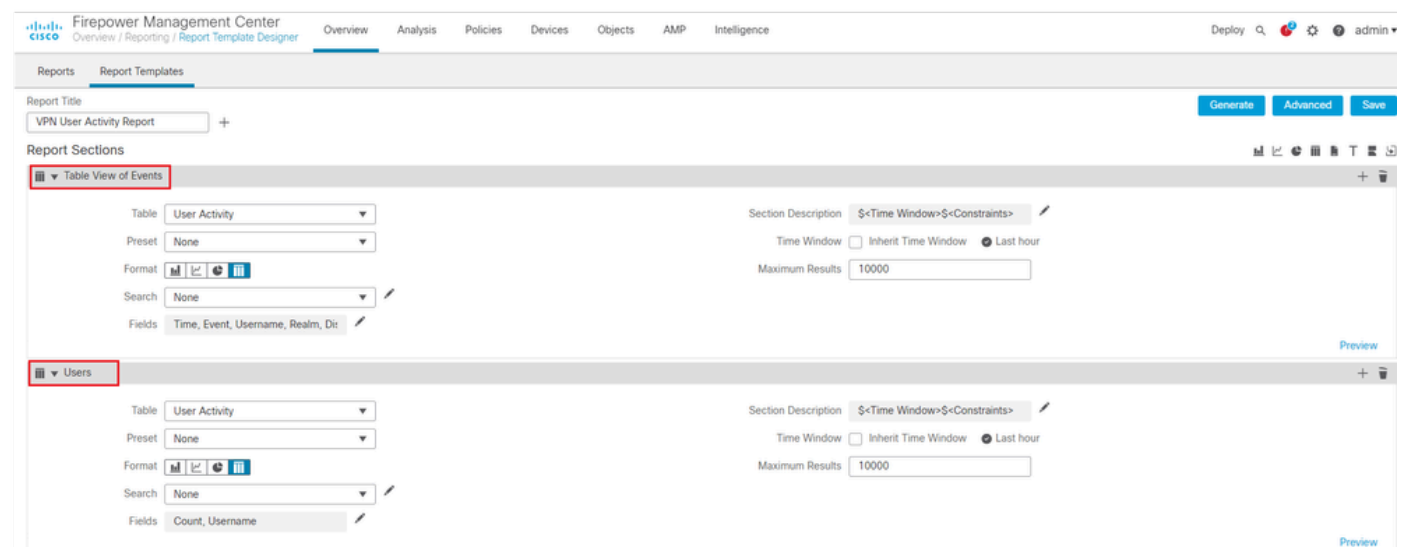
Título del informe

Paso 3. Selecciónelo Add Table View en el conjunto de vistas disponibles en el lado derecho. También puede utilizar gráficos como gráficos de barras, gráficos de líneas, gráficos circulares, etc., según sus necesidades.



Agregar vista de tabla

Paso 4. Introduzca un título para la sección en el Report Section Title campo. Aquí, Table View of Events y Users las vistas de tabla se han agregado como se muestra en la imagen.



Título de la sección de informes

Paso 5. Seleccione User Activity en el menú desplegable Table (Tabla), como se muestra en la imagen.

The screenshot shows the 'Report Template Designer' interface. At the top, the report title is 'VPN User Activity Report'. Below it, the 'Report Sections' are listed. The first section is 'Table View of Events', which is expanded to show a table configuration for 'User Activity'. A dropdown menu is open for the 'Preset' field, with 'None' selected and highlighted in red. Other options in the menu include 'Intrusion Events with Destination Criticality', 'Intrusion Events with Source Criticality', 'Malware Events', 'QoS Rule Statistics', 'Remediation Status', 'Rule Update Import Log', 'SSL Statistics', 'Scan Results', 'Security Intelligence Events', 'Security Intelligence Statistics', 'Servers', 'Third-Party Vulnerabilities', 'URL Category Statistics', and 'URL Reputation Statistics'. To the right of the table configuration, there are fields for 'Section Description', 'Time Window' (set to 'Last hour'), and 'Maximum Results' (set to '10000'). A 'Preview' button is visible at the bottom right of the section.

