

Generate FMC Reports for VPN Users

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Configurations](#)

[Generate Report](#)

[Procedure](#)

[Result](#)

Introduction

This document describes how to generate reports which provide at-a-glance views of consolidated information about VPN users, including the current status of users, device types, client OS, client applications, and duration of connections on the Firepower Management Center.

Prerequisites

Requirements

Cisco recommends that you have the knowledge of these topics:

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

Components Used

The information in this document is based on these software versions:

- Cisco FMC for VMware with version 7.x
- AnyConnect Secure Mobility Client 4.x

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The Firepower System provides a flexible reporting system that allows you to quickly and easily generate reports on your Firepower Management Center. You can also design your custom reports from scratch. A report is a document file formatted in PDF, HTML, or CSV with the content you want to communicate

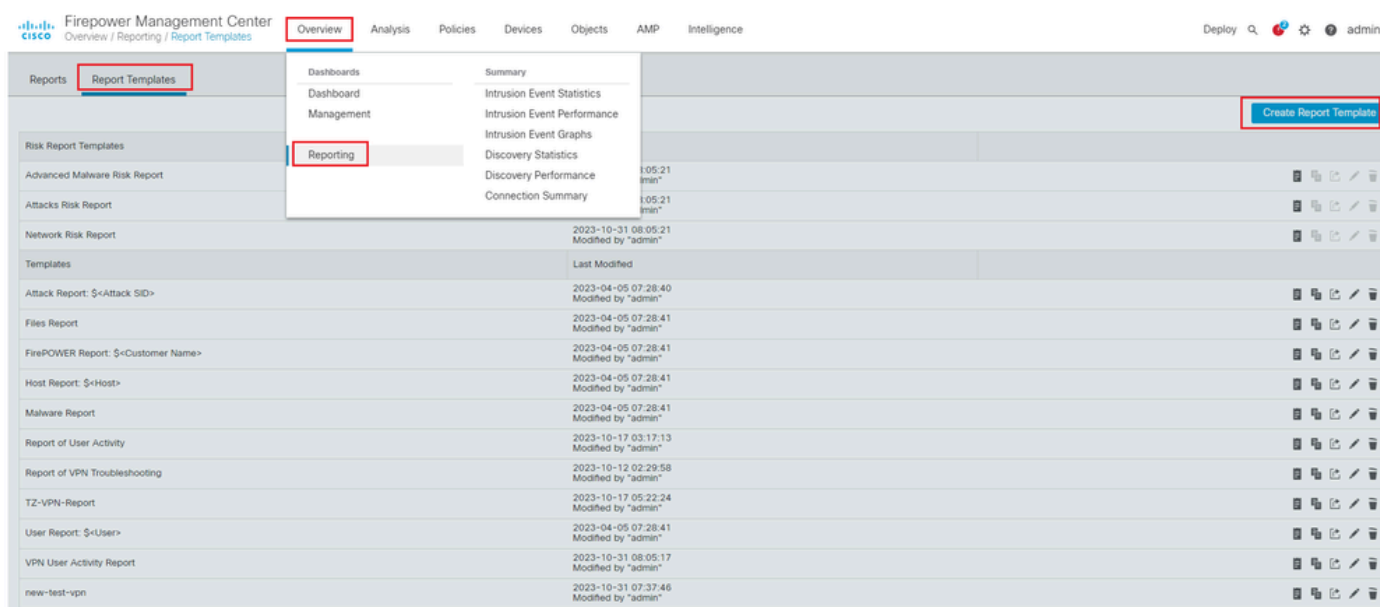
while a report template specifies the data searches and formats for the report and its sections. The Firepower System includes a powerful report designer that automates the design of report templates. You can include field parameters like authentication type, connection duration and so on in a template to expand its usefulness.