Seleccionar actividad de usuario

Paso 6. Elija un valor predefinido si es necesario; de lo contrario, manténgalo como None .

This screenshot is similar to the previous one, but the dropdown menu for the 'Preset' field is now closed, and 'None' is displayed in the field. The 'Format' field is also visible, with a dropdown menu open showing various options like 'Anonymizers and Proxies', 'Application Protocols', etc. The 'Users' section below is also visible, with its own configuration options.

Agregar un valor preestablecido

Paso 7. Seleccione el Table View como formato de salida, como se muestra en la imagen.

The screenshot shows the 'Format' field for the 'Table View of Events' section. The dropdown menu is open, and 'Table View' is selected and highlighted in red. The 'Fields' field is also visible, with the value 'Time, Event, Username, Realm, Di'. The 'Users' section below is also visible, with its 'Format' field also set to 'Table View' and highlighted in red.

Vista de tabla como formato de salida

Paso 8. (Opcional) En el menú de búsqueda, seleccione los atributos que desea utilizar para restringir el informe. Seleccione None si no desea aplicar ninguna restricción de búsqueda.

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::5a3:1370
Start Port		2300
End Port		2500
Description		john
VPN Session Type		AnyConnect IKEv2, AnyConnect SSL, *IKEv2
VPN Group Policy		MyGroupPolicy

Cancel OK

Restricciones de búsqueda

Paso 9. Seleccione el período de tiempo para el que desea generar el informe. Haga clic en Last hour y se abrirá una nueva ventana emergente con opciones de 1 hora, 6 horas, 1 día, 1 mes, etc., como se muestra en la imagen.

Firepower Management Center

Overview / Reporting / Report Template Designer

Reports Report Templates

Report Title: VPN User Activity Report

Generate Advanced Save

Report Sections

Table View of Events

Table: User Activity

Preset: None

Format: [Table View]

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 View]

Search: None

Fields: Count, Username

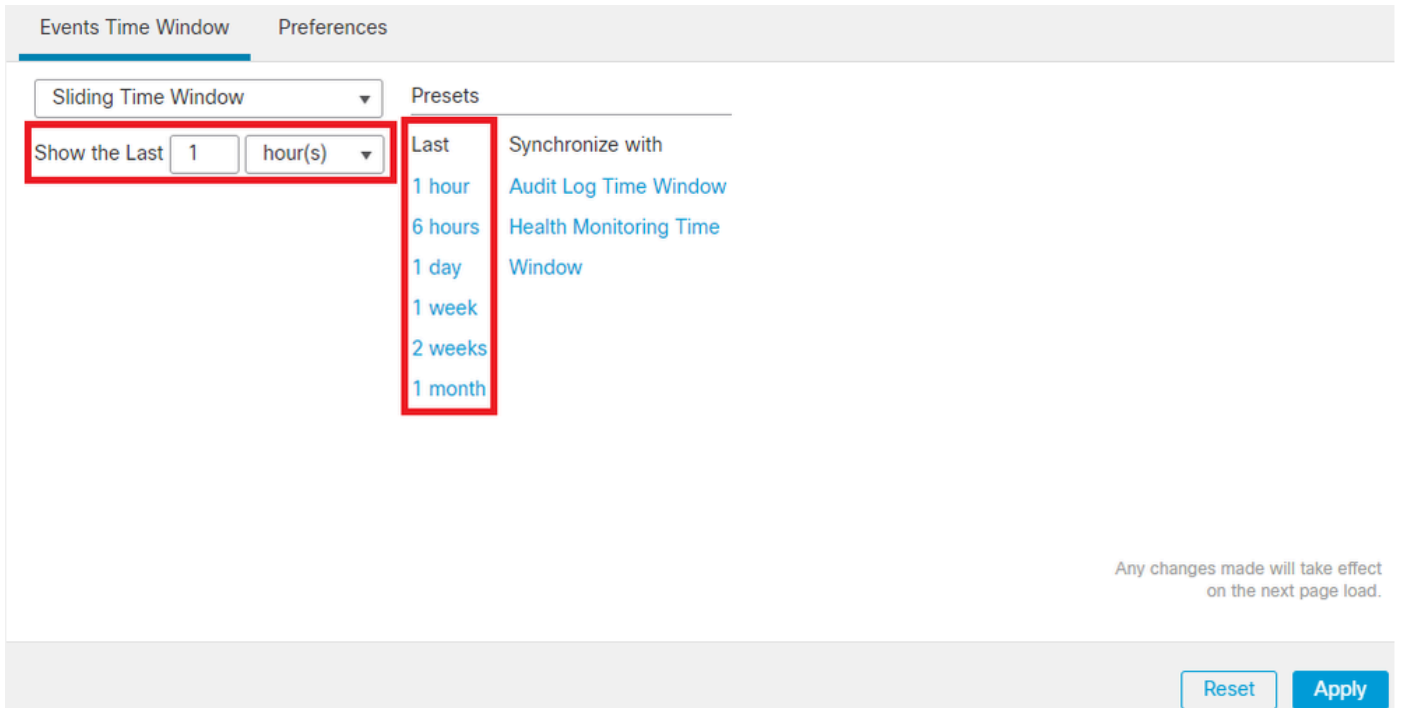
Section Description: \${Time Window}>\${Constraints}