Remote access VPNs provide secure connections for remote users, such as mobile users or telecommuters. Monitoring these connections provides important indicators of connection and user session performance at a glance. You must be an Admin user in a leaf domain to perform this task. The Firepower System monitoring capabilities enable you to determine quickly whether remote access VPN problems exist and you can then apply this knowledge and use your network management tools to reduce or eliminate problems for your network and users.

Configure

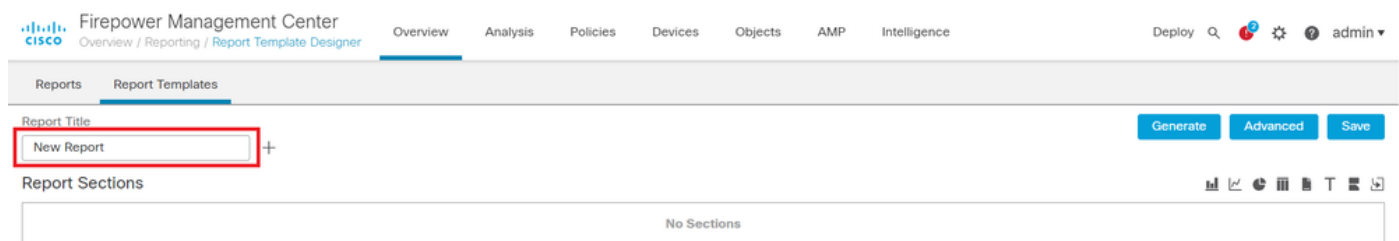
Configurations

Step 1. Select Overview > Dashboards > Reporting > Report Templates and click on Create Report Template as shown in the image.



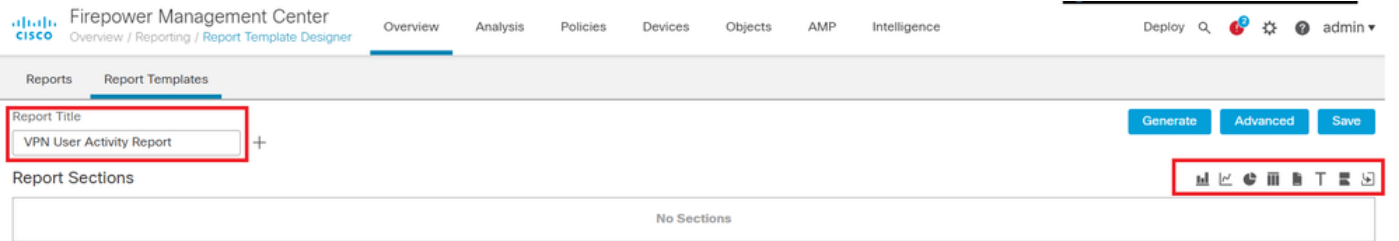
Create Report Template

Step 2. Enter a name for the template in the Report Title field as shown in the image.



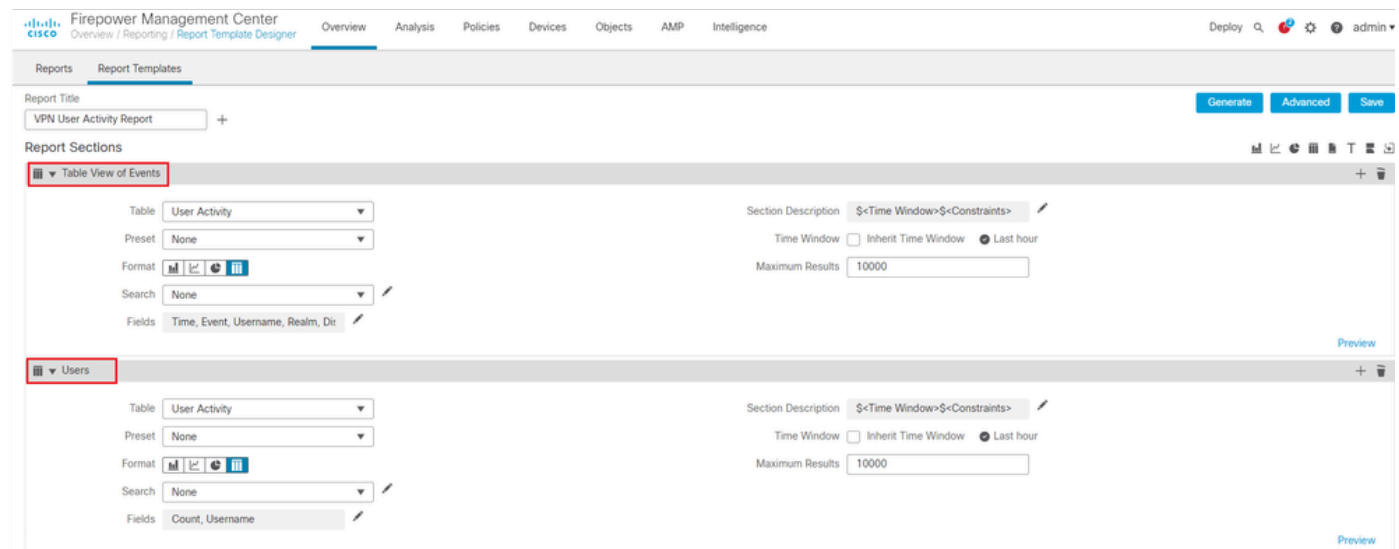
Report Title

Step 3. Select Add Table View from the set of views available on the right side. You can also use charts such as bar charts, line charts, pie charts, and so on as per your requirements.



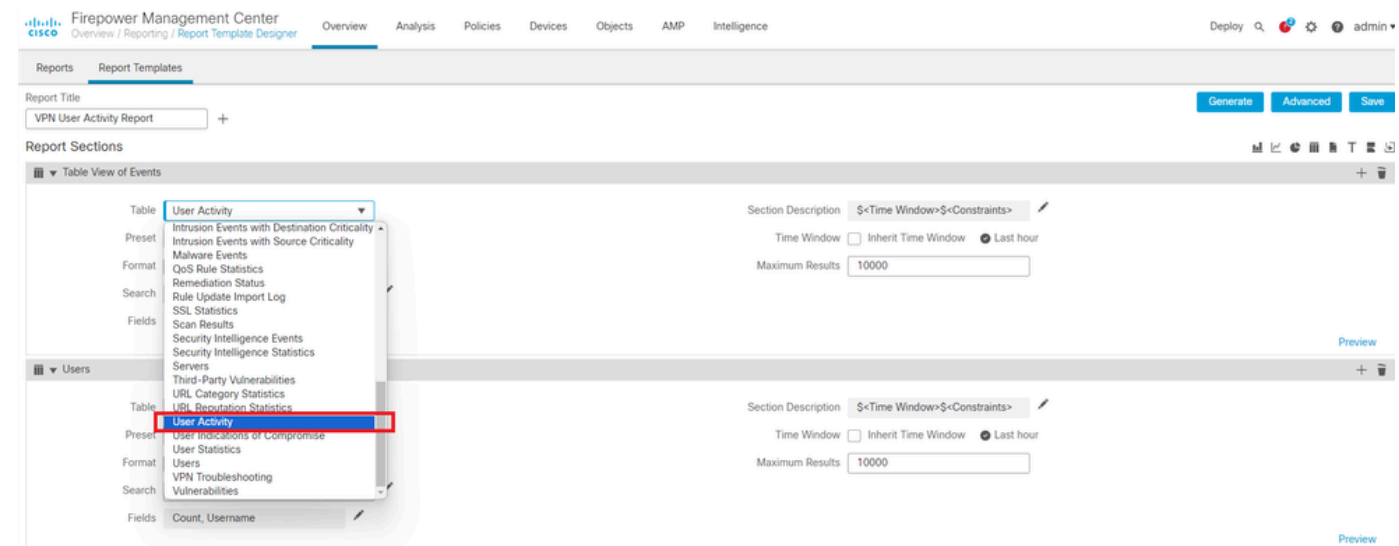
Add Table View

Step 4. Enter a title for the section in the Report Section Title field. Here, Table View of Events and Users table views have been added as shown in the image.