Time Window: Inherit Time Window Last hour

Maximum Results: 10000

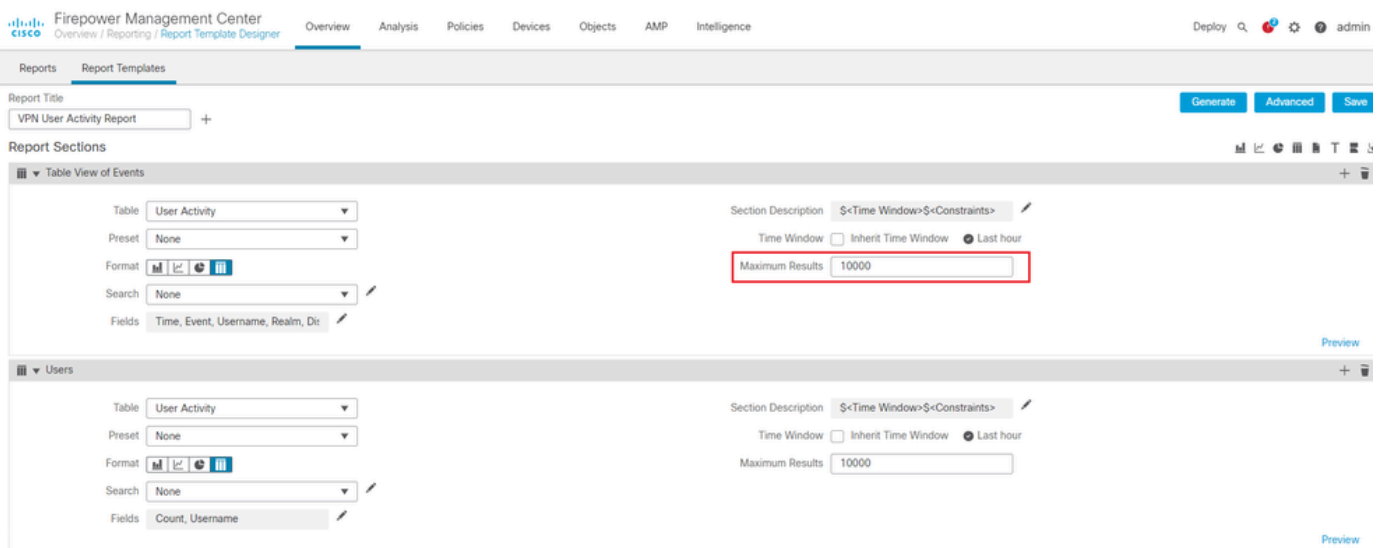
Preview

Seleccionar intervalo de tiempo



Agregar TimeFrame

Paso 10. Para registrar el número específico de resultados, proporcione cualquier valor entre el intervalo de 1 a 400000 en el Maximum Results campo.