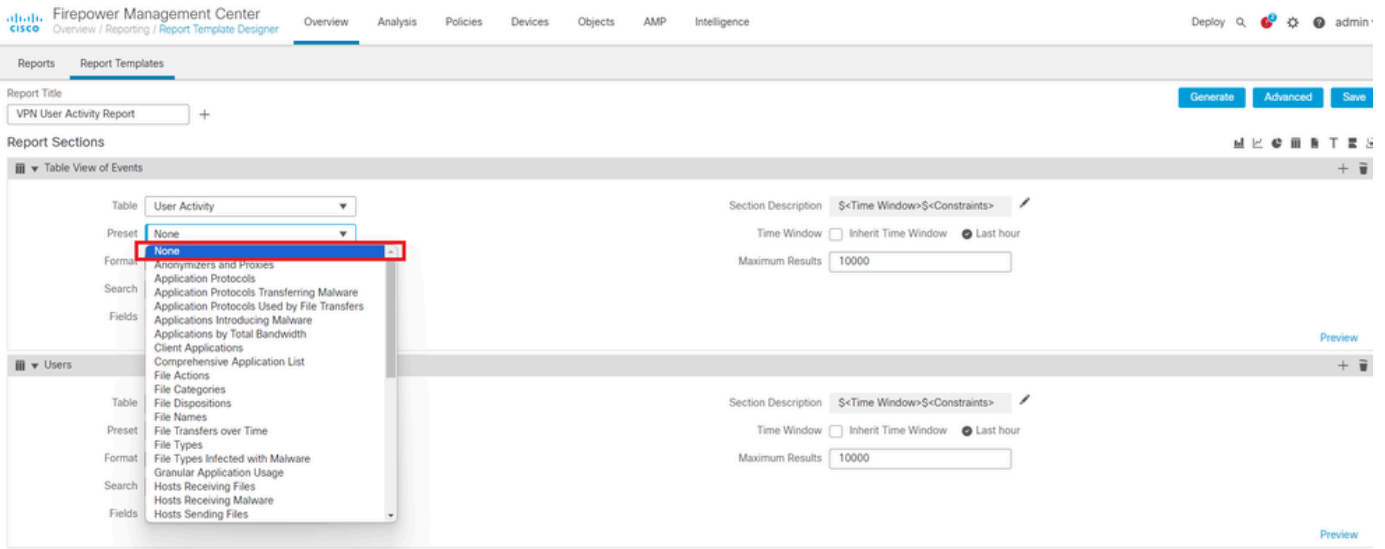
Title for Report Section

Step 5. Select User Activity under the Table drop-down menu as shown in the image.



Select User Activity

Step 6. Choose a Preset value if required, otherwise, keep it as None .



Add a Preset Value

Step 7. Select the **Table View** as the output format as shown in the image.