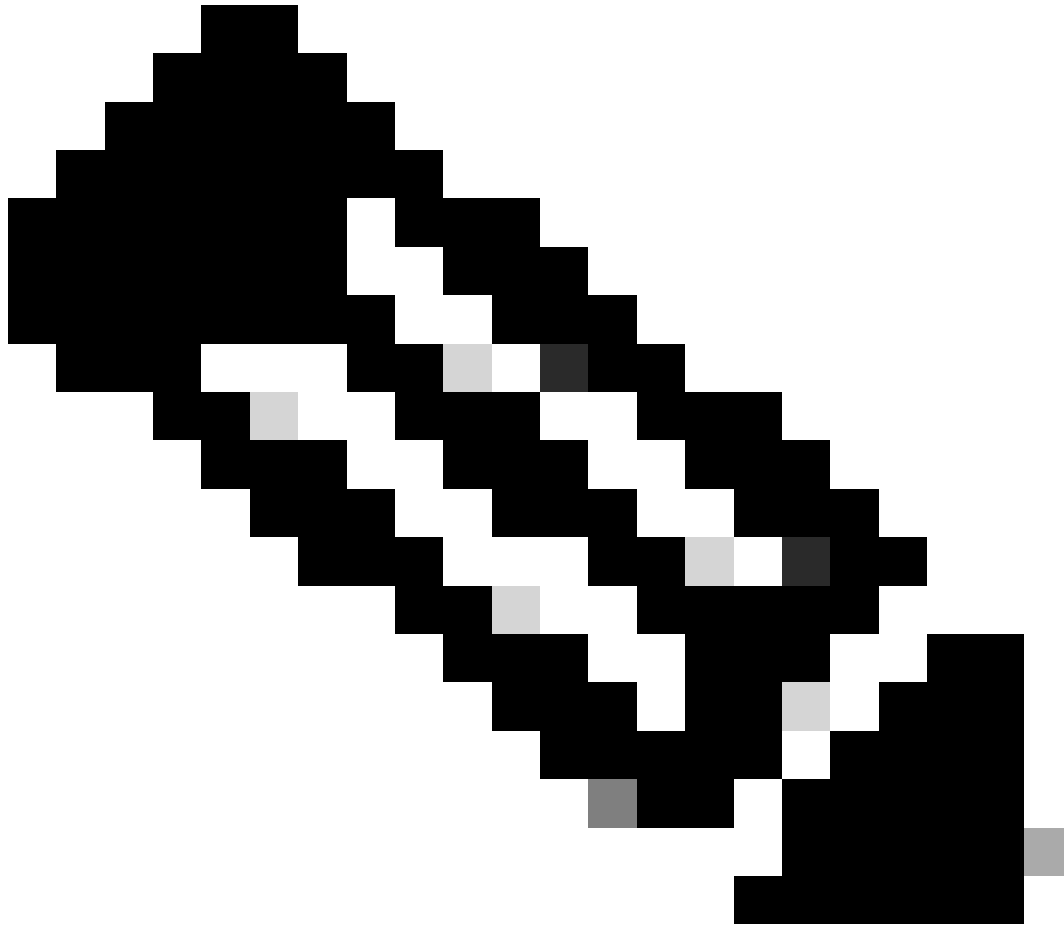
Máximo de resultados para mostrar

Paso 11. Haga clic en el Save botón situado en la parte superior de las secciones del informe para que la plantilla esté lista para su uso.

Guardar informe

Generar informe

Una vez que haya creado y personalizado la plantilla de informe, estará listo para generar el informe. Hay diferentes formatos de salida como HTML, PDF o CSV para ver los datos del usuario.













































Nota: En los informes PDF, no se admiten nombres de archivo que utilicen caracteres Unicode (UTF-8).

Procedimiento

Paso 1. Seleccione Overview > Reporting y haga clic en Report Templates .

Paso 2. Haga clic en el Generate Report icono situado junto a la plantilla que ha configurado, como se muestra en la imagen.

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"		  

Generar vista de informes

Paso 3. Introduzca un nuevo nombre de archivo. Este nombre se utiliza para guardar el informe. Si no introduce un nombre nuevo, el sistema utilizará el nombre por defecto especificado en la plantilla de informe.

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

Agregar nombre de archivo

Paso 4. Elija el formato de salida del informe haciendo clic en: 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!