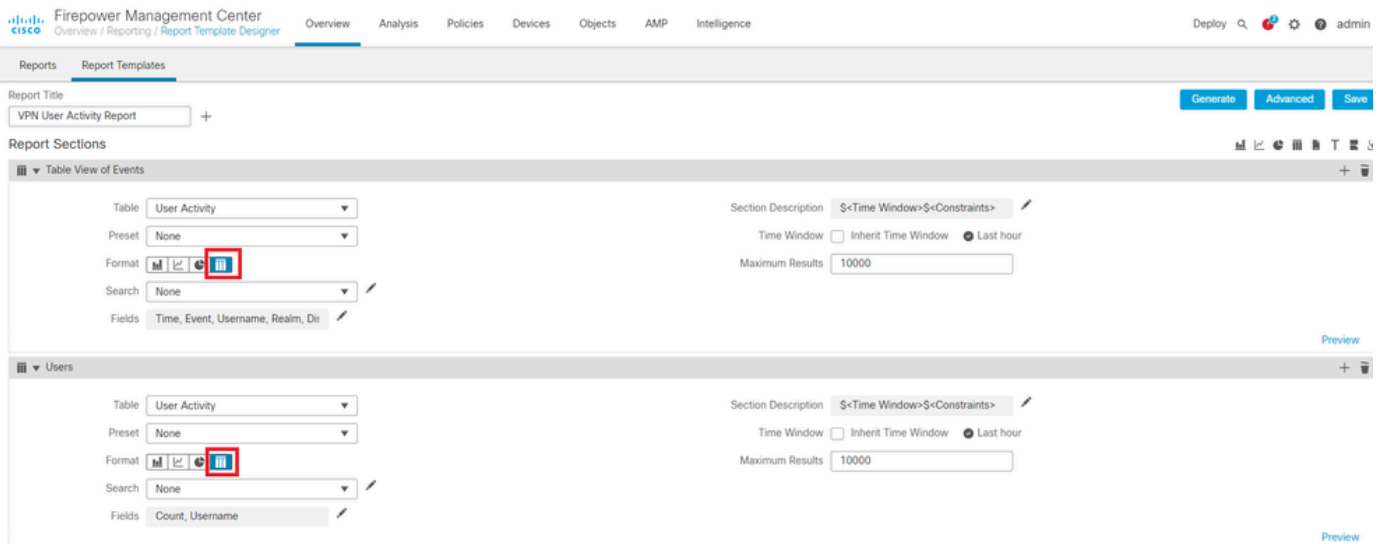


Table View as Output Format

Step 8. (Optional) From the search menu, select the attributes you want to use to constrain the report. Select **None** if you do not want to enforce any search constraints.

Search Editor

Search Information

Table: User Activity

Saved Searches: None

Search Information

Event		New User, Login, Delete, Dropped
Username		jamith
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		jdce
VPN Session Type		AnyConnect IKEV2, AnyConnect SSL, *IKEV2
VPN Group Policy		MyGroupPolicy

Cancel OK

Search Constraints

Step 9. Select the time frame for which you want to generate the report. Click on **Last hour** and a new pop-up window will open with options of 1 hour, 6 hours, 1 day, 1 month, and so on as shown in the image.

Firepower Management Center

Overview / Reporting / Report Template Designer

Overview Analysis Policies Devices Objects AMP Intelligence

Reports Report Templates

Report Title: VPN User Activity Report

Generate Advanced Save

Report Sections

Table View of Events

Table: User Activity	Section Description: \$<Time Window>\$<Constraints>
Preset: None	Time Window <input type="checkbox"/> Inherit Time Window <input checked="" type="radio"/> Last hour
Format: [Icons]	Maximum Results: 10000
Search: None	
Fields: Time, Event, Username, Realm, Di:	

Preview

Users

Table: User Activity	Section Description: \$<Time Window>\$<Constraints>
Preset: None	Time Window <input type="checkbox"/> Inherit Time Window <input checked="" type="radio"/> Last hour
Format: [Icons]	Maximum Results: 10000
Search: None	
Fields: Count, Username	

Preview

Select Time Frame

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

Add TimeFrame

Step 10. To record the specific number of results, provide any value between the range of 1 - 400000 in Maximum Results field.

Firepower Management Center Overview Analysis Policies Devices Objects AMP Intelligence

Reports Report Templates

Report Title VPN User Activity Report

Generate Advanced Save

Report Sections

Table View of Events

Table User Activity

Preset None

Format

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

Search None

Fields Count, Username

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

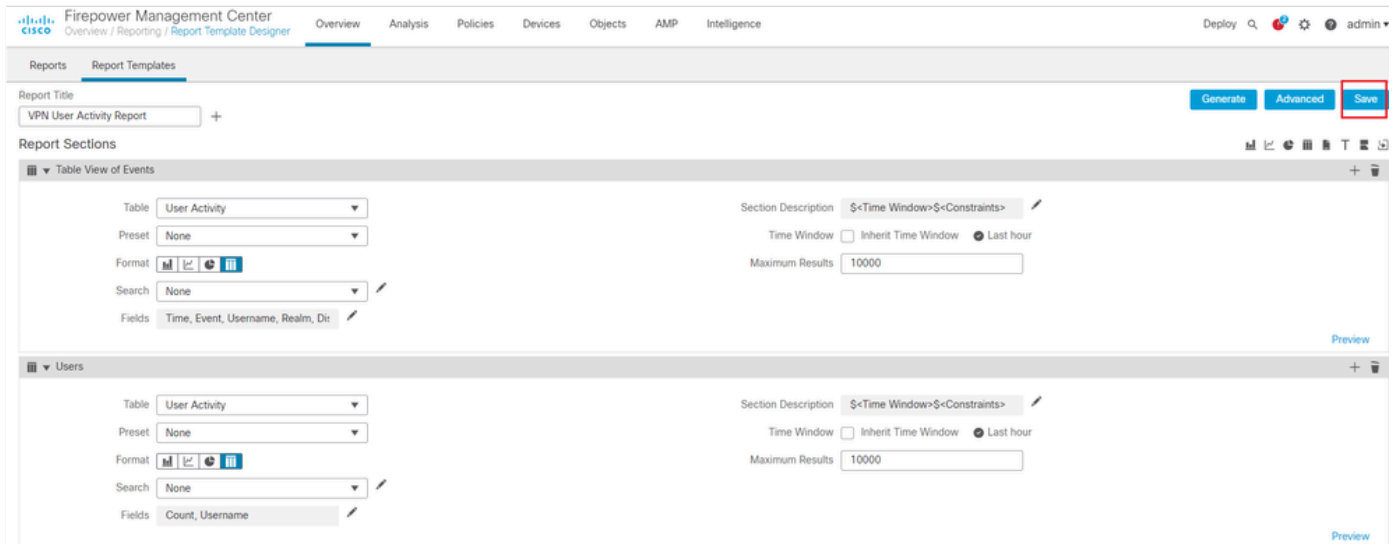
Time Window Inherit Time Window Last hour

Maximum Results 10000

Preview

Maximum Results to display

Step 11. Click on the Save button at the top of the report sections for the template to be ready for use.



Save Report

Generate Report

Once you create and customize your report template, you are ready to generate the report. There are different output formats like HTML, PDF or CSV to view the user data.



























































Note: For PDF reports, file names using Unicode (UTF-8) characters are not supported.

Procedure

Step 1. Select [Overview > Reporting](#) and click on [Report Templates](#) .

Step 2. Click on the [Generate Report](#) icon next to the template that you have configured as shown in the image.

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"		   

Generate Reports View

Step 3. Enter a new File Name. This name is used to save the report. If you do not enter a new name, the system uses the default name specified in the report template.

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

Add Filename

Step 4. Choose the output format for the report by clicking: HTML, PDF, or 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

Select File Output Format

Step 5. (Optional) Change the global time frame for the report from "Time Window". This gets ignored if "Inherit Time Window" is not used in the report template.



Note: Setting the global time window affects the content of individual report sections only if they are configured to inherit the global setting.

Step 6. (Optional) If the generated report has to be delivered via email, [configure](#) a "Relay Host" on the FMC.

Step 7. Click on `Generate` and files will be available for download under "Reports". For CSV format, a zip folder will be created with each section of the template as a separate file.

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

Generate 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	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

Report Generated

Result

This section provides the information of the report generated for the VPN user in a PDF format.

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)

[View Generated Reports](#)