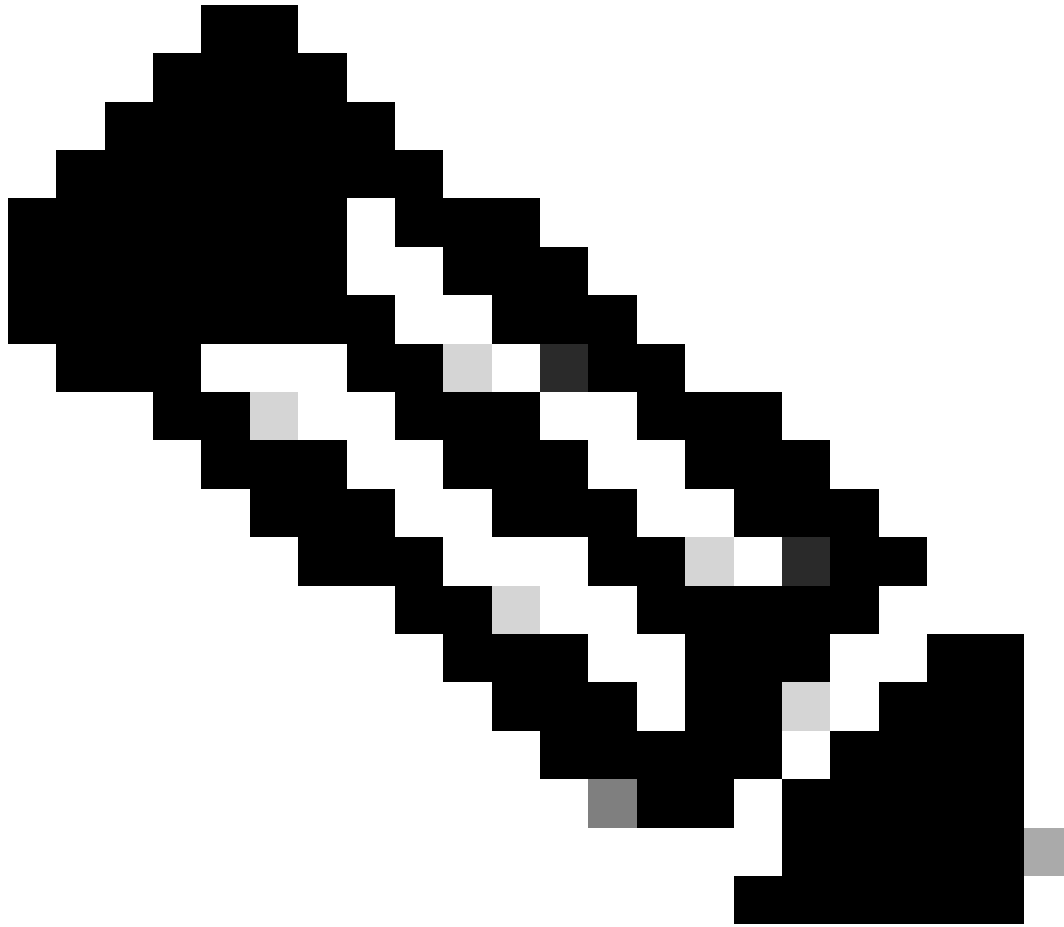


Close

Generate

Seleccionar formato de salida de archivo

Paso 5. (Opcional) Cambie el marco de tiempo global del informe de "Ventana de tiempo". Esto se ignora si "Heredar ventana de tiempo" no se utiliza en la plantilla de informe.



Nota: La configuración de la ventana de tiempo global afecta al contenido de las secciones de informes individuales sólo si están configuradas para heredar la configuración global.

Paso 6. (Opcional) Si el informe generado debe entregarse por correo electrónico, [configure](#) un "host de retransmisión" en el FMC.

Paso 7. Haga clic en Generate y los archivos estarán disponibles para su descarga en "Informes". Para el formato CSV, se creará una carpeta zip con cada sección de la plantilla como un archivo independiente.

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

Generar informe

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	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	2023-11-06 22:09:26	2023-11-06 22:09:27	admin	Local	Successfully Processed

Informe generado

Resultado

Esta sección proporciona la información del informe generado para el usuario de VPN en 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)

Ver informes generados

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).